

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Национальный исследовательский ядерный университет
«МИФИ»

**Материалы
VII Международной
научно-практической конференции
Международного сетевого института в сфере
ПОД/ФТ
«УГРОЗЫ И РИСКИ ФИНАНСОВОЙ
БЕЗОПАСНОСТИ
В КОНТЕКСТЕ ЦИФРОВОЙ
ТРАНСФОРМАЦИИ»**

24-26 ноября 2021 г., Москва

Москва 2021

УДК 330.47:005.334:004.9(06)
ББК 65.012
М 43

Материалы VII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ «УГРОЗЫ И РИСКИ ФИНАНСОВОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ», 24-26 ноября 2021 г., Москва. М.: НИЯУ МИФИ, 2021. - 820 с.

В сборнике рассматриваются актуальные проблемы современных трендов в сфере борьбы с отмыванием денег и представление новейших инициатив и проектов по развитию права, экономики и ИТ в сфере ПОД/ФТ. Ключевые темы, которые рассмотрены в сборнике:

- цифровизация экономики – новый вызов финансовому мониторингу и безопасности государства;
- научно-образовательные платформы и сервисы в целях ПОД/ФТ
- социально-экономическая природа рисков и угроз глобальной экономике и механизмы противодействия им;
- тенденции в сфере борьбы с отмыванием денег: криптоэкономика и криптофинансы, блокчейн-преступность;
- искусственный интеллект: современные приложения в контексте ПОД/ФТ;
- регуляторные технологии в сфере ПОД/ФТ: цифровой иммунитет
- финансовое мошенничество: растущий риск финансовых преступлений

Для специалистов в области технических и общественных наук, преподавателей, аспирантов, студентов вузов.

Редколлегия: А.Н. Норкина, И.П. Комиссарова, В.Г. Когденко, Н.В. Морозов, П.Ю. Леонов.

Материалы издаются в авторской редакции

Получены до 24.11.2021

ISBN 978-5-7262-2839-6

© НИЯУ МИФИ, 2021

© Авторы статей, 2021

Подписано в печать 10.12.2021. Формат 60х84 1/16.

Печ. л. 51,25.

*Национальный исследовательский ядерный университет
«МИФИ»*

115409, Москва, Каширское ш., 31

СОДЕРЖАНИЕ

<i>Азиатский банк развития в региональной системе ПОД и ФТ</i> С.С. Матвеевский	10
<i>Анализ вероятных макроэкономических последствий при принятии криптовалюты как основной денежной единицы</i> С. Мукхерджи, А.В. Трушко, Н.В. Морозов	18
<i>Анализ добросовестности поставщика с помощью системы SAP S4/HANA</i> Ю.И. Мещерякова, Т.А. Соколова	29
<i>Анализ перспектив развития предприятий агрохимической отрасли на примере ПАО «Уралкалий»</i> С.И. Метонидзе, Е.В. Савин, Т.Н. Бочкарева	37
<i>Анализ перспектив развития трубной промышленности и ее роль в обеспечении экономической безопасности Российской Федерации</i> А.А. Стоянова, Т.Н. Бочкарева	51
<i>Анализ применения ESG-принципов в производственном учёте организаций радиоэлектронной промышленности</i> Л.В. Пермитина	61
<i>Анализ применимости модифицированной модели Бениша для отчетности российских компаний</i> Е.А. Кузьмина, Д.Р. Хамитов, Е.В. Савин, Н.С. Белогина	69
<i>Анализ современных подходов разработки криптовалют для их использования в реализации национальной цифровой валюты</i> Ю. Волянский, Ю.В. Терехова	82
<i>Анализ экономических характеристик организаций электронной промышленности</i> А.А. Санжаров	90
<i>Бережливое регулирование: аудиторы и ПОД/ФТ/ФРОМУ</i> М.Ю. Андронов, П.Ю. Леонов	102
<i>Будущее профессий и производительности труда через призму современных цифровых решений</i> В.В. Лымарь	113
<i>Виды и способы оценки эффективности работников департамента внутреннего аудита</i> Н.С. Торопчин	122
<i>Влияние корейской музыкальной субкультуры на экономику Южной Кореи</i> Р.Ч. Авшалумова, Ю.В. Никитинская	129
<i>Влияние процесса цифровизации на развитие малого и среднего бизнеса, его государственного регулирования и поддержку</i> М.Р. Лихачев, Д.Б. Давыдов, А.Н. Майорова	135

<i>Влияние цифровых национальных валют на банковский сектор</i> В.А. Романовский, А.В. Трушко, Н.В. Морозов	143
<i>Влияние ESG рисков на деятельность финансового сектора</i> А.В. Горюнова, В.С. Царева, В.И. Прусова	152
<i>Внедрение риск-ориентированного подхода в кредитные организации</i> Н.В. Александров, Д.А. Шульгин, Д.В. Домашова	161
<i>Внешний и внутренний аудит в целях ПОД/ФТ/ФРОМУ</i> П.М. Абдуллаева, С.В. Сергеев, Н.С. Белогина	174
<i>Внутренний контроль как мера противодействия финансированию терроризма в некоммерческом секторе</i> А.А. Галий, В.М. Сушков, П.Ю. Леонов	183
<i>Выявление симптомов манипулирования финансовой отчетностью с помощью закона Бенфорда на примере компании Enron</i> В.М. Сушков, П.Ю. Леонов	194
<i>Информационная безопасность: современный аспект</i> Ф.Э. Меджитова, В.В. Ворошило	205
<i>Информационные технологии в управлении маркетинговой деятельностью предприятия</i> М.П. Башан, Е.Р. Мысева	212
<i>Информационные технологии как маркетинговый инструмент развития в сфере оценки эффективности бизнес-плана</i> А.С. Лискина, Е.Р. Мысева	218
<i>Информационные технологии как маркетинговый инструмент развития в сфере цифровых развлечений</i> С.А. Михайлов, Е.Р. Мысева	227
<i>Информационные технологии, как маркетинговый инструмент развития в сфере оптимизации бизнес-процессов</i> В.А. Чекунова, А.Н. Норкина	232
<i>Использование инструментов искусственного интеллекта при разработке программного обеспечения в контексте ПОД/ФТ</i> В.Р. Баринов, Н.В. Баринова	241
<i>Использование средств визуального анализа при расследовании операций с виртуальными активами</i> А.К. Вязникова, А.В. Кирина, Д.В. Домашова, Е.Е. Писарчик	247
<i>Исследование влияния социально-экономических показателей стран мира на незаконный оборот наркотических средств</i> Т. Раканов, Д.В. Домашова	259
<i>Исследование отраслевых факторов доходности и рисков (на примере электронной промышленности)</i> В.Г. Когденко, Т.К. Винокурова	274

<i>Кибербезопасность в Республике Беларусь</i> Д.А. Алябьева, У.Ю. Басалыга, В.В. Позняков	282
<i>Комплекс мер по противодействию угрозам финансовой безопасности России с учетом взаимовлияния уязвимостей финансовых институтов и домохозяйств</i> Е.Н. Алифанова, Ю.С. Евлахова, Л.И. Ниворожкина, А.А. Трегубова	288
<i>Комплексная оценка специалиста по финансовой безопасности как основа для построения его компетентностной модели</i> А.Н. Столярова, Д.С. Петросян, А.Д. Петросян	295
<i>Криптовалюта как угроза финансовой безопасности</i> Э.Э. Османова, О.Г. Блажевич	300
<i>Криптовалюта: повторение кризиса или современное средство обмена?</i> Е.М. Бурнашева, Д.Д. Гольцов, А.А. Хоченко, А.К. Завалишина	307
<i>Международный опыт построения системы ПОД/ФТ в современных условиях</i> В.И. Прасолов	314
<i>Методологическая основа SOC</i> В.А. Рычков, В. Давыденко, А.М. Габдуллин	334
<i>Методы и технологии обеспечения кибербезопасности в финансово-экономической сфере</i> Д.В. Капулин, Е.А. Чжан, В.И. Вайнштейн	341
<i>Механизмы противодействия незаконному использованию криптовалют в системе ПОД/ФТ</i> С.А. Сапронов, Е.Н. Алифанова	348
<i>Моделирование профиля поведения пользователя веб-приложения на основе интеллектуального анализа разноуровневых журналов</i> И.К. Егоров, В.Ю. Радыгин	354
<i>Мониторинг рисков IT- безопасности как навигатор ESG-устойчивости цифровой экономики и финансов</i> Н.А. Казакова, А.А. Петюкова	360
<i>Мошенничество с криптовалютой</i> П.М. Аскерко, И.Д. Шикунец, В.В. Позняков	368
<i>Налоговое бремя и его влияние на экономику государства</i> А.П. Николаева, А.Н. Майорова	375
<i>Новые способы отмывания денег в сфере медицины в период COVID-19</i> Д.Ю. Елкина, Д.С. Павлов	380
<i>О специфических особенностях государственного финансового контроля в условиях пандемии COVID-19</i> А.Е. Сорокин, А.С. Кропачева, Е.В. Скребец	386

<i>Обеспечение безопасности банкоматов в условиях цифровизации</i> Т.И. Карабчук, О.Г. Блажевич	393
<i>Обеспечение кибербезопасности в банковской сфере в условиях цифровой трансформации</i> К.Ю. Мяделец, В.В. Позняков	400
<i>Обзор биометрических криптосистем и отменяемой биометрии</i> А.А. Новопавловский, К. Верейкин	407
<i>Обзор ERP-систем в контексте повышения прозрачности деятельности крупных компаний</i> А.В. Михеева, П.Ю. Леонов	413
<i>Обзор ERP-систем в контексте экономической безопасности бизнеса</i> Н.М. Мусин, П.Ю. Леонов	421
<i>Обнаружение поддельных и не поддельных DDoS-атак и их отличие от слэйдот-эффекта</i> В.А. Рычков, Д.М. Якупов, В. Давыденко	429
<i>Описание проведения оценки рисков финансирования распространения оружия массового уничтожения и предложение мер по их минимизации</i> Д.Д. Жусупов	433
<i>Основные тенденции развития FinTech в Российской Федерации</i> Н.С. Колпакова	445
<i>Основы повышения эффективности производства на примере ООО «ЮГСТРОЙИНВЕСТ-КУБАНЬ» в условиях цифровой трансформации</i> О.Д. Ермоленко, М.Н. Мурзинова	451
<i>Оценка и управление финансовыми рисками компании ПАО «НОВАТЭК»</i> Д.С. Журавлёв	457
<i>Оценка риска наличия скрытых доходов в российских домашних хозяйствах на основе модели Писсаридеса-Вебера</i> Л.И. Ниворожкина, А.А. Трегубова	464
<i>Оценка финансовых рисков компаний нефтегазового сектора на примере группы компаний «Татнефть»</i> В.В. Жорова	470
<i>Оценка ESG стратегии ОАО «РЖД»</i> В.С. Книга	478
<i>Первоочередные меры по развитию и обеспечению финансовой безопасности экспортноориентированных малых предприятий торговли в Российской Федерации</i> Р.М. Богданова, А.С. Медведева	487

<i>Положительные и отрицательные аспекты обращения криптовалют</i> М.Д. Исмоилова, Р.И. Каюмов	492
<i>Постпандемическое восстановление мирового рынка прямых иностранных инвестиций и цифровизация в экономике</i> А.Л. Сапунцов	499
<i>Практические аспекты оценки соответствия требованиям защиты информации Банка России</i> А.В. Глазков, О.А. Иванов, И.Ю. Червяков	505
<i>Применение анализа голоса и речи в защите от социальной инженерии</i> В.А. Рычков, В. Давыденко, А.В. Перепечаев	513
<i>Применение искусственных нейронных сетей для прогнозирования девиантной деятельности кредитных организаций как субъектов финансового мониторинга</i> А.С. Приказчикова, В.В. Иванов	517
<i>Применение методов интеллектуального анализа данных для управления финансовыми рисками компании</i> Ж.Д. Даулетханова	526
<i>Применение методов машинного обучения в целях выявления мошеннических транзакций</i> А.В. Кирина, Д.В. Домашова	532
<i>Применение методов машинного обучения и глубокого обучения при решении задачи защиты информации в сфере облачных технологий</i> В.А. Рычков, В. Давыденко, И.П. Чурилов	539
<i>Проблемы безопасности бесконтактных платежей</i> Э.Р. Аблитаров	546
<i>Проблемы идентификации финансовых вложений в учетно-аналитических целях</i> Д.И. Норкина, Н.С. Белогина	552
<i>Проблемы обеспечения финансовой безопасности хозяйствующего субъекта в условиях аутсорсинга бухгалтерских услуг</i> А.Н. Кизиллов	562
<i>Проблемы цифровизации национальных валют</i> М.А. Лынный, В.В. Ворошило	568
<i>Пути обнаружения и предотвращения киберугроз</i> В.М. Гапанович, В.Н. Чернова, А.С. Деревенская, С.Е. Климова	576
<i>Разработка аналитических индикаторов на основе дерева решений для выявления признаков манипуляций в финансовой отчетности на примере строительного сектора</i> А.К. Завалишина	585

<i>Разработка финансовой структуры торговой организации (в рамках разработки системы бюджетирования)</i> А.Б. Романенко, И.П. Комиссарова	592
<i>Риски использования анонимных виртуальных активов и виртуальных валют для легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма</i> С.А. Бойко, И.В. Кольца, М.А. Степаненкова, В.А. Корчинская	604
<i>Риски ОД/ФТ/ПРОМУ и инструменты управления ими на уровне субъектов первичного финансового мониторинга Российской Федерации</i> С.Е. Климова	617
<i>Риски финансирования экспортной деятельности многонациональных предприятий ЮАР</i> С.В. Ефименко, А.Л. Сапунцов	628
<i>Роботизация бизнес-процессов предприятия, как инструмент информационной логистики</i> А.Н. Норкина, А.Р.Азизова	634
<i>Санкционный комплаенс как новый элемент КУС</i> В.Н. Морозова, А.А. Хоченко, Н.В. Морозов	642
<i>Сервисы веб-аналитики как инструмент маркетинга</i> М.М. Джураев, Е.Р. Мысева	648
<i>Современные инструменты по выявлению подозрительных клиентов</i> А.А. Суркова, Д.В. Домашова	656
<i>Современные информационные технологии в обеспечении информационной безопасности логистических процессов</i> В.Г. Гредычан, А.Н. Норкина	663
<i>Современные проблемы информационной безопасности в разработке программного обеспечения</i> А.А. Тулеубаева, А.Н. Норкина	670
<i>Создание цифровой среды взаимодействия банка и корпоративных клиентов</i> Н.Н. Корсунова , С.А. Уразова	677
<i>Состояние мирового рынка аудиторских услуг и его тенденции развития</i> С.В. Сергеев, П.М. Абдуллаева, Н.С. Белогина	692
<i>Состояние, перспективы и риски развития рынка металлов платиновой группы в постпандемийной экономике</i> И.А. Степанов	700
<i>Социальная инженерия и конструирование «несовершенного пользователя» в кибербезопасности</i> А.А. Новопавловский, К. Верейкин	709

<i>Социальная инженерия, как угроза экономической безопасности предприятия</i> А.В. Морозов, В.А. Рычков, В. Давыденко	719
<i>Социальные сети и мессенджеры как площадка для кибервойны с обществом и государством</i> Д.А. Авдеев, В.Ю. Радыгин	725
<i>Тактические и стратегические цели аудита мирового масштаба</i> С.В. Сергеев, Д.В. Сергеев, Н.С. Белогина	735
<i>Торгово-экономические связи России с Германией</i> А.В. Анисимова, М.А. Трубачева, А.Н. Майорова	741
<i>Управление ESG рисками крупных хозяйствующих субъектов на примере компании ПАО «ФосАгро»</i> А.В. Лукьянченко	754
<i>Учетно-контрольная среда компании в условиях цифровизации экономики</i> Ч.А. Нуралиева, О.К. Игликов	762
<i>Формирование встроенной модели управления рисками на предприятии</i> Е.В. Усман	769
<i>Франчайзинг как инструмент стратегического управления и развития в сфере фаст-фуда на примере Макдоналдс</i> М.В. Черненко, Т.Н. Бочкарева	775
<i>Цифровая трансформация в деятельности региональных интеграционных объединений (на примере африканского региона)</i> Е.В. Дробот	783
<i>Цифровой рубль как новая форма российской национальной валюты</i> В.А. Кузнецова, Т.Н. Агапова	793
<i>Цифровой рубль: риски и обеспечение безопасного функционирования</i> Н.К. Норец	799
<i>Due diligence как фактор управления рисками в сделках слияний и поглощений</i> М.Д. Парфенова	805
<i>ESG-трансформация</i> А.А. Николаев, Е.Р. Гордеева, В.Г. Когденко	812

Азиатский банк развития в региональной системе ПОД и ФТ

С.С. Матвеевский
доцент Департамента банковского дела и финансовых рынков
Финансового университета, Москва
E-mail: ssmatveevskii@fa.ru

Аннотация: Дано описание Азиатского банка развития, включая используемый им цикл проекта. Приведены экономические результаты его деятельности в 2020г., описан реализуемый план цифровой трансформации банка. Банк действует в странах Азиатско-Тихоокеанского региона, что определило важную роль банка в методологической и информационной поддержке ПОД и ФТ в странах региона. Особое значение придается небанковским финансовым организациям региона, рейтинговой оценке уровня внедрения ими международных стандартов ПОД и ФТ.

Ключевые слова: банк развития, проект, цифровая трансформация, методология ПОД и ФТ, рейтинговая оценка, небанковские финансовые организации.

Asian development bank in the regional AML and FT system

Abstract: A description of the Asian Development Bank is given, including the project cycle it uses. The economic results of its activities in 2020 are given, the plan for the digital transformation of the bank is described. The Bank operates in the countries of the Asia-Pacific region, which determined the important role of the bank in the methodological and information support of AML and FT in the countries of the region. Particular importance is attached to non-bank financial institutions in the region, the rating assessment of the level of their implementation of international AML and FT standards.

Keywords: development bank, project, digital transformation, AML and FT methodology, rating assessment, non-bank financial institutions.

Банки развития (БР) широко распространены во всем мире (в настоящее время, их количество превышает 700 штук, включая Мировой банк), создаются, как правило, государством и реализуют национальные планы развития, важные проекты в различных отраслях экономики. Принципиальное отличие БР от обычных коммерческих банков в том, что БР не ориентированы на получение прибыли (хотя БР не должен терпеть убытки), работают по планам государства [1].

Все БР принято делить на национальные и многосторонние. Национальные БР создаются правительством одного государства (хотя есть и БР с частным капиталом) и им же финансируются (например, в Индии Эксимбанк регулярно получает вливания денежных средств в капитал из бюджета); в России действует ВЭБ.РФ, который также регулярно получает поддержку из федерального бюджета). Многосторонние БР, например, Африканский и Азиатский БР (АБР) были созданы десятками государств). Многосторонние БР действуют во всех странах-участницах (например, АБР действует во всех странах Азиатско-Тихоокеанского региона (АТР)).

Основное предназначение как национальных, так и многосторонних БР – это финансирование проектов или программ в экономике или социальной сфере, которые не хотят или не могут финансировать классические финансовые институты (это связано с высокими рисками, возможными убытками). Во время кризисов, именно БР «заменяют» коммерческие банки на рынке кредитования предприятий (антициклическая функция БР) [2].

Реализация проектов связана с циклом проекта, который предполагает выполнение следующих этапов:

1. Разработка (или обновление) стратегии партнерства с регионом или со страной. БР, как правило, готовит для каждого региона или страны среднесрочную стратегию развития и операционную программу действий (определяются отрасли и районы, в которых целесообразно реализовывать проекты, определяются последовательность проектов). В рамках данного этапа проводятся необходимые экономические и иные исследования, могут привлекаться консалтинговые фирмы. Стратегия партнерства всегда разрабатывается в тесном контакте с руководством района (правительством страны), другими заинтересованными участниками и завершается подготовкой «дорожной карты» операций.

2. Подготовка проекта. Данный этап предполагает, в свою очередь, два раздела:

- идентификацию проекта. Как правило, БР нанимает внешних консультантов для подготовки технико-экономического обоснования проекта (консультанты обладают необходимым опытом подготовки и реализации проектов в соответствующей отрасли). Внешние консультанты действуют совместно с руководством района или страны, сотрудничают с другими заинтересованными организациями и предприятиями. Анализируется влияние проекта на окружающую среду, население и пр.; если проект требует переселения людей или может негативно повлиять на окружающую среду или коренные народы, на этом этапе готовятся определенные защитные меры,

- юридическую экспертизу. БР, его специалисты, обеспечивают изучение осуществимости проекта (оценка технических, финансовых, экономических, экологических, маркетинговых и управленческих

особенностей проекта). Одновременно подробный анализ всех рисков проекта, его чувствительности к экономическим и иным внешним характеристикам.

3. Утверждение проекта. Представители БР, местного руководства проводят переговоры о кредите, согласуют текст документов и приходят к соглашению по экономическим и техническим характеристикам проекта. Итоговые документы утверждаются руководством БР и подписываются руководством района (правительством страны). Кредитное соглашение вступает в силу после выполнения определенных юридических требований, например, реализации софинансирования.

4. Реализация. Проект реализуется независимым исполнительным агентством (не связано с БР) в соответствии с согласованными графиком и процедурами (расходы, связанные с услугами агентства учитываются на этапе подготовки проекта). Все подготовительные работы по конкретному проекту рекомендуется завершить до переговоров по кредиту, за исключением подписания контрактов. Подразделения Банка анализируют процесс реализации проекта, включая постоянный мониторинг исполнения бизнес-плана, следят за достижением целей развития в районе (или регионе), сотрудничая как с заемщиком, так и исполнительным агентством. Срок реализации проекта, обычно, составляет от двух до пяти лет (разные БР могут использовать различные интервалы времени). Сотрудники БР контролируют реализацию проекта лично, посещая его несколько раз в течение года.

5. Завершение проекта и оценка. Данный этап очень важен, т.к. позволяет оценить эффективность использования ресурсов, достижение поставленных целей. После завершения работ по проекту (включая оказание технической помощи), БР готовит отчет о завершении проекта (время подготовки может составлять до 2-3 лет). В соответствии с используемыми БР процедурами, выполняется оценка не только экономических и финансовых характеристик проекта (использование экономического и финансового анализов), но также оцениваются субъективные показатели, которые использует данный БР (как правило, они согласованы с правительством страны или стран) [3].

Азиатский банк развития (АБР) был создан 24 ноября 1966 г. в Токио (Япония). АБР был основан азиатскими лидерами, которые считали, что региональное сотрудничество, дополненное международными финансовыми ресурсами, поможет ускорить развитие в Азии. Предполагалось, что азиатские страны должны соединиться вместе, что поможет способствовать прогрессу; кроме этого, существовало понимание того, что необходимы дополнительные ресурсы «как изнутри, так и за пределами региона» для содействия развитию и была надежда, что создание сильного и надежного регионального банка обеспечит

эффективное использование указанных ресурсов и достижение поставленных целей.

Необходимо отметить, что именно благодаря деятельности АБР в течение последнего десятилетия, на азиатские страны приходится более 50% мирового экономического роста. Если темпы роста в Азии сохранятся, то средний доход на душу населения в азиатских странах может вырасти в шесть раз (по паритету покупательной способности) к 2050 году. Доля Азии в мировом ВВП будет быстро расти, примерно, с 28% в 2010 г. до более 50% в 2050 г. [4].

В 2020г. АБР принял комплексный пакет мер реагирования на COVID-19 в объеме 20 млрд долларов США, это позволило обеспечить быструю финансовую поддержку 26 странам. В декабре 2020г. был запущен АТР центр доступа к вакцинам на сумму 9 млрд долларов США. Учитывая беспрецедентные спрос на финансовые ресурсы, АБР выделил рекордные 31,6 млрд долларов США в виде займов, грантов, инвестиций в акционерный капитал, гарантий и технической помощи как правительствам, так и частному сектору (16,1 млрд долларов США были выделены на борьбу с COVID-19). АБР сумел увеличить общее финансирование, в том числе, за счет рекордного софинансирования проектов в размере 16,4 млрд долларов США (10,8 млрд долларов США были связаны с пандемией). В 2020г. Банк выделили 4,3 млрд долларов США на климатическое финансирование, операции частного сектора составили 21% от общего объема операций. Впервые, благодаря поддержке со стороны заместителя премьер-министра и министра экономики и финансов Республики Корея, удалось осуществить рекордную программу заимствований на сумму более 35 млрд долларов США (включая использование облигаций в местной валюте). Кроме того, Азиатский фонд развития (входит в группу АБР) был пополнен на более чем, на 4 млрд долларов США [5].

Решающее значение для реализации Стратегии 2030 АБР будет иметь цифровая трансформация (ЦТ) Банка, предполагающая не только использование инновационных технологий обработки данных, но также обновление имеющегося аппаратного и программного обеспечения (АПО).

По мнению специалистов Банка, в настоящее время необходимы дальнейшее обновление информационно-коммуникационных систем (ИКС), увеличение автоматизации ручной обработки данных, реформа несвязанных между собой и разрозненных информационных систем. Необходимы дополнительные инвестиции в ИКТ не только для обеспечения стабильной работы Банка в связи с ростом объема операций, децентрализацией и внедрением инновационных технологий и инноваций, но и для обеспечения кибербезопасности, противодействие отмыванию денег и финансированию терроризма (ПОД и ФТ).

АБР разработал план ЦТ на период до 2030г., который учитывает результаты предыдущих программ обновления АПО, использования новых ИКТ, включая преобразования, начатые в 2016г.

План ЦТ АБР предполагает выполнение ряда этапов, при этом на первом этапе будет проведена оптимизация основных ИТ-систем Банка, что позволит получить выгоду в связи с развитием цифровизации в Азиатско-Тихоокеанском регионе (АТР). Другие этапы плана ЦТ будут связаны с ростом уровня развития и связанности ИКС-систем Банка, совершенствованием используемых цифровых продуктов.

В настоящее время в рамках ЦТ, АБР осуществляет реализацию следующих 6 программ:

- В области операций. Операции Банка должны стать интегрированными, гибкими, эффективными, инклюзивными и прозрачными.

- В области финансовых услуг. Банк должен перейти к предоставлению гибких и инновационных финансовых продуктов.

- В области административных и корпоративных услуг. Должно быть проведено обновление корпоративных систем.

- «Цифровое рабочее место» и обеспечение связанных данных. Должны быть созданы открытые платформы для совместной работы и беспрепятственного взаимодействия с клиентами, партнерами и персоналом (при наличии связанных данных).

- «Цифровая магистраль». Создание условий для совершенствования ИТ-услуг Банка путем разумного использования инновационных технологий.

- Цифровая инновационная «песочница». Подготовка АБР к регулярному использованию инновационных технологий с помощью экспериментов в «песочнице».

В соответствии с указанными 6 программами, АБР на первом этапе реализует 16 проектов в 2019–2023г.г.

Банком были определены следующие цели первого этапа ЦТ:

- улучшение управления данными, в том числе, с помощью использования стандартизованных определений;

- обеспечение модернизации и автоматизации бизнес-процессов;

- внедрение новых технологий;

- улучшение технологической инфраструктуры в штаб-квартире Банка и его полевых отделениях, совершенствование услуг, включая кибербезопасность и отказоустойчивость технологий;

- совершенствование удаленной работы сотрудников (24 часа в сутки, в любом месте);

- улучшение способностей накапливать знания и обмениваться ими;

- развить использование новых технологий для бизнеса.

Предполагается, что АРБ сможет рассчитывать на увеличение прироста эффективности не менее, чем на 6%, что позволит получить прибыль уже от инвестиций в ЦТ на первом этапе (оценка капитальные затраты для данного этапа составляет 118,3 млн долларов США) [6].

Очевидно, что реализация ЦТ АБР ставит новые задачи по совершенствованию ПОД и ФТ.

Совет директоров АБР утвердил политику противодействия отмыванию денег (ПОД) и финансирования терроризма (ФТ) 1 апреля 2003 г. Данная политика предполагала:

- оказание помощи развивающимся странам-членам в создании и внедрении эффективных правовых систем ПОД и ФТ,
- расширение сотрудничества с другими международными организациями,
- укрепление внутреннего контроля для защиты средств АБР.

В соответствии с требованиями политики ПОД и ФТ в 2008г. был проведен первый раз анализ ее исполнения (интервал времени - с апреля 2003г. по март 2008г.), дальнейший контроль последствий использования политики был проведен в 2012г. (интервал времени – с апреля 2008г. по сентябрь 2012г.). Третий (и последний на текущий момент) анализ результатов применения политики был выполнен в 2017г. (интервал времени - с октября 2012г. по июнь 2017г.).

В качестве основных результатов было отмечено:

- продолжалось внедрение международных стандартов ПОД и ФТ в развивающихся странах-членах. Для определения уровня внедрения, использовалась методология ФАТФ, МВФ и Мирового банка взаимных оценок (страны оценивались по уровню эффективности их режимов ПОД и ФТ, в дополнение к их уровню технического соответствия каждой из Рекомендаций ФАТФ 2012 г.),

- был осуществлен переход к использованию рейтингов - высокого, существенного, умеренного или низкого на основании применения 11 непосредственных результатов эффективности применения режима ПОД и/ ФТ,

- с октября 2012г. по июнь 2017г. 9 стран-членов и 12 членов ФАТФ завершили взаимное оценивание: все 9 развивающихся стран-членов получили средний или низкий рейтинг (9 из 12 членов ФАТФ получили высокие рейтинги),

- сделан вывод о том, что страны-члены должны повысить уровень своей операционной эффективности, им нужно улучшить надзор за финансовым и нефинансовым секторами экономики, кроме этого, финансовые учреждения и определенные нефинансовые предприятия, их сотрудники должны улучшить «знание» своих клиентов, они должны бороться с неправомерным использованием юридических лиц для ОД и

ФТ, им необходимо усилить расследование и судебное преследование случаев ОД, они должны целенаправленно конфисковать доходы и средства совершения преступлений, им необходимо обеспечить ситуацию, при которой террористы и террористические организации не могли бы использовать некоммерческие организации для ФТ [7].

АБР осуществляет комплекс действий, направленных на ПОД и ФТ с использованием своего Управления по борьбе с коррупцией (ОАИ). Уже более 10 лет назад Банк признал проблемы, с которыми сталкиваются небанковские финансовые организации (НБФО) при выполнении национальных и международных требований ПОД и ФТ.

Важность НБФО связана с тем, что значительный процент из, примерно, 180 млн бедных домохозяйств в АТР, по-прежнему, имеет ограниченный доступ к институциональным финансовым услугам. По мнению Мирового банка, 200 млн малых и средних предприятий (МСП) в развивающихся странах не имеют доступа к доступным финансовым услугам и кредитам. Эти группы потребителей финансовых услуг вынуждены искать альтернативные каналы финансирования и кредитования, включая неформальных поставщиков подобных услуг, хранить сбережения в натуральной форме и осуществлять операции с наличными деньгами, сталкиваясь с большими комиссионными расходами при транзакциях и высокими рисками.

НБФО предоставляют финансовые услуги указанным группам потребителей и стимулируют экономическую активность, количество данных организаций быстро увеличилось после мирового финансового кризиса 2008-2009 гг. Однако, НБФО увеличивают системные риски для финансовой системы, т.к. они не всегда контролируются должным образом, а их регулирование и надзор существенно отличаются от банковских.

АБР был подготовлен проект технической помощи для развития ПОД и ФТ, методологии и использования мер контроля для НБФО. В рамках данного проекта было разработано «Руководство по противодействию отмыванию денег и финансированию терроризма для НБФО». Цель руководства - помочь НБФО в развитии и внедрении внутренних процедур и использования средств контроля, а также обеспечение руководства необходимой информацией, связанной с практическими проблемами управления рисками, возникающими при отмывании денег и финансировании терроризма.

В соответствии с руководством, НБФО должны обеспечивать:

- оценку и понимание рисков, связанных с ведением бизнеса своих клиентов,
- знать своих клиентов и осуществлять их комплексную проверку,
- осуществлять мониторинг транзакций,

- сообщать правительственным органам о подозрительных транзакциях,
- вести регламентированный учет [8].

Таким образом, АБР в течение более 50 лет реализует успешные проекты и программы в странах АТР, осуществляют ЦТ.

АБР осуществляет ПОД и ФТ в рамках своей группы и, одновременно, проводит методологическую работу по указанным направлениям, организует соответствующую работу в странах АТР.

Список использованных источников:

1. De Luna-Martínez, J. 2017 Survey of National Development Banks / J. De Luna- Martínez / Global report//World Bank Group. <https://documents1.worldbank.org/curated/en/977821525438071799/pdf/2017-Survey-of-National-development-banks.pdf> (accessed: 22.06.2019)
2. The role of development banks in Promoting Growth and Sustainable Development in the South. Economic Cooperation and Integration among Developing Countries. UNCTAD. December 2016. New York. https://unctad.org/system/files/official-document/gdsecidc2016d1_en.pdf (accessed 25.08.2020)
3. Asian development bank. Project Performance and the Project Cycle. Operations Evaluation Department. Reference Number: SST: REG 2008-38. September 2008 (accessed: 20.02.2021)
4. Banking on the future of Asia and the Pacific. 50 years of the Asian development bank. Peter McCawley <https://www.adb.org/publications/50-years-adb> (accessed 25.08.2020)
5. Asian development bank. Annual report 2020. <https://www.adb.org/documents/adb-annual-report-2020> / (accessed: 20.02.2021)
6. Digital Agenda 2030: Special Capital Expenditure Requirements for 2019–2023. Asian development bank. <https://www.adb.org/sites/default/files/institutional-document/472371/adb-digital-agenda-2030.pdf> (accessed: 10.10.2020)
7. Third Review of Enhancing the Asian Development Bank's Role in Combating Money Laundering and the Financing of Terrorism. Asian Development Bank. <https://www.adb.org/sites/default/files/institutional-document/382316/in420-17.pdf> (accessed 25.10.2021)
8. Handbook on anti-money laundering and combating the financing of terrorism for Nonbank Financial Institutions. Asian development bank. <https://www.adb.org/sites/default/files/publication/184373/handbook-aml.pdf> (accessed 26.10.2021)

**Анализ вероятных макроэкономических последствий при принятии
криптовалюты как основной денежной единицы**

С. Мукхерджи

студент 5 курса НИЯУ МИФИ, Москва

E-mail: soumojitmukherjee007@gmail.com

А.В. Трушко

студент 4 курса НИЯУ МИФИ, Москва

E-mail: annatrushkoo@mail.ru

научный руководитель: Н.В. Морозов

к.ю.н., доцент кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: nvmorozov@mephi.ru

Аннотация: Целью работы является моделирование ситуации принятия криптовалюты в качестве основной денежной единицы государства. Для грамотного прогнозирования последствий, обозначения рисков и преимуществ исследуемой ситуации проведен сравнительный анализ свойств криптовалют с национальными валютами. В результате исследования был оценен уровень осуществимости и целесообразности принятия криптовалюты законным платежным средством.

Ключевые слова: криптовалюта, цифровая валюта, центральный банк, функции денег, риски, регулирование.

**Analysis of the likely macroeconomic consequences of adopting
cryptocurrency as the basic monetary unit**

Abstract: the aim of the work is to model the situation of adopting cryptocurrency as the main monetary unit of the state. A comparative analysis of the properties of cryptocurrencies with national currencies was carried out to correctly predict the consequences, to outline the risks and advantages of the situation under study. The study assessed the level of feasibility and expediency of adopting cryptocurrency as a legal means of payment.

Keywords: cryptocurrency, digital currency, central bank, money functions, risks, regulation.

Введение. На сегодняшний день в мире насчитывается более 2000 различных типов криптовалют [1], каждая из которых реализуется через поставщиков, провайдеров услуг и различные приложения. Объем криптовалют в мире по-прежнему намного меньше, чем объем

международных стандартных валют, а уровень их принятия еще ниже. Кроме того, сомнения в классификации криптовалют приводят к еще большему недопониманию: это не совсем валюта, но и не совсем актив.

В то время как во всем мире подчеркивается необходимость более строгого регулирования криптовалют, некоторые государства объявили их полный запрет: в особенности это развивающиеся страны, такие как Китай [2] и Индия [3]. В большинстве западных стран он рассматривается как товар для торговли, при этом уровни регулирования отличаются между представителями данных государств.

Однако ситуация изменилась, когда Сальвадор - страна в Центральной Америке - принял решение сделать крупнейшую криптовалюту в мире по объему торгов и рыночной капитализации Bitcoin своим законным платежным средством [4]. Подобное решение, особенно в таком месте, как Сальвадор, где ранее в качестве законного платежного средства использовались доллары США, стало неожиданностью для всего мира. Такой шокирующий характер решению придает тот факт, что принятие криптовалюты в качестве валюты, а тем более в качестве законного платежного средства, естественно сопряжено с огромными рисками. Тем не менее, будучи первой страной, которая попробовала этот эксперимент, она также может извлечь много пользы из того, что внедрила криптовалюту раньше остальных. Мы анализируем и сравниваем свойства криптовалют со свойствами национальных валют, чтобы понять их различия, риски и различные возможности, которые может принести с собой внедрение криптовалют.

На данный момент важно отметить, что криптовалюта остается нерегулируемой в большинстве стран мира, а в некоторых местах полностью запрещена, однако с ростом технологических инноваций в этой области и ростом популярности криптовалют во всем мире вероятность отмены таких решений остается высокой.

Для простоты мы можем предположить, что криптовалюта, принятая государствами, является биткойном из-за ее рыночной капитализации, охвата и популярности. Другие аналоги, такие как Ethereum, Tether или Cardano, не имеют такого же охвата, инвестиций или внедрения, чтобы серьезно рассматриваться в качестве валюты в различных странах мира.

Функции денег

Деньги должны обладать следующими тремя функциями:

- сохранение ценности;
- единица учета;
- средство обращения.

Под сохранением ценности понимается способность денег иметь одинаковую ценность в течение определенного периода времени [5]. То есть, если у человека есть 100 рублей, то стоимость 100 рублей будет

оставаться неизменной в течение длительного периода времени. Единственная причина, по которой деньги обесцениваются или теряют свою ценность, — это инфляция. Для национальных валют эта функция справедлива.

С другой стороны, криптовалюты не являются лучшим средством сохранения стоимости. Из-за волатильности на международных биржах их стоимость колеблется гораздо больше, чем стоимость валют. Это вызывает огромную волатильность самой валюты, так как она не является безопасным хранилищем стоимости. Кроме того, поскольку количество криптовалют фиксировано, стоимость криптовалют не равна. Люди, которые владеют раньше «добытой» криптовалютой, находятся в лучшем положении - с монетами более высокой стоимостью, - чем те, кто приобрел монеты позже, поскольку внутренняя стоимость монет падает тем больше, чем позднее они покупаются.

Это поднимает основной вопрос о способности криптовалют выполнять данную функцию денег. Однако это не совсем безнадежно, потому что, если существует гипотетический сценарий, при котором все транзакции совершаются в криптовалюте, волатильность по отношению к другим валютам не будет иметь значения, поскольку все товары и услуги будут номинированы в одной и той же криптовалюте. Проблема возникает только тогда, когда транзакции будут происходить за пределами криптоэкосистемы, где в игру вступают курсы иностранных валют: обменные курсы зависят от множества факторов, таких как импорт, экспорт, спрос на валюту и ее предложение.

Предполагая, что страны принимают криптовалюту в качестве своего законного платежного средства, можно ожидать следующих ситуаций:

1) Страны с высоким уровнем дохода: поскольку такие страны характеризуются высокими объемами торговли, то есть большим количеством экспорта технических и готовых товаров, при импорте сырья, их использование иностранной валюты очень велико. В большинстве случаев транзакции обычно номинируются в долларах или других международных валютах, таких как евро, юань, иена и фунты стерлингов. Это подвергает их высокому риску из-за высокой волатильности валютных курсов, особенно когда цены на товары и услуги могут меняться ежедневно, создавая экономический хаос в экономике. Для стран с высоким уровнем дохода, особенно для стран с международными валютами, нет особых причин или смысла делать криптовалюты законным платежным средством. Кроме того, валюта также используется в фискальной и денежно-кредитной политике, обсуждаемой позже, что также будет существенно затронуто.

2) Страны со средним уровнем дохода: такие страны, как правило, не выпускают валюты, номинированные в международных валютах, но используют их в операциях по импорту и экспорту товаров и услуг. Это

опять же означало бы для них хаос из-за волатильности криптовалют. Аналогичным образом, поскольку эти страны проводят стабильную и независимую экономическую политику, они не решились бы менять свою валюту на что-то нестабильное.

3) Страны с низким уровнем дохода: в этом случае объем торговли меньше, и даже в этом сценарии он в основном основан на экспорте сырья и импорте готовой продукции. Здесь существует высокая вероятность внедрения криптовалюты, так как валюта будет в основном функционировать внутри своей собственной экосистемы. Вопрос сохранения стоимости не будет иметь значения, так как 1 единица криптовалюты будет равна 1 единице криптовалюты для всех пользователей внутри экосистемы.

Далее мы переходим к единице учета. Эта функция денег понимается как присвоение стоимости товаров и услуг в денежной форме. Каждый товар и услуга могут быть измерены в денежном выражении [5]. Это функция денег, которая легко работает как для национальных валют, так и для криптовалют, поскольку это всего лишь мера стоимости.

Третья функция денег - средство обмена. Любая валюта должна быть широко принята в качестве формы оплаты как внутри страны, так и за ее пределами, чтобы быть принятой в качестве денег [5]. Здесь вопрос становится немного сложным. Если криптовалюта объявлена законным платежным средством, то по закону валюта должна использоваться и приниматься для всех транзакций. Для общей валюты оплата может быть произведена различными способами оплаты, такими как наличные, карты, чеки, онлайн-платежи и т. д. Основным способом оплаты в обычных валютах чаще всего являются наличные или карты [6]. Однако для платежей в криптовалютах существует базовое требование крипто-кошельков и подключения к Интернету. Предполагая этот барьер, сценарий в различных странах может быть следующим:

1) Страны с высоким уровнем дохода: в большинстве стран с высоким уровнем дохода население имеет высокий уровень подключения к Интернету и финансовой грамотности для подключения и понимания использования криптовалюты через крипто-кошельки. Однако могут быть места, где подключение к Интернету слабое, плохое или недоступное. В таких местах завершение транзакций будет невозможно. Аналогичным образом, в большинстве стран с высоким уровнем дохода наблюдается старение населения [7], что будет означать трудности с внедрением новых технологий и, следовательно, риски мошенничества.

2) Страны со средним уровнем дохода: эти страны сталкиваются с теми же проблемами: подключение к Интернету и финансовая грамотность. Не все смогут совершать транзакции (для некоторых препятствием будет отсутствие надлежащей информации), следовательно, принятие может стать серьезной проблемой.

3) Страны с низким уровнем дохода: в таких странах подключение к Интернету очень низкое, а финансовая грамотность, как правило, отсутствует. Возьмем, к примеру, Сальвадор, где 66% населения не имеют доступа к Интернету [8], и, следовательно, не смогут совершать транзакции, даже если захотят.

Циркуляция

Используя американскую систему измерения денежного обращения [10], деньги могут циркулировать в трех измерениях:

1) M1 – «Узкая» Мера.

M1 включает всю валюту (т. е. наличные деньги) в обращении, дорожные чеки, депозиты до востребования в коммерческих банках (или других депозитных учреждениях), которыми владеет население, и другие проверяемые депозиты. Его часто называют самым узким показателем денежной массы или узкими деньгами. Однако для полноты картины и во избежание путаницы, обращаем ваше внимание на то, что некоторые страны также измеряют аналогичную денежную массу, но в более узком ключе, как M0.

Когда дело доходит до криптовалюты, ее существование в обращении в узкой мере M1 возможно, и, по сути, все криптовалюты, находящиеся в настоящее время в обращении, где они принимаются в качестве способа оплаты, могут быть засчитаны как M1. Это делает их чрезвычайно ликвидными активами, поскольку M1 является наиболее ликвидной категорией обращения.

M2 – «Промежуточная» Мера.

2) M2 включает в себя все, что есть в M1, а также сберегательные депозиты, срочные депозиты на сумму менее 100 000 долларов США и остатки средств в фондах розничного денежного рынка. Его часто называют промежуточной мерой, поскольку он шире, чем M1, но не настолько широк, как M3.

Именно здесь криптовалюта сталкивается с проблемой, поскольку сберегательные депозиты и срочные депозиты в настоящее время не существуют в качестве отдельных продуктов в банковском секторе. Кроме того, практически невозможно создать такие продукты для криптовалют, поскольку на депозиты обычно начисляются проценты. Хотя начисление процентов на депозиты не составляет труда, если проценты выплачиваются в той же криптовалюте, однако поскольку стоимость криптовалют крайне изменчива, конечная стоимость депозита может радикально отличаться от начальной стоимости, в зависимости только от времени вывода средств и рыночных условий, которые будут диктовать стоимость депозитов.

3) M3 – «Широкая» Мера.

M3 включает в себя все, что содержится в M2, а также срочные депозиты на сумму более 100 000 долларов США, остатки средств в фондах институционального денежного рынка и соглашения о срочном выкупе.

МЗ всегда должен существовать более чем в одной валюте, поскольку криптовалюта не охватывает все продукты и виды использования общей валюты. Следовательно, она всегда будет связана с волатильностью. А поскольку волатильность высока, расчет МЗ будет чрезвычайно сложным и, в лучшем случае, бесполезным, так как он не будет должным образом учитывать денежное обращение в экономике из-за нестабильных обменных курсов.

Фискальная и денежно-кредитная политика

Наиболее важным моментом в этом аспекте является тот факт, что криптовалюты децентрализованы. Это означает, что ни одна страна не контролирует их распространение и создание. Правительства, которые могут сделать криптовалюты своим законным платежным средством, по сути, передают свой валютный суверенитет в руки рыночных сил. Эти рыночные силы, в том числе те, которые действуют за пределами национальных границ, могут в любой момент дестабилизировать криптовалюту страны и сделать невозможным для государства контроль над ситуацией. У Центрального банка может быть несколько вариантов, таких как вывод валюты на рынок, но это будет временное решение. Это связано с тем, что Центральный банк не контролирует криптовалюту, поэтому любое вливание капитала будет осуществляться из чрезвычайных резервов Центрального банка, которые он, возможно, сформировал ранее, или Центральному банку придется просить правительство купить криптовалюту на открытом рынке, что, в зависимости от ситуации, может быть чрезвычайно дорогим. С другой стороны, если бы страна решила сделать конкретную криптовалюту своим единственным законным платежным средством, то у нее не было бы средств, чтобы покупать больше на открытом рынке.

Теперь, если мы перейдем к специфике бюджетной политики, а именно к расходам и налогообложению, если правительство хочет увеличить экономический рост в стране, ему необходимо вливать деньги в экономику. Поскольку количество токенов ограничено, они не могут предоставить необходимые суммы без заимствования на открытых рынках. Точно так же, если правительство намерено контролировать инфляцию в стране путем повышения налогов, то на начальном этапе оно добьется успеха за счет сокращения объема денежного потока в экономике, но это будет временным, поскольку контроль за денежным обеспечением осуществляется не правительством, а майнерами и открытым рынком. При этом пользователи и граждане всегда могут приобрести больше токенов с международных рынков или сами "добывать" больше количество токенов. Это сделало бы правительство беспомощным, поскольку его предполагаемая политика контроля не будет работать из-за децентрализованного контроля над криптовалютами.

Центральный банк также может изменять резервные требования в банках, напрямую увеличивая или уменьшая денежную массу. Коэффициент требуемых резервов влияет на денежную массу, регулируя, сколько денег банки должны держать в резерве. Если центральный банк хочет увеличить денежную массу, он может уменьшить объем требуемых резервов, а если он хочет уменьшить денежную массу, он может увеличить объем резервов, необходимых для хранения банками.

Так, главной проблемой, с которой может столкнуться страна, будет ее неспособность брать кредиты у международных кредиторов. Страны и инвесторы не будут покупать их облигации, потому что рейтинговые агентства оценят их как ненужные, как это было сделано с Сальвадором. В случае с Сальвадором чьи облигации были почти мусорными до принятия биткоина в качестве криптовалюты, само по себе принятие не помогло делу [11][12]. Учитывая тот факт, что необходимость в заимствованиях возникнет из-за экономической катастрофы, возможности страны иметь хороший рейтинг практически не будет.

Если страна обратится к международным кредиторам, таким как Всемирный банк или МВФ, государству будет назначен мониторинг различные правила, одним из которых является удаление криптовалюты в качестве законного платежного средства. Это будет обязательным условием, поскольку обе организации выступили с публичными заявлениями по вопросу использования криптовалют в качестве законного платежного средства с решительными предупреждениями против их использования в качестве валюты. Обе организации придерживаются своей позиции, что криптовалюты являются предметом спекуляции и, следовательно, никогда не могут служить национальными валютами.

Помимо упомянутых выше рисков, существует еще несколько дополнительных проблем, когда речь заходит об использовании криптовалюты в целом. Они заключаются в следующем:

1. отсутствие доверия;
2. финансовое принятие;
3. государственное регулирование;
4. проблемы безопасности;
5. волатильность;
6. потребление энергии.

Предполагая, что биткойн является выбранной криптовалютой страны, эти проблемы объясняются практическими приложениями, чтобы лучше понять пробелы в решении выбора криптовалюты в качестве законного платежного средства.

Причины для принятия

- 1) Финансовая доступность.

Это одна из основных причин правительств, поскольку они утверждают, что криптовалюта делает банковские услуги проще, быстрее

и доступнее для людей, особенно для тех, кто-либо был отвергнут традиционным банковским сектором, либо вообще не имеет к нему доступа из-за отсутствия предоставления таких услуг.

Хотя этот аргумент отчасти верен, проблема все равно останется, поскольку использование криптовалют потребует хорошего подключения к Интернету, доступа к Интернету и финансовой грамотности, чтобы действительно понять, как использовать валюту.

2) Денежные переводы и транзакции.

Еще один аргумент заключается в том, что использование криптовалют делает денежные переводы и трансферты проще, быстрее и требует меньших транзакционных издержек. Это позволяет клиентам получать большее количество денег. Как и в случае с Сальвадором, 22% экономики приходится на денежные переводы из других стран. Ранее транзакционные издержки сокращали суммы, получаемые людьми в стране, но теперь из-за принятия биткойна транзакционные издержки снизились.

Этот аргумент тоже отчасти верен. В некотором смысле транзакционные издержки снизились, поскольку нет необходимости платить комиссию за переводы брокерам, таким как Western Union. Однако отправителям все равно приходится платить комиссию за конвертацию своим банкам, чтобы купить биткойн, а затем отправить в свою страну. Во-вторых, процесс протекает не так быстро, как ранее. Биткойн обрабатывает 4-5 транзакций в секунду, в то время как их конкурент MasterCard обрабатывает 65000 транзакций за тоже время, что является огромной разницей между скоростями транзакций [27].

3) Конфиденциальность и финансовая независимость от монополии международных валют.

Одной из важных причин, по которой правительства рассматривают возможность перехода на криптовалюту, является конфиденциальность для своих граждан. Теперь они свободны выбирать, как они тратят свои деньги, и никто не знает, как и где они их используют. Аналогичным образом, в макроэкономическом масштабе страны, которые хотят избавиться от монополии международных валют, предпочли бы перейти на криптовалюту и, следовательно, уйти от санкций, тарифов, комиссий и сборов.

Этот аргумент на самом деле является слабым. Можно было бы сказать, что честному гражданину нечего скрывать и, следовательно, он не требует неприкосновенности частной жизни в качестве приоритета, но есть и аргумент получше. Государственное отслеживание потребительских расходов и расходов бизнеса позволяет ему формировать денежно-кредитную и налогово-бюджетную политику и лучше контролировать стабильность экономики. Выбирая криптовалюту, правительство теряет способность планировать и анализировать свою политику. Затем, поскольку правительство не контролирует валюту, оно также теряет

контроль над денежно-кредитной и фискальной политикой. Таким образом, по сути, страна решила передать свою экономическую политику от избранного правительства алгоритму майнинга и миллионам неизвестных людей по всему миру. Это не является хорошим признаком будущей экономической стабильности.

Вывод

Из всего выше написанного видно, что различные аспекты денег, их функции, обращение, денежно-кредитная и фискальная политика, криптовалюты при различных возможностях, несут в себе огромные риски. В некоторых случаях криптовалюты просто не могут соответствовать требованиям, предъявляемым к общей валюте. Принятие криптовалют гипотетической страной, в зависимости от ее уровня дохода, в основном будет иметь катастрофические последствия для страны и ее экономики.

В дополнение к денежному аспекту криптовалюты также имеют свои врожденные недостатки, которые делают их нежелательными в качестве валюты. Чтобы противодействовать их увеличению, центральные банки разных стран придумали CBDCs, которые обеспечивают преимущества криптовалют без серьезных проблем и могут рассматриваться как альтернатива криптовалютам. Мы в свою очередь уверены, что у CBDC больше шансов стать полноценной валютой для своих стран, чем у криптовалюты, чтобы стать независимой валютой какой-либо отдельной страны.

Список использованных источников:

1. All Cryptocurrencies | CoinMarketCap // CoinMarketCap [Электронный ресурс]. URL: <https://coinmarketcap.com/all/views/all/> (дата обращения: 03.10.2021).
2. China Widens Ban on Crypto Transactions; Bitcoin Tumbles // Bloomberg.com [Электронный ресурс]. URL: <https://www.bloomberg.com/news/articles/2021-09-24/china-deems-all-crypto-related-transactions-illegal-in-crackdown/> (дата обращения: 03.10.2021).
3. Reserve Bank of India - Notifications // Rbi.org.in [Электронный ресурс]. URL: https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=11243&fn=2&Mode=0 (дата обращения: 03.10.2021).
4. The editorial board El Salvador's dangerous gamble on bitcoin // @FinancialTimes [Электронный ресурс]. URL: <https://www.ft.com/content/c257a925-c864-4495-9149-d8956d786310> (дата обращения: 03.10.2021).
5. Деньги, определение денег, деньги как мера стоимости, средство обращения, платежа, накопления // Банки.ру [Электронный ресурс]. URL: https://www.banki.ru/wikibank/dengi_wiki/ (дата обращения: 03.10.2021).

6. Global Payments report: Trends in the global payments business // Payments Cards & Mobile [Электронный ресурс]. URL: <https://www.paymentscardsandmobile.com/global-payments-report-trends-in-global-payments/> (дата обращения: 03.10.2021).
7. Population ages 65 and above (% of total population) | Data // Worldbank.org [Электронный ресурс]. URL: <https://data.worldbank.org/indicator/SP.POP.65UP.TO.ZS> (дата обращения: 03.10.2021).
8. Tidy J. Fear and excitement in El Salvador as Bitcoin becomes legal tender // BBC News [Электронный ресурс]. URL: <https://www.bbc.com/news/technology-58473260> (дата обращения: 03.10.2021).
9. PayPal Accepts Bitcoin for Merchant Payment // Nasdaq.com [Электронный ресурс]. URL: <https://www.nasdaq.com/articles/paypal-accepts-bitcoin-for-merchant-payment-2021-04-05> (дата обращения: 03.10.2021).
10. Money Supply Definition, Effects, & Measurements // Investopedia [Электронный ресурс]. URL: <https://www.investopedia.com/terms/m/moneysupply.asp> (дата обращения: 03.10.2021).
11. // Fitchratings.com [Электронный ресурс]. URL: <https://www.fitchratings.com/entity/el-salvador-80442262> (дата обращения: 03.10.2021).
12. Moody's puts El Salvador on review for downgrade // Latinfinance.com [Электронный ресурс]. URL: <https://www.latinfinance.com/daily-briefs/2020/11/17/moodys-puts-el-salvador-on-review-for-downgrade> (дата обращения: 03.10.2021).
13. Rotberg E. Bitcoin's in a slump — here's why Warren Buffett has hated it all along // Yahoo.com [Электронный ресурс]. URL: <https://finance.yahoo.com/news/bitcoins-slump-heres-why-warren-170000851.html/>. (дата обращения: 03.10.2021).
14. The State of the World's Cash 2020 – Full report // Calpnetwork.org [Электронный ресурс]. URL: <https://www.calpnetwork.org/publication/the-state-of-the-worlds-cash-2020-full-report/> (дата обращения: 03.10.2021).
15. M. Ridgway Barker The U.S. Infrastructure Bill And Cryptocurrency Regulation // Mondaq.com [Электронный ресурс]. URL: <https://www.mondaq.com/unitedstates/fin-tech/1111802/the-us-infrastructure-bill-and-cryptocurrency-regulation> (дата обращения: 03.10.2021).
16. Cryptocurrency Regulations in The United Kingdom (UK) | Sanction Scanner // Sanctionsanner.com [Электронный ресурс]. URL: <https://sanctionsanner.com/blog/cryptocurrency-regulations-in-the-united-kingdom-uk-217> (дата обращения: 03.10.2021).
17. Documents - Financial Action Task Force (FATF) // Fatf-gafi.org [Электронный ресурс]. URL: <https://www.fatf-gafi.org/publications/>

- fatfrecommendations/documents/public-statement-virtual-assets.html (дата обращения: 03.10.2021).
18. PDVSA // Pdvsa.com [Электронный ресурс]. URL: http://www.pdvsa.com/index.php?option=com_content&view=article&id=8734&Itemid=577&lang=es (дата обращения: 03.10.2021).
 19. JJ CipherTrace Analysis of Paymon, Iran's Sanction Evading Crypto-Rial - CipherTrace [Электронный ресурс]. URL: <https://ciphertrace.com/analysis-of-irans-crypto-rial-virtual-currency/> (дата обращения: 03.10.2021).
 20. The Central Bank of Iran delves into Digital Rial // Central Bank of The Islamic Republic of Iran [Электронный ресурс]. URL: <https://www.cbi.ir/showitem/21652.aspx> (дата обращения: 03.10.2021).
 21. Cryptopia Exchange, Currently in Liquidation, Gets Hacked Again: Report - CoinDesk // @coindesk [Электронный ресурс]. URL: <https://www.coindesk.com/policy/2021/02/20/cryptopia-exchange-currently-in-liquidation-gets-hacked-again-report/> (дата обращения: 03.10.2021).
 22. Arjun Kharpal Hackers steal over \$40 million worth of bitcoin from one of the world's largest cryptocurrency exchanges // CNBC [Электронный ресурс]. URL: <https://www.cnbc.com/2019/05/08/binance-bitcoin-hack-over-40-million-of-cryptocurrency-stolen.html> (дата обращения: 03.10.2021).
 23. Global Disruption of Three Terror Finance Cyber-Enabled Campaigns // Justice.gov [Электронный ресурс]. URL: <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns> (дата обращения: 03.10.2021).
 24. IntelBrief: Terrorists' Use of Cryptocurrency IntelBrief: Terrorists' Use of Cryptocurrency - The Soufan Center // The Soufan Center [Электронный ресурс]. URL: <https://thesoufancenter.org/intelbrief-2020-december-10/> (дата обращения: 03.10.2021).
 25. Inside the Takedown of Al-Qaeda and Hamas Terrorist Financial Networks // Chainalysis.com [Электронный ресурс]. URL: <https://go.chainalysis.com/terrorist-crypto-network-takedown.html> (дата обращения: 03.10.2021).
 26. Morris D. Z. Bukele's MS-13 Double Bind // @coindesk [Электронный ресурс]. URL: <https://www.coindesk.com/business/2021/09/10/bukeles-ms-13-double-bind/> (дата обращения: 03.10.2021).
 27. Vlastelica R. Why bitcoin won't displace Visa or Mastercard soon // MarketWatch [Электронный ресурс]. URL: <https://www.marketwatch.com/story/why-bitcoin-wont-displace-visa-or-mastercard-soon-2017-12-15> (дата обращения: 03.10.2021).

Анализ добросовестности поставщика с помощью системы SAP S4/HANA

Ю.И. Мещерякова

студентка 5 курса НИЯУ МИФИ, Москва

E-mail: meshcheryakova_julia@mail.ru

Т.А. Соколова

студентка 5 курса НИЯУ МИФИ, Москва

E-mail: sklvtu@mail.ru

Аннотация: Риски организации существенно возрастают, если ее контрагенты не исполняют свои обязательства по договорам. В данной статье рассмотрены возможности использования ERP-системы SAP S4/HANA для выбора поставщиков при заключении контрактов. Такой автоматизированный подход позволяет более достоверно, экономично и эффективно анализировать информацию о деятельности потенциальных поставщиков в рамках процесса закупок. В статье также описаны возможности сбора данных для проверки благонадежности контрагента из открытых интернет-источников с помощью REST API.

Ключевые слова: анализ добросовестности, госконтракт, закупка, поставщик, ERP, REST API, SAP S4/HANA.

Supplier integrity analysis using SAP S4/HANA system

Abstract: The risks of an organization increase significantly if its counterparties do not fulfill their obligations under contracts. This article discusses the possibilities of using the SAP S4/HANA ERP system to select suppliers when concluding contracts. This automated approach allows for more reliable, economical and efficient analysis of information about the activities of potential suppliers in the procurement process. The article also describes the possibilities of collecting data to verify the reliability of the counterparty from open Internet sources using the REST API.

Keywords: integrity analysis, government contract, procurement, supplier, ERP, REST API, SAP S4/HANA.

Основной целью Федерального закона № 44-ФЗ от 05 апреля 2013 года «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – Закон №

44-ФЗ) является обеспечение открытости и эффективности контрактной системы, следовательно, уменьшение уровня коррупции и снижение затрат бюджетных средств, «здоровая» конкуренция, своевременное и качественное удовлетворение государственных и общественных нужд, доступный к восприятию процесс проведения этапов закупок для специалистов и ее участников [1]. Поэтому для более эффективного совершенствования законодательства в сфере государственных закупок необходимо учитывать специфику потенциальных рисков в данной сфере.

Закупка – это совокупность действий, осуществляемых в порядке, установленном Законом № 44-ФЗ, заказчиком и направленными на обеспечение государственных или муниципальных нужд. Закупка начинается с определения поставщика и завершается исполнением обязательств сторонами контракта.

Укрупненно закупки любой организации можно представить в виде следующей последовательности этапов:

- планирование закупок (включая формирование требований к продукции);
- подготовка к проведению закупок и их объявление;
- проведение закупочных процедур и выбор поставщиков.

По состоянию на 31 марта 2021 года в единой информационной системе в сфере закупок (далее – ЕИС) зарегистрировано 312 тыс. заказчиков. Общий стоимостной объем извещений, размещенных в первом квартале 2021 года, составил 2 трлн рублей [2].

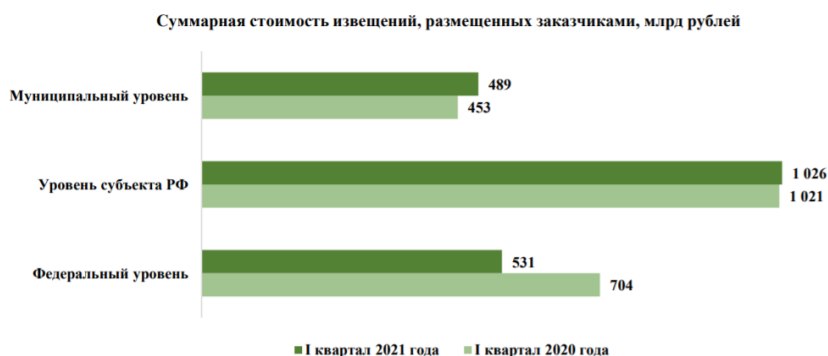


Рисунок 1 – Стоимостной объем извещений

Одним из наиболее рискованных этапов в процессе закупки является этап выбора поставщика. В настоящее время в системе закупок существует проблема недобросовестных поставщиков, которые в целях получения

госконтракта искусственно занижают стоимость предмета контракта без возможности обеспечить его качественное выполнение. Ввиду демпинга цен и необходимости выполнить поставленные задания, заказчики идут на риск, сотрудничая с такими поставщиками, что приводит к не надлежащему исполнению условий закупки поставщиками.

За исследуемый период ФАС России проведено 2,4 тыс. внеплановых проверок (больше на 5% по отношению к первому кварталу 2020 года). При проведении проверок в отношении закупок, осуществляемых в соответствии с требованиями Закона № 44-ФЗ, проверено 6,12 тысяч процедур определения поставщика (подрядчика, исполнителя), из которых в 1,7 тыс. процедур (27%) выявлены нарушения.

Таким образом, мы считаем, организациям необходимо разрабатывать и внедрять систему оценки поставщиков для повышения своей экономической безопасности. На сегодняшний день процесс закупок в большинстве организаций является автоматизированным. С помощью интегрированных систем управления предприятием (далее – ИСУП). Принцип ИСУП – создание единого хранилища данных (репозитория), содержащего всю деловую информацию, накопленную организацией в процессе ведения бизнеса. Лидером рынка ИСУП в мире является решение SAP ERP. SAP ERP – это программное обеспечение для планирования ресурсов предприятия, разработанное компанией SAP SE. ERP представляет собой модульное программное обеспечение, предназначенное для интеграции основных функций основных бизнес-процессов организации в единую систему. Программное обеспечение ERP охватывает все основные области бизнеса организации за счет централизации управления данными.

ERP-системы в целом обычно состоят из программных компонентов, называемых модулями, каждый из которых сосредоточен на основных бизнес-функциях, таких как финансы и бухгалтерия, управление персоналом, производство, управление материалами и управление взаимоотношениями с клиентами (CRM). Организации используют только те модули, которые им необходимы для ведения своего конкретного бизнеса. Некоторые примеры бизнес-процессов включают Корпоративные услуги, Финансы и Управление человеческим капиталом. За закупки отвечает модуль MM – Управление материальными потоками [3].

В рамках нашей работы мы рассмотрим возможный вариант анализа добросовестности поставщика с помощью системы SAP S4/HANA. Основные данные о поставщике в SAP содержатся в Справочнике: Контрагенты. Справочник поставщиков содержит информацию о поставщиках, используемых компаниями. Данные в основных записях

поставщика определяют, как данные транзакции разносятся и обрабатываются для поставщика.

Поставщик	1000
Балансовая единица	1000
Закупочная организация	1000

Общие данные

- ☐ Адрес
- ☐ Управление
- ☐ Платежные операции
- ☐ Контактное лицо

Данные балансовой единицы

- ☐ Бухгалтерская информация
- ☐ Платежные операции
- ☐ Корреспонденция
- ☐ Налог на источники дохода

Данные закупочной организации

- ☐ Данные закупки
- ☐ Роли партнеров

Рисунок 2 – Структура основной записи поставщика

Основные записи поставщиков содержат информацию о поставщиках предприятия.

Примеры данных в основной записи поставщиков:

- имя и адрес поставщика;
- валюта, используемая для операций с данным поставщиком;
- условия платежа;
- имена ключевых контактных лиц.

С точки зрения бухгалтерского учета поставщик является также кредитором компании, поэтому основная запись поставщика также содержит бухгалтерские данные, например, контрольный счет из бухгалтерии Главной книги. Основная запись используется не только в бухгалтерском учете, но и в Управлении материальными потоками. В дополнение к имени и адресу основная запись поставщика содержит номер поставщика, а также основные идентификационные данные, такие как ИНН, ОКПО, КПП и т.д. Каждому поставщику присваивается также

уникальный технический идентификатор – системный номер, который будет выступать ключевым в выборке данных по поставщику [4].

Адрес	Обзор адреса	<u>Идентификатор</u>	Управление	Платежные операции	Статус												
Налоговые номера ☐ Физическое лицо <table border="1"> <thead> <tr> <th>Тип</th> <th>Название</th> <th>Налоговый номер</th> </tr> </thead> <tbody> <tr> <td>☐ RU1</td> <td>Российская Федерация: ИНН</td> <td>7816222096</td> </tr> <tr> <td>☐ RU2</td> <td>Российская Федерация: код ОКПО</td> <td>13855950</td> </tr> <tr> <td>☐ RU3</td> <td>Российская Федерация: номер КПП</td> <td>781601001</td> </tr> </tbody> </table>						Тип	Название	Налоговый номер	☐ RU1	Российская Федерация: ИНН	7816222096	☐ RU2	Российская Федерация: код ОКПО	13855950	☐ RU3	Российская Федерация: номер КПП	781601001
Тип	Название	Налоговый номер															
☐ RU1	Российская Федерация: ИНН	7816222096															
☐ RU2	Российская Федерация: код ОКПО	13855950															
☐ RU3	Российская Федерация: номер КПП	781601001															

Рисунок 3 – Идентификация поставщика

Контактными лицами являются сотрудники компании делового партнера, с которыми осуществляется взаимодействие в письменной форме, лично или по телефону по вопросам проведения бизнес-операций. Данные контактного лица хранятся в общих данных основной записи делового партнера.

В основной записи поставщика можно указать подробные данные контактных лиц, с которыми осуществляется взаимодействие и которые являются реальными сотрудниками компании поставщика. Можно также указать подробные данные собственных сотрудников, ответственных за работу с этим поставщиком. Каждому контактному лицу в основной записи поставщика присваивается новый номер. Данные контактных лиц хранятся в таблице KNVK. Контактные лица, ведение которых осуществляется в основной записи поставщика на уровне клиента, также могут использоваться в качестве ролей партнера на следующих уровнях:

- закупочная организация;
- закупочная организация/завод;
- закупочная организация/субассортимент поставщика;
- закупочная организация/завод/субассортимент поставщика.

Данный отчет о поставщике можно дополнить дополнительными полями, позволяющими делать более объективные суждения о его добросовестности.

Анализ поставщика может проводиться по следующим критериям:

- массовость адреса контрагента;
- время существования КА;
- дисквалификация директора;
- банкротство контрагента;

- наличие в ЕГРЮЛ;
- наличие в базе судебных приставов;
- наличие арбитражных дел;
- действительность паспорта руководителя или ИП;
- действительность лицензий на осуществление деятельности;
- наличие в реестре недобросовестных поставщиков.

Все эти данные можно получить из открытых источников, например, из реестра ЕГРЮЛ/ЕГРИП на сайте Федеральной налоговой службы (<https://egrul.nalog.ru/index.html>), картотеки арбитражных дел (<https://kad.arbitr.ru/>), реестра сведений о банкротстве (<https://old.bankrot.fedresurs.ru/>), перечня организаций и физических лиц, в отношении которых имеются сведения об их причастности к экстремистской деятельности или терроризму (<https://www.fedsfm.ru/documents/terr-list>) и других источников. Возможна также загрузка показателей по бухгалтерской и финансовой отчетности и различных коэффициентов из системы «Спарк» (<https://spark-interfax.ru/>).

Конечно, на сегодняшний день многие организации заранее собирают документы для проверки благонадежности контрагента и создают собственное досье. Мы предлагаем автоматизировать этот процесс. Данные из открытых ресурсов будут загружаться в различные таблицы в рамках базы данных «Проверка поставщика». Ключевым полем со стороны SAP будет выступать уникальный системный номер контрагента. Загрузка и поиск информации из интернет-ресурсов будет происходить по одному из идентификационных данных (или набору нескольких идентификаторов) таких, как ИНН, название, ОГРН и т.д. Выборка данных из интернет-ресурсов будет происходить через REST API ABAP.

REST API – это архитектурный стиль, который использует HTTP в качестве протокола передачи данных для запросов и ответов. Это набор правил для разработчиков программного обеспечения о том, как они должны организовать написание кода серверного приложения, чтобы различные системы могли легко обмениваться данными и масштабировать приложение [5].

REST не имеет какого-то одного стандарта, но при этом должны соблюдаться основные принципы:

1. Архитектура клиент-сервер;
2. Единый интерфейс;
3. Отсутствие состояния между запросами;
4. Кешируемость;
5. Слои;
6. Код по требованию.

Предположим, что существует сервер, который получает входящие сообщения REST и отправляет некоторые данные вместо HTML, и тот, кто отправляет запрос, решает, что делать с этими данными, представлять ли их на веб-странице или перенаправлять. Запросы могут поступать от любого клиента. Таким образом, через REST API мы можем получить базу данных с информацией следующего рода:

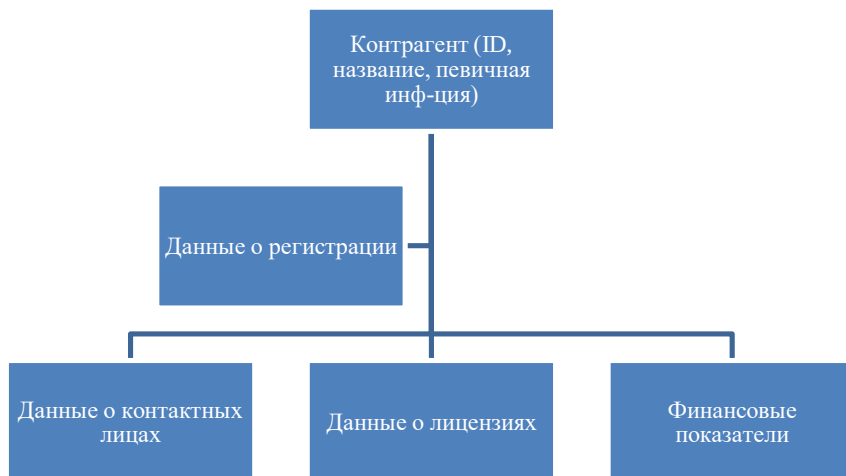


Рисунок 4 – БД с информацией о поставщике

Из данной БД впоследствии через Z-разработку может быть сформирован пользовательский отчет. На селекционный экран будет выведено поле ввода «ID контрагента» с возможностью множественного выбора. После введения пользователем всех номеров КА, участвующих в торгах, будет сформирован ALV-Grid отчет с результатами анализа поставщика. ALV Grid позволяет пользователю отображать отчет в желаемом виде. Пользователю доступны такие операции как: отображение или скрытие указанных полей, изменение порядка вывода столбцов.

Таблица 1 – Примерный вид отчета

<ID контрагента>	<Дата регистрации>	<Место регистрации>	<Массовость адреса>	<Руководитель>	<Наличие в перечне ПОД/ФТ>	<Дисквалификация директора>	

Таким образом, информация о маркерах «подозрительности» по всем возможным поставщикам будет собрана автоматически. Данная система сбора информации может значительно облегчить анализ поставщика на

предмет его добросовестности. Критерии анализа могут быть изменены в соответствии со спецификой закупки/организации. Применение данного метода может стать основой для создания более крупной аналитической системы для выбора поставщика в конкурсной закупке.

Список использованных источников:

1. Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05 апреля 2013 года № 44-ФЗ (ред. от 02 июля 2021 года) [Электронный источник] / http://www.consultant.ru/document/cons_doc_LAW_144624/ (дата обращения 18 ноября 2021 года).
2. Официальный сайт Единой информационной системы в сфере закупок [Электронный ресурс] // Закупки. URL : <https://zakupki.gov.ru/epz/main/public/home.html> (дата обращения 18 ноября 2021 года).
3. SAP Blog [Электронный ресурс] // A Look at Materials Management and Logistics in SAP S/4HANA. URL : <https://blog.sap-press.com/a-look-at-materials-management-and-logistics-in-sap-s4hana> (дата обращения 18 ноября 2021 года).
4. Deloitte [Электронный ресурс] // Demystifying SAP S/4HANA for Finance professionals. URL : <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/technology/deloitte-nl-technology-sap-s4hana-professionals.PDF> (дата обращения 18 ноября 2021 года).
5. IBM [Электронный ресурс] // REST APIs. URL : <https://www.ibm.com/cloud/learn/rest-apis> (дата обращения 18 ноября 2021 года).

УДК 005.52:338.436.33

© С.И. Метонидзе, Е.В. Савин, Т.Н. Бочкарева, 2021

Анализ перспектив развития предприятий агрохимической отрасли на примере ПАО «Уралкалий»

С.И. Метонидзе

студент 4 курса НИЯУ МИФИ, Москва

E-mail: metonidze.sofia@yandex.ru

Е.В. Савин

студент 4 курса НИЯУ МИФИ, Москва

E-mail: savin.evgeniy.victorovich@gmail.com

Т.Н. Бочкарева

к.т.н., доцент кафедры финансового менеджмента

НИЯУ МИФИ, Москва

E-mail: tnbochkareva@mephi.ru

Аннотация: В данной статье рассмотрены возможности применения эконометрических инструментов моделирования для оценки перспектив развития предприятий агрохимической отрасли на примере ПАО «Уралкалий». Авторами проведен фундаментальный анализ выручки ПАО «Уралкалий» за 2010–2020 гг. и оценки факторов, на нее влияющих.

Ключевые слова: агрохимическая отрасль, оценка перспектив развития, моделирование выручки, фундаментальный анализ выручки.

Analysis of prospects for the development of agrochemical industry enterprises on the example of PJSC Uralkali

Abstract: This article discusses the possibilities of using econometric modeling tools to assess the prospects for the development of enterprises in the agrochemical industry on the example of PJSC Uralkali. The authors conducted a fundamental analysis of the revenue of PJSC Uralkali for 2010-2020 and an assessment of the factors affecting it.

Keywords: agrochemical industry, assessment of development prospects, revenue modeling, fundamental revenue analysis.

Устойчивое продовольственное снабжение является одним из определяющих факторов национальной экономической безопасности. На обеспечение стабильного развития данного фактора влияют мощности отраслей обслуживания агропромышленного комплекса. Среди данных отраслей можно выделить агрохимический сектор, основной задачей

которого является изготовление вспомогательного продукта для увеличения объемов и повышения качества продукции растениеводства.

Географические и геологические особенности России обусловили формирование крупного, второго по объему национального производства минеральных удобрений после Канады, промышленного агрохимического комплекса мирового масштаба. Отечественная агрохимическая индустрия прежде всего представлена отраслью минеральных удобрений. Промышленность минеральных удобрений - один из значительных сегментов отечественной экономики, а также одна из значимых статей российского экспорта.

Богатая сырьевая база дает возможность выпускать широкий спектр минеральных удобрений, в том числе: азотные, фосфорные и калийные. [5]

Совершенствование и модернизация существующих производственных мощностей, направленных на повышение эффективности, рациональности ресурсоснабжения и экологической безопасности позволяет сохранить конкурентоспособность на глобальном рынке и ведет к снижению негативного влияния на окружающую среду.

К основным факторам конкурентоспособности отечественного производителя относятся: расширение производства сложных и комплексных удобрений, доступ к дешевому сырью и низкая себестоимость производства.

Сегодня агрохимическая промышленность перешла на новый эволюционный этап: на передний план выходит экономическая эффективность. Но, помимо этого, в рамках современных реалий необходимо наравне с результативностью ведения хозяйства выполнять и социальный запрос на экологичность. [6]

Успешное функционирование предприятия в рассматриваемой отрасли лежит в основе работы на стыке принципов устойчивого развития: экологической, социальной и управленческой ответственности.

По текущим данным агрохимический рынок постепенно растет, по итогу 2020 года объемы производства минеральных удобрений увеличились на 6,6% и достигли 54,7 млн тонн удобрений в физическом весе (рисунок 1). [8]

Протекционистская политика государства благоприятно повлияла на развитие аграрной отрасли и способствовала сохранению стабильного спроса внутри страны. За последние 10 лет потребление минеральных удобрений сельскохозяйственными организациями в России выросло в 1,6 раза, составив в 2020 году 3,1 млн тонн. (рисунок 2) [2]



Рисунок 1 – Объем производства удобрений, млрд т



Рисунок 2 – Внесение минеральных удобрений под посевы в сельскохозяйственных организациях по РФ, млн т.

На фоне активного роста аграрного сектора становится очевидной необходимость наращивания объемов и товарной номенклатуры производства удобрений, а также повышение технологической составляющей. Так в текущем году наблюдается увеличение потребности агропроизводителей в более сложных удобрениях, содержащих дополнительные питательные микроэлементы и вещества, имеющих более

удобную конфигурацию для использования. Также появляется спрос на комплексные индивидуальные удобрения - тукосмеси, изготавливаемые для определенных отраслей сельскохозяйственной промышленности и отдельных агрокомпаний, на основе специфики почв и сельскохозяйственных культур.

За последние три года показатели инвестиций в основной капитал имеют положительную динамику: финансирование за счет собственных средств растет, а привлечение средств извне уменьшается. В период с 2015 по 2020 года объем инвестиций в основной капитал крупных и средних компаний отрасли вырос на 47,06 млрд руб. (рисунок 3)

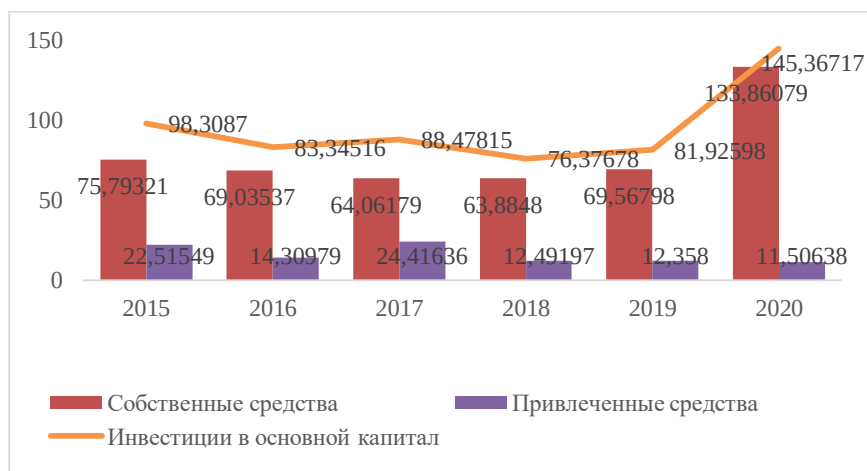


Рисунок 3 – Инвестиции в основной капитал крупных и средних компаний, млрд руб.

На данный момент уровень внесения удобрений в России ниже рекомендуемой нормы на 18–17 кг на гектар, что значительно уступает показателям ведущих европейских стран. Производители удобрений рассматривают данную ситуацию как огромный потенциал российского агропромышленного комплекса.

В течение пяти ближайших лет Российская ассоциация производителей минеральных удобрений планирует инвестировать более 1 трлн рублей в расширение производственных мощностей.

На данный момент отечественное производство способно полностью обеспечить внутренний рынок минеральных удобрений. Доля импорта, не превышает 2% от общего потребления.

Из года в год агрохимическая отрасль поддерживает свою экспортоориентированность. В 2020 году на фоне растущего спроса на внутреннем рынке доля экспортной продукции минеральных удобрений снизилась, составив 34,1 млн тонн в натуральном выражении – 62,4% от общего объема российского производства. За прошедшие 8 месяцев 2021 года показатели свидетельствуют о положительной динамике спроса: ростом азотных удобрений на 1,5%, калийных удобрений на 34,2% и смешанных удобрений на 2,9% относительно аналогичных показателей 2020 года (рисунок 4).

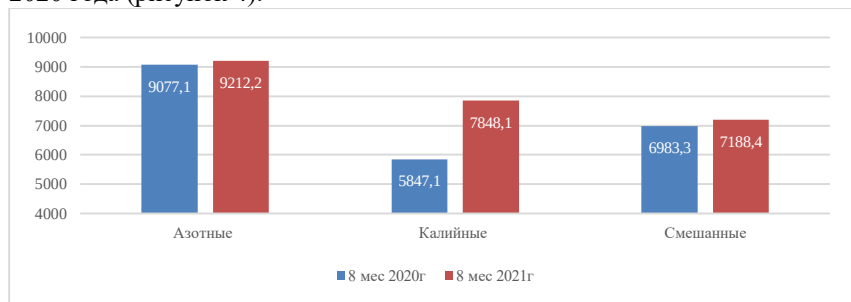


Рисунок 4 – Экспорт удобрений в физическом выражении за 8 мес. 2020г и 2021г, тыс. тонн

Список стран-потребителей российских удобрений насчитывает свыше 130 стран мира. Около 20% от объема экспорта приходится на Бразилию. За 2020 год Россия поставила в Южную Америку порядка 7 млн тонн удобрений: 2,9 млн тонн – азотных, 2,7 млн тонн – комплексных и 1,4 млн тонн – калийных удобрений.

Также к ключевым потребителям российской продукции относятся Китай, Эстония, Индия, Индонезия и США (рисунок 5).

Около 70% мирового олигополистичного рынка калийных удобрений концентрируется в руках отечественного, канадского (PotashCorp) и белорусского производства (Беларуськалий).

Крупнейшим производителем калийных удобрений в России является ПАО «Уралкалий». На его долю приходится свыше 80% от общего объема калийных удобрений, произведенных на территории России. Производственные активы данной компании включают пять рудников и семь обогатительных фабрик, расположенных в Пермском крае.

География продаж ПАО «Уралкалия» насчитывает более 70 стран мира. К основным рынкам сбыта относятся: Бразилия, Индия, Китай, Юго-Восточная Азия, Россия, США и страны Европы.

Компанию можно назвать вертикально интегрированной, так как она ведет деятельность по всей цепочке создания стоимости — от добычи калийной руды до поставок готовой продукции потребителям по всему миру.



Рисунок 5 – Структура экспорта минеральных удобрений и химических калийных удобрений за 2020г, тыс. тонн

Чтобы понять, насколько рационально использовались ресурсы компании в процессе достижения поставленных целей, необходимо обратиться к оценке экономической эффективности данного предприятия.

Одним из критериев, который непосредственно отображает динамику эффективности, является выручка.

В данной статье рассмотрены эконометрические инструменты моделирования для фундаментального анализа выручки ПАО Уралкалий от внешнеэкономической деятельности за 2010–2020 годов и оценки факторов, на нее влияющих.

В основе эконометрического моделирования лежит анализ временных рядов. Этот анализ позволяет прогнозировать изменения выручки компаний с учетом влияющих факторов. [1]

Информационной базой послужили данные из бухгалтерского баланса и пояснительной записки рассматриваемой компании, статистические данные мира и ближайшей страны-конкурента, Белоруссии, за период с 2010 г. по 2020 г.

Далее был выбран ряд факторов, которые, по мнению авторов, могли оказывать влияние на изменение выручки выбранного предприятия. В

качестве источника информации использовались данные официальной статистики (Федеральной службы государственной статистики РФ и Национального статистического комитета Республики Беларусь) и отчетности ПАО Уралкалий. [4]

Чтобы сгладить временные ряды, для всех факторов и значений выручки был рассчитан темп роста к предыдущему аналогичному периоду. (таблица 1)

Таблица 1 – Динамика выручки Уралкалия от внешнеэкономической деятельности, %

Год	Темпы роста выручки Уралкалия от внешнеэкономической деятельности, %
2020	91,196734
2019	105,732295
2018	113,090689
2017	103,615935
2016	72,9064799
2015	141,716679
2014	129,971448
2013	90,4904388
2012	88,4462676
2011	231,200619
2010	100

В качестве факторов, предположительно оказывающих влияние на изменение выручки (Y) рассматриваемой компании, были выбраны следующие макроэкономические и отраслевые факторы (таблица 2):

- Себестоимость производства минеральных удобрений, тыс. руб. – X1; [4]
- Грузоперевозки, млн тонн – X2; [8]
- Мировое потребление калийных удобрений, тыс. тонн – X3; [9]
- Изменение дивидендных выплат Уралкалия (размер дохода на одну акцию), руб. – X4; [4]
- Плечо финансового рычага Уралкалия – X5;
- Основные средства Уралкалия в денежном выражении, тыс. руб. – X6; [4]
- Объем экспорта Белоруссии, тыс. тонн – X7; [3]
- Стоимость экспортируемого из Белоруссии калия, долл. США – X8.[3]

Построим модель вида:

$$Y_i = \beta_0 + \beta_1 x_{i1} + \beta_2 x_{i2} + \dots + \beta_k x_{ik} \quad (1)$$

После построения модели указанным методом было получено уравнение вида:

$$Y_i = -60.58030 - 0.05962x_1 - 1.29380x_2 + 0.54232x_3 - 0.03038x_4 + 0.11941x_5 + 1.30006x_6 - 0.61245x_7 + 1.60574x_8 \quad (2)$$

Из уравнения регрессии можно сделать вывод, что наиболее значимое влияние на Y (выручку ПАО «Уралкалий») оказывают X_2 (грузоперевозки, млн тонн), X_6 (основные средства ПАО «Уралкалий» в денежном выражении, тыс. руб.) и X_8 (стоимость экспортируемого из Белоруссии калия, долл. США).

Таблица 2 – Темпы роста рассматриваемых показателей, %

y	x1	x2	x3	x4	x5	x6	x7	x8
91,19673	115,6011	94,94929	103,6949		0	156,9711	107,5156	114,6779
105,7323	101,9472	102,41	99,46919		100	73,19561	113,3568	94,20616
113,0907	105,6455	102,3218	98,05284	895,5224	74,99533	113,1112	102,7393	120,12
103,6159	121,4057	100,9933	104,4945	4,689906	65,3607	98,26135	112,7918	111,907
72,90648	107,3963	100,5727	104,7696	43,45419	73,53859	112,2022	102,7553	75,53431
141,7167	106,3471	98,53788	102,5388	0,154281	102,5329	124,0358	97,08042	100,2047
129,9714	111,84	96,63979	106,1084	84,585	192,2593	104,9519	166,4242	130,0383
90,49044	107,0885	96,5783	107,3441	49,54359	183,2968	107,8941	93,67675	77,08826
88,44627	121,3557	103,0113	101,7391	124,7139	158,5387	105,0112	78,09706	79,47455
231,2006	162,024	107,7466	103,1919	610,2161	223,7328	157,1186	112,3655	150,5385
100	100	100	100	100	100	100	100	100

Хоть уравнение и получилось значимым, сказать о его достоверности нельзя, так как мы имеем маленькое значение статистики Фишера (F-statistic: 33.62). Также все переменные в уравнении регрессии являются незначимыми, кроме X_6 и X_8 . Заметим, что коэффициент детерминации является высоким (Multiple R-squared: 0.9926) и описывает 99% вариаций между выбранными признаками.

Такая оценка уравнения регрессии может быть вызвана мультиколлинеарностью объясняющих переменных.

Далее рассмотрим график распределения регрессионных остатков и проведем тест Шапиро-Уилка, данный тест хорошо описывает выборки небольшого объема ≤ 100 . (рисунок 6)

График регрессионных остатков показал, что они принадлежат нормальному закону распределения. А тест Шапиро-Уилка подтвердил выдвинутую гипотезу о нормальности их распределения ($p\text{-value} = 0.7234 > 0,05$). Что позволяет осуществлять дальнейшее исследование модели.

Одним из ярко выраженных признаков мультиколлинеарности является высокая оценка коэффициентов корреляции.

Построим корреляционную матрицу на основе коэффициента линейной корреляции Пирсона для оценки взаимосвязи темпов роста всех выбранных (объясняющих) показателей с темпами роста выручки исследуемой компании и взаимосвязи факторных показателей друг с другом (таблица 3).

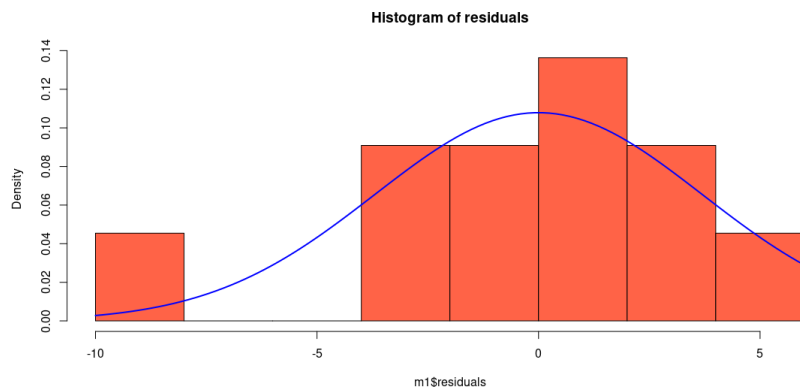


Рисунок 6 – График распределения регрессионных остатков

Таблица 3 – Корреляционная матрица

	y	x1	x2	x3	x4	x5	x6	x7	x8
y	1	0,7818237	0,5595493	-0,0299151	0,4853392	0,5148142	0,8809952	0,2598922	0,8402846
x1	0,7818237	1	0,6100164	0,1904196	0,3598106	0,605458	0,7459342	0,1182703	0,5834053
x2	0,5595493	0,6100164	1	-0,4576758	0,5970329	-0,0136197	0,6116894	-0,3215323	0,4775175
x3	-0,0299151	0,1904196	-0,4576758	1	-0,5106807	0,4926627	-0,0510416	0,4093163	-0,1569023
x4	0,4853392	0,3598106	0,5970329	-0,5106807	1	0,0762239	0,4981698	-0,0232145	0,5878807
x5	0,5148142	0,605458	-0,0136197	0,4926627	0,0762239	1	0,4383915	0,3286182	0,2916295
x6	0,8809952	0,7459342	0,6116894	-0,0510416	0,4981698	0,4383915	1	-0,0247712	0,5682287
x7	0,2598922	0,1182703	-0,3215323	0,4093163	-0,0232145	0,3286182	-0,0247712	1	0,5511764
x8	0,8402846	0,5834053	0,4775175	-0,1569023	0,5878807	0,2916295	0,5682287	0,5511764	1

В корреляционной матрице наблюдается наличие высоких коэффициентов корреляции нашего объясняемого фактора (Y) с объясняющими показателями ($X_1, \dots, X_8$). К показателям, очевидно коррелирующим с Y, относятся: X_1, X_6, X_8 , так как их значения корреляции превышают пороговые значения в 0,6-0,8.

Также из корреляционной матрицы видно наличие коррелирующей связи между самими объясняющими показателями ($X_1, \dots, X_8$), среди них: X_1 и X_2 , X_1 и X_5 , X_1 и X_6 , X_2 и X_6 . Данный факт говорит о наличии мультиколлинеарности.

Для ее устранения воспользуемся методом пошаговой регрессии с включением и исключением переменных.

После проведенного исследования лучшие результаты показал метод пошаговой регрессии с исключением переменных.

$$\hat{Y} = \underset{(99.588974)}{-1.413244} - \underset{(-1.007047)}{1.406423}x_2 - \underset{(0.009357)}{0.031567}x_4 + \underset{(0.042269)}{0.120910}x_5 + \underset{(0.195029)}{1.311952}x_6 - \underset{(0.185631)}{0.569389}x_7 + \underset{(0.208679)}{1.558821}x_8 \quad (3)$$

Уровень значимости регрессии повысился (p-value: 0.000354).

Значение статистики Фишера выросло (F-statistic: 85.68).

А величина коэффициента детерминации осталась на том же уровне (Multiple R-squared: 0.9923), так же повысился скорректированный коэффициент детерминации (Adjusted R-squared: 0.9807). Возрос уровень значимости признаков, теперь можно с большей уверенностью сказать, какие признаками оказывают наибольшее влияние, к таким относятся: X4, X5, X6, X7 и X8. Признак X2 хоть и оказывает значимое влияние на нашу модель, но имеет недостаточный уровень значимости.

Далее проведем исследование регрессионных остатков на нормальность. Сделаем вывод об их распределении (рисунок 7).

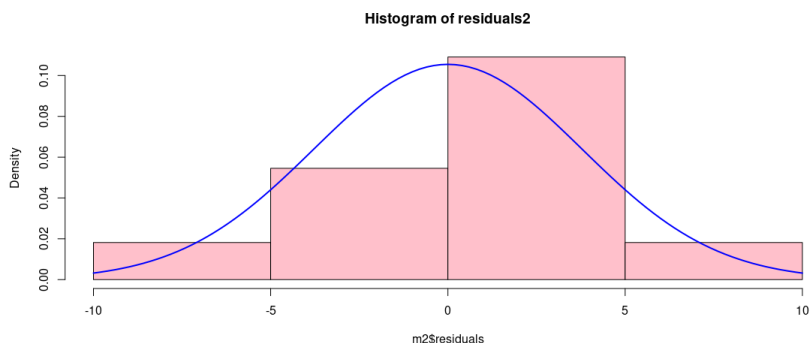


Рисунок 7 – График распределения регрессионных остатков

Нормальность их распределение подтвердилась графиком и тестом Шапиро-Уилка (p-value = 0,4002).

Проверка выполнения требований, предъявляемых к линейным моделям, подтвердила ее качество.

Следует объяснить взаимосвязь выручки с плечом финансового рычага и дивидендными выплатами, так как их наличие напрямую в модели экономически не обосновано.

Дивиденды и плечо финансового рычага характеризуют стратегию финансирования деятельности компании и в этой модели опосредованно показывают ее влияние на выручку. Поскольку дивиденды являются частью чистой прибыли, которая может быть либо выплачена акционерам, либо капитализирована и направлена на развитие основных производственных фондов компании. Нарастивание производственного потенциала способствует росту производства и, естественно, росту доходов (выручки). Компенсация "проедания" собственного капитала за счет привлечения платных устойчивых источников финансирования приводит к тому, что инвестиционные возможности компании ухудшаются из-за необходимости уплаты стоимости привлеченных обязательств, что негативно сказывается на перспективах роста доходов от основного вида деятельности.

Проведен тест Дарбина-Уотсона на наличие автокорреляции, которая может привести к ухудшению качества МНК-оценок, а также к завышению оценок тестовых статистик, по которым проверяется качество модели. Данный тест показал отсутствие значимой статистической взаимосвязи, то есть принимается гипотеза об отсутствии автокорреляции. А также был апробирован тест на гетероскедастичность Бройша-Пагана, с целью исключения неэффективности оценок, полученных с помощью метода наименьших квадратов. Результат теста говорит о гомоскедастичности регрессионных остатков, значит, принимается гипотеза об отсутствии непостоянной дисперсии случайной ошибки полученной модели.

Можно сделать заключение о высоком качестве МНК-оценок и высокой значимости модели.

В итоге работы был построен график, который показал, как хорошо наша модель согласуется с реальными данными по выручке ПАО «Уралкалий» (рисунок 8).

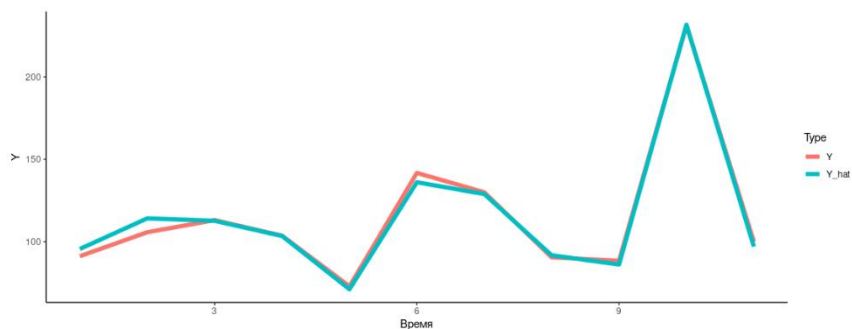


Рисунок 8 – График фактического и прогнозируемого изменения выручки

Модель ярко описывает ключевые факторы формирования выручки Уралкалия и позволяет сделать вывод о том, компании необходимо наращивать объем производственных мощностей. Для этого стоит прибегнуть к увеличению финансовых обязательств, но необходимо учитывать, что плечо финансового рычага не должно достигать предельных значений, так как это ведет к снижению финансовой устойчивости.

Анализируя текущую ситуацию заметно, что соотношение заемного капитала по отношению к собственным средствам снизилось и компания может позволить себе обратиться к заемным источникам финансирования с целью увеличения производства, но необходимо изменить стратегию финансирования. Поскольку практика обращения компании к заемным средствам в валюте привела к «проеданию» прибыли за счет курсовых разниц. При этом стоит отметить, что сильный рост плеча финансового рычага повышает зависимость от заемных средств и снижает устойчивость предприятия. (рисунок 9)

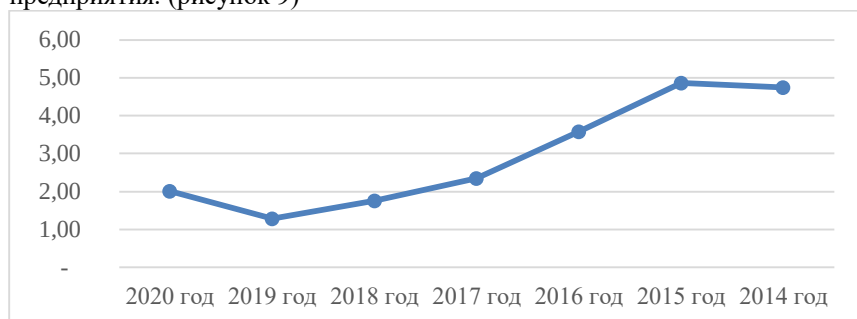


Рисунок 9 – График динамики плеча финансового рычага

Результаты моделирования также свидетельствуют о том, что увеличение экспорта из Белоруссии не оказывает значимого влияния на изменение выручки. Это обусловлено тем, что мировой спрос на калийные удобрения является высоким на всем рассмотренном периоде, и в ближайшей перспективе спад данного показателя крайне маловероятен. В то время как доля рынка Беларуськалия не превышает 20%, как и доля Уралкалия. Однако, повышение стоимости экспортируемых из Белоруссии калийных удобрений оказывает сильное влияние на изменение выручки анализируемой компании, что безусловно логично. Мировой рынок калийных удобрений олигополистичен, из-за малого количества игроков, разделивших этот рынок между собой. Поскольку Беларуськалий является

непосредственным конкурентом Уралкалия, то это предполагает взаимозависимость политики ценообразования.

Увеличение дивидендных выплат уменьшает величину нераспределенной прибыли, что негативно сказывается на динамике собственного капитала. Ведь та часть денежных средств, что пошла на выплату акционерам, могла быть инвестирована в обновление и наращивание производственных мощностей.

Использование этой модели позволяет изменять стратегию финансирования через управление дивидендной политикой при изменении ситуации на рынке (рост или падение спроса).

Как показала практика, выплата больших сумм дивидендов на протяжении достаточно длительного промежутка времени (2010–2014 гг.) привела к снижению доли собственного капитала в валюте баланса компании. Недостаток устойчивых источников финансирования компания была вынуждена компенсировать привлечением заемных обязательств.

На графике видно, что темп прироста устойчивых источников финансирования ниже, чем темп прироста долгосрочных обязательств, что может косвенно свидетельствовать о снижении финансовой устойчивости. А также согласуется с тем, что компании пришлось компенсировать уменьшение собственного капитала путем привлечения заемных обязательств. (рисунок 10)



Рисунок 10 – График динамики источников финансирования

Так как компания имеет устойчивую позицию на мировом рынке и является одним из лидеров по поставкам калийных удобрений в мире, на

данный момент ее стратегия должна быть сконцентрирована на устойчивое развитие деловой активности и охвата большего рынка сбыта, путем поддержания высокотехнологичности производственных процессов и их автоматизации с целью снижения себестоимости и уменьшения расходов.

Исходя из нынешней стратегии компании, представленной в годовых отчетах и новостных публикациях, можно утверждать, что сформулированные выводы согласуются с реальной картиной событий, компания находится на этапе накопления производственных мощностей и грамотного привлечения заемного капитала с целью освоения новых месторождений. Также уменьшился объем дивидендных выплат, что свидетельствует о направленности политики компании на увеличение капитала.

Список использованных источников:

1. М. Ю. Малкина, Е. К. Яковлева Анализ факторов роста курсовой стоимости акций российской компании (на примере ПАО «Уралкалий») // Региональная экономика: теория и практика, 2019. — т. 17 — вып. 1 — стр. 183–200. — URL: <https://cyberleninka.ru/article/n/analiz-faktorov-rosta-kursovoy-stoimosti-aktsiy-rossiyskih-kompaniy-na-primere-pao-uralkaliy/viewer>
2. Официальные статистические показатели РФ/ ЕМИСС. — URL: <https://www.fedstat.ru> (дата обращения — 11.11.2021)
3. Национальный статистический комитет Республики Беларусь. — URL: <https://www.belstat.gov.by> (дата обращения — 11.11.2021)
4. Отчетность ПАО Уралкалий/ Уралкалий. — 10.11.2021. — URL: https://www.uralkali.com/ru/investors/reporting_and_disclosure/ (дата обращения — 11.11.2021)
5. Российский рынок удобрений. Итоги 2020/ DigitalDynamicData. — 26.02.2021. — URL: <https://3dpro.info/site/reviews/russian-fertilizer-market/>
6. Рынок минеральных удобрений в России 2020: уверенный рост вопреки кризису/ DelovoyProfil. — 01.07.2020. — URL: <https://delprof.ru/press-center/open-analytics/rynok-mineralnykh-udobreniy-v-rossii-2020-uverennyy-rost-vopreki-krizisu/>
7. Топ стран-производителей калийных удобрений/ Marketpublishers. — 15.04.2019. — URL: <https://marketpublishers.ru/lists/11780/news.html>
8. Федеральная служба государственной статистики. — URL: <https://rosstat.gov.ru> (дата обращения — 11.11.2021)
9. International fertilizer association/ IFA. — URL: <https://www.fertilizer.org> (дата обращения — 10.11.2021)

Анализ перспектив развития трубной промышленности и ее роль в обеспечении экономической безопасности Российской Федерации

А.А. Стоянова

студент 4 курса НИЯУ МИФИ, Москва

E-mail: arina.stoyanova00@mail.ru

Т.Н. Бочкарева

к.т.н., доцент кафедры финансового менеджмента

НИЯУ МИФИ, Москва

E-mail: tnbochkareva@mephi.ru

Аннотация: В статье рассмотрены состояние и перспективы развития трубной промышленности России, ее роль в реализации программы импортозамещения. Отмечена значительная роль продукции предприятий трубной промышленности в обеспечении экономической безопасности России.

Ключевые слова: трубная промышленность, программа импортозамещения, экономическая безопасность, трубопроводный транспорт.

Analysis of the prospects for the development of the pipe industry and its role in ensuring the economic security of the Russian Federation

Abstract: The article examines the state and prospects of development of the pipe industry in Russia, its role in the implementation of the import substitution program. The significant role of the products of the pipe industry enterprises in ensuring the economic security of Russia is noted.

Keywords: pipe industry, import substitution program, economic security, pipeline transport.

Трудно переоценить роль трубной промышленности в мировой экономике. Ее продукция задействована практически во всех отраслях.

Китай занимает лидирующие позиции в мировой трубной промышленности. По приблизительным данным ИТА, в 2019 году в стране было произведено около 96 млн тонн стальных труб, или около 55% от общемирового показателя. Особенно велико доминирование китайских компаний в секторе бесшовных труб, доля которых превышает 65%.

США и Россия, занимающие второе и третье места в мировом рейтинге ведущих производителей труб, чередуются друг с другом. США значительно превосходят Россию в производстве сварных труб малого и среднего диаметра, широко используемых в национальной нефтегазовой промышленности; в то же время в России производится все больше бесшовных труб и ТБД.

Объемы производства стальных труб и соотношение сил основных мировых производителей труб в 2018-2019 гг. представлены в таблицах 1 и 2.

В последние годы в европейской трубной промышленности наблюдается спад. В частности, немецкие компании понесли большие потери. Это снижение производства обусловлено такими факторами, как снижение промышленного производства (которое в Германии непрерывно происходит с конца 2018 г), сокращение добычи нефти и газа в регионе Северного моря и низкая конкурентоспособность европейской продукции на внешних рынках из-за высоких затрат. Однако такие страны, как Италия и Германия, по-прежнему являются одними из ведущих экспортеров трубопроводной продукции. В число лидеров в этой сфере помимо Китая можно отнести Россию, Турцию, Южную Корею и Японию [1].

В 2020 году почти все крупные экспортеры труб сократили поставки на внешние рынки по сравнению с предыдущим годом. Основной причиной этой рецессии стало снижение спроса со стороны нефтегазового сектора, особенно в США, которые являются крупнейшим рынком сбыта для корейских и канадских компаний. В то же время Турции, третьему по величине экспортеру сварных труб малого и среднего диаметра, удалось немного увеличить поставки в 2020 году из-за более полного закрытия квот на экспорт продукции в европейские страны и увеличения продаж в Ирак и Израиль [6].

Анализ крупнейших импортеров (таблица 3) свидетельствует о том, что импорт стальных труб в Российскую Федерацию в последние годы ощутимо снижается.

Причина этого – стратегия импортозамещения, на которую российские предприятия были вынуждены перейти в результате введения США и странами Евросоюза антироссийских санкций.

В период массового строительства газопроводов отечественная металлургия не производила таких труб. Поэтом в 1970 г. между Советским Союзом и Федеративной Республикой Германия был заключен «контракт века»: договор на поставку труб большого диаметра западногерманских компаний и предоставление кредитов немецких банков в обмен на природный газ из Западной Сибири.

Таблица 1 – Объемы производства стальных труб в 2018–2019 гг., млн т [11]

Страна/ регион	Бесшовные трубы			Сварные трубы диаметром < 406			Сварные трубы диаметром > 406			Всего		
	2018	2019	Δ, %	2018	2019	Δ, %	2018	2019	Δ, %	2018	2019	Δ, %
КНР	27,5	28	1,8	59	60	1,7	8	8	0,0	94,5	96	1,6
ЕС	4	3,6	-10,0	8,2	8,4	2,4	1,5	0,9	-40,0	13,7	12,9	-5,8
в т.ч. ФРГ	1,3	1,1	-15,4	0,9	0,8	-11,1	0,9	0,4	-55,6	3,1	2,3	-25,8
СНГ	4,8	4,5	-6,3	6	6,2	3,3	3,2	3,6	12,5	14	14,3	2,1
в т.ч. РФ	3,9	3,8	-2,6	4,8	4,9	2,1	3,1	3,6	16,1	11,8	12,3	4,2
США	2,4	2,2	-8,3	8,4	7,9	-6,0	1,3	1,8	38,5	12,1	11,9	-1,7
Япония	1,4	1,3	-7,1	3,5	3,3	-5,7	1,2	1,5	25,0	6,1	6,1	0,0
Индия	0,5	0,6	20,0	1,6	1,6	0,0	2	2	0,0	4,1	4,2	2,4
Прочие	3,2	2,9	-9,4	18,8	19,7	4,8	4,6	4,7	2,2	26,6	27,3	2,6
Мир	43,8	43,1	-1,6	105,5	107,1	1,5	21,8	22,5	3,2	171,1	172,7	0,9

Таблица 2 – Крупнейшие экспортеры стальных труб в 2018–2019 гг., тыс. т [11]

Страна/ регион	Бесшовные трубы			Сварные трубы диаметром < 406			Сварные трубы диаметром > 406			Всего		
	2018	2019	2020	2018	2019	2020	2018	2019	2020	2018	2019	2020
Китай	4141	4350	3271	810	818	608	3121	3140	2998	8072	8308	6877
Италия	630	608	454	62	157	113	2722	2727	2408	3414	3492	2975
ФРГ	1165	1035	739	955	533	598	790	726	588	2910	2294	1925
РФ	774	644	532	998	744	567	688	717	827	2460	2105	1926
Турция	20	20	18	335	277	286	1600	1604	1589	1955	1901	1893
Корея	170	131	104	589	558	550	1279	1039	889	2038	1728	1543
Япония	953	924	717	546	478	328	229	199	169	1728	1601	1214
Индия	126	122	70	485	438	479	460	507	343	1071	1067	892
Канада	119	61	21	310	165	33	627	530	589	1056	756	643
США	252	193	156	57	80	63	733	525	420	1042	798	639

Таблица 3 – Крупнейшие мировые импортеры стальных труб в 2018–2019 гг., тыс. т [11]

Страна/ регион	Бесшовные трубы			Сварные диаметром < 406 трубы			Сварные трубы, прочие			Всего		
	018	019	020	018	019	020	018	019	020	018	019	020
США	337	809	49	078	12	35	223	828	996	638	449	080
Германи я	42	30	78	3	32	3	683	540	355	188	202	786
Канада	42	28	59	36	70	29	52	47	78	630	445	166
Франция	78	43	34	6	1	9	96	73	94	250	167	87
ОАЭ	40	83	02	81	51	07	74	88	01	195	222	10
Польша	91	74	54	13	5	9	51	74	17	55	13	50
КСА	22	01	01	39	7	27	14	34	58	75	32	86
Италия	47	47	67	09	40	65	26	76	39	82	63	71
Великоб ритания	09	09	60	8	8	74	95	58	31	52	55	65
Нидерла нды	32	82	28	14	6	6	97	85	30	43	63	54
РФ	17	99	19	5	03	0	02	4	2	64	96	31

С 2014 года Российская Федерация и ее крупные нефтегазовые проекты попали под антироссийские санкции: основным поставщикам труб большого диаметра, которые были необходимы для строительства ряда крупных нефте- и газопроводов, и обустройства новых месторождений углеводородов Восточной Сибири и Дальнего Востока, было «не рекомендовано» продолжать сотрудничество с российскими компаниями. Только в 2014 г. объем импорта трубопроводной продукции в Россию сократился на 25% по сравнению с предыдущим годом. Это позволило российским трубникам укрепить свои позиции на отечественном рынке [3].

В 2015 году специалисты Первоуральского новотрубного и Челябинского трубопрокатного заводов провели несколько встреч с представителями топливно-энергетических компаний («Газпром», «Роснефть», «Газпром нефть», «Лукойл»), в рамках которых были намечены первоочередные шаги по развитию научно-технического сотрудничества в сфере импортозамещения по реализации нового типа газопроводов. Основными объектами комплектации в сегменте труб большого диаметра (ТБД) для заводов стали проекты газопроводов «Сила Сибири» и «Ухта - Торжок-2».

Уже в 2016 г. общий объем отгрузки труб большого диаметра по этим проектам составил около 800 тыс. тонн. Результаты тестирования продукции российских трубных компаний были настолько высоки, что с 2016 г. добывающие и транспортирующие предприятия России полностью отказались от импорта некоторых типов труб и перешли на отечественные продукты [8].

Главным результатом 2017 года для трубных предприятий является 100%-ное замещение импорта труб большого диаметра при поставках на объекты «Газпрома». Сейчас для строительства магистральных газопроводов в Российской Федерации используются только отечественные трубы большого диаметра, то есть предприятия российской трубной промышленности в настоящее время выпускают продукцию, которая котируется на мировых рынках и обладает высокой конкурентоспособностью:

- ПАО «ЧТПЗ» стало расширять номенклатуру труб из нержавеющей стали и производство их фитингов;

- ПАО «Северсталь» начала осваивать технологию промышленного производства холодостойких (криогенных) конструкционных сталей с содержанием никеля 9%, используемых при производстве оборудования для транспортировки и хранения СПГ;

- рядом предприятий освоено производство труб с монослойным полиэтиленовым покрытием на основе материалов российского производства;

– разработаны и представлены на рынок премиальные типы резьбовых соединений.

По данным Фонда развития трубной промышленности [6], уже к 2018 году трубная отрасль не только решила задачу импортозамещения практически во всех сегментах российского рынка, но и создала инновационные продукты в ответ на потребности компаний нефтегазового сектора.

Анализ отрасли по методике Бостонской консалтинговой группы свидетельствует о том, что на рынке стальных труб нет выраженной компании-лидера (рисунок 1).

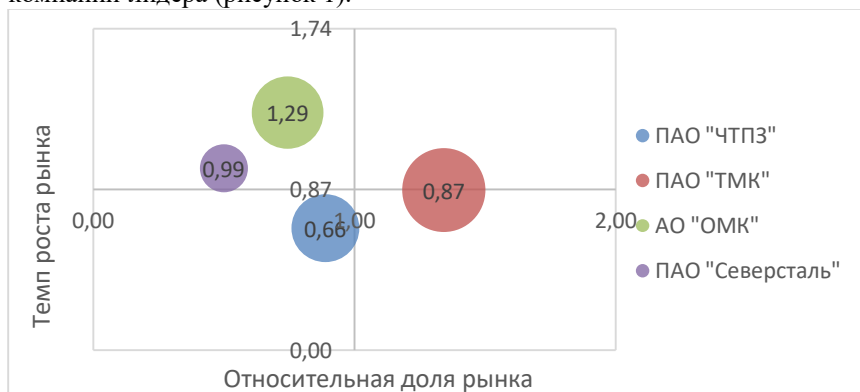


Рисунок 1 – Матрица БКГ: анализ российской трубной отрасли

На российском рынке присутствуют три категории игроков:

– «Трудные дети» - АО «ОМК» и ПАО «Северсталь». Разница между этими компаниями состоит в том, что для АО «ОМК» производство труб – это основной вид деятельности. ОМК реализует на предприятиях группы несколько крупных инвестиционных проектов. Основной целью программы капитальных вложений является комплексная модернизация и строительство новых объектов по производству труб для добычи и транспортировки нефти и газа. Инвестиции ОМК в инвестиционные проекты составляют 87 млрд руб.

ПАО «Северсталь» - одна из крупнейших вертикально интегрированных сталелитейных и горнодобывающих компаний с ключевыми активами в России. Отличие ПАО «Северсталь» от АО «ОМК» заключается не только в масштабах. Главное отличие состоит в том, что для ПАО «Северсталь» производство труб – только один из нескольких видов деятельности предприятия, доля которого в совокупных продажах составляет около 4%, а мощности по производству труб у ПАО «Северсталь» не самые высокие. Дальнейшее развитие этого вида деятельности связано со значительными

инвестициями. В конце апреля 2021 года ПАО "Северсталь" получило от ФАС разрешение на покупку 20% акций ООО "Производственное объединение Нижне-Волжский трубный завод" (НВТЗ). Решение о покупке акций НВТЗ укрепляет позиции "Северстали" на внутреннем рынке труб малого и среднего диаметра, а также в странах СНГ [1].

– «Дойные коровы» - ПАО «ТМК», занимающая наибольшую долю на рынке производства стальных труб. Приоритетным направлением для группы ТМК является нефтегазовая отрасль, на долю которой в 2020 г. пришлось 74% продаж. Значительное количество продукции ТМК поставляется ведущим российским нефтегазовым компаниям, таким как "Газпром", "Газпром нефть", "Лукойл", "Роснефть" и "Сургутнефтегаз". На эту пятерку крупнейших российских клиентов в 2020 году приходилось около 41% от общего числа проданных товаров. Продажи на российском рынке составили 77% от общей выручки ТМК, 11% от продаж на европейском рынке, страны СНГ, страны Ближнего Востока, Центральной и Юго-Восточной Азии и другие страны составили более 9% от выручки и 2% на рынки Северной и Южной Америки [7].

– «Хромые утки» - ПАО «ЧТПЗ». Место компании в отрасли в соответствии с матрицей БКГ определяется ее невысокой прибылью. Компания находится на фазе зрелости ведет борьбу за одну и ту же аудиторию с конкурентами, поэтому основное стратегическое направление деятельности компании – повышение качества продукции. Именно это является целью основных инвестиционных проектов ПАО «ЧТПЗ».

Конкурентный анализ отрасли с помощью метода «Пять сил Портера» свидетельствует о следующем:

1. Высокий уровень конкурентной борьбы;
2. Вход на рынок затрудняется наличием значительного количества институциональных барьеров: объём первоначальных инвестиций, лицензирование и сертификация, антидемпинговые меры на импорт и экспорт, а также экологические стандарты;
3. Угроза появления «товаров-заменителей» связана с появлением пластиковых труб. Пластиковые трубы обладают рядом преимуществ. В частности, вязкий и упругий материал выдерживает расширение из-за замерзания воды, не лопается при низких температурах. Труба малого диаметра выдерживает изгиб до 20 собственных радиусов без излома. Избыток давления нивелируется эластичностью стенки, которая возвращает начальную форму при стабилизации. Пластик не подвергается коррозии, благодаря чему срок эксплуатации пластиковых трубопроводов достигает 50 лет и более. Однако по своим прочностным характеристикам и вследствие низкой стойкости к высоким температурам пластиковые трубы могут конкурировать со стальными только в отдельных нишах. В

сфере коммунального хозяйства они действительно будут постепенно вытеснять стальную продукцию. Полимерные трубы позволяют экономить до 50% затрат на обслуживание водопроводов и канализации, при этом доля таких труб в России составляет лишь 35%, а в Европе – 85%. Но за пределами этого сектора замещение стальных труб полимерными маловероятно;

4. Влияние поставщиков на качество продукции предприятий трубной промышленности велико: первая причина – определенные требования к качеству и составу исходного сырья, которые могут удовлетворить только конкретные поставщики. Вторая причина – ограниченное число ключевых игроков на рынке поставщиков – поставщиков металла, что определяет долгосрочный характер взаимоотношений между предприятиями трубной промышленности и металлургами;

5. Влияние фактора «Власть покупателей» весьма значительно: с одной стороны, специфические требования к качеству, свойствам, размерам труб, с другой стороны, высокая конкуренция производителей между собой позволяют покупателю выбирать продукцию только самого высокого качества в сочетании с комплексными решениями по повышению сроков службы и снижению негативного воздействия на окружающую среду территорий присутствия.

Сопоставление данных по динамике потребления и объемов импорта стальных труб в РФ (рисунок 2 и 3) позволяют сделать следующий вывод:

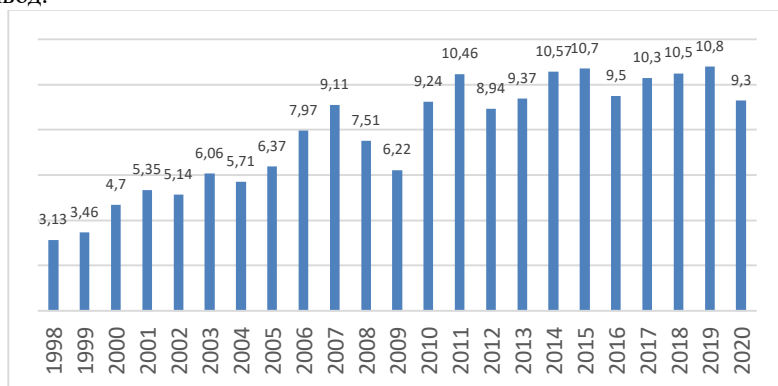


Рисунок 2 – Динамика потребления стальных труб в РФ в 1998–2020 гг., млн т [11]

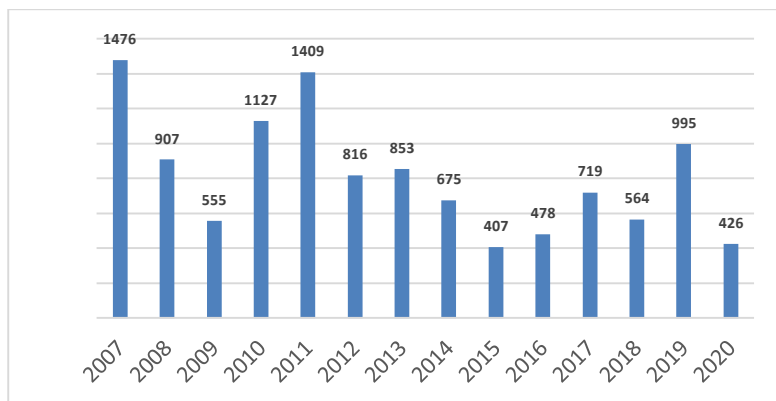


Рисунок 3 – Изменение объема импорта стальных труб в РФ в 2007–2020 гг., тыс. т [11]

разнонаправленность потоков потребления и импорта свидетельствуют о том, что интенсивное, и даже можно сказать, агрессивное развитие трубной промышленности – это не только решение ряда текущих экономических проблем, но снижение перспективной зависимости экономики России от нестабильности как в сфере политических решений, так и в сфере договорных отношений.

Проведенные исследования свидетельствуют о том, что интенсификация трубной промышленности, как следствие не только выбора, но и успешной реализации программы импортозамещения, вносит серьезный вклад в обеспечение экономической безопасности государства: принятие комплекса антироссийских санкций явилось своеобразным катализатором для российской металлургической промышленности, которая в короткий срок освоила выпуск необходимого оборудования и смогла обеспечить бесперебойную поставку труб необходимого типа, диаметра и качества на объекты народного хозяйства:

- глубокая реструктуризация производственных процессов обеспечила крупнейшим трубным компаниям современное электросталеплавильное производство, новые прокатные станы, новые резбонарезные мощности и линии финишной отделки, стимулировала создание научно-исследовательских центров и центров обучения персонала;

- выпускаемый продукт стал более сложным;
- цифровые технологии минимизировали влияние человеческого фактора и ускорили обмен информацией.

В результате качество и эксплуатационная надежность российских труб вышли на новый уровень, а объем выпускаемой продукции способен удовлетворить любые потребности как предприятий сферы ЖКХ, так и нефтегазового комплекса России, который нуждается в продукции трубной промышленности и при освоении и обустройстве месторождений углеводородов, и для транспортировки газа, нефти и нефтепродуктов.

Список использованных источников:

1. <https://metallobazy.ru/news/1630>
2. <https://metallurgprom.org/articles/analytics/3823-jekspress-analiz-rynka-chnoj-metallurgii-v-novyh-jekonomicheskikh-uslovijah-predprijatija-gotovjatsja-k-zatjazhnomu-krizisu.html>
3. <https://sdelanounas.ru/blogs/139882/>
4. <http://www.morvesti.ru/themes/1694/86997/>
5. <http://gksofia.ru/novosti/novosti-metallurgii/1312-rossijskie-trubnye-kompanii-uspeshno-razvivayut-importozameshchenie>
6. <https://www.metaltorg.ru/analytics/publication/?id=4351>
7. <https://newsland.com/community/129/content/trubnaia-promyshlennost-rossii-dostigla-100-importozameshcheniia/6520516>
8. <https://finance.rambler.ru/other/44612397-importozameshchenie-kak-novaya-realnost/>
9. <https://www.metaltorg.ru/analytics/publication/?id=2951>
10. <http://www.garant.ru/article/630000/>
11. https://dcenter.hse.ru/godovye_obzory_po_otraslyam_i_rynkam

Анализ применения ESG-принципов в производственном учёте организаций радиоэлектронной промышленности

Л.В. Пермитина

преподаватель РЭУ имени Г.В. Плеханова, Москва

E-mail: permlyd@mail.ru

Аннотация: В статье проведен анализ применения в производственном учете предприятий радиоэлектронной промышленности принципов устойчивого развития. Обзор и анализ особенностей производственного учета предприятий радиоэлектронной промышленности базируется на основе оценки соответствия компонентов производственного учета ESG-принципам.

Ключевые слова: ESG-расходы, производственный учет, контроль, устойчивое развитие, ESG- риски.

Analysis of the application of ESG principles in the production accounting of radio-electronic industry organizations

Abstract: The article analyzes the application of the principles of sustainable development in the production accounting of radio-electronic industry enterprises. The review and analysis of the features of production accounting of radio-electronic industry enterprises is based on the assessment of compliance of the components of production accounting with ESG principles.

Keywords: ESG-expenses, production accounting, control, sustainable development, ESG- risks.

Одной из развивающихся отраслей современной экономики является радиоэлектронная промышленность. Рынки электронной продукции демонстрируют высокие и опережающие другие сектора темпы роста, их доля в мировой экономике уже сравнима с рынками энергоресурсов. Согласно Стратегия развития электронной промышленности РФ на период до 2030 года, в долгосрочной перспективе вхождение России в число мировых лидеров рынка электронной продукции обеспечит устойчивое развитие экономики наравне с долей в мировом рынке энергоресурсов [1]. Роль радиоэлектронной промышленности для поддержки устойчивого развития экономики страны и обеспечения ее информационной безопасности растет. Предприятия радиоэлектронной промышленности

обеспечивают техническую, экономическую, военно-стратегическую независимость РФ. Объем экспорта радиоэлектронной продукции произведенной российскими организациями в 2020 году составил 5,3 млрд. долларов США. Несмотря на сохраняющуюся импортозависимость в отдельных сегментах радиоэлектроники, к 2020 году удалось значительно увеличить долю российской продукции на внутреннем рынке, на конец 2019 года – 41% [1]. Доля радиоэлектронной промышленности во валовом внутреннем продукте РФ составляет 1,8%, уровень добавленной стоимости составляет 60-80%.

Одним из приоритетных направлений развития электронной промышленности согласно Стратегии развития являются обеспечение создания востребованных потребителем продуктов и организация экспансии на наиболее перспективные рынки, что в данный момент возможно лишь за счет ориентации деятельности предприятий на принципы концепции устойчивого развития.

Ресурсоемкость освоения новых технологических уровней в промышленности возрастает, а следовательно возрастают и расходы на производство продукции.

Усиление экономического, экологического и социального давления и другие процессы оказывают противоречивое влияние на российскую радиоэлектронную промышленность, генерируя и новые возможности, и новые угрозы, усиливая неопределенности как на стороне технологических возможностей, так и рынков.

Радиоэлектронная промышленность, являющаяся одной из развивающихся отраслей современной экономики, оказывает негативное влияние на изменение окружающей среды.

Основными загрязнителями окружающей среды от деятельности предприятий являются выбросы в атмосферу, сбросы со сточными производственными водами и ливневыми стоками, отходы (таблица 1).

Таблица 1 – Динамика основных показателей охраны окружающей среды предприятий радиоэлектронной промышленности [2]

Показатели	2016 г.	2017 г.	2018 г.	2019 г.	2020 г.
1) Выбросы загрязняющих атмосферу веществ, отходящих от стационарных источников всего, тысяч тонн	34,7	43,2	68,9	14,7	40,1
2) Улавливание и обезвреживание загрязняющих атмосферу веществ, отходящих от стационарных источников,	14,8	29,3	63,2	37,1	57,1

тысяч тонн					
3) Выбросы парниковых газов по секторам, млн. тонн CO ₂ -эквивалента в год (промышленные процессы и использование промышленной продукции)	293,5	280,4	283,3	243,3	237,4
4) Образование отходов производства и потребления, тысяч тонн	2099,2	599,4	378,1	777,7	278,4
5) Сброс загрязненных сточных вод в поверхностные водные объекты, миллионы куб. метров	4,5	4,0	3,8	3,1	2,6
6) Утилизация и обезвреживание отходов производства и потребления (тысяч тонн)	0,5	33,1	62,3	904,9	182,6

Во многих случаях главным катализатором усилий по обеспечению устойчивости радиоэлектронных предприятий являются возрастающие затраты на охрану окружающей среды (таблица 2).

Таблица 2 – Текущие затраты на охрану окружающей среды (в фактически действовавших ценах, миллионов рублей) [2]

Наименование текущих затрат	2016 г.	2017 г.	2018 г.	2019 г.	2020 г.
1) На охрану окружающей среды, всего	1389	1408	1464	1493	1445
2) На охрану атмосферного воздуха и предотвращение изменения климата	321	375	369	310	339
3) На сбор и очистку сточных вод	712	720	748	761	797
4) На обращение с отходами	240	258	275	339	218
5) На защиту и реабилитацию земель, поверхностных и подземных вод	11	12	16	20	18
6) На сохранение биоразнообразия и охрану природных территорий	0,6	0,8	0,8	1	0,7

Анализ практики реализации принципов концепции устойчивого развития свидетельствует о том, что наибольших успехов на данном

направлении добились те организации, которые ориентированы на производство продукции для реализации иностранным потребителям: предприятия нефтегазовой отрасли, добыча полезных ископаемых, черная металлургия, электроэнергетика. Наиболее авторитетным ESG-рейтингом является ESG Morgan Stanley Capital International (MSCI), охватывающий более чем 2 800 компаний, ранжируемых от наивысших (AAA, AA) и средних оценок (A, BBB, BB) до отстающих (B, CCC).

На сегодняшний день лидерами с ESG-рейтингом «А» от MSCI являются всего несколько российских компаний: Полиметалл, Полус и Новатэк.

Кроме перечисленных компаний, в России сформировался пул лидеров по абсолютному объему инвестиций в экологию и социальные проекты. Среди них можно выделить представителей металлургического сектора НЛМК, Северсталь и ММК, а также ГМК Норникель и ЭнеЛ Россия [3]. Российские предприятия радиоэлектронной промышленности (далее РЭП) в данных рейтингах отсутствуют.

При осуществлении анализа применения ESG-принципов в производственном учете организаций радиоэлектронной промышленности нами выбраны предприятия входящие в ТОП-25 организаций радиоэлектронной промышленности России по объему выручки продукции и услуг, поставленной на экспорт по данным на 2020 год (ОАО «Завод Манетон», ПАО «Мстатор», ПАО «Морион»). Считаем, что практика организации производственного учета данных промышленных предприятий в полной мере отражает специфику предприятий данной отрасли.

Анализ соответствия производственного учета на предприятиях РЭП ESG-принципам проводится по компонентам производственного учета: бюджетирование, учет и калькулирование, анализ, отчетность и контроль [4,5].

Одним из компонентов производственного учета автором выделено бюджетирование. На исследуемых предприятиях РЭП бюджетирование осуществляется с использованием 1С: ERP Управление предприятием. Традиционно бюджетирование на предприятиях РЭП подразумевает составление бюджет доходов и расходов, бюджетирование ESG-расходов не осуществляется.

Для учета расходов на предприятиях РЭП применяется позаказный метод. Для предприятий радиоэлектронной промышленности характерна высокая материалоемкость продукции (более 45%), удельный вес основной заработной платы находится на уровне 7% и более 50% занимают косвенные расходы.

Прямые расходы аккумулируются на счетах 20,23 (по дебету) а по кредиту счета 10,60,70,69,02 и т.д. Косвенные расходы аккумулируются на счетах 25 и 26. Со счета 25 расходы списываются на основное производство согласно выбранной базе распределения. Предприятия РЭП формируют производственную себестоимость продукции без общехозяйственных расходов. Управленческие (общехозяйственные) расходы отражаются полностью в отчете о финансовых результатах в качестве расходов в периоде их признания (не распределяются на остаток незавершенного производства) и ежемесячно полностью списываются со счета 26 «Общехозяйственные расходы» в дебет счета 90 «Продажи» (субсчет 90.08 «Управленческие расходы»).

Аналитический учет расходов на предприятиях РЭП осуществляется по статьям расходов по заказам.

Предприятия РЭП выбрасывают загрязняющие вещества в воздух, в водные объекты, образуются отходы, вследствие чего уплачивают платеж за негативное воздействие на окружающую среду (НВОС) [6].

Экологические расходы растворяются в элементе расходов «Прочие» и в статье затрат «Охрана труда».

На осуществление деятельности по сбору, транспортированию, обработке, утилизации, обезвреживанию, размещению отходов I-IV класса опасности предприятия РЭП получают соответствующее разрешение (лицензию), выданное Федеральной службой по надзору в сфере природопользования [7,8].

В учете суммы платы за НВОС и в пределах, и сверх нормативов, в пределах допустимых лимитов учитываются в составе общехозяйственных расходов в корреспонденции со счетом 76, к которому открыты субсчета:

- Расчеты по плате за загрязнение окружающей среды в пределах лимитов;

- Расчеты по плате за загрязнение окружающей среды сверх лимитов.

Также предприятия РЭП уплачивают экологический сбор [6,9] - неналоговый доход федерального бюджета, уплачиваемый производителями, импортерами товаров, подлежащих утилизации после утраты ими потребительских свойств. Сумма экологического сбора, в учете предприятий РЭП признается расходом и зависит от ставок устанавливаемых для групп товаров, подлежащих утилизации после утраты ими потребительских свойств.

Исходя из порядка взимания экологического сбора и Инструкции по применению Плана счетов, сумма экологического сбора, начисляемая по мере выпуска в обращение соответствующих товаров, отражается по дебету счета 44 «Расходы на продажу» в корреспонденции со счетом учета

расчетов с бюджетом (счет 68) и отражается в составе коммерческих расходов в бухгалтерской отчетности предприятия.

Затраты на утилизацию накопившихся отходов предприятия РЭП учитывают по дебету 25 счета; накопленные с утилизации суммы относятся на уменьшение начисленного ранее резерва (без уменьшения финансового результата) записью по дебету счета 96 и кредиту счета 25.

Социальные расходы частично представлены в элементе расходов «Расходы на оплату труда» и «Отчисления на социальные нужды» только в виде расходов на оплату труда, начисления по пособиям по временной нетрудоспособности и отчислений с сумм начисленных выплат во внебюджетные фонды и др. Расходы на обучение персонала и другие социальные расходы учитываются на исследуемых предприятиях также на счете 26.

Проблемы учета экологических расходов как на предприятиях РЭП, так и в целом на промышленных предприятиях заключается в точном определении сумм расходов связанных с нарушениями в экологической сфере, учетом и определениям точной суммы расходов по природоохранным мероприятиям, и расходам по возмещению ущерба при возникновении аварий, оказывающих негативное воздействие на окружающую среду.

При анализе отчетности на предмет соответствия международным и российским ориентирам, стандартам и лучшим практикам в области устойчивого развития и информационной открытости по исследуемым предприятиям были изучены годовые отчеты предприятий, бухгалтерская отчетность и другие документы.

Нефинансовые отчеты (отчеты об устойчивом развитии/социальный отчет) или интегрированный отчет на данных предприятиях РЭП не формируется. В годовых отчетах исследуемых предприятий, раздел, посвященный устойчивому развитию отсутствует.

Годовой отчет исследуемых предприятий РЭП не содержит информацию об экологических аспектах деятельности обществ. Целевые стратегические показатели в области охраны окружающей среды в годовом отчете предприятий РЭП не отражены.

Предприятия РЭП заполняют декларацию о потреблении энергетических ресурсов, что отражается в годовом отчете [10-12].

Исследования соответствия производственного учета ESG-принципам предприятий радиоэлектронной промышленности позволили установить, что:

- на предприятиях имеются утвержденная Политика в области организации управления рисками, но экологические и социальные риски в отчетности не отражены;

– в отчетности предприятий не установлены актуально значимые экологические и социальные цели; информация и динамика влияния деятельности предприятий на окружающую среду отсутствует; информация в годовой отчетности в социальной сфере описаны общими словами, имеется информация о фонде оплаты труда и средней заработной плате, а также имеется о вознаграждения акционерам; в отчетности отсутствует описание наиболее значимых социальных и благотворительных проектов;

– у предприятий радиоэлектронной промышленности состав основных социально-экологических рисков не определен, и не предпринимаются меры по управлению рисками в данной области. Годовая отчетность исследуемых предприятий РЭП не содержит исчерпывающего описания всех рисков, которые могут повлиять на деятельность предприятий;

– документы в отношении системы внутреннего контроля, описание процедур внутреннего контроля на предприятиях имеется; контроль экологических расходов затруднителен, вследствие их растворения в себестоимости по статье калькуляции «Охрана труда»; контроль социальных расходов заключается в контроле средней заработной платы и фонда заработной платы; контроль и регулирование расходов на выплаты в случае временной нетрудоспособности в результате полученных травм на рабочем месте; расходов на программы обучения и повышения квалификации/дополнительного образования для сотрудников и/или программы субсидирования обучения в ВУЗах; расходов на выплаты материальной помощи уязвимым категориям сотрудников/ семьям сотрудников не производится;

– на этапе разработки и подготовки к производству радиоэлектронной продукции, контролю экологических и социальных расходов и их учету уделяется не достаточное внимание, акцент установлен на контроль экономических расходов.

Рассмотренный в статье анализ применения в производственном учете предприятий радиоэлектронной промышленности принципов устойчивого развития позволяет сделать вывод о необходимости совершенствования производственного учета на основе принципов устойчивого развития.

Список использованных источников:

1. Стратегия развития электронной промышленности РФ на период до 2030 года [Электронный ресурс] URL: http://static.government.ru/media/files/1QkfNDghANiBUNBbXaFBM_69Jxd48ePeY.pdf (дата обращения 10.11.2021)
2. Охрана окружающей среды в России за 2016-2020 года: статистический

- сборник [Электронный ресурс] URL: <https://rosstat.gov.ru/folder/11194> (дата обращения 15.11.2021)
3. ESG-рейтинг Рейтинговое агентство АК&М [Электронный ресурс]. URL:<https://akmrating.ru/kompaniyesg/> (дата обращения 10.11.2021)
 4. Казакова Н.А., Пермитина Л.В. Совершенствование системы контроля расходов организаций на основе концепции устойчивого развития // Аудитор. 2021. № 10. С. 40-45.
 5. Казакова Н.А., Пермитина Л.В. Развитие производственного учета промышленных организаций на основе концепции устойчивого развития // Управленческий учет. 2021. № 10-1. С. 59-68.
 6. Об отходах производства и потребления. Федеральный закон от 24.06.1998 № 89-ФЗ // Официальный интернет-портал правовой информации [Электронный ресурс]. 2021 – URL: http://www.consultant.ru/document/cons_doc_LAW_19109/ (дата обращения 17.11.2021).
 7. Об утверждении критериев отнесения объектов, оказывающих негативное воздействие на окружающую среду, к объектам I, II, III и IV категорий. Постановление Правительства РФ от 31.12.2020 N 2398 – URL: http://www.consultant.ru/document/cons_doc_LAW_373399/ (дата обращения 17.11.2021).
 8. Об исчислении и взимании платы за негативное воздействие на окружающую среду. Постановление Правительства РФ от 03.03.2017 N 255 // Официальный интернет-портал правовой информации [Электронный ресурс]. 2021 – URL: http://www.consultant.ru/document/cons_doc_LAW_213744 (дата обращения 17.11.2021).
 9. О порядке взимания экологического сбора. Постановление Правительства Российской Федерации от 8.10.2015 N 1073. // Официальный интернет-портал правовой информации [Электронный ресурс]. 2021 – URL: http://www.consultant.ru/document/cons_doc_LAW_187199/ (дата обращения 17.11.2021).
 10. Официальный сайт ПАО «Мстатор». Режим доступа: <https://mstator.ru/ru> (дата обращения 15.11.2021)
 11. Официальный сайт ПАО «Морион». Режим доступа: <https://www.morion.ru/> (дата обращения 15.11.2021)
 12. Официальный сайт АО Завод «Магнетон» Режим доступа: <http://magneton.ru/> (дата обращения 15.11.2021)

Анализ применимости модифицированной модели Бениша для отчетности российских компаний

Е.А. Кузьмина

студентка 4 курса НИЯУ МИФИ, Москва

E-mail: nimzuchka@yandex.ru

Д.Р. Хамитов

студент 1 курса Сколковского института науки и технологий,

Москва

E-mail: hamitov.97@mail.ru

Е.В. Савин

студент 4 курса НИЯУ МИФИ, Москва

E-mail: savin.evgeniy.victorovich@gmail.com

Н.С. Белогина

к.э.н., доцент кафедры бухгалтерского учета и аудита

НИЯУ МИФИ, Москва

E-mail: nsbelogina@mephi.ru

Аннотация: В статье при помощи различных статистических метрик проведен анализ применимости существующей модифицированной модели Бениша для российских компаний, а также предложены альтернативные варианты адаптации данной модели на существующих данных с целью упрощения выявления фальсификации бухгалтерской финансовой отчетности в российских компаниях.

Ключевые слова: аутлаеры, боксплоты, корреляция регрессоров, логистическая модель, матрица ошибок, сбалансированная выборка, фальсификация финансовой отчетности.

Analysis of the applicability of the modified Benish model for the financial statements of Russian companies

Abstract: Using various statistical metrics, the article analyzes the applicability of the existing modified Benish model for Russian companies, and also offers alternative options for adapting this model to existing data in order to simplify the identification of falsification of financial statements in Russian companies.

Keywords: outliers, boxplots, correlation of regressors, logistic model, error matrix, balanced sampling, falsification of financial statements.

Введение. В настоящее время финансовая грамотность людей в развитых и развивающихся странах стремительно возрастает; население всё чаще предпочитает пользоваться различными финансовыми инструментами [9], будь то банковские вклады, инвестиции на фондовом рынке или манипуляции с недвижимостью. Все перечисленные методы объединяет вынужденный риск, направленный на повышение потенциальной доходности. Помимо различных экономических факторов, будь то внешнеэкономическая среда или политическая обстановка, существует ненулевая вероятность искажения отчетности самой организацией с целью выстраивания положительной картины для внешних пользователей, в том числе для потенциальных инвесторов. Анализ, проведенный по такой отчётности, будет нерелевантным, а доступ к другим источникам информации существенно ограничен.

Основная часть.

Виды искажения отчетности. Искажение бухгалтерской отчетности может быть нескольких видов, в зависимости от степени тяжести последствий и намерений организации. Согласно статье 172.1 Уголовного кодекса Российской Федерации, преднамеренное внесение заведомо ложных сведений о сделках, об обязательствах, имуществе организации или о ее финансовом положении называется фальсификацией бухгалтерской отчетности [1]. Помимо фальсификации, многие ученые в своих работах на тему искажения бухгалтерской отчетности так же выделяют такое понятие как «вуалирование» [3,4,5]. При анализе статей на данную тему прослеживается общая мысль о том, что термин «вуалирование» обычно применяется для искажения бухгалтерской финансовой отчетности в рамках существующих стандартов и законов. (Табл.1)

Таблица 1 – Термин «вуалирование» в научной литературе

Источник	Определение
С.М. Бычкова, Е.Ю. Итыгилова «Искажения бухгалтерской финансовой отчетности в аудите» Монография	«Вуалирование баланса подразумевает искажения в бухгалтерской отчетности в пределах, разрешенных нормативными документами.» [3]
Иоган Фридрих Шерр «Бухгалтерия и баланс»	«...под вуалированием баланса следует понимать такую форму составления баланса, которая делает хозяйственные факты неясными или трудно выявляемыми, так что получается неточная или неправильная картина экономического положения соответствующего предприятия.» [5]
Я. М. Гальперин «Основы балансоведения»	«...вуалирование баланса представляет собою неправильное формальное

	построение баланса, предполагающее неясность и затемнение в отношении наименования и группировки отдельных его элементов...» [4]

То есть, в отличие от фальсификации бухгалтерской отчетности, вуалирование - это скорее несоблюдение нейтральности.

Логично, что компании могут фальсифицировать или вуалировать данные в отчетности по разным причинам, среди которых:

- Построение нужной картины о финансовом положении для потенциальных и/или действующих инвесторов
- Уменьшение налогового бремени
- Получение кредита (в том числе льготных условий кредитования).

По нашему мнению, модель выявления фальсификации для каждого из этих случаев должна строиться в индивидуальном порядке из-за различий в паттернах фальсификации для целей искажения отчетностей. К сожалению, на данный момент почти невозможно найти необходимые данные о компаниях, фальсифицирующих отчетность, хотя бы для одной из трех групп, так как, например, при проведении аудиторских проверок, данные компании не подлежат публикации по закону, а в судебной практике данные все чаще изымаются из открытых источников.

Формы бухгалтерской финансовой отчетности являются общедоступным источником информации для анализа деятельности организации, по этой причине, любые искажения, будь то фальсификация или вуалирование, могут привести к некорректной оценке инвестиционной привлекательности компании, что в свою очередь может вызвать значительные финансовые потери. По этой причине потенциальным и действующим инвесторам той или иной организации необходимы доступные методы выявления фактов искажения бухгалтерской финансовой отчетности.

Применимость используемых методов искажений. Одним из таких методов является модель, которую представил общественности Мессод Д.Бениш в 1999 году. Данный метод представляет собой аналитическую процедуру подсчета определенных финансовых показателей (Табл. 2), выявленных в результате анализа финансовых отчетности из 2406 американских компаний (2332 организации с проверенной достоверной отчетностью и 74 организации с выявленными искажениями)[7].

Мессодом Д.Бенишем были определены граничные значения используемых в модели показателей, превышение которых говорит о высокой вероятности фактов фальсификации финансовой отчетности в организации. Данные показатели представлены в таблице ниже:

Таблица 2 – Финансовые показатели в модели Д. Бениша
и их граничные значения для американских компаний

Показатель	Формула для расчета	Граничные значения для американских компаний
Индекс дневных продаж в дебиторской задолженности (<i>DSRI</i>).	$\frac{\text{Дебиторская задолженность}}{\text{Выручка ТГ}} \times \frac{\text{Выручка ПГ}}{\text{Дебиторская задолженность ПГ}}$	1,031
Индекс рентабельности продаж по валовой прибыли (<i>GMI</i>).	$\frac{\text{Валовая прибыль ПГ}}{\text{Валовая прибыль ТГ}} \times \frac{\text{Выручка ТГ}}{\text{Выручка ПГ}}$	1,014
Индекс качества активов (<i>QI</i>)	$\frac{(\text{Активы} - \text{Оборотные активы} - \text{Основные средства})}{\text{Активы ПГ}} \times \frac{(\text{Активы} - \text{Оборотные активы} - \text{Основные средства})}{\text{Активы ТГ}}$	1,039
Индекс роста выручки (<i>SGI</i>)	$\frac{\text{Выручка ТГ}}{\text{Выручка ПГ}}$	1,134
Индекс амортизации (<i>DEPI</i>)	$\frac{\text{Амортизация ПГ}}{\text{Амортизация ТГ}} \times \frac{(\text{Амортизация} + \text{Основные средства}) \text{ТГ}}{(\text{Амортизация} + \text{Основные средства}) \text{ПГ}}$	1,001
Индекс коммерческих и управленческих расходов (<i>SGAI</i>)	$\frac{\text{Коммерческие и управленческие расходы ТГ}}{\text{Коммерческие и управленческие расходы ПГ}} \times \frac{\text{Выручка ПГ}}{\text{Выручка ТГ}}$	1,054
Индекс коэффициента финансовой зависимости (<i>LVGI</i>)	$\frac{\text{Долгосрочные и краткосрочные обязательства ТГ}}{\text{Долгосрочные и краткосрочные обязательства ПГ}} \times \frac{\text{Активы ПГ}}{\text{Активы ТГ}}$	1,037
Индекс начислений на активы (<i>TATA</i>)	$\frac{\text{Чистые оборотные активы} - \text{Денежные средства}}{\text{Активы ТГ}} + \frac{\Delta \text{КЗ по налогу на прибыль} - \text{Амортизация}}{\text{Активы ТГ}} + \frac{\Delta \text{Краткосрочная часть долгосрочных обязательств}}{\text{Активы ТГ}}$	0,018

В результате регрессионного анализа зависимости между вероятностью фальсификации отчетности и представленными выше финансовыми показателями был получен индекс, называемый M-score:

$$M\text{-score} = -4.84 + 0.92 \times DSRI + 0.528 \times GMI + 0.404 \times AQI + 0.892 \times SGI + 0.115 \times DEPI - 0.172 \times SGAI + 4.679 \times TATA - 0.327 \times LVGI$$

Значение данного индекса для компаний, не прибегающим к фальсификации финансовой отчетности, не должен превышать – 2,22.

Так как данная модель была получена на основе анализа американских компаний, использование ее в реалиях российских стандартов бухгалтерского учета не представляется возможным из-за большой разницы в нормативной базе и традиционных пользователях финансовой отчетности. Решение данной проблемы в 2016 году в своей исследовательской работе предложили Н.В. Ферулева и М.А. Штефан. На основе анализа 60 (Табл.3,4) российских компаний они выявили, что модели Бениша способна выявить факт фальсификации финансовой бухгалтерской отчетности лишь в 62% процентах [2].

Таблица 3 – Сводные индексы модели Бениша для российских компаний, в которых был выявлен факт фальсификации бухгалтерской отчетности

DSRI	GMI	AQI	SGI	SGAI	LVGI	Сводный индекс Бениша
0,136	0	106,5	1527	1	1562	889,45
0,52	1,613	26 792	1,594	1,18	0,98	10 821
1,136	1,29	1,258	1,323	0,94	0,942	-1,895
10,781	0,029	1,015	0,11	10,3	1,237	3,418
3,813	0,21	0,663	0,483	3,79	2,883	-2,116
0,408	0,24	0,927	0,915	1	1,517	-3,815
1,905	2,631	0,92	0,565	1	1,287	-1,415
1,678	4,306	3,677	1,992	1,44	2,213	1,268
0,212	34,83	1	2,78	0,01	1,714	16,069
5,716	0,805	0,031	1,443	1,2	1,99	1,286
0,142	1,188	1	3,228	1,14	1	-1,321
1,917	1,304	12,48	0,763	2,34	1,131	2,56
2,241	0,743	0,444	2,218	0,1	0,928	-0,548
0,828	1,089	0	1,408	0,9	0,992	-2,726
1,68	2,015	1966	0,749	0,47	3,15	791,59

0,252	0,63	2297	2,784	1	1,025	925,69
7,257	0,192	0,368	1,045	1,45	0,979	2,448
1,29	0,926	1	1,345	1	1,217	-2,13
1,147	0,919	1,932	1,125	0,96	0,994	-2,006
1	194	1	49,78	1	1,004	142,82
0,856	0,979	1,292	1,033	0,99	0,978	-2,581
0,235	0,912	1	2,395	38	1,922	-8,766
0,923	1,167	1	1,643	1,21	1,1	-2,072
0,254	1,451	30 010	1,142	0,28	1,055	12 121
0,108	2,075	1	1,468	1	1,018	-2,436
5,209	0,466	1	0,757	2,13	1,002	0,583
0,091	1,09	1	14,88	1	1,451	8,849
3,699	1,141	1	1,038	0,85	0,75	0,104

Таблица 4 – Сводные индексы модели Бениша для российских компаний, в которых не был выявлен факт фальсификации бухгалтерской отчетности

DSRI	GMI	AQI	SGI	SGAI	LVGI	Сводный индекс Бениша
0,769	0,964	1,409	1,325	1,18	1,984	-2,723
1,514	1,44	0,859	0,857	1	0,631	-1,953
0,172	0,918	0,831	1,396	0,95	2,73	-3,672
0,51	1,759	0,987	1,003	0,63	0,715	-2,49
0,676	0,99	1,843	1,87	1	0,592	-1,648
0,301	1,098	1,89	1,423	0,68	1,084	-2,421
0,799	2,291	1,15	0,828	1	1,06	-2,21
7,813	7,99	0,091	1,614	1	1,005	7,542
0,853	-1,05	0,985	1,18	2,64	1,127	-3,982
3,392	1,47	1	0,94	1	1,078	-0,228
1,536	0,92	0,114	1,11	0,94	1,036	-2,405
1,003	0,19	1	0,354	1	0,8	-3,53
0,668	0,573	0,188	2,054	1	1,253	-2,596
0,945	-0,23	0,708	1,323	1	0,928	-3,099
1,625	0,362	1,078	0,721	1	0,983	-2,568

0,925	1,032	0,883	1,296	1,11	1,167	-2,503
1	1	2,152	1	1	0,999	-2,129
2,354	0,784	1	0,439	1,56	1,004	-2,06
0,84	2,052	0,662	2,15	0,66	1,218	-1,31
1,656	1,052	1	0,983	1,03	1,619	-2,186
1,215	1,015	1	1,148	1,12	0,97	-2,267
1,097	1,016	0,82	0,977	1,01	0,89	-2,556
1,641	0,792	0,885	0,978	1,26	1,97	-2,543
1,937	0,544	0,97	0,496	1,53	0,921	-2,501
0,882	2,627	1	1,214	1,1	1,411	-1,804
1,877	1,015	0,798	1,127	0,86	0,932	-1,702
0,843	0,666	0,698	2,191	0,63	0,887	-1,874
0,24	1,93	1	4,239	0,61	0,863	0,198
0,99	0,805	0,766	1,091	1,31	0,797	-2,706
0,828	1,31	6,78	1,857	0,68	0,806	0,627
3,05	2,187	0,998	0,395	0,3	1,07	-0,524
1,1	0,96	2,415	1,37	1,05	1,276	-1,72

Для адаптации модели было решено исключить из расчета два фактора: индекс амортизации (*DEPI*) и показатель, характеризующий начисления к активам (*TATA*). По мнению авторов работы, подобное допущение не скажется на качестве результатов анализа [2]. В ходе дальнейшего анализа было получены новые граничные значения финансовых показателей российских компаний, входящих в модель Бениша (Табл.5):

Таблица 5 – Средние значения показателей российских компаний, входящих в модели Бениша

Показатели	DSRI	GMI	AQI	SGI	SGAI	LVGI
Компании, в которых был выявлен факт фальсификации	1,980	9,223	2185,947	58,107	2,774	57,088
Компании, в которых не был выявлен факт фальсификации	1,408	1,265	1,186	1,280	1,026	1,119

На основе данных, представленных в таблице, было пересчитано пороговое значение сводного индекса M-score для российских компаний,

который составил -1,802. После модификации модели, вероятность выявления факта фальсификации в российских компаниях выросла с 62% до 68%. Как отмечают сами авторы данного исследования, несмотря на то, что качество прогноза повысилось, данная модель требует дальнейших доработок и исследований [2].

В своей работе Мессод Д. Бениш отмечает, что одним из ограничений модели является то, что она оценивается с использованием финансовой информации для публичных торгуемых компаний. Следовательно, данный метод нельзя надежно использовать для изучения частных фирм. В работе Н.В. Фирулевой и М.А. Штефан 45% компаний на момент разработки модели для российских компаний имеют правовую форму ЗАО и ООО [2], что говорит о сильном снижении эффективности модифицированной модели.

В статье Н.В. Фирулевой и М.А. Штефан линейная модель выявления фактов фальсификации отчетности Бениша была адаптирована под российские реалии путем исключения из нее индексов, которые, по мнению авторов не являются значимыми, а также пересчетом границы критической области (*M-score*). При этом индексы при коэффициентах остались неизменными, а значит и их вклад в классификацию российских компаний постулируется аналогичным вкладу соответствующих индексов в оригинальной модели Бениша. Это сильное утверждение, которое требует проверки. Кроме того, граничное значение *M-score* было пересчитано на основании среднего значения индексов Бениша лишь для компаний, не фальсифицирующих отчетность, а значит с использованием лишь половины имеющейся информации.

Оценка качества модифицированной модели. Несмотря на то, что предоставленная в статье выборка является практически сбалансированной, для оценки качества предложенной модификации модели рассчитаем по предоставленной выборке основные *performance metrics*: *F1-score*, *precision* и *recall*. Так же для сверки с предоставленными в статье данными будем рассчитывать *accuracy*.

Прежде всего, для описания представленных метрик, введем основное понятие, используемое для оценки эффективности модели в методах машинного обучения – матрица ошибок [6]. В данном случае у нас существует две группы объектов и модель, которая предсказывает принадлежность объекта к одной из групп. Матрица ошибок для двух групп будет выглядеть следующим образом (Табл.6):

Таблица 6 – Матрица ошибок

	$y=1$	$y=0$
$\hat{y} = 1$	True Positive (TP)	False Positive (FP)

$\hat{y} = 0$	<i>False Negative</i> (FN)	<i>True Negative</i> (TN)

В данной таблице $\hat{y}$ – результат работы модели на объекте, а y – истинное значение показателя на объекте. Таким образом, ошибки могут быть двух типов: *False Negative (FN)* и *False Positive (FP)*.

В нашем случае FP – это определение компании с проверенной достоверной отчетностью как компанию, которая свою отчетность фальсифицирует. А FN, следовательно, определение компании, фальсифицирующей отчетность, как компанию с достоверной проверенной отчетностью.

То есть, матрица ошибок для модели Н.В. Ферулевой и М.А. Штефан будет выглядеть следующим образом(Табл.7):

Таблица 7 –Матрица ошибок для модели Н.В. Ферулевой и М.А. Штефан

	$y=1$	$y=0$
$\hat{y} = 1$	18	9
$\hat{y} = 0$	10	23

Самое простой, но почти неиспользуемой метрикой является доля правильных ответов модели – *accuracy*:

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} = \frac{18 + 23}{18 + 23 + 9 + 10} = 0,68(3)$$

Нам необходимо понимать качество работы модели для каждой из двух групп по отдельности. Для этого введем такие метрики, как точность (*precision*) и полнота (*recall*).

$$precision = \frac{TP}{TP + FP} = \frac{18}{18 + 9} = 0,66(6)$$

$$recall = \frac{TP}{TP + FN} = \frac{18}{18 + 10} = 0,64$$

Precision и *recall* не зависят, в отличие от *accuracy*, от соотношения классов и потому применимы в условиях несбалансированных выборок. Для объединения *precision* и *recall* существует агрегированный критерий качества – среднее гармоническое *precision* и *recall*, так называемая F-мера:

$$F_1 = 2 \times \frac{precision \times recall}{precision + recall} = 0,65$$

Для проверки допустимости адаптации модели к данным приведенным в оригинальной статье способом рассчитаем 95-процентный доверительный интервал для *F1-score* такого классификатора используя *bootstrap* [8]. Получим интервал [0.49, 0.79], содержащий значение 0.5. Это

свидетельствует о том, что модель классификации статистически значимо не отличается от случайного угадывания.

Попробуем применить к нашим данным логистическую [10] модель с помощью соответствующей функции в *Python*. Получим следующие метрики:

Таблица 8 – Метрики

<i>Accuracy</i>	0,783
<i>Precision</i>	0,941
<i>Recall</i>	0,571
<i>F1</i>	0,711

Снова рассчитаем 95-процентный доверительный интервал для *F1-score* и получим интервал [0.54, 0.87]. Полученный результат лучше, чем у линейной модели. Этого следовало ожидать, так как логистический классификатор призван решать именно такую задачу, так как в отличие от обычной регрессии, в данном методе не производится предсказание числовой переменной исходя из выборки исходных значений. Вместо этого, значением функции является вероятность того, что данное исходное значение принадлежит к определенной группе.

Исследование взаимных корреляций регрессоров в исходной модели. Далее проведем исследование взаимных корреляций регрессоров в исходной модели Н.В. Ферулевой и М.А. Штефан (Рис.1). Тут уже очевидно, что линейной моделью такие данные описывать не стоит, так как *LVGI* и *SGI* имеют коэффициент корреляции Пирсона практически равный единице, при этом все коэффициенты корреляции Спирмана не вызывают беспокойства.

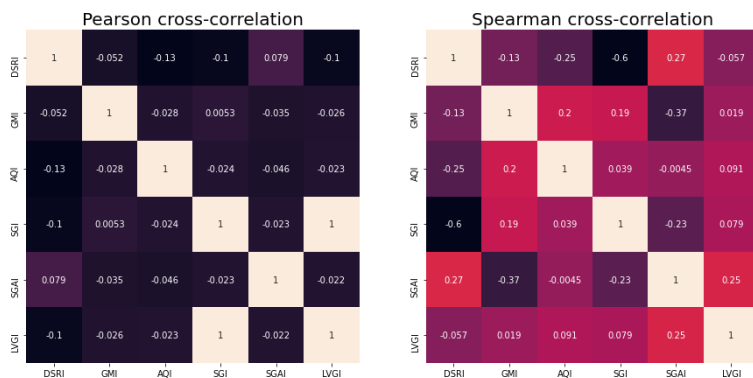


Рисунок 1– Коэффициенты корреляции Спирмана и Пирсона

Посмотрим на распределения значений индексов модели Бениша, для этого построим боксплоты для нормированных значений индексов. Дальнейший анализ используемых в оригинальной статье данных для пяти из шести индексов Бениша продемонстрировал наличие чрезвычайно больших выбросов. (Рис.2)

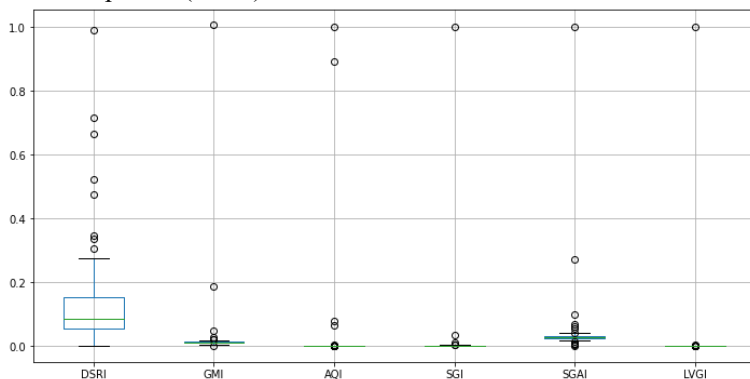


Рисунок 2 – График распределения значений индексов

Очевидно, что в данных имеются чрезвычайно выделяющиеся аутлаеры, по сравнению с ними боксплоты почти неразличимы.

Приравняем значения всех точек, превышающих 0.9 квантиль к значению этого квантиля и посмотрим на результат (Рис.3):

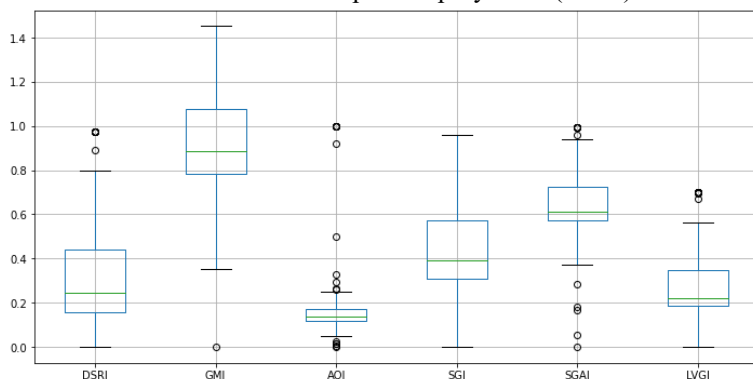


Рисунок 3 – График распределения индексов после отсечки

Проверим гипотезу о том, что классификация данных возможна лишь по наличию в измерении таких выбросов. Построим классификатор, по следующему принципу:

- вычислим квантили (известного уровня) для каждого из индексов Бениша;
- классифицируем фальсификаторами те компании, для которых хотя бы один из индексов превышает соответствующий квантиль;
- квантиль будем выбирать из соображения наиболее эффективного (по $F1$ -score) разделения выборки. (Рис.4)

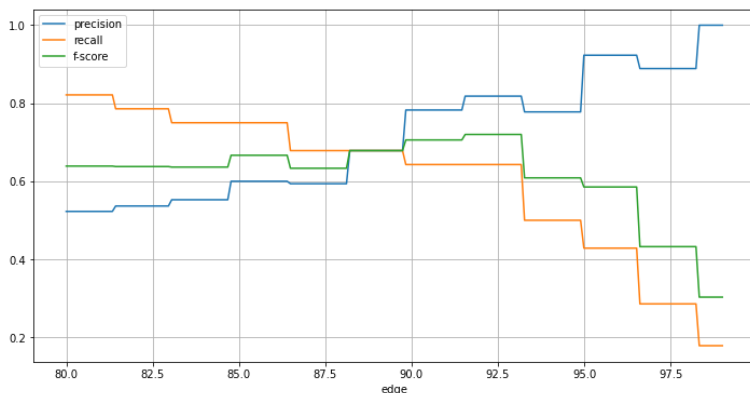


Рисунок 4 – График распределения метрик в зависимости от квантиля

Выводы. Данный подход содержит меньше параметров по сравнению с оригинальной моделью, при этом демонстрирует превосходство по всем используемым метрикам. Доверительный интервал для $F1$ -score равен $[0.58, 0.84]$, это позволяет отвергнуть гипотезу о случайности классификации.

Таблица 9 – Метрики для классификатора по квантильной отсечке

<i>accuracy</i>	0,767
<i>precision</i>	0,818
<i>recall</i>	0,643
<i>F1</i>	0,720

Наш классификатор по "квантильной отсечке" продемонстрировал лучшее значение $F1$ – score статистически значимо отличающееся от 0.5. При этом данная модель проще линейной, а значит её и следовало бы использовать для подобных данных.

Несмотря на полученный результат, раскрытие данной темы в дальнейшем остается актуальным, так как полученная модель работает для конкретной выборки компаний, уличенных в фальсификации бухгалтерской отчетности для получения кредитования, что является достаточно узким направлением для комплексного анализа и модификации модели Мессода Д. Бениша.

Список использованных источников:

1. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 01.07.2021) [Электронный ресурс] // СПС КонсультантПлюс: Студент – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 05.11.2021);
2. Фирулева Н.В., Штефан М.А. Выявление фактов фальсификации в финансовой отчетности в российских компаниях: Анализ применимости моделей Бениша и Роксас // Russian Management Journal. – 2016. – Том 14, №3. – С.49 – 70.
3. Бычкова С.М., Итыгилова Е.Ю., Искажения бухгалтерской финансовой отчетности в аудите // Москва: АУДИТОР, 2014. – 213 с.
4. Гальперин Я.М., Основы балансоведения. Общие положения теории учета. Тифлис: Практический институт счетоведения, 1925.
5. Шерр И.Ф., Бухгалтерия и баланс. М.: Экономика и жизнь, 1926.
6. Powers, D.M.W., Evaluation: From precision, recall and F-measure to ROC, informedness, markedness & correlation // Journal of Machine Learning Technologies – 2011. – ISSN: 2229-3981 & ISSN: 2229-399X, Volume 2, Issue, pp-37-63
7. Beneish M. // The detection of earning manipulation. Financial Analysts Journal – 1999. – 55 (5): 24–36.
8. B. Efron, Bootstrap Methods: Another Look at the Jackknife // Ann. Statist.– 1979. – 7 (1) 1 – 26
9. «Статистика по клиентам участникам торгов фондового рынка за 2012 – 2021 год» [Электронный ресурс] // Московская биржа – URL: <https://www.moex.com/s719/> (дата обращения 05.11.2021);
10. "Rouhani-Kalleh, O. Analysis, Theory and Design of Logistic Regression Classifiers Used For Very Large Scale Data Mining. Master Thesis. 2006.

Анализ современных подходов разработки криптовалют для их использования в реализации национальной цифровой валюты

Ю. Волянский

студент 1 курса НИЯУ МИФИ, Москва

E-mail: julyk.volyansky13@yandex.ru

Ю.В.Терехова

старший преподаватель кафедры финансового мониторинга

НИЯУ МИФИ, г. Москва

E-mail: YVTerekhova@mephi.ru

Аннотация: В статье рассмотрены механизмы и принципы работы современных криптовалют, которые можно применить для создания национальных цифровых валют. Выявлено, что одним из слабых мест криптовалют часто является скорость проведения транзакций. Рассмотрен блокчейн Solana как пример ориентира для создания национальных цифровых валют.

Ключевые слова: блокчейн Solana, криптовалюта, леджер, смарт-контракт.

Analysis of modern approaches to the development of cryptocurrencies for their use in the implementation of the national digital currency

Abstract: The article discusses the mechanisms, principles of operation and capabilities of modern cryptocurrencies that can be used to create national digital currencies. It has been revealed that one of the weaknesses of the cryptocurrency is the speed of transactions. The Solana blockchain is considered as a reference point for the creation of national digital currencies.

Keywords: Solana blockchain, cryptocurrency, ledger, smart contracts.

Введение

В связи с широким применением цифровизации в современном обществе, становится актуальным вопрос о надежном хранении, доступе и обмене данными. Для решения этой проблемы может применяться технология блокчейн, которая все больше затрагивает различные сферы деятельности человека. На ее основе во многих государствах разрабатываются собственные проекты национальных цифровых валют.

Блокчейн – это реестр децентрализованных данных, которыми можно безопасно обмениваться. Распределенный журнал дублируется и распространяется по всей сети компьютерных систем на блокчейне. Каждый блок в цепочке содержит несколько транзакций, и каждый раз, когда в блокчейне происходит новая транзакция, запись о ней добавляется в леджер каждого участника. Децентрализованная база данных, управляемая несколькими участниками, известна как «технология распределенного реестра» или DLT.

На данный момент блокчейн уже применяется в следующих предметных областях:

- электронное голосование;
- авторство и право собственности;
- медицина;
- поставки товаров;
- денежные операции.

Благодаря возможностям обеспечения целостности и непротиворечивости данных, исполнения децентрализованных смарт-контрактов и быстрой синхронизации данных в большинстве государств идут процессы по разработке и внедрению цифровых аналогов собственных валют. В Российской Федерации проводится разработка криптовалюты [1].

Основной материал

Современные криптовалюты и их правовой статус.

В настоящее время на крупных, средних и специализированных биржах зарегистрировано более 1600 криптовалют [2]. Из них можно выделить 11 наиболее популярных [3]:

- Bitcoin (BTC);
- Ethereum (ETH);
- Litecoin (LTC);
- Cardano (ADA);
- Polkadot (DOT);
- Bitcoin Cash (BCH);
- Stellar (XLM);
- Dogecoin (DOGE);
- Binance Coin (BNB);
- Tether (USDT);
- Monero (XMR).

По мере того, как трансформация криптовалюты из спекулятивных инвестиций в стабильный сбалансированный портфель продолжает набирать обороты, правительства во всем мире по-прежнему расходятся во

мнениях о том, как регулировать формирующийся класс активов. Правила регулирования сильно различаются по всему миру, некоторые правительства принимают криптовалюты, а другие – запрещают их. Задача регулирующих органов в современных реалиях этапе состоит в том, чтобы разработать правила, ограничивающие традиционные финансовые риски, не препятствуя инновациям.

В данный момент криптовалюта на законодательном уровне может рассматриваться в виде товара, инвестиционного актива или отдельной денежной единицы. Ниже приведен не полный список стран, которые легализовали или частично признали криптовалюту [4]:

- Нигерия;
- Танзания;
- Маврикий;
- Канада;
- США;
- Мексика;
- Российская Федерация (Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 г. № 259-ФЗ);
- Никарагуа;
- Республика Беларусь (Декрет № 8 «О развитии цифровой экономики»);
- Новая Зеландия;
- Сальвадор.

Так же вслед за легализацией криптовалюты, национальные банки предпринимают попытки создать свои аналоги, которые будут использоваться внутри страны на равных условиях с действующими валютами. На государственном уровне создаются и развиваются блокчейн решения для обмена смарт-контрактами, создания автономных компаний, для хранения документов, подтверждающих право собственности, т. е. практически для всего, от владения цифровыми книгами до автомобилей, недвижимости и многого другого. Все эти проекты используют ресурсы Национальной программы мер поддержки технологий распределенных реестров. [9]

Ниже представлены страны, которые занимаются разработкой или тестированием национальной цифровой валюты, а также их названия (таблица 1) [5].

Таблица 1 – Национальные криптовалюты разных стран

Название страны	Название цифровой валюты	Предполагаемый запуск
Дубай (ОАЭ)	Emcash	2017 год
Венесуэла	Petro	2018 год
Эстония	Estcoin	Отклонена
Российская федерация	Cryptoruble	2022 год
Швеция	E-Krona	Не определен
Япония	J-Coin	2020 год
Китай	DCEP	2022 год

Характеристики криптовалют.

Криптовалюты можно сравнивать по ряду показателей. Ключевыми свойствами, которые следует учитывать, являются:

1. Смарт-контракты, представляющие собой небольшие компьютерные программы, работающие на блокчейне, позволяющие использовать дополнительные функции, которая реализована не во всех криптовалютах. Смарт-контракты работают как строки заранее запрограммированных условных событий, например, перевод X денег сегодня, но только после того, как получатель подтвердил личность. Смарт-контракты позволяют не только осуществлять платежи, но и переводить все, что можно перевести в цифровую форму: цифровое искусство (NFT), цифровые ценные бумаги, кредиты и т.д. Они также являются основой децентрализованного финансирования (DeFi) и первого размещения монет (ICO);

2. Алгоритм консенсуса, применяющийся для управления децентрализованной сетью без традиционного посредника, для проверки всех транзакций в сети. В алгоритме консенсуса указано как проверяются транзакции в сети. Наиболее известным является доказательство работоспособности (PoW), используемое, например, Биткойном, где майнеры управляют сетью, применяя криптографические алгоритмы на энергопотребляющих компьютерах и центрах обработки данных. Другим важным алгоритмом консенсуса является доказательство ставки (PoS), где сетью управляют не агенты с большой вычислительной мощностью, а владельцы базовой криптовалюты;

3. Скорость и масштабируемость. Для использования криптографии в качестве средства для проведения транзакций на глобальной и ежедневной основе требуется как высокая скорость транзакций, так и способность обрабатывать множество транзакций в секунду. Эти цифры приведены в таблице 2 для различных криптосистем. По сравнению с возможностью Visa обрабатывать около 1700 транзакций в секунду увеличивать скорость обработки, старые криптосистемы испытывают трудности с достижением подобного результата. Однако разработчики первых криптовалют работают над решениями повышения пропускной способности блокчейна;

4. Сохранение ценности и инфляция. Несмотря на высокую волатильность в криптопространстве, многие инвесторы рассматривают

криптовалюты, такие как Bitcoin, Cordana и Litecoin, имеют ограниченный первичный объем монет, другие криптовалюты, такие как Ethereum и Stellar, не имеют верхнего предела для выпущенного количества криптокоинен и, следовательно, являются инфляционными по своей природе. Недавно выпущенные криптокоины обычно поступают в качестве вознаграждения валидаторам вызывая инфляцию. Некоторые криптосистемы, однако, стремятся ограничить инфляцию, сжигая (уничтожая) часть комиссионных за транзакции, сохраняя инфляцию на минимальном уровне для запуска сети.

В отношении национальных цифровых валют, а в частности – крипторубля, выдвигаются следующие критерии [1]:

- простота использования;
- высокая скорость;
- надежность;
- повсеместность приема;
- безопасность хранения средств на электронном кошельке;
- удобство и легкость конверсии;
- конфиденциальность информации о потребителе;
- бесшовная интеграция с цифровыми платформами;
- поддержка смарт-контрактов;
- возможность использования в офлайн-режиме.

Исходя из вышеперечисленных свойств, можно сделать вывод, что одним из возможных слабых мест крипторубля может являться скорость работы – показывает, как быстро транзакция может быть подтверждена сетью, и обычно измеряется в транзакциях в секунду. Скорость транзакции криптовалюты важна по двум причинам:

1. Сообщает, как быстро транзакция будет записана сетью и станет необратимой. Чем дольше транзакция должна ждать подтверждения, тем выше вероятность того, что кто-то сможет потратить эту валюту снова, прежде чем она будет подтверждена в альтернативной блокчейн-развилке;

2. Влияет на то, как быстро возможно потратить валюту. Например, если цифровой кошелек должен дожидаться подтверждения, прежде чем тратить какие-либо средства с этого адреса, то время ожидания повлияет на удобство его использования.

В таблице 2 приведена скорость транзакций в различных блокчейнах [6], а также у платежных систем Visa и MasterCard [7].

Таблица 2 – Примеры скорости работы блокчейнов, Visa и MasterCard

Система	Транзакции в секунду	Среднее время подтверждения транзакции

Bitcoin	3–7	60 min
Ethereum	15–25	6 min
Ripple	1500	4 s
Bitcoin Cash	61	60 min
Stellar	1000	2–5 s
Litecoin	56	30 min
Monero	4	30 min
Dash	10-28	15 min
DCEP	220,000 (пиковые)	–
Visa	1700	–
MasterCard	5000	–

Как видно из таблицы 2, не все современные блокчейны имеют высокую скорость транзакций в отличие от платежных систем. В случае использования подобных криптовалют на национальном уровне могут возникать задержки в переводе сумм и оформлении смарт-контрактов, что является недопустимым для национальных цифровых валют.

Ethereum является второй по величине криптовалютой в мире и первой, применившей смарт-контракты. Однако, проблема в том, что сеть Ethereum сильно перегружена, и транзакции стали дорогими. В результате основное внимание уделяется более новым платформам, которые являются как более быстрыми, так и менее дорогостоящими. Существует несколько, так называемых «убийц Ethereum», борющихся за лидирующие позиции, каждый из которых пытается привлечь разработчиков и претендовать на долю рынка.

Разработчики блокчейна Solana представили вариант решения проблемы со скоростью проведения транзакций.

Solana – это блокчейн, обеспечивающий быстрые, безопасные, масштабируемые, децентрализованные приложения и торговые площадки. В настоящее время система поддерживает 50 тыс. TPS (транзакций в секунду) и время блокировки 400 мс [8].

Главная цель программного обеспечения Solana – продемонстрировать, что существует возможный набор программных алгоритмов для создания блокчейна, который позволит увеличить пропускную способность транзакций пропорционально пропускной способности сети и удовлетворяющей всем свойствам. Кроме того, система теоретически имеет верхнюю границу 710 тыс. TPS в стандартной гигабитной сети и 28,4 млн. TPS в 40-гигабитной сети.

Так же в блокчейн системах применяются различные алгоритмы валидации. Например, Bitcoin использует Proof-of-Work, для Ethereum применяется модель Proof-of-Stake. Для Solana был разработан алгоритм Proof-of-History.

Proof-of-History (PoH) – это последовательность вычислений, которая может обеспечить способ криптографической проверки прохождения времени между двумя событиями. Он использует криптографически защищенную функцию, написанную так, что вывод не может быть предсказан по входным данным, и должен быть полностью выполнен для генерации выходных данных.

Так же блокчейн Solana поддерживает все основные критерии современных блокчейнов. Благодаря алгоритму PoH реализуется защита проводимых операций и обеспечивается защита от атак на старые блоки. Для проведения подобной атаки и восстановления леджера из любого момента в прошлом потребовалось бы, чтобы злоумышленник вовремя опередил действительный реестр, опередив скорость генератора PoH, что является сильно затратным по ресурсам.

В блокчейне Solana были реализованы более гибкие смарт-контракты. Подход Solana к выполнению смарт-контрактов основан на том, как операционные системы загружают и выполняют динамический код. Клиент может создать программу на любом языке программирования, скомпилировать ее для дальнейшего использования в LLVM и отправить в блокчейн Solana. Во многих блокчейн-сетях один смарт-контракт за один раз влияет на состояние блокчейна и изменяет его. Однако в Solana среда выполнения может обрабатывать десятки тысяч контрактов параллельно. Это позволяет одновременно выполнять транзакции, которые не перекрываются и, которые считывают только одно и то же состояние.

Исходя из перечисленных достоинств блокчейна Solana, он представляет собой современное решение, которое может использоваться в качестве ориентира для создания национальных цифровых валют.

Заключение

В статье проведен краткий анализ правовой ситуации рынка криптовалют в различных странах, проанализированы современные подходы разработки криптовалют, выявлена их слабая сторона – скорость проведения транзакций. В качестве современного примера блокчейна рассмотрен блокчейн Solana, представлены его преимущества и основные возможности. Показано, что данный блокчейн можно использовать, как пример для разработки национальной цифровой валюты.

Список использованных источников:

1. Центральный банк Российской Федерации. ЦИФРОВОЙ РУБЛЬ // Цифровой рубль. Банк России. [2020]. URL: https://cbr.ru/analytics/d_ok/dig_ruble/ (дата обращения: 15.11.2021).
2. What Are the Most Traded Cryptocurrencies? [Электронный ресурс] // Plus500: [сайт]. [2020]. URL: <https://www.plus500.com/en->

- AU/Trading/CryptoCurrencies/What-are-the-Most-Traded-Cryptocurrencies~2 (дата обращения: 15.11.2021).
3. The 10 Most Important Cryptocurrencies Other Than Bitcoin [Электронный ресурс] // Investopedia: [сайт]. [2021]. URL: <https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/#citation-1> (дата обращения: 16.11.2021).
 4. Правовой режим криптовалют [Электронный ресурс] // Wikipedia: [сайт]. [2021]. URL: https://ru.wikipedia.org/wiki/Правовой_режим_криптовалют (дата обращения: 16.11.2021).
 5. List of Countries That Have Plans To Roll Out Their Own Cryptocurrencies [Электронный ресурс] // CoinSutra: [сайт]. [2020]. URL: <https://coinsutra.com/national-cryptocurrencies/> (дата обращения: 17.11.2021).
 6. Cryptocurrency Transaction Speeds in 2021 [Электронный ресурс] // Tezro: [сайт]. [2021]. URL: <https://blog.tezro.com/cryptocurrency-transaction-speeds/> (дата обращения: 17.11.2021).
 7. The Lightning Network is Poised to Disrupt Utility Payments [Электронный ресурс] // Utilli: [сайт]. [2021]. URL: <https://utilli.com/2021/04/26/the-lightning-network-is-poised-to-disrupt-utility-payments/> (дата обращения: 17.11.2021).
 8. Introduction [Электронный ресурс] // Solana Docs: [сайт]. [2020]. URL: <https://docs.solana.com> (дата обращения: 18.11.2021).
 9. «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [Электронный ресурс] // URL: <https://digital.ac.gov.ru/about/> (дата обращения 18.11.2021)

Анализ экономических характеристик организаций электронной промышленности

А.А. Санжаров
старший преподаватель кафедры бухгалтерского учета и аудита
НИЯУ МИФИ, Москва
E-mail: AASanjarov@mephi.ru

Аннотация: В статье рассмотрены некоторые экономические характеристики организаций, относящихся к электронной промышленности, в связи с реализацией положений Стратегии развития отрасли.

Ключевые слова: электронная промышленность, отраслевой анализ, электроника, стратегия развития.

Analysis of the economic characteristics of electronic industry organizations

Abstract: The article discusses some of the economic characteristics of organizations related to the electronics industry, in connection with the implementation of the provisions of the Industry Development Strategy.

Keywords: electronics industry, industry analysis, electronics, development strategy.

Наметившиеся в последние годы тенденции развития различных отраслей экономики не обошли вниманием и электронную промышленность. Это связано, прежде всего, с резким подъемом оборонно-промышленного комплекса, для чего необходимо соответствующее развитие электроники. Но необходимо отметить также и потребность в создании и продвижении электронной продукции гражданского назначения, поскольку механизм внешних санкций подталкивает развивать внутреннее промышленное производство для рядовых потребителей.

Не вдаваясь глубоко в специфику электронной промышленности, отметим лишь, что эта сфера задействует весьма широкий круг экономических и иных процессов, таких как научные исследования и разработки, их коммерциализация, определение технологической карты производства, логистика и т.д. Также, необходимо принять во внимание

необычайно высокий уровень конкуренции в данной отрасли, что требует от отечественных производителей не просто воспроизводить то, что уже имеется на зарубежных рынках, а работать «на перспективу», вкладывая значительные средства в научные разработки.

Государство в развитии электронной промышленности, на наш взгляд, может играть двоякую роль. С одной стороны, путем административных барьеров «заставить» приобретать отечественную электронную продукцию (которая, прямо скажем, проигрывает во многих аспектах зарубежным аналогам) и взять на себя функцию главного производителя (например, путем создания государственной корпорации). С другой стороны, путем различных экономических механизмов (налоговые льготы, преференции в сфере государственных закупок, импортные пошлины) стимулировать привлечение в отрасль частного капитала, что позволит не только сэкономить государственные деньги, но и обеспечить дополнительные налоговые поступления. Разумным, по нашему мнению, является сбалансированное сочетание административных рычагов и экономического стимулирования.

С целью определения приоритетных направлений развития отечественной электроники была разработана и утверждена «Стратегия развития электронной промышленности Российской Федерации на период до 2030 года» (далее по тексту - Стратегия), которая позволит «создать новый конкурентоспособный облик электронной промышленности Российской Федерации на основе развития научно-технического и кадрового потенциала, оптимизации производственных мощностей ...» [1]. Приведенное в Стратегии количество организаций отрасли (1600 - 1700) относится к предприятиям с государственным участием, а также к предприятиям оборонно-промышленного комплекса. Количество организаций с частным капиталом определено как 1 200 [1]. Представляется необходимым уточнить реальный список компаний отрасли.

В данной статье предпринята попытка составить как можно более полный реестр организаций электронной промышленности (сведения приводятся по состоянию на 01.11.2021) исходя из тех видов деятельности (ОКВЭД2), которые характерны для рассматриваемой отрасли [2]. Далее, будут проанализированы некоторые экономические характеристики выбранных организаций (такие как форма собственности, возраст, размер, объем чистой прибыли и т.д.) с целью дать представление о текущем состоянии отрасли. Для выполнения этих задач использовалась информационная система СПАРК и данные за 2017-2020 годы [3].

Для видов деятельности (ОКВЭД2) отрасли было выбрано 13 226 организаций различных форм собственности и организационно-правовых

форм. Необходимо отметить широкую географию представленной выборки (рисунок 1).

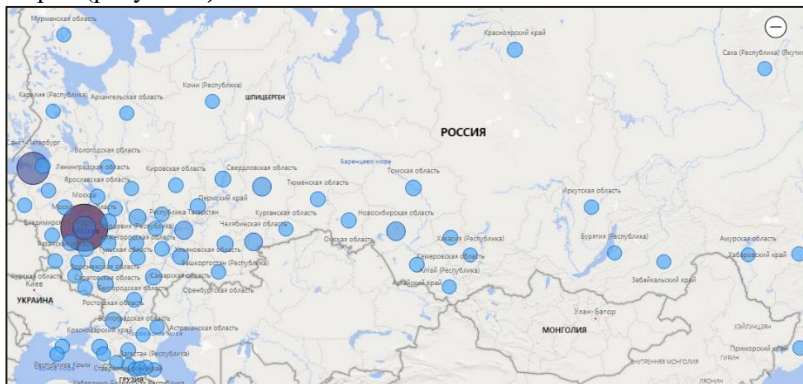


Рисунок 1 – География компаний, выбранных для проведения анализа

Как видно, большинство компаний зарегистрированы в Москве, Санкт-Петербурге и Московской области. Детально распределение по регионам видно на рисунке 2 (представлены наиболее крупные по количеству компаний регионы):

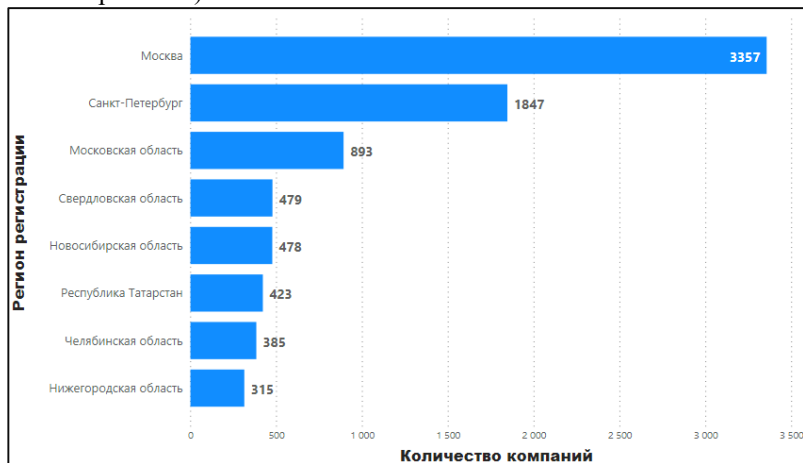


Рисунок 2 – Распределение компаний по регионам (приведены наиболее значимые)

Далее, рассмотрим распределение компаний по размеру: малые, средние, крупные (таблица 1). Необходимо отметить тот факт, что по 2 240 компаний (17% от общего количества) в информационных ресурсах нет

данных для оценки размера. Это обусловлено, в частности, отсутствием отчетной информации, по которой определяется размер организации в соответствии с 209-ФЗ «О развитии малого и среднего предпринимательства в Российской Федерации».

Таблица 1 – Распределение компаний по размеру

<i>Размер компании</i>	<i>Количество компаний</i>	<i>% от общего количества компаний</i>
Крупные предприятия	165	1,25%
Средние предприятия	294	2,22%
Малые предприятия	1 574	11,9%
Микропредприятия	8 953	67,69%
Нет данных	2 240	16,94%
Всего	13 226	100%

Из таблицы видно, что большинство представленных компаний относятся к малому бизнесу (79,6% от общего количества), в котором отдельно выделяются микропредприятия (67,7% от общего количества). Количество крупных компаний (1,25% от общего количества) значительным не может быть в принципе, их распределение по регионам представлено на рисунке 3.

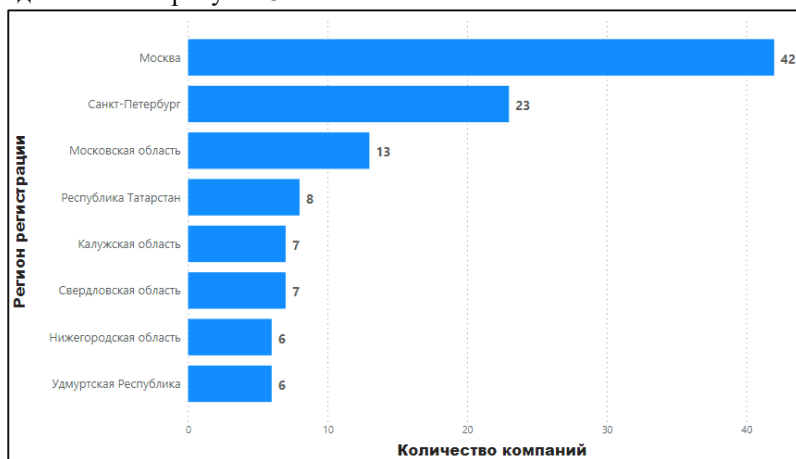


Рисунок 3 – Распределение крупных компаний по регионам (приведены наиболее значимые)

Рассматривая структуру компаний в разрезе организационно-правовых форм, необходимо отметить, что 11 793 компании (89,17% от общего количества) – это общества с ограниченной ответственностью, 1 188 (8,98% от общего количества) – публичные акционерные общества и 201

(1,52% от общего количества) – непубличные акционерные общества. На прочие организационно-правовые формы (такие как автономные организации, унитарные предприятия и др.) приходится всего лишь 0,33% от общества количества компаний.

В ходе анализа распределения компаний по формам собственности было получено, что подавляющее большинство (12 264) относится к российской частной собственности (92,73% от общего количества). Интересным представляется тот факт, что доля компаний с иностранным участием (здесь объединены собственности: совместная частная и иностранная собственность, собственность иностранных физических и юридических лиц, смешанная иностранная собственность) составляет лишь 4,17% от общего количества (552 компании). Далее будет показано, что, несмотря на это, на иностранные компании приходится значительная доля выручки и выплаченных дивидендов. Также, необходимо отметить, что применительно к крупным компаниям соотношение российской частной собственности и компаний с иностранным участием выглядит совершенно по-другому: 66% и 20% соответственно (таблица 2). Это говорит о том, что среди компаний с иностранным участием преобладает как раз крупный бизнес.

Таблица 2. Распределение крупных компаний по формам собственности

<i>Форма собственности</i>	<i>Доля крупных предприятий</i>
Частная собственность	66,06%
Собственность иностранных юридических лиц	13,33%
Иная смешанная российская собственность	7,27%
Совместная частная и иностранная собственность	6,67%
Смешанная российская собственность с долей федеральной собственности	3,03%
Смешанная российская собственность с долей собственности субъектов РФ	1,82%
Собственность государственных корпораций	1,21%
Федеральная собственность	0,61%
Всего	100%

Рассматривая структуру компаний в разрезе основных видов деятельности (ОКВЭД2 из бухгалтерского баланса), отметим, что преобладает код 26 «Производство компьютеров, электронных и оптических изделий». Более детально распределение можно увидеть на рисунке 4.

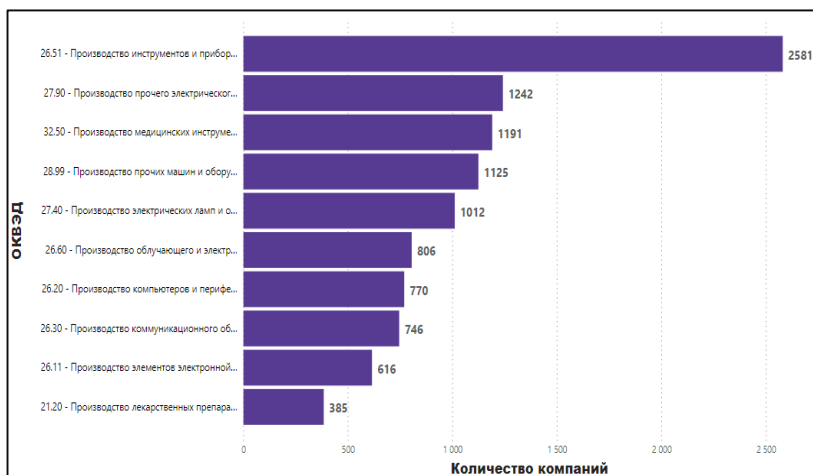


Рисунок 4 – Распределение компаний по ОКВЭД2 (первые 10 видов деятельности)

Отметим сразу недостаток представленных на рисунке 4 данных. В используемом информационном ресурсе имеется только основной код по ОКВЭД2 из финансовой отчетности, в то время как у компаний может быть достаточно много других «основных» видов деятельности. К сожалению, информация об этом на момент написания статьи не была доступна.

Далее, перейдем к характеристике компаний в разрезе их возраста. Как видно из рис.5, преобладают, в основном, молодые компании с возрастом в диапазоне 3-8 лет.

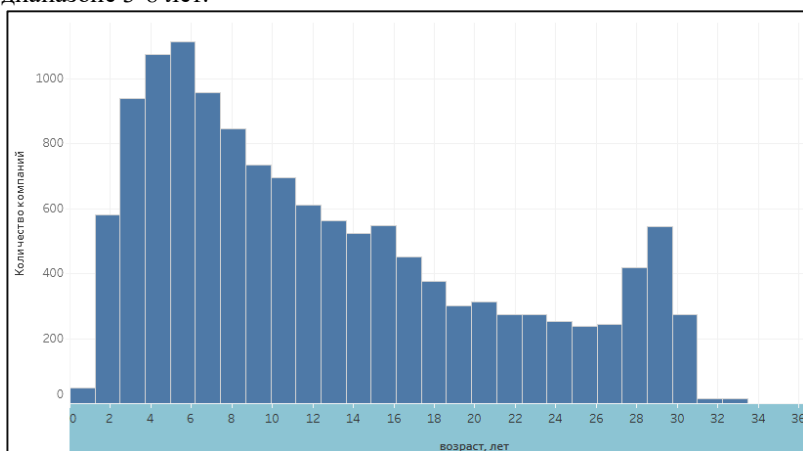


Рисунок 5 – Распределение компаний по возрасту

Можно заметить, что с увеличением возраста количество организаций неуклонно снижается, но затем наблюдается небольшой рост «долгожителей» в интервале 28-30 лет. Первоначально напрашивается вывод, что долгожители представлены крупным бизнесом, но, как ни странно, этот вывод ошибочен: более 50% относятся к микропредприятиям и только порядка 5% относятся к крупному бизнесу. Это может свидетельствовать о том, что многие компании не растут на протяжении длительного периода времени, а это, в свою очередь, замедляет развитие отрасли в целом.

Теперь сосредоточимся на некоторых финансовых показателях, дополняющих полученную картину организаций электронной промышленности, в том числе на тех, которые являются индикаторами выполнения целей Стратегии.

Динамику выручки и чистой прибыли за период 2017 – 2020 гг. можно увидеть на рисунках 6, 7.

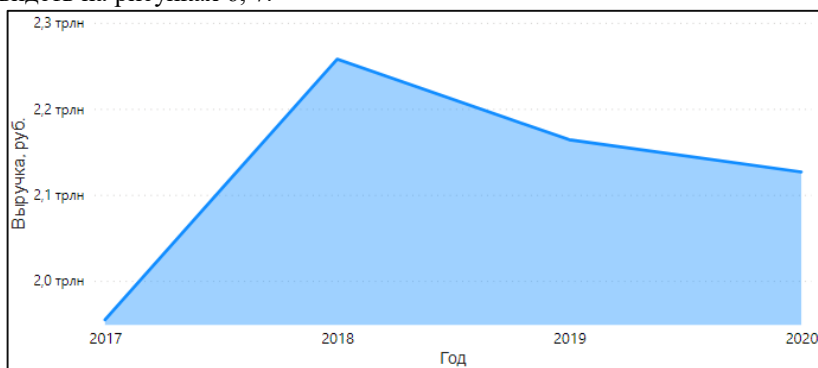


Рисунок 6 – Динамика выручки по компаниям за 2017-2020 гг.

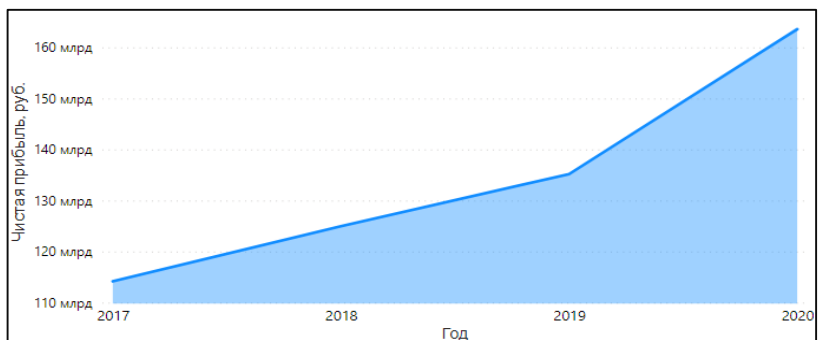


Рисунок 7 – Динамика чистой прибыли по компаниям за 2017-2020 гг.

Из приведенных рисунков можно сделать вывод, что на фоне нестабильно меняющейся выручки чистая прибыль показывает уверенный рост, даже по итогам «ковидного» 2020 года. Для понимания того, организации каких форм собственности внесли наибольших вклад в рассмотренные показатели, изобразим еще 2 рисунка (по данным 2020 года):

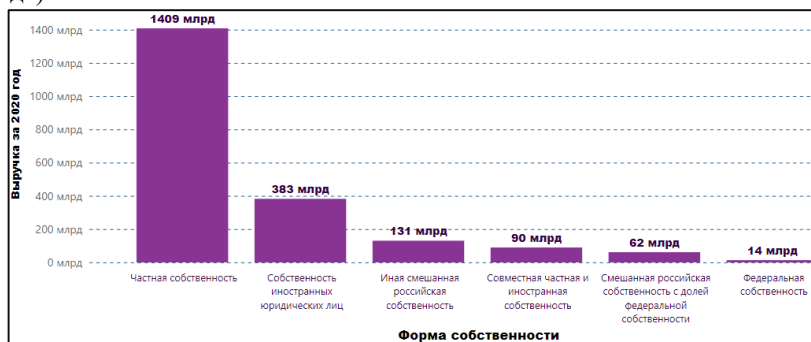


Рисунок 8 – Величина выручки в разрезе форм собственности (показаны наиболее значимые элементы за 2020 год)

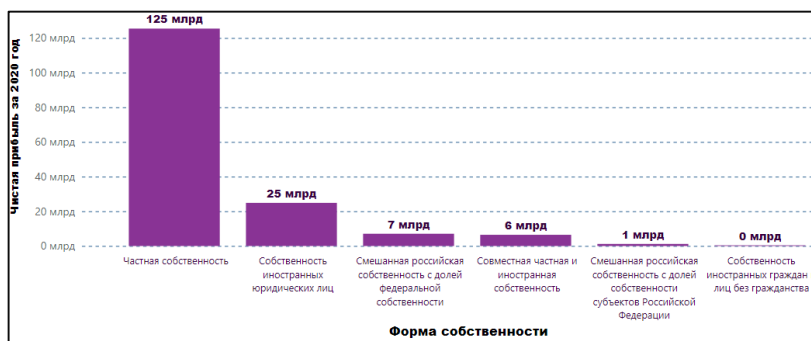


Рисунок 9 – Величина чистой прибыли в разрезе форм собственности (показаны наиболее значимые элементы за 2020 год)

Сопоставляя рисунки 8, 9 с количеством компаний с иностранным участием (напомним, что доля таких компаний составляет 4,17% от общего количества) можно получить очень важные соотношения. Количество компаний, относящихся к российской частной собственности (12 264), больше количества компаний с иностранным участием (552) в 22,2 раза. Однако, выручка, получаемая компаниями, относящихся к российской частной собственности, больше выручки, получаемой компаниями с иностранным участием, всего лишь в 3 раза (рис.8). Это подтверждает

ранее сделанный вывод о том, что среди компаний с иностранным участием преобладает крупный бизнес. При этом, чистая прибыль, получаемая компаниями, относящихся к российской частной собственности, больше чистой прибыли, получаемой компаниями с иностранным участием, в 4 раза (рисунок 9). Также, информативным является расчет выручки, приходящейся в среднем на одну компанию:

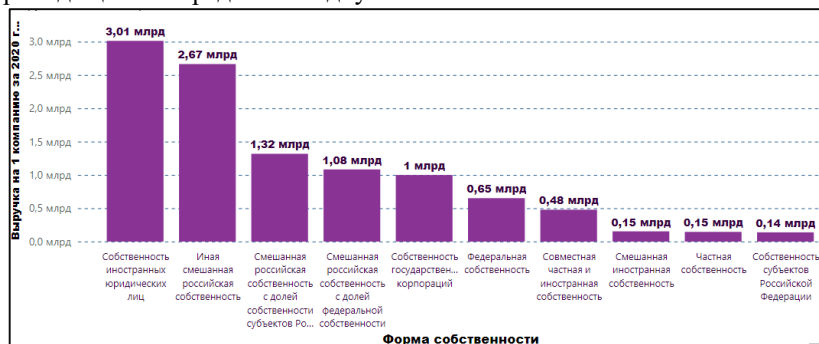


Рисунок 10 – Размер выручки на 1 компанию в разрезе форм собственности (показаны наиболее значимые элементы за 2020 год)

Из рисунка 10 можно сделать вывод, что в частном капитале преобладает, в основном, малый бизнес, в то время как средние и крупные компании относятся к сегменту с иностранным участием, либо с государственным участием.

Рассмотрим теперь, как происходит распределение прибыли в разрезе форм собственности. Сразу оговоримся, что далеко не все компании (а тем более микропредприятия) составляют иные формы отчетности, кроме бухгалтерского баланса и отчета о финансовых результатах, поэтому в полной мере оценить направления использования прибыли не представляется возможным. К тому же, в информационном ресурсе [3] отсутствуют показатели отчета об изменениях капитала, что еще больше затрудняет проведение анализа использования прибыли. Поэтому, в качестве источников информации будут использоваться данные об уплаченном налоге на прибыль и о выплаченных дивидендах из отчета о движении денежных средств (с оговоркой, что не все компании данный отчет составляют) по средним и крупным предприятиям.

На рисунках 11 и 12 приведена информация о выплаченных дивидендах и налоге на прибыль в разрезе форм собственности. Обращает на себя внимание тот факт, что крупные компании с иностранным участием выплатили в 1,5 раза больше дивидендов, чем компании частного российского бизнеса, несмотря на то, что крупных компаний с

иностранным участием в 3 раза меньше, чем компаний частного российского бизнеса.

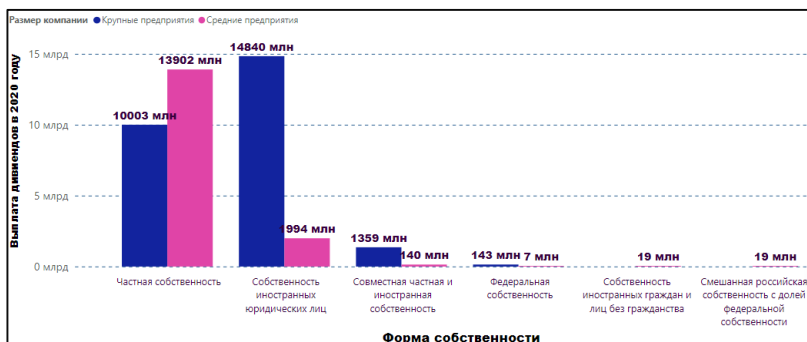


Рисунок 11 – Выплаченные дивиденды в разрезе форм собственности (по средним и крупным компаниям за 2020 год)

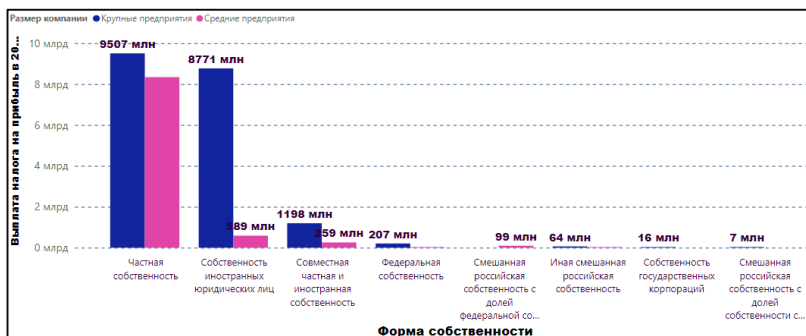


Рисунок 12 – Выплаченный налог на прибыль в разрезе форм собственности (по средним и крупным компаниям за 2020 год)

В свою очередь, величина налога на прибыль распределилась между российскими и иностранными частными крупными компаниями практически одинаково (рис. 12).

Для оценки соотношения налога на прибыль и выплаченных дивидендов рассчитаем соответствующий безразмерный показатель (Налог на прибыль / Выплаченные дивиденды) и построим его распределение в разрезе форм собственности за 2020 год:

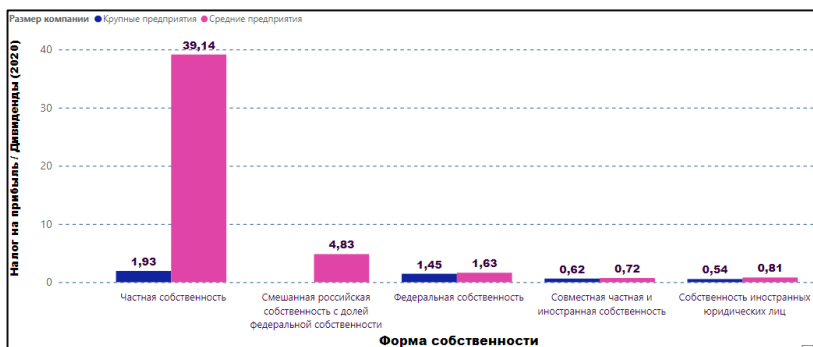


Рисунок 13 – Отношение налога на прибыль к дивидендам в разрезе форм собственности (по средним и крупным компаниям за 2020 год)

Из рисунка 13 можно сделать вывод, что по российскому частному бизнесу значение данного показателя больше 1, в то время как по компаниям с исключительно иностранным участием – на уровне 0,54 – 0,8. Это говорит о том, что российские частные компании (крупные и средние) отдают собственникам существенно меньше, чем направляют в бюджет, в то время как частные иностранные компании поступают наоборот: в российский бюджет направляют ощутимо меньше, чем выплачивают собственникам.

Подводя итоги проведенного анализа, можно отметить следующие основные моменты. Из всей выборки по 13 226 компаниям большинство относятся к малому бизнесу (79,6% от общего количества) и являются обществами с ограниченной ответственностью (89,17% от общего количества). В выборке преобладают, в основном, молодые компании с возрастом 3-8 лет (рис. 5). По формам собственности подавляющее большинство компаний относится к российской частной собственности (92,73% от общего количества), в то время как доля компаний с иностранным участием составляет лишь 4,17% от общего количества. Однако, на иностранные компании приходится значительная доля выручки и выплаченных дивидендов, поскольку в этих компаниях преобладает крупный бизнес.

В заключение было бы целесообразно дать оценку того, на сколько результаты 2020 года соответствуют тем целям, которые указаны в Стратегии (применительно к рассмотренным выше показателям). В соответствии со Стратегией, целевыми значениями показателей развития отрасли за 2020 год, в частности, являются: объем выручки промышленных и научных организаций электронной промышленности - 2 200 млрд. рублей по консервативному сценарию, выработка на одного сотрудника

(производительность труда) в электронной промышленности – 5,6 млн. рублей по всем сценариям [1]. При этом, доля выручки от реализации российской электронной продукции в ВВП страны должна составлять 2,1%.

По фактическим данным (рис. 14) на основе 13 226 организаций получаем, что выручка за 2020 год составляет 2 130 млрд. руб., производительность труда – 6,75 млн. руб. Учитывая объем ВВП за 2020 год по данным Росстата (106 967,5 млрд. руб. [4]), можно сделать вывод, что доля фактической выручки от реализации в ВВП составляет 2%.

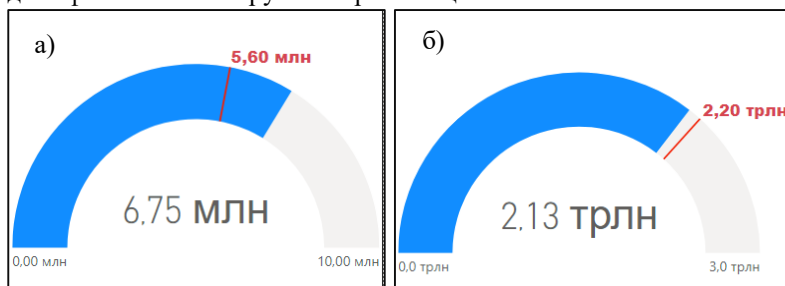


Рисунок 14 – Индикаторы достижения целей стратегии за 2020 год: (а) - производительность труда, (б) – выручка

Из рисунка 14 видно, что в части производительности труда наблюдается выполнение целей стратегии по итогам 2020 года, в то время как по выручке отмечается небольшое отставание. Но, учитывая нестабильную динамику выручки (рис. 6), делать прогнозы на будущее в данный момент крайне затруднительно.

Список использованных источников:

1. Распоряжение Правительства Российской Федерации от 17 января 2020 г. № 20-р «Стратегия развития электронной промышленности Российской Федерации на период до 2030 года».
2. Приказ Министерства промышленности и торговли Российской Федерации от 14 декабря 2020 года № 4343 «О распределении кодов классифицируемых группировок видов экономической деятельности...».
3. Информационный ресурс СПАРК (<https://spark-interfax.ru/>).
4. Сайт Федеральной службы государственной статистики (<https://rosstat.gov.ru/>).

Бережливое регулирование: аудиторы и ПОД/ФТ/ФРОМУ

М.Ю. Андронов

доцент кафедры финансового мониторинга НИЯУ МИФИ, Москва

E-mail: m-andronov78@yandex.ru

П.Ю. Леонов

к.э.н., доцент кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: pyleonov@mephi.ru

Аннотация: Концепция Бережливого регулирования [7] предполагает постоянный поиск и устранение излишних затрат, связанных с регулированием и контролем предпринимательской и иной экономической деятельности, – процесс непрерывного улучшения. В том числе в соответствии с принципами риск-ориентированного подхода. В данной статье анализируются обязательные требования в части «антиотмывочного» законодательства к аудиторским организациям.

Ключевые слова: Бережливое регулирование, внутренний контроль, ПОД/ФТ/ФРОМУ.

Lean regulation: auditors and AML/CFT

Abstract: The Lean Regulation concept implies a constant search and elimination of unnecessary costs associated with the regulation and control of business and other economic activities - a process of continuous improvement. Including in accordance with the principles of a risk-based approach. This article analyzes the mandatory requirements in terms of anti-money laundering legislation for audit firms.

Keywords: Lean Regulation, internal control, AML/CFT.

Ситуация

В соответствии с Федеральным законом от 07.08.2001 г. №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» (далее по тексту – Закон №115-ФЗ) [1] аудиторы обязаны:

Таблица 1 – Требования к аудиторам

№	Требование
1	При оказании аудиторских услуг при наличии любых оснований полагать, что сделки или финансовые операции аудируемого лица могли или могут быть осуществлены в целях ОД/ФТ, обязаны уведомить об этом уполномоченный орган. (п.2.1 ст.7.1 Закона №115-ФЗ)
2	Не вправе разглашать факт передачи информации в уполномоченный орган. (п.4 ст.7.1 Закона №115-ФЗ)
3	Лица, указанные в статье 7.1 настоящего Федерального закона (<i>примечание авторов: в т.ч. аудиторы</i>), обязаны в целях ПОД/ФТ/ПРОМУ разрабатывать правила внутреннего контроля, назначать специальных должностных лиц, ответственных за реализацию правил внутреннего контроля, а также принимать иные внутренние организационные меры в указанных целях. (п.2 ст.7 Закона №115-ФЗ, в редакции Федерального закона от 18 марта 2019 г. №33-ФЗ)

Обращаем внимание, что в рамках данной статьи рассматривается деятельность аудиторских организаций (далее по тексту – АО или аудиторы), оказывающих только аудиторские услуги. При оказании иных услуг, например, бухгалтерских, юридических, перечень обязательных требований в соответствии с Законом №115-ФЗ шире.

Росфинмониторинг в письме от 18.06.2018 г. №04-03-03/12322 [2] в целях выполнения указанных выше требований предполагает разработку рекомендаций со стороны Саморегулируемая организация auditors (далее по тексту – СРО auditors), включающие в том числе:

Таблица 2 – Требования к аудиторам

№	Требование
1	Идентификация клиентов.
2	Определение лиц, ответственных за направление информации в Росфинмониторинг, обладающих необходимым уровнем знаний в области ПОД/ФТ.
3	Регистрация в Личном кабинете Росфинмониторинга аудиторские организации – код 156, индивидуальные аудиторы – код 157.

Информационное сообщение Минфина России от 10.04.2019 г. №ИС-аудит-29 [3] обязывает auditors:

Таблица 3 – Требования к аудиторам

№	Требование
1	Разрабатывать правила внутреннего контроля в соответствии с постановлением Правительства Российской Федерации от 30.06.2012 г. №667.
2	Назначать специальных должностных лиц, ответственных за реализацию правил внутреннего контроля.
3	Принимать иные внутренние организационные меры.

4	Уведомлять Росфинмониторинг о наличии любых оснований полагать, что сделки и финансовые операции аудируемого лица могли или могут быть осуществлены в целях ОД/ФТ.

СРО аудиторов разработало Методические материалы по внутреннему контролю в целях ПОД/ФТ/ФРОМУ (далее по тексту – Стандарт) [4], которые размещены в Личном кабинете каждого аудитора:

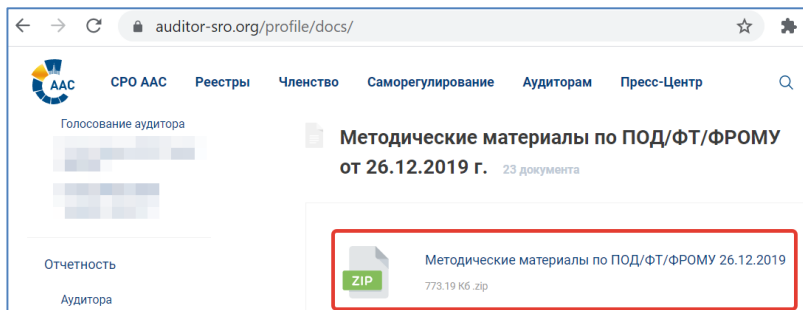


Рисунок 1 – Пример личного кабинета аудитора

В этом Стандарте обязанности аудиторов практически такие же, как у лиц, указанных в статье 5 Закона №115-ФЗ, – полноценных субъектов финансового мониторинга. Вот некоторые из них:

Таблица 4 – Обязанности аудиторов

№	Требование
1	Формирование, утверждение, уточнение Перечня сотрудников, подлежащих обучению. Периодичность: не определена в Стандарте. Предполагается при смене сотрудников на должностях: 1. Руководитель. 2. СДЛ. 3. Главный бухгалтер. 4. Юрист. 5. Сотрудник службы внутреннего контроля. 6. Иные по усмотрению руководителя АО.
2	Разработка и утверждение программы инструктажа: • Вводного; • Дополнительного. Примечание: может выполняться в составе ПВК, а не как отдельный документ.
3	Вводный инструктаж: подготовка и проведение. Для кого: все, кроме СДЛ. Проводит: СДЛ. Периодичность: при приеме на работу или переводе на должности Перечня обучаемых.
4	Дополнительный инструктаж: подготовка и проведение. Для кого: все, кроме СДЛ. Проводит: СДЛ.

	Периодичность: при изменении действующих и вступлении в силу новых нормативных правовых актов, при изменении действующих ПВК. По практике: 2-3 раза в год.
5	Целевой инструктаж: прохождение. Для кого: руководитель, СДЛ, главный бухгалтер, юрист. Проводит: организации, учрежденные Росфинмониторингом, и другими организациями по программам, устанавливаемым Росфинмониторингом. Периодичность: однократно. СДЛ – до начала выполнения обязанностей СДЛ. Остальные – в течение 1 года с даты начала выполнения своих обязанностей.
6	Повышение уровня знаний: прохождение. Для кого: все из Перечня обучаемых. Проводит: организации, которые могут проводить целевой инструктаж. Периодичность: не реже 1 раза в 3 года. СДЛ – до начала выполнения обязанностей СДЛ. Остальные – в течение 1 года с даты начала выполнения своих обязанностей.
7	Учёт прохождения обучения. Журнал учета вводного инструктажа/ дополнительного инструктажа. Документы сторонних организаций, свидетельствующие прохождение целевого инструктажа, повышение уровня знаний.

Кроме указанных в таблице требований по направлению «Подготовка и обучение сотрудников», в Стандарте СРО также определены обязанности по другим задачам внутреннего контроля:

- Организация внутреннего контроля;
- Идентификация клиентов, представителей клиентов, выгодоприобретателей, а также бенефициарных владельцев;
- Оценка степени (уровня) риска совершения клиентом операция, связанных с ОД/ФТ/ФРОМУ;
- Выявление операций (сделок), имеющих признаки связи с ОД/ФТ/ФРОМУ;
- Документальное фиксирование информации;
- Представление сведений в уполномоченный орган;
- Хранение информации и документов;
- Применение мер по замораживанию (блокированию) денежных средств или иного имущества;
- Проверка осуществления внутреннего контроля.

Перечень требований к аудиторам по Стандарту СРО получается весьма обширным.

Проблема

Способствует ли выполнению требований Закона №115-ФЗ обучение главного бухгалтера АО вопросам ПОД/ФТ/ФРОМУ? Сокращает ли выполнение этого требования риск в сфере ОД/ФТ/ФРОМУ?

Стандарт СРО содержит требования практически такие же как для полноценного субъекта первичного финансового мониторинга, например, лизинговой компании или организации, осуществляющие куплю-продажу драгоценных металлов.

Избыточные требования – это излишние затраты. Причем не только для аудиторов, но и для тех, кто определяет эти обязанности и проверяет – на разработку Стандарта и контроль его выполнения. Напомним, что в соответствии с изменениями Закона №115-ФЗ, действующими с 27.06.2021 г. на основании Федерального закона от 11.06.2021 г. №165-ФЗ, контроль в сфере ПОД/ФТ/ФРОМУ в отношении аудиторских организаций осуществляется саморегулируемой организацией аудиторов. Избыточное регулирование влечет дополнительные риски привлечения к административной ответственности.

Ключевое требование к аудиторам: уведомить уполномоченный орган при наличии любых оснований полагать, что сделки или финансовые операции аудируемого лица могли или могут быть осуществлены в целях ОД/ФТ. Разработка ПВК и назначение СДЛ обеспечивают выполнение этой задачи.

Надо ли при этом:

- Идентифицировать представителей клиентов-аудируемых лиц? И соответственно фиксировать эту информацию, например, в анкетах представителей клиентов?

- Не реже чем один раз в три месяца проверять наличие среди клиентов организаций и физических лиц, в отношении которых применены либо должны применяться меры по замораживанию (блокированию) денежных средств или иного имущества? И сообщать о любых результатах в уполномоченный орган?

Перечисленные обязанности скорее избыточны относительно требований Закона №115-ФЗ к аудиторам.

Но так ли это?

Для ответа на этот вопрос необходимо проведение объемной работы по сбору статистических данных:

- Перечень обязанностей;
- Риски, которые сокращаются в результате выполнения этих обязанностей;
- Время, которое тратится на их выполнение;
- Влияние исполнения этих обязанностей на предотвращение вреда охраняемым законом ценностям.

Ниже представлен возможный вариант оценки излишних затрат по одному из направлений «Подготовка и обучение сотрудников».

Предположим, типичную аудиторскую организацию в составе:

1. Руководитель – 1, выполняет также функции аудитора.
2. Аудиторы – 4.
3. Главный бухгалтер – 1.
4. СДЛ – 1.

5. Юрист – 1, выполняет также функции сотрудника службы внутреннего контроля.

В соответствии со Стандартом СРО в Перечень обучаемых должны быть включены все сотрудники.

Однако, применительно к требованию Закона №115-ФЗ, по мнению авторов, достаточно обучить только аудиторов и СДЛ. Причем обучение должно быть более специализированным, без излишней информации, например: «доведение должностных инструкций до сотрудников, переведенных на постоянную работу, связанную с проведением операций (сделок)».

Исходя из сокращения количества обучаемых, в том числе в сторонних организациях, сокращения программ обучения, а значит времени на подготовку и проведение, предположим совокупное сокращение времени сотрудников АО в год примерно на 40 человеко-часов.

Рассчитаем ежегодные излишние затраты на соблюдение избыточных требований:

Таблица 5 – Расчет затрат

№	Показатель	Значение
1	Затраты на выполнение избыточных требований в год одним контролируемым лицом (одна АО), человеко-час	≈40 чел-час
2	Затраты на выполнение избыточных требований в год одним контролируемым лицом (одна АО), руб. Расчет: стр.2.3 * стр.2.4 * стр.1 + стр.2.5	≈₽47'400
2.1	Среднемесячная номинальная заработная плата в организациях с деятельностью финансовая и страховая, руб. [5]	₽91'070
2.2	Среднее количество часов в месяце (на примере 2021 года)	164
2.3	Средняя заработная плата за 1 час, руб. Расчет: стр.2.1 / стр.2.2	₽555
2.4	Коэффициент, учитывающий затраты на оплату страховых взносов и накладные расходы на содержание сотрудника (оборудование, аренда и пр.). Примечание: безусловно этот коэффициент, обеспечивающий расчет общей себестоимости у каждой организации разный; взято среднее значение на основе анализа структуры себестоимости нескольких АО.	2
2.5	Оплата обучения в сторонних организациях (2 человека примерно 1 раз в 2 года по 3'000 рублей).	₽3'000
3	Количество контролируемых лиц на 31.12.2020 г., шт. [6]	3'600
4	Излишние затраты в рублях за год всеми контролируемыми лицами только по требованиям в части подготовки и обучения сотрудников, миллионы рублей	≈171 миллион рублей

Однако, этот теоретический расчет требует подтверждения на широкой выборке контролируемых лиц.

Анализ проблемы

Как определить какое обязательное требование является избыточным, а какое – нет?

Это ключевой вопрос.

Проводимая в России масштабная реформа государственного регулирования и контроля призвана обеспечить системный подход к его решению.

Регулирование и контроль в сфере ПОД/ФТ/ФРОМУ исключены из-под действия недавно вступивших в силу Федеральных законов «Об обязательных требованиях» (от 31.07.2020 г. №247-ФЗ) и «О государственном контроле (надзоре)» (от 31.07.2020 г. №248-ФЗ).

Однако, Федеральная служба по финансовому мониторингу всегда стремилась, насколько это возможно, применять единые с общими по стране подходы к регулированию и надзору. Об этом свидетельствует в том числе вступивший в силу с 27.06.2021 г., Федеральный закон от 11.06.2021 г. №165-ФЗ, в котором определяется требование применять риск-ориентированный подход, в том числе оценки рисков по секторам экономической деятельности с учетом результатов национальной оценки рисков, при организации контроля (надзора) в сфере ПОД/ФТ/ФРОМУ.

Обязательные требования (далее по тексту – ОТ) устанавливаются исключительно в целях защиты охраняемых законом ценностей (ст.5 Федерального закона от 31.07.2020 г. №247-ФЗ).

Охраняемые законом ценности (далее по тексту – ОЗЦ) в сфере ПОД/ФТ/ФРОМУ:

- Жизнь и здоровье граждан;
- Права, свободы и законные интересы граждан и организаций, их имущество;
- сохранность животных, растений, иных объектов окружающей среды, объектов, имеющих историческое, научное, культурное значение;
- Поддержание общественной нравственности;
- Обеспечение установленного порядка осуществления государственного управления и местного самоуправления;
- Обеспечение обороны страны и безопасности государства;
- Обеспечение стабильности финансового сектора;
- Единство экономического пространства;
- Свободное перемещение товаров, услуг и финансовых средств;
- Поддержка конкуренции;
- Свобода экономической деятельности;
- и другие.

Большое количество защищаемых ценностей обуславливает важность деятельности ПОД/ФТ/ФРОМУ.

Вред (ущерб) ОЗЦ:

- Смерть и ущерб здоровью граждан;
- Нарушение прав, свобод и законных интересов интересов граждан и организаций, ущерб их имуществу;
- Подрыв конкурентной среды;
- Сокращение иностранных инвестиций;
- Необоснованный рост волатильности рынка ценных бумаг;
- В целом нарушение работы национальной экономики, так как невозможно выявить и предвидеть поведение лиц, занимающихся легализацией (отмыванием) доходов, полученных преступным путем;
- И другие.
- События, в следствии которых наносится вред (ущерб) ОЗЦ:
- Легализация (отмывание) доходов, полученных преступным путем;
- Финансирование террористической и экстремистской деятельности, в том числе:
 - 1) Оплата расходов на идеологическую пропаганду;
 - 2) Подкуп чиновников и правоохранительных органов;
 - 3) Содержание связанных легальных структур, в том числе деятельность которых признана нежелательной на территории Российской Федерации;
 - 4) Подготовка боевиков;
 - 5) Подготовка и проведение террористических актов, незаконных акций;
 - 6) Выплата вознаграждений наемникам;
 - 7) И другие;
- Финансирование распространения оружия массового уничтожения.

Также в число событий, наносящих вред (ущерб) ОЗЦ можно отнести предикатные преступления. С одной стороны, они предшествуют, являются источником доходов, которые в дальнейшем легализуются. А с другой стороны, эффективная система ПОД/ФТ/ФРОМУ обеспечивает снижение уровня предикатных преступлений, так как в условиях невозможности воспользоваться преступными доходами теряется смысл совершение таких преступлений.

Указанные события также можно определить как Угрозы национальной системе ПОД/ФТ/ФРОМУ.

Таким образом, связка (ОЗЦ – Вред (ущерб) – События (угрозы)) очевидна!

Более сложная задача заключается в определении Источников рисков – какая деятельность финансовых и установленных нефинансовых организаций, лиц может привести к реализации угроз. А также конкретные значения параметров этой деятельности (Факторы риска) и их сочетания (Профили риска). Росфинмониторинг решает эту задачу путем проведения национальной оценки рисков, а также оценки рисков ОД/ФТ/ФРОМУ по секторам экономики.

Ещё сложнее с определением Обязательных требований. Их состав и содержание в разных организациях зависят от оценки рисков.

Надо ли в целях ПОД/ФТ/ФРОМУ обучать главного бухгалтера ювелирного магазина? С какой периодичностью? По какой программе? И множество подобных вопросов.

Национальная «антиотмывочная» система включает в себя два блока: финансовый мониторинг и правоохранный блок. В свою очередь финансовый мониторинг включает: обязательный и внутренний контроль, который проводится соответственно уполномоченным органом и субъектами первичного финансового мониторинга.

Непросто определить ОТ для организаций, осуществляющих операции с денежными средствами и иным имуществом, для того чтобы достичь такие результаты как:

- Риски ОД/ФТ/ФРОМУ понимаются.
- Соразмерно рискам принимаются превентивные меры для предотвращения проникновения преступных доходов, средств на поддержку терроризма/экстремизма в финансовый и другие сектора экономики.
- Информация о подозрительных операциях оперативно, полно, достоверно направляется в подразделение финансовой разведки.
- Предотвращено использование в противозаконных целях юридических лиц и образований для ОД/ФТ/ФРОМУ, а информация касательно бенефициарного владения ими беспрепятственно доступна компетентным органам.

Однако, в отношении аудиторов Закон №115-ФЗ четко определяет требование: «Уведомлять Росфинмониторинг о наличии любых оснований полагать, что сделки и финансовые операции аудируемого лица могли или могут быть осуществлены в целях ОД/ФТ».

Исходя из вышеизложенного, авторы статьи определяют, что обоснованными обязательными требованиями к аудиторам являются те, которые обеспечивают выявление подозрительных операций и сообщение о них в уполномоченный орган!

Такие ОТ обеспечивают защиту ОЗЦ!

На основании этого:

– Обучение главного бухгалтера АО – необоснованно. Главный бухгалтер не изучает документы аудируемого лица.

– А вот более глубокое и предметное обучение аудиторов типологиям ОД/ФТ/ФРОМУ, наоборот, является очень важным.

Перспективным действием, которое обеспечит решение задачи аудиторов, может быть, автоматизация поиска подозрительных операций. Ведение учёта в современных условиях невозможно вне информационных систем. Поэтому вполне реальным, по крайней мере в качестве вспомогательного действия, является запуск в базе данных аудируемого лица, к которой имеют доступ аудиторы, «робота» поиска подозрительных операций по алгоритмам, в которые «зашиты» типологии ОД/ФТ/ФРОМУ. Конечно, ничто не заменит аналитических способностей человека, особенно в условиях неточностей в учете клиента. Однако, быстрая обработка большого массива данных поможет как минимум выявить наиболее рискованные направления. Технологии способны трансформировать привычную реальность и при этом существенно снижать издержки.

Ещё один аспект проблемы избыточных требований к аудиторам в сфере ПОД/ФТ/ФРОМУ: являются ли методические материалы СРО обязательными для его членов? Практика такова, что аудиторы, избегая потенциальных проблем с контролем их деятельности, полностью принимают Стандарт СРО. В любом случае, считаем необходимыми методические материалы от СРО. Но при этом четко определить какие требования обязательные, а какие рекомендованные.

Выводы

Риск-ориентированный подход является важнейшим элементом сокращения излишней административной нагрузки на предпринимателей. И таким образом способствует развитию национальной экономики. Однако, применение этого метода требует тщательной оценки рисков и затрат на выполнение обязательных требований. И это предмет отдельного масштабного исследования.

Список использованных источников:

1. Федеральный закон от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», ст.7.1.
2. <Письмо> Росфинмониторинга от 18.06.2018 №04-03-03/12322 «Об организации системы внутреннего контроля аудиторами при оказании аудиторских услуг в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

3. Информационное сообщение Минфина России от 10.04.2019 №ИС-аудит-29 <Об изменениях Федерального закона от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма">.
4. СРО Ассоциация аудиторов «Содружество». Методические материалы по ПОД/ФТ/ФРОМУ. – URL: https://auditor-sro.org/pc/actions/metodicheskie_materialy_sro_aas_po_podftfromu/ (19.11.2021 г.).
5. Федеральная служба государственной статистики. Среднемесячная номинальная начисленная заработная плата работников организаций по видам экономической деятельности – URL: https://rosstat.gov.ru/labour_costs (19.11.2021 г.).
6. Министерство финансов Российской Федерации. Основные показатели рынка аудиторских услуг в РФ в 2020 году. – URL: https://minfin.gov.ru/common/upload/library/2021/05/main/POKAZATELI_IA-_ZA_2020---170521.docx (19.11.2021 г.).
7. Андронов М.Ю. Бережливое регулирование предпринимательства в России // Государственное управление: Россия в глобальной политике. Материалы XVII Международной конференции (16 мая – 18 мая 2019 г.): [Сборник], электронное издание сетевого распространения / Коллектив авторов. – М.: «КДУ», «Университетская книга», 2019. – 878 с. С. 373-380. – URL: <https://bookonlime.ru/node/4705/> и http://ифэб.пф/images//content/files/documents/ru/statji/Lean_business_regulation_Andronov.pdf (01.07.2021 г.).

Будущее профессий и производительности труда через призму современных цифровых решений

В.В. Лымарь
соискатель кафедры финансового менеджмента,
НИЯУ МИФИ, Москва
E-mail: buhlvv@yandex.ru

Аннотация: цифровые решения и технологии стремительно меняют модели ведения бизнеса и профессиональную роль человека в достижении производственных результатов. Статья дает представление об отличиях цифровизации от автоматизации с целью оценить качественно новый этап индустрии 4.0 и ее влияние на профессиональные сообщества.

Ключевые слова: цифровые технологии, промышленная революция, цифровой двойник, автоматизация.

The future of professions through the modern digital solutions

Abstract: digital solutions and technologies are rapidly changing business models and the professional role of a person in achieving production results. The article gives an idea of the differences between digitalization and automation in order to assess a qualitatively new stage of industry 4.0 and its impact on professions.

Keywords: digital technologies, industrial revolution, digital twin, automation.

В настоящее время регулярно раздаются заявления о цифровой трансформации и следующей за ней «гибелью» целых профессиональных отраслей. От рядового чиновника до министра можно услышать суждения о том, как стремительно охватывающая все отрасли цифровизация меняет наш мир и что профессия бухгалтера, юриста, специалиста по закупкам, водителя и продавца больше не востребована.

Выражу мнение, что пока строятся дороги и беспилотные автомобили, создаются и совершенствуются системы управления ресурсами предприятия, меняется законодательство, а искусственный интеллект учится рисовать цифровые шедевры, у человека есть время для осмысления перемен и поиска своего места в новой реальности.

Конечно, отрицать влияние информационных решений на профессиональную деятельность и жизнь не имеет смысла, но не слишком ли рано и поверхностно мы делаем заявления о не востребованности опираясь на термин «цифровизация»? Предлагаю настоящей публикацией оценить, как цифровые технологии меняют производство и профессии и заглянуть в будущее!

Не смотря на повсеместную автоматизацию и цифровизацию, современный процесс развития организации труда требует непрерывного участия всех членов команды, а значимость человеческого фактора не снижается, человеческий капитал остается главным ресурсом. Но очевидно, что без ИТ-решений и технологичных средств труда, сам по себе, человеческий капитал, не сможет обеспечить рыночное лидерство и конкурентное преимущество.

Таким образом, на первое место выходит сложно интегрированная биполярная система взаимодействия и использования факторов производства «человек - цифровизация», каждый из которых сам по себе не дает глобального преимущества в текущий момент развития. Только синергетический эффект этой связки, правильно встроенный в производственный процесс способен показать высокие темпы роста производительности труда востребованной и конкурентоспособной продукции [9, 12].

В эпоху начала четвертой промышленной революции, примерно с 2010 года становится понятно, что главным драйвером роста производительности становится разделение труда между человеком и машиной (автоматизированными ИТ-системами управления производством) таким образом, чтобы обеспечить максимально возможную и гибкую настройку эффективности ведения хозяйственной деятельности.

Обоюдно направленный трансфер знаний в системе «человек – ИТ-продукт» сейчас является залогом успеха. Это многопоточный процесс обмена информацией, в котором человек обеспечивает быструю и гибкую настройку системы, а цифровой инструмент обрабатывает огромный объем информации и возвращает человеку smart данные для очередного витка настройки с еще более качественными производственными (экономическими) характеристиками [2].

Если делать сопоставление с предыдущими промышленными революциями, то мы наблюдаем сейчас экспоненциальный график скорости внедряемых технологий и цифровизация приобретает качественно новый характер.

Для примера, первая промышленная революция (индустриальная революция) характеризовалась переходом от ручного труда к станкам и охватывала период от второй половины XVIII века до конца XIX века.

Сегодня, с момента идентификации первых признаков четвертой промышленной революции в Германии и США в начале второго десятилетия XXI века до реализации и повсеместного внедрения базовых технологий прошло менее 10 лет [3, 7].

Рассуждая о любом предмете, важно за ранее договориться о дефинициях и терминологии. Как показывает мой опыт профессиональной деятельности в качестве руководителя в атомной отрасли не многие, даже эксперты своего дела, способны внятно привести отличия цифровизации от автоматизации. Почему это важно? Потому что цифровизация представляет собой качественно новый эволюционный этап развития трудовой функции человеческого общества. Подобно разделению труда, механизации, конвейеру, роботизации, информатизации, автоматизации - предмет нашего исследования явился результатом деятельности человека в борьбе за достижения высоких производственных показателей. Видится важным отметить, что, двигаясь от этапа механизации до кибер-физических систем, каждый последующий индустриальный скачок базировался на достижениях предыдущего, делая его своим составным элементом. Чтобы понять влияние цифровизации на каждого из нас важно разобраться, что это такое?

Итак, искать ответ на этот вопрос на полках библиотек не имеет смысла - его там нет, а поиск ответа в глобальной сети Internet выведет исследователя на сотни тысяч ссылок в поисковике Google (который уже сам по себе является цифровым продуктом) и, скорее всего, не внесет однозначной ясности. Предлагаю провести сопоставление понятий автоматизации и цифровизации по ключевым характеристикам.

Во-первых, по степени влияния на процессы и управление данными. Автоматизация позволяет настроить и ускорить локальные, отдельно взятые бизнес-процессы и собрать аналитические данные по ним. Информация течет от источника сбора данных к потребителю сведений.

Цифровизация (цифровая трансформация) априори не локальна и охватывает производственный цикл (организацию) целиком и обеспечивает сбор данных о нем во всех «плоскостях» с последующим анализом и набором управляющего воздействия. Это единое информационное пространство с непрерывным разнонаправленным обменом информацией между элементами системы, результатом анализа которых является выверенное действие для достижения конечного результата с наибольшей эффективностью и без потерь (часто без участия человека) [5, 9].

Применительно к учетно-аудиторской профессии примеров хорошей автоматизации много. Так, современные системы управления ресурсами предприятия ERP- системы, представляют собой образец управленческой автоматизации: финансовое планирование, ресурсное планирование, организация склада, поставка, бухгалтерский и налоговый учет, расчеты с контрагентами, бухгалтерская (финансовая), управленческая отчетность, план-факт анализ, результаты выполнения КПЭ и т.д. Кто-то сейчас справедливо может задать вопрос: но почему же это не пример цифровизации, ведь информация передается разнонаправленно, ERP-система существует в своем едином информационном поле?

Давайте разберемся! Для понимания нам следует взглянуть на ERP-систему «сверху», что позволяет разглядеть ее локальность, применительно к деятельности предприятия. Она обеспечивает исключительно управленческие (организационные) процессы, потребителем ее данных является менеджер, который, в свою очередь уже принимает управленческое решение о корректировке финансовых и производственных целей. ERP-система не предложит заменить сырье, если оно не надлежащего качества, не «увидит» потери от простоев и недопоставок, не сравнит в режиме онлайн показатели деятельности с бенч-марками, не найдет ошибку или подлог в накладной, не скорректирует алгоритм сбора бухгалтерской (финансовой) отчетности, если изменится законодательство, не произведет оплату поставщику за отгруженную продукцию и много еще чего «не сделает». Система управления ресурсами беспомощна без управленца, который является конечным потребителем ее данных. Все это приводит нас к выводу, что системы управления ресурсами предприятия – это инструменты информатизации и автоматизации [11, 12].

Сегодня наука и ИТ-рынок не может предложить доступную универсальную цифровую систему управления предприятием, поскольку система управления является производной от объекта управления, а именно от того насколько точно, быстро и экономично создан цифровой двойник.

К сожалению, в России успешных полноценных примеров цифровой трансформации бизнеса на сегодня нет, но работу в этом направлении активно ведут металлурги, авиастроители, атомная отрасль, железнодорожники, тяжелая промышленность и автомобилестроение (грузовое).

Полноценные успешные примеры цифровой трансформации в мире являются результатом дорогой и кропотливой работы отдельных коммерчески эффективных и устойчивых производственных объединений, которые могут себе позволить полную и дорогую перестройку бизнес-

процессов под тотальную цифровизацию. К таким примерам можно отнести завод электроники по производству контроллеров SIMATIC Siemens в г. Амберге, завод Chrysler в Толедо, заводы Boeing.

Финансовые, качественные и производственные результаты этих зарубежных примеров цифровизации без преувеличения потрясающи. Так, Siemens в г. Амберге выпускает более 1000 номенклатурных единиц продукции с качеством в 99,999%, при уровне роботизации в 75%. Сотни-миллионы записей технологической информации выполняются и анализируются машинами ежедневно, время от заказа клиентом продукции до отгрузки в таком высокотехнологичном секторе составляет всего 24 часа [7, 8].

Последовательное и результативное внедрение в производственный процесс цифровых технологий способствует повышению эффективности предприятия, росту бизнеса и валового внутреннего продукта страны в целом.

Подходы к цифровой организации труда необходимо изучать и совершенствовать для получения качественной модели управления и высоких производственных показателей.

Четвертая промышленная революция предлагает нам технологию интернета вещей. Взаимодействие бытовых и промышленных единиц оборудования между собой и с внешним окружением без участия человека посредством встроенных программных технологий способны трансформировать большую часть экономических процессов. Эта трансформация ведет к изменению скорости и качества протекания производственных процессов, что влечет стремительный рост производительности, как видно на примере Siemens.

Второй отличительной характеристикой цифровизации является объект управления и моделирования – цифровой двойник. Он может имитировать в виртуальной среде производственный объект или изделие и представляет собой цифровой макет основных физико-технических характеристик с возможностью моделирования процессов. Связь между физическим и цифровым двойником продолжается и после создания физического объекта. Это позволяет отслеживать характеристики обслуживания каждого изделия или технологического процесса. Таким образом цифровой двойник может решать задачи поддержания своего физического прототипа на всех стадиях жизненного цикла от создания до утилизации [5,9].

В свою очередь автоматизация процессов и управления производственными объектами представляет собой моделирование в специальных программных продуктах с ограниченным, не аналогичным реальному прототипу количеством параметров. Как правило,

автоматизированные расчеты и проектирование являются частью цифровой модели.

Сегодня многие российские и зарубежные компании в области автомобилестроения, аэрокосмической отрасли, судостроении, нефтегазовом секторе, электроэнергетики, атомной отрасли и здравоохранении могут продемонстрировать весьма продвинутые модели цифровых двойников своих изделий и отдельных испытательных процессов. Это существенно снижает расходы на испытания, наладку, перенастройку и проектирование конечного продукта.

Мало кого можно сейчас удивить технологией 3-D печати. В основе этой технологии лежит именно цифровая модель изделия. От экспериментальных и развлекательных задач в начале 2000-х годов к настоящему моменту она выросла и эффективно используется в оружейной отрасли, при строительстве зданий, в медицине при производстве медикаментов, протезировании и даже трансплантологии. И снова мы видим качественное и количественное улучшение производительности по отношению к работе выполняемой человеком. В совокупности с технологией интернета вещей 3-D печать может принципиально изменить подходы к созданию и воспроизводству производственных мощностей посредством само воспроизводства деталей и запасных частей без участия человека [7, 8].

Нельзя обойти стороной технологию виртуальной (дополненной) реальности, которая меняет процессы ремонта и наладки оборудования, капитального строительства и сооружения сложнейших и высокотехнологичных единиц техники, таких как самолеты, карьерные самосвалы, железнодорожное оборудование и т.п. Скорость, качество и уровень производительности труда при использовании данной технологии позволяет говорить о ее конкурентоспособности и ценности в производственном процессе.

На этом этапе анализа роли цифровых решений в производственных процессах уместно было бы задать вопрос о том, каким образом связать технологические достижения и самостоятельность машин и оборудования с выполнением законодательных норм, соблюдением договорных условий, выполнением платежей, обеспечением бухгалтерского и налогового учета и иными обслуживающими производство функциями? Ведь машина не знает законов и принципов их применения!

Четвертая промышленная революция дает ответ на этот вопрос посредством технологии блокчейна. Технология последовательной распределенной записи с кодировкой через хеш-сумму позволяют сформировать самостоятельную цифровую экосистему, функционирующую по заложенным правилам (законам), которую

практически невозможно взломать или подделать. Таким образом, выполнение условий контракта, например, в части оплаты поставки будет безусловно выполнено, если настроенная посредством блокчейна платежная система идентифицирует ключевые события для этого действия объективно исполненными. Аналогичный подход в ближайшие годы мы будем наблюдать в области бухгалтерского и налогового учета, договорного права, в банковском секторе, инвестиционном бизнесе, биржевой торговле, ведении государственных реестров (например, земельного реестра или актов записи гражданского состояния), в вопросах объективной идентификации человеческой личности, в платежных системах.

В качестве третьего идентификатора цифровизации и автоматизации представляется необходимым обозначить принцип управления данными.

Цифровизация предполагает непрерывное управление данными об объектах, на протяжении всего их жизненного цикла, включая автоматический сбор, накопление, изменение и анализ информации, а также генерацию smart данных.

Мы наблюдаем масштабные цифровые проекты по обработке big data любого уровня сложности и качества структурирования. Сейчас эти данные используются повсеместно в страховании, банковском секторе, научной среде (от военных технологий до астрофизики), торговле, здравоохранении, производстве, при разработке операционных систем и цифровых устройств и так далее. За неполные 10 лет big data не просто потеснила, а заменила собой системы управления базами данных и решения business intelligence, которые обеспечивали обработку информации с момента появления первых вычислительных устройств с середины XX века [1].

Сейчас мы можем прогнозировать во что трансформируется эта технология, когда горизонтально масштабируемые программные инструменты big data получат в свое распоряжение квантовые компьютеры с принципиально новым принципом оперирования кубитами (в отличие от битов обычного компьютера), что позволит обрабатывать все возможные состояния информации не последовательно, а одновременно и тысячекратно повысить производительность алгоритмов. Вероятно - это положит начало формирования полноценного искусственного интеллекта, способного изменить наше представление о производительности и профессии.

Автоматизация, в свою очередь, направлена на решение рутинных задач одного или смежных бизнес-процессов, таких как, торговый, складской, бухгалтерский, управленческий учет, электронный документооборот и не

рассматривает дальнейшее использование данных за границами этих процессов [8].

По итогам проведенной идентификации процесса цифровой трансформации выделим три главных отличительных признака цифровизации:

1. Влияет на все процессы жизненного цикла предприятия.
2. Имеет в своей основе цифрового двойника процесса или изделия для моделирования и предиктивного управления.
3. Осуществляет непрерывное накопление, управление и обмен данными для smart-анализа в режиме он-лайн.

Сегодня можно воочию наблюдать результаты четвертой промышленной революции, где уже происходит перераспределение ролей между человеком и машиной. Меняется уровень производительности труда и роль человека в ней.

Беспилотные автомобили – это уже реальность в США и Канаде. Ближайшие годы эта технология станет повсеместной нормой для каждой страны.

На вредных и сложных промышленных производствах полностью роботизированные производственные линии выполняют опасные и трудозатратные операции.

В медицине появляются смарт-ассистенты врачей общей практики и хирургов. Отдельные типовые хирургические операции уже полностью выполняют роботизированные устройства.

Очевидно, что беспилотные устройства и не только автомобили, но и дроны полностью поменяют логистическую отрасль. Человек больше не будет тратить время на управление средствами доставки. Скорость и мобильность логистических процессов значительно возрастёт.

Планшеты и смартфоны на работе и дома используются сейчас повсеместно и как средство коммуникации и как средство платежа, как часть интернета вещей, как фото- и видео- устройство, как способ контроля состояния здоровья, занятия спортом, навигации, обучения, музыкального, художественного, литературного творчества.

В ближайшие десятилетия мы получим не только стремительное технологическое развитие, но кратно более высокую скорость этого развития. Это неизбежно изменит мир внутри и вокруг нас, включая профессиональную деятельность человека любой профессии, как элемента производственной системы.

Список использованных источников:

1. Клаус Шваб. Технологии четвертой промышленной революции / М.: Эксмо, Бомбора, 2018.

2. Автономов Ю. В., Елизарова Е. Т. Доверие, ожидания и чрезмерный оптимизм: экспериментальное исследование //Журнал Новой экономической ассоциации. 2016. №1 (29). С. 27–53.
3. Идрисов А. Производительность труда как ключевой фактор конкурентоспособности российской экономики. URL: <http://strategy.ru/research/3/>
4. Красильников О. Ю. Изменение трудовых отношений в условиях становления информационной экономики // Известия Саратовского университета. Серия Экономика. Управление. Право. 2009. № 7. С. 3–13.
5. Прохоров А., Лysачев М. Научный редактор профессор Боровков А. Цифровой двойник. Анализ, тренды, мировой опыт. Издание первое, исправленное и дополненное. – М.: ООО «АльянсПринт», 2020. – 401 стр., ил.
6. Рачек С.В., Мирошник А.В. Производительность труда как основной показатель эффективности трудовой деятельности. URL: <http://www.science-education.ru/113-11461/>
7. Самые цифровые страны мира: рейтинг 2020 года // <https://hbrussia.ru/innovatsii/trendy/853688>
8. Экспертное мнение. Примеры наиболее удачных проектов цифрового производства России // https://uppro.ru/library/information_systems/automation_production/primer-y-russia/
9. Digital Twin: Mitigating Unpredictable, Undesirable Emergent
10. Behavior in Complex Systems [Electronic resource]. – Available
11. at: https://link.springer.com/chapter/10.1007/978-3-319-38756-7_4.
12. The digital twin paradigm for future NASA and U.S. air force vehicles [Electronic resource]. – Available at: https://www.researchgate.net/publication/268478543_The_digital
13. [twin_paradigm_for_future_NASA_and_US_air_force_vehicles](https://www.researchgate.net/publication/268478543_The_digital).
14. McKinsey Global Institute The age of analytics: competing in a data-driven world. McKinsey & Company in collaboration with McKinsey Analytics. 2016. 123p. URL: <https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world> (accessed: 26.03.2020).
15. Moser H. Reshoring Was at Record Levels in 2018. Is It Enough? Industry Week, Jul 08. 2019. URL: <https://www.industryweek.com/economy/reshoring-was-record-levels-2018-it-enough> (accessed: 26.03.2020). National Intelligence Council. (2012) Global Trends 2030: Alternative Worlds. A publication of the National Intelligence Council, USA. 140 p.

Виды и способы оценки эффективности работников департамента внутреннего аудита

Н.С. Торопчин

студент 5 курса НИЯУ МИФИ, Москва

E-mail: torop4innik@yandex.ru

Аннотация: В статье представлены предложения и обзор способов оценки ключевых показателей эффективности внутренних аудиторов в целях получения возможности оценки работы сотрудников департамента. Раскрывается методология осуществления процедур оценки сотрудников, выполняющих внутренний аудит клиента.

Ключевые слова: внутренний аудит, оценка эффективности сотрудников внутреннего аудита, виды и способы оценок эффективности аудиторов.

Employees of the Internal Audit Department. Estimation effectiveness methods.

Abstract: The article presents proposals and an overview of ways to estimate key performance indicators of internal auditors in order to be able to evaluate the work of auditor department. The methodology of the evaluation procedures for employees performing internal audit of the client is solved.

Keywords: internal audit, employees performance evaluation.

Введение

Внутренние аудиторы оказывают помощь во внутреннем контроле, в корпоративном управлении, в управлении рисками. Но как проверить и оценить работу самого аудитора? Эта функция также должна кем-то выполняться. Необходимо иметь возможность измерить полезность аудиторов, так как их деятельность косвенно влияет на выводы и решения, формируемые руководством.

Для оценки эффективности работы аудиторов используется термин «ключевые показатели эффективности» (далее – КПЭ). Они устанавливаются управленческим составом, советом директоров или аудиторским комитетом, это зависит от организационной структуры компании. Возможен также вариант формирования КПЭ сотрудниками внутреннего аудита и последующей передачи этой информации на более высокие уровни.

Естественно, особое значение стоит придать лицу, которое осуществляет оценку этой деятельности. Оно должно быть непредвзято, объективно и честно. Возможно, лучшим вариантом будет последовательное формирование оценки сначала руководителем проекта, а затем вышестоящим сотрудником или комитетом.

В данной статье рассмотрены способы оценки эффективности работников внутреннего аудита, а также варианты ее формирования таким образом, чтобы не подвергать сомнению независимость и объективность сотрудников.

Сроки выполнения аудиторских проектов

Чаще всего к срокам выполнения какой-либо работы предъявляются конкретные требования. Поэтому естественно, что время оказания услуг внутреннего аудита и момент принятия решений необходимо вписать в конкретные рамки.

Для эффективной проверки сроков выполнения аудиторских проектов необходимо учитывать множество факторов. Некоторыми из них аудитор попросту не может управлять. Например, сотрудник может реально работать на проекте меньшее количество времени, а формировать отчет дольше. Такое может случиться, если помимо рекомендаций аудита требуется осуществить дополнительные сопутствующие услуги. В таком случае предлагается разработать и следовать методологии, которая могла бы разделить аудиторские процедуры на временные интервалы. Каждому интервалу должен будет соответствовать этап. На основании анализа времени, потраченного на работу по каждому этапу, получится сформулировать оценку эффективности. Например, на этапы может быть отведено стандартное время выполнения или оно может определяться индивидуально для каждого проекта в зависимости от объемов работы и сложности.

Качество выполнения аудиторских проектов

При оценке качества выполняемых услуг могут быть использованы формы с определенными критериями по выполненным работам. Чаще всего этими формами являются опросники, однако, для точной оценки КПЭ необходимо прежде всего обратить внимание на компетенции сотрудника и на его активные проекты. Важно определить кто перед нами: ассистент, аудитор или начальник департамента. Более того, разные проекты могут иметь разную сложность и одно и то же лицо будет на одном проекте в роли обычного аудитора, а на втором, к примеру, руководителем. Исходя из этого, необходимо назначать соответствующие критерии оценки для каждого работника, исходя из его ситуации. Способы оценки должны быть сформированы таким образом, чтобы учитывались не только формальные обязанности и должность, но и выполняемая роль сотрудника.

Также важно обратить внимание на навыки. Для каждого работника они делятся на две категории. В современном мире их принято называть *soft-skills* и *hard-skills*. Другими словами – качества, которые раскрывают человека как личность и профессиональные навыки в конкретной области.

Для аудитора будут важны *hard-skills* такие как:

1. Знание стандартов внутреннего аудита
2. Владение соответствующим программным обеспечением
3. Грамотная устная речь
4. Грамотная письменная речь
5. Знание иностранных языков
6. Знание бухгалтерского учета

Естественно, для оценки КПЭ внутреннего аудитора необходимо определить и перечень требуемых профессиональных навыков. Они могут быть подтверждены с помощью заполнения опросника, теста. Узкопрофильное тестирование – это отличный способ сэкономить время и проверить профессиональные знания.

Источниками получения аудиторских доказательств являются:

- *Все ответы правильные*
- *Первичная документация проверяемой организации*
- *Регистры бухгалтерского учета*
- *Результаты анализа финансово-хозяйственной деятельности*

Рисунок 1 – Пример вопроса из теста для внутреннего аудитора

На запрос аудитора получен ответ третьей стороны. Это свидетельствует о том, что третьей стороне был направлен запрос:

- *Комбинированный*
- *Негативный*
- *позитивный*
- *Утвердительный*

Рисунок 2 – Пример вопроса из теста для внутреннего аудитора

Среди *Soft-skills* внутреннему аудитору необходим такой набор навыков, который бы позволял эффективно взаимодействовать с другими членами коллектива и клиентами.

К ним могут относиться:

1. Умение работать в команде
2. Стрессоустойчивость
3. Управление конфликтами
4. Быстрая обучаемость

Наличие этих навыков, а главное, их применение в процессе деятельности внутреннего аудита тоже должно быть зафиксировано должностным лицом, так как они влияют на качество. Произвести оценку сможет руководитель проекта, который является вышестоящим контролирующим звеном. Однако, для комплексности оценки качества, а также для ее объективности предлагается формирование мнения каждого члена команды о результатах работы других. В частности, руководителя проекта и финальный отчет будет оценивать вышестоящий руководитель отдела. Однако, при таком методе оценивания может возникнуть проблема - есть риск возникновения ситуации, при которой сотрудник будет избыточно лоялен при оценке коллеги, зная, что его работу будет оценивать также коллега. К сожалению, хоть стандарты и требуют от аудиторов избегать внутреннего конфликта, в данном случае, он все же может возникнуть. Но снизить подобный риск реально. Например, можно составить такой опросник, при котором члены команды будут оценивать друг друга и руководителя при соблюдении условий конфиденциальности. Участникам будет предоставлена возможность ответить на вопросы анонимно, а также дать развернутый отзыв-комментарий о работе.

Таким образом, получится оценить качество выполнения аудиторских проектов с точки зрения примененных аудиторами навыков, включая их индивидуальные способности.

Устранение выявленных недостатков

После выпуска отчета аудиторы могут не заканчивать свою работу с клиентом, а сопровождать его по мере устранения выявленных, при изучении деятельности заказчика, недостатков. Это естественно, ведь целью внутреннего аудита является совершенствование работы компании. На протяжении этого этапа происходит отслеживание качества мероприятий по реализации корректирующих мер. В этой связи могут быть осуществлены дополнительные действия аудитора, такие как выпуск отчетности о статусах закрытия недостатков, разработка новых рекомендаций до закрытия недостатков.

Развитие и квалификация

Очевидно, что повышение квалификации сотрудников внутреннего аудита будет положительно влиять на уровень их КПЭ. Конечно, такие сертификаты как CIA, ACCA не являются обязательными и лишь подтверждают навыки аудитора, тем не менее, при подготовке к их получению аудитор не только усваивает новые знания, но и фиксирует старые. Более того, наличие подобных документов свидетельствует о высоком уровне профессионализма и повышает престиж данной профессии, так как компетенции, относящиеся к ней, можно подтвердить сертификатом.

Именно поэтому, для повышения эффективности работы внутреннего аудитора необходимо регулярное дополнительное обучение (не менее определенного количества раз в год), а руководству аудиторской компании следует мотивировать своих сотрудников на улучшения качества и количества их знаний. Применяя такой подход, общий уровень эффективности деятельности возрастет, так как компетенции каждого работника увеличатся.

Дополнительные проекты

При обычном осуществлении аудиторской деятельности в течение года могут возникать запросы от клиентов по внеплановым проверкам, а также по рассмотрению и анализу отдельных бизнес-процессов. Качество исполнения дополнительных проектов должно отображаться и при оценке общей эффективности. Не стоит забывать о времени, которое должен учесть руководитель при постановке задачи под подобные заказы, основываясь на практике предыдущих лет. Если сроки и качество по внеплановым проектам соблюдены и удовлетворяют критериям эффективности, тогда организация работы внутренних аудиторов устроена верно и должна быть надлежащим образом оценена по КПЭ по каждому сотруднику и по каждой рабочей группе в целом.

Развитие и продвижение внутреннего аудита

Если для развития внутреннего аудита требуется совершенствование методологии и соответствие международным стандартам и общемировой практике, то для повышения значимости внутреннего аудита для заказчика необходимо увеличение доверия участников бизнеса к этому процессу. Необходимо делиться информацией с клиентами и потенциальными клиентами о важности контроля и управления рисками. В этих целях могут проводиться лекции, семинары, конференции, на основании материалов которых клиент сформирует мнение о необходимости проведения внутреннего аудита. Осуществление аудитором разъяснительных мероприятий положительно повлияет и на его КПЭ.

Показатели эффективности, которые не следует устанавливать

Одним из проблемных вопросов внутреннего аудита является то, в каком объеме бизнес прислушивается и принимает решения на основании рекомендации аудитора по бизнес-процессу. С одной стороны, аудитор может не обладать информацией о всех бизнес-процессах и картине в целом, поэтому его рекомендация может быть не самой оптимальной. И тогда, если в компании сильна позиция внутреннего аудита, его рекомендации и предложения будут исполнены в точности. С другой стороны, даже если рекомендация недостаточно эффективна, факт обнаружения проблемы свидетельствует о полезной функции внутреннего

аудита и облегчает задачу менеджменту. В этой связи трудно установить КПЭ внутреннего аудита.

Другой проблемой является оценка качества выполненной работы на основании количества выявленных недостатков в процессе работы по ряду причин:

1. Бизнес-процессы отличаются по объему
2. Такой способ оценки может привести к излишним придиркам со стороны аудитора, и как следствие, к увеличению затрат бизнеса по их устранению.
3. Выявленные недостатки будут искусственно разбиваться на более мелкие.

Необходимость оценки эффективности работы аудиторов.

Показатели КПЭ аудиторов могут потребоваться совету директоров или департаменту аудита для оценки эффективности самой деятельности аудита.

Также они могут пригодиться руководителю департамента аудита или его сотрудникам, чтобы коллектив мог сформировать единое мнение о векторе их деятельности.

КПЭ могут нести в себе стратегический характер, а именно закладывать цели развития в будущем, помочь избежать повторяющихся ошибок, повысить собственную деловую активность и эффективность.

В департаменте внутреннего аудита могут устанавливаться следующие цели для повышения КПЭ его деятельности:

1. Увеличение количества сертифицированных аудиторов в подразделении.
2. Повышение среднего бала по индивидуальным оценкам сотрудников
3. Выполнение аудиторского плана
4. Покрытие бизнес-процессов аудиторскими проверками
5. Выполнение дополнительных проектов
6. Эффективность загрузки персонала
7. Соответствие международным стандартам

Заключение

Таким образом, выбрать стратегию для повышения качества внутреннего аудита не всегда легко. Стоит отметить, что некоторые критерии оценки могут существенно усложнять процесс работы департамента. Критерии оценки деятельности сотрудников не должны быть слишком высокими и в тоже время не должны быть легкодостижимыми. Также стоит обращать внимание на динамичность изменений в хозяйственной деятельности, поэтому некоторые способы оценки могут быть устаревшими и тормозить работу аудиторов.

Список использованных источников:

1. Международные основы профессиональной практики внутреннего аудита [Электронный ресурс]. – Режим доступа: <https://www.iaa-ru.ru/contact/Standards-rus.pdf>.
2. Броило Е.В. Теоретические основы аудита – 2019. – С. 184.
3. Галкина Е. В. Современная модель внутреннего контроля в корпоративном менеджменте // Рос. предпринимательство. 2018. № 1(223).
4. Информационный портал - Бухгалтерский учет. Налоги. Аудит [Электронный ресурс]. – Режим доступа <https://www.audit-it.ru>
5. Щербакова Е. П. Комплексный подход к вопросу оптимизации процессов регламентации и стандартизации внутреннего аудита в российских коммерческих организациях // Менеджмент сегодня. 2019. № 2. № 19.
6. Суйц В.П., Хорин А.Н., Жакипбеков Д.С. Диагностика недостоверности отчетности организации: статистические методы в оценке достоверности бухгалтерской отчетности // Аудит и финансовый анализ. – 2015. – № 1. – С. 179-188.

УДК 330.3:78.03(519)

© Р.Ч. Авшалумова, Ю.В. Никитинская, 2021

Влияние корейской музыкальной субкультуры на экономику Южной Кореи

Р.Ч. Авшалумова

студентка 1 курса НИЯУ МИФИ, Москва

E-mail: rashka.avshalumova@yandex.ru

Ю.В. Никитинская

к.э.н., доцент кафедры финансового менеджмента

НИЯУ МИФИ, Москва

E-mail: yvnikitinskaya@mephi.ru

Аннотация: проанализировано влияние корейского культурного движения и молодежной субкультуры как фактора развития экономики Южной Кореи и предмета южнокорейского экспорта на примере ведущей k-pop группы BTS, корейская волна Халлю.

Ключевые слова: молодежная субкультура, k-pop, монетизация, вклад в экономическое развитие.

The influence of the Korean musical subculture on the economy of South Korea

Abstract: the influence of the Korean cultural movement and youth subculture as a factor in the development of the economy of South Korea and the subject of South Korean exports is analyzed on the example of the leading k-pop group BTS, korean wave Hallyu.

Keywords: youth subculture, k-pop, monetization, contribution to economic development.

Анализ влияния популярного культурного движения на молодежь как носителя элемента потребительского спроса, следовательно, фактора изменения величины ВВП и экономического развития, приобретает особую важность, поскольку за последние несколько лет популярность корейской культуры и современной корейской музыки (k-pop) среди молодого поколения всего мира значительно увеличилась. Это проявляется не только в свободном распространении музыкальных произведений, но и в так называемой монетизации практически всего, что связано с k-pop.

В современных условиях с помощью достижений НТП и применением возможностей сети Интернет сложилось «Движение свободной культуры»,

участники которого придерживаются позиций свободного обмена идеями и информацией в различных сферах, с использованием сети Интернет и СМИ.

Изучение влияния новых направлений в музыке на экономическое развитие и экономический рост Южной Кореи в последние годы, а также анализ влияния этих направлений на экономики других стран благодаря молодежному течению является актуальным.

Проводя подобное исследование необходимо определить и проанализировать современные молодежные корейские культурные движения. Определить их влияние на национальную экономику Южной Кореи и с учетом этого оценить развитие страны за последний год.

Теоретической базой данного исследования выбраны сбор, анализ и систематизации информации о современных молодежных культурных движениях Южной Кореи, о их особенностях, о каналах распространения, статистических данных по экспорту товаров, связанных с подобными движениями.

Практическая значимость исследования заключается в том, что результаты проведенного анализа следует принимать во внимание при разработке экономической политики, если страна ищет новые факторы и источники роста потребительского спроса как фактора роста ВВП, поскольку современные музыкальные движения можно использовать в качестве подобных, что видно из опыта Южной Кореи.

В современном обществе существуют множество субкультур, увлечение которыми характерно для различных социально-возрастных групп, в том числе и для молодежи.

Под молодежью понимается особая социально-возрастная группа, имеющая определенные возрастными ограничения и особый статус в современном обществе, который определяется как переходный период от детства и юности к возрасту социальной ответственности.

Субкультура определяется как часть общей культуры, системы ценностей, правил, норм поведения, традиций и обычаев, присущих четкой выраженной группе в обществе.

Для анализа влияния современной молодежной культуры Южной Кореи обратимся к исторической справке об условиях и особенностях формирования корейской молодежи и ее субкультур к началу XXI века.

Разделение Корейского полуострова в 1948 г., а также экономические и социальные реформы западного образца оказали значительное влияние на фундаментальные изменения общества Южной Кореи. С 1960-х гг. южнокорейское общество по своей структуре стало значительно усложняться, что является характерным для обществ других стран, которые

находятся в стадии индустриализации. Усложнение структуры привело к формированию в Южной Корее оппозиционных студенческих и молодежных движений за демократические свободы. Параллельно с этим процессом правительство Пак Чонхи объявило проведение программы «Модернизация Родины». Реализация данной государственной программы протекала как процесс навязывания институтов западного образца и одновременный отказ от корейских традиций. Базой для общественных преобразований в Южной Корее, как определяет антрополог Ким Джин Мён, [1] всегда воспринималась корейская молодёжь со стороны властных и политических структур. Кроме того, значению слова «субкультура» со стороны государственной власти Южной Кореи всегда давалась отрицательная окраска. Государственные реформы, жесткость политического режима внутри страны, которые проводились в соответствии с курсом США, привели к формированию большого количества студенческих движений в 1960-1980-е гг. как особой субкультуры Южной Кореи с многочисленными направлениями. В результате к началу 1990-х гг. модернизированная Южная Корея имела глубоко диверсифицированное общество с различными молодежными субкультурами, корнями большинства которых являлись европейские и американские. [2, с. 23]. Тем не менее среди южнокорейских молодежных субкультур есть группы отличные только для Южной Кореи. Причина их появления в сочетании глобализации, высокой степени открытости южнокорейского общества и трех «Н» - неуверенность, неудовлетворённость и беспокойство (тревога) [3, с. 49].

В современном южнокорейском обществе выделяются следующие субкультуры: кей-поп (k-pop) фанатов, блогеров мокпан, косплея, андерграунда и хиппи, ольджанов, клубных тусовщиков. У каждой из групп существует собственная символика и отличительные атрибутами, позволяющие определять их принадлежности к субкультуре. Основными отличительными атрибутами являются общий язык, сеть коммуникаций, личные связи, поверхностные знакомства, общие нормы и ценности, модели поведения и формы взаимоотношений.

В середине 1990-х годов начинается распространение современной культуры Южной Кореи по миру в виде так называемой «Корейской волны» или «Халлю». Данный термин был введен в обиход пекинскими журналистами на фоне резко возрастающей популярности южнокорейских субкультур в Китае и других странах Юго-Восточной Азии, а в дальнейшем распространившихся по всему миру. Корейская волна (Халлю) возникла на фоне экономического кризиса 1997 г. в Южной Корее, когда одним из путей преодоления кризиса стало привлечение инвестиций в индустрию шоу-бизнеса с высокими дивидендами. Это привело к появлению моды на

«всё корейское» в таких азиатских странах как Китай, Тайвань, Япония, Малайзия, Сингапур и др. Со стороны государства двигателем корейской волны стало Министерство культуры Кореи, поскольку именно оно стимулировало инвестиции в медиа-сектор и стало продвигать корейскую культуру за рубеж как экспортный товар [4].

Одним из направлений индустрии шоу-бизнеса для инвестиционных вложений с целью высоких дивидендов стала корейская поп-музыка или движение k-пор как неотъемлемая часть корейской волны (Халлю).

Раскроем особенности данной субкультуры «К-пор» и проанализируем ее влияние на экономику Южной Кореи.

К-пор представляет собой музыкальный жанр Южной Кореи, возникший в 1990-х годах. Этот жанр включает в себя элементы рока, хип-хопа, рэпа, кроссвера, фолка, R&B и других направлений [5].

Являясь музыкальным жанром, К-пор постепенно трансформировался в одну из современных южнокорейских субкультур, которая как часть корейской волны (Халлю) получила распространение по всему миру. В результате, благодаря сети Интернет и коммерциализации жанра со стороны крупнейших южнокорейских развлекательных и звукозаписывающих компаний, а также поддержке со стороны Министерства культуры Кореи К-пор выходит за пределы Южной Кореи и становится полномасштабной молодежной субкультурой, приносящей весомый вклад в ВВП страны.

Поклонники корейской популярной музыки k-пор встречаются по всему миру. Исполнителей k-пор`а называют «айдолы» (от англ. idols). Отметим сходство со словом «идол» и его смыслом, поскольку фанаты им действительно поклоняются и стремятся максимально подражать - покупают потребительские товары, которые их кумиры («айдолы») используют и рекламируют.

Среди самых популярных южнокорейских групп, получивших мировую известность и вносящих свой вклад в создание ВВП и развитие экономики Южной Кореи, первое место занимает группа BTS [6].

BTS — южнокорейский бойзбэнд, образованный в 2013 году южнокорейской звукозаписывающей и развлекательной компанией Big Hit Entertainment. Музыкальная группа состоит из 7 человек, каждый из которых является «айдолом» для фанатов группы. Стремление фанатов быть похожими на своих кумиров («айдолов») выливается не только в посещение любых концертов, но и в приобретение любой сувенирной продукции и товаров, рекламируемых музыкантами. Южнокорейские звукозаписывающие и продюсерские компании создали уникальную систему подготовки и раскрутки своих музыкантов, начиная с создания

музыкальных композиций и заканчивая максимальной монетизацией абсолютно всего, что может ассоциироваться у фанатов с их кумиром («айдолом»).

По оценкам экспертов исследовательского Института Hyundai в Сеуле, проанализировавших рост популярности BTS не только в Южной Корее, но и по всему миру, экономическое влияние группы в несколько десятков раз превышает среднегодовой доход среднестатистической южнокорейской компании. Ежегодный рост экономики Южной Кореи на 3,5 млрд. долл. происходит благодаря реализации сувенирной и рекламной продукции фанатам, подражающим своим кумирам («айдолам») [7].

Уникальная программа создания подобных групп изначально нацелена на достижение успеха «айдолами» с тем, чтобы затем максимально его (успех) монетизировать. Монетизация на примере BTS приносит сопоставимый вклад в ВВП (0,3%) Южной Кореи наравне с крупнейшей корейской авиакомпанией “Korean Air” (0,7%), которая входит в первую двадцатку ведущих авиакомпаний мира.

Успех группы на мировом музыкальном Олимпе, высокие строчки в мировых чартах, огромная популярность и многомиллионная армия фанатов вывели BTS в разряд самых высокооплачиваемых музыкантов. Так в 2019 году BTS признана самым высокооплачиваемым бойзбэндом с годовым доходом более 60 млн. долл [7].

Кроме основного заработка от концертной деятельности и продажи альбомов BTS также как и другие k-поп группы получает доход от проката документальных фильмов о своих концертных турне, продажи сувенирной продукции (фотографии, коллекционные карточки, комиксы, книги и т.п.), рекламных контрактов, стриминга музыки. BTS совместно со своей продюсерской компанией Big Hit Entertainment создали альтернативную вселенную - «Вселенная BTS», для продвижения и общения с фанатами [6]. В итоге поклонники группы являются одним из крупнейших фэндомов в мире, что увеличило экономическое влияние BTS на экономику Южной Кореи через экспорт таких корейских товаров как одежда, косметика, украшения, продукты питания и через приток иностранных туристов, приезжающих в Южную Корею благодаря интересу к BTS. Примерный ежегодный объем экспорта корейских потребительских товаров, приобретаемых поклонниками BTS по всему миру, составляет 64-66 млрд. долл. — это примерно 1,7% от общего экспорта южнокорейских потребительских товаров. По оценкам экспертов Института Hyundai и государственной туристической организации Кореи ежегодный приток в страну иностранных туристов благодаря группе составляет 7,6% от общего притока иностранцев, интересующихся Южной Кореей [5].

Эксперты также прослеживают зависимость увеличения стоимости акции компании, если коллектив начинает с ней свое сотрудничество. Такую зависимость назвали «Эффект BTS».

Проанализировав влияние корейской музыкальной субкультуры на примере самой успешной k-поп группы BTS на экономику Южной Кореи, можно сделать вывод, что подобные корейской волне Халлю субкультуры благоприятно воздействуют на экономику страны и вносят в неё значительный вклад.

Список использованных источников:

1. А.С. Шмаков «Молодежные субкультуры в контексте трансформации идентичности южных корейцев» [электронный ресурс] <https://vestnik.nsu.ru/historyphilology/files/3a3bcfd946b8458c61d01fa40de8b51d.pdf>
2. Ji Soo Ha, Judy Park. Significance of Changing Korean Youth Subculture Styles. *Asian Culture and History*, 2011, vol. 3, no. 1, p. 23–30
3. Park Kyungro. The political Economy of South Korean Trade Growth and Social Change, 1963– 2013. *Journal of Contemporary Korean Studies*, 2017, vol. 4, no. 1: National Museum of Korean Contemporary History, p. 35–64
4. Корейская волна [электронный ресурс] <https://m.korea.net/russian/AboutKorea/Culture-and-the-Arts/Hallyu>
5. <https://thewallmagazine.ru/k-pop-ekonomika-i-politika>
6. <https://www.scmp.com/culture/music/article/2184058/power-k-pop-supergroup-bts-felt-industry-wide-band-release-films-books>
7. <https://zen.yandex.ru/media/id/5b1cdf500422b48be4eca65b/fanbaza-bts-stoit-milliardy-dlia-ekonomiki-iuinoi-korei-5c51afaa4ff65800ad438398>

Влияние процесса цифровизации на развитие малого и среднего бизнеса, его государственного регулирования и поддержку

М.Р. Лихачев

студент 3 курса НИЯУ МИФИ, Москва

E-mail: likhachevm021001@gmail.com

Д.Б. Давыдов

студент 3 курса НИЯУ МИФИ, Москва

E-mail: DBDavydov@mephi.ru

А.Н. Майорова

к.э.н., доцент кафедры бухгалтерского учета и аудита

НИЯУ МИФИ, Москва

E-mail: albina_mayorova@mail.ru

Аннотация: В статье рассматриваются методы и способы влияния государства на субъекты малого и среднего предпринимательства. Продемонстрирована трансформация и внедрение цифровых технологий в налоговые органы РФ и воздействие автоматизации на создание конкурентной среды.

Ключевые слова: малое и среднее предпринимательство, цифровизация, ФНС РФ, специальные налоговые режимы, налогоплательщик, налоги.

Impact of the digitization process on the development of small and medium-sized businesses, their government regulation and support

Abstract: the article discusses methods and techniques of state influence on small and medium-sized businesses. The transformation and introduction of digital technologies in the tax authorities of the Russian Federation and the impact of automation on the creation of a competitive environment are demonstrated.

Keywords: small and medium-sized entrepreneurship, digitalization, Federal Tax Service of the Russian Federation, special tax regimes, taxpayer, taxes.

На сегодняшний день субъекты малого и среднего предпринимательства занимают особое место в РФ. Связано это с постоянным увеличением малых и средних предприятий, благодаря чему создаются новые рабочие места, увеличивается предложение на рынке и,

как следствие, возрастает конкуренция. По сравнению с крупными и градообразующими предприятиями у субъектов малого бизнеса есть существенное преимущество – они требуют меньше вложений и быстро адаптируются к различным нестабильным экономическим ситуациям. Во многих странах налоговая политика направлена на стимулирование малого бизнеса, на рост и дальнейшее развитие таких экономических субъектов. РФ уверенно следует мировой практике, в нашей стране созданы и законодательно установлены специальные налоговые режимы для расширения возможностей развития малого предпринимательства.

Для начала стоит определить значение и функции малого бизнеса. В масштабах страны - это предприятия, соответствующие определенным в законодательстве критериям, не являющиеся монополистическими объединениями, работающие в большинстве случаев в полиполии, где присутствует множество продавцов и покупателей. Экономические функции малых предприятий заключаются в том, что они придают гибкость рыночной экономике, создают конкурентную среду и являются инноваторами, малому бизнесу значительно легче создать новые потребности. К социальным функциям относится создание рабочих мест, рост среднего класса и снижение социальной напряженности.

Малое предпринимательство становится фактором развития только при комплексном выполнении всех задач. Малое и среднее предпринимательство включено в «Стратегию развития РФ до 2030 года» и различными способами поддерживается государством. В данной статье рассмотрим налоговые преференции для малых предприятий. Самая существенная – это право перехода с общего режима налогообложения на специальные режимы. Более того, конечное решение принимает экономический субъект малого предпринимательства, но для того, чтобы получить возможность выбора, необходимо соответствовать определенным условиям.

Таблица 1 – «Критерии отнесения к субъектам малого и среднего бизнеса»

Критерии отнесения	Вид субъекта предпринимательства		
	Микро	Малый	Средний
Среднесписочная численность сотрудников за предыдущий год, чел.	0-15	16-100	101-250
Максимальный доход за год по правилам налогового учета, млн. руб.	120	800	2000

Отметим, что микробизнес относится к субъектам малого предпринимательства.

Графики динамики количества субъектов малого и среднего предпринимательства за последние 2 года представлены на рисунках 1 и 2. [4]

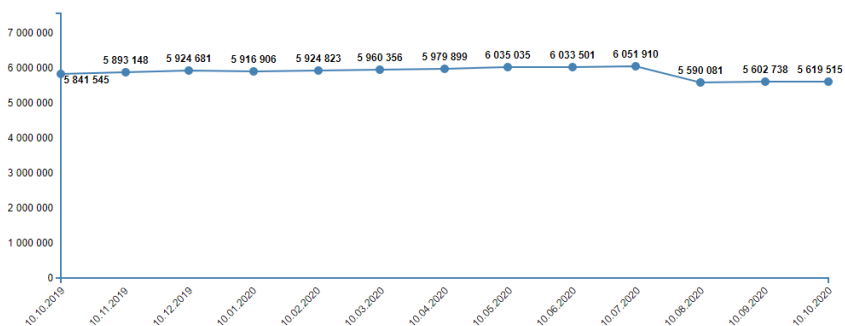


Рисунок 1 – «График динамики количества субъектов малого и среднего предпринимательства в период с 10.10.2019 по 10.10.2020»

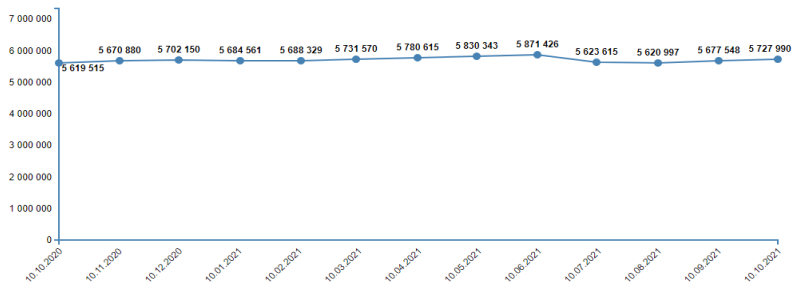


Рисунок 2 – «График динамики количества субъектов малого и среднего предпринимательства в период с 10.10.2020 по 10.10.2021»

Преимущество использования специальных налоговых режимов состоит в том, что организации освобождаются от уплаты ряда налогов, таких как НДС, налог на прибыль организации, налог на имущество организации. ИП освобождаются от уплаты НДФЛ (включаются только доходы, полученные от предпринимательской деятельности), налог на имущество физических лиц, если это имущество задействовано в предпринимательской деятельности и НДС. Также к преимуществам УСН относится упрощенный порядок ведения учета, подачи декларации и расчета налога. Теперь проанализируем более подробно специальные налоговые режимы.

Специальные налоговые режимы — это режимы налогообложения, предоставляющие возможность субъектам бизнеса упростить отчетность и

документооборот, за счет уплаты в сущности одного налога. Ставки и порядок уплаты, условия применения обозначены в НК РФ, а также в других федеральных и местных законах.

Законодательство предусматривает, что изначально индивидуальный предприниматель или организация при прохождении регистрации в ФНС руководствуется общей системой налогообложения (ОСН или ОСНО). ОСН подразумевает под собой внушительный перечень отчетности и наибольшую налоговую нагрузку. Для того, чтобы совершить переход на специальный режим налогообложения, субъекту бизнеса потребуется по месту регистрации оформить заявление в инспекцию Федеральной налоговой службы. Заявление можно подать сразу после прохождения регистрации, в альтернативном случае до 31 декабря и только раз в год.

Специальный режим — это режим налогообложения, который предусматривает особую методику подсчета и формирования налога за конкретный срок; это льготы распространяющиеся на субъекты малого предпринимательства, потому как данный налоговый режим освобождает от уплаты некоторых общеобязательных платежей.

В сущности все они обязуют налогоплательщика уплачивать только один обязательный платеж, что, конечно же, заметно облегчает предпринимателям и организациям задачу ведения документооборота и отчетности. В частности, субъекты предпринимательства ценят возможность неуплаты налога по НДС, потому как данный налоговый сбор, осуществляемый в пользу государства, довольно сложен в реализации и расчете.

Правила перехода на специальный режим налогообложения, а также порядок их использования обозначены в пункте 7 статьи 12 Налогового кодекса Российской Федерации [2]. Налогоплательщик добровольно решает стоит ли ему переходить на специальный режим или остаться на общем.

В 2021 году были внесены правки в перечень специальных налоговых режимов, которые постановили главу 26.3 НК РФ [2], регламентирующую правила применения единого налога на вменённый доход, как утратившую силу. Вследствие чего, начиная с 2021 года, специальный режим в формате ЕНВД в пользовании недопустим.

Таким образом, перечень специальных налоговых режимов в Российской Федерации включает:

- для сельхозпроизводителей (ЕСХН);
- упрощенная (УСН);
- соглашений о разделе продукции (СРП);
- патентная (ПСН).

Таблица 2 – «Принципиальные особенности спец. режимов»

Показатель	ЕСХН	УСН	ПСН	СРП
Глава НК РФ, регулирующая применение	26.1	26.2	26.5	26.4
Кто применяет	Организации и ИП		ИП	Организации
Для какой деятельности возможно применение	Сельское хозяйство и рыболовство	Все, за исключением приведенной в п. 3 ст. 346.12 НК РФ	Только для указанной в п. 2 ст. 346.43 НК РФ	Поиск, разведка и добыча минерального сырья
Необходимость специального разрешения	—		Патент	Соглашение о разделе продукции
Размер выручки, млн руб.	—	До 150 с корректировкой на коэффициент-дефлятор для соответствующего года (применение коэффициента приостановлено на период 2017-2019 годов)	До 60 (а для расчета стоимости патента – до 1 с корректировкой на коэффициент-дефлятор для соответствующего года)	—
Численность работников, чел.	До 300 — для рыболовецких хозяйств	До 100	До 15	—
Остаточная стоимость ОС, млн руб.	—	До 100	—	
Участие других юрлиц в УК организаций, %	—	До 25	—	

Аналитическое исследование федеральной службы государственной статистики «Росстат» постановило, что на территории Российской Федерации проживает более 74,5 млн. чел. трудоспособного населения. Однако большая часть (10,9-15 млн. человек) из представленной оценки не являются официально трудоустроенными и получают теневой доход.

Бюджет страны пополнится примерно на 40 млрд. руб. налогов, если предположить, что половина самозанятых работников будут уплачивать налог на прибыль.

Поэтому с учетом данной проблемы был разработан обязательный, индивидуально безвозмездный платёж, регулирующий деятельность самозанятых граждан - налог на профессиональный доход (НПД). Ставка налога не является единой и зависит от рода деятельности самозанятого: оказание услуг людям – 4 %, компаниям – 6%. Также существует лимит на уровень годового дохода, он не может быть выше 2,4 млн. руб. По словам заместителя мэра Москвы Владимира Ефимова, только за первое полугодие 2020 года рост самозанятых в городе Москве составил 70%, на 324 000 человек. [5]

Новый налоговый режим для самозанятых имеет выгоды с каждой стороны налогообложения: граждане, работающие на себя, стали частью законной предпринимательской среды в России; регионы получили дополнительное бюджетирование, что способствует формированию устойчивого развития, улучшению инфраструктуры, повышению качества жизни населения.

Главным преимуществом НПД является то, что налогоплательщик обязан уплачивать платёж лишь при условии получения дохода, что выгодно отличает данный режим от ранее существующих принципов налогообложения. Если самозанятый гражданин не получает доход, он не уплачивает налог. Поэтому в период пандемии коронавирусной инфекции, самоизоляции, сложной экономической ситуации для малого бизнеса, были зафиксированы случаи перехода из ИП на НПД, потому как малое предпринимательство не имело возможности уплачивать платеж.

К сожалению, с развитием и популяризацией нового налогового режима, появились угрозы для бюджетирования регионов, так как некоторые предприниматели, нежелающие уплачивать за своих сотрудников 13 % подоходного налога и 30 % взносов во внебюджетные фонды, стали переводить работников на налоговый режим для самозанятых. Сейчас данным вопросом занимается Федеральная налоговая служба, отслеживая деятельность предпринимательств.

Новый налоговый режим имеет главную цель - агрегаторы, сервисы такие как Profi.ru, Яндекс и так далее, которые предоставляют площадку для продвижения своих услуг и заработка гражданам, работающим на себя. Через выстраивание качественных отношений нужно прийти к тому, чтобы все самозанятые, пользующиеся такого рода площадками, стали уплачивать налог как официально зарегистрированные работники с помощью налогового режима НПД.

Благодаря сотрудничеству ФНС с агрегаторами получилось привлечь значительное число самозанятых к законному предпринимательству, а более 30% граждан, работающих на себя, стали налогоплательщиками из-за пользования цифровыми платформами, которые освещают данный вопрос.

Налоговые системы различных стран стремительно развиваются, исходя из этого можно выделить три мировых тренда, к которым стремятся налоговые органы государств. Важно отметить, что РФ совместно с ФНС не только следует этим трендам, но и активно задает их. Многие технические решения ФНС РФ не имеют мировых аналогов. Теперь более подробно про эти тенденции. Во-первых, прозрачность, которая заключается в том, что налоговый орган должен владеть максимально возможной информацией о налогоплательщике и беспокоить его в редких случаях. Во-вторых, ориентированность на партнерские отношения. Идея заключается в том, что налоговая стремится выполнять роль сервиса, который будет удобен и прост для использования. С помощью машинного обучения и нейросети планируется создать голосового помощника, оказывающего консультационную услугу для налогоплательщика. Идеальный вариант осуществления партнерских отношений состоит в том, что налогоплательщик заходит в приложение, проверяет корректность данных и соглашается с суммой начисленного налога, а функцию по составлению и расчету всех обязательных платежей полностью возьмет на себя налоговый орган. Третий тренд дополняет предыдущие два и называется – цифровизация. Общая тенденция – сделать экономику цифровой, а уплата налога должна восприниматься как особая культура, которая будет простой, удобной и неизбежной.

С помощью такой адаптивной системы налогового администрирования, технологий, встроенных в жизнь бизнеса и человека, планируется также сократить теневой сектор экономики. Предприятия малого и среднего бизнеса, скрывающие свои доходы от государства и налоговых органов негативно влияют на всю экономику страны, в частности на конкурентную бизнес- среду. Однако тенденция сокрытия доходов начинает уменьшаться. В современных условиях целесообразнее честно вести бизнес, чем скрывать доходы от налоговой службы и нарушать законодательство. Более того, в РФ создается осознанная культура уплаты налогов и в ближайшем будущем произойдут существенные изменения. В любом случае РФ плавно трансформировала бы налоговую систему, но ситуация с COVID-19, из-за которой произошел перевод на дистанционные форматы всей экономики, существенно ускорила процесс развития системы. Уже сегодня налогоплательщик может лично убедиться, насколько удобным стало использование официального сайта ФНС РФ, быстро, удобно, не

нужно тратить огромное количество времени на личное посещение налоговых органов и сбор документов. Резюмируя вышесказанное, ФНС РФ хочет максимально «упростить жизнь» малого и среднего бизнеса, предоставляя большую возможность предпринимателям заниматься операционной деятельностью. От налогоплательщиков требуется исполнять свои обязанности перед государством и предоставлять объективную информацию налоговым органам.

Таким образом, подводя итог всему вышесказанному, можно сделать вывод, что в условиях современной экономики, во времена пандемии COVID-19, от которой до сих пор не оправилась ни одна экономика мира, странам необходимо поддерживать малый и средний бизнес. Конкурентная среда в этих отраслях способна держать на плаву всю государственную экономику. Благодаря стремительному развитию ФНС, которая является самым цифровым ведомством РФ, трансформации многих процессов, грамотной налоговой политики, предоставляющей множество возможностей и льгот предпринимательству, у компаний открываются новые перспективы для восстановления и развития.

Список использованных источников:

1. Налоговый кодекс Российской Федерации (НК РФ). Часть первая от 31.07.1998 года № 146-ФЗ // Официальный интернет-портал правовой информации. - 18.11.2021 г. - с изм. и допол. в ред. от 02.07.2021 года № 309-ФЗ.
2. Налоговый кодекс Российской Федерации (НК РФ). Часть вторая от 05.08.2000 № 117-ФЗ // Официальный интернет-портал правовой информации. - 18.11.2021 г. - с изм. и допол. в ред. от 02.07.2021 года N 309-ФЗ.
3. Бренделева Е.А., Столбов М.И. Основы цифровой экономики : учебное пособие. - М.: Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации, 2018. - 238 с.
4. Официальный сайт Федеральной налоговой службы [Электронный ресурс]. – Режим доступа: <https://ofd.nalog.ru/statistics.html>. – Дата доступа: 18.11.2021.
5. Официальный сайт мэра Москвы [Электронный ресурс]. – Режим доступа: <https://www.mos.ru/news/item/77740073/>. – Дата доступа: 18.11.2021.

Влияние цифровых национальных валют на банковский сектор

В.А. Романовский

студент 4 курса НИЯУ МИФИ, Москва

E-mail: romanovsky01@mail.ru

А.В. Трушко

студентка 4 курса НИЯУ МИФИ, Москва

E-mail: annatrushkoo@mail.ru

Н.В. Морозов

к.ю.н., доцент кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: nvmorozov@mephi.ru

Аннотация: Данная работа нацелена на изучение цифровых валют центральных банков в качестве новой формы денежных средств. Задача авторов - рассмотреть не только ключевые позиции внедрения новой технологии, а также интерпретировать возможные экономические последствия, которые могут возникнуть для банковского сектора в целом. Объектом исследования был выбран цифровой рубль.

Ключевые слова: цифровая валюта, центральный банк, платежная система, транзакции, E-CNY, фондирование, ставка рефинансирования.

Impact of digital national currencies on the banking sector

Abstract: This work is aimed at studying digital currencies of central banks as a new form of money. The task of the authors is to consider not only the key positions of the introduction of new technology, but also to interpret the possible economic consequences that may arise for the banking sector as a whole. The object of the study was the digital ruble.

Keywords: digital currency, central bank, payment system, transactions, E-CNY, funding, refinancing rate.

Введение

В последнее время большая часть мирового сообщества стремится к цифровизации своих национальных экономик, данная тенденция сопровождается кардинальными изменениями в финансово-технологическом пространстве. Наиболее перспективным направлением технологии распределенных реестров (distributed ledger technology — DLT)

выступает цифровая валюта центральных банков (ЦБ). Несмотря на популяризацию внедрения цифровых национальных валют, общепризнанного определения цифровой валюты, выпускаемой центральным банком (central bank digital currency — CBDC), в настоящее время нет. Данное понятие несет в себе электронное обязательство ЦБ, выраженное в национальной единице (1:1), которое выступает в роли новой формы денежных средств. Наравне с безналичными и наличными средствами, цифровая валюта выполняет основополагающие функции денег: средства обращения (платежа), меры стоимости и средства сбережения.

Опираясь на данные отчета McKinsey о глобальных платежах за 2020 год [2], можно констатировать характерное снижение транзакций, осуществляемых за наличную плату (Рисунок №1).

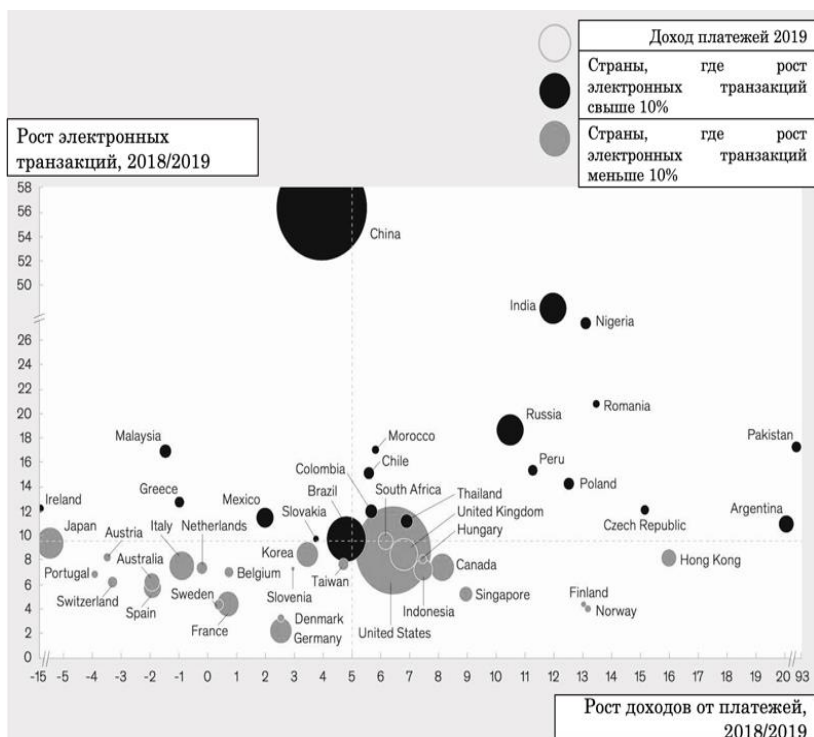


Рисунок 1 – Перераспределение электронных транзакций, 2018/2019

Очевидно, что при внедрении цифровых валют распределение потоков наличных и безналичных транзакций существенно изменится, однако на данный момент не представляется возможным дать количественную оценку таких изменений. Таким образом, учитывая мировой финансово-технологический прогресс, рост использования различных платежных систем и цифровизацию национальных экономик, можно с уверенностью сказать, что транзакции, осуществляемые за счет цифровой валюты ЦБ всего мира, замедлят как рост безналичных расчетов, так и сокращение платежей наличными денежными средствами.

Учитывая актуальность разработки и внедрения цифровых валют на сегодняшний день, необходимо точно понимать какие преимущества несет в себе данный шаг для разных сфер деятельности государств, как будет работать механизм, какие потенциальные проблемы и угрозы могут возникнуть и, соответственно, как сделать внедрение CBDCs наиболее эффективным и перспективным. В данной работе с этой целью авторами проведен анализ пилотного проекта КНР цифрового юаня, не имеющего пока аналогов в мире: рассмотрена система функционирования, основные результаты за существующий период и оказанный экономический эффект. Также рассмотрен проект пилотного запуска цифрового рубля и дан прогноз на дальнейшее развитие ситуации в Российской Федерации. Отметим, что особенное внимание было уделено последствиям введения цифровых валют на коммерческие банки.

Цифровой юань

Вопрос создания собственных цифровых национальных валют характерен не только для государств с развитой экономической системой — на данный момент около 80 стран заявили о подобных намерениях. Анализируя техническую, правовую, а также экономическую готовность, дальше всех в создании цифровой валюты (ЦВ) продвинулась Китайская Народная Республика, Швеция и Российская Федерация. На данный момент Китай запустил несколько пилотных проектов в десяти регионах страны, а также обозначил намерение использовать цифровой юань (E-CNY) во время зимних Олимпийских игр в Пекине [1]. По оценкам китайских коллег общий объем цифровой валюты может достичь 1 триллиона юаней (11,5 триллионов российских рублей) в ближайшие годы, что в свою очередь эквивалентно конвертации в цифровую валюту одной восьмой наличной денежной массы Китая.

На данном этапе Китайская модель CBDC выглядит следующим образом (Рисунок №2): Центральный банк Китая утвердил двухуровневую модель цифровой валюты.

1	<u>Народный банк Китая</u>	Эмиссия цифровой валюты (E-CNY)
2	<u>Финансовые организации (6 крупных банков и 2 онлайн банка)</u>	Открытие электронных кошельков потребителям
3	<u>Юридические и физические лица</u>	Услуги оказываемые в цифровой валюте (E-CNY)
4	<u>Другие банки, провайдеры платёжных систем</u>	Использование цифрового юаня потребителями

Рисунок 2 – Модель внедрения цифрового юаня

Однако в данной системе, с точки зрения пользователей электронного юаня, уровней больше, чем два. Центральный банк Китая занимает первый уровень данной модели в качестве регулятора цифровой валюты. Для создания электронного кошелька пользователю необходимо обратиться в одно из учреждений второго уровня системы. К учреждениям второго уровня на данный момент относятся 6 крупнейших государственных банков и два интернет-банка (WeBank и MYBank). На следующем этапе у пользователей электронных кошельков E-CNY появляется возможность осуществлять платежи через посредников в лице других банков, а также различных платёжных систем. В результате базисом модели выступает уровень пользователей цифрового юаня (физические и юридические лица).

E-CNY может оказать глубокое влияние на бизнес, спектр услуг и деловую практику в коммерции, связанной с Китаем. Если китайская практика и стандарты CBDC повлияют на международную практику (например, путем разработки стандартов), то в долгосрочной перспективе они могут повлиять и на другие предприятия. В краткосрочной перспективе CBDC, скорее всего, затронет широкий круг международных предприятий, особенно тех, которые присутствуют в Китае, или тех, кто обычно совершает сделки с китайскими субъектами. Статус законного платежного средства электронного китайского юаня означает, что прием электронного китайского юаня в конечном итоге станет обязательным в Китае.

Рассмотрим влияние на банки и платежную систему третьих сторон: в этом вопросе все будет зависеть от скорости внедрения DC/EP, равно как и операционной модели между DC/EP и этими игроками. Естественно, между банками Китая может возникнуть конкуренция касательно депозитов, однако также надо учитывать и потенциальные возможности, которые принесет данный шаг: к примеру, банки могут получать плату от своих клиентов за хранение их цифровых кошельков. Также, учитывая, что банки выступают посредниками цифрового юаня, как уже упоминалось ранее, — это создает дополнительные преимущества по привлечению клиентов. В тоже время, для повышения качества своих платформ, сторонние платежные системы должны повысить качество обслуживания клиентов на своих цифровых кошельках [3].

При этом банки, могут столкнуться с различными проблемами, включая:

- взаимодействие между e-CNY и банковскими счетами, и услугами мобильных платежей;
- возможные трансграничные платежи физических и юридических лиц с использованием электронного кошелька;
- вопросы связанные с комплаенсом (например, контроль за отмыванием денег и финансированием терроризма, защита потребителей и раскрытие информации, конфиденциальность данных, лицензирование и пруденциальное поведение, совместимость с другими валютами и системами);
- управление денежными средствами и валютные стратегии.

Цифровой рубль

Российская модель цифрового рубля достаточно схожа с моделью КНР. После рассмотрения четырех вариантов создания системы цифровой валюты РФ, центральный банк принял решение утвердить розничную двухуровневую модель с ролью финансовых организаций в качестве участников расчетных операций. ЦБ РФ, как и другие участники данного проекта, считает, что данная модель имеет максимальную доступность цифровой валюты как для бизнеса, так и для всех граждан в целом. При использовании такой модели можно будет значительно сократить издержки в экономике за счет оптимизации стоимости расчетов, а также появится возможность расширения инфраструктуры финансовых организаций с целью взаимодействия с клиентами. Модель цифрового рубля работает следующим образом [Рисунок №3]:



Рисунок 3 – Модель внедрения цифрового рубля

На первом уровне. Цифровой рубль будет представлен в виде уникального кода (токена) и будет находиться на электронных кошельках клиентов на платформе цифрового рубля. Создание такой платформы запланировано на декабрь текущего года. Центральный банк РФ в свою очередь, как регулятор сопровождает функционирование данной платформы и занимается ее развитием. Также требуется отметить, что ЦБ РФ подключает к данной платформе финансовые организации и Федеральное казначейство как специального участника пилотных проектов. В качестве оператора ЦБ разрабатывает правила осуществления операций и утверждает внутренние стандарты взаимодействия. Если рассматривать ЦБ РФ как эмитента, можно выделить еще несколько обязанностей: эмиссия цифровых рублей, зачисление и списание цифровой валюты для финансовых организаций и Федерального казначейства, а также открытие для них электронных кошельков на цифровой платформе.

На втором уровне. В компетенции финансовых организаций входит открытие и пополнение кошельков физическим и юридическим лицам на платформе цифрового рубля. Помимо этого, банки продолжают осуществление процедур, предусмотренных законодательством в сфере ПОД/ФТ/ФРОМУ и валютным законодательством. Непосредственно финансовые организации будут осуществлять переводы и платежи по поручению клиентов на платформе цифрового рубля. Роль Федерального казначейства на данном уровне состоит в проведении операций с кошелька Федерального казначейства в счет обеспечения деятельности бюджетных организаций.

Не исключено, что после положительного проведения пилотных проектов, ЦБ РФ привлечет к тестированию цифрового рубля организации, осуществляющие сервисы платежных систем.

По результатам опроса ЦБ РФ большинство респондентов положительно отреагировали на внедрение собственной национальной цифровой валюты. На данный момент положительными факторами использования такой технологии выступают [4]:

- повышение доступности безналичных платежей;
- уменьшение стоимости, ускорение и упрощение проведения транзакций;
- повышение конкуренции на финансовом рынке;
- гарантируемая Банком России сохранность средств;
- возможность совершения расчетов в онлайн и офлайн режимах, независимо от операционного дня Банка России и кредитных организаций;
- возможность интеграции с другими цифровыми платформами;
- упрощение проведения государственных платежей.

Изменения в банковском секторе

Несмотря на перспективность и значимость такой технологии, возникают некоторые вопросы перераспределения ликвидных активов банков, а также изменения кредитно-денежной политики банковского сектора в целом. Одним из возможных видов экономических перераспределений в банковском секторе выступает снижение чистой прибыли банков. В большей степени, чистая прибыль (ROE) формируется у банков за счет высоколиквидных активов, таких, например, как зарплатные карточки и текущие расчетные счета банка. Данные средства не приносят никакого дохода клиентам или же объемы процентного остатка по счетам сводятся к нулю. Банки, зная, что суммы устойчивых остатков таких высоколиквидных денег можно разместить на счетах ЦБ РФ или же вложить в другие низкорискованные активы, приносящие доход банку с минимальными рисками ликвидности, наравне с кредитованием, используют данную возможность для легкого заработка. Учитывая масштабы деятельности крупных банков, такой источник дохода играет важную роль в формировании чистой прибыли. В последнее время банки уже ощущают конкуренцию за высоколиквидные пассивы частного нефинансового сектора с учетом многообразия услуг провайдеров платежных систем. Поэтому внедрения цифрового рубля сподвигнет банки задуматься о полномасштабном изменении стратегий работы с высоколиквидными денежными средствами. С одной стороны, часть населения нефинансового сектора получит определённую долю процентного дохода из-за хранения денежных средств в цифровой валюте на электронных кошельках, однако, в данном вопросе есть другая сторона

монеты. Банки будут вынуждены поднять ставки по остаткам на зарплатных, расчетных, а также текущих счетах, дабы избежать перетока высоколиквидных пассивов в цифровой рубль. Есть точка зрения, что сокращение процентных доходов на стороне пассивов банков вынудит их компенсировать выпадающие доходы принятием большего риска в кредитовании (risk-taking). Как следствие, указывается, что могут вырасти риски финансовой стабильности.

Опираясь на основную функцию использования цифровой валюты, клиенты банков будут взаимодействовать с цифровым рублём как с альтернативой наличным денежным средствам. В таких условиях может возникнуть дефицит фондирования, конечно, ЦБ РФ будет следить за объемами оттока ликвидности. Но чтобы предоставить банкам нужную сумму средств для контроля процентных денежных ставок, ЦБ РФ должен проработать несколько вариантов процедур управления ликвидностью, особенно в предкризисных обстоятельствах. Для снижения влияния цифровой валюты на ликвидность банкам следует: сокращать объем депозитов в Банке России, поднять ставки, вплоть до уровня рыночных ставок по высоколиквидным пассивам, тем самым сдержав их переток в цифровой рубль, поднять ставки по срочным депозитам.

Насколько вырастут ставки кредитования из-за внедрения цифрового рубля на данный момент спрогнозировать тяжело. Несмотря на это, можно с уверенностью сказать, что цифровой рубль не усугубит рост кредитования из-за природы установления ставки по кредиту. Банк сравнивает процент, который получит по кредиту с альтернативным доходом, который может получить вместо выдачи кредита (найти другое применение деньгам). Минимальный альтернативный доход в нормальной ситуации на рынке представлен безрисковой рыночной доходностью соответствующей кредиту срочности. Как правило, это уровень доходности ОФЗ соответствующей срочности.

Итак, переток депозитов в цифровые рубли скажется главным образом на депозитных ставках банков. При этом может возрасти стоимость банковских услуг, так как банки переложат часть потерянных доходов на комиссии, в том числе, возможно, за обслуживание банковских счетов. В таком случае на первый план выйдет задача поддержания достаточной конкуренции в банковском секторе, чтобы стимулировать повышение банками эффективности своей деятельности и снижение расходов. Важно отметить, что даже без введения цифрового рубля банки столкнутся с этой необходимостью из-за растущей конкуренции с финтех-компаниями.

Заключение

Проанализировав модели планируемых систем и рассмотрев их основные составляющие, можно сделать обоснованный вывод о том, что

введение цифровых национальных валют не может не повлиять на банковский сектор государства. Существует мнение о том, что CBDCs более привлекательны, чем депозиты, и могут привести к финансовой дезинтермедиации, “сужению” банковского сектора и кредитному сжатию, в то время как другие утверждают, что легкая доступность CBDCs может повысить ставки рефинансирования на денежно-кредитных рынках. Если цифровые валюты будут представлять интерес на относительно привлекательном уровне, институциональные инвесторы могут перейти от активов с низким уровнем риска, таких как краткосрочные государственные ценные бумаги, к CBDCs, что окажет влияние на цену этих активов. Однако потенциальное воздействие на денежно-кредитную политику будет смягчено если по CBDCs вообще не будут начисляться проценты, снижая таким образом риск конкуренции их с безрисковыми активами, такими как депозиты коммерческих банков. Поэтому при их разработке центральные банки должны принимать во внимание формулирование и реализацию денежно-кредитной политики.

Список использованных источников:

1. Progress of Research & Development of E-CNY in China, People's Bank of China - July, 2021;
2. Global Banking Practice - The 2020 McKinsey Global Payments Report – October, 2020;
3. May В.А. Национальные цели и модель экономического роста: новое в социально-экономической политике России в 2018–2019 гг. Вопросы экономики. 2019;
4. Киселев А. Есть ли будущее у цифровых валют центральных банков: Аналитическая записка. М.: Банк России; 2019.

Влияние ESG рисков на деятельность финансового сектора

А.В. Горюнова

студент 4 курса ГТУ МАДИ, Москва

E-mail: goryunova.nastya@yandex.ru

В.С. Царева

студенты 4 курса ГТУ МАДИ, Москва

E-mail: veratsaryova@mail.ru

В.И. Прусова

к.э.н., доцент кафедры финансов ГТУ МАДИ, Москва

E-mail: loveprus@gmail.com

Аннотация: Данная статья посвящена влиянию ESG рисков на деятельность финансового сектора. Авторы отмечают, что произошло смещение фокуса с концепции устойчивого развития от национального уровня к корпоративному, а также больше инициатив по поводу ESG исходит от организаций. В этой связи финансовый сектор не остается в стороне, он активно финансирует ESG направление.

Ключевые слова: ESG, финансовый сектор, банки, «зеленые» облигации, кредитный рейтинг.

The impact of ESG risks on the activities of the financial sector

Abstract: This article contains information about the impact of ESG risks on the activities of the financial sector. The authors note that the focus has shifted from the idea that the development can be sustained from the national to the corporate level, and more initiatives about ESG come from organizations. In this regard, the financial sector does not stand aside, it actively finances the ESG direction.

Keywords: ESG, financial sector, banks, «green» bonds, credit rating.

ESG (англ. Environmental, social and corporate governance), что можно перевести, как экологическое, социальное и корпоративное управление. Это совокупность характеристик управления компаниями, когда достигается максимальное вовлечение в решение экологических, социальных и управленческих проблем. Риски ESG появились не два не пять лет назад, когда о них только начали говорить, а достаточно давно. Они определяются зависимостью бизнеса от среды, в которой он существует – это

потребление ресурсов, воздействие на окружающую среду, люди (работники, клиенты), изменение цепочек поставок и т.д.

Из-за широкого обсуждения за последние два года, ESG стало мировым трендом, и находит все больший отклик в России. Меняются запросы инвесторов, клиентов, общества, трансформация бизнес-моделей российских банков, все становится более ориентированным на принципы ESG, что является дифференцирующим фактором для банков в России. Перспективность этого подхода оценивается в повышении лояльности со стороны клиентов и сотрудников, в привлечении новых инвесторов и деловых партнеров, а также минимизации рисков и разработки стратегий новых возможностей.

На сегодняшний день произошла трансформация фокуса с концепции устойчивого развития от национального уровня к корпоративному. Предлагается все больше инициатив от организаций по применению адаптаций в мировой практике, которые будут учитывать влияние социальных, экологических и корпоративных действий компаний. Необходимо, чтобы развитие соответствовало не только потребностям настоящего времени, но и не ставило под угрозу потребности будущих поколений.

1987 г. начало преобразований. Докладом Всемирной комиссии ООН по окружающей среде и развитию «Наше общее будущее» [1], была представлена концепция устойчивого развития – экономический рост, не нанося вред окружающей среде, находит баланс между экономическим, социальным и экологическим развитием.

COVID – 19 не только затормозил развитие рынков, но также обратил внимание на важность экологических проектов, сфер здравоохранения и образования. В 2020 году на Всемирном экономическом форуме, главными стали риски, которые связаны с изменением климата [2].

В 2021 году была создана Net Zero Banking Alliance – ассоциация финансового сектора, которая объединяет банки по всему миру, представляющие более 40% глобальных банковских активов, которые стремятся к 2050 году обеспечить своим кредитным и инвестиционным портфелям нулевые выбросы. Ассоциация будет продвигать и поддерживать стратегии декарбонизации, предоставляя такую структуру, которая будет согласована на международном уровне, а руководящие принципы для работы будут опираться на коллегиальное обучение банков. Альянс признает жизненно важную роль банков в поддержке глобального перехода реальной экономики к нулевым выбросам [3].

Последняя статистика членства			
95	39	66 трлн.\$	95
Банки	Страны	Активы	Глобальные банковские активы

Рисунок 1 – Статистика Net Zero Banking Alliance
 Источник: UNEP FI 11.2021 www.unepfi.org/net-zero-banking/members/

Говоря о зарубежном опыте, стоит отметить, что компании начали намного больше финансировать в направлении ESG и разрабатывать новые продукты, которые позволят интегрировать такие решения в политику организации.

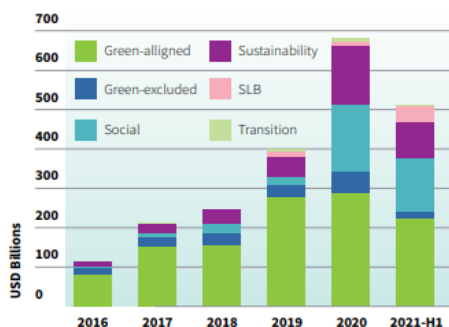


Рисунок 2 – Рынок заимствований ESG
 Источник: Climate Bonds Initiative - Sustainable Debt Market Summary H1 2021 [4]

Зеленые облигации	Зеленые кредиты	Социальные облигации	Облигации УР	Оrientированные облигации УР	Оrientированные кредиты УР

Общие объемы зеленых, социальных и устойчивых облигаций, облигаций, привязанных к устойчивому развитию (SLB), достигли почти половины триллиона (496,1 млрд долларов США) в первой половине 2021 года. Эта сумма составляет 59% по сравнению с предыдущим годом.

Эти тенденции подтверждают, что финансирование переходного периода набирает обороты, однако существующий переход еще не осуществляется в достаточных масштабах, которые удовлетворяли бы целям Парижского соглашения [5].

Увеличение международных активов, направленных на реализацию стратегий устойчивого инвестирования по прогнозам достигнет 140,5 трлн.\$ США к 2025 году [6].

В России компании добывающей промышленности, считаются самыми активными в системном учете ESG факторов, в силу их непосредственного воздействия на данные факторы, а также находясь под влиянием инвесторов и деловых партнеров.

«В мире уже сформировалась тенденция финансирования «зеленых» проектов. Поэтому сейчас правительство, ЦБ и институты развития находятся на стадии активной разработки <...> Сектор устойчивого развития существует на Московской бирже и состоит из трех самостоятельных субъектов, а именно, «зеленых» облигаций, социальных облигаций и национальных проектов.» - об этом рассказал министр экономического развития России Решетников Максим Геннадьевич 7 апреля 2021 года, на Биржевом форуме.

Финансовые институты активно внедряют учет ESG принципов для лучшего управления рисками и получения стратегических преимуществ. На сегодняшний день правовая база в этой области только начала свое формирование, но инициативы предлагаются.

В 2016 году Россия подписала Парижское соглашение [5] по изменению климата, под которым подразумевается уменьшение содержания углекислого газа в атмосфере с 2020 года. Страны-участники определяют свои вклады в достижение общей цели в индивидуальном порядке и пересматривают их каждые пять лет. Россия предусматривает снижение парниковых газов на 70% от 1990 до 2030 года.

В 2018 году был издан Указ № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» [7], который включает в себя Национальный проект «Экология». Проект содержит множество целей: ликвидация нелегальных свалок, снижение выбросов в наиболее загрязненных городах, восстановление лесов, повышение качества питьевой воды и т.д.

В 2020 году были запущены первые торги российского биржевого паевого инвестиционного фонда «РСЧБ Управление Активами» [8]. Также была сформирована межведомственная рабочая группа, в которую вошли: Минприроды, Минтранс, Минфин, Банк России и пр. Создан экспертный совет по устойчивому развитию, в который входит 30 компаний как российских, так и зарубежных. Представителями банковского сектора являются ПАО Сбербанк и ПАО РОСБАНК.

«Спрос на ESG инструменты финансирования достаточно высок и будет продолжать повышаться в ближайшем будущем. ESG банкинг и принцип устойчивого развития экономики – это не частный выбор отдельно взятого банка или реального сектора экономики. Это запрос общества и государства.» – сказал Заместитель Председателя Совета Федераций – Журавлев Николай в 2021 году.

В сентябре 2021 года Минэкономразвития России находится в ожидании подписания Правительством РФ таксономии «зеленых» финансов, которая может быть утверждена в течении месяца. Об этом сообщает заместитель министра экономического развития России Илья Торосов на панельной сессии в рамках XVIII Международного банковского форума «Банки России - XXI век» [9].

Хотя ESG банкинг существует только на начальных этапах своего развития в России, авторы видят значительный потенциал применения этой практики как с точки зрения всей российской экономики, так и с точки зрения развития банковского сектора. Стремительный рост внимания к ESG в России свидетельствует о том, что эта тенденция в банковском секторе соответствует вектору развития других секторов экономики. Имея примеры наилучшей практики регулирования и внедрения некоторых элементов ESG в банковский бизнес, российская экономика может воспользоваться преимуществами, используя ESG, как один из инструментов построения устойчивой, экологически чистой и диверсифицированной экономической модели.

Конечно же, формирование данной модели невозможно без активного участия финансовых институтов, а, следовательно, их добровольная включенность в работу над стратегией ESG и рисками.

Неоднородность распространения ESG в отраслях экономики, создает пространство для оптимизации их влияния на элементы экономики, окружающую среду и социальную сферу. Опираясь на опыт зарубежных банков, можно заметить значительный потенциал для развития ESG банкинга в России.

По оценке экспертов, объемы ESG активов в России к 2036 году могут достигнуть 360 трлн. Р. А объемы «зеленых» кредитов 1,3 трлн. Р к 2030 году [10].

Стоит отметить, что льготные условия, последовательный и комплексный подход для рынка в целом, повышение осведомленности всех экономических объектов о преимуществах практики устойчивого развития и стимулирование их интеграции в бизнес-модель, будут главными методами для создания ESG проектов финансовых институтов.

Управление устойчивым развитием, является сложной задачей для банка, требующей выделения и финансовых, и человеческих ресурсов. Важна вовлеченность всех сотрудников компании, а не отдельных групп. Повестка устойчивого развития должна быть включена в повседневную деятельность всех подразделений, в независимости от объемов организационных ресурсов в банке.

Активно ESG-трансформацией занимаются банки, входящие в топ-20, а остальные банки включатся в данный процесс в следующем году.

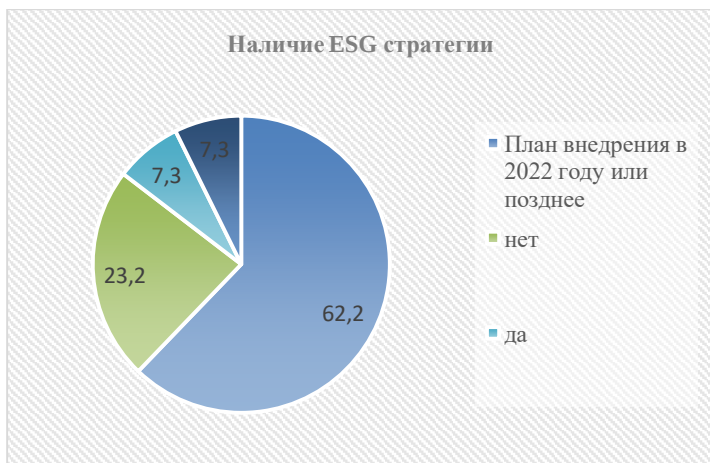


Рисунок 3 – Диаграмма наличия ESG стратегии

Источник: Эксперт РА – ESG-банкинг за 1-е полугодие 2021 года: Зеленая книга.
Глава 1

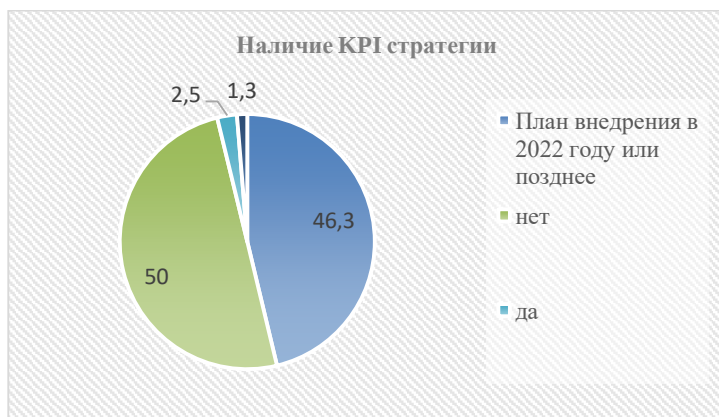


Рисунок 4 – Диаграмма наличия KPI стратегии

Источник: Эксперт РА – ESG-банкинг за 1-е полугодие 2021 года: Зеленая книга.
Глава 1

Утвержденные стратегии устойчивого развития либо экологические политики по итогам этого года будут внедрены у 15 % банков-респондентов, а 62 % опрошенных планируют внедрить их только к 2022-му году и позднее. В банках с KPI дела на устойчивые инвестиции обстоят хуже. По итогам 2021-го года стратегии будут внедрены только у 4 %

респондентов, 46 % банков видят их введение целью на последующие годы, а оставшаяся половина опрошенных вообще не рассматривает включение таких KPI в свои политики в настоящее время[11].

Исследования показывают, что банки, уделяющие внимание развитию существенных ESG категорий, показывают лучшие финансовые результаты в долгосрочном периоде.

Рейтинговые агентства всегда учитывали факторы ESG при формировании кредитного рейтинга, в связи с тенденцией, эти факторы стали выделять, как наиболее важные. ESG факторы за последнее время были существенным кредитным фактором в 33% рейтинговых действий для эмитентов частного сектора. Около 29% касались корпоративного управления, 6,6% социальных вопросов и 5,3% проблем окружающей среды. Экологические, социальные, политические и регуляторные факторы имеют долгосрочные последствия, поэтому и оказывают такое сильное влияние на кредитный рейтинг [12].

Таблица 1 – Факторы ESG, учитываемые международными и российскими агентствами при присвоении кредитного рейтинга

Экологические	Социальные	Корпоративные
-Загрязнение атмосферы, почвы, воздуха	-Условия труда и безопасности	-Организационная структура
-Регулирование углеродных выбросов	-Волонтерская и благотворительная деятельность	-Структура собственности
-Природные и техногенные угрозы	-Охрана труда и здоровья	-Менеджмент и корпоративное управление
-Ограничения землепользования	-Доступ к основным услугам	-Деловая репутация
-Климатические риски	-Уровень образования	- Стратегия развития
	-Соблюдение прав и свобод человека	

Источник: CFA INTEGRATION – ESG-ИНТЕГРАЦИЯ: рынки, методы и данные, 2019 [13]

Анализ опыта ESG в реальном и финансовом секторах среди компаний, показал, что банки в ближайшее время определяют повестку ESG в России. Таким образом, 80% компаний реального сектора не придают значения опыту ESG, а треть банков топ-20 включили в свои кредитные и инвестиционные процессы ключевые показатели эффективности для показателей ESG. К концу 2021 года доля таких кредитных организаций

достигнет 50%, что значительно ускорит процесс трансформации ESG. Реализуя бизнес-цели, связанные с показателями ESG, банки призывают заемщиков внедрять методы устойчивого развития, а также финансировать такие проекты.

Список использованных источников:

1. World Commission on Environment and Development. Our Common Future. Oxford: Oxford University Press, 1987.
2. Демидова О. Форум в Давосе назвал климатические катастрофы крупнейшим риском для мировой экономики [Электронный ресурс] // <https://p.dw.com/p/3WEc9>
3. Net Zero Banking Alliance [Электронный ресурс] // <https://www.unepfi.org/net-zero-banking>
4. Climate Bonds Initiative. Sustainable Debt Market Summary H1 2021 [Электронный ресурс] // https://www.climatebonds.net/files/reports/cbi_susdebtsum_h12021_02b.pdf
5. Парижское соглашение [Электронный ресурс] // <https://unfccc.int/ru/peregovorny-process-i-vstrechi/parizhskoe-soglashenie/chto-takoe-parizhskoe-soglashenie>
6. Iman Ghosh. Visualizing the Global Rise of Sustainable Investing [Электронный ресурс] // <https://www.visualcapitalist.com/rise-of-sustainable-investing/>
7. Указ Президента Российской Федерации от 07.05.2018 г. № 204 [Электронный ресурс] // <http://www.kremlin.ru/acts/bank/43027>
8. РСХБ и Мосбиржа запустили торги паями фонда российских корпоративных еврооблигаций стандарта ESG [Электронный ресурс] // <https://www.rshb.ru/news/453052/>
9. Илья Торосов: до конца 2021 года должна быть запущена национальная система зеленого финансирования [Электронный ресурс] // https://economy.gov.ru/material/news/ilya_torosov_do_konca_2021_goda_dolzha_byt_zapushchena_nacionalnaya_sistema_zelenogo_finansirovaniya.html
10. Sustainable Investing: Shaping the future of finance [Электронный ресурс] // <https://www.greengrowthknowledge.org/research/sustainable-investing-shaping-future-finance>
2. «Эксперт РА». ESG-банкинг за 1-е полугодие 2021 года: Зеленая книга. Глава 1 [Электронный ресурс] // https://raexpert.ru/researches/banks/esg_1h2021/
3. Moody's - ESG risks material in 85% of private-sector issuer rating actions in 2020 [Электронный ресурс] // <https://www.moody's.com/>

research/Moodys-ESG-risks-material-in-85-of-private-sector-issuer--
PBC_1292949

4. CFA INTEGRATION – ESG-ИНТЕГРАЦИЯ: рынки, методы и данные, 2019 [Электронный ресурс] // <https://www.unpri.org/download?ac=9522>

Внедрение риск-ориентированного подхода в кредитные организации

Н.В. Александров

студент 5 курса НИЯУ МИФИ, Москва

E-mail: u-n-1-k@yandex.ru

Д.А. Шульгин

студент 5 курса НИЯУ МИФИ, Москва

E-mail: shul-di@yandex.ru

Д.В. Домашова

к.э.н., доцент кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: janedom@mail.ru

Аннотация: В статье рассмотрена разработка стратегии выдачи займа с целью повышения устойчивости экономической безопасности микрокредитной организации. Основой для работы послужили реальные данные микрокредитной организации, клиенты которой были классифицированы с использованием кластерного анализа. Выявлены наиболее информативные признаки и разработана скоринговая модель на основе нечетких множеств.

Ключевые слова: кредитные организации, риск-ориентированный подход, скоринговая модель, кластерный анализ, нечеткие множества.

Integration of a risk-based approach to credit organizations

Abstract: The article considers the development of a loan issuance strategy in order to increase the stability of the economic security of a micro-credit organization. The basis for the work was the real data of a micro-credit organization, whose clients were classified using cluster analysis. The most informative features were identified and a scoring model based on fuzzy sets was developed.

Keywords: credit organizations, risk-based approach, scoring model, cluster analysis, fuzzy sets.

Введение

В настоящее время, в каждой стране мира имеется очень много финансовых, кредитных или не кредитных организаций. При выдаче кредитов существует определенный набор правил, которых та или иная

компания придерживается для принятия решения о выдаче или не выдаче средств потенциальному клиенту. За последние три года портфель МСП-займов вырос в 2,5 раза: наибольший прирост произошел в 2020 году – более 50% за год (в 2019 году – 37%, в 2018 – 23%). Динамика роста и актуальность займов в Микрофинансовых организациях (далее МФО) видна и на рисунке 1.

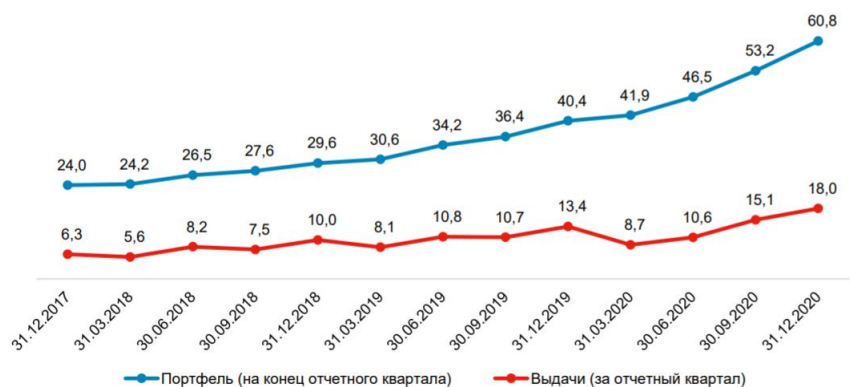


Рисунок 1 – Динамика объема выданных кредитов в МФО

Количество заемщиков в сегменте малого и среднего предпринимательства (далее – МСП) за три года увеличилось на 37% и на конец 2020 года составило 39 тыс. ед. – дополнительное финансирование позволило привлечь новых заемщиков (у большинства организаций более 50% заемщиков – новые). Очевидно, что вовлечено огромное количество людей в данные займы, это подтверждает рисунок 2.

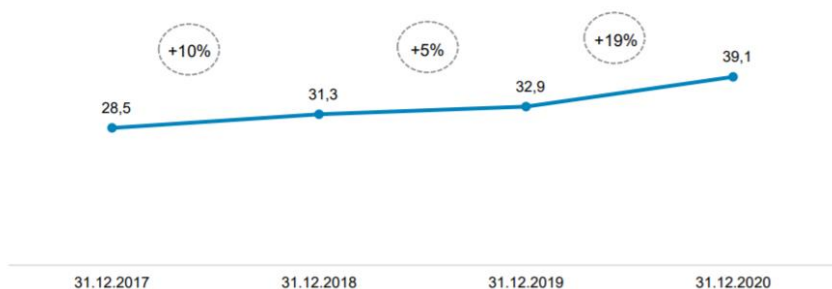


Рисунок 2 – Количество текущих заемщиков МФО в форме МСП, тыс.чел.

Согласно статье 5, Федерального закона от 07.08.2001 N 115-ФЗ, микрофинансовые организации являются субъектами первичного финансового мониторинга. Поэтому, крайне важно осуществлять риск-ориентированный подход. При выдаче слишком большого числа невозвратных средств, данная цель будет недостижима. Поэтому, зачастую, в крупных компаниях, используют какие-то системы или программы, которые помогают принять решение.

Спрос на услуги МФО значительно возрос за последнее время, также можно отметить динамичный рост выданных кредитов, однако вместе с этим и возросло количество просроченных займов. Это связано с отсутствием у микрокредитных компаний адекватной системы оценки риска кредитозаемщика.

Целью работы является: разработка стратегии выдачи займа с целью повышения устойчивости экономической безопасности микрокредитной организации.

Анализ нормативной базы регулирования деятельности МФО

Эксперты заявляют, что в виду повышающегося спроса на микрозаймы, ожидается прирост рынка не менее, чем на 30% по результатам 2021 года. Однако госреестр таких компаний ожидает сокращения до 1 тыс. организаций, что приведет к усилению концентрации крупнейших МФО.

Основные регуляторные меры и их различия для разных типов МФО представлены в таблице 1.

Таблица 1– Различия МКК и МФК

	МФК	МКК
Максимальный размер микрозайма физическому лицу	1 млн Р	500 тыс. Р
Максимальный размер микрозайма юридическому лицу и индивидуальному предпринимателю	5 млн Р	5 млн Р
Привлечение денег от физических лиц, не являющихся учредителями, участниками или акционерами	Разрешено на сумму не менее 1,5 млн Р	Запрещено
Привлечение средств юридических лиц и учредителей (участников, акционеров)	Разрешено без ограничений	Разрешено без ограничений
Размер собственных средств (капитала)	Не менее 70 млн Р	Не менее 2 млн Р
Выпуск облигаций	Разрешен	Запрещен
Резервы на возможные потери по займам	Обязаны формировать	Обязаны формировать
Производственная и торговая деятельность	Запрещена	Разрешена

Ежегодный аудит	Обязаны проводить и представлять в Банк России аудиторское заключение о годовой финансовой отчетности	Не обязаны предоставлять аудиторский отчет в Банк России
Членство в саморегулируемой организации (СРО)	Обязательное членство	Обязательное членство
Надзор со стороны Банка России	Постоянный надзор	Проводится, только если: 1) МКК временно не входит в СРО; 2) есть информация о том, что МКК, вероятно, нарушает законодательство; 3) Банк России проводит проверку СРО, в которую входит МКК.

МФО созданы для того, чтобы выдавать небольшие займы людям и предприятиям. Как правило, получить микрозаем проще, чем кредит в банке, хотя и процент по нему часто значительно выше.

Построение скоринговой модели для микрокредитной организации

Построение модели проводилось на основе реальных данных МКК. Выбранная организация привлекла на себя внимание выгодными продуктами и условиями получения займа. Она работает на рынке только полгода. Поэтому у нее не было полноценной бухгалтерской отчетности для того, чтобы в полной мере оценить экономическую безопасность организации.

Был проведен анализ процесса организации выдачи займа.

Когда клиент подает заявку на получение займа, специалист проводит проверку заявки на стоп-факторы, и в случае их обнаружения отказывает в выдаче кредита.

Обращается внимание на:

- возраст заемщика (клиент моложе или старше возраста, установленного МКК для пользования займом),
- отсутствие документа, подтверждающего доход,
- отсутствие справки с места жительства граждан
- текущие просрочки в других МФО и банках,

– действительность паспорта.

Были выявлены следующие недостатки на этапе проверки клиента:

Не вносится в базу данных досье клиента и информация с КБ, чтобы в дальнейшем ее можно было анализировать и не обращается внимание на кредитную нагрузку. Данный параметр был рассчитан нами самостоятельно, он показывает, насколько большую часть человеку придется выплачивать ежемесячно для погашения кредита от его текущей зарплаты.

При успешном прохождении проверки на стоп-факторы заключается договор и выдаются денежные средства.

Кредитный отдел осуществляет мониторинг выполнения условий договора и финансового состояния заёмщика, пока займ не будет полностью погашен: если условия нарушены, то проводится работа с проблемной задолженностью (пени, штраф, комиссия, пролонгация кредитного договора и т.д.).

Таким образом основной угрозой экономической безопасности для микрокредитной организации является риск невозврата, который зависит от того, как проработан процесс выдачи займа.

Далее, на рисунке 3 представлена схема проведения исследования для разработки скоринговой модели



Рисунок 3 – Схема проведения исследования

Первым шагом, стала предобработка данных, вызванная необходимостью структурировать имеющуюся информацию. Для этого было решено воспользоваться теорией нормальных форм, определить структуру хранения декомпозированных данных и сохранить их в локальной базе данных. Для начала были отобраны необходимые для анализа признаки и собраны в одной таблице. Итоговая база данных содержит таблицу информации о клиентах, таблицу продуктов и таблицу займов, ее схема представлена на рисунке 4.

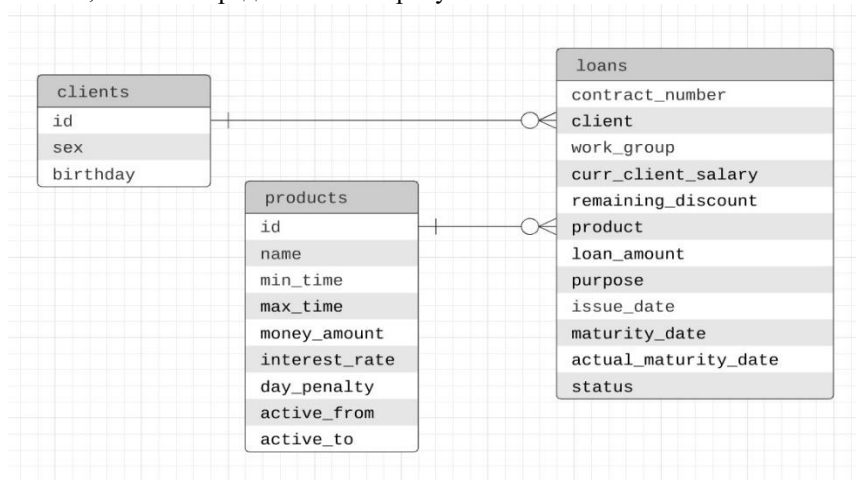


Рисунок 4 – Схема разработанной базы данных

Далее был проведен визуальный анализ, по его результатам, было выбрано признаковое пространство (Таблица 2).

Таблица 2 – Признаковое пространство

Поле	Пояснения
<i>sex</i>	Пол (м/ж)
<i>loan_amount</i>	Количество заемных средств (руб)
<i>time_limit</i>	Срок займа (дней)
<i>curr_client_salary</i>	Зарплата на момент выдачи (руб)
<i>age</i>	Возраст (лет)
<i>work_group</i>	Профессия

Данные признаки были выбраны из всех имеющихся на основании проведенных исследований, так как они обладают наибольшей ценностью, с точки зрения возможности описания потенциального клиента.

Для удобной работы, при обработке данных, были высчитаны возраст клиента и срок кредита по дате рождения и сроку открытия/закрытия соответственно. В дополнение, данные были очищены от пустых строк. По результату, было высчитано в качестве дополнительной информации общая сумма невозврата. Она составила 731266.8 рублей.

При формировании признакового пространства была введена категория профессиональной принадлежности заемщика, возраст заемщика и кредитная нагрузка. В частности, было выделено 20 профессиональных категорий, среди которых такие как, например, учитель, продавец, повар и др. А показатель кредитной нагрузки показывает, какую долю от среднемесячных доходов заемщика будет составлять ежемесячный платеж по займу.

Для последующей работы с данными они были стандартизованы, а также выполнено преобразование категориальных признаков. Были опробованы несколько методов для приведения к соответствующему виду, среди них:

- one hot encoder;
- label encoder, ordinal encoder;
- frequency encoder;
- mean encoder;
- weight of evidence encoder;
- probability ratio encoder.

В итоге был выбран метод *Mean Encoder*. В качестве целевой переменной выбрана невозвращенная сумма кредита.

Кроме того, для получения дополнительной информации, были рассчитаны случаи невозврата. Не вернуло: 590 из 826 человек. В то же время выборка является равномерной по гендерному составу, соотношение женщин и мужчин: 416 / 410.

При проведении кластерного анализа разными методами было выявлено, что графики средних к-средних и Уорда значений почти одинаковы, а DBSCAN имеет сильное отличие с ярко выделенным кластером выбросов.

Для более точного определения числа кластеров, были рассчитаны метрики, которые помогают в принятии решения. Среди них – метод локтя, метод силуэта, а также построение дендрограммы по методу Уорда. Визуализация состава кластеров по методу К-средних с помощью метода главных компонент представлена на рисунке 5.



Рисунок 5 – Визуализация состава кластеров по методу К-средних

Разбиение было проведено на 4 кластера

Кластер 1 можно охарактеризовать как «абсолютные плательщики» - имеют средние показатели возраста и зарплаты, однако наименьшую кредитную нагрузку ввиду того, что срок займа – наибольший и близок к году

Кластер 2 можно выделить, как «Богатые неплательщики», т.к. имеют высокие зарплаты.

Кластер 3 «Пожилые неплательщики» - Яркой чертой из остальных выделяется средний возраст, он выше, чем в других классах

Кластер 4 «Основные клиенты», наиболее многочисленный и имеет среднюю сумму задолженности, среднюю зарплату, возраст, срок и сумму займа, но наибольшую кредитную нагрузку, что говорит о том, что чаще всего берут микрозайм молодые люди на маленькие суммы и короткий срок, то есть они являются самыми массовыми клиентами.

С помощью метода *DBSCAN* были проанализированы объекты, указанные в качестве выбросов, ими в основном оказались добропорядочные клиенты, их было меньшинство.

Для построения скоринговой модели была выяснена значимость признаков с помощью алгоритма «Случайный лес». Для получения результата и принятия решения, кому стоит выдать кредит, а кому нет, было решено собрать значения каждого из нецелевых параметров, каждый параметр будет взвешен с индивидуальным значением веса, который получен с использованием метода «случайный лес». Для обучения были

взяты случайные 70% объектов. Среди наиболее значимых признаков оказались срок займа, сумма кредита и кредитная нагрузка.

Далее были построены нечеткие функции для каждого признака. Для этого поочередно брался каждый параметр из признакового пространства, кроме целевого, по ним строились гистограммы средних сумм задолженности. Было решено, что нечеткая функция должна давать значения близкие к 0 при небольшом риске заёмщика. На основании этого график был стандартизирован. Далее, для наглядности и устранения пропусков, были реализованы методы сглаживания графика: сглаживание скользящей средней и метод взвешенной скользящей средней. На рисунке 6 представлен график нечеткой функции для стандартизированного параметра «Возраст заемщика». Можно сделать вывод, что молодые заемщики чаще остальных допускают просрочки по займам, а также локальный экстремум наблюдается у заемщиков в возрасте примерно 45-50 лет.



Рисунок 6 – График нечеткой функции относительно параметра «Возраст заемщика»

Для определения надежности нового клиента, необходимо определить его кредитный рейтинг. Это некая количественная оценка того, насколько можно быть уверенным, что клиент вернет заемные средства. Для этого, было решено провести линейную аппроксимацию графиков нечетких функций.

Оценка риска по скоринговой модели происходит следующим образом. Рассчитывается степень риска по каждому признаку, результаты взвешиваются в соответствии с найденными весами и нормируются (Рисунок 7).

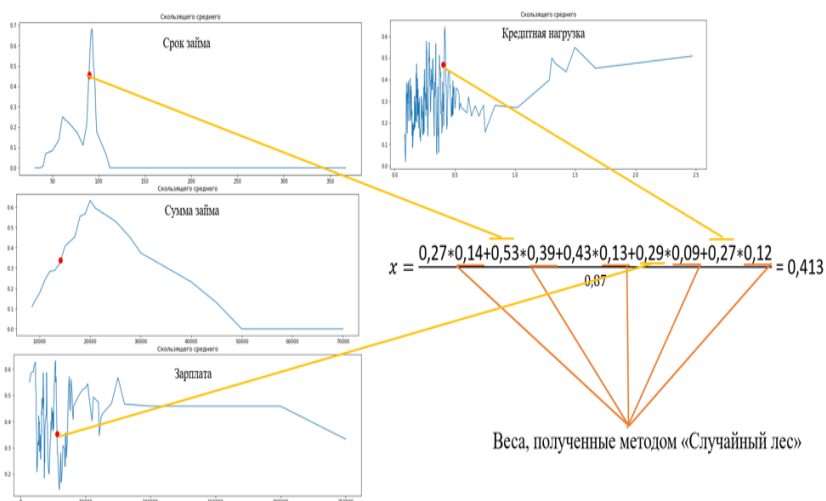


Рисунок 7 – Пример расчета риска

Кроме того, были построены гистограммы, которые демонстрируют зависимость суммы невозврата и прибыли клиента в зависимости от его кредитного рейтинга, а также количество заемщиков, распределенных по диапазонам кредитного рейтинга. Они представлены на рисунках 8-10.

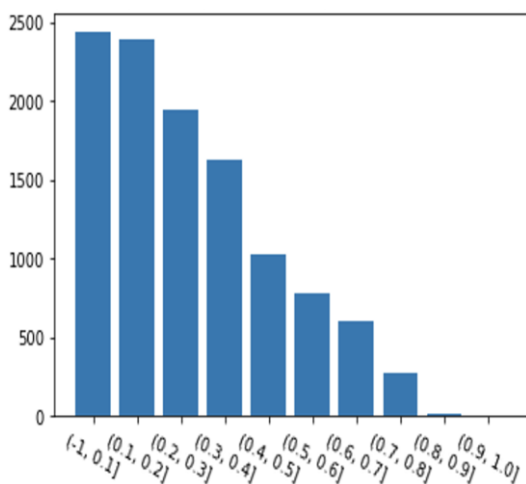


Рисунок 8 – Гистограмма средней суммы невозврата от кредитного рейтинга

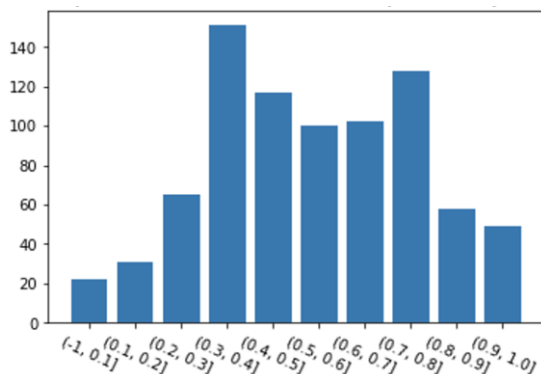


Рисунок 9 – Гистограмма количества клиентов от кредитного рейтинга

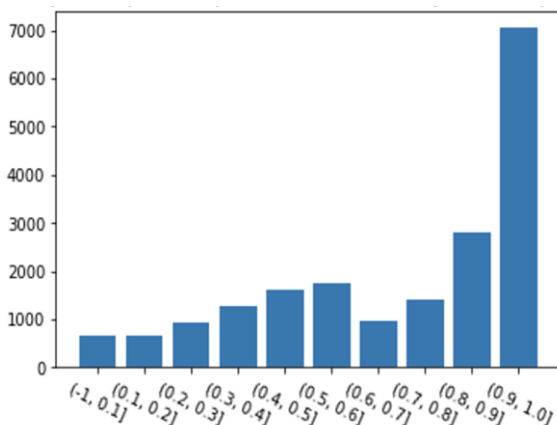


Рисунок 10 – Гистограмма средней прибыли с клиента в зависимости от кредитного рейтинга

Можно сделать вывод, что клиенты с рейтингом от 0,65 как правило возвращают кредит, от 0,35 до 0,65 - вероятность возврата средняя, а с рейтингом ниже 0,35 практически не возвращают.

В работе был разработан алгоритм расчета кредитного рейтинга в зависимости от индивидуальных показателей клиента, а также от суммы и срока выдачи кредита.

Результаты расчетов по алгоритму представлены в виде матрицы «карточка помощи» (Рисунок 11), по оси X отображается сумма займа, по оси Y - срок, а в ячейках - кредитный рейтинг и пометки цветом, к какой из трех категорий будет относиться данный займ для данного клиента. В

левом верхнем углу показаны условия, запрошенные клиентом изначально. В момент запроса кредита на данных условиях (18000 рублей на 89 дней) кредитный рейтинг клиента составил 0.163 и вероятность того, что он вернет кредит, была низкая (красная зона). В результате, так и получилось, по имеющейся информации данный займ повлек возникновение задолженности. Однако, этого было нетрудно избежать, незначительно изменив условия выдачи кредита. Например, клиенту можно предложить увеличение срока кредитования или уменьшение суммы, при которых клиент перейдет в желтую или зеленую зону, при этом риск невозврата займа существенно снизится.

89	0.163	0.307	0.277	0.254	0.234	0.322	0.337	0.353	0.380	0.380
97	0.632	0.672	0.664	0.663	0.689	0.737	0.728	0.726	0.697	0.760
106	0.639	0.668	0.651	0.696	0.671	0.663	0.685	0.678	0.705	0.760
115	0.555	0.622	0.671	0.644	0.640	0.739	0.706	0.698	0.719	0.760
124	0.563	0.587	0.654	0.688	0.624	0.690	0.685	0.640	0.735	0.760
133	0.579	0.598	0.697	0.655	0.681	0.694	0.733	0.740	0.749	0.760
142	0.629	0.643	0.668	0.673	0.651	0.685	0.635	0.740	0.760	0.760
151	0.639	0.689	0.699	0.693	0.675	0.692	0.719	0.681	0.760	0.760
160	0.633	0.660	0.616	0.690	0.660	0.706	0.733	0.685	0.760	0.760
169	0.634	0.662	0.682	0.707	0.594	0.690	0.686	0.695	0.760	0.760
178	0.602	0.662	0.682	0.709	0.684	0.667	0.733	0.706	0.760	0.760
	18000	16200	14400	12600	10800	9000	7200	5400	3599	1799

Рисунок 11 – Пример «карточки помощи»

Заключение

На основе анализа деятельности организации и моделировании основного бизнес-процесса были выявлены основные риски экономической безопасности МКК. Кластерный анализ клиентов МКК позволил выделить портретные характеристики клиентов каждого класса. В рамках исследования была построена скоринговая модель, которая не только оценивает риск заемщика, но и позволяет определить размер суммы и срок займа, при котором для конкретного заемщика риск невозврата будет минимизирован. Эффективность данной системы, основанной на расчете кредитного рейтинга, доказывает свою работоспособность на имеющихся клиентах, то есть при высокой вероятности возврата, клиенты действительно выплачивают кредит в установленный срок, а при низкой –

имеют большую задолженность. Разработанная процедура должна улучшить качество выдачи кредитов и экономическое состояние данной организации.

Список использованных источников:

1. Федеральный закон от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" (Дата обращения 10.11.2021)
2. Войшвилло И.Е., Шахназарян Г.Э. Макроэкономические риски деятельности микрофинансовых институтов и способы их минимизации // Научно–исследовательский финансовый институт. Финансовый журнал. 2013. № 4. С. 21–30.
3. Нестеренко Ю.Н. Институт микрофинансирования в системе финансового обеспечения субъектов микробизнеса // Вестник Российского государственного гуманитарного университета. 2013. № 15. С. 171–178.
4. Рыжановская Л.Ю. Социальная и финансовая составляющие микрофинансовой деятельности: выявление рисков // Научно–исследовательский финансовый институт. Финансовый журнал. 2013. № 3. С. 5–16.
5. Методы оценки качества чёткой кластеризации [Электронный ресурс]—URL: <http://ipo.spb.ru/journal/content/1349/Методы%20оценки%20качества%20чёткой%20кластеризации.pdf> (дата обращения 22.11.2021)
6. Ю. С. Кашницкий, Д. И. Игнатов, Ансамблевый метод машинного обучения, основанный на рекомендации классификаторов // Интеллектуальные системы. Теория и приложения — 2015. — №19. — С. 37–55.;
7. 15. Breiman L. Random Forests // Machine Learning. — 2001. — №1. — P. 1–32.;
8. Официальный сайт рейтингового агентства «РА Эксперт». [Электронный ресурс] URL: <https://raexpert.ru/researches/mfo/2020/>
9. Официальный сайт Центрального банка РФ. [Электронный ресурс] URL: https://cbr.ru/Collection/Collection/File/32241/mfi_market_trends_2020_4.pdf

Внешний и внутренний аудит в целях ПОД/ФТ/ФРОМУ

П.М. Абдуллаева
студентка 2 курса НИЯУ МИФИ, Москва
E-mail: a.patimat98@yandex.ru

С.В. Сергеев
студент 2 курса НИЯУ МИФИ, Москва
E-mail: SVSergey.sergeev@yandex.ru

Н.С. Белогина
к. э. н., доцент кафедры бухгалтерского учета и аудита
НИЯУ МИФИ, Москва
E-mail: nsbelog@gmail.com

Аннотация: В статье рассматриваются обязанности аудиторов при проведении внешнего аудита и обязанности предприятий при организации системы внутреннего контроля в целях по противодействию отмыванию денег и финансированию терроризма. Дана оценка влиянию изменений в законодательстве в сфере ПОД/ФТ на этапы проведения внешнего аудита (позиция авторов).

Ключевые слова: ПОД/ФТ, внешний аудит, профессиональное суждение, искажение финансовой отчетности, внутренний аудит, система внутреннего контроля.

External and internal audit for AML/CFT/FTMA purposes

Abstract: The article considers responsibilities of auditors when performing external audit and responsibilities of enterprises when organizing internal control system to combat money laundering and terrorism financing. The changes in the AML/CFT legislation and their impact on the stages of external audit are outlined (authors' position).

Keywords: AML/CFT, external audit, professional judgment, misrepresentation of financial statements, internal audit, internal control system.

Введение.

Отмывание доходов — это одно из серьезных экономических преступлений, которое представляет собой обработку преступных доходов с целью сокрытия их незаконного происхождения. В последние годы в мире, в частности и в России, активно принимаются меры по

противодействию легализации преступных доходов и финансированию терроризма, и в целом наблюдается становление и развитие «антиотмывочной» системы. Аббревиатура «ПОД/ФТ» получила дополнение в виде «ФРОМУ» – финансирование распространения оружия массового уничтожения – относительно недавно.

ПОД/ФТ и нормативное регулирование.

Одним из мощнейших регуляторов в области ПОД/ФТ/ФРОМУ является ФАТФ – Financial Action Task Force [1]. В данную Группу вовлечены более 30 стран, интересы Российской Федерации в этой организации представляет Росфинмониторинг. Совместно с Роскомнадзором и другими федеральными надзорными органами Росфинмониторинг осуществляет контроль за деятельностью как граждан, так и организаций в части соблюдения законодательства ПОД/ФТ [2]. В целом за всю антиотмывочную систему отвечает Росфинмониторинг, в части осуществления выездных и камеральных проверок, расследований схем отмывания денег, привлечение к ответственности. Также есть и Центральный Банк РФ, который отвечает за разработку и принятие нормативно-правовых актов в соответствии с требованиями, установленными законодательством, а также осуществляет контрольно-надзорные процедуры за поднадзорными Банку России организациями, осуществляющими операции с денежными средствами или иным имуществом.

Федеральный закон №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» выступает главным законодательным актом в сфере ПОД/ФТ. Принятие данного закона в целом было обусловлено существенным ростом угрозы со стороны оборота нелегальных денег, что, как следствие, могло привести к рискам и угрозам в системе национальной безопасности.

Действие Федерального закона № 115-ФЗ (в соответствии со статьей 2 закона) распространяется на деятельность ряда юридических и физических лиц, в том числе на деятельность *аудиторских организаций и индивидуальных аудиторов* [4]. Роль аудита в системе ПОД/ФТ с каждым годом становится всё более важной. Шаг за шагом, с каждой принимаемой правкой или законом, обозначается значимость, ответственность и обязанности аудиторских организаций в сфере ПОД/ФТ.

Как известно, аудит – это независимая проверка бухгалтерской (финансовой) отчетности аудируемого лица – экономического субъекта – с целью выражения мнения о надежности (достоверности) такой отчетности. В современной практике выделяют разные формы аудита. Если кратко: внешний аудит – это проверка независимой аудиторской фирмой, и цель внешнего аудита – выдача аудиторского заключения. А внутренний аудит

– в отличие от внешнего, нельзя назвать независимым, так как осуществляется по заданию руководства компании и цель: оценка эффективности системы внутреннего контроля и предложение решений по устранению выявленных недостатков в этой системе. Общепринятой является классификация аудита на внешний и внутренний. С точки зрения ПОД/ФТ обе формы аудита преследуют цели по выявлению недобросовестных действий.

Внешний аудит в целях ПОД/ФТ.

Под внешним аудитом понимают предоставление аудиторских услуг (проведение проверки, оказание сопутствующих услуг) независимой аудиторской компанией или независимым аудитором, имеющим квалификационный аттестат аудитора. Как правило, внешний аудит проводится по требованию законодательства [3] или по инициативе собственников экономического субъекта.

В соответствии с Методическими рекомендациями по рассмотрению аудиторскими организациями и индивидуальными аудиторами при оказании аудиторских услуг рисков ОД/ФТ (информационное письмо Росфинмониторинга №56), аудитор руководствуется профессиональным суждением при наличии оснований полагать, что операции экономического субъекта (аудируемого лица) могут быть исполнены в целях ОД/ФТ. Аудитор должен оценить риски, приняв во внимание следующие аспекты:

- принадлежность аудируемого лица к той или иной отрасли;
- специфика сектора экономики, в котором аудируемое лицо осуществляет деятельность;
- распространённые схемы (типологии) ОД/ФТ;
- аудиторские доказательства, полученные в результате аудита.

В целом, помимо указанных выше требований, в Федеральном законе № 307-ФЗ указаны обязанности, которые должны выполняться аудитором (аудиторской организацией) при осуществлении аудита. Наряду с предоставлением комментариев аудируемым лицам по их запросу, передачей аудиторского заключения, хранением документов и проч., Федеральным законом от №165-ФЗ «О внесении изменений ...» был введен пункт об обязанности извещать уполномоченный орган о возникновении любых оснований полагать, что сделки или финансовые операции аудируемого лица могли или могут быть осуществлены в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма.

В качестве уполномоченного органа выступает Федеральная служба по финансовому мониторингу (Росфинмониторинг). При этом аудиторы не имеют права разглашать факт передачи в Росфинмониторинг

соответствующей информации (отсылка к части 4 статьи 7.1 Федерального закона № 115-ФЗ).

Исходя из положений перечисленных законодательных актов, можно сделать следующий вывод. Росфинмониторинг поставил перед аудиторами новую, ранее не имевшую место и не входившую в их обязанности задачу – проверка законодательства в сфере соблюдения ПОД/ФТ у аудируемых лиц. В рамках ПОД/ФТ, аудит представляет собой систематическую проверку оценки рисков программы ПОД/ФТ независимым и подходящим квалифицированным специалистом (аудитором).

Можно выделить три области внешнего аудита, в отношении которых вновь введенная норма требует от аудиторов более внимательного отношения и профессионального суждения.

Во-первых, на начальном этапе, при проведении тестирования операционной эффективности средств внутреннего контроля и изучения (оценки) бизнеса экономического субъекта. Как правило, ранее аудиторы, в соответствии со своим профессиональным суждением, основываясь на рисках или/и результатах обсуждения с клиентом, принимали решение о тестировании системы внутреннего контроля. И самостоятельно устанавливали «параметры», проблемные секции. Сейчас, аудитор, тестируя систему внутреннего контроля, будет проверять в обязательном порядке внешние параметры, установленные Росфинмониторингом. Такого рода действия со стороны уполномоченного органа справедливо могут расцениваться как вмешательство в дела аудита, ведь самому аудиту это внутренне не присуще. Аудитор всегда был на стороне клиента, и независимое положение аудитора вызывало доверие и уважение со стороны руководства компании-клиента.

Во-вторых, при проведении аудита по существу, аудитор, помимо соответствующих стандартов аудита и бухгалтерского учета, должен помнить и проверять соблюдение требований законодательства по ПОД/ФТ. Это вносит дополнительный объем работы в процесс аудита.

В-третьих, на этапе проведения заключительных процедур и выдачи аудиторского заключения. Ответность аудируемого лица является недостоверной, если выявлены недостатки в системе учета, которые и привели к искажению. Влияние на достоверность финансовой отчетности изъянов системы внутреннего контроля не настолько очевидно. Нарушение правил контроля как таковое к искажению представленной в отчетности информации не приводят. Следовательно, оснований для выдачи аудиторского заключения с оговоркой не возникает. Однако, возможны ситуации, когда выявление нарушений в СВК может поставить под сомнение непрерывность деятельности экономического субъекта (речь идет о процедуре блокировки (заморозки) счетов организации,

деятельность которых вызывает подозрения. В этом случае меры по блокировке принимаются Росфинмониторингом и Банком России. Данные меры приостанавливают деятельность на неопределенный срок, в зависимости от деталей и причин, что прямым образом нарушает принцип непрерывности деятельности.

Еще один важный аспект – это принцип независимости аудитора. Сам факт осуществления передачи по требованию Росфинмониторинга информации о деятельности компаний-аудируемых лиц может поставить под угрозу отношения между клиентами и аудиторскими компаниями. Доверие с его стороны может снизиться, так как аудитор имеет доступ почти ко всем данным компании, и передача какой-либо её части без уведомления (как указано выше – аудиторы не имеют права ставить в известность саму компанию) даже с этической точки зрения может внести напряженность в отношения между клиентом и аудитором.

Кратко резюмируя, аудиторы, при возникновении достаточных оснований подозревать причастность компаний к террористической деятельности, должны незамедлительно сообщить в Росфинмониторинг. Можно еще раз упомянуть, что одной из новых обязанностей аудиторов является постоянная проверка соответствия требованиям ПОД/ФТ в ходе аудита и уведомление Росфинмониторинга наличии подозрений, нарушений. И так как это обязательство, то его нарушение влечет административную ответственность.

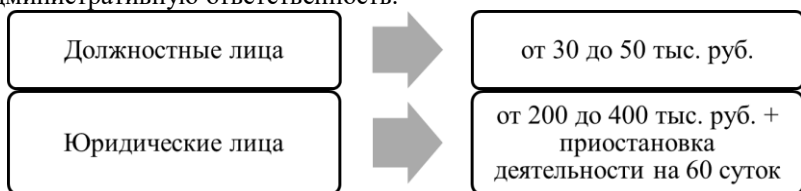


Рисунок 1 – Административные правонарушения

Кодекс об административных правонарушениях предусматривает санкции за несоблюдение указанных обязанностей. Непредставление сведений о подозрительных операциях и сделках является основанием для привлечения аудиторских организаций и индивидуальных аудиторов к административной ответственности по части 2 статьи 15.27 КоАП РФ.

Согласно данной норме, несоблюдение влечет наложение штрафа.

Внутренний аудит в целях ПОД/ФТ.

Внутренний аудит справедливо можно рассматривать как элемент системы внутреннего контроля. В отличие от внешнего, внутренний аудит осуществляется непрерывно, штатными или привлеченными сотрудниками. Внутренний аудит самостоятелен и независим от тех лиц,

деятельность которых подвергается проверке. Но в целом его нельзя охарактеризовать как полностью независимым, так как сотрудник при проведении внутреннего аудита действует в соответствии с заданием руководства организации (например, от имени Совета Директоров).

Международный стандарт МСА 610 приводит следующее определение: служба внутреннего аудита – это отдел или департамент, выполняющий консультационную деятельность, и цель этой консультационной деятельности заключается в том, что аудитор оценивает и предлагает решения по повышению действенности процессов корпоративного управления, управления рисками, а также процессов внутреннего контроля [14].

То есть, если внутренний контроль направлен на организацию, построение, автоматизацию и внедрение контролей в целом, то внешний аудит отвечает за их качество и эффективность работы в рамках всей системы и выявление недочетов.



Внутренний контроль в целях ПОД/ФТ – неотъемлемая часть общей системы внутреннего контроля организации. Согласно положениям статьи

3 Федерального закона № 115-ФЗ, организация внутреннего контроля должна включать следующее:

- Разработка правил внутреннего контроля;
- Назначение специальных сотрудников, ответственных за выполнение правил внутреннего контроля.

Обязанность по созданию и исполнению ПВК в рамках ПОД/ФТ/ФРОМУ является прерогативой организаций, которые осуществляют операции с денежными средствами или иными активами и имуществом [4]. То есть речь идет как и о банках, компаниях страхового сектора, так и НКО, ломбардах, фондах и другие.

Документ, утвержденный постановлением Правительства Российской Федерации от 30 июня 2012 г. № 667, регламентирует Требования к разработке правил внутреннего контроля, осуществляемого в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.

Разработка правил внутреннего контроля должна охватывать ряд программ осуществления внутреннего контроля (см. рис).

Соответствие разработанных Правил внутреннего контроля перечисленным выше требованиям (программам) крайне желательно.

В рамках темы статьи можно выделить пункт под номером 12, под которым подразумевается разработка инструкции по взаимодействию с Росфинмониторингом (или ЦБ России) в части выполнения их указаний относительно функции блокировки транзакций (счетов) при выявлении сомнений в добросовестности и легальности операций того или иного клиента. Осуществляется данная процедура при участии ЦБР методом отказа в проведении конкретной операции или полным блокированием счетов компании. Помимо этого, например, в разработку ПВК обязательно должна входить программа по идентификации клиента, оценка рисков, проведение инструктажа с сотрудниками, их обучение, подготовка в области ФРОМУ/ПОД/ФТ.

И, возвращаясь к внутреннему аудиту, специалист (внутренний аудитор) должен определить следующее:

- уровень эффективности работы подразделений в части соблюдения внутреннего контроля;
- риски и предложения по их устранению.

Роль внутреннего аудита в данной ситуации становится ключевой. Корректное функционирование службы внутреннего аудита, соответствие разработанному плану, применение профсуждения, осведомленность об изменениях в законодательстве в совокупности влияет на результаты проверки соответствия ПВК требованиям ПОД/ФТ. В противном случае,

при выявлении нарушений уже надзорными органами, возможно привлечение экономического субъекта к административной ответственности.

Таким образом, относительно функционирования внутреннего аудита (СВК) Росфинмониторингом, хоть и косвенно (через внутренний контроль) также устанавливается ряд обязательств, возрастают требования со стороны надзорных органов. Вследствие этого организациям следует обратить внимание на рост рисков, связанных с соблюдением законодательства в области ПОД/ФТ и санкционных режимов. И в целом быстрее реагировать на действия регуляторов и поддерживать эффективность системы внутреннего контроля, в частности соблюдение требований по ПОД/ФТ [11]. Из-за высоких требований организации могут столкнуться с ростом затрат, в связи с устранением нарушений, внедрением автоматизации процессов, обучением сотрудников, уплатой штрафов и проч.

Выводы. В заключение стоит отметить, что нормы и требования законодательных актов, направленных на борьбу с отмыванием преступных денег и финансированием терроризма, являются мерой необходимой. Изменения в актах федеральных законов и ужесточение требований затрагивает, как мы уже выяснили, и деятельность аудиторских организаций (индивидуальных аудиторов) и обязывает их сообщать в Росфинмониторинг о сомнительных операциях в деятельности аудируемого лица. Также повышены требования и к самим экономическим субъектам, в части организации внутреннего контроля. И, мы считаем, что если со стороны внутреннего аудита – введение таких норм оправданно и даже необходимо (для защиты компаний; снижения риска быть втянутыми в мошеннические действия, улучшения качества работы СВК, снижение рисков искажения информации), то для внешнего аудита такого рода обязательства могут повлиять на отношения с клиентами, так как аудитор – лицо независимое, с высоким уровнем доверия со стороны руководства компании, а также непосредственно на сам процесс аудита, в тех областях, которые ранее обозначены.

Список использованных источников:

1. Официальный сайт ФАТФ <https://www.fatf-gafi.org/>;
2. Официальный сай Федеральной службы по финансовому мониторингу. <https://www.fedsfm.ru/activity>;
3. Федеральный закон от 30 декабря 2008 г. № 307-ФЗ «Об аудиторской деятельности»;

4. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
5. Информационное письмо Росфинмониторинга от 23.11.2018 № 56 «О методических рекомендациях по рассмотрению аудиторскими организациями и индивидуальными аудиторами при оказании аудиторских услуг рисков легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма»;
6. Федеральный закон от 11 июня 2021 г. № 165-ФЗ «О внесении изменений в Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
7. Бадмаева С. С., Противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в аудиторской деятельности. Статья. – <http://www.esa-conference.ru/>.
8. Постановление Правительства РФ от 30.06.2012 № «Об утверждении требований к правилам внутреннего контроля, разрабатываемым организациями, осуществляющими операции с денежными средствами или иным имуществом, и индивидуальными предпринимателями, и о признании утратившими силу некоторых актов Правительства Российской Федерации»;
9. Приказ Росфинмониторинга от 03.08.2010 № 203 «Об утверждении положения о требованиях к подготовке и обучению кадров организаций, осуществляющих операции с денежными средствами или иным имуществом, в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
10. Международный стандарт аудита (МСА) 240 «Обязанности аудитора в отношении недобросовестных действий при проведении аудита финансовой отчетности»
11. Исследование «Делойт Форензик»: ПОД/ФТ. Результаты опроса участников рынка. – 2021;
12. Доклад об осуществлении Федеральной службой по финансовому мониторингу государственного контроля (надзора) в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма за 2020 год. – <https://docviewer.yandex.ru/view/324343981/>;
13. Обзор событий в сфере ПОД/ФТ, Банк России, сентябрь 2021. – https://cbr.ru/Collection/-Collection/File/38961/Sep_2021.pdf.

Внутренний контроль как мера противодействия финансированию терроризма в некоммерческом секторе

А.А. Галий

студент 5 курса НИЯУ МИФИ, Москва

E-mail: seniora-galiy@yandex.ru

В.М. Сушков

студент 5 курса НИЯУ МИФИ, Москва

E-mail: vmsushkov@mail.ru

П.Ю. Леонов

к.э.н., доцент кафедры финансового мониторинга

НИЯУ МИФИ, аттестованный аудитор, Москва

E-mail: p.u.leonov@gmail.com

Аннотация: В статье производится оценка необходимости внедрения и эффективности реализации внутреннего контроля в целях противодействия финансированию терроризма на примере некоммерческих организаций, которые являются особенно уязвимой формой юридических образований к риску использования в террористических целях. Описываются схемы вовлечения некоммерческого сектора в финансирование терроризма. Даются рекомендации по построению системы внутреннего контроля в некоммерческих организациях.

Ключевые слова: внутренний контроль, финансирование терроризма, некоммерческие организации, ФАТФ.

Internal control as a measure of countering terrorist financing through the non-profit sector

Abstract: The article assesses the need to implement and the effectiveness of internal control in order to counter terrorist financing on the example of non-profit organizations, which are a particularly vulnerable form of legal entities to the risk of being used for terrorist purposes. The schemes of involving the non-profit sector in terrorist financing are described. Recommendations are given on the development of an internal control system in non-profit organizations.

Keywords: internal controls, terrorist financing, non-profit organizations, FATF.

Введение

Терроризм как крайняя форма экстремизма – это наиболее общественно опасное преступление. Финансирование терроризма на сегодняшний день представляет собой серьезную угрозу всему мировому сообществу, вследствие чего разработка эффективных мер по его противодействию, а также их непрерывное совершенствование, является как никогда актуальной задачей каждого государства.

Поскольку хозяйствующие субъекты на ежедневной основе производят большое количество финансовых транзакций, которые, в частности, могут осуществляться с преступными целями, юридические лица подвержены риску использования в целях финансирования террористов террористических организаций, что обуславливает необходимость как внешнего, так и внутреннего контроля за их деятельностью.

Понятие и порядок организации внутреннего контроля

Классификация контроля с позиции подконтрольных экономических субъектов впервые была сформулирована и закреплена в Лимской декларации руководящих принципов контроля, принятая в 1977 году на IX Конгрессе Международной организации высших органов финансового контроля в городе Лима. Под внешним контролем понимается контроль государственных органов и негосударственных контролирующей организацией в лице аудиторских фирм, экспертных, сертификационных, лицензионных объединений и пр. за отдельными элементами финансово-хозяйственной деятельности юридических лиц. Внутренний контроль, напротив, осуществляется советом директоров, менеджментом и другим персоналом организации в целях принятия эффективных управленческих решений. Основные положения о порядке реализации внутреннего контроля находят отражение в локальном нормативном акте – внутрифирменных правилах внутреннего контроля (сокр. ПВК), в которых фиксируется порядок организации и работы службы внутреннего контроля или отдельных сотрудников, наделенных подобными функциями, их задачи, полномочия и соответствующие процедуры.

Механизмы внутреннего контроля могут решать широкий спектр задач – обеспечение точности и полноты документации бухгалтерского учета, подготовка достоверной бухгалтерской (финансовой) отчетности, исполнение приказов и распоряжений руководства, предотвращение случаев корпоративного мошенничества, краж, коррупции и т.д. Так, организация и осуществление внутреннего контроля совершаемых фактов хозяйственной жизни – это обязанность любого экономического субъекта в соответствии со статьей 19 Федерального закона от 06.12.2011 N 402-ФЗ «О бухгалтерском учете».

Внутренний контроль в целях противодействия финансированию терроризма обязателен только для определенных категорий юридических лиц и регламентируется следующими нормативно-правовыми актами:

1. Международные стандарты (рекомендации) Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ)

Рекомендация 18 «Внутренний контроль и зарубежные филиалы и дочерние предприятия», а также Пояснительная записка к ней требуют, чтобы финансовые учреждения разрабатывали программы по противодействию отмыванию денег и финансированию терроризма (сокр. ПОД/ФТ), включая разработку внутренних мер, процедур и средств контроля.

2. Федеральный закон от 07.08.2001 N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Статья 4 данного федерального закона устанавливает, что «организация и осуществление внутреннего контроля» являются одной из мер, направленных на ПОД/ФТ. Порядок реализации данной меры конкретизируется в последующих статьях. Так, согласно пункту 2 статьи 7, организации, осуществляющие операции с денежными средствами или иным имуществом (субъекты финансового мониторинга), а также лица, указанные в статье 7.1 (адвокаты, нотариусы, аудиторские организации и пр.), обязаны в целях ПОД/ФТ разрабатывать правила внутреннего контроля, а в ряде случаев целевые правила внутреннего контроля, назначать специальных должностных лиц (сокр. СДЛ), ответственных за их реализацию, а также принимать иные внутренние организационные меры в данных целях.

Кроме того, федеральный закон №115-ФЗ описывает порядок разработки правил внутреннего контроля, квалификационные требования к специальным должностным лицам, ответственным за их реализацию, и иные аспекты, касающиеся организации и осуществления внутреннего контроля в целях противодействия финансированию терроризма.

В список нормативно-правовых актов также включаются документы, устанавливающие требования к организации внутреннего контроля в различных хозяйствующих субъектах, перечень которых постоянно расширяется. Так, например, под действие федерального закона №115-ФЗ с 2018 года попали аудиторские компании и индивидуальные аудиторы, а с 13 января 2022 года вступит в силу новое Постановление Правительства РФ, обновляющее требования к правилам внутреннего контроля в аудиторском секторе.

Уязвимость некоммерческого сектора к финансированию терроризма

Согласно рекомендациям, лучшим практикам и типологическим исследованиям ФАТФ, представители некоммерческого сектора особенно уязвимы к риску вовлечения в финансирование терроризма, которое в большинстве случаев является следствием слабого внутреннего контроля. В российском законодательстве под некоммерческой организацией (сокр. НКО) понимают организацию, не имеющую извлечение прибыли в качестве основной цели своей деятельности и не распределяющую полученную прибыль между участниками [1]. Прежде всего, это организации, которые осуществляют сбор и распределение средств для благотворительных, социальных, культурных, религиозных, братских, образовательных и прочих целей.

Некоммерческий сектор в России на сегодняшний день все еще в стадии становления и нормативная база их функционирования постоянно меняется. Так, в 2021 году законодательство о некоммерческих организациях обновлялось дважды – в январе и октябре. Ключевые изменения включают расширение понятия «иностранный агент» и порядка проведения контрольных мероприятий в их отношении, ослабление требований к проведению обязательного аудита фондов и кадровой политике, а также введение налоговые льготы по аренде имущества.

Федеральная служба государственной статистики (Росстат) с 2019 года перестала публиковать число некоммерческих организаций по видам в ежегодном сборнике социально-экономических показателей «Россия в цифрах», что значительно осложнило оценку размера некоммерческого сектора в России. По данным Министерства юстиций РФ, на 2021 год в России зарегистрировано 210 793 некоммерческих организаций, из них в Москве 15% – более 30 тыс. некоммерческих организаций [2]. При этом наиболее распространенной формой являются автономные некоммерческие организации (24%), далее следует фонды (22%), общественные организации (17%) и ассоциации (16%) (рисунок 1). Также следует отметить, что большинство некоммерческих организаций молодые – 34% некоммерческих организаций Москвы зарегистрированы менее 5 лет назад, а их средний возраст составляет 9 лет (рисунок 2).

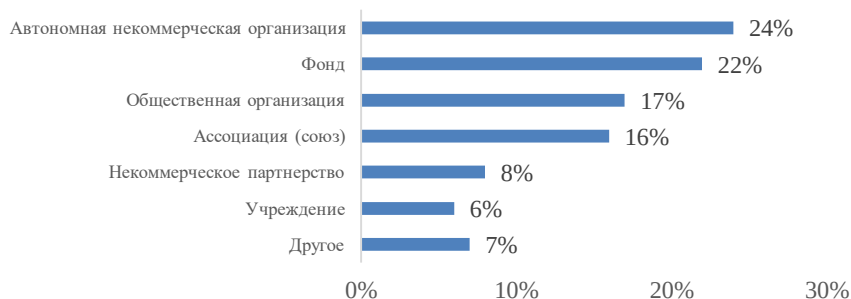


Рисунок 1 – Организационно-правовые формы некоммерческих организаций Москвы, 2020 г. [2]

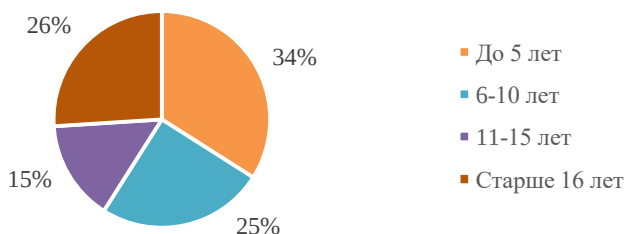


Рисунок 2 – Возраст некоммерческих организаций Москвы, 2020 г. [2]

Следует признать, что мировое сообщество значительно продвинулось в борьбе с террористической деятельности за последние десятилетия. Тем не менее, угроза терроризма все еще сохраняется, и одним из наиболее доступных способов финансирования нужд как отдельных террористов, так и крупных террористических организаций является злоупотребление деятельностью некоммерческих организаций. Уязвимость представителей некоммерческого сектора к данному риску обуславливается спецификой их деятельности. Некоммерческие организации, обладая доверием общества, зачастую получают доступ к значительным источникам финансирования, что позволяет аккумулировать и распределять большие объемы денежных средств

На рисунке 3 представлены наиболее часто практикуемые способы использования некоммерческих организаций в целях финансирования терроризма, которые ФАТФ выделил по результатам типологических исследований [3].

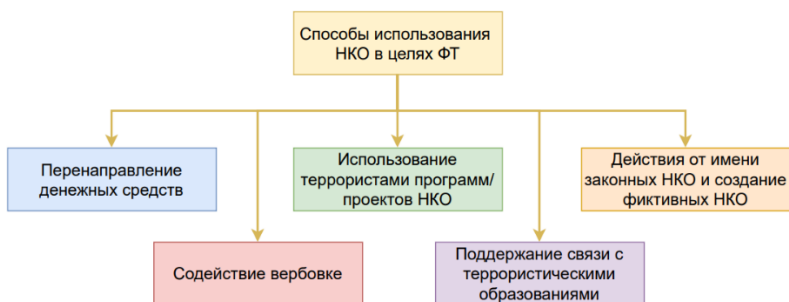


Рисунок 3 – Типологии использования некоммерческих организаций для финансирования терроризма

Правовая защита некоммерческого сектора

На международном уровне необходимость государств, а также самих некоммерческих организаций принимать надлежащие меры по минимизации риска вовлечения в финансирование нужд террористов устанавливается Рекомендациями ФАТФ [4]. В частности, некоммерческому сектору посвящена Рекомендация 8 «Противодействие использованию некоммерческих организаций в целях финансирования терроризма» и Пояснительная записка. Помимо этого, ФАТФ ежегодно проводит типологические и ситуационные исследования и на их основе публикует лучшие практики и руководства в отношении отдельных рекомендаций [4]. Так, в 2015 году ФАТФ издала документ по лучшей практике «Противодействие незаконному использованию некоммерческих организаций», разработанный в том числе на основе типологического исследования 2014 года «Риск незаконного использования некоммерческих организаций в террористических целях». [5, 6] На их основе в июне 2016 года была пересмотрена Рекомендация 8.

Бдительное отношение к некоммерческому сектору проявляется и в Российской Федерации. В 2018 году Международный Учебно-методический Центр Финансового Мониторинга (МУМЦФМ) опубликовал рекомендации для некоммерческого сектора по противодействию финансированию терроризма, в котором на основании стандартов и лучших практик ФАТФ изложил меры, которые следует принимать некоммерческим организациям в указанных целях [3].

Тем не менее, на данный момент некоммерческие организации не включены в перечень организаций, указанных в ст. 5 и ст. 7.1 федерального закона №115-ФЗ, вследствие чего требования законодательства о ПОД/ФТ напрямую к ним не относятся. Данные организации не обязаны формировать правила внутреннего контроля в целях противодействия финансированию терроризму, назначать специальных должностных лиц,

ответственных за их реализацию, и осуществлять иные меры в данных целях.

Рекомендации по построению системы внутреннего контроля в некоммерческом секторе

Требований федерального закона №115-ФЗ не распространяются на некоммерческий сектор в связи с тем, что некоммерческие организации в большей степени рассматриваются не как организации, осуществляющие операции с денежными средствами и иным имуществом, а как их клиенты. В этой связи борьба с незаконным использованием некоммерческие организации производится преимущественно методами внешнего контроля со стороны субъектов финансового мониторинга и государства в лице уполномоченного органа Росфинмониторинга и контрольных (надзорных) органов в зависимости от категории подконтрольного субъекта (Банк России, Пробириная палата и Роскомнадзор).

Тем не менее, современное состояние экономики и нарастающие угрозы финансирования терроризма заставляют задуматься специалистов в этой области и руководство стран как о состоянии и развитии некоммерческих организаций, так и о создании условий для безопасного и в то же время ответственного их функционирования [7]. Одним из методов достижения этой цели является обязательность организации внутреннего контроля в целях противодействия финансированию терроризма.

Основой для разработки правил внутреннего контроля в данных целях могут послужить Рекомендации для некоммерческого сектора, опубликованные МУМЦФМ. В частности, крайне ценной выступает Глава III «Меры, которые следует предпринимать некоммерческим организациям в целях противодействия угрозе использования в целях финансирования терроризма». Описанные в данной главе процедуры и мероприятия разработаны на основе лучших практик ФАТФ и относятся непосредственно к внутреннему контролю, осуществляемому собственниками и персоналом некоммерческих организаций, а именно:

1. анализ риска вовлечения некоммерческих организаций в финансирование терроризма и меры по его нейтрализации;
2. использование организационных ресурсов некоммерческого сектора;
3. надлежащее внутреннее управление некоммерческих организаций.

За основу структуры правил внутреннего контроля можно взять программы, обязательные для включения в правила внутреннего контроля субъектов, перечисленных в ст. 7.1 федерального закона №115-ФЗ (адвокаты, нотариусы, аудиторы и пр.). Данные организации и лица законодатель сознательно не включил в состав субъектов финансового мониторинга, однако наложил на них ряд обязанностей по

противодействию финансированию терроризма в силу специфики осуществляемой ими деятельности. Список данных программ следующий (на основе Постановления Правительства РФ от 14.07.2021 № 1188, который вступит в силу с 13.07.2022):

1. программа, определяющая организационные основы внутреннего контроля;
2. программа идентификации клиентов, представителей клиентов и (или) выгодоприобретателей, а также бенефициарных владельцев;
3. программа изучения клиента;
4. программа оценки рисков и управления рисками финансирования терроризма;
5. программа выявления сделок и финансовых операций, имеющих признаки связи с финансированием терроризма;
6. программа подготовки и обучения кадров в сфере финансирования терроризма;
7. программа проверки системы внутреннего контроля;
8. программа хранения информации и документов, полученных в результате реализации обязанностей по финансированию терроризма [8].

Раскроем специфику положений отдельных программ в случае их реализации в некоммерческих организациях.

Программы идентификации и изучения клиентов, их представителей клиентов, выгодоприобретателей и бенефициарных владельцев (№ 2 и № 3) рационально преобразовать в программы идентификации и изучения лиц и организаций, от которых некоммерческие организации получают и в отношении которых направляют средства и пожертвования (благотворителей и благополучателей). Некоммерческие организации не производят как таковой финансово-хозяйственной деятельности, а занимаются привлечением и распределением денежных средств на социальные цели. В связи с этим требуется всесторонняя проверка не только лиц и организаций, которым средства и пожертвования предоставляются в качестве благотворительности, но и тех, от кого организаторы добровольческой (волонтерской) деятельности получают данные средства. В первую очередь, необходимо осуществлять проверку по международным и национальным перечням террористов и террористических организаций. Помимо этого, с партнерами следует заключать письменные соглашения, закрепляющих задачи и взаимную ответственность сторон, направления распределения полученных средств, порядок контроля и предоставления отчетности по произведенным операциям [7].

Программа оценки и управления рисками финансирования терроризма (№ 4) должна содержать описание системы внутренней оценки рисков

некоммерческой организации, позволяющей заблаговременно предупреждать, выявлять и устранять данные риски и угрозы. Международные стандарты ФАТФ и документы по лучшим практикам регламентируют, что грамотная и актуальная оценка рисков вовлечения некоммерческих организаций в схемы финансирования терроризма, их предупреждение, выявление и пресечение является одним из наиболее эффективных способов минимизации риска злоупотребления некоммерческих организаций в террористических целях.

На основе рекомендаций МУМЦФМ в состав правил внутреннего контроля можно включить новую программу – программу надлежащего внутреннего управления некоммерческой организацией в целях противодействия финансированию терроризма, включающую положения, представленные в таблице 1.

Таблица 1 – Структура программы надлежащего внутреннего управления некоммерческой организацией

Положение	Содержание
Организационная целостность	Руководство некоммерческой организации, действуя в целях противодействия финансированию терроризма, должно разрабатывать методический инструментарий по привлечению квалифицированных и ответственных кадров, а также обеспечивать постоянный мониторинг текущей финансовой и операционной деятельности организации. Расходы некоммерческой организации, в том числе административные, должны санкционироваться и контролироваться высшим органом управления.
Финансовая прозрачность	Бухгалтерская служба некоммерческой организации должна вести непрерывный учет денежных операций и на регулярной основе подготавливать финансовую отчетность, позволяющую поэтапно проследить процесс перемещения средств от донора до бенефициара. Рационально проводить независимый аудит финансовой отчетности некоммерческой организации с целью проверки ее достоверности, а также целей распределения средств.
Разработка внутренних программ	Помимо правил внутреннего контроля, некоммерческой организации рекомендуется разрабатывать правила, программы, методические рекомендации для сотрудников по целевому использованию привлекаемых средств.

Программы № 1 и № 5-8, касающиеся организационных аспектов, обучения кадров, хранения информации в целях противодействия финансированию терроризма в своей основе могут быть заимствованы из

правил внутреннего контроля субъектов, перечисленных в ст. 7.1 федерального закона №115-ФЗ.

Заключение

Угроза использования некоммерческих организаций субъектами террористической деятельности в преступных целях остается крайне актуальной для Российской Федерации, в связи с чем необходимо обеспечивать надежную систему не только внешнего контроля, но и внутреннего, подразумевающего активные действия самих некоммерческих организаций по нейтрализации имеющихся рисков.

Стоит, тем не менее, отметить, что внутренний контроль по своей сути не способен противодействовать типологии, заключающей в создании фиктивных некоммерческих организаций. Внутренний контроль позволяет минимизировать риски использования легитимных некоммерческих организаций в целях финансирования терроризма отдельными сотрудниками или внешними лицами. В отношении организаций, изначально созданных в незаконных целях, должны применяться меры внешнего контроля со стороны государства и субъектов финансового мониторинга.

На сегодняшний день некоммерческие организации могут добровольно организовывать систему внутреннего контроля на основе принципов, описанных в статье. В перспективе внутренний контроль в целях противодействия финансированию терроризма в данной форме юридических образований может стать обязательным. Однако это потребует внесения изменений как в федеральный закон №115-ФЗ, так и иные законодательные акты, регулирующие деятельность некоммерческих организаций. По аналогии с иными хозяйствующими субъектами, законодатель может разработать и опубликовать требования к правилам внутреннего контроля, квалификации специальных должностных лиц, типовые формы некоммерческие организации в некоммерческих организациях. Конечной целью предлагаемых мер является минимизация рисков по использованию некоммерческого сектора в целях финансирования нужд террористов и террористических группировок во исполнение рекомендаций ФАТФ.

Список использованных источников:

1. Федеральный закон «О некоммерческих организациях» от 12.01.1996 N 7-ФЗ [Электронный ресурс]. – Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_8824.
2. НКО Москвы: статистический портрет и оценка состояния. Аналитический доклад Центра оценки общественных инициатив Института прикладных политических исследований НИУ ВШЭ

- [Электронный ресурс]. – Режим доступа : hse.ru/mirror/pubs/share/482698951.pdf.
3. Рекомендации для некоммерческого сектора в сфере противодействия финансированию терроризма [Электронный ресурс]. – Режим доступа : <https://fedsfm.ru/documents-nko>.
 4. Рекомендации ФАТФ. Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения / Пер. с англ. – М. : Вече, 2012. – 176 с.
 5. Лучшие практики. «Противодействие незаконному использованию НКО» (Рекомендация 8) [Электронный ресурс]. – Режим доступа : <http://www.fatf-gafi.org/media/fatf/documents/reports/BPP-combating-abuse-non-profit-organisations.pdf>.
 6. Отчет ФАТФ «Риск незаконного использования некоммерческих организаций в террористических целях» [Электронный ресурс]. – Режим доступа : <https://fedsfm.ru/documents-nko>.
 7. Гольская Ю.Н. Система внутреннего контроля в некоммерческих организациях // Вестник Алтайской академии экономики и права. – 2016. – № 2(44). – С. 104-107.
 8. Постановление Правительства РФ от 14.07.2021 N 1188 «Об утверждении требований к правилам внутреннего контроля, разрабатываемым адвокатами, нотариусами, лицами, осуществляющими предпринимательскую деятельность в сфере оказания юридических или бухгалтерских услуг, аудиторскими организациями и индивидуальными аудиторами» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_390495.

Выявление симптомов манипулирования финансовой отчетностью с помощью закона Бенфорда на примере компании Enron

В.М. Сушков

студент 5 курса НИЯУ МИФИ, Москва

E-mail: vmsushkov@mail.ru

П.Ю. Леонов

к.э.н., доцент кафедры финансового мониторинга

НИЯУ МИФИ, аттестованный аудитор, Москва

E-mail: p.u.leonov@gmail.com

Аннотация: В статье производится обоснование эффективности применения статистического инструмента закон Бенфорда в целях выявления признаков манипулирования финансовой отчетностью. Раскрывается методология применения закона в отношении отчетности компании Enron за 2000 год, впоследствии ставшей банкротом по причине искажения отчетности и корпоративного мошенничества.

Ключевые слова: закон Бенфорда, манипулирование отчетностью, искажение данных, Enron, Arthur Andersen.

Identifying signs of financial reporting manipulation using Benford's law based on the example of Enron

Abstract: The article substantiates the effectiveness of using the statistical tool Benford's law in order to identify signs of financial reporting manipulation. The methodology for applying the law to the reporting of Enron for the year 2000, which subsequently became bankrupt due to misrepresentation of reporting and corporate fraud, is disclosed.

Keywords: Benford's law, mis-reporting, data manipulation, Enron, Arthur Andersen.

Введение

В 2021 году исполняется 20 лет с банкротства американской энергетической корпорации Enron, которое является крупнейшим в мировой истории. Причиной краха седьмой по величине компании США явилось недостоверное представление финансового положения и результатов деятельности компании в финансовой отчетности, вводившее инвесторов в заблуждение. Банкротство Enron положило начало череде

событий, которые привели к изменению федерального законодательства США, устанавливающего требования к финансовой отчётности и процессу её подготовки, а также разорение ее аудитора – некогда лидирующей компании «Большой пятерки» Arthur Andersen [6].

Дело Enron является классическим при изучении истории финансового мошенничества. Enron по праву занимает ведущую позицию с точки зрения масштабов проводимых манипуляций. Несмотря на то, что случай Enron является далеко не единственным – приукрашивание отдельных статей финансовой отчетности компаний по всему миру за последние 20 лет не прекратилось, повторить «успех» Enron на сегодняшний день вряд ли получится. Масштабы проводимых манипуляций поражают воображение – компания осуществляла приписки прибыли любым проектам, которые в действительности оказывались убыточными. Несовершенства законодательства США и коррупционная составляющая позволили Enron совершать подобного рода махинации в течение нескольких лет, не только оставаясь незамеченными, но и принося собственникам и акционерам компании огромные доходы.

Тем не менее, даже без комплексного анализа финансово-хозяйственной деятельности Enron, отчетность компании могла вызывать обоснованные подозрения. Так, используя несложный в реализации статистический инструмент под названием закон Бенфорда в отношении отчетности компании за 2000 год можно было выявить признаки ее искажения.

Материалы и методы

Американские ученые С. Ньюком в 1881 году и Ф. Бенфорд в 1938 году независимо друг от друга обнаружили особое эмпирическое распределение частот появления первых цифр в естественно сформированных массивах данных, впоследствии получившее название «закон Бенфорда» (закон первой цифры, закон аномальных чисел) [3, 8]. Вероятность цифры оказаться на первом месте измеряется по формуле:

$$P(d) = \log_b(d + 1) - \log_b(d) = \log_b\left(1 + \frac{1}{d}\right),$$

где b – система счисления ($b > 2$);

d – цифры в данной системе счисления ($d \in \{1, \dots, b - 1\}$).

Так, для десятичной системы счисления вероятности появления первой цифры представлены на рисунке 1.

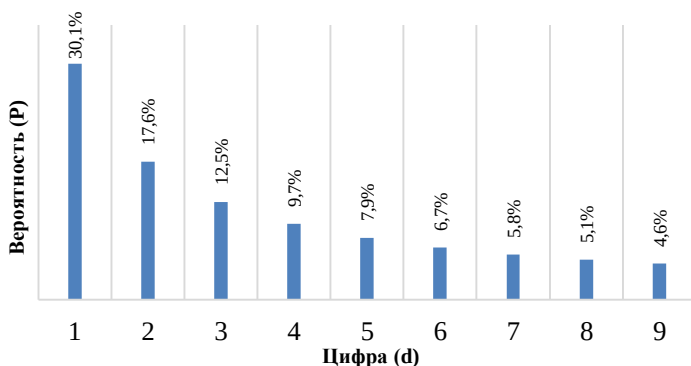


Рисунок 1 – Вероятности появления первой цифры для десятичной системы счисления

Начиная с 1990-х годов, научным сообществом стали разрабатываться статистические тесты проверки соответствия распределения в различных выборочных совокупностях закону Бенфорда. Наиболее распространенными являются тест первой цифры, второй цифры, а также первой пары цифр. На их основе можно делать выводы о степени «естественности» массивов данных, то есть отсутствия намеренного человеческого вмешательства в их формирование [9]. В список массивов данных, подчиняющихся закону Бенфорда, помимо площадей бассейнов рек, численностей населения, показателей рождаемости и смертности и прочих природно-социальных данных, также входят корпоративные данные. Отклонения распределения частот появления первых цифр в финансовой отчетности экономических субъектов от распределения Бенфорда может служить основанием для возникновения подозрений относительно их причин, которые среди прочего могут быть вызваны ошибками или мошенническими действиями.

Известные случаи манипулирования финансовой отчетностью компаний представлены в таблице 1.

Таблица 1 – Примеры известных случаев фальсификации финансовой отчетности

Компания	Страна	Год выявления	Факты фальсификации	Последствия
Cendant	США	1998	Завышение финансовых результатов	Штраф в размере 2,68 млрд долларов Падение цены акций более чем на 50%

Xerox	США	2000	• Завышение финансовых результатов	Исправление отчетности Падение цены акций на 67,53%
Enron	США	2001	• Совершение мнимых операций • Необоснованная переоценка ценных бумаг • Соккрытие долгов • Завышение финансовых результатов	Падение цены акций на 99,8% Банкротство
Sunbeam	США	2002	• Создание необоснованных резервов • Завышение прибыли	Обесценение акций Банкротство
WorldCom	США	2002	• Необоснованная капитализация расходов • Завышение финансовых результатов	Падение цены акций на 96,9% Увольнение более 17 000 сотрудников
Rite Aid	США	2003	• Завышение финансовых результатов	Падение цены акций на 37% Отказ от услуг аудитора KPMG
Parmalat	Италия	2004	• Завышение денежных средств	Банкротство
Royal Dutch Shell	Нидерланды	2004	• Искажение неаудируемой информации • Занижение амортизации	Падение цены акций на 10% Изменение рейтинга S&P на негативный
Siemens	Нидерланды	2008	• Завышение затрат	Обесценение акций Штрафы более чем на 300 млн долларов
Satyam Computer Services	Индия	2009	• Завышение финансовых результатов	Падение цены акций на 95,3% Поглощение
Kinross Gold	Канада	2010	• Завышение активов	Существенные последствия отсутствуют
Sino-Forest Corporation	Китай	2011	• Завышение активов	Падение цены акций на 82%

			• Завышение прибыли	Снижение рейтинга S&P
Olympus Corporation	Япония	2011	• Соккрытие убытков	Падение цены акций на 80% Реструктуризация бизнеса
Pescanova	Испания	2013	• Занижение долгов	Возмещение убытков инвесторам в размере 126,8 млн евро
Toshiba	Япония	2015	• Завышение финансовых результатов	Падение цены акций на 35% Увольнение топ-менеджмента
Wells Fargo	США	2017	• Создание фиктивных банковских счетов	Штраф в размере 185 млн долларов
Luckin Coffee	Китай	2020	• Завышение финансовых результатов	Падение цены акций на 80% Штраф в размере 8,98 млн долларов

Объектом данного исследования выступает финансовая отчетность энергетической компании Enron, поскольку в ней было подвержено искажению наибольшее число статей.

Статистический анализ на основе закона Бенфорда можно реализовывать с помощью массы программных продуктов, среди которых программа для работы с электронными таблицами Microsoft Excel, в том числе встроенный язык программирования VBA, реляционная система управления базами данных Microsoft Access, языки программирования R и Python, пакет прикладных программ MATLAB, BI-системы Power BI, QlikView, Tableau и др.

В данном исследовании выбор пал на объектно-ориентированный язык программирования Python 3, который на сегодняшний день является одним из наиболее востребованных инструментов обработки и анализа данных. Так, по сравнению с прикладными программами автоматизированной обработки табличных данных, Python 3 обладает следующими преимуществами:

1. Оптимизированная реализация однотипных задач. В случае необходимости модификации задачи или работы с новыми данными, время изменения кода на Python в разы меньше по сравнению с количеством времени, требующимся для внесения изменений в электронные таблицы.

2. Возможности обработки большого массива данных. Так, например, в отличие от Python, рабочий лист MS Excel 2019 ограничен 1 048 576 строками и 16 384 столбцами.

3. Удобство работы с большими массивами данных. Команды на Python позволяют извлекать только необходимую для решения текущей задачи информацию.

Среди прочих языков программирования Python 3 выделяет:

1. Несложный синтаксис, который позволяет использовать язык пользователями, ранее не имеющими опыт программирования.
2. Наличие большого количества качественных библиотек, которые помогают решать в том числе специфические задачи без написания массивного программного кода [7].

Так, сообщество программистов на Python создано несколько библиотек, посвященных статистике Бенфорда. Наиболее полной и производительной из них представляется разработанная Марселем Милсентом в 2017 году библиотека `Benford.py`, которая использовалась в данной работе [4].

Результаты

Проверяемый массив данных был сформирован из показателей следующих форм финансовой отчетности корпорации Enron и взаимосвязанных организаций за 2000 год:

1. Консолидированный отчет о доходах;
2. Консолидированный баланс;
3. Консолидированный отчет о движении денежных средств;
4. Консолидированный отчет об изменениях в капитале [5].

Выбор финансовой отчетности именно за 2000 год обусловлен тем, что это была последняя публикуемая годовая отчетность корпорации перед банкротством и в ней искажено максимальное, в сравнении с предыдущими периодами, число статей.

Полученная выборка подверглась предварительному анализу, а именно:

1. Отобраны только числовые показатели, характеризующие финансовое состояние, результаты деятельности и движение денежных средств экономического субъекта, выраженные в миллионах долларов США;
2. Из выборки исключены отрицательные (вычитаемые) показатели;
3. Проверено, что отобранные показатели не ограничены максимальными или минимальными значениями, за исключением нуля;
4. Проверено, что распределение полученной выборочной совокупности имеет экспоненциальный характер;
5. Проверено, что объем выборки является достаточным для проведения статистических тестов (больше 100).

Полученные данные проверены с помощью теста первой цифры, который предполагает сопоставление распределения первых цифр

финансовых показателей в отчетности Enron за 2000 г. с распределением Бенфорда. Результаты представлены на рисунке 2.

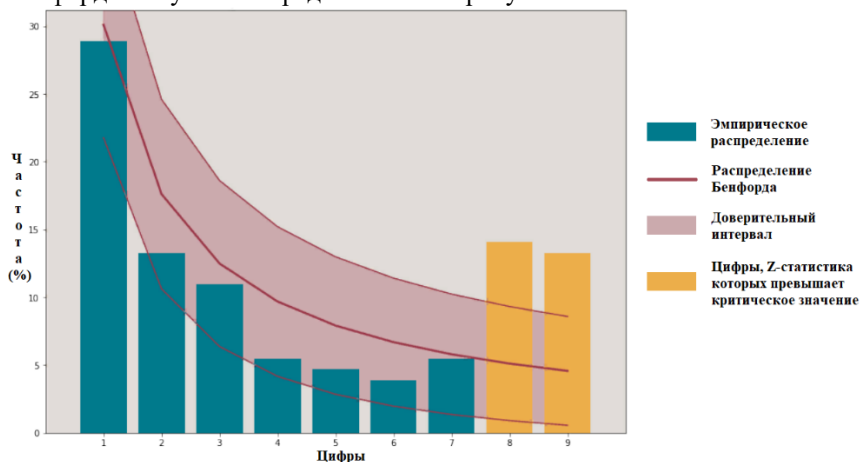


Рисунок 2 – Сопоставление распределения первых цифр в отчетности Enron с распределением Бенфорда

Статистические характеристики выборочной совокупности представлены в таблице 2.

Таблица 2 – Статистические характеристики выборки первых цифр в отчетности Enron

Характеристика	Значение	Интерпретация
Среднее абсолютное отклонение (MAD)	0.039	MAD превышает 0.015. Несоответствие распределению Бенфорда.
Коэффициент Бхаттачария	0.969	Коэффициент близок к 1. Распределение выборки значительно отличается от распределения Бенфорда.
Расстояние Бхаттачария	0.031	Расстояние близко к 0. Распределение выборки значительно отличается от распределения Бенфорда.
Статистика Z Колмогорова-Смирнова	0.177	Статистика превышает критическое значение на 95% доверительном уровне 0.120. Несоответствие распределению Бенфорда.
Статистика хи-квадрат	48.455	Статистика превышает критическое значение на 95% доверительном уровне 15.507. Несоответствие распределению Бенфорда.

Z-статистика для цифр 1-7	0.160–1.465	Статистика не превышает критическое значение на 95% доверительном уровне 1.960. Частота появления цифр 1-7 соответствует распределению Бенфорда.
Z-статистика для цифры 8	4.394	Статистика превышает критическое значение на 95% доверительном уровне 1.960. Частота появления цифры 8 не соответствует распределению Бенфорда.
Z-статистика для цифры 9	4.502	Статистика превышает критическое значение на 95% доверительном уровне 1.960. Частота появления цифры 9 не соответствует распределению Бенфорда.

Обсуждение

На основе проведенного анализа можно утверждать, что распределение первых цифр показателей в отчетности компании Елгон за 2000 год значительно отклоняется от распределения Бенфорда. Эмпирически видно, что сначала частоты первых цифр убывают, а начиная с цифры 7 возрастают. Число восьмерок и девяток в отчетности компании Елгон существенно больше, чем ожидается для естественно сформированного массива данных. Некоторые из показателей, первой цифрой которых в 2000 г. явились 8 и 9, приведены в таблице 3.

Таблица 3 – Показатели отчетности Елгон, значение которых в 2000 г. начинается с 8 и 9 [5]

Показатель	2000 г., млн дол.	1999 г., млн дол.	Изменение, %
Активы от деятельности по управлению ценовыми рисками	8 988	2 929	+207
Волоконно-оптические сети и оборудование	839	379	+121
Запасы	953	598	+59
Обязательства от деятельности по управлению ценовыми рисками	9 423	2 990	+215
Кредиторская задолженность	9 777	2 154	+354
Выручка от продажи металлов	9 234	0	—
Себестоимость газа, электроэнергии, металлов и других товаров	94 517	34 761	+172
Расходы на амортизацию	855	870	-2
Процентные расходы	838	656	+28
Итого расходы	98 836	39 310	+151
Чистая прибыль	979	893	+8

Одной из причин отклонений от распределения Бенфорда можно выделить стремление собственников и менеджмента компании преувеличивать результаты деятельности. Недостаточно высокие показатели в отчетности подвергались искажению, что повлекло за собой неестественно большое количество первых чисел высокого порядка – 8 или 9.

Основной мошеннической схемой, с помощью которой Enron «рисовали» показатели финансовых результатов, являлась необоснованная оценка финансовых инструментов, в отношении которых отсутствовал какой-либо реальный рынок. Это позволяло компании определять стоимость финансовых инструментов и доходов от их владения на основе собственных предположений, прогнозов, калькуляций и сомнительных операций [10]. Необоснованность отраженных в отчете финансовых результатов подтверждается наблюдаемой обратной зависимостью между показателями чистой прибыли и денежных потоков, в то время как доброкачественная прибыль должна обеспечиваться сопоставимыми денежными потоками (таблица 4).

Таблица 4 – Чистая прибыль и денежные потоки Enron [5]

Показатель	1998 г., млн дол.	1999 г., млн дол.	2000 г., млн дол.	CAGR, %
Чистая прибыль	703	839	979	18,01
Денежные потоки	-205	-815	-2 306	235,39

При более внимательном рассмотрении финансовых результатов Enron возникают и другие вопросы. Общая выручка компании в 2000 году составила 100,79 млрд долларов. Если бы данный показатель был раскрыт в сумме, меньше всего на 1%, он также попал бы в выборку подозрительных показателей на основе закона Бенфорда. С 1999 по 2000 год выручка компании выросла на 151%, что является весьма резким увеличением, учитывая, что в то время было всего несколько компаний с сопоставимыми доходами. Прежде всего, это были международные конгломераты, основанные более 100 лет назад. Для сравнения, динамика роста доходов Enron была вдвое больше Microsoft, выручка которой в то время составляла порядка 25 млрд долларов в год.

Кроме того, статистика Бенфорда выявила ряд сомнительных балансовых показателей. Среди них оказались «активы и обязательства от деятельности по управлению ценовыми рисками», которые, скорее всего, были завышены из-за неправомерной переоценки активов на основе текущих цен и путем мнимых продаж. Опубликованные данные подтверждают, что «активы от деятельности по управлению ценовыми

рисками» компании Enron были завышены минимум на 25% или порядка 2 млрд долларов [6].

Сумма по показателю «волоконно-оптические сети и оборудование» в составе активов также вызывает сомнения, поскольку для 2000 года было не редкостью существенное обесценение инвестиций, связанных с высокими технологиями. Тем не менее, Enron сохраняла верность своим бухгалтерским оценкам и не поддавалась предложениям рынка уценить эти активы [1].

Заключение

Таким образом, применение закона Бенфорда в отношении финансовой отчетности компании–лидера по масштабам проводимых манипуляций Enron показало, что данный инструмент эффективен для предварительного анализа финансовой информации на наличие признаков искажения. Заблаговременная проверка отчетности с помощью несложного в реализации закона Бенфорда, который в то время уже применялся в отношении налоговой отчетности, мог позволить инвесторам избежать потерь, вызванных банкротством компании. Учитывая усиление законодательства после скандала с Enron, а также развитие научно-технического прогресса, позволившего автоматизировать процедуры финансового контроля, допустимый процент потенциально не выявляемых искажений в отчетности снизился в десятки раз. Несомненно, это является позитивным фактором, однако мошенничество в учете и отчетности до сих пор практикуется, вследствие чего требуется разработка новых методов его выявления и совершенствование существующих. Так, сегодня тесты на основе распределения Бенфорда рационально применять не только к показателям из публикуемой отчетности, но и к прочим финансовым данным (операции по счетам, суммы в налоговых декларациях, платежи контрагентам, объемы страховых и гарантийных выплат и пр.). При этом увеличение объема проверяемых выборочных совокупностей влечет улучшение точности проводимых тестов и надежности получаемых результатов.

Список использованных источников:

1. Блэк Э. Вопросы стоимости. Овладейте новейшими приемами управления, инвестирования и регулирования, основанными на стоимости компании [Пер. с англ. Мельник, Н. А.]. — М.: ЗАО «Олимп-Бизнес». — 2009. — С. 400.
2. Суйц В.П., Хорин А.Н., Жакипбеков Д.С. Диагностика недостоверности отчетности организации: статистические методы в оценке достоверности бухгалтерской отчетности // Аудит и финансовый анализ. — 2015. — № 1. — С. 179-188.

3. Benford F. The law of anomalous numbers // Proceedings of the American Philosophical Society. – 1938. – Т. 78. – № 4. – С. 551-572.
4. Benford_py's documentation [Электронный ресурс]. – Режим доступа : <https://pypi.org/project/benfordslaw>.
5. Enron Annual Report 2000 [Электронный ресурс]. – Режим доступа : <https://www.sec.gov/Archives/edgar/data/1024401/000102440101500010/enr10-k.txt>.
6. Li Y. The case analysis of the scandal of Enron // International Journal of business and management. – 2010. – Т. 5. – №. 10. – С. 37-41.
7. Millman K.J., Aivazis M. Python for scientists and engineers // Computing in Science & Engineering. – 2011. – Т. 13. – №. 2. – С. 9-12.
8. Newcomb S. Note on the frequency of use of the different digits in natural numbers // American Journal of Mathematics. – 1881. – № 4(1). – С. 39-40.
9. Nigrini M.J. Benford's law: applications for forensic accounting, auditing and fraud detection. – Hoboken, New Jersey: John Wiley & Sons. – 2012. – С. 320.
10. Powers P.C.Jr., Troubh R.S., Winokur H.S.Jr. Report of Investigation by the Special Investigative Committee of the Board of Directors of Enron Corp. // Challenge. – 2002. – Т. 45. – № 3. – С. 117-127.

Информационная безопасность: современный аспект

Ф.Э. Меджитова

студент 2 курса ФГАОУ ВО «КФУ имени В. И.

Вернадского», Симферополь

E-mail: deka793@yandex.ru

научный руководитель: В.В. Ворошило

доцент кафедры финансов и кредита ФГАОУ ВО «КФУ имени В. И.

Вернадского», Симферополь

E-mail: Mivik06@mail.ru

Аннотация: В данной статье рассмотрена информационная безопасность как важнейшая составляющая национальной безопасности, в том числе исследовано понятие «информационная безопасность». Изучены угрозы информационной сферы. Исследование показало, что состояние информационной безопасности оказывает огромное влияние на все сферы деятельности человека и на дальнейшее развитие страны.

Ключевые слова: информационная безопасность, новые технологии, информация, национальные интересы, информационные угрозы, киберпреступность.

Information security: a modern aspect

Abstract: This article discusses information security as an essential component of national security. The threats of the information sphere have been identified. The concept of "information security" is formulated. The study showed that the state of information security has a huge impact on all spheres of human activity and on the further development of the country.

Keywords: information security, new technologies, information, national interests, information threats, cybercrime.

В современных условиях развития страны все больше уделяют внимание обеспечению информационной безопасности, которая включает в себя состояние защищенности общества и государства в целом от внутренних и внешних информационных угроз. Владение информацией, информационными технологиями и предоставление информационных услуг должно быть под пристальным вниманием у ученых и требуют должного изучения, поскольку использования их в отмывании денег и

финансовых мошенничествах террористами или мошенниками могут нанести предприятиям, государству и экономике большой урон, поскольку несут в себя ряд рисков. Именно поэтому информационная безопасность необходимо рассматривать в сфере ПОД/ФТ. Эффективное применение различных видов технологий является повышает уровень экономического развития государства. А вместе с тем, одновременно растет значимость обеспечения информационной безопасности при использовании этих технологий, а также эффективного противодействия киберпреступности. Информация все в большей мере становится стратегическим ресурсом любой страны.

Тема информационной безопасности актуальна в рамках исследования отмыывания денег и финансирования терроризма, так как страны продолжают создавать новые технологии, усовершенствовать их и внедрять во все сферы деятельности человека, а этим могут воспользоваться лица в противоправных действиях.

Большинство стран уделяют внимание информационной безопасности своей страны в том или ином объеме. Но именно страны с развитой экономикой понимают необходимость в должном внимании к проблеме информационной безопасности. С помощью информационного фактора возможно решения ряда государственных возможностей – решение национальных интересов, с помощью воздействия на региональную политику, мировую политику.

Для более детального изучения информационной безопасности необходимо исследовать национальные интересы и национальную безопасность.

Если рассматривать точку зрения Ковалева, то это «наличие сформулированных и осознанных национальных интересов, и потребностей нации в самосохранении и развитии является основанием для определения содержания национальной безопасности в рамках классических традиций и имеющейся мировой практики» [1].

Если рассматривать нормативно-правовые документы, то в Указе Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» под национальной безопасностью понимается «состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны»[2]. Основными интересами России являются: территориальная целостность державы, соблюдение прав и свобод

граждан, обеспечение высокого уровня жизни, повышение уровня и развития экономики. В Российской Федерации национальная безопасность занимает особое место, что связано с ее географическими и историческими характеристиками. Большая территория государства требует большего внимания в отдельных регионах, так как в России проживают разные национальности, права которых не должны ущемляться, и высоких затрат на обеспечение нужных методов регулирования в стране.

Обычно информационную безопасность представляют в виде системы, которую, свою очередь, можно рассматривать с двух сторон. Первая – способность противостоять внешним и внутренним информационным угрозам, вторая – при своем функционировании не создает угрозы. Однако, сама информация, как объект может быть подвержена различным внешним и внутренним рискам в связи с ее использованием.

Обеспечение информационной безопасности становится объектом исследования у различных авторов, среди которых можно выделить Ищейнова. Автор считает, что при решении таких проблем может быть достигнута информационная безопасность как: «1) защита информации, находящейся в системе, от дестабилизирующего воздействия различных угроз; 2) защита элементов системы от дестабилизирующего воздействия информационных угроз; 3) защита внешней среды от информационных угроз со стороны рассматриваемой системы» [3].

Информационную безопасность можно рассмотреть как многомерную область исследования и только при ее исследовании с помощью комплексного подхода может быть достигнут необходимый результат. В данных целях рассматривают три составляющие информационной безопасности: доступность, целостность и конфиденциальность информации и поддерживающей инфраструктуры.

Что собой представляет каждый из элементов. Доступность заключается в возможности получить требуемую услугу за определенное время. Целостность представляет собой актуальную, непротиворечивую информацию, а также подлежит защите от разрушения и изменения. Конфиденциальность заключается в защите от несанкционированного доступа к информации.

Необходимо отметить, что все проблемы, связанные с информационной безопасностью связаны с информационными технологиями, которые имеют высокие темпы развития. К сожалению, современные технологии программирования направлены на быстроту разработки программ и получение прибыли за счет скорости выпуска новых версий в ущерб процессам тестирования и проверки на безопасность, что не позволяет создавать безошибочные программы и не способствует быстрому развитию средств обеспечения информационной безопасности.

«Под угрозой обычно понимают потенциально возможное событие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. Угрозой интересам субъектов информационных отношений является потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию, ее носители и процессы обработки может прямо или косвенно привести к нанесению ущерба интересам данных субъектов» [3, с.36].

В зависимости от того, как распространяется информация по различным информационным каналам, угрозы утечки бывают следующих видов:

- видовая информация;
- акустическая (речевая) информация;
- утечка распространения по каналам ПЭМИН и т. д.

В теории существует классификация угроз по четырем классификационным признакам (по аспекту информационной безопасности, по компонентам информационной системы, по способу осуществления и по расположению источника угрозы), которая представлена на рисунке 1.



Рисунок 1 – Классификация угроз информационной безопасности
Источник: составлено автором на основе [1, с. 21]

Источниками угроз конфиденциальной информации являются собственные сотрудники организации, технические средства разведки или случайные люди. Все источники угроз информационной безопасности можно разделить на следующие группы: антропогенные (обусловленные действиями субъекта), техногенные (обусловленные техническими средствами) и стихийные.

По мнению Моргунова: «Человек является самым слабым звеном любой системы. А поскольку именно человек создает и использует ИС (информационные системы), то грамотно продуманная атака может помочь

получить доступ к самому защищенному серверу даже плохо подготовленному аудитору» [4, с.22-27]. Часто используют социальную инженерию, которая направлена на психологическую манипуляцию человеком, чтобы он выполнил определенные действия, необходимые для атакующего пользователя. Пользователь представляет собой первую линию защиты; если она падет, то вся система рухнет довольно быстро. Существует множество типов информационных атак: претекстинг, подделка принадлежности; фишинг, телефонный фишинг; техники, позволяющие скрыть от пользователя реального получателя письма; поддельные сайты и др.

Именно с помощью различных информационных атак осуществляется хищение конфиденциальной информации, а также денежных средств граждан. Современная ситуация, связанная с пандемией коронавируса, негативно повлияла на уровень защиты денежных средств, что связано с увеличением объема операций с использованием электронных средств платежа. Следовательно, увеличилось количество информации, которую можно использовать в корыстных целях. Согласно данным Федеральной службы по финансовому мониторингу за 2020 год в России зарегистрировано 510,4 тыс. преступлений, совершённых с использованием информационно-телекоммуникационных технологий. Это на 73,4% больше, чем в предыдущем году. В 2020 году количество и объем операций по переводу денежных средств с использованием электронных средств платежа (ЭСП) физических лиц составили 49,6 млрд единиц и 91,08 трлн руб., увеличившись по сравнению с 2019 годом на 23,1 и 28,2% соответственно. При этом количество операций без согласия клиента увеличилось на 34,0%. Объем таких операций вырос на 52,2%, составив 9777,3 млн руб. (за аналогичный период 2019 года – 6425,8 млн руб.). Общая сумма мошеннических операций в третьем квартале 2020 года достигла 2,5 млрд руб. Это на 32% больше к такому же периоду прошлого года. В 2019 году с июля по сентябрь мошенникам удалось похитить 1,9 млрд руб. [5]

Согласно данным МВД России в период самоизоляции на 76% выросло число дел, связанных с телефонным и интернет-мошенничеством. За первое полугодие 2021 года мошенники уже украли у граждан 6 млрд руб., а вернулось им всего 7,4%. Доля возврата снижается от года к году – по итогам 2019 г. гражданам вернули 14,6% похищенных средств, по итогам 2020 г. – уже 11,3% (1,1 млрд). В 2021 году наблюдается рост ИТ-преступлений в 1,5 раза. По статистике МВД, за семь месяцев 2021 года произошло почти 320 тысяч киберпреступлений. Это на 16% больше, чем за тот же период в прошлом году. Около 127 тысяч преступлений

совершены с использованием мобильной связи, 104 тысячи — с применением карт [6].

Активно развивающиеся технологии становятся оружием для введения информационных войн. Государственная политика в области международной информационной безопасности включает в себя совокупность скоординированных мер, которые направлены на формирование новой системы обеспечения международной информационной безопасности с учетом национальных интересов нашей страны. В связи с ростом ИТ-преступности органы создают специализированные подразделения для предотвращения возникающих угроз информационной безопасности. Также правительство Российской Федерации разрабатывает стратегии развития, согласно которым способами борьбы с проблемами в информационной сфере являются: 1) совершенствование безопасности направлены на социально значимые и другие объекты повышенной опасности; 2) повышение уровня защищенности информации предприятий и личных информационных систем; 3) создание единой системы информационно-телекоммуникационной поддержки для нужд системы обеспечения информационной и национальной безопасности в целом.

Поскольку информационные технологии охватили жизнь общества возникает необходимость в защите ее информационного пространства. При решении данной проблемы должны быть учтены следующие моменты:

1) информационная безопасность должна отвечать условиям социально-экономического направления и политическим условиям государства, что обуславливает необходимость дальнейшего научно-практического исследования;

2) должны быть учтены права граждан на использование информации, что направлено на совершенствование механизма реализации данных прав;

3) рассматривать информационную безопасность как составную часть национальной безопасности.

4) разработка современных методов и технических средств, обеспечивающих решение проблем в информационной сфере.

Обеспечение информационной безопасности дает возможность удовлетворять национальные интересы, сохраняя свои позиции на мировой арене, а также достигать новых высот в развитии.

Список использованных источников:

1. Ковалев, Д. В. Информационная безопасность: учебное пособие: [16+] / Д. В. Ковалев, Е. А. Богданова; Южный федеральный университет. – Ростов-на-Дону: Южный федеральный университет, 2016. – 74 с.: схем.,

- табл., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=493175> (дата обращения: 11.11.2021). – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст: электронный.
2. Указ президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». – Текст: электронный. – 2021. – URL: <https://www.garant.ru/products/ipo/prime/doc/401325792/> (дата обращения: 11.11.2021).
 3. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: учебное пособие: [16+] / В. Я. Ищейнов. – Москва; Берлин: Директ-Медиа, 2020. – 271 с.: схем., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=571485> (дата обращения: 11.11.2021). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст: электронный.
 4. Моргунов, А. В. Информационная безопасность: учебно-методическое пособие: [16+] / А. В. Моргунов; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2019. – 83 с.: ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=576726> (дата обращения: 12.11.2021). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст: электронный.
 5. Федеральная служба по финансовому мониторингу: официальный сайт. – Москва. – 2001-2021. – URL: <https://www.fedsfm.ru/> (дата обращения: 12.10.2021). – Текст: электронный.
 6. Министерство внутренних дел Российской Федерации: официальный сайт. – Москва. – 2021. – URL: <https://мвд.рф/> (дата обращения: 12.11.2021). – Текст: электронный.

Информационные технологии в управлении маркетинговой деятельностью предприятия

М.П. Башан

студент 4 курса НИЯУ МИФИ, Москва

E-mail: bashanm@mail.ru

Е.Р. Мысева

заместитель начальника отдела правового и методического обеспечения учебного процесса ИФТЭБ НИЯУ МИФИ, Москва

E-mail: ERMyseva@mephi.ru

Аннотация: В данной статье были рассмотрены ведущие тренды развития информационных технологий (ИТ), применение которых является одной из основных тенденций деятельности человечества для повышения качества жизни населения, конкурентоспособности экономики государства и повышения вероятности ее успешной интеграции в мировую экономическую систему, и их воздействие на сферу управления маркетинговой деятельностью предприятий.

Ключевые слова: Интернет; Интернет-технологии; информационные технологии; маркетинг, маркетинговая информация; сервис; ERP; CRM-системы, SMM.

Information technology in the management of the marketing activities of the enterprise

Abstract: This article considers the leading trends in the development of information technologies (IT), the use of which is one of the main trends in human activity in order to improve the quality of life of the population, the competitiveness of the state's economy and increase the likelihood of its successful integration into the world economic system, and their impact on the management sphere. marketing activities of enterprises.

Keywords: Internet, Internet technologies, information technologies, marketing, marketing information, service, ERP, SRM-systems, SMM.

На данный момент в условиях рыночной экономики ИТ являются основным инструментом научно-технического и социально-экономического прогресса. Они активно способствуют форсированию

добычи, распространения и эксплуатации новой информации, и тем самым в значительной степени меняют методики бизнеса.

Информатизация позволяет оптимизировать многие бизнес-процессы, что, в свою очередь, способствует более эффективному применению ресурсов, а также позволяет обеспечить потребителя максимальным количеством информации и качественными услугами.

В связи с ужесточением конкуренции среди предприятий прослеживается тенденция активного использования ИТ в бизнес-процессах, а также в маркетинге [3, 4]. Круг задач маркетологов, в свою очередь, подвергается существенным изменениям.

Были рассмотрены главные тенденции развития информационных технологий с точки зрения их влияния на управление маркетинговой деятельностью предприятия.

Понятием «информационные технологии» обозначают совокупность программных и технических средств вычислительной техники, а также приемов, способов и методов их использования для реализации функций сбора, хранения, обработки, передачи и использования информации в конкретных предметных областях [1, 6].

Рынок ИТ является одним из самых перспективных активно развивающихся. И хотя по прогнозам компании Gartner темпы развития отрасли замедлятся в 2022 году, она продолжит расти и ее объем увеличится почти до 4.5 трлн долларов. По данным аналитиков IDC от 8 июля 2021 года, в 2020 году объем рынка ИТ в России достиг 6.75 млрд долларов, что на 4.9% больше показателей предыдущего года.

В методическом смысле выделяют два главных пути использования ИТ:

1. Использование ИТ, в частности функционала сети Интернет для сопровождения компании и расширения спектра ее маркетинговых возможностей

Так, решение маркетинговых задач, что является продуктом обработки маркетинговых данных посредством использования информационных технологий – одно из перечня основных направлений деятельности предприятия.

В больших компаниях для сопровождения бизнеса популярно создание и эксплуатация информационных технологий и систем (ИТС) подготовки и принятия управленческих решений. Корпоративные информационные системы (КИС) обычно сочетают программные и аппаратные средства, ИТ и ресурсы для успешного руководства компаний.

Системы для планирования ресурсов предприятия (ERP-системы) являются эффективным инструментом для интеграции важных элементов производственной составляющей и деятельности по продажам.

Для небольших компаний целесообразны вложения в введение CRM (Customer Relationships Management) – систем регулирования отношений с клиентами. Такие системы используются главным образом для поддержания уровня продаж.

Маркетинговые информационные системы (МИС), включающие в себя индивидуумов, оснащение и процессы сбора, сортировки, анализа, мониторинга и сегрегации данных, применяются для разработки маркетинговых решений и решений задач стратегического планирования [5].

Становится заметным постепенное становление МИС в качестве составляющей КИС.

Большинство предлагаемых на рынке ERP-, CRM-систем включают в себя комплексы маркетинговых программ.

Наблюдается тенденция введения ERP- и CRM-систем на предприятиях очень разных масштабов: как в больших корпорациях, так и в среднем и мелком бизнесе. В качестве примера может выступать пакет программного обеспечения Microsoft Dynamics CRM 3.0, разработанный для внедрения в компании как малого, так и среднего и крупного бизнесов, который предоставляет широкий спектр возможностей в сфере маркетинговой деятельности, сбыта продукции и клиентского сервиса с использованием знакомого интерфейса Microsoft Office.

2. ИТС, предназначенные для разработки различных типов виртуальных компаний (стриминговые платформы, Интернет-магазины и т. д.).

В процессе того, как Интернет становился ведущим по популярности средю других медиа, возникло такое понятие, как Интернет-маркетинг, которое объединяет в себе различные концепции и способы проведения маркетинговых кампаний.

Интернет как инструмент маркетинга открывает перед специалистами такие возможности, как использование интерактивных средств (игры, опросы), мультимедиа, лендинга. Благодаря всему этому Интернет распространяется на многие направления деятельности служб маркетинга.

В работах [2] отмечается, что появление Интернета как нового инструмента маркетинга способствовало уменьшению трат на проведение исследований рынка, так как позволило создать принципиально новые виды интерактивных маркетинговых исследований. В качестве примера можно привести оценку популярности различных сайтов, интернет-опросы, оценку эффективности рекламы. Анализ поисковых запросов потребителя позволяет демонстрировать рекламу товаров и услуг, которые с наибольшей вероятностью его заинтересуют.

В частности, изменились возможности проведения опросов с помощью сети Интернет. Сейчас сбор информации производится в виртуальном пространстве, что означает решение многих логистических проблем данного процесса, его упрощение и уменьшение всяческих затрат, в частности времени. Также с помощью анализа, данных для которого благодаря Интернету стало значительно больше, появляется возможность более успешно ограничивать целевую аудиторию для проведения опросов.

Как правило, на начальном этапе маркетинговых исследований производится наблюдение за поведением гостей сайта. Незаметно и без призыва посетителей к действию, на данной ступени производится сбор важной информации о целевой аудитории и компаниях-конкурентах.

Так, Интернет в качестве средства для осуществления исследования рынка показывает высокую эффективность и имеет ряд определенных особенностей. [5,7].

Эволюция систем электронной коммерции является определяющим фактором, играющим важную роль во многих сферах деятельности предприятия. При этом системы для работы на различных рынках – B2B (бизнесы, чьими клиентами являются другие бизнесы и предприятия), B2C (бизнесы, продающие услуги клиентам для личного пользования), B2G (бизнесы, предоставляющие услуги государственным органам и учреждениям) и др. – имеют ряд важных различий. Устойчивые темпы роста сохраняет розничная интернет-торговля. Более того, объем продаж товаров и услуг посредством сети Интернет неминуемо захватывает рынок. Так, по прогнозам [statista.com](https://www.statista.com), в 2021 году на e-commerce (электронную коммерцию) будет приходиться до 17.5% объема розничных продаж.

Интернет играет все более важную роль в коммуникативной политике. Сейчас многие компании имеют свой собственный web-сайт, который способствует узнаванию компании и формированию ее имиджа.

Таким образом, маркетинг в сети Интернет и применение ИТ позволяет минимизировать издержки, способствует упрощенному проведению маркетинговых исследований, что объясняет популяризацию данных методов в ведении маркетинговой политики предприятий. Это определяет важность роли специалистов, которые отвечают за оперативный сбор и систематизацию информации, а также за корректную работу средств, обеспечивающих данные процессы. В их компетенции обычно входит создание и сопровождение контента на сайте, налаживание торговли посредством сети Интернет и обратной связи с клиентами, анализ эффективности маркетинга в сети Интернет и подготовка рекомендаций по внесению изменений.

При анализе в связи с ростом важности Интернет-коммуникаций в деятельности предприятий в сфере маркетинга компании группируют по

признакам их стратегических целей, а также стратегических задач по применению ИТ, и выставляемым требованиям в отношении компетентности работников и членам руководства отдела маркетинговой деятельности.

Деятельность компаний первого типа полностью основана на применении ИТ и предоставлении услуг в сфере ИТ. В группу предприятий такого типа входят прежде всего компании, занимающиеся разработкой и сопровождением ПО. Специалисты по маркетингу в таких компаниях должны быть осведомлены о тенденциях развития рынка информационных продуктов, на достаточном уровне знать рынок технических и программных средств, более того должны иметь определенную базу знаний для работы с информацией, для работы с большими объемами данных, а также сочетать все эти навыки для успешного управления маркетинговой деятельностью компании на различных ранках.

Следующий тип – компании, стремящиеся к использованию ИТ для более успешного ведения уже существующего бизнеса или совершенствованию используемых средств ИТ. В этом случае специалисты по маркетинговой деятельности ставят перед собой следующие задачи:

- разработку сайта для продажи услуг, повышение удобства пользования сайта (например, разработку мобильного приложения), привлекательности для клиентов, создание средств для связи с клиентами на сайте, системы отзывов, каталога товаров и услуг и т. д.
- введение в эксплуатацию разноуровневых КИС для сбора, анализа и систематизации для дальнейшего использования данных как во внутренней, так и из внешней среды организации;
- развитие маркетинга взаимодействия и внедрение CRM-систем;
- эффективная реклама в сети Интернет.

Таким предприятиям требуются сотрудники, компетентные в частности в сфере сетевого маркетинга, имеющие достаточные знания рынка, на котором торгует компания, а также навыки работы с программными и аппаратными средствами и анализа информации, полученной путем грамотного применения Интернет-технологий.

Крайне востребованы SMM-специалисты – профессионалы в сфере маркетинга в таких популярных сетях, как Вконтакте, Instagram, Facebook и т. д. Данная тенденция объясняется тем, что все чаще для поиска нужной информации люди посещают Интернет и соцсети, в следствие чего происходит вытеснение таких средств коммуникации, как радио, телевидение и печатные СМИ.

Третья группа предприятий нацелена на использование ИТ для создания новых форм ведения бизнеса. Такие компании могут, например,

оказывать услуги предприятиям второго типа. Таким компаниям требуются компетентные кадры в сфере маркетинга, обладающие способностями к адаптации к инновациям, а также эффективному использованию новых возможностей.

Анализируя данные группы предприятий, легко прийти к выводу о сходстве некоторых требований к специалистам в сфере маркетинга, которыми является компетентность в области маркетинга и способность эффективно применять ИТ и работать с технологиями в сети Интернет.

Таким образом, развитие ИТ в ощутимой степени влияет на технологии управления маркетинговой деятельностью компаний, способствует внедрению новых типов систем на предприятиях (ERP, CRM), создает новые специальности и диктует тенденции на различных рынках. Успешное внедрение таких технологий, которому способствует высокий уровень компетенции специалистов как в сфере маркетинга, так и в сфере ИТ, достаточное техническое и программное обеспечение компании, обеспечивает повышение конкурентоспособности компании, формирование ее уникального имиджа, узнаваемость и популярность.

Список использованных источников:

1. Федеральный закон № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и защите информации».
2. Бернс Э., Буш Р. Основы маркетинговых исследований с использованием Microsoft Excel: пер. с англ. М.: Вильямс, 2006.
3. Информационные системы и технологии в экономике и управлении: учебник/под ред. В. В. Трофимова: Высшее образование, 2012.
4. Козырев А. А. Информационные технологии в экономике и управлении. СПб.: Изд-во В. А. Михайлова, 2005.
5. Котлер Ф. Маркетинг менеджмент. СПб.: Питер Ком, 2020.

УДК 004:005.216.1:005.511(083.92)

© А.С. Лискина, Е.Р. Мысева, 2021

Информационные технологии как маркетинговый инструмент развития в сфере оценки эффективности бизнес-плана

А.С. Лискина

студент 4 курса НИЯУ МИФИ, Москва

E-mail: alisk1024@mail.ru

Е.Р. Мысева

заместитель начальника отдела правового и методического обеспечения учебного процесса ИФТЭБ НИЯУ МИФИ, Москва

E-mail: ERMyseva@mephi.ru

Аннотация: В статье рассматриваются особенности использования информационных технологий в процессе оценки маркетинговых решений, сформированных при составлении бизнес-плана. Определяются понятие, цели, структура и значение маркетинговых информационных систем в выборе управленческих решений.

Ключевые слова: маркетинговые исследования, маркетинговые информационные системы.

Information technology as a marketing development tool in the field of assessing the effectiveness of business plans

Abstract: The article discusses the features of the use of information technology in the process of evaluating marketing decisions formed during the preparation of a business plan. The concept, goals, structure and importance of marketing information systems in the choice of management decisions are determined.

Keywords: marketing research, marketing information systems.

Важнейшей частью любого бизнеса является планирование. Начиная новую предпринимательскую деятельность, компаниям необходимо учитывать актуальные потребности рынка, поскольку рынок – это динамичная система, в которой постоянно происходят изменения. В начале каждого периода, когда перед компанией появляется задача совершенствования своего производства, расширения видов деятельности или же выпуска нового товара, встает вопрос: стоит ли вкладывать ресурсы и затрачивать силы на реализацию конкретной деятельности?

Инструментом всестороннего анализа и моделирования является бизнес-план.

Бизнес-план является наиболее комплексным планирующим бизнес-документом. Он обобщает анализ возможностей бизнеса для конкретной ситуации и дает представление о том, какой стратегией менеджмента необходимо воспользоваться. А также является как путем получения финансирования, так и привлечения деловых партнеров. Любому руководителю стоит понимать, что бизнес-план – перспективный документ. Не имея представлений о будущем рынка сбыта, – а особенно о перспективах собственного развития, – организация может столкнуться с низкой эффективностью и потерей вложенных ресурсов.

Корректные маркетинговые решения напрямую связаны с будущими успехами и финансовым положением компании. Обнаружение ошибок в маркетинговой модели на этапе бизнес-планирования может иметь существенную ценность, поскольку позволит вовремя внести изменения в план маркетинга и избежать неудач в будущем.

Развитие информационных технологий способствует появлению маркетинговых инструментов и практик, позволяющих получать достоверные данные о состоянии рынка и тем самым предупредить формирование ошибочных решений.

В настоящее время роль информации и информационных технологий возрастает во всех сферах, в том числе и при разработке и ускорении принятия решений. Информация стала одним из важнейших ресурсов современного общества, с помощью которого успешно реализуется управление функционированием всех субъектов ведения хозяйства. У этого можно найти как положительные, так и отрицательные стороны. Среди положительных – повышение точности и надежности расчетов при подготовке управленческих решений. Однако это так же приводит к сокращению времени, затрачиваемого на обработку данных, что, как следствие, влечет рост вероятности принятия ошибочных и неэффективных решений.

Индустриальная экономика, которая основывалась на использовании природных ресурсов, сменяется экономикой знаний, основывающейся на информационных ресурсах. Теперь, в условиях роста объема внутренних и внешних информационных потоков, одними из наиболее важных составляющих эффективного управления становятся информационно-коммуникативные технологии и информационные системы. Свидетельством этого является расчет международной финансовой организацией «Всемирный Банк» показателя «индекс экономики знаний», отражающего «состояние основных слагаемых экономики знаний:

экономических стимулов и институционального режима, инновационной активности страны, уровня образования населения и развития ИКТ» [2].

В основе информационного обеспечения маркетинговой деятельности и принятия успешных управленческих решений лежит эффективное использование информационного потенциала предприятия. От него в значительной степени же зависит успешность проведения такой деятельности. Используя современные технологии в области коммуникаций (в первую очередь, Интернет), организация не только практически снимает пространственное ограничение на доступ к хранилищам данных, но и получает возможность получать новые данные в интерактивном режиме от потребителей, то есть непосредственно от главных участников рынка.

Целью данной статьи является определение особенностей использования информационных технологий в процессе формирования маркетинговых решений в бизнес-планировании.

В современных реалиях можно проследить влияние трех тенденций, обусловленных тем, что организации максимально заинтересованы в получении наиболее широкой информации, связанной с маркетингом, более высокого качества:

1. маркетинг на уровне местных рынков изменяется в сторону маркетинга в общенациональном масштабе;
2. траектория внимания организаций к покупательским способностям смещается к покупательским требованиям;
3. происходит стремительный переход от открытой конкурентной борьбы к борьбе в области неценовых факторов.

Увеличение роли и количества информации приводит к необходимости в информационных системах, одной из составляющих которых является информационная технология обработки данных.

Среди основных тенденций, в сторону которых развиваются информационные технологии в маркетинге, выделяют следующие:

- новые практики по сбору и преобразованию информации, появление новых средств, с помощью которых реализуется маркетинговая разведка;
- оптимизация автоматизированных процессов работы с имеющимися в организации базами данных;
- развитие использования цифровых технологии в маркетинге;
- ведение маркетинговой активности в социальных сетях;
- усовершенствование маркетинговых информационных систем (МИС), путем дополнения их системой поддержки и автоматизацией процессов в сфере маркетинга;

– объединение маркетинговых и корпоративных информационных систем, а также интеграция МИС с другими внешними системами и источниками информации [4].

Главной целью информационного обеспечения маркетинговой деятельности является создание системы взаимосвязанных и взаимодополняющих показателей, позволяющих получать необходимые и достаточные количественную и качественную характеристики изучаемых объектов.

Современная маркетинговая деятельность отличается технологичностью и высокой сложностью, которая связана с потребностью в больших объемах информации, чтобы управленческое решение было принято обосновано. Поэтому становится необходимо обращаться к компьютерным технологиям не только для того, чтобы собрать и обработать данные или использовать их как средство коммуникации, но и чтобы получить комплексную поддержку принятия решений.

В современных реалиях организации могут обеспечить конкурентные преимущества в маркетинговой деятельности за счет использования маркетинговых информационных систем (МИС). При изучении литературы по данной теме можно встретить различные подходы к описанию подобной системы и определению ее термина. Его возникновение традиционно связывают с именами Дональда Ф. Кокса и Роберта И. Гуда. В их совместной статье «Как построить маркетинговую информационную систему» (опубликована в 1967 г.) [1] данный термин определен как набор процедур и методов для регулярного, запланированного сбора, анализа и представления информации для использования при принятии маркетинговых решений.

С последующим развитием компьютерной индустрии и ее проникновением во все сферы управления становится возможным применение программных продуктов для решения маркетинговых задач, что приводит к развитию концепции маркетинговой информационной системы.

Среди множества трактовок, выдвигаемых различными авторами, можно выделить основные функции данных систем, которые отмечаются всеми:

- обеспечение процессов сбора, обработки и хранения информации;
- ориентация на использование как внешних, так и внутренних источников информации;
- использование современных компьютерных технологий, методов анализа и обработки данных;
- обеспечение процесса принятия управленческих решений;

- обеспечение преобразования первичных необработанных данных в релевантную информацию;
- обеспечение постоянного потока маркетинговой информации, за счет работы на регулярной плановой основе [4].

Исходя из этого, маркетинговую информационную систему можно определить не только как группу технических и программных средств, призванных упростить работу с большим потоком информации, сюда также входят методические и организационные средства поддержки. Но, конечно, все это не может функционировать без персонала, который будет обеспечивать принятие опережающих маркетинговых решений на основе регулярного сбора, обработки и анализа информации о состоянии и изменениях, происходящих как во внутренней, так и во внешней среде организации.

То есть в состав МИС входят: технические средства, процедуры и методы сбора, обработки и анализа информации, а также лица, принимающие управленческие решения (ЛПР). Перед МИС ставится задача собрать информацию об объекте исследования и его среде, преобразовать ее, оценить состояние этого объекта и возможное развитие ситуации в будущем, сделать прогноз относительно происходящих изменений и их последствий для предприятия, а затем предоставить результаты проделанных операций ЛПР в доступной им форме.

Операции, осуществляемые над информацией в рамках функционирования МИС, можно представить в виде последовательного ряда (рис. 1):

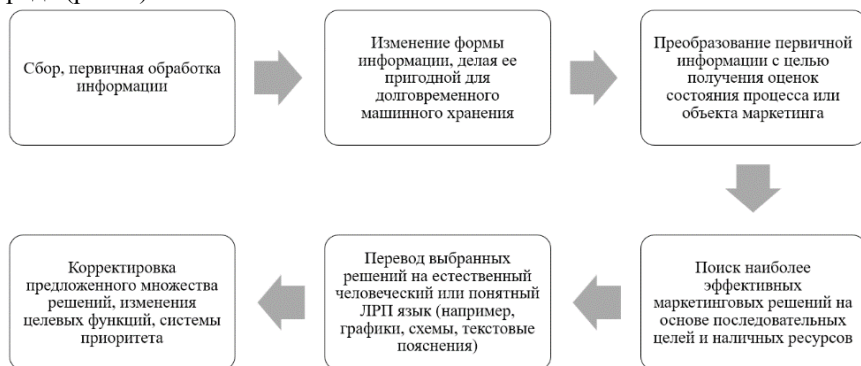


Рисунок 1 – Операции МИС над информацией

Можно сделать вывод о том, что для МИС разрабатывают, – а затем закладывают в них, – специальные алгоритмы, которые совершают операции по преобразованию информации. Это и есть так называемые

модели принятия маркетинговых решений. С помощью них происходит определение процедур, необходимых для реализации оценки качества исходной информации, и на основании результатов делаются выводы об объекте маркетинга.

Американский академик Филип Котлер, при определении структуры МИС, представил ее в виде четырех компонентов:

- системы внутренней отчетности;
- системы сбора текущей внешней маркетинговой информации;
- системы маркетинговых исследований;
- системы анализа маркетинговой информации [3].

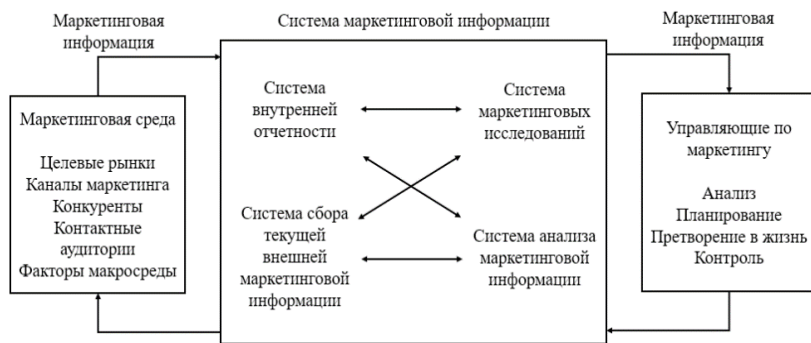


Рисунок 2 – Модель МИС по Ф.Котлеру

Данная модель является традиционной. В современных разработках именно над ней происходят работы по усовершенствованию МИС: ее адаптируют под необходимую специфику, диктуемую отраслью и регионом, в которых существует организация; дополняют и детализируют, обращая внимание на особенности производства или продвижения товаров. В зависимости от требований, предъявляемых модели, она может быть расширена или укрупнена функциональными элементами, необходимыми для обработки информации.

Наличие тех или иных элементов маркетинговой системы является одним из основных различий моделей, разрабатываемых разными авторами. Например, Р. Гуд делает акцент на значимости операционной и поддерживающих систем, Ф. Котлер – на подсистемах маркетинговых исследований и разведки, а также системе поддержки принятия решений.

В общем виде МИС разделяют на три типа:

1. Система управления маркетингом. Предоставляет управленческую информацию, касающуюся тенденций и проблем на рынке, а также маркетинговых возможностей. Система полезна для контроля затрат на маркетинг и выяснения причин плохих продаж.

2. Система маркетингового планирования. Предоставляет информацию, необходимую для будущего планирования продуктов, в наиболее удобной и понятной форме. Эта система решает следующие задачи: прогнозирование продаж, планирование продвижения, кредитный менеджмент и т.д.

3. Система маркетинговых исследований. Полезна для анализа и решения текущих маркетинговых проблем. Она измеряет характеристики разных типов клиентов и их поведение. Маркетинговые исследования решают проблемы, связанные с рекламой, ценами и т.д.

Из вышеизложенного следует, что маркетинговая информационная система обеспечивает:

- организованный сбор, обработку и анализ информации;
- широкий взгляд на рынок, конкурентов и потребителей;
- прогнозирование рисков и потерь от их наступления;
- координацию плана маркетинга;
- оперативность принятия решений;
- возможность проведения анализа затрат и выгод;
- дополнительные возможности повышения прибыльности за счет наличия многоаспектных знаний о рынке.

МИС дают компании множество преимуществ, потребность в них общепринята. Однако одна и та же система не может использоваться для всех типов компаний. У каждой организации и ее маркетинговых служб существуют свои специфические требования, обусловленные особенностями своей деятельности, поэтому любая маркетинговая информационная система является индивидуальной. Из этого следует вывод: создание единого формализованного плана по совершенствованию данных систем вряд ли возможно. Все они отличны друг от друга по своей структуре и характеристикам входящих элементов. Практика показывает, что системы начинают подвергаться изменениям, когда у организации, – а точнее лиц, отвечающих за принятие решений в маркетинге, – появляется потребность в дополнительной маркетинговой информации, и ее руководители готовы выделить денежные средства, чтобы получить ее.

Однако можно отметить, что современный уровень развития информационных технологий предоставил возможность использования облачных технологий не только для хранения данных, но и для получения доступа к программному обеспечению и средствам аналитической обработки. Это весьма полезная технология для применения в маркетинговых информационных системах, особенно для начинающих предприятий с малым бюджетом, поскольку реализацию определенных функциональных модулей можно осуществлять через облачные сервисы,

что позволит существенно экономить на затратах формирования, сопровождения и поддержания.

На эффективность маркетинговой деятельности предприятия оказывает влияние ряд факторов. Среди них особое место занимает процесс маркетингового исследования и принятие на его основе маркетинговых решений. Это связано с тем, что для поиска источников с высокой степенью достоверности и полноты отражения реальных рыночных процессов, совершается значительный и трудоемкий объем работ. К тому же приходится учитывать большое количество факторов внешней и внутренней среды, которые подвержены быстрым изменениям. Выбор правильного источника информации очень важен, поскольку в случае ошибки компания обрекает себя на неверную интерпретацию данных, и, как следствие, ошибочную оценку экономической ситуации. Опираясь на ложные выводы, не соответствующие реальному положению рынка, руководители принимают ошибочные управленческие решения и могут понести тяжелые последствия.

Для повышения эффективности процесса обработки данных и подготовки управленческих решений возникает необходимость использования автоматизированных информационных систем.

Информационные технологии помогли облегчить разработку различных методов маркетинга, что позволило более эффективно распределять данные, необходимые для успеха в бизнесе. Благодаря этим достижениям, менеджеры получили превосходные инструменты для интерпретации имеющихся данных о потребителях и товарах и использования этой информации в рамках своего бизнес-планирования.

В статье рассмотрена маркетинговая информационная система как информационная технология, оказывающая поддержку в принятии маркетинговых решений на основе полного анализа рынка. Однако стоит отметить, что сама по себе информационная технология не может быть единственным инструментом в достижении поставленных целей. Важным аспектом остаются индивидуальные качества лиц, входящих в группу по принятию решений.

Список использованных источников:

1. Cox D. F., Good R. How to Build a Marketing Information System // Harvard Business Review. 1967. May–June. P. 145–154.
2. Индекс экономики знаний :: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. – Режим доступа: <https://digital.gov.ru/ru/activity/statistic/rating/indeks-ekonomiki-znaniy/#tabs|Compare:Place> (дата обращения: 03.11.2021).

3. Котлер Ф., Келлер К. Л. Маркетинг менеджмент. 12-е изд. — СПб.: Питер, 2012. — 816 с.
4. Матвеева Л. Г. Маркетинговые информационные системы : учебное пособие / Л. Г. Матвеева, А. Ю. Никитаева, О. А. Чернова ; Южный федеральный университет. — Ростов-на-Дону : Издательство Южного федерального университета, 2015. — 224 с.

Информационные технологии как маркетинговый инструмент развития в сфере цифровых развлечений

С.А. Михайлов

студент 4-го курса НИЯУ МИФИ, Москва

Е.Р. Мысева

заместитель начальника отдела правового и методического обеспечения
учебного процесса ИФТЭБ НИЯУ МИФИ, Москва

E-mail: ERMyseva@mephi.ru

Аннотация: Цифровые развлечения неразрывно связаны с нынешней жизнью общества. Они везде: видео игры, социальные сети, потоковые сервисы. Это малая часть из общего числа и их комбинаций.

Ключевые слова: цифровые развлечения, социальные сети, реклама, потоковые сервисы, digital-маркетинг.

Information technology as a marketing development tool in the field of digital entertainment

Abstract: Digital entertainment is inextricably linked with the current life of society. They are everywhere: video games, social networks, streaming services. This is a small part of the total number and their combinations.

Keywords: digital entertainment, social networks, advertisement, streaming services, digital-marketing.

В последние несколько лет в маркетинге произошли революционные изменения в технологиях. По данным Freely 76% специалистов в области маркетинга считают, что последние 2 года в маркетинге произошло больше изменений чем за предыдущие 50 лет. Эти изменения связаны, во-первых, с развитием информационных технологий, что дает кардинально новые возможности привлечения потребителя, во-вторых, появление глобализации экономических процессов и усиление конкуренции, из-за которой возникла необходимость искать новые способы привлечения потребителя. Массовая доступность информации о товарах или услугах заставляет компании снижать цены и повышать качество своей продукции, так как потребитель может сравнивать предложения тех или иных компаний. Таким образом, чтобы сохранить свою конкурентоспособность компании перешли с массового маркетинга к узконаправленному,

ориентированному на конкретные группы потребителей, используя новые возможности информационных технологий.

Актуальность данной темы обуславливается тем, что цифровой маркетинг открывает новые возможности для развития бизнеса. В интернете можно найти целевую аудиторию для любого направления. Даже небольшая компания может продвигать свои товары и услуги по всему миру.

Сегодня люди пользуются огромным количеством гаджетов, каждый из которых подключен к интернету. Например, планшеты, браслеты, умные колонки, смарт-часы и, конечно, в первую очередь смартфон. Гаджеты – отправная точка для получения услуг и совершения покупок. В любом смартфоне можно найти существенное количество приложений, которые позволяют совершать финансовые операции, помогают передвигаться по городу, стране, миру или же совершать заказы в ресторанах или онлайн-магазинах. Этим всем занимается digital- или цифровой маркетинг – способ для бизнеса продвижения услуг и товаров с помощью цифровых технологий, поддерживать контакт с потребителем на всех этапах взаимодействия, нет больше границ между онлайн и офлайн жизнью.

Digital-маркетинг или цифровой маркетинг представляет собой комплекс передовых цифровых возможностей для охвата максимума целевых потребителей и регулирования эффективности взаимодействия с ними. Основными инструментами digital-маркетинга являются:

- Контекстная реклама. Она заключается в размещении рекламных объявлений на тематических сайтах.

- SEO-продвижение. Используется как канал привлечения трафика сайта рекламодателя в выдаче по тематическим запросам.

- Баннерная реклама. Размещение графических баннеров с предложением продукта или услуги на сторонних тематических ресурсах.

- Радиореклама. Достаточно дорогой способ, но способен донести свое предложение до широкой аудитории.

- Рекламные окна. Подразумевает показ всплывающих рекламных окон на тематических площадках.

- Телевизионная реклама. Это тоже достаточно дорогой способ по сравнению с интернет-рекламой, зато позволяет захватить максимальную аудиторию различных возрастов.

- СМС-рассылки, Email-маркетинг. Рассылка рекламных сообщений. Одним из плюсов является то, что реклама рассылается людям, которые уже имели знакомство с брендами и предложениями компании, а значит выше вероятность продажи продукта или услуги.

– Нативная реклама. Она заключается в публикации на сторонних ресурсах «естественных» отзывов и мнений, подталкивающих к покупке товара или услуги.

– QR-коды в offline. Направлено на то, чтобы потребитель устанавливал приложение. Так создается практически постоянный контакт с потребителем.

– Вирусная реклама. Направлена на создание контента, который пользователи или владельцы социальных сетей будут сами распространять в сети (делиться в соцсетях с друзьями, в блогах и т.п.).

Цифровые развлечения и цифровой маркетинг всегда идут рука об руку. Люди, которые подписаны на влиятельных людей в социальных сетях, получают внушительное количество рекламы. Цифровые товары продаются почти в каждой видео игре, а всплывающая реклама и аналогичные товары – в каждом приложении.

В наше время люди все больше уходят в цифровой мир и нельзя не упомянуть сферу контента и развлечений. Раньше для получения эмоций необходимо было ходить в театр, кинотеатры, парки, стадионы, но сейчас есть новая инфраструктура с возможностью передачи какого-либо развлекательного контента на большее расстояние, на большее количество потребителей, следовательно, получать больше итогового дохода. Локдаун из-за коронавирусной инфекции COVID-19 явно показал недостаток развлекательного контента. Киностудиям пришлось перестраивать свои бизнес-модели и предоставлять свой продукт в потоковых сервисах, а снимающиеся картины – переносить на более поздний срок.

На данный момент наблюдается рост доли рынка цифровых развлечений и сервисов их предоставляющие. Например, согласно отчету компании Netflix итоговая прибыль составила в 2019 году – 1,8 миллиардов долларов, в 2020 году - 2,7 миллиарда долларов, а количество подписчиков достигло порядка 203,7 миллионов в 190 странах. На мировом рынке главную конкуренцию ему составляет Amazon Prime Video от Amazon с 150 миллионами подписчиков. Тем не менее, своим успехом сервис обязан грамотной стратегии цифрового маркетинга. Не секрет, что в маркетинге активно используют социальные сети, и Netflix не отстает от тренда. При этом digital-маркетологам сервиса не приходится вкладываться в спонсорские посты, они создают оригинальный контент, которым хочется поделиться. Так многие посты становятся вирусными и разлетаются по сети. Причем подписчики активно комментируют посты и обсуждают с друзьями, что показывает высокую вовлеченность аудитории.

На сегодняшний день в мире проживает 7,8 миллиарда человек и по данным на 31 марта 2021 года 5,1 (65,6%) из них используют интернет. [5]

Каждый год We Are Social и Hootsuite составляют статистику о состоянии мирового интернета - Digital 2021. Но с учетом того, что COVID-19 продолжает препятствовать исследованиям, реальные цифры могут быть значительно выше.

Состояние цифровых технологий в октябре 2021 [6]: количество уникальных интернет пользователей составила 4,88 миллиарда человек; за последние 12 месяцев к платформам социальных сетей присоединилось более 400 миллионов новых пользователей и их общее число составило 4,55 миллиарда. В среднем интернет пользователь тратит 1 час 13 мин на видео игры, 57 мин на прослушивание контента подкастов, 2 часа 27 мин – социальные медиа, 3 часа 21 мин на просмотр телевизора (телепередачи и потоковое).

С каждым годом эти числа растут, как и количество рекламы. В 2020 году 47% пользователей использовали блокировщик рекламы. [7]

Воздействие COVID-19 на потребителей привело к существенному росту онлайн-продаж.

В 2021 году выручка на видео игры 155,3 миллиардов долларов, музыку – 25,06 миллиардов долларов, видео (телепередачи и потоковое) – 85,75 миллиардов долларов. [8]

Таким образом, бизнес идет в сеть и направляет свои маркетинговые ресурсы в online. Определенно digital-продвижение стало новым эволюционным этапом в сфере маркетинга. Информационные технологии тесно переплелись с жизнью каждого человека, что последний уже не мыслит жизни без них. В настоящее время информационные технологии широко используются в маркетинге. Уже невозможно собрать и обработать огромные массивы информации без использования компьютерной техники и специального программного обеспечения. Но и отдача от подобных вложений колоссальна. Статистика интернета показывает digital-маркетологам как обеспечить эффективность бизнеса, конкурентоспособность товара или услуги и на какие рынки можно входить.

Список использованных источников:

1. «Что такое диджитал-маркетинг? Про основы, принципы и технологии», 2021. [В Интернете]. Available: <https://marketing.hse.ru/news/452686021.html>
2. А. Скороходова, «Digital Marketing – универсальный игрок на поле маркетинга», [В Интернете]. Available: https://www.comagic.ru/blog/posts/jun/digital_marketing_universalnyy_igr_ok_na_pole_marketinga/.

3. «Digital-маркетинг». [В Интернете]. Available: <https://blog.ingate.ru/seo-wikipedia/digital-marketing/>.
4. Д. Трепольский, «Как digital-маркетинг сделал Netflix гигантом индустрии развлечений», 2020. [В Интернете]. Available: <https://delovoymir.biz/kak-digital-marketing-sdelal-netflix-gigantom-industrii-razvlecheniy.html>.
5. Internet World Stats. [Электронный ресурс]. Available: <https://www.internetworldstats.com/stats.htm> (дата обращения: 04.11.2021).
6. Simon Kemp, «Digital 2021 october global statshot report», 2021. [В Интернете]. Available: <https://datareportal.com/reports/digital-2021-october-global-statshot/>.
7. Statcounter GlobalStats. [Электронный ресурс]. Available: <https://gs.statcounter.com/> (дата обращения: 04.11.2021).
8. Stasista. [Электронный ресурс]. Available: <https://www.statista.com/> (дата обращения: 04.11.2021).

Информационные технологии, как маркетинговый инструмент развития в сфере оптимизации бизнес-процессов

В.А. Чекунова

студент 4 курса НИЯУ МИФИ, Москва

E-mail: v.a.chekunova@gmail.com

А.Н. Норкина

к.э.н., заместитель директора ИФТЭБ НИЯУ МИФИ, Москва

E-mail: ANNorkina@mephi.ru

Аннотация: Актуальность вопроса оптимизации бизнес-процессов на предприятиях остается неизменной, что способствовало распространению и повсеместному использованию информационных технологий в ежедневной работе. Данная статья посвящена анализу преимуществ использования информационных технологий в рамках функционирования предприятий во время пандемии.

Ключевые слова: бизнес-процессы, информационные технологии, оптимизация бизнес-процессов, информационный маркетинг.

Information technology as a marketing tool for development in business processes optimization

Abstract: The issue of optimization of business processes in enterprises remains unchanged, which has contributed to the spread and widespread use of information technology in daily operations. This article analyses the benefits of using information technology in enterprise operations during the pandemic.

Keywords: business processes, information technology, business processes optimization, information marketing.

Рыночная экономика всегда была и остается динамичной и требует от своих игроков готовности к адаптации под текущую ситуацию. Последние изменения на рынке обусловлены влиянием пандемии, что сказалось на функционировании многих компаний в различных сферах и отраслях по всему миру. Ряд ограничительных мер, предпринятых в рамках предотвращения распространения коронавирусной инфекции, существенно повлиял на подходы к управлению в компаниях. В связи с событиями последних двух лет многие предприятия и организации столкнулись с определенными ограничениями реализации деятельности, а

также возникли определенные однотипные вопросы, которые необходимо было решить для поддержания дальнейшего функционирования на должном уровне.

Целью данной работы является изучение предметной области в сфере оптимизации бизнес-процессов, изучение тенденций модернизации функционирования организаций в мире и в России.

В соответствии с поставленными целями определены задачи:

1. Изучение предметной области;
2. Исследование влияния пандемии на мировые и российские организации;
3. Выявление преимуществ использования информационных технологий в текущей ситуации.

В процессе исследования использованы следующие методы:

1. Сбор и анализ статистических данных.

Вопрос необходимости управления и оптимизации бизнес-процессов на предприятиях в настоящее время получил широкое распространение как на российском рынке, так и на мировой арене. Но прежде чем рассматривать последствия влияния пандемии на деятельность компаний, необходимо разобратся в предметной области.

Любую деятельность предприятий можно рассматривать как комплекс взаимосвязанных внутренних и внешних бизнес-процессов, нацеленных на достижение поставленных перед предприятием целей и задач, а также создания продукции или услуги для удовлетворения как внешних, так и внутренних потребителей. При этом у каждого бизнес-процесса можно выделить вход и выход, необходимые для реализации ресурсы, владелец, основные поставщики и потребители процесса, а также ряд показателей, по которым оценивается эффективность бизнес-процесса.

Зачастую от уровня и полноты понимания того, что и как происходит внутри предприятия, зависит уровень качества выполняемой работы, эффективность бизнеса, а также сроки достижения поставленных целей. Для этого необходимо вести документацию существующих бизнес-процессов и своевременно вносить изменения в случае моделирования новых цепочек взаимосвязанных процессов, оптимизации или реинжиниринга. Согласно концепции уровней зрелости процессов (Владимир, 2012) (CMMI – capability maturity model integration), представленной ниже в таблице 1, данный шаг реализуют предприятия, находящиеся на третьем уровне зрелости.

Таблица 1 – Описание уровней зрелости бизнес-процессов по модели CMMI

Уровень зрелости	Описание процессов
1 уровень (начальный)	Процессы не определены, нет документации по процессу. Такие процессы характеризуются высоким

	уровнем непредсказуемости, большими временными и финансовыми затратами.
2 уровень (повторяемый)	Определены основные процессы, можно использовать неоднократно. Идет снижение временных затрат.
3 уровень (определенный)	Определена основная часть процессов на уровне всего предприятия. Большая часть описана более детально и определены взаимосвязи между процессами.
4 уровень (управляемый)	Все процессы определены, подлежат систематическому анализу и управлению в случаях, требующих изменения.
5 уровень (оптимизируемый)	Все процессы определены и документированы, находятся в процессе непрерывного улучшения.

В теории, любому предприятию или организации необходимо стремиться к последнему уровню зрелости - оптимизируемому. Как показывает практика, многие предприятия и организации ведут свою деятельность, находясь на первом или втором уровнях зрелости. Тем не менее этап моделирования и описания бизнес-процессов остается одним из важнейших этапов в функционировании предприятия.

Однако события последних лет поставили перед необходимостью пересмотра бизнес-модели, по которой функционировали многие предприятия, а также пересмотра бизнес-процессов. Те, у кого были определены все процессы (другими словами – находящиеся хотя бы на третьем уровне зрелости), не потерпели временные и финансовые затраты на моделирование и описание внутренних и внешних бизнес-процессов, а смогли оперативно приступить к анализу текущих бизнес-процессов для дальнейшего рассмотрения возможности улучшения и функционированию организации в целом, тем самым на тот момент уже были более конкурентоспособными.

Согласно Федеральному закону №149-ФЗ «Об информации, информационных технологиях и о защите информации» (ФЗ121) информационные технологии характеризуются процессами, методами поиска, сбора, хранения, обработки, предоставления, распространения информации и способами осуществления таких процессов и методов.

Динамичное развитие цифровых технологий в наше время требует оперативных мер реагирования на внешнеэкономические изменения, быстроты принятия решений, внесения изменений в деятельность компаний. Использование информационных технологий, а именно специализированных программных решений позволяют вести свою работу более оперативно и эффективно. Рассмотрим ряд ключевых преимуществ:

1. Получение актуальной информации по текущим бизнес-процессам и обстановке на предприятии в целом;
2. Устранение неэффективных бизнес-процессов;
3. Моделирование и документирование актуальных бизнес-процессов в целях дальнейшего использования в рамках функционирования предприятия;
4. Сокращение временных, финансовых и трудовых ресурсов, которые можно перенаправить на создание новых проектов/товаров/услуг, за счет автоматизация типовых бизнес-процессов;
5. Повышение качества предоставляемых услуг.

Все эти и многие другие функции реализуются в программных решениях в сфере BPM (управление бизнес-процессами). Большинство программных продуктов поддерживают следующее:

1. Управление бизнес-процессами реализуется непрерывно;
2. Предоставление мониторинга и администрирования не только процессов, но и вовлеченных специалистов;
3. Диагностика и прогнозирование развития процессов;
4. Оперативное внедрение в цепочку бизнес-процессов новых процессов;
5. Различные методы описания бизнес-процессов (графический вид, с использованием специализированных методологий).

С помощью использования подобных систем повышается качество предоставляемых услуг, снижаются временные и финансовые затраты, а также позволяют открыто управлять деятельностью предприятия.

В связи с последними событиями в мире за последние два года следует рассмотреть и изменения, произошедшие в работе компаний. Согласно результатам совместного исследования (РБК) от «РБК Исследования рынков» и SAP CIS в 2020 году около 62% компаний ощутили негативное влияние пандемии на бизнес. При этом 56% респондентов отметили о существенном влиянии ограничительных мер по работе компаний, а также по перемещению сотрудников на функционирование организаций в целом. Переход на удаленный режим работы, перевод многих процессов организаций потребовали пересмотра текущей бизнес-модели, а также пересмотр самих бизнес-процессов. Также в рамках исследования от РБК респонденты были опрошены о том, какие бизнес-процессы потребовали пересмотра и модернизации в первую очередь. В ТОП-5 наиболее распространенных бизнес-процессов вошли следующие процессы:

1. Управление персоналом (53%)
2. Маркетинг (51%)
3. Планирование и управление (51%)
4. Продажи онлайн (51%)

5. Закупки (37%)

При этом было отмечено, что большинство компаний, проходящих опрос, использовали специальные программные решения для оптимизации и автоматизации многих процессов. Результаты данного опроса представлены на рисунке №1.

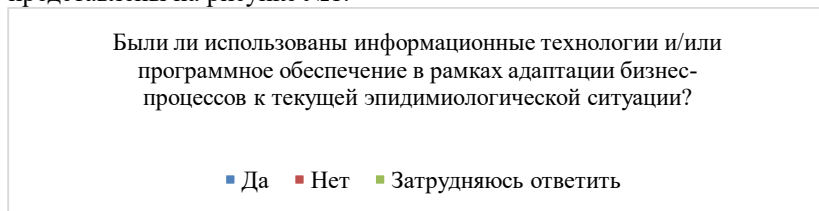


Рисунок 1 – Результаты опроса из исследования РБК

Кроме того, большинство респондентов, учувствовавших в исследовании, отметили, что предпочли использовать уже готовые программные решения от мировых и российских производителей вместо разработки собственного, что могло значительно потребовать как финансовых, так и временных затрат. Рассмотрим специализированные информационные технологии, а именно BPM-системы.

В общих чертах BPM – это целостный, процессно-ориентированный подход к принятию управленческих решений, который направлен на улучшение способности компании оценивать свое состояние и управлять эффективностью деятельности на всех уровнях, объединяя усилия собственников, менеджеров, персонала и внешних контрагентов в рамках общей интегрированной среды управления. На данный момент рынок содержит множество информационных систем (BPM-систем, другими словами BPMS), каждая из которых определенным образом создана для полного управления бизнес-процессами, а именно стратегией, проектированием, внедрением, контролем.

Рассмотрим наиболее популярных представителей BPM-систем мирового производителя IBM (IBM) и отечественного производителя ELMA (ELMA). Сравнительный анализ двух систем будет проводиться по некоторым ключевым показателям, которые необходимо исполнять в рамках полного управления бизнес-процессами. Результаты представлены в таблице 2.

Таблица 2 – Сравнительный анализ ELMA BPM и IBM BPM

Критерии	ELMA BPM	IBM BPM
Наличие пробной версии	+	+
Стоимость	От 1200 рубл. /месяц	От 600\$
Облачное решение	+	+
Моделирование		

Поддержка нотации BPMN для моделирования бизнес-процессов	+	+
Импорт и экспорт регламентов по реализованным бизнес-процессам	+	+
Графическое моделирование	+	+
Импорт моделей бизнес-процессов, описанных с помощью других нотаций	-	+
Наличие инструмента проверки на эффективность и внесения изменения в бизнес-процессы	+	+
Исполнение		
Наличие инструмента по построению очереди исполнения определенных бизнес-процессов а назначенное время	+	-
Запуск как отдельных бизнес-процессов, так и цепочку взаимосвязанных из внешних систем	+	-
Контроль		
Механизмы комплексного мониторинга исполнения бизнес-процессов	+	+
Механизмы контроля эффективности сотрудников	+	+
Механизмы прогнозирования значений показателей по эффективности реализации бизнес-процессов	-	+
Улучшение		
Управление изменениями в процессах	+	+
Возможность оперативно вносить изменения в случаях, когда это необходимо сделать в короткий срок	+	+

Проведя сравнительный анализ, можно сказать, что ELMA BPM и IBM BPM в целом похожи, так как многие необходимые функции реализованы в обеих системах. Использование подобных информационных систем позволяет компаниям поддерживать свою конкурентоспособность на рынке, быстро реагировать на изменения в сферах реализации их деятельности, в том числе и пересматривать свои бизнес-модели и оптимизировать малоэффективные бизнес-процессы.

Подводя итоги, можно сказать, что вопрос управления и оптимизации бизнес-процессов как никогда актуален. Без мониторинга ситуации на

рынке, без своевременной адаптации, предприятия и компании не смогут оставаться конкурентоспособными и уровень эффективности их деятельности будет неукоснительно падать. Одним из способов изменения данной ситуации остается использование специализированных информационных технологий в рамках управления и оптимизации бизнес-процессов.

Список использованных источников:

1. Basel institute on Governance [Статья] = Cryptocurrencies and money laundering investigations / авт. Senior Financial Investigation Specialist Paesano Federico. - Базель : Basel institute on Governance, 2021 г.. - Т. 1.
2. BBC News journal [Статья] = El Salvador Bitcoin city planned at base of Conchagua volcano / авт. journal BBC News. - Latin American country : BBC News journal, 2021 г..
3. BPM-система ELMA365 [В Интернете] / авт. ELMA. - 8 11 2021 г.. - <https://elma365.com/ru/products/bpm/>.
4. Facing the sanctions challenge in financial services.A global sanctions compliance study / авт. Deloitte. - [б.м.] : Deloitte, 2009 г..
5. Federal Reserve Bank of Cleveland [Статья] = Bitcoin's Decentralized Decision Structure / авт. Cleveland Federal Reserve Bank of. - Cleveland : Federal Reserve Bank of Cleveland, 2019 г..
6. Forbes [Статья] = A Former Bank Of England Governor Warned The 2008 Crash That Inspired Bitcoin Could Happen Again / auth. Bambrough Billy / ed. Bambrough Billy. - [б.м.] : Forbes ; Bambrough, Billy, Октябрь 27, 2019.
7. How-To Geek [Публикация] = How Anonymous Is Bitcoin? / авт. O'SULLIVAN FERGUS. - [б.м.] : FERGUS O'SULLIVAN, @fergusosullivan (twitter), 2021 г..
8. Know Your Customer in banking [В Интернете] / авт. Group Thales // Digital Identity and Security. - 2020 г..
9. Sanctions compliance: Plotting a new course for sanctions compliance with technology solutions that drive efficiency and effectiveness. [В Интернете] / авт. International KPMG // KPMG. - 2020 г..
10. The verge [Публикация] = Feds arrest founder of bitcoin 'mixer' they say laundered \$335 million over ten years / авт. Lyons Kim. - [б.м.] : Kim Lyons, @SocialKimLy, 2021 г..
11. We've all heard of sanctions, but how could they impact your business? Here's all you need to know about sanctions. [В Интернете] / авт. KYC-Chain // Sanctions 101. - 5 февраль 2020 г..
12. Аналитический отчет по результатам исследования "Е - commerce 2021" / авт. E-Promo. - 2021 г..

13. Бизнес-процессы. Моделирование, внедрение, управление. [Книга] / авт. Владимир Репин. - 2012.
14. Веб-аналитика 2.0 на практике. Тонкости и лучшие методики (+ CDROM) [Книга] / авт. Кошик Авинаш. - [б.м.] : М.: Диалектика.
15. ГОСТ Р 56020-2020 "Бережливое производство. Основные положения и словарь" [В Интернете]. - 2021 г.. - <https://docs.cntd.ru/document/1200174885>.
16. ГОСТ Р ИСО/МЭК 17799-2005 "Практические правила управления информационной безопасностью" [В Интернете]. - <https://docs.cntd.ru/document/1200044724>.
17. Иновации и инвестиции [Статья] = Государственная система мониторинга операций в криптовалюте / авт. Кандидат экономических наук доцент, доцент кафедры экономической безопасности СПбГАУ Дурандина Анна Павловна. - Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, 2021 г.. - Т. 2.
18. Исследование влияния пандемии COVID-19 на российский бизнес [В Интернете] / авт. РБК. - 2 11 2021 г.. - https://sapmybiz.rbc.ru/RBK_Issledovanie_vliyaniya_pandemii_COVID_19_na_rossiyskiy_biznes.pdf.
19. Исследование роли веб-аналитики в повышении эффективности деятельности организации [Журнал] / авт. Демкина О.В. Шаламова Н.Г.. - [б.м.] : / О.В.Демкина, Н.Г. Шаламова // Вестник университета., 2019 г.. - №5, -С. 56-61.
20. Исследование российского рынка programmatic buying / авт. PWC. - 2021 г..
21. Международные санкции: что следует учитывать российским компаниям? [Конференция] / авт. С.В. Гландин // «Санкционный комплаенс как способ минимизации рисков для бизнеса».. - 31 марта 2021.
22. Научно-образовательный журнал для студентов и преподавателей "StudNet" [Статья] = Безопасность финансовой системы в рамках появления криптовалюты / авт. Попов В.Г Галиаскаров Д.Ф, Киселев И.Д. - Москва : Научно-образовательный журнал для студентов и преподавателей "StudNet", 2021 г.. - Т. 4.
23. Обзор IBM Business Process Manager [В Интернете] / авт. IBM. - 8 11 2021 г.. - <https://www.ibm.com/docs/ru/bpm/8.6.0?topic=manager-business-process-overview>.
24. Объем рекламы в средствах ее распространения в январе-июне 2021 года [В Интернете] // Ассоциация Коммуникационных Агенств России.

- 2021 г.. - ноябрь 2021 г.. -
https://www.akarussia.ru/knowledge/market_size/id9802.
25. Определение понятия и содержания инфраструктуры логистики [В Интернете] / авт. Детлеф Венде Франк Рыкалина Ольга, Степанов Владимир. - 2014 г.. - <https://elibrary.ru/item.asp?id=22744028>.
 26. РБК.Крипто [Статья] = Минфин предложил ужесточить регулирование криптовалют в России / авт. Теткин Михаил. - Москва : Михаил Теткин, 2020 г..
 27. Санкции и односторонние ограничительные меры: проблема различия терминов и тождественности явлений [Статья] / авт. Пятибратов И.С. // Вестник Финансового университета. - 2020 г..
 28. Санкционный комплаенс в 2019 г.: тенденции и новые веяния [Журнал] / авт. INSIGHT LEGAL. - 2019 г..
 29. Сквозная аналитика: система, примеры и инструменты [В Интернете] // Центр развития компетенций в маркетинге НИУ ВШЭ. - 2020 г.. - ноябрь 2021 г.. - <https://marketing.hse.ru/news/397981286.html>.
 30. Справка - Google Analytics [В Интернете]. - ноябрь 2021 г.. - <https://support.google.com/analytics/?hl=ru>.
 31. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 02.07.2021) "Об информации, информационных технологиях и о защите информации" [Книга].
 32. ФЗ № 149-ФЗ [В Интернете]. - 30 10 2021 г.. - http://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233a cca771e9adb35b47d3fb82c9ff1c/.
 33. Яндекс.Метрика [В Интернете] // Яндекс справка. - ноябрь 2021 г.. - <https://yandex.ru/support/metrika/>.

Использование инструментов искусственного интеллекта при разработке программного обеспечения в контексте ПОД/ФТ

В.Р. Баринов
преподаватель кафедры «Инфокогнитивные Технологии», Московский
Политехнический Университет, Москва
Email: inarael@yandex.ru
Н.В. Баринова
к.э.н., ведущий специалист отдела научных мероприятий РЭУ им. Г.В.
Плеханова, Москва
Email: barinova23@mail.ru

Аннотация: В статье рассматриваются вопросы применения современных информационных технологий в финансово-экономической сфере. Стремительные темпы информатизации и возрастание объёмов транзакций и электронных платежей диктуют необходимость мониторинга рисков ПОД/ФТ и применения современного программного обеспечения на основе алгоритмов работы с неструктурированными данными, машинного обучения, графовых структур и нейросетей. В статье также обозначены направления подготовки квалифицированных кадров для работы в данном направлении.

Ключевые слова: ПОД/ФТ, машинное обучение, программный продукт, финансовые операции, мониторинг.

Use of artificial intelligence tools in software development in the context of AML / CFT

Abstract: The article discusses the application of modern information technologies in the financial and economic sphere. The rapid pace of informatization and the increasing volume of transactions and electronic payments dictate the need to monitor AML/CFT risks and use modern software based on algorithms for working with unstructured data, machine learning, graph structures and neural networks. The article also outlines the directions of training qualified personnel to work in this direction.

Keywords: AML/CFT, machine learning, software product, financial transactions, monitoring.

Современная жизнь характеризуется стремительными темпами развития информационных технологий. Информационные технологии используются во всех областях жизни, но особенно широкое применение они получили в финансово-экономической сфере. В каждый момент времени по всему миру осуществляется огромное количество транзакций. Поэтому в последние годы значительно возросла необходимость организации и эффективного мониторинга финансовых операций в контексте ПОД/ФТ.

Как уже отмечалось выше, ежесекундно во всем мире происходит колоссальное количество транзакций. Применяемые системы мониторинга должны иметь возможность обработки сверхбольших объёмов данных, в том числе неструктурированных. Большинство СУБД, применяемых в финансово-экономической сфере в последние десятилетия настроены преимущественно на реляционные БД, так как они имеют упорядоченную структуру, что в свою очередь, определяет тип программного обеспечения для их обработки. В то же время сегодня имеется большое количество записей с неструктурированными данными, к которым не применимы методы обработки для реляционных БД.

Для решения задач, содержащих неструктурированные данные, следует применять программные продукты, созданных на основе других алгоритмов, отличных от используемых при работе с реляционными БД. При этом их важной составляющей является возможность подстраивания под изменяющиеся условия пользователя.

Наиболее известными программными продуктами в области ПОД/ФТ, используемыми на сегодняшний момент в финансово-кредитной и государственной сфере являются: Attivio, BAE Systems, FICO TONBELLER, Fiserv, IdentityMind, NICE Actimize, OutsideIQ, SAS. Большинство из них уже обладают этими характеристиками, но некоторые из систем (напр. Fiserv, NICE) пока не обладают такими возможностями, что требует их программной доработки.

В последние годы значительно возросли не только объёмы финансово-экономической информации, что во многом затрудняет применение некоторых программных продуктов, но и появилось большое количество электронных валют, механизм работы с которыми отличен от традиционных расчётов. При работе с такими платежами необходимо применение новых программных средств и инструментов, основанный на графовых структурах, машинном обучении и использовании нейросетей, которые способны самообучаться и выявлять скрытые связи, которые невозможно выявить иными средствами [1].

Так, например, в рамках борьбы с мошенничеством компания PayPal использует проприетарный инструмент, который сравнивает миллионы

транзакций и обнаруживает среди них подозрительные. Результатом использования этого программного обеспечения стало снижение количества мошеннических транзакций по сравнению с стандартным уровнем в финансовом секторе — 1,32% до 0,32% в PayPal [10]

Исследователи Прасолов В.В., Фешина С.С. пишут, что использование нейронных сетей позволит построить более совершенные поведенческие прогнозы при помощи выстраивания потенциальных вариантов событий. Если создать алгоритм развития событий на основе определенных критериев и возможных вариантов дальнейшего сценария и выбрать из них оптимальный, то такой вариант можно представить как наиболее рациональный и обучить нейросеть [7]. Аналогичные исследования изложены в работе авторов Чмырь Ю.Н., Михальской Л.С., которые посвящены риск-ориентированному подходу в сфере ПОД/ФТ [9].

Заслуживают внимания исследования в информационной области, опубликованные группой ученых Карповой Е. Н., Колесник И.А., Коноваловым А.А. Большинство цифровых систем, в частности Attivio и OutsidelQ имеют возможность автоматического анализа потоков данных, в том числе получаемых из социальных сетей, а также имеют возможности кластеризации данных, что, безусловно, является прорывными технологическими решениями в информационной области. [5].

По данным, опубликованным компанией Juniper Research, исследователями было сделано заключение о том, что к 2020 году эффективность методов защиты от мошенничества, основанных на использовании искусственного интеллекта, значительно возросла и представляет из себя хороший «щит» против преступников. Это связано с тем, что к данному моменту накопилось достаточно большое количество данных о моделях, которые обычно используют кибер-преступники, отмечает Джон Джонстон в своей работе. С другой стороны, в этой же работе отмечается и необходимость дальнейших разработок в этой сфере, что связано со значительной популяризацией нового метода — использования поддельных данных. Согласно прогнозам, потери на таком виде мошенничества вырастут на 130% к 2024 году. Именно поэтому Джонстон, Морроу и Мейнард предлагают развивать системы, основанные на использовании машинного обучения, теперь уже в направлении распознавания поддельных аккаунтов и кредитных карт. С помощью правильных данных получится определить разницу между мошенником и обычным клиентом. Основной проблемой данного способа мошенничества является отсутствие возможности у злоумышленников имитации ваших вкусов, поведения и истории покупок, именно в этом направлении и предлагается провести исследования. [11]

Большие возможности для обработки и анализа неструктурированных данных предоставляют программные решения, основанные на графовых структурах. Их основным преимуществом являются алгоритмы с возможностью обработки данных различных типов, а также трансформаций под различные типы задач, что особенно важно в изменяющихся экономических условиях.

Исследователи Лашенко Р.А., а также Воробьев В.А., Захарчук Е.А. опубликовали исследования о современных проблемах в системах финансового контроля. Как указывает Лашенко Р.А, большинство традиционных систем слежения за сомнительными транзакциями настроены таким образом, что обнаруживают подозрительные типологии, которые достаточно легко можно обойти. При этом настройка данных систем проведена таким образом, что призвана блокировать максимальное количество сомнительных операций с целью недопущения пропусков подозрительных операций. При этом результаты такой обработки образуют достаточно большой массив данных для ручной перепроверки. Если же снизить некоторые пороговые значения, то данный массив данных еще больше увеличится и существует вероятность пропуска сомнительных транзакций. [2, 6]

В этой связи необходимо отметить, что создание программного обеспечения на основе систем искусственного интеллекта имеет большие перспективы, так как обладает возможностями поиска и анализа скрытых данных, которые нельзя обнаружить с помощью традиционных алгоритмов. [3, 8]

Обратим внимание на важный момент. Важно не только разработать программное обеспечение, отвечающее потребностям организации, но и эффективно его использовать. Как известно, внедрение и отладка новых информационных систем в финансовых организациях в среднем занимает временной интервал от одного до полутора лет, даже в тех, где аналогичное программное обеспечение уже использовалось.

Не менее важным моментом, на который стоит обратить внимание, является кадровый. Стоит согласиться с исследователями Ищановой Р.К., Турмаханбетовой Г.А., Исаковой З.Д. одним из наиболее важных вопросов в области ПОД/ФТ являются вопросы подготовки кадров высокой квалификации, обладающих современными компетенциями в данной области. [4].

Для успешной реализации этого направления, необходимо решить ряд задач: подготовка профильных специалистов в ВУЗе для работы в финансовой области и специалистов, непосредственно не связанных с осуществлением финансовых операций, обеспечивающих консультационные и иные виды действий, а также направление

переподготовки кадров и повышения уровня квалификации сотрудников, работающих в данной сфере.

Сформулируем основные задачи для каждого направления:

- Для специалистов первого направления (выпускников ВУЗа) необходимо разрабатывать дополнительные модули в образовательных программах, связанные с изучением юридических вопросов в сфере ПОД/ФТ, возможностей информационных ресурсов, систем искусственного интеллекта для определения сомнительных операций;

- В направлении обучения специалистов-консультантов необходимо создание открытых ресурсов по повышению финансовой грамотности населения (в том числе онлайн ресурсов), а также обучение работающих специалистов-консультантов основам психологических особенностей различных групп населения по профилактике финансовых рисков;

- В направлении переподготовки и повышения уровня квалификации специалистов необходимо обеспечить разработку и внедрение современных программ обучения на основе последних достижений в информационных, экономических, юридических областях наук, а также с учётом государственной политики в данной области (в том числе онлайн программ).

В заключение, стоит отметить, что разработки в сфере машинного обучения направленные на ПОД/ФТ являются наиболее перспективными, что связано с тем, что данные методы позволяют качественно выявлять и предотвращать сомнительные транзакции. В последние годы мошенники ищут и находят всё новые и новые способы «пробивания» защиты информационных систем. Поэтому сегодня существует большая потребность в разработке контрмер к новым вызовам кибер-преступников. В этой области перспективы машинного обучения поистине безграничны.

Список использованных источников:

1. Баринов В.Р. Возможности применения программного обеспечения на основе ориентированно детерминированных графов для выявления манипуляций в финансово-экономической сфере в контексте ПОД/ФТ В сборнике: Система ПОД/ФТ в глобальном мире: риски и угрозы мировой экономики. Сборник тезисов докладов участников V Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ. 2020. С. 103-106.
2. Воробьев В.А., Захарчук Е.А. Проблемы государственного контроля и надзора над современными финансово-техническими инструментами. Социальные и экономические системы. 2021. № 2 (20). С. 155-164.
3. Гладкова С.Б. Обеспечение безопасности банковской системы в контексте противодействия легализации доходов, полученных

- преступным путем. В сборнике: Архитектура финансов: форсаж-развитие экономики в условиях внешних шоков и внутренних противоречий. Сборник материалов X Юбилейной международной научно-практической конференции. Под научной редакцией И.А. Максимцева, Е.А. Горбашко, В.Г. Шубаевой. 2020. С. 22-25.
4. Ищанова Р.К., Турмаханбетова Г.А., Исакова З.Д. Кадры как решающий фактор в борьбе с теневыми финансовыми потоками в контексте эффективной системы ПОД/ФТ. В сборнике: Актуальные проблемы формирования эффективной системы ПОД/ФТ. Материалы Всероссийской с международным участием научно-практической конференции студентов, аспирантов и молодых ученых. 2019.С.104-110
 5. Карпова Е.Н., Колесник И.А., Коновалов А.А. Современные тенденции в области цифровизации внутреннего контроля в целях противодействия отмыванию преступных доходов и финансированию терроризма в кредитных организациях Карпова Е.Н., Колесник И.А., Коновалов А.А. Фундаментальные исследования. 2020. № 4. С. 52-56.
 6. Лашенко Р.А. Использование систем искусственного интеллекта и машинного обучения в целях предупреждения преступлений в сфере легализации (отмывания) денежных средств или иного имущества приобретенного преступным путем Лашенко Р.А. В сборнике: Научное обозрение. сборник статей Международного научно-исследовательского конкурса. Пенза, 2021. С. 216-219.
 7. Прасолов В.И., Фешина С.С. Влияние цифровой трансформации на процессы выявления легализации доходов, полученных преступным путем. Экономика: вчера, сегодня, завтра. 2020. Т. 10. № 8-1. С. 130-145.
 8. Хамидов Л.Ж.У., Кудревич В.В. Применение информационных технологий в рамках финансовой разведки: проблемы и перспективы. В сборнике: Финансово-экономическое и информационное обеспечение инновационного развития региона. Материалы III Всероссийской научно-практической конференции с международным участием. Ответственный редактор А.В. Олифиров. 2020. С. 388-391.
 9. Чмырь Ю.Н., Михальская Л.С. Риск-ориентированный подход в сфере ПОД/ФТ: отечественный и зарубежный опыт. В книге: Оценка социально-экономического развития: опыт и перспективы. Тезисы докладов и выступлений III Международной научно-практической конференции студентов и молодых ученых. Общая редакция О.Н. Головинова. 2019. С. 173-175.
 10. C. B. Frey M. A. Osborne. The future of employment: How susceptible are jobs to computerisation? Oxford, 2013.
 11. Susan Morrow, Nick Maynard Online payment fraud: Emerging threats, Segment analysis & Market forecasts 2021-2025; Juniper Research; 2021

Использование средств визуального анализа при расследовании операций с виртуальными активами

А.К. Вязникова

студентка 5 курса НИЯУ МИФИ, Москва

E-mail: s.vznkv@gmail.com

А.В. Кирина

студентка 5 курса НИЯУ МИФИ, Москва

E-mail: nstkirina@yandex.ru

Д.В. Домашова

доцент кафедры финансового мониторинга НИЯУ МИФИ, Москва

E-mail: janedom@mail.ru

Е.Е. Писарчик

директор по аналитике, ООО CBS

E-mail: episarchik@cbrains.ru

Аннотация: Возможность визуального анализа транзакций дает доступ к качественному анализу и поиску новых признаков совершения преступлений связанных с отмыванием денег и финансированием терроризма. В статье представлены результаты рассмотрения и визуализации операций с виртуальными активами, связанных с нелегальной деятельностью.

Ключевые слова: виртуальные активы, криптовалюта, блокчейн, визуализация, ПОД/ФТ, ХАМАС, OTC Exchange, SUEX.

The application of visual analysis tools in the investigation of transactions with virtual assets

Abstract: The ability to visualize analysis of transactions gives access to thorough analysis and search for new red-flags of crimes related to money laundering and terrorist financing. The article presents the results of the review and visualization of transactions with virtual assets related to illegal activities.

Keywords: virtual assets, cryptocurrency, blockchain, visualization, AML/CFT, HAMAS, OTC Exchange, SUEX.

Создание новых средств оплаты, таких как цифровые валюты, не обеспеченные золотом, или другими драгоценными металлами, - новый, но достаточно стремительно набирающий темп процесс на международной

арене. Нормативные базы еще не регулируют все возможные аспекты деятельности, связанные с ним, а резкий скачок популярности виртуальных активов создает большое количество рисков и угроз не только для экономики, но и является удобным инструментом для финансирования терроризма и экстремизма.

Данное явление в различных источниках может обозначаться различными понятиями: «виртуальные деньги», «виртуальные активы», «цифровые деньги», просто «криптовалюты», что можно объяснить следующим образом:

1. Сложности перевода – каждая страна называет новое явление как ей удобнее, языковые группы начинают это адаптировать по-своему в зависимости уже от состоявшейся нормативно-правовой базы.

2. Развитие самой системы и регуляторных требований означает то, что раньше попадало под понятие «виртуальной валюты» сейчас уже не полностью покрывает все возможности или не удобно для актуализации нормативно-правовых актов (НПА). Тем самым создаются новые названия для того же явления.

С этой целью будем использовать определение «виртуальных активов», взятое из руководства Группы разработки финансовых мер по борьбе с отмыванием денег (ФАТФ) «Виртуальные активы и провайдеры виртуальных активов» [1]:

«Виртуальные активы (ВА) — это цифровое выражение ценности, которое может цифровым образом обращаться или переводиться и может быть использовано для целей платежа или инвестиций. Виртуальные активы не включают в себя цифровое выражение фиатных валют, ценных бумаг и других финансовых активов, которые уже покрыты где-либо в Рекомендациях ФАТФ».

В отчете ФАТФ, посвященном виртуальным активам [2], выделен ряд признаков отмывания денег и финансирования терроризма (ОД/ФТ) посредством криптовалюты. Все они схожи с признаками, характерными для фиатных денег, в тех случаях, когда они используются в нелегальных целях.

Основные признаки, на которые нужно обратить внимание при отслеживании операций, можно разбить на несколько смысловых блоков:

1. Признаки, связанные с процессом проведения транзакции,
 - а разбиения на небольшие суммы либо на суммы, не превышающие пороговых значений, установленных для обязательной регистрации операций или для передачи сообщений;
 - б проведение нескольких операций на большую сумму:

- в короткие сроки, например, в пределах 24-часового периода;
 - с регулярным сдвигом во времени, после чего операции на продолжительное время прекращаются;
 - на вновь открытый либо на ранее спящий счет.
2. Признаки, связанные с регистрацией и целями создания адреса а внесение ВА депозитом на биржу, а затем нередко немедленный:
- вывод ВА с биржи без проведения каких-либо операций обмена на другой ВА;
 - обмен ВА на ВА нескольких других видов;
 - перевод ВА от провайдера услуг виртуальных активов (ПУВА) непосредственно в личный кошелек (аналог миксера);
- б снятие и внесение средств с адреса или кошелька, связанного с подозрительными источниками, такими как теневые маркетплейсы, сервисы миксинга, адресами, связанными с программами-вымогателями, и другой незаконной деятельностью.
3. Признаки, связанные с работой провайдеров услуг виртуальных активов
- а открытие нескольких счетов под разными именами для обхода ограничений провайдеров услуг виртуальных активов на торговлю и снятие средств;
- б получение или отправка средств ПУВА, у которых процедуры надлежащей проверки клиента (НПК) или знай своего клиента (ЗСК).
4. Признаки, связанные с географическими рамками проведения транзакций
- а Средства клиента поступают либо отправляются на биржу, не зарегистрированную в стране (территории), где находится этот клиент или биржа;
- б клиент имеет офисы на территориях, где не регулируются ВА
- Для исследования операций с виртуальными активами удобно использовать инструментарий, позволяющий их визуализировать.

Обзор функциональности Bitfury Crystal

Bitfury Crystal собирает всю информацию, доступную онлайн, в одном удобном и удобном для пользователя формате. Цепочки блоков содержат огромные объемы данных; Crystal просматривает эти данные и анализирует их. Данные блокчейна часто не привязаны к конкретной организации, особенно когда речь идет о незаконной деятельности. Crystal - выходит за

рамки блокчейна и собирает информацию о биткойн-адресах и сущностях из других источников, таких как веб-форумы и другие веб-сайты, на которых собираются пользователи блокчейна. Благодаря такому комплексному подходу Crystal может раскрывать не только адрес организации, но и ее фактическое имя в реальном мире.

Данный сервис позволяет оценивать соответствие требованиям в сфере ПОД/ФТ провайдеров услуг виртуальных активов, а также рассчитывать риск в процессе визуализации Crystal предоставляет доказательства связей между различными участниками блокчейна, позволяющий легко определить, происходили ли какие-либо транзакции между двумя субъектами. Затем Crystal сообщает об этих транзакциях в удобном для пользователя формате, включая общее количество входов и выходов, а также сумму, переведенную между двумя организациями за указанный промежуток времени.

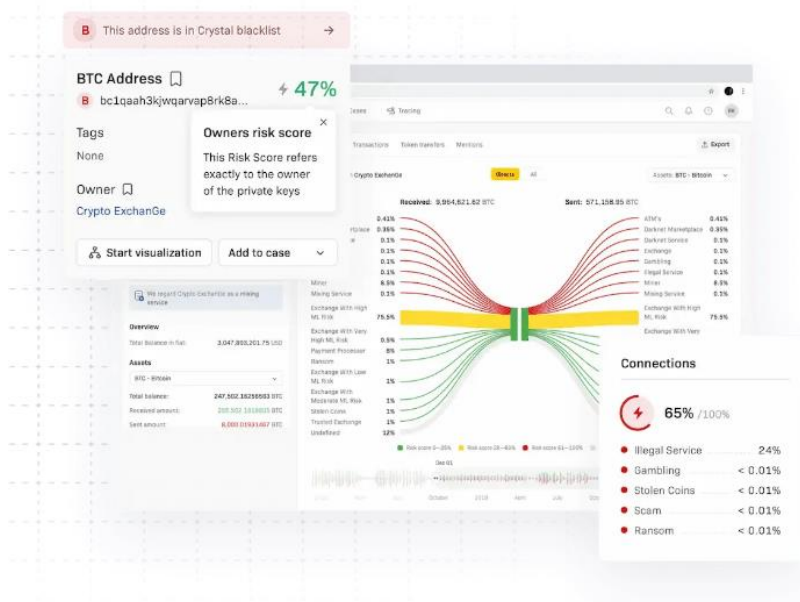


Рисунок 1 – Функциональность Bitfury Crystal

В данной работе проведено исследование криптовалютных операций, последовавших после совершения предикатного преступления (хищение средств, вымогательство и т.д.) с возможной целью отмыwania денег, а также операций, с высокой вероятностью связанных с финансированием

экстремисткой деятельностью. Исследование проводилось с использованием информационных ресурсов, доступных пользователям Bitfury Crystal, и инструмента мониторинга и визуализации криптовалютных транзакций.

В работе представлено исследование [3] подозрительной активности на рынке криптовалют. В первом деле применение инструментов визуального анализа позволило выявить признаки финансирования терроризма через криптовалюты в деятельности группировки ХАМАС. Второе дело связано со взломом криптовалютной биржи Zaif и последующим выводом денежных средств путем дробления. Дело SUEX является примером использования методов визуального анализа в случае расследования преступлений, связанных с деятельностью внебиржевого криптоброкера.

Дело ХАМАС.

ХАМАС - это группировка, базирующаяся в Палестине. В начале 2021 года было установлено [4], что ХАМАС получил биткойны на сумму почти 100 000 долларов. Эти средства, как предполагалось, затем использовались для финансирования нападений на Израиль. Во время конфликта был зафиксирован всплеск криптовалютных пожертвований из разных уголков мира. Некоторые из этих пожертвований были затем обналичены через криптовалютную биржу Binance. Эти транзакции вызвали углубленное расследование в отношении кошельков, принадлежащих и управляемых ХАМАС.

Bitfury Group постоянно отслеживает отчеты официальных властей, чтобы своевременно формировать список адресов связанных со сбором средств. О кошельках ХАМАСА официально сообщило Национальное бюро Израиля по борьбе с финансированием терроризма [4].

В июле 2021 года Израиль объявил [5], что начал захват криптовалютных счетов, связанных с ХАМАС. Страна также сообщила, что обнаружила обширную сеть крипто-кошельков, которые использовались для финансирования деятельности против нее. Кроме того, Министерству юстиции США также удалось изъять миллионы долларов с таких счетов с 2020 года.

На рисунке 2 представлена схема взаимодействия адресов, выполненная в продукте Chainalysis Reactor [6].

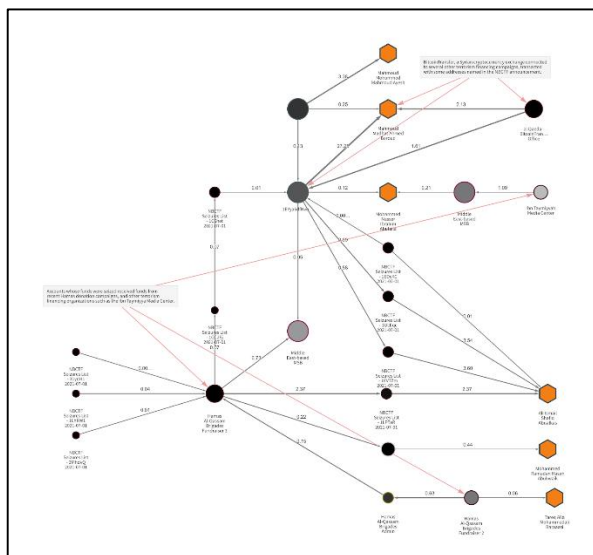


Рисунок 2 – Результат визуализации расследования, проведенного Chainalysis Reactor

В процессе анализа транзакций исходя из визуализации Chainalysis Reactor, мы обратили внимание на появление признаков подозрительных операций связанных с финансированием терроризма и экстремизма, а именно: проведение переводов на маленькие суммы, а на данном фрагменте схемы видно, что они были совершены за один день. Все эти суммы пришли на адрес 1EYua5dfNvuYDwpeboGKBtkXzJcEHMCQXR, а далее были выведены на адрес, принадлежащий ХАМАС.

Таким образом инструменты визуального анализа позволяют выявлять все связанные между собой адреса в целях проведения расследования. Визуальный анализ следующего события позволил выявить дробление и интеграцию средств, полученных преступным путем.

Дело Zaif.

Согласно майскому исследованию The Block [7], с 2012 года были скомпрометированы 42 криптовалютные биржи, и это без учета небольших по объемам платформ. Общая сумма украденных средств превысила \$1,35 млрд, при этом около 59% от нее (795,5 млн) были похищены в 2018 году. Одним из ярких примеров взломов бирж является случай с Zaif (Японская криптовалютная биржа), которая базируется в Осаке. Она потеряла биткоины и другие монеты на сумму около \$60 млн в результате хакерской атаки.

Неустановленные лица получили несанкционированный доступ к бирже 14 сентября 2018 года между 17:00 и 19:00 по местному времени (8:00 и 10:00 UTC). Они успешно перевели 5966 биткоинов (BTC) и неизвестные суммы Bitcoin cash (BCH) и MONA. Биржа Zaif получила информацию об этом несанкционированном доступе, когда 17 сентября была обнаружена неисправность сервера. Об этом сообщило издание Japan Times [8], оператор биржи подтвердил факт взлома. Около \$40 млн из похищенных средств лежали на депозитных счетах пользователей Zaif, остальные принадлежали самой бирже. В глобальном рейтинге CoinMarketCap биржа занимает 85 место с суточным объемом торгов \$4,92 млн.

Биткоин, который до распространения новости колебался на уровне \$6330 за монету, отреагировал на инцидент стремительным падением до \$6100, а через несколько минут — взлетом до \$6500.

Если удастся установить адрес, на который были отправлены украденные биткоины, можно найти адреса или организации, на которые были переведены украденные биткоины с этого адреса. В работе проведена интерпретация данного случая с помощью инструмента визуализации Bitfury Crystal.

Таким образом был определен адрес, через который шел вывод денег с взломанной биржи: 1FmwHh6pgkf4meCMoqo8fHh3GNRF571f9w. У него было выявлено 9 исходящих транзакций, в дальнейшем была отслежена каждая из них. После мониторинга этих транзакций было обнаружено, что 5109 адресов получили часть украденных средств.

Результаты отслеживания показали, что значительная часть средств (30 % от общей суммы) была переведена на два биткоин-адреса:

1. 3MyE8PRRitpLxy54chtf9pdpjf5NZgTfbZ — 1,007.6 BTC
2. 3EGDAa9rRNhxnRzpyRmawYtcYg1jP8qb7 — 754,5 BTC

Эти адреса получали биткоины в рамках очень короткой цепочки транзакций (средняя длина составляла 3 транзакции). Раньше они не появлялись в блокчейне, поэтому адреса были отнесены к открытым специально для данных транзакций, и, следовательно, к мошенническим.

Значительная часть биткоинов (1451,7 BTC или 24%) была отправлена на криптовалютную биржу Binance, как серия транзакций на небольшую сумму на адрес 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s. Биржа Binance подтвердила, что она владеет этим адресом. Binance позволяет пользователям выводить до 2 BTC без прохождения строгого процесса ЗСК/ПОД, поэтому средняя сумма, отправленная на каждый адрес депозита Binance, составляла 1,99–2 BTC. Данный факт подтверждает подозрительность проведенных транзакций.

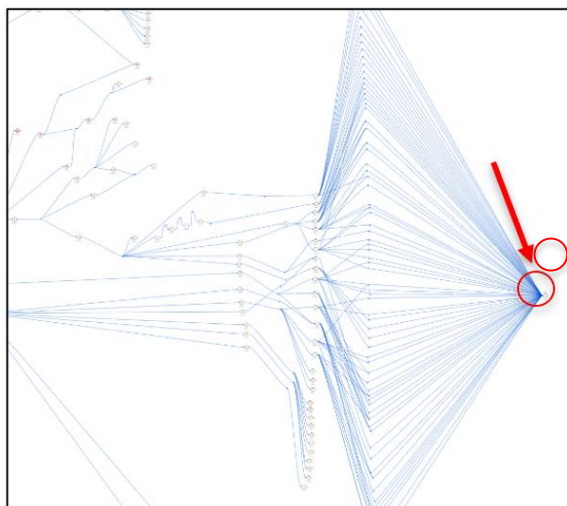


Рисунок 3 – Дробление суммы с последующей интеграцией на бирже Binance

Некоторая часть биткоинов была отправлена на ChipMixer.com, Bitcoin Fog и bestmixer.io. К сервисам миксинга вели довольно короткие цепочки транзакций, которые привели к ChipMixer.com, представлены на рисунке 4.

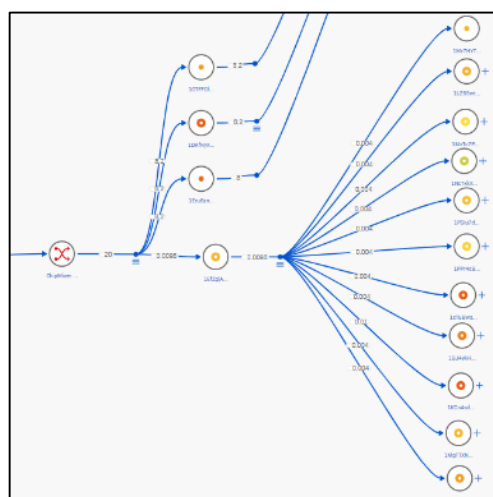


Рисунок 4 – Вывод криптовалюты из схемы посредством использования сервиса миксинга

Остальные средства осели по адресам с неизвестными владельцами. Таким образом, данный случай демонстрирует использование тех же самых технологий дробления, свойственных, как отмечает ФАТФ, и для подозрительных операций с фиатными деньгами. Следует отметить, что операции дробления и слияния гораздо удобнее проводить с цифровыми валютами, чем с фиатными деньгами. Визуальный анализ следующего события также позволил обнаружить транзакции, имеющие признаки ОД/ФТ.

Дело SUEX.

В сентябре 2021 года Минфин США внес [9] ОТС-платформу SUEX OTC S.R.O. в список специально назначенных граждан и заблокированных лиц (список SDN) в результате анализа, выполненного компанией Chainalysis. Инструментом для проведения расследования стал продукт Chainalysis Reactor. В статье [10], посвященной расследованию компании Chainalysis, утверждается, что в период с 2018 года адреса депозитов компании, размещенные на крупных биржах (Binance, OKEx, Huobi), получили более \$160 млн от вымогателей, мошенников и операторов рынка даркнета (в первую очередь, с российского рынка Hydra).

Данный случай был воспроизведен на платформе Crystal Expert на основе адресов, опубликованных Управлением по контролю за иностранными активами. Кроме того, дополнительно были использованы адреса, связанные с криптообменником Chatex, который также был внесен [11] в санкционные списки в связи с подозрением в содействии компании SUEX.

На рисунке 5 можно видеть процесс вывода средств на SUEX с закрытой в 2017 году криптобиржи BTC-е за содействие крупномасштабному отмыванию денег от имени киберпреступников.

Красным на рисунке обведены адреса SUEX, внесенные в список SDN. Анализ цепочки транзакций позволил выделить некоторые из признаков ОД/ФТ, сформулированных в отчете ФАТФ [2]. Среди них – проведение операций с регулярным сдвигом во времени на вновь открытые счета. Важно отметить, что переводы с BTC-е на адреса SUEX осуществлялись значительно позже закрытия биржи. Исследователи Chainalysis предполагают [10], что SUEX, возможно, обрабатывала эти переводы от имени администраторов и бывших пользователей BTC-е с целью ликвидации криптовалюты, заблокированной на бирже путем обмена криптовалюты на наличные.

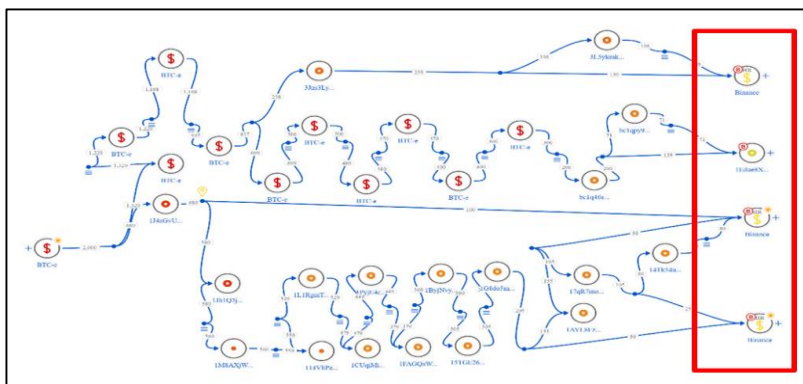


Рисунок 5 – Визуализация транзакций вывода денежных средств с BTC-e на адреса SUEX

На рисунке 6 можно видеть еще два фрагмента визуализации. На фрагменте слева можно видеть, как средства, полученные с адресов российского теневого маркетплейса Hydra, направлялись на адреса биржи Chatex. Также можно видеть транзакцию, подтверждающую отставку средств с Chatex на адрес SUEX. Фрагмент справа также подтверждает связь Chatex с Hydra.

Здесь можно выделить такие признаки как проведение операций с использованием сервисов миксинга с целью сокрытия потока незаконных средств между известными адресами кошельков и маркетплейсами даркнета. Снятие и внесение средств с адресов, связанными с маркетплейсами даркнета также являются признаком ОД/ФТ посредством ВА согласно отчету ФАТФ.

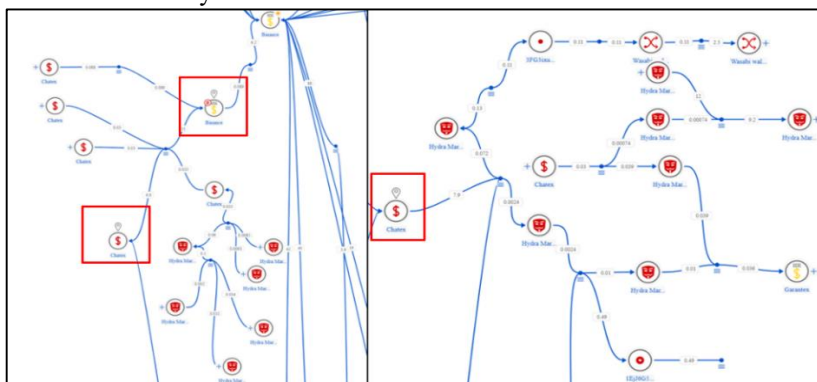


Рисунок 6 – Визуализация транзакций, связанных с теневым рынком

Таким образом, продукты, позволяющие проводить визуализацию связей адресов, могут полноценно помочь в проведении расследований. В рамках исследования с помощью инструментов визуализации были выявлены такие признаки ОД/ФТ как операции разбиения на небольшие суммы, проведение операций с регулярным сдвигом во времени на вновь открытые счета, использование сервисов миксинга, а также снятие и внесение средств с адресов, связанными с маркетплейсами даркнета.

Список использованных источников:

1. Documents - Financial Action Task Force (FATF) // Fatf-gafi.org [Электронный ресурс]. URL: <https://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html>
2. Documents - Financial Action Task Force (FATF) // Fatf-gafi.org [Электронный ресурс]. URL: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>
3. How Crystal Investigations Truly Make a Difference – Crystal Blockchain Analytics for Crypto Compliance // Crystalblockchain.com [Электронный ресурс]. URL: <https://crystalblockchain.com/investigations/how-crystal-investigations-truly-make-a-difference/>
4. Minister of Defense Benny Gantz Signs an Administrative Order to Seize Electronic Wallets Used by Hamas to Trade Different Types of Cryptocurrency // Mod.gov.il [Электронный ресурс]. URL: <https://nbctf.mod.gov.il/en/Pages/CryptoSeizureEN072021.aspx>
5. Jazeera A. Israel says it is targeting Hamas's cryptocurrency accounts // Aljazeera.com [Электронный ресурс]. URL: <https://www.aljazeera.com/news/2021/7/9/israel-says-it-is-targeting-hamas-cryptocurrency-accounts>
6. Israeli Government Seizes Cryptocurrency Addresses Associated with Hamas Donation Campaigns // Chainalysis.com [Электронный ресурс]. URL: <https://blog.chainalysis.com/reports/israel-hamas-cryptocurrency-seizure-july-2021>
7. The Block Crypto // Theblockcrypto.com [Электронный ресурс]. URL: <https://www.theblockcrypto.com/tiny/biggest-crypto-hacks-ever>
8. Japan's Financial Services Agency criticizes hacked crypto-exchange over lack of details on \$62 million theft // The Japan Times [Электронный ресурс]. URL: <https://www.japantimes.co.jp/news/2018/09/25/business/financial-markets/japans-financial-services-agency-criticizes-hacked-crypto-exchange-lack-details-62-million-theft/>

9. Publication of Updated Ransomware Advisory; Cyber-related Designation // U.S. Department of the Treasury [Электронный ресурс]. URL: <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921>.
10. Chainalysis in Action: OFAC Sanctions Russian Cryptocurrency OTC Suex that Received Over \$160 million from Ransomware Attackers, Scammers, and Darknet Markets//blog.chainalysis.com [Электронный ресурс]. URL: <https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021> (дата обращения: 17.11.2021)
11. Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange // U.S. Department of the Treasury [Электронный ресурс]. URL: <https://home.treasury.gov/news/press-releases/jy0471> (дата обращения: 17.11.2021).

Исследование влияния социально-экономических показателей стран мира на незаконный оборот наркотических средств

Т. Раканов

студент 6 курса НИЯУ МИФИ, Москва

E-mail: rakanov.t@gmail.com

Д.В. Домашова

доцент кафедры финансового мониторинга НИЯУ МИФИ, Москва

E-mail: janedom@mail.ru

Аннотация: В статье представлены результаты применения методов анализа данных, в частности кластерного анализа и регрессионного анализа оборота и применения наркотических средств. Результаты исследования могут быть использованы органами государственной власти для разработки, организации и принятия соответствующих мер противодействия.

Ключевые слова: наркотики, незаконный оборот, кластеризация, регрессия.

Study of the Impact of Economic Indicators of the World Countries on Illicit Drug Trafficking

Abstract: The article presents the results of the application of data analysis methods, such as cluster analysis and regression analysis of the illegal drug trafficking and its consumption. The results of the research can be used by government authorities to develop, organize, and take countermeasures.

Keywords: drugs, illicit trafficking, clustering, regression.

Введение

За последние несколько десятилетий распространение наркотиков стало одним из главных угроз национальной безопасности стран, подвергаящая опасности здоровье общества, а также внутреннюю безопасность. Управление ООН по наркотикам и преступности (УНП ООН) постоянно отслеживает и исследует глобальные рынки запрещенных наркотиков, чтобы получить более полное представление об их динамике.

На сегодняшний день на мировом рынке объемы героина составляют около 430–450 тонн. Из этого объема около 380 тонн героина и морфина, производится исключительно из афганского опиума. В то время как,

большая часть, в размере 375 тонн, распределяется по всему миру, по маршрутам, пролегающим через соседние страны.

Различают следующие основные маршруты наркотрафика. Балканский и северные маршруты являются основными коридорами незаконного оборота героина, связывающими Афганистан с огромными рынками России и Западной Европы. Балканский маршрут, изображенный на рисунке 1а, проходит через Иран, Турцию, страны Балканского полуострова и выходят на западноевропейский рынок с годовой рыночной стоимостью около 20 миллиардов долларов. Северный маршрут проходит в основном через Центральную Азию в Казахстан и Россию. Размер этого рынка оценивается в 13 миллиардов долларов в год [1].



Рисунок 1а – Пути распространения героина: Балканский путь



Рисунок 1б – Пути распространения наркотиков: Америка

На североамериканский рынок кокаин обычно доставляется из Колумбии, Мексики или Центральной Америки по морю, а затем по суше в Соединенные Штаты и Канаду (рисунок 1б). В Европу кокаин доставляется в основном по морю, часто в контейнерах. Колумбия остается основным источником кокаина, обнаруженного в Европе. Но прямые поставки из Перу и Боливии в Европу более распространены, чем на рынке Соединенных Штатов.

«Золотой треугольник», в который входят три страны Мьянма, Лаос и Таиланд, на протяжении десятилетий был регионом, связанным с «традиционным» производством и оборотом наркотиков. Значительное влияние на оборот наркотических средств данные три страны оказывают на Индию, Юго-Западную Азию и Тихоокеанский регион (Австралия, Новая Зеландия) [2].

Пагубное воздействие организованной преступности, связанной с наркотиками, на общество включает проникновение в легальную экономику. Незаконная торговля наркотиками — это международный

бизнес, требующий перевода больших сумм денег по всему миру. Большое распространение наркотиков в стране ставит под удар ее национальную безопасность. Встает вопрос легализации огромных доходов, полученных нелегальным путем, а именно сбытом наркотических средств [3].

Возможность предугадать тенденции роста наркобизнеса в стране поможет в принятии своевременных и эффективных решений.

Данное исследование посвящено анализу влияния социально-экономических факторов на уровень оборота наркотиков в странах мира. Схема проведения комплексного анализа состоит из следующей последовательности процедур:

- Сбор данных и формирование признакового пространства
- Предобработка данных
- Кластеризация стран мира на основе социально-экономических показателей, характеристика кластеров по методу Уорда
- Построение регрессионной зависимости объема изъятых наркотиков и уровня их потребления от социально-экономических показателей

Сбор данных и формирование признакового пространства

Источниками данных послужили:

- Управления Организации Объединенных Наций (ООН) по наркотикам и преступности [4]
- Программы развития ООН [5]
- Всемирный банк [6]
- Международная организация уголовной полиции (Интерпол) [7]

Распределенные по группам признаки представлены в Таблице 1.

Таблица 1 – Показатели для проведения исследования

Образованность	Средняя продолжительность обучения в школе (лет) (X1); Количество детей обучающихся в начальных классах (X3); Количество детей обучающихся в средних классах (X4); Количество детей обучающихся в старших классах (X5); % населения в городах (X2); Соотношение учеников и учителей, начальная школа (учеников на учителя) (X16);
Здравоохранение	Смертность на 1 000 человек (X6); Бюджет на здравоохранение (% от ВВП) (X8);
Экономика	ВВП на душу населения (по ППС) (X7); Соотношение занятости и населения (X9); Безработица. Молодежь, не посещающая школу или не работающая (X10); Интернет-пользователи (% населения) (X15); Коэффициент Gini (Джини) (X17);
Миграция	Количество иммигрантов (% населения) (X12);

	Международная студенческая мобильность (% от общего числа учащихся высших учебных заведений) (X13); Международные въездные туристы (в тысячах) (X14);
Криминогенность	Количество убийств (на 100 000 человек) (X11); Количество полиции на 100,000 (X18).

Предобработка данных

Дополнительно проведена работа с данными:

- Рассчитано количество полиции на 100,000 человек населения страны;
- Отфильтрованы признаки, по которым достаточное количество данных (более 80% заполненности);
- Удалены страны, у которых отсутствует большинство признаков (более 20%);
- Заполнены пустые ячейки средними значениями по столбцу;
- Данные стандартизованы;
- Проверена корреляция между признаками;
- Удалены признаки, которые сильно коррелируют с другими.

По итогу объем выборки составил 117 стран мира, размерность признакового пространства 19 признаков (таблица 1).

Кластерный анализ

Задача кластеризации заключается в разбиении стран на однородные группы (кластеры) по социально-экономическим признакам.

Дендрограмма объединения по методу Уорда представлена на рисунке 1, при пороговом значении расстояния $p = 17$, все страны разбиваются на 6 кластеров.

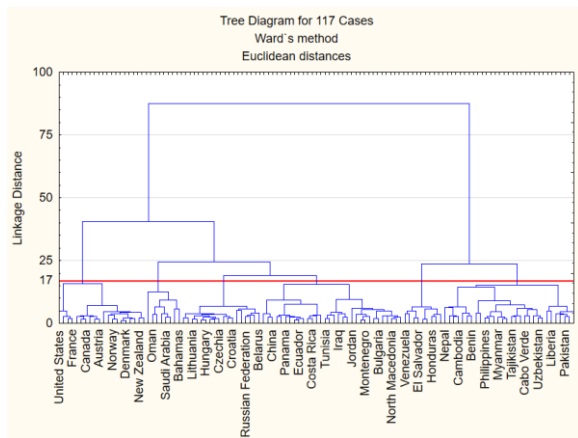


Рисунок 2 – Дендрограмма по методу Уорда

График средних значений признаков в классах представлен на рис.3.

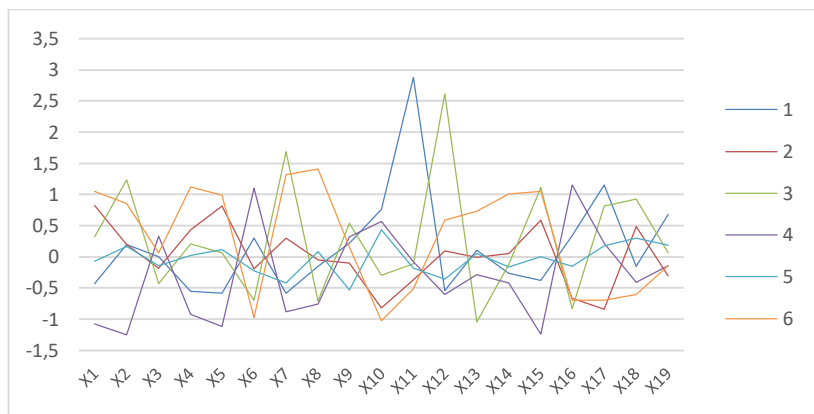


Рисунок 3 – График средних значений признаков в каждом кластере. Метод Уорда

При построении кластеризации методом К-средних было принято решение о разбиении выборки на 6 кластеров, по аналогии с разбиением в методе Уорда.

Таблица, представленная на рисунке 4 содержит информацию о значимости нулевой гипотезы о равенстве межгрупповой и внутри групповой дисперсии. На уровне значимости 0,05 по всем признакам нулевая гипотеза отвергается. Это означает, что каждый из признаков вносит существенный вклад в разделение объектов на кластеры.

Variable	Analysis of Variance (Лист1 in dat_an.stw)					
	Between SS	df	Within SS	df	F	signif. p
X1	84,33134	5	31,6687	111	59,11698	0,000000
X2	68,57388	5	47,4261	111	32,09920	0,000000
X3	23,24458	5	92,7554	111	5,56334	0,000130
X4	76,16607	5	39,8339	111	42,44840	0,000000
X5	70,14043	5	45,8596	111	33,95404	0,000000
X6	77,90645	5	38,0936	111	45,40199	0,000000
X7	79,51971	5	36,4803	111	48,39154	0,000000
X8	53,15917	5	62,8408	111	18,77973	0,000000
X9	43,79786	5	72,2021	111	13,46654	0,000000
X10	60,12425	5	55,8758	111	23,88797	0,000000
X11	63,42549	5	52,5745	111	26,78191	0,000000
X12	38,42389	5	77,5761	111	10,99579	0,000000
X13	15,64589	5	100,3541	111	3,46113	0,006048
X14	27,36093	5	88,6391	111	6,85265	0,000013
X15	83,13481	5	32,8652	111	56,15646	0,000000
X16	82,78643	5	33,2136	111	55,33458	0,000000
X17	36,22871	5	79,7713	111	10,08229	0,000000
X18	35,27560	5	80,7244	111	9,70114	0,000000

Рисунок 4 – Анализ дисперсий

График средних значений признаков в классах представлен на рис. 5.

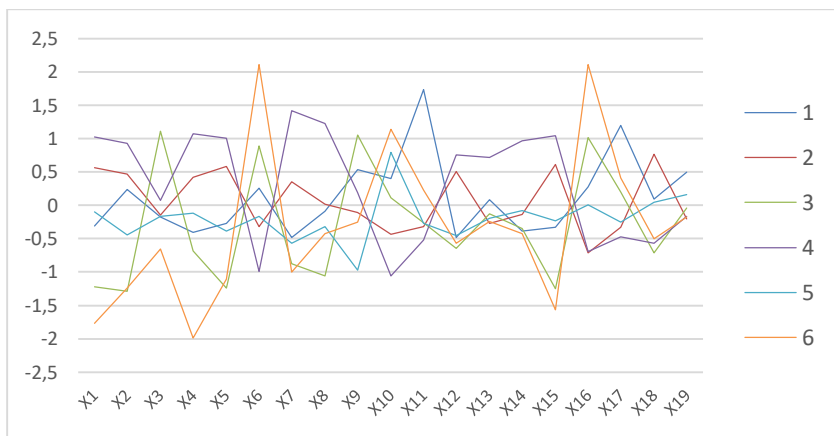


Рисунок 5 – График средних значений признаков в каждом кластере. Метод К-средних

С помощью метода Уорда и метода К-средних были получены различные кластеризации. Для выбора лучшей кластеризации использовался функционал качества разбиения, рассчитанный по формуле 1.

$$Q_1(S) = \sum_{l=1}^p \sum_{O_i \in S_l} d^2(O_i, \bar{X}(l)) \rightarrow \min \quad (1)$$

Сравнивая функционалы качества для классификации, полученной методом Уорда и методом К-средних:

$$Q(S_1) = 1089,56 \quad Q(S_2) = 1068,75$$

Можно сделать вывод о том, что оба метода практически равноценны.

Характеристики кластеров по методу уорда

1-й кластер – попали страны Южной и Центральной Америки. Такие как Бразилия, Колумбия, Венесуэла, Мексика и другими небольшими странами центральной Америки. Объединяющим фактором среди данных стран является не только социально-экономические факторы, но также и то, что вышеперечисленные страны являются главными поставщиками различного рода наркотических средств. А именно кокаина и его производных, такие как листья коки, и различные масла.



Рисунок 6 – Визуальное отображение стран входящих в 1-й кластер

В данном кластере, на фоне остальных, резко выделяется признак X11 (уровень убийств на 100 000 человек). Что не удивительно, так как среди стран 1-го кластера, 5 входят в десятку стран с самым высоким уровнем преступности в мире [8]. Также можно выделить признак X17 (коэффициент Джини). Коэффициент Джини является показателем степени расслоения в обществе, чем выше данный показатель, тем в большей степени доходы страны сконцентрированы в руках определенного класса общества [9]. Безработица среди молодежи, не посещающая школу, либо колледж (X10), самая высокая среди всех кластеров. Однако несмотря на то, что количество полиции на душу населения (X18) в данных странах не велико (средний показатель среди кластеров), по странам данного кластера средний объем изъятых наркотических средств (X19) является самым высоким.

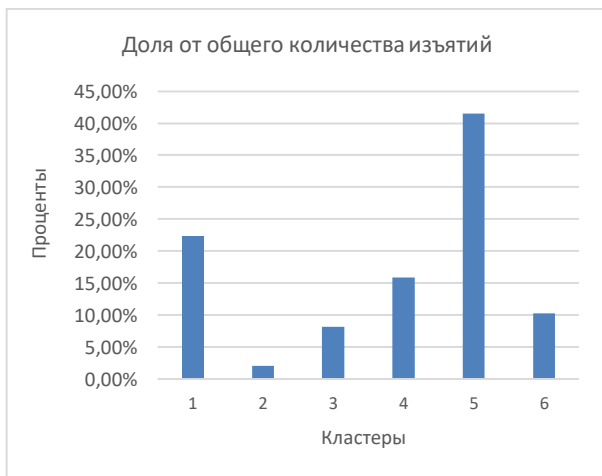


Рисунок 7 – Гистограмма доли изъятий в странах от общего количества

Объем изъятий в странах этого кластера составляет почти четверть от общемирового объема, 22,34%. Наибольшее количество изъятых наркотиков в Гватемале, Колумбии, Бразилии и Мексике. Что не удивительно, так как еще с 80-х годов прошлого века на весь мир был известен Медельинский кокаиновый картель и другие. Картель, который за годы своей активности смог переправить сотни тонн кокаина в страны северной Америки и Европы [10].

2-й кластер – включает в себя страны восточной Европы, также Россию, Казахстан, Португалию, Грецию и Малайзию (рисунок 8).



Рисунок 8 – Визуальное отображение стран входящих в 2-й кластер

За исключением относительной схожести экономического развития данных стран можно подметить тот факт, что вышеперечисленные государства являются транзитными странами для незаконной переправки наркотиков из стран южной Америки – Португалия. Из стран центральной Азии – Казахстан, Россия и другие страны восточной Европы. И Малайзия, которая находится в непосредственной близости со странами «золотого треугольника» – Мьянма, Лаос и Таиланд. Страны, где еще в середине XX века возникла система производства опиума и торговли с различными преступными группировками [11].

Страны в данном кластере, в основном, характеризуются средними показателями по большинству признаков. Однако выделяются признаки X1 (Средняя продолжительность обучения в школе), X10 (Безработица среди молодежи, которая не учится в школе или колледже), X17 (Коэффициент Джини). По коэффициенту Джини страны второго кластера показывают наилучший результат. В среднем среди стран 2-го кластера объем изъятых наркотических средств минимальный. И большинство приходится на Малайзию. Данный факт может быть связан с географическим расположением страны, так как находится в непосредственной близости к странам, производящим наркотики в больших объемах. Но также и с тем, что в Малайзии соблюдение закона строго регулируется.

Но доля, занимаемая от общего объема мировых изъятий, составляет всего 2,06% (рисунок 9). На основании этого можно выдвинуть гипотезу о том, что в данных странах не задерживается основной поток наркотических средств, так как покупательская способность граждан в большинстве этих государств, низкая.

3-й кластер – является набором стран с высокой экономической развитостью и относительно небольшой площадью. Это такие страны как Гонконг, Сингапур, Кувейт, Саудовская Аравия, Оман, Люксембург.



Рисунок 9 – Визуальное отображение стран входящих в 2-й кластер

Страны данного кластера имеют наибольший процент населения в городах (X2), процент интернет-пользователей (X15), наибольшее ВВП на душу населения по ППС (X7), лучшее соотношение учеников к учителям (X16) и наименьшее количество иностранных студентов (X13). Также занятость населения (X9) на самом высоком уровне среди кластеров. Объем изъятий в данных странах занимает 8,12% от общемирового объема. Учитывая то, что мы имеем всего 6 кластеров, доля не является большой. Но в то же время страны не большие по площади и населения относительно не много. Одним из возможных вариантов такого большого количества изъятий является их высокая покупательская способность, но в то же время довольно строгие законы, которые в должной мере выполняются сотрудниками правоохранительных органов.

4-й кластер – страны входящие в этот кластер — это страны Центральной, Южной, Юго-Восточной Азии и страны Африки. Всего в этот список входят 30 стран среди которых наибольший объем изъятий имеют Афганистан, Пакистан, Таджикистан, Нигерия и Индия.



Рисунок 10 – Визуальное отображение стран, входящих в 4-й кластер

В данный кластер попали страны, производящие опиум в Азии. Это такие страны как Афганистан, Мьянма, Лаос, а также близко к ним страны центральной и юго-восточной Азии. Туда же попал один самых больших рынков – Индия. Страны в данном кластере являются самыми низко развитыми в плане экономики, образования и медицины. Так как в подавляющем большинстве признаков страны данного кластера демонстрируют самые низкие показатели. От общемирового объема данный кластер имеет 15,82%, что не так уж и много. Но снова стоит учитывать покупательскую способность граждан. А страны в данном кластере являются наиболее низко развитыми в плане экономики среди всех остальных кластеров.

5-й кластер – в него входят 32 страны, расположенные на ближнем востоке, северной Африке и балканские страны, а также Китай, Таиланд и страны Южной и Центральной Америки (рисунок 11).

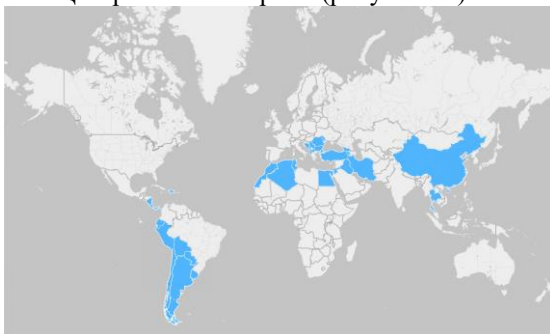


Рисунок 11 – Визуальное отображение стран, входящих в 5-й кластер

Страны, попавшие в данный кластер, расположены вдоль следования так называемого «балканского пути» [3]. Окно в Европу для Афганского наркотрафика. Более того Турция является наиболее удобной страной для

переправки веществ, так как граничит со странами Евросоюза. От Афганистана ее отделяет всего одна страна – Иран. Но, с другой стороны, наибольшее количество изъятий нелегальных наркотических средств приходится на Турцию (4349 тонн). Следом за Турцией идет Иран с 829 тоннами. Однако стоит отметить, что большинство изъятий в Турции приходится на растения каннабиса, около 97% от общих изъятий в Турции (рисунок 12).

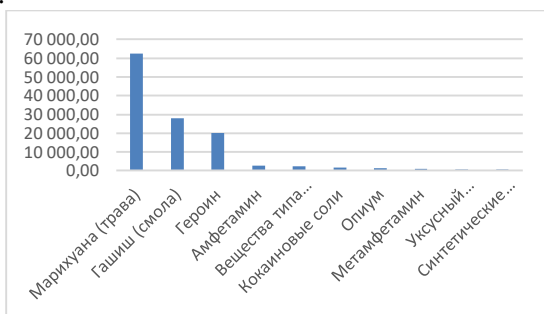


Рисунок 12 – Гистограмма объема изъятых наркотиков в Турции (кг). Исключая растения каннабиса

Но в соседней стране, в Иране, лидером по объему изъятий является опиум (рисунок 13), который в также промышленных масштабах выращивается не только Афганистане, но и самом Иране. Однако, если в Афганистане более 90% произведенных наркотиков уходит на экспорт, то в Иране правоохранительные органы изымают значительное количество запрещенных веществ.

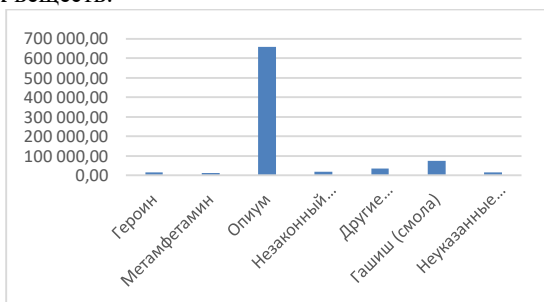


Рисунок 13 – Гистограмма объема изъятых наркотиков в Иране (кг)

Анализируя график средних значений признаков 5-го кластера (рисунок 3), можно констатировать факт, что в этом кластере собраны страны со средними показателями по большинству признаков. Но выделяется признак X9 (Соотношения занятости и населения), количество

безработных на душу населения довольно высокое, также параметр X10 (Безработица. Молодежь, не посещающая школу или не работающая) не самый высокий, но заметно выше среднего. Наряду с этим признак X19 (Количество изъятых наркотиков) на втором месте среди остальных кластеров. Что говорит о возможной связи между данными признаками.

6-й кластер – в данный кластер входят страны Западной Европы, Северной Америки, Австралия и Япония.

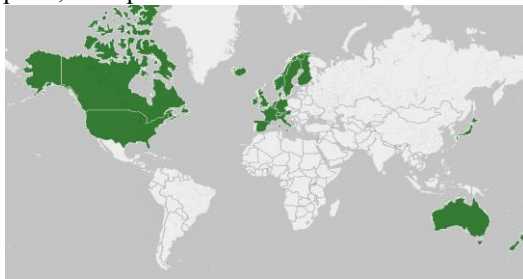


Рисунок 14 – Визуальное отображение стран, входящих в 6-й кластер

Этот список явно включает в себя развитые страны, которые предположительно являются конечным пунктом назначения всех путей распространения наркотиков. Примером этому может служить тот факт, что в США и Испании наибольшее количество изъятых наркотических веществ среди стран данного кластера (рисунок 14). Одной из причин является экспорт наркотических веществ странами латинской Америки, такими как Мексика и Колумбия. Окном в Европу для данных стран является Испания, благодаря удобному расположению и языковой связи, что облегчает коммуникацию с принимающей стороной. Страны в данном кластере лучшие по большинству параметров, уступая лишь странам 3-го кластера, Сингапур, Кувейт, Гонконг и другие.

Построение регрессионной зависимости объема изъятых наркотиков и уровня их потребления от социально-экономических показателей

Объем выборки 117 стран, в качестве факторных признаков выступают вышеописанные признаки, по которым проводился кластерный анализ (таблица 1), результирующий признак – объем изъятых наркотиков (кг) - Y1.

По результатам регрессионного анализа построения зависимости объема изъятых наркотиков от социально-экономических показателей, после устранения мультиколлинеарности были получены следующие оценки коэффициентов пошаговой регрессии, построенной в программе Statistica (рисунок 15).

Regression Summary for Dependent Variable: Y1 (Лист1 in dat_an.stw)						
R= ,39662973 R²= ,15731514 Adjusted R²= ,13494298						
F(3,113)=7,0317 p<,00022 Std.Error of estimate: ,93008						
N=117	b*	Std.Err. of b*	b	Std.Err. of b	t(113)	p-value
Intercept			-0,000000	0,085986	-0,000000	1,000000
X17	0,238376	0,089931	0,238376	0,089931	2,650668	0,009186
X14	0,282981	0,089594	0,282981	0,089594	3,158482	0,002035
X10	0,188860	0,092927	0,188860	0,092927	2,032354	0,044463

Рисунок 15 – Оценки коэффициентов пошаговой регрессии для Y1

Оценка уравнения линейной регрессии имеет следующий вид:

$$\hat{y} = 0.188 x_{10} + 0.282 x_{14} + 0.238 x_{17}$$

(0.092) (0.089) (0.089)

Значение статистики F(3.113) = 7.03, $p < 0.05$, следовательно уравнение регрессии значимо.

Наиболее значимыми переменными являются x10 (Безработица. Молодежь, не посещающая школу или не работающая), x14 (Международные въездные туристы, в тысячах), x17 (Коэффициент Gini). Иными словами, на уровень изъятий наркотических средств влияет количество иностранцев, въехавших в страну, что вполне закономерно, так как среди них могут быть и люди нелегально перевозящие с собой наркотические вещества. Также при сильном расслоении в обществе (Коэффициент Gini) и высокой безработице люди склонны прибегать к употреблению запрещенных веществ, что в свою очередь повышает спрос на эти вещества.

Построим уравнение регрессии зависимости доли употребляющих наркотические вещества от населения возрастом от 15 до 65 лет (%) - Y2 от показателей, представленных в таблице 1. После устранения мультиколлинеарности были получены следующие оценки коэффициентов пошаговой регрессии, построенной в программе Statistica (рисунок 16).

Regression Summary for Dependent Variable: Y2 (Лист1 in dat_an.stw)						
R= ,53692687 R²= ,28829047 Adjusted R²= ,26287227						
F(4,112)=11,342 p<,00000 Std.Error of estimate: ,85856						
N=117	b*	Std.Err. of b*	b	Std.Err. of b	t(112)	p-value
Intercept			0,000000	0,079374	0,000000	1,000000
X8	0,418375	0,085807	0,418375	0,085807	4,87579	0,000004
X11	0,134143	0,088245	0,134143	0,088245	1,52012	0,131300
X14	0,176566	0,085866	0,176566	0,085866	2,05630	0,042078
X17	-0,158255	0,087968	-0,158255	0,087968	-1,79901	0,074710

Рисунок 16 – Оценки коэффициентов пошаговой регрессии для Y2

Оценка уравнения линейной регрессии имеет следующий вид:

$$\hat{y} = 0.418 x_8 + 0.134 x_{11} + 0.176 x_{14} - 0.158 x_{17}$$

(0.085) (0.088) (0.085) (0.087)

Значение статистики $F(4.112) = 11.34$, $p < 0.05$, следовательно уравнение регрессии значимо.

Наиболее значимым признаком является X_8 (Бюджет на здравоохранение). То есть, уровень здравоохранения в стране напрямую влияет на процент наркозависимых граждан. Также подталкивают к употреблению и объемы ввозимых туристами запрещенных веществ (X_{14}). И уровень криминальной активности (X_{11}), и высокое расслоение в обществе (X_{17}) не оказывают положительного влияния на уровень потребления наркотических и психотропных веществ в стране.

Заключение

В рамках работы предложена схема исследования уровня оборота наркотиков от социальных и экономических показателей в различных странах мира. Предложен перечень источников данных, а также построен набор информативных показателей, оказывающих наибольшее влияние на уровень коррупции, проведена кластеризация стран мира по отобранным признакам.

Построена регрессионная модель по уровню оборота и потреблению нелегальных веществ. Выделенные признаки могут использоваться для того, чтобы определить области, которые непосредственно влияют на выше названные показатели. В частности, увеличение значений таких показателей, как бюджет на здравоохранение, а также снижение уровня безработицы и уровня расслоения общества, может привести к уменьшению уровня потребления и оборота наркотиков в стране.

Результаты данной работы можно использовать для развития законодательства стран в области противодействия употреблению и нелегальному распространению наркотических веществ, а также для разработки политики развития экономики и социальной сферы.

Список использованных источников:

1. Управление ООН по наркотикам и преступности [Электронный ресурс]. – URL: <https://www.unodc.org/unodc/en/drug-trafficking/> (дата обращения 17.11.2021)
2. Хэмиш Уокер. Маршруты наркотиков из Золотого треугольника [Электронный ресурс]. – URL: <https://www.afp.gov.au/news-media/platypus/drug-routes-out-golden-triangle-afp-helps-tell-story/> (дата обращения 19.11.2021)
3. Европейский центр мониторинга наркотиков и наркомании. Отчет ЕС по рынкам наркотиков 2019. – С. 50.

4. Управление ООН по наркотикам и преступности [Электронный ресурс]. – URL: <https://www.unodc.org/> (дата обращения 19.09.2021)
5. Программа Развития ООН [Электронный ресурс]. – URL: <http://hdr.undp.org/en/> (дата обращения 21.09.2021)
6. Всемирный банк [Электронный ресурс]. – URL: <https://www.worldbank.org/en/> (дата обращения 21.09.2021)
7. Интерпол [Электронный ресурс]. – URL: <https://www.interpol.int/> (дата обращения 26.09.2021)
8. World Population Review [Электронный ресурс]. – URL: <https://worldpopulationreview.com/country-rankings/crime-rate-by-country/> (дата обращения 13.10.2021)
9. Сирвида-Льорентэ С., Коэффициент Джини: все ли равны? [Электронный ресурс]. – URL: <https://journal.openbroker.ru/economy/koefficient-dzhini/> (дата обращения 08.11.2021)
10. Сапронова Ю., Антипова А., Пять самых известных наркобаронов [Электронный ресурс]. – URL: <https://www.rbc.ru/photoreport/17/07/2019/5d2f30b49a79470a9bab0134> (дата обращения 08.11.2021)
11. Пугачева Е. В., Наркобизнес в механизме функционирования политических решений Таиланда, 2019. – С. 38–39.

УДК 657.9:005.334:681.5

© В.Г. Когденко, Т.К. Винокурова, 2021

Исследование отраслевых факторов доходности и рисков (на примере электронной промышленности)

В.Г. Когденко

заведующая кафедрой финансового менеджмента

НИЯУ МИФИ, Москва

E-mail: vggkogdenko@mephi.ru

Т.К. Винокурова

старший преподаватель кафедры финансового менеджмента

НИЯУ МИФИ, Москва

Аннотация: Исследование посвящено выявлению отраслевых факторов доходности и рисков, характерных для секторов экономики и отдельной отрасли. На примере электронной промышленности рассмотрен состав факторов доходности и рисков. Предложен комплекс показателей для оценки доходности и рисков.

Ключевые слова: отраслевой анализ, риски, электронная промышленность.

Research of sectoral factors of profitability and risks (on the example of the electronics industry)

Abstract: The study is devoted to identifying industry-specific factors of profitability and risks specific to sectors of the economy and a particular industry. On the example of the electronics industry, the composition of the factors of profitability and risks is considered. A set of indicators for assessing the profitability and risks is proposed.

Keywords: industry analysis, risks, electronics industry.

Внимание к отраслевому анализу в современной аналитике связано с ростом сложности экономики и институциональной среды, усилением влияния крупных экономических образований, необходимостью увязки микро и макроуровня для разработки государственной политики. Значимость отраслевого анализа возрастает в процессе разработки, реализации и мониторинга государственных программ развития отраслей. Отраслевой анализ позволяет оценить отраслевые факторы доходности и рисков, проанализировать интенсивность конкуренции в отрасли, исследовать поведение предприятий, оценить их эффективность и

результативность государственной промышленной политики. Государственная политика, опирающаяся только на макроанализ, оказывается не эффективной, поскольку не способна предвидеть поведение предприятий, наступление кризисов и предотвратить их последствия [2].

Отраслевые факторы доходности и рисков могут быть сгруппированы по секторам экономики [3]:

1. Первичный: добыча и переработка сырья (горючие полезные ископаемые, руда, горно-химическое сырье, камнесамоцветное сырье, нерудные полезные ископаемые, др.), в полуфабрикаты, сельское хозяйство. Основные характеристики:

- ключевой вид капитала – природный капитал;
- снижение доли сектора в ВВП;
- сокращение численности персонала сектора.

2. Вторичный: промышленное производство, строительство. Основные характеристики:

- ключевой вид капитала – производственный капитал;
- снижение доли сектора в ВВП;
- сокращение численности персонала сектора.

3. Третичный: производственные услуги и обслуживание человека. Основные характеристики:

- ключевой вид капитала – человеческий капитал;
- увеличение доли сектора в ВВП;
- увеличение численности персонала сектора.

4. Четвертичный сектор: информационные, компьютерные и иные новые технологии, формирующие экономику знаний, информационную экономику. Основные характеристики:

- ключевой вид капитала – интеллектуальный капитал;
- увеличение доли сектора в ВВП;
- увеличение численности персонала сектора.

Особенности секторов экономики обуславливают состав факторов их доходности и риска. Для отраслей первичного сектора одним из ключевых факторов доходности является достаточность и качество ресурсной базы; для вторичного сектора – степень вертикальной интеграции, контроль над предприятиями, добывающими сырье, что обеспечивает высокую маржинальность продукции; для третичного сектора – качество инфраструктуры и профессионализм персонала; для четвертичного – уникальность ключевых продуктов, эффективность инновационной деятельности таблица 1. При этом некоторые факторы, в частности, вертикальная интеграция, продуктовая диверсификация, инвестиционная активность, важны практически для всех отраслей экономики. Кроме того, доходность зависит от силы воздействия сил конкуренции (модель Майкла

Портера). Так, при значительной степени концентрации покупателей или поставщиков снижается операционная эффективность и маржинальность производителей отрасли. Следует отметить, что в современной экономике значимым фактором доходности для всех секторов экономики становится степень цифровизации бизнеса, это позволяет сократить операционные расходы, повысить оборачиваемость капитала и маржинальность продукции.

Таблица 11 – Факторы доходности по секторам экономики

Сектор экономики	Факторы доходности
Первичный сектор	– Достаточность и качество ресурсной базы – Уровень расходов на разведку, добычу и переработку – Глубина переработки сырья – Продуктовая диверсификация – Степень концентрации на одном месторождении – Доступность и диверсификация рынков сбыта
Вторичный сектор	– Уровень производственных расходов – Степень концентрации на одном заводе (производственной площадке) – Уровень износа производственных мощностей – Степень вертикальной интеграции – Технологичность производства – Продуктовая гибкость и диверсификация – Доля добавленной стоимости в продукции – Стабильность контрактной базы – Доступность и диверсификация рынков сбыта, доля экспорта
Третичный сектор	– Качество инфраструктуры (в том числе степень износа, технологический уровень) – Право собственности на инфраструктуру – Диверсификация услуг – Профессионализм персонала – Уровень риска поставщиков – Регуляторные факторы – Широта охвата рынка сбыта – Эластичность спроса – Уровень социально-экономического развития обслуживаемых регионов
Четвертичный сектор	– Качество инфраструктуры (принадлежность к последнему технологическому поколению) – Уровень квалификации персонала – Уникальность ключевых продуктов – Диверсификация выручки – Волатильность спроса – Уровень инновационности

Уровень отраслевых рисков определяется следующими параметрами:

- цикличность отрасли: подверженность циклическим колебаниям усиливает рискованность отрасли;
- стадии жизненного цикла отрасли: наименее рискованные отрасли – находящиеся на стадии зрелости и роста; наиболее рискованные – на фазе упадка и зарождения;
- уровень внутриотраслевой конкуренции: чем она выше, тем выше отраслевой риск.

Эти факторы усиливают волатильность отраслевых показателей и увеличивают уровень отраслевого риска. Принадлежность к определенному сектору приводит к возникновению специфических для данного сектора рисков.

Риски первичного сектора связаны с волатильностью цен на добываемое сырье, с экспортно-ориентированностью сектора, с опасными производственными факторами и негативным влиянием предприятий сектора на окружающую среду; состав рисков включает рыночные ценовые и валютные риски, экологические риски, риски промышленной безопасности, риск утраты социальных лицензий.

Риски вторичного сектора связаны с эксплуатацией производственных мощностей и возможными событиями технико-производственного характера, возможным отставанием в сфере НИОКР, технологическом развитии, возможным снижением конкурентоспособности продукции; состав рисков включает технико-производственные и технологические риски.

Риски третичного сектора связаны с человеческим капиталом, поскольку персонал непосредственно взаимодействует с потребителями, формирует лояльность и рыночную компоненту социально-репутационного капитала; состав рисков включает кадровые и репутационные риски.

Риски четвертичного сектора связаны с интеллектуальным капиталом, с необходимостью постоянно генерировать инновации для удержания рыночных позиций, а также с агрессивной стратегией инвестирования предприятий сектора; состав рисков включает инновационные, кадровые, репутационные [4].

Состав отраслевых рисков представлен в таблице 2.

Таблица 2 – Риски для отраслей отдельных секторов экономики

Сектор экономики	Риски сектора
Первичный сектор	- Рыночные ценовые и валютные риски - Правовые риски - Риски истощения месторождений - Экологические риски
Вторичный сектор	- Технико-производственные риски

	– Технологические риски – Рыночные ценовые риски на сырье – Ценовые риски на продукцию
Третичный сектор	– Кадровые риски – Репутационные риски
Четвертичный сектор	– Инновационные риски – Кадровые риски – Репутационные риски – Инвестиционные риски – Риски информационной безопасности

Переходя к рассмотрению факторов доходности и рисков электронной промышленности следует отметить, что реализуемая Правительством Стратегия развития электронной промышленности [1] обеспечивает повышение привлекательности отрасли в результате поддержки спроса на отечественную электронику, снижения налоговой нагрузки на производителей, увеличения объема финансовых ресурсов, направляемых в отрасль. В качестве ключевых факторов доходности отрасли можно отметить следующие:

- доступность финансовых ресурсов для своевременного обновления оборудования и технологий;
- технологический уровень оборудования;
- активная инвестиционная деятельность, агрессивная стратегия инвестирования;
- уровень профессионализма персонала;
- способность генерировать инновации;
- репутация у потребителей;
- стабильность контрактной базы, наличие государственных контрактов;
- устойчивые связи с зарубежными поставщиками, сотрудничество с мировыми IT разработчиками.

Что касается отраслевых рисков, то поскольку отрасль можно отнести к четвертичному сектору экономики, то для нее наиболее значимыми являются риски этого сектора [1]:

- недостаточность объема финансирования;
- неэффективное использование финансовых ресурсов;
- непрогнозируемый рост стоимости входа на новые рынки и освоения новых технологий;
- гиперконкуренция на глобальных рынках;
- дефицит квалифицированных кадров;
- несоответствие продукции ожиданиям потребителей;
- появление потребностей, которые не могут быть удовлетворены отраслью электронной промышленности;

- недоступность передовых технологий;
- низкая скорость принятия решений, административные барьеры;
- недостаточность информации для принятия решений.

Комплексная оценка факторов доходности и рисков предприятий электронной промышленности выполнена на основе выборки предприятий электронной промышленности, таблица 3.

Таблица 3 – Характеристики отраслевой выборки

Показатели	Значения
Период	2017-2020 г.
Регион деятельности	Любой
Вид деятельности по ОКВЭД	ОКВЭД 26 Производство компьютеров, электронных и оптических изделий, отдельные пункты ОКВЭД 27 Производство электрических изделий, 28 Производство готовых металлических изделий, 32 Производство прочих готовых изделий
Организационно-правовые формы юридических лиц	Любая
Форма собственности	Любая
Статус	Любой: действующая организация, в состоянии банкротства, в состоянии ликвидации
Ограничения по выручке	От 1 млн руб.
Объем выборки	8 202 организаций

Результаты расчетов представлены в таблице 4.

Таблица 4 – Комплексная оценка факторов доходности и рисков предприятий отрасли

Показатели	Значения (медианы), 2019 год	Значения (медианы), 2020 год
Среднегодовой темп прироста активов (за 3 года), %	11,98	12,09
Среднегодовой темп прироста выручки (за три года), %	7,80	4,04
Среднегодовой темп прироста чистой прибыли (за три года), %	10,47	6,94
Доля собственного капитала в источниках финансирования, %	43,40	44,54
Доля организаций, имеющих долгосрочный заемный капитал, %	21,06	24,59
Доля долгосрочного заемного капитала в источниках финансирования, %	14,76	12,67
Производительность труда, тыс. руб. / чел.	2 695	2 960
Средняя годовая заработная плата, тыс. руб. / чел.	661	689

Инвестиции к выручке, %	1,61	1,41
Норма инвестирования (инвестиции к прибыли до вычета процентов, %	11,17	9,86
Отношение инвестиций к дивидендам	0,33	0,25
Рентабельность собственного капитала, %	20,40	19,69
Рентабельность инвестированного капитала, %	17,31	16,54
Средневзвешенная стоимость капитала, %	11,61	12,23
Спред, %	5,70	4,31
Экономическая прибыль (медиана), тыс. руб.	142,91	151,84
Коэффициент Д. Бейна (медиана), %	11,85	10,02
Вклад в ВВП, %	1,74	1,79

Выполненные расчеты не позволяют сделать вывод о значительных позитивных изменениях в отрасли. Важнейшие факторы роста – приток финансовых ресурсов, инвестиции и качество персонала не демонстрируют требуемой динамики. Так, менее 25% предприятий отрасли имеют долгосрочный заемный капитал, который, наряду с собственным является источником финансирования развития отрасли. Инвестиционная активность снижается, предприятия тратят менее 2% от выручки на инвестиционные цели. Динамика производительности и заработной платы положительная, но темп изменения крайне низкий.

Следует отметить, что рост активов предприятий отрасли усилился, что, вероятно, связано с реализацией Стратегии развития электронной промышленности [1], при этом рост финансовых результатов, наоборот, замедлился, поэтому можно констатировать снижение эффективности использования активов, но при этом повышение эффективности контроля над расходами (поскольку темп прироста чистой прибыли опережает темп прироста выручки). Финансовая политика предприятий становится более агрессивной в части дивидендных выплат – соотношение инвестиций и дивидендов снижается, отражая снижение инвестиционной активности и повышение дивидендных выплат. Показатели эффективности достаточно высоки, но это в значительной степени связано со снижением инвестиционной активности и капитала предприятий отрасли. Доля отрасли в ВВП увеличивается за счет небольшого роста при снижении ВВП страны в 2020 году, вследствие пандемии. Такие результаты 2020 года, первого года реализации Стратегии развития отрасли, отчасти связаны с глобальной стагнацией, нарушением глобальных цепочек поставок и дефицитом электронных компонентов, сокращением покупательной способности потребителей. Однако в будущем, с учетом принимаемых Правительством дополнительных мер по стимулированию развития отрасли можно ожидать роста показателей роста и доходности отрасли при поддержании приемлемого уровня рисков.

Список использованных источников:

1. Стратегия развития электронной промышленности РФ на период до 2030 г. и плане мероприятий по ее реализации. Утв. Распоряжением Правительства РФ от 17 января 2020 г. №20-р
2. Клейнер Г.Б. Мезоэкономическая одиссея: между Сциллой макроэкономики и Харибдой микроэкономики //Вопросы экономики. 2020. №10. С. 144-153
3. В.Г. Когденко. Исследование рисков в рамках стейкхолдерского подхода / Экономический анализ: теория и практика, 2018, т. 17, вып. 6, стр. 1051–1072 <http://fin-izdat.ru/journal/analiz/>
4. Когденко В.Г. Управление финансами и рисками. Монография. М.: ЮНИТИ-ДАНА. 527 с.

Кибербезопасность в Республике Беларусь

Д.А. Алябьева

студент 3 курса ФФБД БГЭУ, Минск

E-mail: aljabjevadasha@gmail.com

У.Ю. Басалыга

студент 3 курса ФФБД БГЭУ, Минск

E-mail: basalyga1010@gmail.com

Научный руководитель: В.В. Позняков

к.э.н., доцент кафедры банковского дела БГЭУ, Минск

E-mail: Pozniakov@bseu.by

Аннотация: статья посвящена исследованию кибербезопасности на территории Республики Беларусь. Авторами представлены виды киберпреступлений, рассмотрены способы мошенничества, а также предложены пути их решения и перспективы развития информационной безопасности при изменяющихся тенденциях в экономике.

Ключевые слова: кибербезопасность, киберпреступления, мошенничество, кибератака, кибертерроризм, вишинг, фишинг.

Cybersecurity in the Republic of Belarus

Abstract: the article is devoted to the study of cybersecurity on the territory of the Republic of Belarus. The authors present the types of cybercrimes, consider the methods of fraud, and also suggest ways to solve them and the prospects for the development of information security in the face of changing trends in the economy.

Keywords: cybersecurity, cybercrime, fraud, cyberattack, cyberterrorism, wishing, phishing.

В наше время все без исключения секторы экономики активно внедряют продукты цифровизации, а пандемия лишь способствовала ускорению этого процесса. Поэтому масштаб распространения киберугроз год за годом в мире увеличивается и происходит большая утечка данных. Актуальность темы исследования заключается в том, что, учитывая быстрые темпы компьютеризации населения и технологического развития общества, кибербезопасность должна обладать защищенностью в

отношении информации, которая может пострадать в результате противоправных действий тех или иных лиц.

Можно выделить факторы, которые стимулируют рост киберпреступлений. Поскольку в 2020 году доля населения, пользующаяся Интернетом, составила 85,1 %, то следует говорить об опережающих темпах освоения сети Интернет в Беларуси. Как итог, наша страна вышла на европейские показатели по плотности проникновения в сеть, а по скорости – на одни из первых позиций в мире. Говоря об уровне компьютерной грамотности граждан, он недостаточно высок, что свидетельствует о нехватке скорости внедрения компьютерных систем в повседневную жизнь. Первопричиной стало неответственное отношение к защите и безопасности личных данных и собственной информации. Также пандемия способствует ускорению перехода многих сфер экономических отношений, включая товарный и денежный обороты, в сеть Интернет [3].

Соответственно причинами существования кибератак являются: прибыльность, простота исполнения, низкий уровень риска, появление новых сервисов информационные войны. К типам угроз кибербезопасности относятся: вредоносное ПО, социальная инженерия, программы-вымогатели, фишинг.

Из-за того, что увеличилось число пользователей электронных платежных систем, абонентов сотовой связи, держателей платежных карт, которые в сумме составляют интернет-пользователей, произошел рост киберпреступности в Республике Беларусь. Этому поспособствовало развитие системы безналичных расчетов и появление устройств, осуществляющих финансовые транзакции. Приведенные причины привели к увеличению сегмента рынка визуальной территории, то есть людей уже не удивляет изобилие и доступность гаджетов, а также возможность подключения к интернету многих видов бытовой техники [5, с. 162].

Сравнивая 2014, 2019 и 2020 годы, можно судить о преобладании преступлений, связанных с малообеспеченными гражданами и пенсионерами путем использования IT-технологий, что составляет четвертую часть всех преступлений. В 2020 году всего зарегистрировано 95 тыс. преступлений, включая более 25 тыс. компьютерных преступлений, 92% из которых составляли хищения. В 2014 году их численность составляла 2,3 тыс., а по сравнению с 2019 годом – в два с половиной раза больше. Поэтому сегодня наблюдается рост подобных преступлений в 10 раз [1].

Актуальной проблемой является большое число актов кибертерроризма на территории Республики Беларусь, потребовавших немедленное реагирование со стороны правоохранительных органов, большинство из которых – сообщения о минировании аэропортов, торговых центров и

других мест массового скопления людей. Ни в одном случае не было найдено взрывчатых веществ, однако, правоохранительными органами были предприняты все необходимые меры по обеспечению безопасности в кратчайшие сроки. Необходимо подчеркнуть, что дезинформирование влечет за собой негативные последствия: ложное сообщение об опасности может спровоцировать панику; существенные затраты человеческих, материальных и финансовых ресурсов; причинение неудобств гражданам; нарушение работы субъектов хозяйствования.

Второй немаловажной проблемой является вишинг. Он подразумевает звонок клиентам банков злоумышленниками, которые представляются сотрудниками. Далее они под различным предлогом просят предоставить реквизиты банковских карт или паспортные данные. Обычно преступники используют программу-анонимайзер. С помощью нее обычный телефон злоумышленника определяется как официальный, так как подлог на одну цифру из номера визуально не заметен. При разговоре на фоне также используется имитация звука контакт-центра банка. Следует помнить, что сотрудники банка заранее должны знать все данные о клиенте, поэтому не следует сообщать личную информацию любому звонящему человеку. Если так случилось, что данные оказались у преступника и был установлен факт хищения, то следует заблокировать карту и обратиться с заявлением в правоохранительные органы. На первое полугодие 2021 года зафиксирован рост хищений денежных средств на 270% больше, чем с аналогичным периодом 2020 года [1,6].

В течение последних лет участились случаи формирования фишинговых веб-сайтов, направленных под требования пользователей в сети Интернет. Жители Республики Беларусь после запросов из Яндекс и Google напрямую попадают на них. Пользователи, не удостоверившись в правильности и соответствии адреса необходимой страницы, полагаясь на знакомый логотип или заголовок в выдаче итогов проделанного запроса, заполняют предложенную конфигурацию авторизации, сведения которой переходят не банку, а злоумышленнику.

Помощь другим людям – еще один тип аферы в сети Интернет, деятельность которого состоит в создании поддельных благотворительных фондов, реализующих сбор средств на лечение. В подобных ситуациях, мошенники формируют группу для распространения ложной информации о том, что необходимы денежные средства с целью лечения труднобольного человека (в большинстве случаев – ребенка). Чтобы не угодить в руки таких мошенников, следует требовать дополнительные данные и документы.

Большая часть киберпреступлений осуществляется за пределами страны с применением технологических, финансовых площадок

(криптовалютных кошельков) и Интернет-ресурсов. А также с использованием специализированных сервисов, позволяющих мошенникам укрывать собственные сведения и место доступа к сети, из-за пределов Республики Беларусь. Злоумышленники пользуются доступом банковских сайтов и учетными записями физических лиц с зарубежных либо анонимных IP-адресов, с использованием подставных лиц, на которых оформлены банковские платежные карточки, абонентские номера операторов мобильной связи, почтовые доставки.

Согласно суждению специалистов, изучающих вопрос о самой подвергаемой мошенничеству массе населения, чаще всего потерпевшей становится та часть людей, которая использует множество устройств в доме и на работе, при этом обладая незначительным пониманием основ кибербезопасности или в целом не имеют такого понимания. В большинстве случаев подобные пользователи выбирают идентичный пароль к различным социальным сетям и также могут им поделиться с другими лицами. Поэтому такая масса населения обладает низкой правовой грамотностью по вопросам кибербезопасности и формирует обширную почву для развития правонарушений и преступлений в информационной области. Недостаток знаний создает иллюзию дозволенности действий, нарушающих права и свободы других граждан, права обладателей авторских и смежных прав. Низкая цифровая грамотность пользователей в вопросах защиты личных сведений при нехватке базовых основ, согласно общепринятым методам распространения компьютерных программ и программных продуктов, приносящих вред, приводят к многочисленным негативным случаям, когда граждане Республики Беларусь становятся жертвами, а принадлежащие им технические средства — орудиями противоправного применения ИКТ.

Таким образом, статистика свидетельствует о том, что проблема киберпреступности с каждым годом привлекает к себе всё больше внимания и требует совершенствования существующих подходов для эффективного противодействия преступникам новой информационной эры. В то время как кибертерроризм – явление для Республики Беларусь принципиально новое, и на сегодняшний день опыт Беларуси показывает, что акты кибертерроризма в стране имеют одну и ту же форму [4, с. 327].

Поэтому киберпреступность является удобным способом причинения вреда злоумышленниками. Это объясняется тем, что, используя современные технологии, можно достаточно быстро и анонимно совершить преступления, находясь практически в любой точке Земли. Киберпреступления необходимо анализировать и распространять информацию о них среди обычных граждан [2, с.234].

Итак, можно выделить компоненты для защиты, например, интеллектуальные устройства, маршрутизаторы и облачная среда. Защита происходит от временной потери доступа к важной информации, что несет остановку бизнес-процессов, потерю контактов, ущерб репутации компании, повышение страховых взносов. Технологией для защиты перечисленных компонентов является защита от вредоносного ПО, фильтрация DNS, антивирусное ПО, межсетевые экраны.

В Республике Беларусь проходит Декада кибербезопасности – это профилактическая акция, которая включает комплекс мероприятий по информированию населения о методах и способах хищений, используемых киберпреступниками, мерах противодействия и профилактики. То есть сотрудники правоохранительных органов расскажут в радио, телеэфирах и газетах о видах киберпреступлений. Данный материал будет распространяться в виде видеороликов и листовок в транспорте, магазинах и других общественных местах. Кроме того, организуют профилактические беседы в организациях и учреждениях с уязвимыми категориями населения. С помощью таких акций за полугодие 2021 года количество киберпреступлений снизилось на 17,6%, чем в прошлом году в аналогичном периоде.

Защита данных компонентов определена в Государственной программе развития цифровой экономики и информационного общества на 2021—2025 года. Данная программа содержит основные мероприятия по предотвращению и недопущению угроз в сфере кибербезопасности: повышение компетенций в информационной безопасности компаний и государственных структур; непрерывный обмен данными об информационных инцидентах и технологиях защиты между компаниями и общественными организациями на международном уровне; организация мер защиты и безопасности не только основных объектов экономики, но и банковской и платежных систем; запуск новых продуктов и программ страхования от киберугроз, повышение финансовой грамотности населения. Таким образом Государственная программа повлияет на усиление мер кибербезопасности при активном развитии цифровизации в экономике, мы увидим в ближайшем будущем.

Список использованных источников:

1. В Беларуси в 2020 году зарегистрировано более 25 тыс. киберпреступлений. URL: <https://pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2021/aprel/62257/> (дата обращения: 18.11.2021).
2. Киберпреступность в Республике Беларусь: состояние и пути противодействия. URL:

- <http://rep.barsu.by/bitstream/handle/data/3968/Kiberprestupnost%20v%20Respublike%20Belarus%20sostojanie%20i%20puti%20protivodejstviya.pdf?sequence=1&isAllowed=y> (дата обращения: 17.11.2021).
3. Основные аспекты профилактики киберпреступности В Республике Беларусь. URL: https://minsk.gov.by/ru/actual/view/209/2021/inf_material_2021_05.shtml (дата обращения: 17.11.2021).
 4. Проблема обеспечения кибербезопасности в Белоруссии, России и Украине. URL: <https://cyberleninka.ru/article/n/problema-obespecheniya-kiberbezopasnosti-v-belorussii-rossii-i-ukraine/viewer> (дата обращения: 18.11.2021).
 5. Проблемы обеспечения кибербезопасности в Республике Беларусь. URL: <https://elib.bsu.by/bitstream/123456789/215917/1/162-163.pdf> (дата обращения: 17.11.2021).
 6. Профилактика и противодействие киберпреступности. URL: http://www.mogileviro.by/?page_id=6798 (дата обращения: 17.11.2021).

Комплекс мер по противодействию угрозам финансовой безопасности России с учетом взаимовлияния уязвимостей финансовых институтов и домохозяйств

Е.Н. Алифанова

д.э.н., профессор, зав.кафедрой финансового мониторинга и финансовых рынков РГЭУ (РИНХ), г. Ростов-на-Дону

E-mail: alifanovaen@mail.ru

Ю.С. Евлахова

д.э.н., профессор кафедры финансового мониторинга и финансовых рынков РГЭУ (РИНХ), г. Ростов-на-Дону

E-mail: evlahova@yandex.ru

Л.И. Ниворожкина

д.э.н., профессор, зав.кафедрой статистики, эконометрики и оценки рисков РГЭУ (РИНХ), г. Ростов-на-Дону

E-mail: lin45@mail.ru

А.А. Трегубова

к.э.н., доцент кафедры статистики, эконометрики и оценки рисков РГЭУ (РИНХ), г. Ростов-на-Дону

E-mail: alexandra_a_t@mail.ru

Аннотация: в статье представлен комплекс мер по противодействию угрозам национальной безопасности России в финансовой сфере с учетом взаимосвязи рисков финансовых институтов и домохозяйств. Данные рекомендации сформулированы по итогам авторских исследований.

Ключевые слова: риск-ориентированный подход, финансовая безопасность, финансовые институты, финансовое поведение населения, противодействие отмыванию денег и финансированию терроризма.

Measures to counter threats to Russia's financial security considering the mutual influence of financial institutions and households vulnerabilities

Abstract: the article presents a set of measures to counter threats to Russia's national security in the financial sphere, taking into account the relationship between the risks of financial institutions and households. These recommendations are formulated on the basis of research.

Keywords: risk-focused approach, financial security, financial institutions, financial behaviour of households, countering money laundering and terrorist financing.

Современная экономическая неопределенность, в которой усилия стран по сохранению экономического суверенитета и стабильного финансового развития сопровождаются беспрецедентным внешним экономическим, политическим, информационным давлением, актуализирует важность обеспечения национальной безопасности в финансовой сфере, в рамках которой оценка национальных рисков отмывания денег и финансирования терроризма способна дать ориентиры для превентивных действий и расставить приоритеты при выборе мер реагирования.

Объективная потребность в оценке национальных рисков отмывания денег и финансирования терроризма учитывать и прогнозировать отклики населения на изменения в условиях функционирования финансовых институтов, с одной стороны, и возможное воздействие девиантного поведения населения на деятельность финансовых институтов, с другой стороны, легли в основу ключевой идеи исследования – концепции взаимовлияния уязвимостей финансовых институтов и домохозяйств как нового элемента методологии национальной оценки риска отмывания денег и финансирования терроризма [1]. На основе выявленных в исследовании закономерностей с учетом взаимосвязи рисков домохозяйств и финансовых институтов был разработан комплекс мер по противодействию угрозам национальной безопасности России в финансовой сфере и мероприятий по снижению рисков финансовой безопасности.

Выявление и структурирование угроз национальной финансовой безопасности проведено на основе отчетов 27 стран мира о национальной оценке риска отмывания денег и финансирования терроризма за период 2013–2018 гг. В основе оценки - использование авторского коэффициента интенсивности проявления угроз национальной финансовой безопасности, который является нормированной величиной, принимающей значение от 0 до 1. В случае если все страны испытывают угрозы, то коэффициент равен 1. Если нет ни одной угрозы, то коэффициент равен 0. Таким образом, предлагаемый коэффициент является статистической мерой, отражающей распространенность угроз среди анализируемых стран. На этой основе составлена матрица распределения угроз финансовой безопасности по странам и выявлена структура угроз по степени их интенсивности [2].

Количественная оценка частоты распространения угроз финансовой безопасности в страновом разрезе показала, что угрозы национальной финансовой безопасности могут быть общими, встречающимися разных странах, или уникальными, наблюдаемыми только в конкретной стране.

Соответственно, общие для стран угрозы могут предотвращаться общими, типовыми способами, тогда как уникальные угрозы требуют разработки уникальных способов противодействия им. Практическая значимость авторского коэффициента интенсивности проявления угроз национальной финансовой безопасности состоит в том, что с его помощью становится возможным определить характер угрозы, и в соответствии с ним использовать адекватные инструменты реагирования.

Проведенный авторами анализ [2] показал, что в России не наблюдаются уникальные, редко встречающиеся, обусловленные экономической, правовой и иной спецификой угрозы. Поэтому в качестве меры по противодействию угрозам финансовой безопасности России нами рекомендуется опираться на лучшую отечественную практику выявления угроз, а также расширить данную практику за счет применения используемых в зарубежной практике подходов к оценке уровня конкретных угроз финансовой безопасности.

Одним из таких подходов является сопоставление масштаба угрозы с размерами того или иного сектора экономики или отрасли народного хозяйства. Например, в Австралии уровень угрозы финансирования терроризма в секторе некоммерческих организаций (НКО) оценивается как средний, и НКО продолжают оставаться привлекательными для финансирования терроризма в качестве канала привлечения денежных средств и перевода их в офшор [3]. Тем не менее, объем финансирования терроризма с участием НКО является низким по сравнению с экономическими размерами сектора. Следовательно, важно выявлять НКО высокого риска, а не ужесточать требования по противодействию финансированию терроризма для всего сектора НКО [3].

Кроме того, считаем целесообразным в целях противодействия угрозам национальной финансовой безопасности в дополнение к оценке коэффициентов интенсивности проявления угроз в России и странах мира провести аналогичный анализ по отраслям и секторам российской экономики, что также может послужить ценным инструментом при проведении секторальной оценки рисков. Кроме того, количественная оценка частоты распространения угроз финансовой безопасности на основе предложенного коэффициента может быть проведена и на уровне межстрановых (региональных) объединений, участником которых является Россия, что позволит получить практически значимую информацию для международной оценки рисков.

Среди новых угроз национальной безопасности следует отметить пандемию коронавируса. Сложившаяся экономическая ситуация, картина рисков отмывания денег и финансирования терроризма свидетельствует о том, что на фоне пандемии возросли угрозы кибермошенничества с

использованием социальных сетей и фишинговых атак. Из-за масштабной государственной финансовой поддержки пострадавших от пандемии отраслей экономики и граждан увеличились риски хищения бюджетных средств. Своевременно принятые меры государственного контроля, а также мероприятия в сфере ПОД/ФТ, комплексно изложенные в [4], способствовали оперативному реагированию на данную угрозу национальной финансовой безопасности.

Однако помимо точечных источников рисков, связанных со спецификой борьбы с коронавирусом, значимой стала угроза финансовой нестабильности, нарастающая в периоды локальных локдаунов, обусловленных волнообразным характером распространения пандемии. Нестабильность деловой активности, особенно в среде малого и среднего предпринимательства, а также в отраслях, наиболее страдающих от локдаунов в региональной, национальной и зарубежных экономиках, снижение реальных доходов населения, отток вкладов физических лиц из банков и частичный их переток на фондовый рынок – во вложения в иностранные ценные бумаги – все это и многое другое свидетельствует о макроэкономическом шоке, спровоцированном пандемией коронавируса.

Мы полагаем, что для разработки органами государственной власти мер противодействия угрозе финансовой нестабильности может быть использован выявленный в работе [5] паттерн поведения российского банковского сектора в ответ на изменение активности домохозяйств на кредитном и депозитном рынках под влиянием макроэкономических шоков. Данный паттерн включает последовательность «реализация риска оттока вкладов – формирование зоны уязвимости к невозврату розничных кредитов – депозитный пузырь – кредитный пузырь».

Первая стадия – отток вкладов физических лиц – с середины 2020 года по настоящее время находится в активной фазе. Среди наиболее распространенных направлений перетока средств: инвестиции в фондовые инструменты, вложения в накопительные счета вместо срочных вкладов, а также приобретения полисов инвестиционного и накопительного страхования жизни. Полагаем, что в краткосрочной перспективе на поддержание оттока средств физических лиц с депозитов в российских банках будут сонаправленно действовать следующие факторы:

- фактор фондового рынка, означающий развитие систем дистанционного брокерского обслуживания и одновременно активизацию процессов по защите массовых инвесторов и противодействию недобросовестным практикам;
- налоговый фактор, подразумевающий распространение с 2022 г. налога на доходы физических лиц на проценты по вкладам, превышающие необлагаемый процентный доход.

Второй стадией паттерна является уязвимость к невозврату розничных кредитов. В работе [6] при анализе системно значимых банков как зоны уязвимости к угрозам финансовой безопасности мы обнаружили экспансию банков с государственным участием в капитале и их дочерних банков, в числе которых есть и системно значимые, на рынок необеспеченного потребительского кредитования. При этом в секторе необеспеченного кредитования населения сохраняются повышенные кредитные риски. Возможности по дальнейшему снижению ставок, поддерживавшие высокий спрос, к настоящему времени практически исчерпаны, вследствие чего исчезнет компенсирующее влияние снижения ставок на уровень долговой нагрузки домохозяйств, которое наблюдалось в течение 2015–2018 гг.

Таким образом, в секторе необеспеченного кредитования населения сформировались две уязвимости – в деятельности банков, включая системно значимые, и в поведении домохозяйств, взаимовлияние которых (через реализацию кредитных рисков, рост наличного денежного оборота и сокрытие доходов домохозяйствами) может привести к отрицательному синергетическому эффекту для всего российского финансового сектора.

Ключевым средством противодействия угрозе пандемии стало дистанцирование, перевод работы и услуг в дистанционный режим с помощью цифровых технологий. В свою очередь, это ускорило цифровую трансформацию российского финансового сектора и привело к появлению потенциальных – «цифrogenных» - угроз, обусловленных влиянием цифровизации на разные аспекты функционирования финансового рынка. Наиболее интенсивно финтех внедряется в область взаимодействия населения с финансовым рынком – цифровые платежные сервисы, открытие вкладов и кредитование без личного присутствия заемщика, инвестиционные услуги онлайн, робоэдвайзинг, маркетплейсы и краудфандинговые платформы и много другое. Все это свидетельствует о том, что есть практическая потребность в продолжении исследования операций населения на проходящем цифровую трансформацию финансовом рынке.

На основе данных мер по снижению угроз финансовой безопасности России, а также проведенного исследования нами также разработаны предложения Росфинмониторингу по совершенствованию национальной оценки риска отмыывания денег и финансирования терроризма, которые состоят в следующем.

Во-первых, считаем важным на этапе идентификации уязвимостей при проведении национальной оценки риска отмыывания денег и финансирования терроризма использовать матрицы уязвимостей финансовых организаций к риску отмыывания денег, которые позволяют

систематизировать индикаторы риска отмыwania денег в координатах «факторы влияния/зоны уязвимости».

Во-вторых, предлагаем при анализе зон риска в российской экономике в целях предотвращения пропусков (не идентификации) существующих или потенциальных угроз и/или уязвимостей проводить построение целостной цепочки событий /ситуаций – «угрозы – уязвимости - риски».

В-третьих, полагаем существенным для более точной оценки национального риска отмыwania денег и финансирования терроризма проводить расширение круга объектов мониторинга и оценки, являющихся реальными или потенциальными носителями риска отмыwania денег и финансирования терроризма, как за счет выделения конкретных фокус-групп в рамках известных объектов (в частности, системно значимых банков и страховщиков), так и за счет вовлечения в национальную оценку риска новых объектов (в частности, домохозяйств).

Таким образом, рекомендации, предложения и меры, подготовленные по результатам исследования проблемы развития системы национальной оценки риска отмыwania денег и финансирования терроризма на основе взаимовлияния уязвимостей финансовых институтов и домохозяйств, формируют основу для принятия решений государственными органами власти, мегарегулятором финансового рынка, подразделением финансовой разведки и правоохранительными органами в целях обеспечения национальной финансовой безопасности.

Статья подготовлена при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта 18-010-00657.

Список использованных источников:

1. Алифанова Е.Н., Евлахова Ю.С. Развитие методологии оценки рисков отмыwania денег и финансирования терроризма: интеграция концепции взаимовлияния уязвимостей финансовых институтов и домохозяйств // Экономика и управление: теория и практика. 2018. №4, Том 4 (ч.2). С.33-37.
2. Алифанова Е.Н., Ниворожкина Л.И., Евлахова Ю.С. Структура угроз финансовой безопасности по интенсивности проявления на международном уровне: методический подход и эмпирическая оценка// Статистика – язык цифровой цивилизации: сб. докладов международ. научно-практ. конф. «II Открытый российский статистический конгресс» (Ростов-на-Дону, 4-6 декабря 2018 г.): в 2 т. Т. 1./ Российская ассоциация статистиков; Федеральная служба государственной статистики РФ, Рост. гос. экон. ун-т (РИНХ),

- Ростовское региональное отделение ВЭО России. Ростов н/Д: АзовПринт, 2018. С. 115-120.
3. Australia's non-profit organization sector: money laundering and terrorism financing risk assessment, 2017. – Текст: электронный. // Официальный сайт Правительства Австралии. – URL: <http://www.austrac.gov.au/australias-npo-sector-risk-assessment> (дата обращения: 06.04.2020).
 4. Заявление Президента ФАТФ: COVID-19 и меры по борьбе с незаконными финансовыми операциями. – Текст: электронный // Официальный сайт Федеральной службы по финансовому мониторингу России. – URL: <https://www.fedsfm.ru/releases/4485> (дата обращения: 06.04.2020).
 5. Евлахова Ю.С., Алифанова Е.Н., Трегубова А.А. Паттерны поведения российских банков – ответ на финансовую активность населения в условиях макроэкономических шоков // Журнал НЭА. 2021. №2 (50). С.74-95.
 6. Евлахова Ю.С., Алифанова Е.Н. Системно значимые кредитные организации как зона уязвимости к угрозам финансовой безопасности России // Финансы и кредит. 2019. Т.25, №8. С.1712-1726. DOI: 10.24891/ fc . 25. 8. 1712

Комплексная оценка специалиста по финансовой безопасности как основа для построения его компетентностной модели

А.Н. Столярова

д.э.н., доцент, профессор кафедры менеджмента и экономики
ГОУ ВО МО «Государственный социально-гуманитарный университет»

E-mail: stolyarova2011@mail.ru

Д.С. Петросян

д.э.н., профессор, начальник отдела стратегических исследований
инновационного развития

АО «Институт региональных экономических исследований»

E-mail: pet_dav@mail.ru

А.Д. Петросян

к.э.н., заместитель директора Института социальной инженерии
ФГБОУ ВО «Российский государственный
университет им. А.Н. Косыгина»

E-mail: pad10806@yandex.ru

Аннотация: Одним из важных условий обеспечения национальной безопасности России является подготовка квалифицированных специалистов по финансовой безопасности. В статье показана роль объективной комплексной оценки специалистов по финансовой безопасности как основы для построения его компетентностной модели. Предложены комплексный подход к оценке специалистов по финансовой безопасности и основные составные элементы комплексной оценки, на основе которой определяется профессиональная пригодность специалиста по финансовой безопасности для построения его компетентностной модели.

Ключевые слова: специалист по финансовой безопасности, комплексная оценка, методы оценки, компетентностная модель профессиональная пригодность.

Financial security specialist complex assessment as a basis for building his competent model

Abstract: One of the important conditions for ensuring the national security of Russia is the training of qualified specialists in financial security. The article showed the role of an objective set of assessments of financial security

professionals as a basis for building its competent model. A complex approach to the evaluation of financial security specialists and the main components of the complex assessment were proposed, on the basis of which the professional suitability of the financial security specialist for the construction of his competent model was determined.

Keywords: financial security specialist, complex assessment, evaluation methods, competent model, professional suitability.

Анализ литературы в области подготовки специалистов по финансовой безопасности [3,4,6] показал, что оценка указанных специалистов является своеобразным инструментом, с помощью которого реализуется работа с кадрами в сфере обеспечения финансовой безопасности, а определение комплексной и объективной оценки указанных специалистов должна быть использована при построении компетентностной модели. Указанным вопросам посвящена предлагаемая статья.

Обобщение имеющихся результатов исследований в области оценки персонала [1,2] и наши исследования [5] позволили разработать методы комплексной оценки специалистов по финансовой безопасности. Комплексная оценка включает в себя следующие компоненты.

1. *Объективные характеристики*, которые охватывают используемые на практике «анкетные характеристики» и выходят согласно определению за их пределы, так как могут быть не привязаны к документу персонального учета кадров - «анкета». Объективные характеристики можно подразделить на три группы: необходимые, желательные и нежелательные. К первой группе относятся, например, наличие высшего образования и определенный в соответствии с должностью стаж работы, ко второй - определенный возрастной диапазон, к третьей - негативные параметры (дисциплинарные взыскания, судимость и т.д.). Объективные характеристики должны использоваться при реализации элементов работы со специалистами по финансовой безопасности в естественном виде, по наличию у оцениваемого специалиста требуемого значения характеристики. На основе этого принципа отбираются специалисты по финансовой безопасности, имеющие в наличии заданные значения характеристики.

2. *Личностные качества*. Все множество личностных качеств можно подразделить на качества, характеризующие личность специалиста по финансовой безопасности с точки зрения общественных позиций (нравственно-этические качества) и на качества, определяющие его как индивида (психологические качества). Основной проблемой методов оценки личностных качеств, является невозможность их измерения стандартными методами измерения параметров материальных объектов.

Наиболее эффективным подходом, снижающим субъективность оценки личностных качеств, выступают методы психологического тестирования.

3.Квалификационные характеристики. Уровень специальных знаний специалиста по финансовой безопасности и его практические умения можно оценивать методом экспертных оценок и при помощи квалификационных тестов. Методы экспертных оценок в данном случае представляют собой традиционный способ выявления и оценки знаний и умений и страдают известным субъективизмом. Более предпочтительнее применение специальных квалификационных тестов, позволяющих объективно оценивать знания и умения специалиста по финансовой безопасности.

4.Межличностные отношения. При социально-психологических исследованиях малых групп большое внимание уделяется методу социометрии. Социометрические статусы, определяющие положение (позицию) специалиста по финансовой безопасности в системе его взаимосвязей с членами коллектива рассчитываются по формулам:

- а) позитивный статус $A_j^+ = (\sum_i a_{ij}^+) : (n \cdot m)$
- б) негативный статус $A_j^- = (\sum_i a_{ij}^-) : (nm)$
- в) индекс социального внимания $A_j = A_j^+ + A_j^-$

n – число вопросов социометрического теста; m – число членов коллектива; a_{ij}^+ , a_{ij}^- – число позитивных и соответственно негативных выборов i -м членом коллектива j -го специалиста по финансовой безопасности.

5.Результаты труда. Предлагается подход суть которого сводится к тому, что результаты труда, представлены в виде единого количественного показателя, учитывающего в виде коэффициентов относительную сложность выполняемых трудовых функций, фактический и плановый индивидуальный вклад специалиста по финансовой безопасности, качество и своевременность выполнения функций. При определении коэффициентов необходимо добиваться их максимальной объективности.

Величина результатов труда Q специалиста по финансовой безопасности за некоторый период рассчитывается по формуле:

$$Q = \sum_r W_r \alpha_r \beta_r$$

где W_r - относительная оценка объема r - ой трудовой операции, расчет которой наиболее целесообразно методом парных сравнений экспертных оценок, так как число операций может быть довольно большим. Трудовая операция – это однородная технологически неделимую часть трудового процесса, направленную на достижение одной определенной цели, реализуемой специалистом по финансовой безопасности; α_r и β_r - соответственно коэффициенты качества и своевременности выполнения r - ой трудовой операции.

Результат труда специалиста по финансовой безопасности может быть рассчитан как разность между фактическим и плановым вкладом в совокупный результат труда коллектива.

Определение комплексной оценки специалиста по финансовой безопасности может стать основой для построения его компетентностной модели, определяющей профессиональную пригодность специалиста как степень развитости тех личностных качеств, которые способствуют эффективному осуществлению деятельности в сфере обеспечения финансовой безопасности. В самом общем виде все множество специалистов по финансовой безопасности, с точки зрения их пригодности к профессиональной деятельности, можно условно разделить на три большие группы: первая группа P_1 - это специалисты по финансовой безопасности, непригодные к данной деятельности, ко второй группе P_2 можно отнести специалистов по финансовой безопасности условно пригодных к данной деятельности. И, наконец, третья группа P_3 - это специалисты по финансовой безопасности относительно пригодные к данной деятельности. Мы назвали указанных специалистов «относительно пригодные», так как множество всех необходимых и достаточных качеств, которыми должен обладать идеальный специалист в данной деятельности в принципе вряд ли возможно определить.

Таким образом, оценка пригодности специалиста к профессиональной деятельности по обеспечению финансовой безопасности сводится к оценке личностных качеств и отнесению специалиста к одной из определенных выше трех групп. Для этого по каждому k -му качеству определяются три множества значений количественных оценок развития данного качества.

В первое множество оценок $O_1(k)$ включаются наиболее негативные оценки. В случае, если оценка специалист по финансовой безопасности входит в это множество, хотя бы по одному качеству, то его можно считать непригодным к осуществлению деятельности по обеспечению финансовой безопасности, так как не представляется возможным изменение этого качества за относительно короткий период обучения или самостоятельной подготовки. Второе множество оценок $O_2(k)$ определяет такие негативные значения оценок, которые возможно устранить за период обучения.

В случае, если все оценки специалиста по финансовой безопасности по всем качествам не принадлежат множеству $O_1(k)$, а хотя бы по одному качеству оценка принадлежит множеству $O_2(k)$, то специалист считается условно пригодным к тому или иному виду деятельности.

И, наконец, третье множество $O_3(k)$ определяет позитивные значения качества для осуществления деятельности по обеспечению финансовой безопасности. Если по всем качествам, оценки специалиста принадлежит

множеству $O_3(k)$, то он относительно пригоден к деятельности по обеспечению финансовой безопасности.

Формализовано условия профессиональной пригодности p -го специалиста по финансовой безопасности определяются по формуле:

$p \in P_1$, если $o(p,k) \in O_1(k)$, хотя бы по одному k ;

$p \in P_2$, если все $o(p,k) \notin O_1(k)$, а $o(p,k) \in O_2(k)$, хотя бы по одному k ;

$p \in P_3$, если $o(p,k) \in O_3(k)$ по всем k .

где $o(p,k)$ – оценка k -го качества p -го специалиста по финансовой безопасности.

В заключении отметим, что конкретизация параметров комплексной оценки и условий профессиональной пригодности явится методической основой для разработки компетентностной модели специалиста по финансовой безопасности.

Список использованных источников:

1. Анцупов А. Я., Ковалев В.В. Социально-психологическая оценка персонала. - М.: Юнити-Дана, 2017. - 391 с.
2. Асалиев А.М., Вукович Г.Г., Кириллова О.Г., Косарева Е.А. Оценка персонала в организации: учебное пособие. - 2-е изд., испр. и доп. – М. : ИНФРА-М, 2020. - 171 с.
3. Воробьев Ю.Н., Буркальцева Д.Д., Абибуллаев М.С. Финансовая безопасность: системный подход к подготовке специалистов // Финансы хозяйствующих субъектов: современные проблемы и пути их решения. сборник трудов по материалам Межкафедрального научно-практического семинара. - Симферополь: Крымский федеральный университет имени В.И. Вернадского, 2017. С. 50-52.
4. Муконина И.А. Разработка новых методов обучения специалистов финансовых организаций в области финансовой безопасности// Научные труды Нижневартковского государственного университета. Отв. ред. - А.В. Коричко. Нижневартовск: Нижневартковский государственный университет, 2017. С. 394-397
5. Петросян Д.С., Столярова А.Н., Лочан С.А., Чеглов В.П., Боташева Л.С., Машин Д.В. Объективная оценка результатов труда как фактор обеспечения национальной безопасности: вопросы теории и методологии//Инновации и инвестиции.2020.№3. С.128-135.
6. Хабибулин А.Г. Подготовка специалистов для обеспечения экономической и финансовой безопасности //Экономическая безопасность России: проблемы и перспективы. материалы V Международной научно-практической конференции. - Нижний Новгород: НГТУ им. Р.Е. Алексеева, 2017. С. 358-361.

Криптовалюта как угроза финансовой безопасности

Э.Э. Османова

студентка 2 курса Института экономики и управления,
ФГАОУ ВО «Крымский федеральный университет имени В.И.

Вернадского», Симферополь

E-mail: elmaz-osmanova@list.ru

Научный руководитель: О.Г. Блажевич

к.э.н., доцент кафедры финансов и кредита

Института экономики и управления, ФГАОУ ВО «Крымский
федеральный университет имени В.И. Вернадского», Симферополь

E-mail: blolge@rambler.ru

Аннотация: Статья посвящена проблеме криптовалюты как одной из важнейших угроз финансовой безопасности. В статье будут подниматься вопросы основных угроз, возникающих вследствие роста популярности такой цифровой валюты как криптовалюта. Кроме того, приведены примеры мошеннических операций на рынке криптовалюты. А также рассмотрен вопрос вероятности возникновения финансового кризиса, который может превзойти по своим масштабам кризис 2008 года.

Ключевые слова: криптовалюта, криптовалютный рынок, финансовый рынок, биткойн, цифровая валюта.

Cryptocurrency as a threat to financial security

Abstract: the article is devoted to the problem of cryptocurrencies as one of the most important threats to financial security. The article will raise issues of the main threats arising from the growing popularity of such a digital currency as cryptocurrency. In addition, examples of fraudulent transactions in the cryptocurrency market are given. And also, the question of the probability of a financial crisis, which may surpass the crisis of 2008 in its scale, is considered.

Keywords: cryptocurrency, cryptocurrency market, financial market, bitcoin, digital currency.

В настоящее время технологии способствуют не только изменению условий работы людей, методов их общения, способов совершения покупок, но даже форм оплаты товаров и услуг. Стоит отметить, что теперь

компании и их клиенты довольно редко стали использовать наличные деньги, так как теперь стали отдавать предпочтение бесконтактным средствам оплаты, таким как Apple Pay, Qivi, Pay Pal и другие. Кроме того, теперь появились смартфоны, функции которых позволяют потребителям оплачивать товары в цифровых форматах, не выходя из дома. Развитие цифровизации не стоит на месте и стала набирать популярность новая платежная система - криптовалюта.

Помимо криптовалюты, быстрыми темпами набирает популярность биткойн. Биткойн представляет собой первый в мире вид криптовалюты, который стал мейнстримом, но при этом популярность других видов криптовалют ежедневно увеличивается. На данный момент уже существует более двух тысяч различных видов криптовалют, и с каждым днем разрабатываются новые.

С 1 января 2021 года в Российской Федерации за криптовалютой официально закреплён статус имущества, что позволило россиянам декларировать доход от криптовалют. Кроме того, нововведения затронули и сферу налогообложения: был введен налог на прибыль от цифровых активов.

Криптовалюта представляет собой определенный вид цифровой платежной системы, при котором банками не проводится проверка транзакций. Кроме того, это одноранговая система, с помощью которой любой человек в любом месте без каких-либо сложностей и помех может отправлять и получать платежи. Потому что криптовалюта это не физические деньги, которые приходится носить с собой и обменивать в реальном мире, ведь платежи через криптовалюту существуют исключительно в виде цифровых записей в онлайн-базах данных, которые описывают конкретные транзакции. При осуществлении переводов средств в криптовалютах происходит запись транзакций в открытые регистры. Хранится криптовалюта в цифровых кошельках пользователей. Для хранения и передачи данных о криптовалюте между кошельками и в открытые регистры используется расширенное кодирование. Основной целью данного кодирования, или шифрования, является обеспечение безопасности.

Основным способом создания криптовалют является технология блокчейн. Блокчейн описывает определенные способы записи транзакций в «блоки» с отметками времени, что представляет собой достаточно сложный технический процесс, в результате которого создается цифровой регистр криптовалютных транзакций, который хакерам очень сложно взломать.

Кроме того, данные транзакции требуют двухфакторной аутентификации. Но стоит отметить, что все перечисленные защитные

меры не дают уверенности в том, что криптовалюты невозможно взломать. Существует немало случаев, когда несколько подготовленных взломов слишком дорого обошлись владельцам цифровых кошельков. По данным Investopedia, в 2018 году злоумышленники взломали Coincheck и BitGrail. Общая сумма украденных средств составила 534 миллиона долларов и 195 миллионов долларов соответственно [3].

Активное использование в настоящее время криптовалюты обусловлено упрощенностью многих операций с данными видами валюты. Цифровые деньги, или криптовалюта имеют много общего с текстовыми файлами, ведь переводы проходят не сложнее рассылки электронной почты друзьям. Еще одной особенностью криптовалюты, которая активно привлекает мошенников, занимающихся легализацией (отмыванием) доходов, полученных преступным путем, является анонимность проводимых операций. Ведь владельцы криптовалюты могут проводить необходимые транзакции напрямую, без какого-либо участия банков и других посредников. Для этого необходимо знать лишь номер кошелька. Такие персональные данные о владельце криптовалюты, как имя, страна или номер телефона не обязательны, так как большая часть криптовалют является анонимной. Примером таких криптовалют является биткойн, на который в настоящее время, по данным CoinMarketCap, являющимся в своем роде аналогом Forbes для криптовалют, приходится около 40% от общей капитализации рынка криптовалют, а общий объем капитализации рынка криптовалют в настоящее время составляет 138 млрд долларов [4].

Но стоит разобраться в теме более углубленно и данный вид цифровой валюты перестает казаться таким удобным и безопасным. В статье будут выделены основные риски для финансовой безопасности, связанные с ростом активности на рынке криптовалют.

К основным угрозам криптовалюты можно отнести: нестабильность курса криптовалют, ошибки системы криптовалюты, высокая вероятность возникновения так называемого «финансового пузыря», активное развитие мошенничества в данной сфере. Разберем каждую угрозу более подробно.

Сущность первой угрозы обусловлена нестабильностью и цикличностью курса и рынка криптовалют в целом, так как криптовалюта сама по себе не имеет единого курса. К примеру, курс популярного в настоящее время биткойна изменяется несколько раз в день, и когда участники рынка криптовалют стараются на этом заработать, то есть купить данную цифровую валюту как можно дешевле, чтобы в дальнейшем при повышении курса продать ее дороже. Однако из-за высокой цикличности курса, во время продажи биткойн успевает изменить свой курс несколько раз. Поэтому вкладывая в него участники рынка должны учесть особенности данного рынка и быть готовыми к потере инвестиций.

Более того, большинство видов криптовалют не только не имеют единого курса, но и не имеют единого банка, который мог бы контролировать систему в общем. В основе данных цифровых валют лежит доверие пользователей. После глобального хакерского взлома в июле 2017 года одной из крупнейших биткоин-бирж, курс биткоина резко упал с 2,6 тысяч долларов до 1,9 тысяч долларов за единицу. Что в дальнейшем повлекло за собой потерю доверия к криптовалюте, хотя хакеры взломали не сам биткоин, а лишь его стороннюю систему.

Редакция журнала The Outline, рассказывающего о цифровом мире, предположила, что значительный рост курса криптовалют вызван ростом популярности данного вида цифровой валюты. Один из журналистов The Outline для подтверждения данной гипотезы провел наблюдение и обнаружил, что большая часть его коллег, которые освещают темы криптовалют, уже имеют собственные счета в биткоинах. Он отметил, что после публикации его коллегами некоторых статей курс биткоина вскоре может в корне измениться. Это говорит о том, что существует некоторая вероятность того, что в случае, если о биткоине перестанут говорить, то он потеряет популярность, а вскоре и часть своей стоимости [5].

Следующая угроза связана с ошибками системы криптовалюты. Появление функционирующих криптовалют, таких как биткоин, произошло относительно недавно в 2009 году, поэтому сейчас они находятся на стадии разработки и исправления ошибок. Например, в августе 2017 года произошло деление биткоина на две самостоятельные криптовалюты - Bitcoin и Bitcoin Cash. А произошло это из-за того, что многие пользователи биткоина решили вмешаться в код и улучшить биткоин. Однако другая часть пользователей наоборот хотела оставить без изменений существующую систему. Важным условием рынка криптовалют является то, что изменения в системе не могут быть произведены, пока на это не дадут согласие все пользователи децентрализованной системы криптовалюты. Так как стороны не пришли к компромиссу, то произошло разделение биткоина на две части. То же самое произошло и с другой криптовалютой Ethereum, которая в результате взлома хакеров разделилась на две части.

Ежедневно увеличивалось количество пользователей системой биткоина, но пропускная способность биткоина ограничивалась всего семью транзакциями в секунду, что было достаточно неудобно для участников рынка. Например, в настоящее время такие платежные системы как Visa и Mastercard уже могут производить около 2000 транзакций в секунду, что говорит о развитии цифровой сферы.

Также немаловажной угрозой для финансового рынка является высокая вероятность возникновения финансового пузыря. Возникновение

финансового пузыря происходит, когда большое количество денег стоит за небольшим количеством активов, результатом чего становится переоценка данных активов. Роберт Шиллер, лауреат Нобелевской премии по экономике 2013 года, считает, что биткоин выступает наилучшим примером спекулятивного пузыря.

Анонимность криптовалюты, которая и привлекает владельцев данной цифровой валюты, также может сыграть против них. Ведь из-за отсутствия возможности отследить владельцев криптовалют, она и пользуется большой популярностью у мошенников, торговцев оружием и наркотиками. Криптовалюта выступает очень удобным средством, которое позволяет преступным группам проводить переводы средств и при этом оставаться незамеченными. Криптовалюта также имеет высокую популярность среди участников «даркнета», так как пользователей данной сети сложно и в большинстве случаев даже невозможно отследить из-за нестандартных протоколов связи.

Также из-за анонимности транзакций и различных связей между кошельками полностью исключается возможность возвращения биткоинов, украденных мошенниками. Программист Джеймс Хауэллс потерял свой жесткий диск, на котором хранились данные о 7500 биткоинах. Из-за полной анонимности системы биткоинов Хауэллс не смог доказать, что именно он является владельцем потерянных биткоинов. Кроме того, если владелец цифровой валюты потеряет свой секретный ключ, из-за высокого уровня анонимности восстановить его будет невозможно.

Рост популярности данного вида цифровой валюты повлек за собой и рост мошенничества в данной сфере. Кроме того, что существует высокая вероятность того, что биткоин-кошелек может быть украден из-за уязвимости операционной системы компьютера, хакеры придумывают множество новых и более изощренных способов добычи криптовалют. В настоящее время активное развитие получили вирусы-майнеры. По данным лаборатории Касперского около 9000 компьютеров уже заражены этим вирусом. После установления этого вируса на компьютер, он начинает самостоятельно производить многочисленные вычислительные операции на компьютере, в результате которых мошенник переводит на свой кошелек все денежные суммы, находящиеся на счету владельца компьютера. Используются различные механизмы сокрытия вируса [1].

Кроме того, активная торговля криптовалютами поставила мир под угрозу глобального финансового кризиса, так как в мировой экономике возникла высокая вероятность образования пузыря, аналогичного тому, что образовался на американском рынке во время ипотечного кризиса.

Это связано с высокими темпами роста рынка криптоактивов и с увеличением рынка субстандартной ипотеки в 2008 году. Капитализация рынка цифровых денег резко выросла с 16 миллиардов долларов в 2016 году до 2,3 триллионов долларов на сегодняшний день. Схожими темпами происходило и расширение ипотечного рынка в США, буквально в течении одного года он увеличился на 1,2 триллиона долларов.

Регулирующие органы во всем мире начали активно разрабатывать систему регулирования, с целью управления экспоненциальным ростом криптоактивов. Конечно, на данный момент у цифровых денег не получится обрушить мировую финансовую систему, но текущие способы применения криптоактивов несут значительную угрозу финансовой стабильности, поскольку большинство из них не имеют внутренней стоимости и подвержены серьезным ценовым корректировкам. Мир криптовалют начинает подключаться к привычной традиционной финансовой системе, и мы наблюдаем появление игроков с финансовым рычагом, которые используют заемные средства с целью увеличения прибыли, при этом не имея достаточного капитала. И главная опасность заключается в том, что все эти процессы происходят в нерегулируемом пространстве. Именно большая закредитованность, а также высокий уровень взаимосвязанности банковской системы, привели к обвалу финансовой системы США в 2008 году.

Bitcoin и Ethereum - две крупнейшие криптовалюты, которые упали в цене более чем на 30 процентов в начале 2021 года. Конечно, спустя определенное время они восстановились, но все равно остались чрезвычайно нестабильными. У многих экспертов вызывает беспокойство факт того, что, что существует множество факторов, которые оказывают неблагоприятное влияние на изменение цены на криптовалюты.

В результате стоит отметить, что с ростом популярности криптовалюты появляется вероятность нарушения функционирования финансового рынка и возникновения нового мирового финансового кризиса, который по свой масштаб может превзойти мировой финансовый кризис 2008 года. Именно поэтому появляется необходимость усиления контроля над рынком криптовалют, а в особенности над стейблкоинами, криптовалютным кредитованием и биржами. Грамотный и своевременный подход к разработке стандартов и правил позволит управлять рисками на рынке цифровых денег так же, как ими управляют в сфере традиционных финансов.

Список использованных источников:

1. Вирусы-майнеры [Электронный ресурс] // Лаборатория Касперского. – Режим доступа: <https://www.kaspersky.ru/about/contact> (дата обращения 12. 11. 2021 г.)
2. Курс криптовалют [Электронный ресурс] // Официальный сайт Министерства финансов Российской Федерации. – Режим доступа: <https://minfin.gov.ru/ru/> (дата обращения 11.11.2021 г.)
3. Мошеннические операции с криптовалютами [Электронный ресурс] // Официальный сайт Investopedia. – Режим доступа: <https://www.kaspersky.ru/about/contact> (дата обращения 12.11.2021 г.)
4. Рейтинг криптовалют [Электронный ресурс] // CoinMarketCap. – Режим доступа: <https://coinmarketcap.com/> (дата обращения 12. 11. 2021 г.)
5. Цифровой мир криптовалют [Электронный ресурс] // Официальный сайт журнала The Outline. – Режим доступа: <https://theoutline.com/> (дата обращения 12.11.2021 г.)

Криптовалюта: повторение кризиса или современное средство обмена?

Е.М. Бурнашева

студент 3 курса НИЯУ МИФИ, Москва

E-mail: burnasheva2311@mail.ru

Д.Д. Гольцов

студент 3 курса экономического факультета

МГУ им. М. В. Ломоносова, Москва

E-mail: ddg1377@gmail.com

А.А. Хоченко

студент 3 курса НИЯУ МИФИ, Москва

E-mail: nastja.ho4enko@yandex.ru

А.К. Завалишина

ассистент кафедры финансового менеджмента

ИФТЭБ НИЯУ МИФИ, Москва

E-mail: akzavalishina@gmail.com

Аннотация: В данной статье рассматривается криптовалюта как новая современная реальность, децентрализованное цифровое средство обмена, основанная на технологии блокчейн. Главной отличительной чертой от привычных видов фиатных денег, доллара или евро, остается отсутствие центрального органа управления и поддержки стоимости криптовалюты, так как эти задачи распределяются между пользователями системы через Интернет. Отсутствие полноценного урегулирования ставит под вопрос риск кризиса на мировой арене и дестабилизацию экономической системы в целом. Для подробного анализа рассматривается статистика, собранная на территории Российской Федерации, проанализированы данные официальных сетевых ресурсов, материалы периодической печати, научные работы зарубежных и отечественных авторов, а также использованы личные наблюдения. По результатам исследования сформулирован вывод, что криптовалюты, несомненно, стали важной частью финансового сектора, выступая в качестве растущей альтернативы более традиционным формам инвестирования. Однако присутствие волатильности как фактора риска свидетельствует о низкой правовой защищенности и неустойчивой системы контроля за проведенными транзакциями, что создает почву для

финансовых преступлений, нарушений требований ПОД/ФТ как в каждом отдельном государстве, так и по всему миру в целом.

Ключевые слова: *криптовалюта, блокчейн, ПОД/ФТ, мировой кризис.*

Cryptocurrency: a repeat of the crisis or a modern medium of exchange?

Abstract: This article considers cryptocurrency as a new modern reality, a decentralized digital medium of exchange based on blockchain technology. The main distinguishing feature from the usual types of fiat money, dollar, or euro, remains the absence of a central management body and support for the value of cryptocurrencies since these tasks are distributed among users of the system via the Internet. The absence of a full-fledged settlement calls into question the risk of a crisis on the world stage and the destabilization of the economic system. For a detailed analysis, statistics collected on the territory of the Russian Federation are considered, data from official network resources, periodical materials, scientific works by foreign and domestic authors are analyzed, and personal observations are used. It is concluded that cryptocurrencies have undoubtedly become an important part of the financial sector, acting as a growing alternative to more traditional forms of investment. However, the presence of volatility as a risk factor indicates low legal protection and an unstable system of control over transactions, which creates the ground for financial crimes, violations of AML/CFT requirements both in each individual state and around the world.

Keywords: *cryptocurrency, blockchain, AML/CFT, global crisis.*

За последние годы криптовалюта из цифровых новинок, известных малочисленному количеству людей, превратилась в технологию со стоимостью выше триллиона долларов, такой рост способен разрушить стабильную финансовую систему, чей механизм формировался ни один десяток лет, претерпевал изменения и приобрел тот вид, к которому привыкли все. Биткойн, как самый известный вид, и иные криптовалюты все чаще используются в качестве индивидуального инструмента инвестиций, и как следствие становятся средством платежей, начиная от законной покупки товаров или услуг, заканчивая незаконным отмыванием денег, финансированием терроризма и прочих операций, нарушающих международное и российское право.

С одной стороны, необходимо уточнить, что данный вид валюты является некой демократизирующей силой, позволяющей контролировать деятельность центральных банков и работу бирж, например таких, как Уолл-стрит. Однако негативное влияние заключается в распространении возможностей реализации преступной деятельности, а также

дополняющим аргументом некоторых критиков является вред окружающей среде за счет потребления электроэнергии криптомайнерами.

Финансовые регулирующие органы прилагают усилия, чтобы отреагировать на изменчивость рынка, но нормативная база различается по всему миру. Некоторые правительства признают криптовалюту, делают ее официальной и не преследуют по закону. Так поступила первая в мире страна, перешедшая на биткоин, Сальвадор. [2] «Биткоин Сити» планируется построить за счет вулканической энергии, сообщается, что жители города не будут платить налоги на доходы, имущество и прирост капитала, но останется налог на добавленную стоимость со ставкой 10% для дальнейшего развития региона. В это же время другие государства ограничивают или вовсе запрещают действия, производимые майнерами на криптобиржах, например, Китай в мае 2021 года запретил данную деятельность с полным контролем над финансовыми операциями с токенами, не имеющих собственного блокчейна, создаваемых на базе криптовалют.

Изучая экосистему электронного средства платежа, у которого отсутствует физическая форма выражения, отмечается, что последний год стал прорывом в его росте, тема становится *актуальной* в каждом государстве, поскольку создается необходимость постоянной ревизии транзакций из-за масштабности и технологичности изучаемого феномена. Можно сформулировать *гипотезу* о том, что криптовалюта предоставляет не только возможности, но и совокупность проблем, выраженных в вероятности мирового кризиса из-за раздувания рынка, и увеличением количества финансовых преступлений, ставящих под угрозу требования ПОД/ФТ.

Так по сообщениям Forbes, со ссылкой на замглаву Банка Англии, из-за роста криптовалют возможен кризис масштабов 2008 года. «Схожими темпами рос пузырь на ипотечном рынке США», - отмечают эксперты. «Когда что-то в финансовой системе растет очень быстро, причем растет в практически нерегулируемом пространстве, органам финансовой стабильности стоит очнуться и обратить на это внимание», — заявил Канлифф. [4] Его слова действительно правдивы, поскольку новая валюта ничем не подкреплена, а это есть причина резких колебаний, показывая уязвимость и отсутствие реальной ценности. По сути, неожиданные падения на несколько десятков процентов в течение дня, являются нормой, что не скажешь про национальные курсы. Экспоненциальный рост отмечала и глава Центрального Банка Российской Федерации, Эльвира Набиуллина. Финансовая структура настроена отрицательно, поскольку, как правило, ЦБ никогда не дает советов по вложению, инвестированию, но что касается данного случая, идет полное отрицание, настороженность

из-за нестабильности. Если проанализировать деятельность государства, то преждевременно говорить о том, чтоб биткойны или иные монеты, токены стали эквивалентом, например, российскому рублю.

Сколько бы мнений на эту тему ни существовало, рост криптовалют не остановить, по статистике, за последние полгода биткоин вырос на 350%, побив абсолютный рекорд, но это еще не предел, так как его активно поддерживает компания Tesla. Проводя финансовую оценку уже точно понятно, что такая категория, как «биткоин» есть ценовой «пузырь», раздувающийся все больше в критические сроки. Спекуляция – общее, что объединяет 2021 год и рост электронных платежных систем, неподвластных осязанию, и 2008 год, когда наблюдался неконтролируемый процесс выдачи ипотек заемщикам с низким уровнем кредитоспособности. Когда активы очень быстро растут в цене, обычно это делает крах гораздо более вероятным. Или, по крайней мере, способствует коррекции, когда цена снова упадет до более “нормального” уровня. Именно в такой ситуации сейчас находятся криптовалюты. Хотя никто не может точно сказать, что такое “нормальный” уровень в такой ситуации. Куда он направится дальше, столь же непредсказуемо. Однако почему возникают такие проблема непредсказуемости и неконтролируемости процесса реализации на рынке?

Реакция правительства варьировалась от агрессивной до безразличной, причем инвесторы и спекулянты настороженно следили за международными событиями, отметим, что действия мирового сообщества по отношению к нынешним реалиям неизбежны. Попытка снизить преступность в финансовом секторе, минимизировать шанс незаконного оборота средств, заставляет укреплять правительственные решения, чтобы бороться с отмыванием денег и финансированием терроризма.

Препятствием этому служит децентрализованность, которая доказывает, что отсутствие единого управления не приговор, и структура может работать на практике для институционального управления. Изначально она служила как главная цель создания криптовалюты, то есть борьба за независимую платежную систему, которая завязана на идеологии безопасных платежей, возможных только, если несколько пользователей проведут проверку и обработку операции. Следовательно, это делает сильно медленнее процесс проведения транзакций в отличии от обычных платежных систем (Visa, Mastercard) с едином центром скопления информации.

Второй особенностью криптовалют, которая приводит к появлению риска, становится конфиденциальность владельцев, что затрудняет мониторинг потоков денежных средств. Третьи лица могут только косвенными способами, используя открытую информацию в соцсетях,

получить информацию о переводах, но не полная защита позволяет реализовать деятельность в даркнете, или теневой сети. Криптовбиржи — это новшество для киберпреступников, стремящихся отмыть активы. С криптовалютными биржами требуется гораздо меньше мер идентификации. Для осуществления транзакций требуется только адрес кошелька отправителя и получателя для осуществления переводов. Такие переводы не отслеживаются, не помечаются и не проверяются каким-либо сторонним посредником или банковским органом. Также нет никаких бумажных следов с крипто-транзакциями, кроме записи в блокчейне. В дополнении для сохранения анонимности используется так называемая технология миксер. Биткойн-миксер можно определить как сервис анонимизации, который делает невозможным отслеживание транзакций в блокчейне, разделяя их на небольшие части и перемещая несколько раз между разными адресами. Случаи арестов, конечно же были, например в апреле этого года были задержаны граждане РФ и Швеции, разработчики и администраторы технологии. В течение 10 лет их система BitcoinFog смогла отмыть около 335 миллионов долларов. «Основная часть этой криптовалюты поступила с рынков даркнета и была связана с незаконными наркотиками, компьютерным мошенничеством», - заявили правоохранительные органы. [6] Обвинение строится на нескольких частях: отмыwanie денег, ведение нелегального бизнеса по переводу денег и их передачи. Несмотря на конкретные кейсы, подобные сервисы доступны на открытых сайтах и остаются шансом для преступников скрыть свои реальное происхождение денег.

Конечно, у правительства остается возможность отследить правонарушителей, когда и где проводились сделки, так как вся история сохранена, то есть «идти по следам» гораздо легче, но остаются способы обхода, так технологии и код криптовалюты Монето, считающаяся самой анонимной в мире.

Обратим внимание, что вопрос выявления становится прост, так как задача сводится только к идентификации владельцев кошельков, помощь в этом составляет нормативная база по данному вопросу. Однако на территории РФ майнинг может попадать под Уголовный кодекс, в случае незаконных банковской деятельности (ст. 172) или мошенничества (ст.159), в дополнении Минфин предложил внести поправки, так чтобы в случае неуплаты налогов хотя бы два раза за три года, владельцев валют преследовало уголовное наказание. [9] По своей сущности Федеральные законы РФ сочетают лучшие стороны из международных практик, запрет на использования как средства платежа, как ранее в КНР, но при это остается возможным их оборот. Трудность всего состоит в отсутствии четкой позиции и формулировке, что тормозит развитие законодательства,

персонифицированность систем на биржах, что позволило бы взимать налоги с пользователей, остановить отмывание денежных средств и в целом нарушение правил ПОД/ФТ, разработанных крупнейшими международными и региональными субъектами, в том числе ФАТФ.

Таким образом, проведя анализ текущей ситуации с использованием зарубежного и отечественного опыта, можно сказать, что гипотеза подтверждается, поскольку криптовалюта остается масштабным явлением в экономической системе мира, сохраняющая свои первоначальные принципы, как независимость, свобода, безопасность и анонимность, в сущности, транзакций и деятельности криптобирж, включая их участников, майнеров. Это становится основой для преступлений, за счет недостаточно своевременного регулирования рынка, так как новые нормы права только находятся на стадии принятия и обсуждения, что является ключевой ошибкой в действии правительства. Необходимо усовершенствовать технологичную оснащенность при борьбе с ОД/ФТ, повысить правовую грамотность сотрудников правоохранительных органов по данному вопросу, а со стороны государства на территории нашей страны осуществлять поддержку системы «прозрачный блокчейн», разработанной в феврале 2021 года. Только применяя данные меры в совокупности, возможно добиться честного осуществления финансовых операций, без попыток провести нелегальные сделки.

Список использованных источников:

1. Basel institute on Governance [Статья] = Cryptocurrencies and money laundering investigations / авт. Senior Financial Investigation Specialist Paesano Federico. - Базель: Basel institute on Governance, 2021 г.. - Т. 1.
2. BBC News journal [Статья] = El Salvador Bitcoin city planned at base of Conchagua volcano / авт. Journal BBC News. - Latin American country: BBC News journal, 2021 г..
3. Federal Reserve Bank of Cleveland [Статья] = Bitcoin's Decentralized Decision Structure / авт. Cleveland Federal Reserve Bank of. - Cleveland: Federal Reserve Bank of Cleveland, 2019 г.
4. Forbes. A Former Bank Of England Governor Warned The 2008 Crash That Inspired Bitcoin Could Happen Again / auth. Bambrough Billy / ed. Bambrough Billy. - [б.м.]: Forbes; Bambrough, Billy, Октябрь 27, 2019.
5. How-To Geek. How Anonymous Is Bitcoin? / авт. O'SULLIVAN FERGUS. - [б.м.]: FERGUS O'SULLIVAN, @fergusosullivan (twitter), 2021 г.
6. The verge. Feds arrest founder of bitcoin 'mixer' they say laundered \$335 million over ten years / авт. Lyons Kim. - [б.м.]: Kim Lyons, @SocialKimLy, 2021 г.

7. Иновации и инвестиции. Государственная система мониторинга операций в криптовалюте / авт. Кандидат экономических наук доцент, доцент кафедры экономической безопасности СПбГАУ Дурандина Анна Павловна. - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, 2021 г. - Т. 2.
8. Научно-образовательный журнал для студентов и преподавателей "StudNet". Безопасность финансовой системы в рамках появления криптовалюты / авт. Попов В.Г Галиаскаров Д.Ф, Киселев И.Д. - Москва: Научно-образовательный журнал для студентов и преподавателей "StudNet", 2021 г. - Т. 4.
9. РБК.Крипто. Минфин предложил ужесточить регулирование криптовалют в России / авт. Теткин Михаил. - Москва: Михаил Теткин, 2020 г.

Международный опыт построения системы ПОД/ФТ в современных условиях

В.И. Прасолов
к.полит.н., доцент Департамента экономической безопасности
и управления рисками ФГБОУ ВО «Финансовый университет
при Правительстве Российской Федерации», г. Москва
E-mail: VIPrasolov@fa.ru

Аннотация. В статье рассматриваются основные характеристики современных международных систем ПОД/ФТ, отображены и проанализированы лучшие практики стран большой семерки по осуществлению антиотмывочной деятельности. Проведен глубинный анализ трансформации механизма ПОД/ФТ зарубежных государств в современных условиях. Акцент в работе делается на приложении опыта передовых стран в отечественной действительности. Целью статьи выступает разработка ряда мероприятий, которые призваны повысить результативность механизма ПОД/ФТ.

Ключевые слова: Легализация, международный опыт, отмывание, преступные схемы, финансовые расследования, ПОД/ФТ.

International experience in building an AML / CFT system in modern conditions

Abstract. The paper discusses the main characteristics of modern international AML / CFT systems, reflects and analyzes the best practices of the G7 countries on anti-laundering activities. An in-depth analysis of the transformation of the AML / CFT mechanism of foreign countries in modern conditions is carried out. The emphasis in the work is on the application of the experience of advanced countries in domestic reality. The aim of the article is the development of a number of measures that are designed to increase the effectiveness of the AML / CFT mechanism.

Keywords: Legalization, international experience, money laundering, criminal schemes, financial investigations, AML / CFT.

Для ПОД/ФТ/ПРОМУ большинство стран создают специализированную национальную систему, в рамках которой функционирует служба финансового мониторинга. При этом решающее

воздействие на организационно-правовую структуру оказывают международные стандарты в области ПОД/ФТ/ФРОМУ, которые разрабатываются ООН, ФАТФ, ЕС, Вольфсбергской группой, Базельским комитетом. Они становятся источником для правовой базы при создании национальной системы, что приводит к наличию общих характерных черт системы финансового мониторинга в отдельных государствах. Установленные международные и национальные требования в сфере обеспечения ПОД/ФТ формируют правила и рекомендации для компаний.

Согласно классификации, предложенной В.Н. Мельниковым и А.Г. Мовсисяном страны в рамках противодействия легализации преступных доходов и финансирования терроризма подразделяются на следующие группы:

- 1) развитые страны, в которых удельный вес теневой экономики небольшой: например, США;
- 2) развитые страны, удельный вес теневой экономики в которых высок: Италия;
- 3) развивающиеся страны с небольшой долей коррупции и теневой экономики;
- 4) сильно коррумпированные развивающиеся страны, в которых теневая экономика превышает 25 — 30% ВВП;
- 5) страны с переходной экономикой;
- 6) оффшорные юрисдикции, для которых сомнительные операции по «оптимизации налогообложения» и т.п. являются важной составляющей бюджетных поступлений.

Так, в развивающихся странах финансовый мониторинг характеризуется низким правовым регулированием отношений в области ПОД/ФТ, отсутствием важных финансовых институтов, малоэффективными государственными методами принуждения (административными и уголовными наказаниями). При этом основной целью в сфере ПОД/ФТ является организация эффективной правовой основы в системе финансового мониторинга. В то же время для группы экономически развитых стран главной задачей является доработка законодательства в функционирующей системе для противостояния возникающим вызовам международной преступности. Вместе с тем следует отметить, что для всех видов экономических систем причины легализации преступных доходов и финансирования терроризма, как правило, одинаковы: к ним следует относить коррупцию в государственных органах; недостаток контроля над использованием компаниями оффшорных юрисдикций и проведение платежей, которые обеспечивают анонимность или затрудняют идентификацию участника операции; применение системы международных переводов финансовых

средств; несовершенство механизмов финансово-хозяйственной деятельности, позволяющее создать возможность незаконного вывода средств; присутствие в обороте фирмы значительной суммы наличных денежных средств.

Анализ международного и российского опыта свидетельствует о необходимости совершенствования нормативно-правового регулирования ПОД/ФТ в отечественных организациях, поскольку развитие России в этом направлении значительно отстает от ведущих стран. В современных условиях компаниям зачастую не выгодно внедрять процедуры комплаенса и внутреннего контроля в части ПОД/ФТ, а для некоторых сегментов рынка и вовсе отсутствуют рекомендации и стандарты регулирования.

Согласно рекомендациям Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) странам необходимо проводить национальные оценки рисков ОД/ФТ/ФРОМУ (НОР) и полученный материал доводить до сведения государственных органов и частного сектора.

Национальная оценка рисков является системообразующим элементом, на который в конечном итоге опираются все субъекты ПОД/ФТ/ФРОМУ для формирования секторальных оценок, а также программ по борьбе с недобросовестными участниками рынка. При проведении НОР в масштабах государства проводят сопоставление выявленных угроз и современное состояние секторов экономики, их устойчивость к данным угрозам. Таким образом государство способно выявить области реализации угроз, а также определить факторы, способствующие минимизировать вероятность их проявления. Регулярность проведения подобных оценок позволяет в динамике отследить эффект от внедренных реформ, а также оценить эффективность тех или иных мероприятий и технологий.

В целом для мирового сообщества существует ряд традиционных, хорошо известных рисков, которые выделяются большинством государств, реализующих требования ФАТФ. К таким относятся уровень коррупции в стране, масштаб нерегулируемого оборота наличности и использования криптовалют, уровень мошенничества, контрабанды, незаконного оборота наркотиков и другие. Однако каждая страна оценивает критичность того или иного риска по-разному, учитывая особенности национальной системы ПОД/ФТ/ФРОМУ.

Для анализа были взяты последние национальные оценки рисков стран «большой семерки», как ведущих мировых лидеров.

Последняя национальная оценка рисков США проводилась в 2018 году (следует за НОР 2015 года). Америка представляет свои отчеты отдельно по оценке рисков легализации и финансирования терроризма, выделяя тем самым специфические риски, выделяющие различия между двумя

незаконными деяниями. В своем исследовании мы подробнее остановимся на НОР ОД.

НОР ОД США основана, в первую очередь, на интервью с органами власти и исследованиями частного сектора, а также обзоре правительственных действий и отчетов, представленных после оценки 2015 года. В своей оценке штаты отмечают, что большинство предикативных преступлений совершено на территории страны, то есть капитал, зачастую, не выводится за пределы Америки, а легализуется в пределах границ. Тем не менее штаты являются привлекательным местом для незаконных доходов, полученных за пределами страны. США отдельно отмечают характерные предикативные преступления, а именно мошенничество (в наибольшей степени, в том числе банковское, потребительское, в сфере здравоохранения, с ценными бумагами, с возвратом налогов), незаконный оборот наркотиков, торговлю людьми, незаконную миграцию, организованную преступность и коррупцию.

Самой распространенной сферой проведения мошеннических схем является здравоохранение, которая ежегодно приносит порядка 100 млрд долл. незаконных доходов. Медицинские работники часто представляют фальсифицированные счета страховщикам, при этом страховые платежи и последующие транзакции могут проходить через банковскую систему и выглядеть законными.

Правоохранительные органы США отмечают рост киберпреступности, что выходит за рамки национальной оценки рисков и представляет собой глобальную угрозу. К данной форме преступлений относят фишинг, атаки вредоносных программ, мошенничество с кредитными картами, компрометация деловой электронной переписки. Данные преступления выходят за пределы страны, так как могут быть совершены из любой точки мира. Обостряется ситуация тем, что наряду с повсеместным присутствием оборота наркотиков, возросло число глобальных синдикатов по отмыванию денег, соучастники которых являются специалисты по финансовым услугам и специалисты по отмыванию, нанимаемые преступниками. Такие профессионалы в отмывании и их объединения работают независимо, получая заказы от различных преступников, что вызывает новую угрозу ввиду их возможности быстрой адаптации под реформы.

Традиционно для штатов Мексика представляет собой доминирующем каналом оборота наркотиков. Специалисты по отмыванию зачастую овладевают доходами от продажи наркотиков и инициируют процесс легализации, задействуя в своих схемах комбинацию из банковских депозитов, выводных счетов и массовой контрабанды. Типичная схема, иллюстрирующая, как эти методы отмывания денег работают вместе,

включает консолидацию поступлений на один счет посредством небольших денежных вкладов в отделениях банков по всей стране, а затем либо перевод собранных средств в Мексику, либо вывод их в валюте вблизи юго-запада, для переправки контрабандой в Мексику. Другим распространенным методом является отмывание денег на основе торговли, которое включает использование цепочки брокеров и экспортеров товаров для маскировки и перемещения денег от наркотиков. Продажа товаров является эффективным способом легализации денег и предоставляет поставщикам наркотиков оплату в местной валюте. Торговцы, которые получают оплату чеком или банковским переводом за свои товары, могут не знать, что они участвуют в схеме отмывания денег, но некоторые охотно принимают наличные деньги от продажи наркотиков, зная их происхождение.

Особой зоной риска штаты выделяют увеличение оборота наркотиков-аналогов фентанила со стороны Китая, платежи за товар проходят через банковские и небанковские переводы, а также через использование криптовалют.[1] В октябре 2017 года Министерство юстиции объявило о первых обвинениях китайских граждан в незаконной торговле фентанилом и аналогами в Соединенных Штатах.[2] После серии смертельных передозировок и проведенном расследовании 32 участникам преступной группировки предъявлено обвинение. По сообщению генерального прокурора, данный сговор был одним из самых продуманных и тонких. Преступники использовали около 30 различных псевдонимов в сети интернет, криптовалюту, офшорные счета и шифровку сообщениями, а также отмывали доходы путем привлечения третьих лиц на международном уровне.[3] В апреле 2018 года американские активы преступников были заблокированы в соответствии с Kingpin Act, так как Управление по контролю за иностранными активами (OFAC) признало обвиняемых иностранными торговцами наркотиками.

Самым значительными рисками легализации в США являются незаконное использование наличности, вовлечение граждан (complicit individuals) и сотрудников финансовых организаций, а также слабый уровень реализации комплаенс-функции в финансовых институтах. Однако это остаточные риски, вызванные объемом системы регулирования и надзора в сфере ПОД/ФТ/ФРОМУ в США. Необходимо принятие мер по совершенствованию системы, однако факт наличия таких рисков не является неожиданным.

Анонимности при совершении транзакций и фондовых трансферов по-прежнему остается основным риском, способствующим легализации. Преступники, вовлеченные в незаконный оборот наркотиков, контрабанду, торговлю людьми, незаконные розничные операции и различные виды

деятельности, связанные с организованной преступностью, по-прежнему предпочитают наличные деньги в долларах США из-за их широкого использования как на территории Америки, так и за рубежом из-за их широкого признания как стабильного средства обмена.

Виртуальные валюты, когда их администраторы и сайты по обмену не регулируются законодательно, также обеспечивают анонимность и генерируют риски, связанные со скоростью их передачи, отсутствием посредников, глобального охвата и недостаточности регулирования и контроля во многих юрисдикциях.

Тем не менее риски незаконного использования наличных денег и виртуальной валюты в Соединенных Штатах снижается благодаря введению программы по борьбе с легализацией, отчетности о подозрительных и валютных операциях и требований к документированию идентификации клиентов в финансовых учреждениях. Кроме того, в определенных случаях юридические и физические лица несут ответственность по предоставлению кассовой отчетности, чтобы снизить риски использования наличных денег. Но эти обязательства эффективны только в той мере, в которой они выполняются. Преступники ищут подставных лиц (*complicit individuals*), профессиональных финансовых работников. Министерство юстиции сосредоточило свое внимание на замешанных профессионалах, что привело к судебному преследованию специалистов по торговой легализации (TBML), а также к адвокатам (поверенным) и риелторам.

Также угрозу представляют лица, злоупотребляющие своим профессиональным положением в финансовых учреждениях. Они способствуют открытию счетов, переводу средств и проверке наличных денег, сознательно не проводя идентификацию клиента, точных записей транзакций или не предоставляя требуемых отчетов. Финансовые учреждения, где комплаенс-функция развита слабо, также представляют риск отмывания денег.

США отмечает в категорию значительного риска создание фирм-однодневок (неправомерное использование юридических лиц), процесс установления бенефициарного владельца таких организаций для правоохранительных органов является ресурсоемким, особенно когда следы собственности ведут за границу или являются многослойными.

Отсутствие у определенных финансовых учреждений обязанности идентифицировать физическое лицо (лица), которое является бенефициаром или выгодополучателем корпоративного клиента, позволило физическим лицам получать анонимный доступ к финансовым услугам, действуя через подставные компании. Тем не менее в США внедрена программа Надлежащей проверки клиентов (CDD), в виду этого

при полной её реализации данный риск должен быть снижен, хотя еще слишком рано прогнозировать полное его влияние на систему по борьбе с финансовыми преступлениями.

США использует терминологию и методологию оценки рисков ОД/ФТ в соответствии с рекомендациями ФАТФ. В качестве основных определений в НОР используется следующие понятия:

Угроза – это предикативные преступления легализации доходов. Условия, в которых совершаются основные правонарушения и генерируются доходы от преступлений, имеют отношение к пониманию того, почему в некоторых случаях конкретные преступления связаны с конкретными методами отмывания денег.

Уязвимости – это конкретные элементы системы, создающие возможность для реализации легализации. Они могут относиться к конкретным финансовым сегментам, продуктам, несовершенству законодательства, слабостью в регулировании, надзоре или правоприменении. Также сюда включены уникальные обстоятельства, при которых квалификация преступления может быть затруднена ввиду смешения законной и незаконной деятельности. Методы, позволяющие отмывать большие суммы денег наиболее эффективно или наиболее быстро, представляют наибольшую потенциальную уязвимость.

Риск – функция угрозы и уязвимости, представляет собой суммарное суждение, учитывающее влияние проведенных мер противодействия, включая регулирование, надзор и правоприменение.

В первом разделе НОР США представлен обзор угроз отмывания денег и связанных с ними методов отмывания денег. К ним относят (в порядке степени риска – от большего к меньшему):

1. Мошенничество (отдельно выделяют мошенничество в здравоохранении, мошенничество в сфере возврата налогов, киберпреступления)
- 2.оборот наркотиков (марихуаны, кокаина, героина и синтетических опиоидов, метамфетамина, синтетических психоактивных наркотиков)
3. Незаконная миграция (контрабанда людей)
4. Торговля людьми
5. Коррупция
6. Транснациональные преступные группировки (африканские, азиатские, мексиканские и колумбийские, евроазиатские).

Во втором разделе отчета более подробно рассматриваются уязвимости, связанные с отмыванием денег, и остаточные риски, которые иллюстрируются рядом примеров из практики. К основным уязвимостям США относят:

1. Наличные денежные средства (массовая контрабанда наличности)

2. Схемы структурирования
3. Денежную «воронку» (использование единого банковского счета или нескольких банковских счетов в нескольких банках для сбора депозитов в различных местах и от отдельных лиц)
4. Криптовалюты
5. Злоупотребление юридическими лицами (подставные фирмы, которые не ведут реальной коммерческой деятельности, а создаются с целью вовлечения в схемы легализации)
6. Подставные лица, специалисты по отмыванию (особенно адвокаты и ритейлеры) и сотрудники финансовых организаций
7. Недостаточность комплаенс-функции
8. Преступные нарушения.

Новые требования по идентификации бенефициарного владельца юридических лиц при открытии счета, принятые в США, должны снизить риск отмывания денег.

Пока преступление совершается ради экономической выгоды, а уязвимости предоставляют возможности, отмывание денег будет адаптироваться, развиваться и сохраняться. Незаконное использование виртуальных валют, масштаб операций международных сетей по отмыванию денег и вовлечение индивидуумов-пешек для облегчения процесса легализации демонстрируют, как ОД адаптируется и развивается. Правоохранительные органы США и регулирующие органы работают вместе, чтобы быть в курсе методов легализации и поддерживать тесные отношения с зарубежными коллегами для обмена информацией и расширения возможностей для сотрудничества.

Ключевыми недостатками НОР США являются:

- отсутствие описания конкретных уязвимостей системы, которые выделяет государство из чего вытекает недостаточность приведенных рисков, так как отсутствует некий реестр рисков, позволяющий определить какая именно угроза и уязвимость порождает тот или иной риск;

- критерии, по которым риски были отнесены к той или иной степени значимости отсутствуют, исходя из документа сложно понять, за счет чего были сделаны выводы о присвоении тому или иному риску (а также угрозе) высокой или низкой степени. Так же из-за отсутствия подобного реестра события, отнесенные к понятиям «уязвимость» и «риск», которые объединены в один раздел документа, перемешаны между собой, что не дает четкого понимания отношения к ним государства, а также пониманию точки приложения воздействия предпринимаемых государством мер по борьбе с ОД;

- отсутствие списка характерных мер, предпринятых и/или предпринимаемых государством в отношении митигации рисков, приводит

к тому, что по документу невозможно здраво оценить реальную степень значимости для страны тех или иных рисков. Также данный список мог бы побудить частный сектор качественнее выполнять предписанные нормы ПОД/ФТ/ФРОМУ на уровне государства, что могло бы повысить значимость и эффективность реализации комплаенс-функции в бизнесе.

К положительным сторонам НОР США можно отнести достаточное описание предикативных преступлений, которые по своей сути являются факторами реализации ОД (хотя в рамках НОР штаты относят эту группу к угрозам, порождающим риски). Ранжирование подобных правонарушений по степени значимости позволяет определить первоочередные цели национальной системы ПОД/ФТ/ФРОМУ.

Меры по борьбе с отмыванием денег в Японии [56] разрабатываются шаг за шагом в соответствии с инициативами международного сообщества. Впервые деятельность по отмыванию доходов была криминализована в 1992 году в законе, определяющим правила обращения наркотиков в стране. В данном законе прописана система отчетности о подозрительных операциях (в отношении доходов от продажи наркотиков) финансовыми учреждениями. В виду того, что финансовым организациям было сложно определить источник происхождения доходов (его аффилированность с оборотом наркотиков) данная система отчетности работала не эффективно. Для устранения недочетов в Японии был принят Закон о наказании за организацию преступлений и контроль за преступными доходами, опирающийся на 40 рекомендаций ФАТФ. Данный закон имел положительный эффект. Был расширен охват основных правонарушений, связанных с отмыванием денег, а также охват преступлений, на которые распространяется режим сообщений о подозрительных операциях (преступления, помимо незаконного оборота наркотиков). Кроме того, закон определил Агентство финансового надзора (позднее Агентство финансовых услуг) в качестве органа финансовой разведки Японии, где агрегируется, размещается и анализируется для распространения в следственных органах информация о легализации.

Японский центр финансовой разведки (JAFIC) ежегодно (начиная с 2007 года) публикует Годовой отчет [82]. В последнем годовом отчете ставится целью развитие понимания и поддержки мер ПОД / ФТ среди не только тех, кто непосредственно вовлечен в эту область, но и широкой общественности, а также способствование предотвращения движения преступных доходов, что приведет к повышению уровня общественной безопасности и устойчивому экономическому развитию.

Национальная оценка рисков ОД/ФТ в Японии проводится ежегодно, начиная с 2014 года. Последняя НОР [85] была опубликована в декабре 2018 года. По своей структуре она сильно отличается от той, что проводит

США. JAFIC представляет полноценный реестр рисков, в котором описывает риски, присущие каждому финансовому продукту или услуге, разделяя их на основные и остальные, а также меры по их митигации.

Основными продуктами и услугами, в которых усматривается риски ОД/ФТ/ФРОМУ являются:

1. Продукты и услуги, связанные с депозитным размещением средств (очень высокая степень риска)

В период с 2015 по 2017 год финансовыми организациями было зарегистрировано 1 100 248 сообщений о подозрительных операциях (СПО), что составляет 91,6% от общего числа отчетов.

К данному разделу в Японии относят:

- депозитные или сберегательные счета (особенностью является тот факт, что данные счета застрахованы и для их открытия не обязательно физическое присутствие клиента в банке, операцию можно совершить посредством сети Интернет);

- операции с депозитами (люди могут снимать\класть наличные денежные средства в рамках своих депозитных счетов независимо от места и времени, а с развитием технологий и упрощением системы перевода средств между счетами, вывод наличности представляет собой существенную угрозу);

- внутренние валютные операции (позволяют клиентам совершать безопасные и быстрые расчеты без физического перемещения денежных средств между удаленными районами. Из-за такого удобства многие люди используют данный продукт как привычный расчетный сервис, особенно с распространением банкоматов и интернет-банкинга. Тем не менее использование счетов, зарегистрированных на имя третьей стороны, могут обеспечить анонимность для проведения операции легализации доходов. Текущее законодательство в сфере ПОД/ФТ/ФРОМУ Японии при совершении клиентом переводов между разными финансовыми организациями фирма-адресат обязана запросить информацию о последних операциях клиента у фирмы-адресанта);

- банковская (депозитная) ячейка (зачастую в таких ячейках хранятся ценные документы, драгоценные металлы и камни, однако, поскольку принимающие депозитарии не проверяют содержимое хранилищ, данная категория является также высокорисковой, так как может являться эффективной мерой по физическому хранению криминальных доходов);

- векселя и чеки (широко распространено в Японии, так как векселя и чеки физически легче наличных денег эквивалентной стоимости и их легко транспортировать и обналичивать через депозитные учреждения)

2. Страхование (высокая степень риска).

В виду того, что страховые компании представляют продукты, связанные с накоплением денежных средств, что может обеспечить одновременное получение значительной суммы средств без каких-либо потерь. В период с 2015 по 2017 год субъектами страхового дела было зарегистрировано 7610 СПО (6840 по страхованию жизни, 746 по общему страхованию и 24 по программе взаимного страхования). При этом более 80% сообщений регистрировались из-за потенциальной связи с крупной японской преступной группировкой «Борекудан».

Поскольку страховые продукты с функциями накопления денежных средств позволяют конвертировать преступные доходы в текущий или отсроченный актив, они могут быть высоко применимы для ОД / ФТ.

3. Инвестирование в финансовые инструменты (высокая степень риска)

Инвестиции в акции, облигации и другие инвестиционные продукты также является распространенным способом управления доходами. Таким образом, инвестирование может быть использовано для преобразования большого количества средств в различные продукты, более того некоторые инвестиционные инструменты состоят из сложных схем и могут использоваться, с целью сокрытия истинного источника средств, а также затруднения отслеживания цепочки отмывания денег.

Также в НОР подробно рассмотрены другие продукты и услуги, а именно трастовые фонды, кредитование, денежные переводы, криптовалюты, обмен валют, финансовый лизинг, кредитные карты, недвижимость, драгоценные металлы и камни, почтовые получения, предоставление и получение услуг связи, налоговое и бухгалтерское консультирование. Отдельной группой выделены продукты и услуги, использующие новые технологии, требующие дальнейшего изучения целей фактического использования.

К зоне повышенного риска в Японии относят анонимные транзакции, движение наличности, международные транзакции. Для каждого вида риска определены факторы, повышающие степень риска, принятые меры по митигации рисков, а также непосредственно оценка риска.

НОР Японии выделяет отдельные страны и регионы, которые в большей степени оказывают влияние на риски ОД/ФТ/ПРОМУ. Для данного раздела также определены факторы, повышающие степень риска, меры по митигации рисков и произведена непосредственная оценка риска.

Также в НОР Японии выявлены основные типы клиентов, оказывающие влияние на проведение сделок по отмыванию доходов. В первую очередь к ним относят внутренние антисоциальные силы, другими словами, преступные группировки по типу «Борекудан». В период с 2015 по 2017 год насчитывалось 1 200 642 СПО, связанных с преступными группировками (194 805 сообщений - 16,2% от общего числа, связанных с

борекуданскими участниками). Другим типом являются международные террористические группировки, в основном исламские экстремисты.

Необходимо отметить исключительный формат изложения результатов оценки. Документ ключевой своей целью ставит призыв частного и государственного сектора к объединению и борьбе с проблемами легализации. Исходя из данной цели, публикуется подробное описание и характеристика каждого типа операции, а также приводятся конкретные примеры по использованию тех или иных финансовых инструментов в процессе легализации. Меры митигации рисков прописаны как общие, так и по отдельности для органов государственной власти и представителей бизнес-сообщества.

Истории борьбы Великобритании с отмыванием преступных доходов уже более 10 лет, однако впервые национальная оценка рисков в сфере ПОД/ФТ/ФРОМУ была произведена лишь в 2015 году, спустя два года Соединенное королевство опубликовало вторую национальную оценку рисков.

В отличие от первого издания, в НОР 2017 года [4] к зоне повышенного риска относят отмывание с использованием финансового сектора и связанные с этим профессиональные услуги (high-end money laundering), а также отмывание с использованием наличных денежных средств. При этом постоянно появляющиеся новые технологии и их вовлечение Великобританией оценивается менее рисковыми, нежели традиционные, давно обозначенные большинством стран мира.

После появления НОР 2015 года Великобритания опубликовала план реагирования на выявленные риски ОД/ФТ. В этом плане действий намечены широкомасштабные реформы по:

- реагированию правоохранительных органов на незаконное финансирование,
- надзорному режиму в сфере ПОД / ФТ,
- взаимодействию на международном уровне для устранения рисков ОД/ФТ,
- укреплению государственно-частного партнерства.

В результате реализации плана действий были пересмотрены отдельные положения Закона об уголовных финансах 2017 года (CFA) и Положений по борьбе с отмыванием денег 2017 года (MLR). Другие изменения коснулись также общего способа функционирования британской системы ПОД/ФТ, в том числе расширение Объединенной целевой группы по расследованию случаев отмывания денег (JMLIT), которая способствует обмену информацией между финансовым сектором и правоохранительными органами. JMLIT добилась конкретных результатов

в пресечении отмыывания денег и финансирования терроризма и послужила примером для других стран.

НОР 2017 года основывалась на работе, проведенной в 2015 году, чтобы определить динамику рисков и более детально изучить те области, которые были отнесены к категории высокого риска. Основные выводы оценки 2017 года включают в себя:

- Отмыывание денег с использованием финансового сектора и связанные с этим профессиональные услуги и отмыывание денег на основе наличных денежных средств остаются самыми серьезными областями риска легализации в Великобритании. По-прежнему появляются новые типологии, в том числе риски отмыывания денег на рынках капитала, хотя они менее распространены, чем давние и общеизвестные риски.

- Все сложнее становится определить законность происхождения доходов из-за тенденции к смешиванию легальных и «грязных» денег еще на низком уровне. Правоохранительные органы видят, что преступники переходят от отмыывания мелких сумм, к накоплению более крупных для отправки за границу при помощи более сложных методов, включая розничные банковские услуги и услуги по переводу денег.

- Использование услуг профессионалов в сфере финансовых инструментов становится одним из ключевых методов преступников, стремящихся скрыть происхождение своих средств.

- Наличные денежные средства, а также сектора экономики с повышенным накоплением наличности, остаются предпочтительным способом для перемещения средств через Великобританию. Угроза финансирования терроризма в Великобритании в основном связана с низким уровнем капитализации со стороны британских граждан для отправки за границу, финансирования поездок или планирования терактов. Основными средствами для этого являются наличные деньги, розничные банковские операции или услуги по обслуживанию денежных средств.

- Широкое правительственное реформирование завершено не в полной мере. Эти в большей степени направлены на борьбу со злоупотреблением профессиональными услугами, совершенствование законодательства для улучшения реагирования правоохранительных органов и реализацию мер по повышению прозрачности корпоративной деятельности. Кроме того, изменения, коснувшиеся сферы ГЧП уже показали значительные результаты.

В 2017 году Великобритания выпустила новый документ по регулированию ОД (Money Laundering Regulations 2017), где были прописаны требования к субъектам системы ПОД/ФТ (компаниями, ведущими свою деятельность в сферах с повышенным риском

использования их продуктов и/или услуг в целях легализации), ключевыми из которых являются следующие:

оценка рисков

проведение надлежащей проверки клиентов (KYC)

наличие политики и процедуры по управлению рисками, а также системы мониторинга и контроля за их выполнением

- проведение регулярного обучения персонала
- наличие системы документирования и отчетности

В дополнение к MLRs соответствующими казначейскими органами выпускается руководство, написанное для большинства сфер, попадающих под регулирование. Это руководство помогает фирмам в практической реализации правовых и нормативных требований к их бизнесу или отрасли. Руководство также рассматривается Консультативным комитетом по борьбе с отмыванием денег (MLAC) - форумом, на котором высокопоставленные представители бизнеса, правоохранительных органов, надзорных органов и правительства консультируют по вопросам применения эффективного и пропорционального режима ПОД / ФТ.

В НОР термин «угроза» понимается как деятельность, которая ведет к преступному умыслу отмывания доходов. Это связано как с внутренними угрозами (предикатными преступлениями, порождающими доходы в Великобритании), так и с трансграничными угрозами (подверженность Великобритании преступникам, действующим за рубежом, которые пытаются отмывать деньги в Великобританию или через нее, а также рискам легализации доходов, образовавшихся в Великобритании, за границей).

К первой группе угроз относят:

- Незаконный оборот наркотиков (в период 2015-2017 гг составляет порядка 54% от общего числа преступлений и 16% по стоимости)

- Мошенничество и уклонение от уплаты налогов (определить точный масштаб мошенничества в Великобритании проблематично, хотя экспериментальные статистические данные, опубликованные в рамках CSEW 2016/17, указывают на то, что было зафиксировано 3,4 миллиона случаев мошенничества, причем большинство из них касалось банковских и кредитных счетов[5]; размер уклонения от уплаты налогов в 2017-18 годах оценивается в 35 млрд фунтов стерлингов, что составляет 5,6% от общего размера предполагаемого сбора налоговых обязательств в стране[6])

- Киберпреступность (в Великобритании был создан отдельный национальный центр по обеспечению информационной безопасности, который занимается противодействием преступлений, совершенных с

использованием информационно-коммуникационных технологий, а также посредством сети Интернет)

- Уголовная преступность (включает в себя кражу, грабеж, кражи со взломом и могут быть совершены отдельными лицами или организованными преступными группировками)

- Миграционные преступления (в 2015 году было совершено более миллиона незаконного пересечения границ Европейского союза, в 2016 году данный показатель составил более 510 000 случаев, что приводит к росту преступлений, совершенных мигрантами по всей Европе)

- Современное рабство (в данную категорию включают торговлю людьми, рабство, подневольное состояние и принудительный или обязательный труд, точное число таких преступлений выявить сложно, тем не менее в последние годы замечен рост обращений, однако это может быть связано с совершенствованием системы выявления таких преступлений правоохранительными органами)

К международным угрозам относят:

- угрозы от организованной преступности и коррупции за рубежом
- международные денежные переводы и другие финансовые потоки
- международные финансовые центры (ряд международных финансовых центров сталкивается с аналогичным набором угроз отмывания денег, как и Лондон и подвергаются особому риску использования в качестве пунктов назначения или транзитных пунктов для преступных доходов)

Проводя оценку рисков, Великобритания выделяет три категории (высокий, средний и низкий уровень риска), разделяя уровни отдельно для ОД и ФТ, что является интересной практикой, поскольку часто риски имеют разный уровень значимости для данных двух категорий.

Первый большой блок оценки посвящен финансовым услугам. Тут на первый план выходит деятельность коммерческих банков, а именно обслуживание счетов физических и юридических лиц, сберегательные счета и платежные сервисы. Данный риск оценивается как высокий и для ОД, и для ФТ. Далее идет оценка транзакций между крупными институтами (всемирный банкинг), который для целей ОД попадает в категорию повышенного риска, а для целей ФТ – низкого. Группа персонального банкинга, включающая в себя оказание финансовых и инвестиционных консультаций и услуг для состоятельных людей, является высоким риском для ОД, но низким для ФТ. Услуги страхования попали в категорию низкого уровня рисков как для ОД, так и для ФТ, так данный рынок хорошо регулируется как со стороны надзорных органов, так и внутри себя сам по себе (благодаря высокому развитию комплаенс-функции у бизнес-единиц).

Вторым блоком оценки являются финансовые технологии. Электронные деньги выделяются отдельной категорией, но представляют средний уровень риска как для ОД, так и для ФТ, так как ограничены в применении и размере сумм, возможных для использования. Хотя отмечается, что в предыдущей оценке рисков для целей ФТ электронные деньги имели низкий уровень риска. Повышение категории связано с ростом использования виртуальных карт с электронными деньгами для перевода средств через границу. Криптовалюты при этом попали в категорию низкого уровня риска, как в НОР 2015, так и в НОР 2017. Отдельно в данном блоке выделяются краудфандиговые платформы, хотя конкретный уровень риска не присваивается.

Третьим блоком являются бухгалтерские услуги (в том числе фальсификация бухгалтерской отчётности, взаимодействие с подставными лицами, налоговое мошенничество), которые оценены высоким уровнем риска для ОД и низким для ФТ.

Четвертым блоком выделяют юридические услуги, которые также как бухгалтерские имеют высокий риск в ОД и низкий в ФТ. К данному блоку относят вопросы, связанные с созданием новых юридических лиц, особенно трастовых компаний, составление актов передачи прав собственности на недвижимость, злоупотребление использованием клиентских счетов.

Пятым блоком выделяют рынок недвижимости, в который входит злоупотребление имуществом (использование в криминальных целях), услуги риелторов и агентств недвижимости. Первая группа оценивается как средний риск для ОД и низкий для ФТ, вторая же как низкий риск ОД/ФТ, так как их деятельность строго регламентирована и жестко регулируется в стране.

Наличность определяется как высокий риск, в основном к нему относят сектора экономики, аккумулирующие большой оборот наличности. Помимо данной группы выделяют отдельно бизнес по обслуживанию денежных средств (обмен валюты, чековое обслуживание, конвертация денежных средств), который также попадает в зону повышенного риска ОД/ФТ.

При этом некоммерческие организации, дилеры с высоким оборотом денежных средств и организации игорного бизнеса Великобритании оцениваются как низкий риск.

Список ключевых терминов, используемых в ходе НОР 2017, состоит из:

- Угроза - люди или действия, которые могут причинить вред. К угрозам отмывания денег относятся основные правонарушения и преступники, которые их совершают, а к угрозам финансирования

терроризма относятся группы и отдельные лица, занимающиеся террористической деятельностью.

- Уязвимость – методы и инструменты, которые могут быть использованы угрозой.

- Последствия - воздействие или вред, которые могут быть вызваны отмыванием денег или финансированием терроризма, включая влияние основной преступной и террористической деятельности на финансовые системы и учреждения.

- Риск - функция угрозы, уязвимости и последствий. Присущие риски могут быть сопоставлены с смягчающими факторами для оценки чистых рисков.

В Канаде действует надежный и всеобъемлющий режим борьбы с отмыванием денег и финансированием терроризма, который способствует целостности финансовой системы и безопасности канадцев. Он поддерживает борьбу с транснациональной организованной преступностью и является ключевым элементом контртеррористической стратегии Канады.

Правительство Канады провело оценку [7] для выявления рисков, связанных с отмыванием денег и финансированием терроризма. В этом отчете не оценивается, насколько эффективно Канада реагирует на проблемы, связанные с ОД/ФТ, скорее, он предназначен для повышения ситуационной осведомленности финансовых учреждений Канады и о всех канадцах, которые, будучи участниками мировой экономики, могут столкнуться с проблемами при нормальном ведении бизнеса. В отчете представлен обзор рисков отмывания денег и финансирования терроризма до применения каких-либо мер по смягчению последствий. Однако эти меры включают ряд законодательных, нормативных и оперативных мероприятий, которые предотвращают, выявляют и препятствуют отмыванию денег и финансированию терроризма.

В Канаде действует национальная система ПОД/ФТ, которая обеспечивает скоординированный подход к снижению рисков, присущих данной оценке, и более широкую борьбу с отмыванием денег и финансированием терроризма. Система ПОД / ФТ включает в себя 11 партнеров по федеральным подразделениям, восемь из которых получают целевое финансирование на общую сумму около 70 миллионов долларов США в год. Выявленные риски устраняются с помощью:

- жесткого режима, который фокусируется на координации политики как внутри страны, так и на международном уровне;

- предотвращения и обнаружения отмывания денег и финансирования терроризма в Канаде;

- раскрытие преступной деятельности, включая расследование, судебное преследование и арест незаконных активов;
- реализация мер по обеспечению постоянного совершенствования режима ПОД/ФТ.

НОР предназначен для предоставления информации о критических рисках населению и, в частности, примерно 31 000 организаций, которые имеют обязательства по отчетности в соответствии с Законом о доходах от преступной деятельности (отмывание денег) и финансировании терроризма (PCMLTFA), чье понимание неотъемлемых основополагающих рисков имеет жизненно важное значение в применении профилактических мер и мер контроля, необходимых для эффективного снижения этих рисков. Правительство Канады рекомендует организациям использовать выводы, содержащиеся в НОР, для информирования их усилий по оценке и снижению рисков. Понимание канадского контекста риска и основных характеристик, которые подвергают секторы и продукты рискам, присущим рискам ОД / ФТ в Канаде, важно для возможности применения мер для их эффективного смягчения.

Оценка неотъемлемого риска состоит из оценки угроз ОД / ФТ и уязвимостей ОД / ФТ, присущих Канаде в целом и ее ключевым экономическим секторам, и финансовым продуктам, с учетом последствий отмывание денег и финансирование терроризма. Общие риски, связанные с ОД / ФТ, оценивались путем сопоставления угроз с уязвимыми секторами и продуктами с помощью методов ОД / ФТ, которые используются преступниками и их посредниками для эксплуатации этих секторов и продуктов. Установив взаимосвязь между угрозами и уязвимостями, был разработан ряд сценариев риска, позволяющих идентифицировать секторы и продукты, которые подвержены наибольшему риску ОД / ФТ.

Для оценки рисков ОД/ФТ был изучен 21 вид преступной деятельности в Канаде, которая в наибольшей степени связана с получением доходов от преступлений, которые могут быть отмыты. Уровень угрозы ОД был оценен очень высоко за коррупцию и взяточничество, контрафакцию и пиратство, некоторые виды мошенничества, незаконный оборот наркотиков, незаконную контрабанду табака и торговлю, а также отмывание денег третьими лицами. Транснациональные организованные преступные группировки и профессионалы по отмыванию доходов являются ключевыми субъектами угрозы ОД в канадском контексте. Многие из этих угроз похожи на те, с которыми сталкиваются некоторые другие развитые и развивающиеся страны.

Угроза ФТ была оценена для групп и участников, которые вызывают наибольшую обеспокоенность в Канаде. Оценка показывает, что в Канаде действуют сети, которые подозреваются в сборе, сборе и передаче средств

за границу различным террористическим группам. Несмотря на эти действия, угроза ФТ в Канаде не так выражена, как в других регионах мира, где можно найти более слабые режимы АТО и где террористические группы закрепились как в плане операций, так и в плане финансирования своей деятельности.

Присущие уязвимости ОД / ФТ представлены для 27 секторов экономики. Оценка показывает, что существует много секторов и продуктов, которые достаточно сильно уязвимы для отмывания денег и финансирования терроризма. Из оцененных областей наиболее уязвимыми были оценены местные банки, корпорации (особенно частные коммерческие корпорации), определенные виды предприятий, оказывающих денежные услуги, и экспресс-трасты. Уязвимость была оценена как высокая для 16 секторов и продуктов, средняя для пяти секторов и продуктов и низкая для одного сектора. Многие из секторов и продуктов имеют высокую доступность для физических лиц в Канаде и на международном уровне и связаны с большим объемом, скоростью и частотой транзакций. Многие ведут значительный объем транзакционных сделок с клиентами с высоким уровнем риска и подвергаются юрисдикциям с высоким уровнем риска, которые имеют слабые режимы ПОД / ФТ и значительные угрозы ОД / ФТ. Во многих секторах также имеются возможности для совершения транзакций с различной степенью анонимности и сложного структурирования транзакций.

Связав угрозы с неотъемлемо уязвимыми секторами или продуктами, оценка показала, что множество из них подвержены очень высоким неотъемлемым рискам ОД, связанным с субъектами угроз. В ходе оценки также были выявлены пять сценариев с достаточно высокими рисками ФТ, в которых участвуют пять различных секторов.

В ходе анализа международного опыта формирования и публикации национальных оценок риска ОД/ФТ, рабочей группой было выявлено, что ряд крупнейших мировых держав используют предикативный подход к идентификации и оценке такого рода рисков. Наглядно данный подход отражен в НОР ОД США, где выводится классификация угроз по предикативным преступлениям, оценивается масштаб их реализации в стране, затем анализируются уязвимости экономики и на их стыке формулируются присущие стране риски

Список использованных источников:

1. Sean O'Connor, Fentanyl: China's Deadly Export to the United States, U.S.-China Economic and Security Review Commission, February 1, 2017.

2. DOJ, Press Release, “Justice Department Announces First Ever Indictments Against Designated Chinese Manufacturers of Deadly Fentanyl and Other Opiate Substances”, October 12, 2017.
3. DOJ, Press Release, “Attorney General Sessions Announces New Indictments in International Fentanyl Case”, April 27, 2018.
4. National risk assessment of money laundering and terrorist financing 2017 [Электронный ресурс]. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf (Дата обращения: 30.08.2021).
5. Crime in England and Wales: Year ending March 2017. ONS. Statistical Bulletin. July 2017
6. Measuring tax gaps 2019 edition. Tax gap estimates for 2017-18 [Электронный ресурс]. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/820979/Measuring_tax_gaps_2019_edition.pdf (Дата обращения: 21.08.2021).
7. Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada, 2015 [Электронный ресурс]. URL: <https://fin.gc.ca/pub/mltf-grpcfat/index-eng.asp> (Дата обращения: 30.08.2021).
8. Sean O'Connor, Fentanyl: China's Deadly Export to the United States, U.S.-China Economic and Security Review Commission, February 1, 2017.
9. DOJ, Press Release, “Justice Department Announces First Ever Indictments Against Designated Chinese Manufacturers of Deadly Fentanyl and Other Opiate Substances”, October 12, 2017.
10. Данные судебной статистики // Судебный департамент при Верховном Суде Российской Федерации [Электронный ресурс]. URL: <http://www.cdep.ru/index.php?id=79> (Дата обращения 14.09.2021).

УДК 001.8:005.934

© В.А. Рычков, В. Давыденко, А.М. Габдуллин, 2021

Методологическая основа SOC

А.М. Габдуллин

студент 2 курса НИЯУ МИФИ, Москва

E-mail: aziz096@mail.ru

В.А. Рычков

старший преподаватель кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: VARYchkov@mephi.ru

В. Давыденко

старший преподаватель кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: VIDavydenko@mephi.ru

Аннотация: Проанализирована методологическая основа построения SOC в Организации любого масштаба. Описаны ключевые подходы.

Ключевые слова: SOC, мониторинг инцидентов информационной безопасности, кибератаки.

Methodological basis for SOC

Abstract: The methodological basis for building a SOC in an organization of any size has been analyzed. Key approaches are described.

Keywords: SOC, information security incident monitoring, cyber attack.

Введение

Пока существуют глобальные компьютерные сети, злоумышленники будут использовать уязвимости. Ранее угрозы компьютерным сетям представлял самораспространяющийся код. Прогресс в области антивирусных технологий значительно снизил этот автоматизированный риск. Появился новый класс угроз, направленных на компрометацию данных для экономического или военного прогресса.

Security operations center (SOC) – синергия людей, процессов и технологий, которая позволяет обеспечить оперативное реагирование на инциденты кибербезопасности, проактивное выявление киберугроз, релевантных для организации, и защиту от них.

Внедрение SOC в организации позволит обеспечить:

- отражение кибератак на организацию;

- выявление киберугроз, которые применимы к организации, и выстраивание своевременной защиты от них;
- получение руководителями организации актуальной информации о защищенности инфраструктуры организации;
- минимизацию финансовых и репутационных потерь от кибератак.

Предлагается рассмотреть методологическую основу с позиции развития SOC либо внедрение отдельных практик SOC.

Модель Cyber-Kill Chain

Cyber Kill-Chain представляет собой перечень действий, выполняемых злоумышленником для достижения поставленных перед собой целей. Суть Cyber Kill-Chain заключается в том, что злоумышленник должен определить, каким образом проникнуть в ИТ-инфраструктуру организации, закрепиться в ней и предпринять действия, необходимые для достижения цели. Таким образом Cyber Kill-Chain является интегрированным сквозным процессом, описываемым в качестве "цепочки", т.к. прерывание на любом этапе приведет к разрыву всего процесса и, как следствие, недостижению злоумышленником поставленной цели.

Модель Cyber-Kill Chain указывает на то, что для осуществления своих намерений нарушители проходят ключевые этапы (рис. 1).

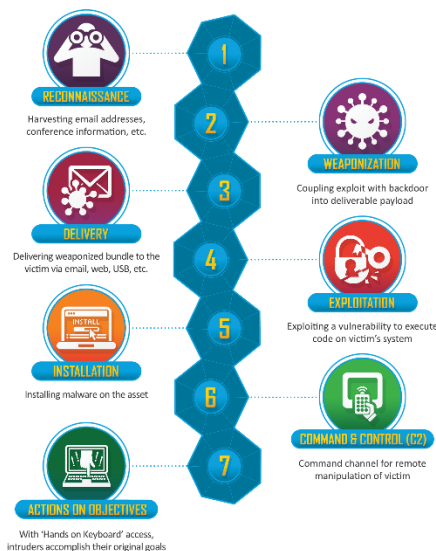


Рисунок – 1 Этапы кибератаки

Понимание модели Cyber Kill-Chain может помочь организациям выстроить системы защиты для противодействия злоумышленнику на каждом из этапов Cyber Kill-Chain. Так же службы кибербезопасности могут оценить эффективность средств противодействия в зависимости от того, на каком этапе может быть обнаружен злоумышленник.

Таблица 1 – Этапы кибератаки

Этапы	Пояснение
Этап 1. Reconnaissance - Разведка	Злоумышленник осуществляет активный и/или пассивный сбор информации, которая необходима для реализации конечной цели, а также для выполнения промежуточных этапов кибератаки. Информация может включать сведения о организации, ИТ-инфраструктуре, персонале организации, клиентах организации и прочее.
Этап 2. Вооружение	Злоумышленник подготавливает средства, включающие в себя создание, покупку или компрометацию/хищение ресурсов, которые могут быть использованы для кибератаки. Такие ресурсы включают компоненты ИТ-инфраструктуры, учетные записи, поддельные адреса электронной почты, эксплойты и прочее средства, которые помогут совершить кибератаку.
Этап 3. Доставка	Первоначальный доступ состоит из техник, которые используют различные способы проникновения в инфраструктуру. Методы, используемые для закрепления позиций, включают доставку фишинга, подключение сторонних устройств в сеть организации или эксплуатацию уязвимостей на общедоступных веб-сервисах организации. Данная техника используется, в основном, для поиска точки, из которой существует возможность доставить вредоносный код в инфраструктуру жертвы, или скомпрометировать необходимые учетные записи.
Этап 4. Эксплуатация	Применение нарушителем кибербезопасности средств и методов удаленного и локального выполнения различных команд, сценариев и исполняемых файлов на атакуемом объекте защиты (компоненте объекта защиты), доставка которых была выполнена на предыдущем этапе кибератаки. Методы запуска часто сочетаются с методами из всех других тактик для достижения более широких целей, таких как исследование ИТ-инфраструктуры или хищение данных.

Этап 5. Установка	Закрепление в инфраструктуре необходимо для наличия доступа у атакующего в случае перезагрузки, изменении учетных данных и других изменениях в инфраструктуре из-за которых он может потерять свою точку входа. Техники, используемые для закрепления в системе, включают в себя определенные изменения доступа, действий или конфигурации системы, которые позволяют атакующему сохранять свою точку входа в инфраструктуру организации, например, подмена легитимного кода или добавление кода запуска при загрузке ОС.
Этап 6. Управление и контроль	Данная тактика состоит из методов, которые атакующие могут использовать для связи с системами, находящимися под их контролем, в сети жертвы. Данные техники чаще всего используют легитимные каналы связи, такие как DNS для построения туннелирования или штатные утилиты проксирования трафика.
Этап 7. Действия по достижению целей	После прохождения первых шести этапов, злоумышленники могут предпринять действия для достижения своих первоначальных целей. Обычно эта цель - кража данных, которая включает сбор, шифрование и извлечение информации из среды жертвы; нарушения целостности или доступности данных также являются потенциальными целями. В качестве альтернативы злоумышленникам может потребоваться доступ только к исходному ящику жертвы для использования в качестве точки перехода для компрометации дополнительных систем и горизонтального перемещения внутри сети.

Особенностью Cyber-Kill Chain является ее нелинейность. Как только нарушитель реализовывает один из этапов, он может снова начинать цепочку, осуществляя дополнительную разведку и выполняя горизонтальное продвижение внутри известной ему инфраструктуры.

Эффективное развитие методологии, команды, технологий SOC направлено на противодействие атакам на каждом этапе модели Cyber-Kill Chain с целью разрыва цепочки действий потенциальных нарушителей.

Разработка сценариев

Сценарий (Use Case) - возможный сценарий реализации угрозы кибербезопасности в отношении важных для Организации активов, таких как критически важные системы, сегменты сети, группы сотрудников с учетом негативного влияния на целостность, конфиденциальность и доступность информации, соответствия внешним и внутренним

требованиям и т.д. Сценарий представляет собой набор правил корреляции событий, то есть описание ситуации или набора ситуаций, которую требуется наблюдать, отслеживать и предпринимать определенные действия в случае обнаружения. В процессе разработки Сценария определяются необходимые источники информации, подлежащие мониторингу, правила корреляции системы мониторинга, дополнительные атрибуты и т.п.

Основой разработки Use Cases является матрица MITRE. Она состоит из тактик проникновения злоумышленника в инфраструктуру организации и каждая тактика имеет набор техник, которыми данная цель может быть достигнута.

Так как методология MITRE не учитывает специфические угрозы, релевантные определенной организации, поэтому, кроме матрицы MITRE разработка Use Case также основана на анализе возможных угроз и поиске уязвимостей, которые, по определению, существуют в ИТ-среде и критичных системах Организации. Для актуальных угроз в порядке приоритета разрабатываются конкретные сценарии, позволяющие детектировать такие угрозы средствами системы мониторинга и затем выполнить действия по их локализации и уничтожению. Таким образом эффективность использования системы мониторинга в решающей степени зависит от используемых Сценариев.

Каждый Сценарий разрабатывается с учетом выявленной угрозы и ее связи с риском, подразделением бизнеса, системой и группой пользователей. Между угрозой и Сценариями установлена связь «один-ко-многим», поскольку одна угроза реализуется разными способами. При этом каждый Сценарий сопоставляется только с одной угрозой, что позволяет однозначно определить угрозу и риск, связанные со Сценарием.

Этапы разработки Сценариев представлены в таблице 2.

Таблица 2 – Этапы разработки сценариев

Этапы	Пояснение
1. Формализация требований	– определение результатов работы Сценариев. Результатом является непосредственное действие (оповещение, создание заявки) или отчет; – определение угроз, на которые отвечают Сценарии. Каждый Сценарий отвечает на конкретную угрозу; – сопоставление Сценариев с классификацией рисков и угроз Организации. Сопоставление позволяет выявить полноту охвата Сценариями вышестоящих уровней за длительный период (несколько месяцев) для выявления тенденций в изменении тактик, техник и практик злоумышленников.

	Результатом этого этапа является набор требований, на основании которых разрабатываются Сценарии.
2. Разработка требований	– создание описания Сценария; – согласование разработанного Сценария; – определение и описание источников событий, необходимых для внедрения Сценария.
3. Разработка правил и подключение источников	– разработка необходимых правил корреляции системы мониторинга на основе описания Сценария; – подключение источников данных, необходимы для работы правил.
4. Тестирование	– тестирование и настройка каждого правила корреляции в отдельности, а также его выходных данных, влияющих на Сценарий; – проверка работы Сценария.
5. Внедрение	– включение Сценария в продуктивную среду; – проверка количества срабатываний; – проведение дополнительной настройки для устранения ложных срабатываний.

Ключевыми задачами проактивного управления являются выявление, определение знаний для формирования понятного описания киберугроз, разработка рекомендации по защите, фиксирование трендов в развитии киберугроз.

Описание киберугрозы выделяет индикаторы компрометации на основании которых разрабатываются и внедряются правила мониторинга, а также действия по реагированию в соответствии с моделью Cyber-Kill Chain.

Пример проактивного управления инцидентами. 14 октября 2021 года в открытых источниках (VirusTotal) были обнаружены вредоносные XLS-документы, используемые в рамках кампании по распространению ВПО SquirrelWaffle. В качестве первоначального вектора атаки злоумышленники использовали письма со ссылками на вредоносные файлами формата Excel. Документы содержали скрытые страницы, на которых в процессе анализа были обнаружены дополнительные сценарии и адреса C2 серверов. Во время исполнения макросов осуществлялась сборка команд для загрузки и запуска полезной нагрузки. Для обхода средств защиты использовалась техника LoLbin ("Living off the Land"), реализованная через легитимное приложение Regsvr32.

В реальной жизни анализ киберугрозы может быть очень и очень сложным. Выполняется реверс кода вирусного программного обеспечения, выявляются тактики, техники, практики, которые использует

злоумышленник, вектор атаки, география распространения, подготавливается подробный отчет от киберугрозе. Проводится анализ взаимодействия с ранее выявленными киберугрозами и строится граф связности.

Список использованных источников:

1. Gaining the advantage. Applying Cyber Kill Chain. Methodology to Network Defense – URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf (дата обращения: 18.11.2021).
2. Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amín, Ph.D., Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. URL: <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf> (дата обращения: 18.11.2021).
3. Carson Zimmerman. Ten Strategies of a World-Class Cybersecurity Operations Center // The MITRE Corporation 2014. – URL: <http://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf> (дата обращения: 18.11.2021).

Методы и технологии обеспечения кибербезопасности в финансово-экономической сфере

Д.В. Капулин

канд. техн. наук, и.о. директора Института космических и
информационных технологий Сибирского федерального университета,
Красноярск

E-mail: dkapulin@sfu-kras.ru

Е.А. Чжан

канд. техн. наук., доцент кафедры интеллектуальных систем управления
Сибирского федерального университета, Красноярск

E-mail: echzhan@sfu-kras.ru

В.И. Вайнштейн

канд. физ.-мат. наук., заведующий научно-учебной лабораторией
информационной безопасности Сибирского федерального университета,
Красноярск

E-mail: vvaynshtyayn@sfu-kras.ru

Аннотация: В работе рассматривается применение методов и средств искусственного интеллекта, применительно к задачам передачи данных, криптографии и обработки неструктурированной информации. Приведены результаты некоторых исследований сотрудников Сибирского федерального университета в области защиты информации и искусственного интеллекта.

Ключевые слова: искусственный интеллект, кибербезопасность, защита данных, распознавание образов.

Methods and technologies for cybersecurity ensuring in the financial and economic sphere

Abstract: The paper considers the application of artificial intelligence methods and tools, applying to the problems of data transmission, cryptography and processing of unstructured information. The set of some results of Siberian Federal University researchers in the field of information security and artificial intelligence are presented.

Keywords: artificial intelligence, cybersecurity, data protection, pattern recognition.

Технологии искусственного интеллекта становятся мощным инструментом обеспечения кибербезопасности в различных сферах и видах деятельности. В финансово-экономической сфере, как и в других отраслях экономики, участие человека считается важным, незаменимым элементом. Обеспечение кибербезопасности по-прежнему во многом зависит от работы специалистов, но при этом решение ряда ключевых задач неизбежно связано с масштабным применением средств вычислительной техники. Каждое технологическое улучшение с применением средств искусственного интеллекта позволяет более эффективно поддерживать роль человека в сфере безопасности [1].

Согласно национальной стратегии развития искусственного интеллекта на период до 2030 года согласно указу Президента Российской Федерации от 10.10.2019 № 490, искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека [2].

Искусственный интеллект наиболее применим в тех областях, где есть большой объем накопленных данных, полученных на значительном числе параметров, часть из которых – неструктурированные. В этой связи основное назначение методов и технологий искусственного интеллекта (ИИ) – наделить вычислительную технику некоторой способностью человеческого разума к особому реагированию на заданные проблемы. На этой основе работают прикладные модели и алгоритмы, включая машинное обучение и глубокое обучение.

Наряду с непосредственно обучением следует выделить применением методов обучения к решению самой задачи обучения. Такой подход получил название «Метаобучение». Изначально, при решении задач приобретения знаний, их представления предполагаются априорно известными и истинными, и нужно построить некоторую систему в рамках этих представлений. В то же время в задачах метаобучения ставится вопрос об автоматическом построении самих представлений знаний, детализация которых сильно изменяется в зависимости от рассматриваемой предметной области. Использование и развитие принципа метаобучения необходимо для преодоления ограничений машинных систем функционировать только в узких предметных областях. Системы, работающие по принципам метаобучения, способны выполнять задачи принятия решений самого разного вида, что позволяет говорить о создании универсальных подходов к решению прикладных задач.

Дальнейшее развитие технологий искусственного интеллекта связано с повышением степени универсальности машинных систем. Достигается это за счет накопления значительного объема первичных данных, организации широкого доступа к информации при исследовании воплощенных систем, к которым относятся системы, помещенные в конкретное информационное, физическое или социальное окружение. Кроме того, следует говорить о развитии подходов метаобучения, переходе к гиперобучению, при котором существует несколько уровней искусственного интеллекта, предназначенных для: интеллектуального решения прикладной задачи, обучения интеллектуальному решению задачи и обучению учителя для интеллектуального решения задачи. В воплощенных системах подразумевается, что поступающая информация должна служить основой обучения, в результате которого формируется система знаний с целью их применения для решения поставленных задач [3].

Спрос на технологии искусственного интеллекта, машинного обучения озвучивают многие отечественные заказчики в различных отраслях, включая социальный и государственный сектора экономики. Так, Федеральная налоговая служба с 2017 г. начала использовать технологии ИИ в личном кабинете налогоплательщика: используется интеллектуальный чат-бот, для решения вопросов, связанных с налоговым администрированием. Он обучен обрабатывать около 150 тыс. различных типовых жизненных ситуаций. Управление информационных технологий Росимущества применяет некоторые элементы искусственного интеллекта при формировании прогнозов доходов федерального бюджета с использованием блокчейн-технологии для организации взаимодействия с другими органами власти. Кроме того, Департамент проектной деятельности правительства России еще в 2017 г. предложил концепцию новой системы правоприменения, в которой будет использоваться искусственный интеллект. В соответствии с инициативой, по типовым делам машинная система сможет самостоятельно генерировать судебные решения и проверять решения на ошибки, а также устранять коррупционную составляющую. В финансовой отрасли интерес к технологиям искусственного интеллекта особенно высок – о спросе и развитии этих технологий заявляли многие российские банки. Специалисты «Сбербанка» считают, что через 5 лет до 80 % всех решений будут приниматься с помощью средств искусственного интеллекта. В «Альфа-банке» прогнозируют, что отрасль активно будет переходить на безлюдные технологии, с устранением операторов и массовым внедрением ботов. Все больше классических банков и страховых компаний понимают экономическое обоснование эффективности использования

искусственного интеллекта в их процессах и создают финансовые продукты с использованием машинного обучения и компьютерного зрения.

В этой связи следует использовать практику наращивания количества отечественных технологий искусственного интеллекта, совершенствовать имеющиеся и создавать новые методы. В противном случае, возможно отставание от мировых тенденций, хотя на сегодняшний день российские разработки достаточно конкурентоспособны на мировом рынке. Не следует также ограничиваться только прикладными технологиями искусственного интеллекта – нужно масштабировать сферу их применения, создавая «сквозные» технологии. Именно такой подход дает значительный эффект уже через короткое время, когда, например, защищенная передача данных использует методы машинного обучения для анализа кодовой последовательности или навигационная аппаратура использует алгоритмы глубокого обучения для решения задач высокоточного определения координат подвижного объекта. Некоторые известные разработки Сибирского федерального университета направлены на решения ряда проблем обеспечения безопасности в современных условиях развития цифровой экономики.

Так, известна работа [4], ключевым аспектом в которой является решение задачи интеллектуальной киберзащиты некоторой абстрактной системы от исследования. Абстрактная техническая или организационно-техническая система формализуется как абсолютно защищенная от исследования, обосновывается применимость технических решений в области информационной безопасности. Интересными практическими результатами работы являются методы, применимые в области информационной безопасности, которые гарантируют создание невоскрываемых операций за счет размывания характеристик системы. Доказывается вариант создания абсолютно неразличимого канала передачи информации с одновременной неполиномиальной сложностью системы с размытыми параметрами компрометации.

Отметим также работу [5], направленную на исследование проблем обеспечения информационной безопасности при беспроводной передаче данных, использовании технологий Интернета вещей. Широкое распространение таких технологий в корпоративном секторе и в секторе электронных устройств для частного пользования закономерным образом привело к росту внимания к этим технологиям со стороны производителей и интеграторов различного рода специализированной аппаратуры. Внедрение интеллектуальных беспроводных технологий расширяет области применения систем автоматизации, контроля и управления за счет новых функциональных характеристик, направленных на мониторинг доступа, контроль периметра, наблюдение за перемещениями персонала,

автоматизация контроля инспекций и технического обслуживания оборудования, контроль экологических параметров и т. д. В качестве алгоритмов шифрования данных в подобных интеллектуальных сетях беспроводной связи широкое применение находят алгоритмы шифрования данных DES и AES. Основными недостатками алгоритма шифрования данных DES являются существование слабых ключей, низкая устойчивость алгоритма к прямому перебору ключей, в том числе с использованием аппаратных средств, низкая устойчивость при атаке с использованием дифференциального криптоанализа. В качестве основного недостатка алгоритма шифрования данных AES следует отметить недостаточную изученность математического аппарата шифрования. Проблема безопасности беспроводных сетей передачи данных в промышленности усугубляется тем, что в России отсутствуют государственные стандарты по информационной безопасности автоматизированных систем управления технологическими процессами, аналогичные таким стандартам как ISA SP99, IEEE 1402, IEC 62351 и пр.

При создании нового средства обеспечения кибербезопасности была поставлена цель обеспечить безопасную передачу данных по промышленным беспроводным сетям передачи данных с использованием отечественного алгоритма криптографического преобразования ГОСТ 28147-89 при работе с устройствами (в том числе мобильными) сторонних производителей. В результате выполнения работы разработана и запатентована конструкция устройства для защиты передачи данных на базе криптографического модуля, реализованного на базе программируемой логической интегральной схемы Xilinx Spartan-6 XC6SLX25 с использованием серийного комплекта разработчика на базе данной ПЛИС на языке описания аппаратуры Verilog. Разработанное устройство подтвердило свою эффективность в ходе экспериментальных исследований, обеспечивает взаимодействие с мобильными устройствами сторонних производителей посредством протоколов USB 2.0 и IEEE 802.11 [6].

При решении задач идентификации различных объектов также широко применяются методы и средства искусственного интеллекта. Такого рода задачи распространены при построении новых систем обработки неструктурированных данных, проектировании систем контроля доступа и автоматического мониторинга и т. д. Зачастую задача идентификации сводится к такой постановке: существует набор образов (например, база изображений) и необходимо по данным, полученным с устройств видеонаблюдения, однозначно идентифицировать текущий образ. Широко распространенный вариант такой идентификации основан на бесконтактном распознавании образов изображений, но при этом обладает

чувствительностью к изменению внешности человека и, как следствие, влечет повышение вероятности ложных срабатываний в действующих системах контроля. В качестве дополнительного метода идентификации подвижных объектов предлагается применять распознавание ходьбы и телосложения, если речь идет о контроле за сотрудниками или людьми в целом. Исследования, проводимые учеными Сибирского федерального университета, позволили дополнить универсальные методы идентификации изображений картами оптического потока, линейно переведенными в заданный интервал по аналогии с RGB каналами. Карты потока разделяются на блоки по 10 кадров с 5-кадровым пересечением и для каждого блока вычисляется рамка, содержащая фигуру человека во всех кадрах блока. Карты оптического потока сегментируются на квадраты, содержащие фигуру человека для подачи на вход нейронной сети. Для настройки искусственной нейронной сети использованы открытые базы изображений CASIA Gait Dataset B и TUM-GAID Dataset. В результате обучения нейронной сети вероятность распознавания человека доведена до 94 %. Кроме того, исследован подход, основанный на идентификации скелета, что дает возможность классифицировать действия человека.

Приведенные примеры разработок выполнены при финансовой поддержке как стороны государства, так и с привлечением средств частных инвесторов. Это показывает высокую заинтересованность различных категорий потенциальных потребителей в использовании прикладных интеллектуальных средств, в том числе для защиты данных и информации. Развитие технологий искусственного интеллекта позволяет расширить возможности и функциональные характеристики приборов, сделать их применение более удобным для потребителей. Кроме того, масштабное развитие средств цифровизации, передачи конфиденциальных данных по беспроводным каналам передачи, позволяет с уверенностью говорить о необходимости применения методов и технологий интеллектуальной защиты данных и в финансово-экономической сфере.

Список использованных источников:

1. Искусственный интеллект и машинное обучение в кибербезопасности – прогноз на будущее [Электронный ресурс] / Официальный веб-сайт Лаборатории Касперского. – Режим доступа: <https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity>.
2. Указ Президента Российской Федерации от 10.10.2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».
3. Альманах «Искусственный интеллект». Аналитический сборник [Электронный ресурс]. – Режим доступа: <https://aireport.ru/>.

4. Стюгин, М. А. Повышение защищенности информационных систем на основе технологий защиты от исследования / М. А. Стюгин // Прикладная информатика. – 2017. – Т. 12. – № 3(69). – С. 103-115.
5. Капулин, Д. В. Устройство аппаратного шифрования производственных данных / Д. В. Капулин, О. В. Дрозд // Информационные технологии. – 2015. – Т. 21. – № 8. – С. 618-624.
6. Патент на полезную модель № 147520 U1 Российская Федерация, МПК H04L 9/00. Устройство для обработки данных: № 2014117249/08: заявл. 28.04.2014: опубл. 10.11.2014 / О. В. Дрозд, Д. В. Капулин; заявитель Федеральное государственное автономное образовательное учреждение высшего профессионального образования Сибирский федеральный университет (СФУ).

Механизмы противодействия незаконному использованию криптовалют в системе ПОД/ФТ

С.А. Сапронов

студент 3 курса магистратуры РГЭУ (РИНХ), гр. ФКZ-833

E-mail: 1karlmarks1@mail.ru

научный руководитель: Е.Н. Алифанова

д.э.н., профессор, заведующая кафедрой «Финансового мониторинга и финансовых рынков» РГЭУ РИНХ, Ростов-на-Дону

E-mail: Alifanovaen@mail.ru

Аннотация: Появление криптовалюты на финансовом рынке привело к новым возможностям для физических и юридических лиц в финансовых операциях. Рост популярности криптовалют как средства платежа приводит к появлению альтернативных стандартным деньгам криптоматов. Упрощение операций с криптовалютой также приводит к росту популярности данного способа платежа в противозаконных схемах.

Ключевые слова: криптовалюта, криптомат, ПОД/ФТ, НОН.

Mechanisms for countering the illegal use of cryptocurrencies in the AML/CFT system

Abstract: The emergence of cryptocurrency in the financial market has led to new opportunities for individuals and businesses in financial transactions. The growing popularity of cryptocurrencies as a means of payment leads to the emergence of alternative cryptomats to standard money. Simplification of operations with cryptocurrency also leads to an increase in the popularity of this payment method in illegal schemes.

Keywords: cryptocurrency, cryptomat, AML / CFT, DT.

Введение

С ростом популярности криптовалют растет и необходимость перевода этой цифровой «наличности» в фиатные деньги. Для некоторых людей криптовалюта является лишь более удобным способом в передаче больших сумм денег, так как комиссии низкие, а переброс больших сумм денег происходит быстрее, так как минует контролирующие инстанции. При такой схеме, если человек честно заработал деньги и лишь ищет способ более удобной передачи нет ничего плохого, однако есть и другие люди,

которые используют такую схему для сокрытия доходов полученных преступным путём, для анонимного для госорганов финансирования терроризма или банальной покупки запрещенных товаров. Естественно, контролирующие органы государства не могут допустить роста незаконного оборота денежных средств и даже электронных денежных суррогатов. Ежедневно разрабатываются всё новые и новые способы вычисления незаконного оборота даже в блокчейне, что помогает выявить преступную сеть и лишить её анонимности.

ЗАКОННЫЙ ОБОРОТ КРИПТОВАЛЮТЫ

В статье были подробно рассмотрены темы вывода денежных единиц из системы блокчейн в фиатные деньги, сопутствующие при этом риски для клиента и для государства, опыт европейских стран в этом вопросе, а также механизмы противодействия использованию криптовалюты при незаконном обороте наркотических и психотропных веществ.

Итак, рассмотрим основные способы перевода:

1. Самостоятельно с помощью бирж;
2. С помощью бирж, но через специальные сервисы-обменники;
3. Через сервисы электронных кошельков;
4. Через терминал.

Это основные способы, доступные сегодня в России.

Рассмотрим каждый способ поподробнее:

1. В России функционируют криптобиржи, которые требуют от своего клиента подтверждения личности для соответствия AML/KYC, а также анонимные. Риски подстерегают клиента с момента регистрации. Сегодня в России не существует законодательной базы, регулирующей создание криптобиржи, правило ее организации, защиты информации пользователей и т.д. Криптобиржи не раз становились жертвами хакерских атак, и пользователи теряли со своих счетов все единицы криптовалют. Удачный механизм противодействия осуществили в Евросоюзе, в частности, в Германии. 25 мая 2018 года официально вступил в силу Регламент (ЕС) 2016/679 (англ. General Data Protection Regulation, рус. Общие положения о защите данных) в текущей версии OJ L 119, 04.05.2016; ред. OJ L 127, 23.5.2018 в качестве обязательного к исполнению для компаний, ведущих свою деятельность на территории 28 стран ЕС, но также и на любые компании вне зависимости от их местонахождения, предлагающие товары и услуги субъектам ЕС, либо ведущие их мониторинг [2]. Закон расширил сферу действия европейского законодательства, детализировал права субъектов персональных данных и ужесточил обязанности операторов при обработке и защите данных с учетом современных технологий;

Российским компаниям стоит обратить внимание на то, что соответствие отечественному законодательству не обеспечивает

автоматического соблюдения GDPR, так как многие процессы и требования введены европейским законом впервые.

Дополнительно к данному закону о защите данных граждан ЕС, Германия позаботилась о защите интересов государства: 27 февраля 2018 года вступил в силу закон, закрепляющий за криптовалютой статус денежных средств. В целях стимулирования интереса людей к выходу из «серой» зоны, Германия признает за криптовалютой именной платежное средство и не только освобождает от возможного налога на прибыль в случае схем «криптовалюта-ценная бумага» или «криптовалюта-товар», все товары, купленные через криптовалюту не облагаются НДС, но с условием, что транзакцию совершил верифицированный пользователь, а сама фирма обязана во всяком случае занести в бухгалтерию такую проводку.

2. Через сервисы-обменники существуют те же риски, что и с криптобиржей, но их можно умножать на два, так как здесь появляется посредник, который так же неофициально занимается своей деятельностью (как и криптобиржа, если зарегистрирована в странах без регулирующего законодательства), поэтому пользоваться можно лишь на свой страх и риск;

3. При использовании сервисов электронных денег на многих из них уже реализован принцип KYC, поэтому для использования сервиса при передаче крупных сумм денег необходимо подтверждать свою личность;

4. Сегодня практически в каждом населенном пункте, даже самом маленьком можно найти банкомат. Они стали обыденной вещью, без которой современному человеку сложнее управлять своими финансами, так как всегда существует необходимость перевода средств из наличной формы в безналичную и обратно. В мире возрастает популярность так называемых криптоматов. Это целое семейство терминалов, которые выполняют подобные банкоматам функции, но могут отличаться по функционалу. Некоторые являются односторонними и предоставляют возможность только занести наличные средства на криптокошелёк, либо предоставляют возможность передачи ед. криптовалюты с одного счета на другой. Это самый распространенный вид криптоматов в России, так как создатели понимают, что в случае предоставления возможности ввода и вывода денежных средств им будет необходимо предпринять ряд действий для соответствия даже российскому законодательству, в частности, доказать, что нет нарушения Статьи 75 Конституции РФ «1. Денежной единицей в Российской Федерации является рубль» [1]. Как мы видим из примера, данный криптомат является ненадежным и все данные, введенные в данном криптомате могут быть украдены и использованы в преступных целях. Телефон, указанный на нем, был недоступен.

Тем не менее, авторы изучили двухсторонний криптомат в Польше, который позволяет переводить криптовалюту с одного кошелька на другой, выводить денежные средства и зачислять на счет с помощью наличных, снимать большие суммы денег, а также прямо в криптомате производить конвертацию из одной криптовалюты в другую. Однако, с условием, что все операции происходят с использованием кошелька, прошедшего идентификацию.

Это обязательное условие было введено Пятой директивой ЕС по борьбе с отмыванием денег (5AMLD), рассмотрением которой занимались ещё с 2018 года, а с января 2020 года директива вступила в законную силу.

НЕЗАКОННЫЙ ОБОРОТ КРИПТОВАЛЮТЫ

Необходимо понимать также тот факт, что сегодняшние организаторы наркоторговли являются продвинутыми пользователями всех новых информационных ресурсов и схем, поэтому и криптовалюта нашла свое применение в ОД/ФТ.

Наиболее часто наркозависимые лица в целях оплаты заказа используют сеть DarkNet.

DarkNet - скрытая сеть, соединения которой устанавливаются только между доверенными пирами, иногда именующимися как «друзья», с использованием нестандартных протоколов и портов.

Анонимная сеть представляет собой систему не связанных между собой виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде. Даркнет отличается от других распределённых одноранговых сетей, так как файлообмен происходит анонимно (поскольку IP-адреса недоступны публично), и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства. Именно поэтому даркнет часто воспринимается как инструмент для осуществления коммуникации в различного рода подпольях и незаконной деятельности. В более общем смысле термин «даркнет» может быть использован для описания некоммерческих «узлов» интернета или относиться ко всем «подпольным» интернет-коммуникациям и технологиям, которые в большинстве своём связаны с незаконной деятельностью или инакомыслием.

В последствии наркозависимые перечисляют наличные д/с на электронные кошельки, которые затем конвертируют в одну из криптовалют. В дальнейшем данные средства переводятся на биткоин-кошельки, зарегистрированные на участников преступной группы, которые впоследствии конвертируются обратно в электронные денежные средства на карты закладчиков, организаторов нарколабораторий, операторов сайта, предоставляющих заказ наркотиков, либо обналачиваются.

Зачастую количество адресов криптокошельков может достигать до 1 тыс. на одного наркоторговца. В целях анонимизации транзакций, правонарушители используют «верную» форму платежей.

Данная схема характеризуется перечислением 80-90% всех активов на один из кошельков, при этом, оставшиеся 10-20% рассылаются на множество других адресов. В конечной итерации все транзакции ведут к миксерам, биржам (не используемым KYC) или на кошельки другим участникам наркоторговли.

Основной проблемой является отсутствие законодательства в РФ, регулирующего операции с криптовалютой.

Таким образом, среди механизмов противодействия финансированию наркоторговли следует выделить:

- разработку соответствующих законов, регулирующих операции с криптовалютой;
- формирование более жестких требований к информационной безопасности. Здесь следует понимать, что как сейчас существуют номинальные юридические лица и оффшорные компании, также в скором времени возможно появятся криптобиржи-однодневки и биржи в странах, где законодательство в сфере криптовалюты не урегулировано (либо регулируется слабо);
- возложить обязанность на банки выявлять по конкретным признакам подозрительные операции, понимать, что даже за реально действующими фруктовыми компаниями могут стоять организаторы наркотрафика;
- разработку соответствующих законов, позволяющих правоохранительным органам оперативно реагировать на деятельность компании, обладающих признаками «финансовой пирамиды», «черного кредитора», «нелегального обменника» или «нелегального брокера»;
- ограничение использования на территории РФ программных комплексов, служащих анонимизации пользователей (анонимных мессенджеров Whois, VPN-программ, браузера Tor);
- подготовка специалистов новой формации, готовых отвечать на новые вызовы и угрозы мировой экономики;
- развитие международного сотрудничества. Только эффективное взаимодействие всех подразделений финансовых разведок мира позволит решить проблему с финансированием наркоторговли посредством использования криптобирж и криптовалют.

При этом, необходимо понимать, что данная отрасль набирает популярность уже сейчас и игнорировать её – значит подвергнуться угрозе появления новой серой экономической сферы, которая не регулируется законодательством.

Заключение

Рассмотрев сложившуюся ситуацию, можно сделать вывод, что несмотря на скептицизм некоторой части сообщества экономистов, криптовалюта набирает популярность и всё больше развивается в качестве средства платежа. Это особенно необходимо учитывать и принимать во внимание тот факт, что с ростом популярности растёт и незаконное использование криптовалюты в преступных схемах, поэтому необходимо уже сейчас поднимать вопросы о её регулировании.

Список использованных источников:

1. Статья 75 Конституции Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // Собрание законодательства РФ. - 04.08.2014.
2. Regulation (EU) 2016/679 (General Data Protection Regulation). // General Data Protection Regulation. / Электронный ресурс / <https://gdpr-info.eu> (Дата обращения 20.02.2020).
3. Anti-money laundering and counter terrorist financing. // European Commission. / Электронный ресурс / https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en#enhancingaccesstofinancialinformationbylawenforcement (Дата обращения 20.02.2020).

Моделирование профиля поведения пользователя веб-приложения на основе интеллектуального анализа разноуровневых журналов

И.К. Егоров

студент 2 курса аспирантуры НИЯУ МИФИ, Москва

E-mail: egorovi.k@yandex.ru

В.Ю. Радыгин

к.т.н., доцент кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: vyradygin@mephi.ru

Аннотация: В статье описывается применение моделирования поведения пользователей для решения актуальных задач, обосновывается необходимость разработки собственного алгоритма, выполняющего поведенческий анализ в рамках проводимого исследования. Также приводится описание архитектуры опытной информационной системы и способ сбора необходимых данных для проведения моделирования.

Ключевые слова: моделирование поведения пользователей, информационная система, персональные данные, User-Agent, Ruby on Rails.

Modeling the User Behavior Profile of a Web Application Based on Multilevel Log Mining

Abstract: The article describes the application of user behavior modeling to solving urgent problems, substantiates the need to develop a custom algorithm that performs behavioral analysis within the framework of the research. It also provides a description of the architecture of the experimental information system and a method for collecting the necessary data for modeling.

Keywords: user behavior modeling, information system, personal data, User-Agent, Ruby on Rails.

В современном мире организациям трудно вести свою деятельность без использования информационных технологий. С распространением сети Интернет и ростом его доступности, самым эффективным способом взаимодействия с клиентами является обратная связь через веб-сайт организации. С увеличением функционала веб-приложения возникает задача его оптимизации из-за роста числа и длины возможных веб-путей и

количества пользователей. Оптимизация веб-информационной системы для повышения эффективности веб-приложения – на сегодняшний день одна из наиболее востребованных задач в сети Интернет.

С подобной проблемой сталкивается и НИЯУ МИФИ. Причем задача актуальна для информационных систем, предназначенных не только для широкого доступа всех сотрудников и студентов, но и для систем узкой направленности административного использования. Для решения данного вопроса выбран подход, использующий моделирование поведения пользователей с целью оптимизации взаимодействия информационных систем с учётом особенностей веб-браузеров разных групп пользователей, использующих разные устройства. Исходными данными являются записи разноуровневых журналов, в том числе данные об использовании веб-приложения пользователями.

Моделирование поведения пользователей на сегодняшний день может быть использовано в разных областях. На основе анализа публикаций, среди решаемых задач можно выделить обеспечение безопасности, разработку эффективных веб-интерфейсов и её автоматизацию, оптимизацию выдачи поисковых систем и анализ профилей социальных сетей.

Обеспечение безопасности с помощью моделирования поведения пользователей описано в публикации [1], в которой авторы предлагают использовать анализ последовательности кликов для определения вредоносных аккаунтов и для понимания особенностей поведения групп таких аккаунтов. Несмотря на схожесть исходных данных, разработанная система, описанная в публикации, не может быть использована для решения поставленной задачи, так как она используется для анализа данных социальных сетей, функционал которых не предусмотрен в рассматриваемой информационной системе.

В публикации [2] рассматривается использование моделирования поведения пользователей для автоматизации некоторых процессов в разработке веб-интерфейсов. Описанные в работе методы могут быть использованы в исследовании, но для достижения цели их недостаточно, так как оптимизация интерфейса является подзадачей исследования.

Использование моделирования поведения пользователя описывается в публикации [3]. В ходе исследования, как и в представленной работе, будет строиться граф по схожим принципам. Соответственно, для анализа активности пользователей может быть использована предложенная авторами модификация стандартного алгоритма графовой нейронной сети. Но в представленной работе исходные данные покрывают слишком много различных областей, из-за чего разработанная модификация может иметь

недостаточную точность при работе с данными, используемыми в исследовании.

Анализ профилей в социальных сетях с помощью моделирования поведения пользователей описывается в работе [4]. Разнородность данных, используемых в публикации, чем также обладают исходные данные в исследовании, позволяет использовать описанные авторами методы предварительной обработки и машинного обучения. Но, как и в первом случае, из-за того, что разрабатываемая авторами система имеет функционал, отсутствующий в исследуемой системе, предложенный способ моделирования не подходит для поставленной задачи.

В связи с тем, что не было выявлено подходящих систем для моделирования поведения пользователей в информационных системах в области образования, было принято решение о разработке собственного программного обеспечения для выполнения этого анализа.

Так как разрабатываемое программное обеспечение должно стать частью существующей информационной системы, необходимо описать информационные технологии, с помощью которых эта система разрабатывалась. Исследуемая информационная система является веб-приложением на базе архитектуры «клиент-сервер». Серверная часть, обладающая большими вычислительными мощностями, выполняет автоматизацию необходимых процессов, и взаимодействует с клиентами по протоколу *HTTP*, предоставляя интерфейс, который отображается в веб-браузере клиента. Такое взаимодействие реализуется с помощью веб-фреймворка *Ruby on Rails*, который позволяет настроить взаимодействие сервера базы данных, веб-сервера и программных средств для обеспечения необходимой автоматизации.

Веб-фреймворк использует архитектуру «Модель-Представление-Контроллер», в которой Представление предназначено для отображение данных пользователю через веб-браузер, Модель предоставляет доступ к данным и изменяет Представление, а Контроллер — взаимодействует с пользователем по протоколу *HTTP* и манипулирует Моделью необходимым образом. Для хранения данных используется реляционная система управления базами данных *PostgreSQL*. *Ruby on Rails* с помощью программных интерфейсов позволяет составлять запросы к выбранной СУБД, таким образом обеспечивается доступ к хранимым данным через Модель. Программный пакет *Ahoy*, подключаемый к Контроллеру, получает данные об использовании веб-интерфейса пользователями путем анализа заголовка *User-Agent* пакета протокола *HTTP*, и отправляет полученные данные на хранение. На основе обработки полученных данных будет производиться моделирование поведения пользователей.

Предназначение заголовка *User-Agent* подробно описано в спецификации [5] протокола *HTTP*. Значение этого поля позволяет серверам адаптировать ответ для устройств с разными техническими характеристиками, определить возможные проблемы совместимости и для аналитики использования программных средств, а именно операционной системы и браузера. При этом заголовок *User-Agent* отправляется при каждом запросе в случае, если в настройках сервера не указано иное поведение. Значением заголовка является строка, в которой указываются идентификаторы продуктов в порядке убывания значимости. Например, в значении *Mozilla/5.0 (Linux; Android 8.1.0; ZB602KL) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.74 Mobile Safari/537.36* указывается: операционная система *Android* версии 8.1.0 на базе *Linux*, модель устройства *ZB602KL*, движок отображения веб-страниц *AppleWebKit* версии 537.36 с указанием инструмента просмотра веб-страниц *KHTML* на базе *Gecko*, веб-браузер *Chrome* версии 95.0.4638.74, тип устройства *Mobile* и совместимость с веб-браузером *Safari* версии 537.36.

Можно заметить, что в поле передаются достаточно подробные данные об устройстве пользователя. С одной стороны, это может помочь улучшить взаимодействие между сервером и клиентом за счет формирования передаваемых данных таким образом, что для конкретного устройства они будут отображены наиболее корректным образом. А с другой — уменьшают пропускную способность канала связи из-за большого объема данных, и при перехвате могут быть использованы злоумышленниками для компрометации пользователей. Значение заголовка генерируется программным обеспечением на стороне клиента и может изменяться в зависимости от параметров программного продукта.

Формировать значение заголовка *User-Agent* может не только программное обеспечение, но и сам пользователь при использовании современного браузера. В режиме адаптивного дизайна, предназначенном для отладки отображения веб-страниц, пользователь может вручную ввести как значение заголовка *User-Agent*, так и размеры отображаемой веб-страницы. Данный факт может быть использован как по назначению, так и для предотвращения нежелательного сбора статистики сторонними веб-страницами. Такой метод составления значения заголовка допустим, так как *User-Agent* не является необходимым для взаимодействия веб-браузера клиента и сервером, и значение поля, сгенерированное вне разработанных спецификаций, не нарушает работоспособность программного обеспечения. Данный факт более значим, если учесть, что в недавнем прошлом был принят новый стандарт [6], описывающий способ оптимизации отображения содержимого веб-страниц с помощью медиа-

запросов, выполняемых на стороне клиента для определения разрешения дисплея устройства.

Тем не менее, не соответствующее спецификации значение заголовка *User-Agent*, при выполнении поставленной задачи, может затруднить определение поведения конкретного пользователя. Для решения этой проблемы применяется моделирование поведения пользователей. Имея набор корректных данных о способах использования веб-интерфейса различными пользователями, можно опираться не на данные об устройстве пользователя, а на характер его взаимодействия с информационной системой для оптимизации её работы.

Процесс моделирования поведения пользователей будет проходить следующим способом. При переходе пользователя на веб-страницу в рамках веб-приложения, в базу данных будет вноситься соответствующая запись, содержащая ip-адрес пользователя, исходная и целевая веб-страницы, информация об устройстве пользователя, в том числе и значение поля *User-Agent*, а также идентификатор пользователя, если он авторизован в системе. За внос этой записи в базу данных отвечает программный пакет *Ahoу*, описанный ранее в архитектуре существующего веб-приложения. Затем, запись будет сопоставлена с систематизированными ранее данными с помощью реляционной СУБД *PostgreSQL*, и внесена в граф переходов пользователей по веб-страницам.

После обновления данных графа и актуализацией настроек информационной системы, будет определяться текущая сессия пользователя для дальнейшего анализа использования веб-интерфейса. Далее, на основе выделенных сессий по выбранным параметрам будет проведена кластеризация с помощью языка программирования Ruby статистическими методами, либо методами машинного обучения в зависимости от выбранных параметров. Из полученных данных будут составлены профили поведения пользователей, которые в дальнейшем будут использоваться для расчета вероятного поведения конкретного пользователя в зависимости от данных, которые поступают во время взаимодействия пользователя с веб-интерфейсом. Итоговый программный продукт будет интегрироваться в существующую информационную систему в виде *gem*-пакета, что также позволит использовать его в разных информационных системах независимо друг от друга.

В процессе моделирования поведения пользователей возникают вопросы обеспечения информационной безопасности, в частности о необходимости обеспечения конфиденциальности данных о пользователях. В разрабатываемой системе используемые данные не будут являться персональными. Во-первых, за идентификацию пользователей должна отвечать авторизационная система, наличие которой является

необходимым для корректной работы разрабатываемого программного обеспечения. Взаимодействие авторизационной системы и разрабатываемого программного обеспечения будет производиться путем передачи идентификаторов пользователей, данные которых в этом случае являются обезличенными. Во-вторых, полученные данные в ходе использования пользователем веб-интерфейса необходимы лишь только для выявления активности конкретного пользователя в потоке поступающих данных без установления его личности. Таким образом, использование разрабатываемого программного обеспечения не требует проведения дополнительных мероприятий для соблюдения конфиденциальности существующих персональных данных в информационной системе.

В результате исследования будет разработано программное обеспечение, которое будет производить моделирование поведение пользователей на основе данных использования веб-интерфейса информационной системы, и интегрирование будет выполняться путем подключения модуля в виде программного пакета. При этом в существующую систему будут вноситься лишь дополнения, а не изменения структуры, что позволит использовать разрабатываемое программное обеспечение в веб-приложениях на базе *Ruby on Rails*. Возможность выбора метода построения моделей сделает разрабатываемое программное обеспечение универсальным.

Список использованных источников:

1. Clickstream User Behavior Models / Wang G. [и др.]. - ACM Transactions on the Web. - 2017. № 4 (11). - с. 1-37.
2. Bakaev, M. Manual and Automated Labeling of Web User Interfaces for User Behavior Models / A. Stepanova, M. Bakaev. - 2020
3. Gao, Q. Graph Neural Network and Context-Aware Based User Behavior Prediction and Recommendation System Research / Gao Q., Ma P. - Computational Intelligence and Neuroscience. -2020. - с. 1–14.
4. Personality Predictions Based on User Behavior on the Facebook Social Media Platform / Tadesse M. M. [и др.]. - IEEE Access. - 2018. (6). - с. 61959–61969.
5. Fielding, R. T. Internet Engineering Task Force. Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content / Fielding R. T., Reschke J. - 2014.
6. Jackson, D. Media Queries Level 5 / D. Jackson, F. Rivoal, T. Atkins (мл.). – 2020.

Мониторинг рисков ИТ- безопасности как навигатор ESG-устойчивости цифровой экономики и финансов

Н.А. Казакова

д.э.н. наук, профессор, профессор базовой кафедры финансовой и
экономической безопасности, Российский экономический университет
имени Г.В. Плеханова

E-mail: kazakova.na@rea.ru

А.А. Петюкова

магистрант программы «Бизнес-аналитика в экономике и управлении»
Российский экономический университет имени Г.В. Плеханова

E-mail: petyukovaaa@mail.ru

Аннотация: В статье рассмотрены проблемы и риск-факторы информационной безопасности цифровой экономики, предложены индикаторы для мониторинга ESG-устойчивости цифровой экономики, сделаны прогнозы расходов на информационную безопасность на период до 2025 года.

Ключевые слова: мониторинг, риски, информационная безопасность, аудит, финансы, ИТ-компетенции.

IT security risk monitoring as a navigator of ESG sustainability of the digital economy and finance

Abstract: The article examines the problems and risk factors of information security of the digital economy, proposes indicators for monitoring the ESG sustainability of the digital economy, makes forecasts of information security costs for the period up to 2025.

Keywords: monitoring, risks, information security, audit, finance, IT competencies.

Введение

Сегодня стратегия устойчивого развития (Environmental, Social and Governance или ESG - стратегия) - одна из ведущих тем самых авторитетных международных и национальных форумов мира, ей посвящены многочисленные исследования в самых разных областях науки и практики. Понимая данную проблему и ее значимость для дальнейших шагов по сближению международных практик, Всемирный экономический

форум 2020 года предложил новый проект по формированию единой релевантной системы показателей, ориентированной на оценку устойчивого развития экономики как отдельных компаний, так и отраслей и государств, в целом.

Учет, бизнес-аналитика и аудит являются высоко автоматизированными процессами, и с ростом информационных технологий растет и несанкционированный доступ к информационным системам и данным, угрозы для социальных и технологических процессов, сопутствующих информатизации и цифровизации экономики и финансов. В результате информационная безопасность является главным условием разработки программного обеспечения и баз данных для хранения информации во всех секторах экономики. Кроме того, формирование и оценка ИТ-компетенций у будущих кадров в сфере учета, аудита, финансов и экономической безопасности должны соответствовать требованиям международных и национальных стандартов информационной безопасности.

Проблемы безопасности информации в России и за рубежом

За последнее десятилетие объём хранимой информации в компаниях, в банковской и некредитной финансовой сфере, а также в госсекторе вырос в десятки раз. Данные стали ключевым компонентом работы всех субъектов экономики - от государственных учреждений до малого бизнеса. Как утверждает один из основателей китайского гиганта Alibaba, Джек Ма, - в наше время «данные – это новая нефть» [1]. Как результат, информация стала одним из самых дорогих и нелегальных товаров, а информационная безопасность превратилась в одну из ключевых составляющих экономической безопасности национальной и мировой экономики [2].

О росте киберпреступности говорит статистика и аналитики ведущих информационно-консалтинговых компаний. Так, по данным отчёта о глобальных утечках российской компании InfoWatch, в 2020 году только было официально зарегистрировано 2395 утечек, при этом их количество сократилось, что довольно странно, на 4,5% по сравнению с 2019 годом, однако увеличились объёмы утечек и масштабы последствий, то есть количество кибератак выросло с 47% в 2019 году до 56% в 2020 году [3].

На рис. 1 представлена статистика случаев утечки информации вследствие кибератак за период 2006-2020 гг.

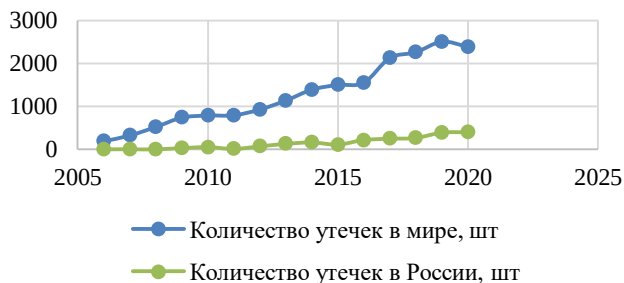


Рисунок 1 – Статистика случаев утечки информации в результате кибератак за 2006-2020 гг.

В 2020 году на территории Российской Федерации было зарегистрировано 404 случая утечки информации. Чаще всего утечки фиксировались в медицине (19%) и высокотехнологичных компаниях (18,2%), реже всего в промышленности (6%). По объему утечек лидируют высокотехнологичные компании (интернет-сервисы) — 18% случаев утечки информации. На банки и другие финансовые организации приходится 10% случаев утечки информации. На долю государственных и муниципальных органов приходится в совокупности 32,4% от всех случаев, зафиксированных в 2020 году [4].

Доля России в общем объеме зарегистрированных утечек информации в мире ежегодно растет, достигнув 17% в 2020 году (рис.2). В результате в 2020 году Россия оказалась на пятом месте в мире среди стран с наибольшей суммой ущерба от действий киберпреступников в 2020 году, млрд долл. (рис.3) [5].

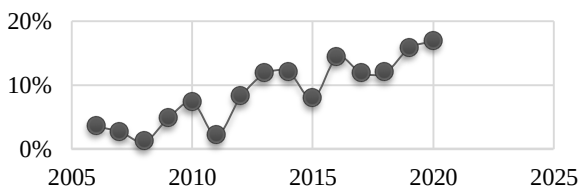


Рисунок 2 – Динамика доли России в общем объеме зарегистрированных утечек информации в мире за период 2006-2020 гг.

Рынок кибербезопасности является одним из быстроразвивающихся рынков: в 2010 году, по данным ежегодного отчёта компании Gartner, он достигал 31,1 млрд. долл., в 2015 году - 75,5 млрд. долл., в 2019 г. – более 120 млрд. долл., а в 2021 году компания прогнозирует объем рынка 150 млрд. долл. [6].

По итогам 2020 г. больше половины рынка приходится на услуги информационной безопасности, 10-15% - на сегменты защиты инфраструктуры и оборудования для сетевой безопасности [7].

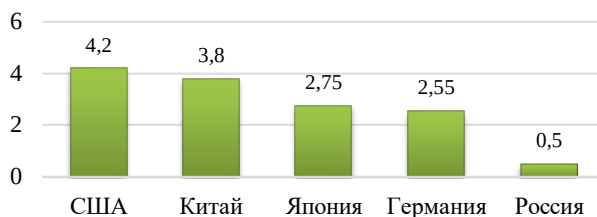


Рисунок 3 – Первая пятерка стран с наибольшей суммой ущерба от действий киберпреступников в 2020 году, млрд долл.

По оценкам экспертов компании McAfee, киберпреступность обходится мировой экономике более чем в 1 трлн долл., что составляет 1% мирового ВВП. При этом под потерями от киберпреступности понимают повреждение и уничтожение данных, кражу интеллектуальной собственности и денежных средств.

Согласно отчёту «Internet Crime Report», представленному ФБР, США является страной, понёсшей наибольшие потери от действий киберпреступников, сумма ущерба составила около 4,2 млрд долл. [7]. По данным Сбербанка за 2020 год российская экономика потеряла около 2,5 трлн руб. или 0,5 млрд долл. [8].

Факторы, тенденции, индикаторы уровня ИТ- безопасности цифровой экономики

Мониторинг рисков ИТ- безопасности представляет собой процесс наблюдения, анализа и диагностики информационной безопасности цифровой экономики в целях обеспечения ее устойчивого развития и в условиях высокой турбулентности происходящих в ней процессов в их тесной взаимосвязи с мировым пространством.

Проведенное исследование позволило выявить целый ряд факторов, которые оказывают сегодня и могут оказывать в дальнейшем существенное влияние на расходы бизнеса и государственного сектора и соответственно уровень информационной безопасности экономики. Среди них ключевая роль отведена факторам, связанным с пандемией и цифровизацией, что ведет к увеличению доли сотрудников, работающих в удаленном режиме, а также децентрализации инфраструктуры, переводу информационных ресурсов в облачные технологии, развитию средств коллаборации сотрудников, что повышает риски ИТ- безопасности и соответственно увеличивает расходы компаний и государственное финансирование информационной безопасности.

Для мониторинга уровня информационной безопасности могут быть использованы такие показатели, как: динамика доли IT-сектора в ВВП, доля сегмента IT-безопасности, количество программ/средств защиты информации, объем финансирования проектов информационной безопасности, объем инвестиций в данный сектор, динамика численности персонала, относящегося к IT-безопасности, уровень развития законодательства, наличие стандартов IT-безопасности, уровень их внедрения в госсектор и бизнес.

Проводимые сегодня международные исследования опираются на комплаенс – подход и экспертные, субъективные оценки. Фактографические показатели используются лишь в отдельных локальных исследованиях, и даже расчет глобального индекса кибербезопасности (Cyber Readiness Index (CRI) 2.0) Потомакским институтом политических исследований (США) основывается всего лишь на комплаенс - оценке национальных законодательств. При этом, данных по России в их исследованиях нет, очевидно, потому, что в российском законодательстве отсутствует понятие киберпреступности, оно включено в общее понятие информационной безопасности [7].

В этой связи, наши прогнозы уровня IT-безопасности основывались на тенденциях развития рынка кибербезопасности в мире и в России, с использованием математико-статистического инструментария и сценарного подхода. На рис. 4 и 5 представлены результаты прогноза расходов на кибербезопасность на 2021-2025 гг. на основе факторов доли IT-сектора в ВВП и численности сотрудников, занятых в IT-секторе в области кибербезопасности [6].

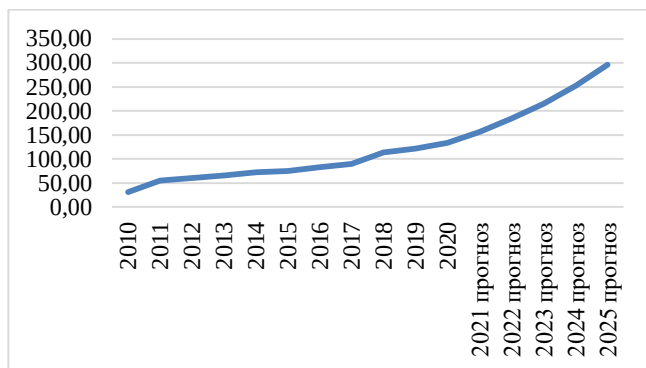


Рисунок 4 – Динамика мировых расходов на кибербезопасность за период 2011-2020 гг. и прогнозы на 2021-2025 гг., млрд долл.

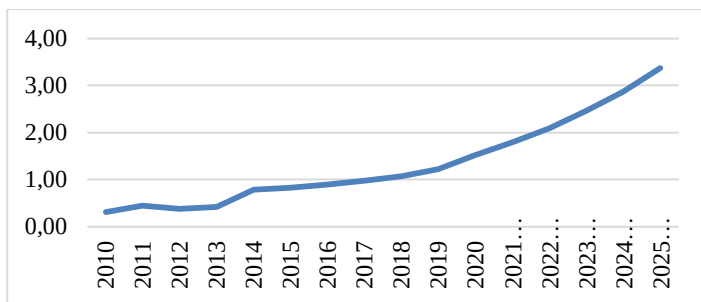


Рисунок 5 – Динамика расходов на кибербезопасность в РФ за период 2011-2020 гг. и прогнозы на 2021-2025 гг., млрд долл.

Таким образом, IT-сектора наше исследование показало, российский сектор информационной безопасности развивается более быстрыми темпами нежели мировой, что подтверждает, начиная с 2014 года, более крутая кривая динамики расходов на кибербезопасность в РФ. По данным прогноза от Gartner [6], в 2021 году ожидается объём мирового рынка кибербезопасности около 150 млрд долл., что вполне коррелирует с нашим оптимистическим прогнозом расходов на информационную безопасность в объеме около 156 млрд долл.

Кроме того, необходимо обратить внимание на то, что на российском рынке информационной безопасности наблюдается тенденция вытеснения западного влияния на российские разработки, так как одними из главных потребителей средств информационной безопасности являются госсектор и крупный бизнес. Аналогичные тенденции происходят и в ряде других стран, например, в Китае.

Еще одним стимулом для роста рынка информационной безопасности в России является развитие законодательства. Растет число проектов, связанных с приведением инфраструктуры информационной безопасности в соответствие с требованиями регуляторов: проектов в области защиты критической информационной структуры, исполнения требований ГОСТ Р 57580.1–2017 для финансовых организаций, а также ужесточившихся требований ФЗ-152 «О защите персональных данных» в отношении локализации данных граждан РФ на территории страны. 2 июля 2021 год президент России подписал Указ № 400 «О Стратегии национальной безопасности Российской Федерации», ключевым вопросом которого является защита электронного информационного пространства от киберпреступности.

Таким образом, обобщая результаты исследования, следует заметить, что по мере внедрения информационных технологий, вместе с

позитивными аспектами, улучшающими бизнес-процессы, коммуникации и качество жизни, развитие ИТ-систем несет значительные риски и приводит к негативным последствиям, и потому должно быть под контролем государства. На обеспечение безопасности информации направлены государственные программы, законодательная база, стратегия развития национальной электронной промышленности и информационных технологий в сфере противодействия финансированию терроризма и экстремизма.

Заключение

Ответом на вызовы тотальной цифровизации и пандемии стала цифровая трансформация бизнеса, и связанные с ней изменения в приоритетах в бизнес-образовании и управленческих технологиях [9]. Сегодня учет, аналитика, аудиторско-консалтинговая деятельность являются высоко технологичными процессами, а безопасность цифровой среды стала главным условием работы с программным обеспечением и базами данных [10]. Проведенное исследование позволяет прогнозировать дальнейший рост рисков информационной безопасности. Понимая повышение потребности аудиторско-консалтингового бизнеса в молодых кадрах, хорошо владеющих ИТ-технологиями и умеющих их применять в аудиторской деятельности Единая аттестационная комиссия по проведению квалификационного экзамена на право осуществления аудиторской деятельности в РФ в 2021 году существенно увеличила долю вопросов на ИТ-компетенции в тестовой базе и практических заданиях экзамена [11]. Профессиональное образование в аудите и финансах будет опираться на цифровые технологии, обработку и аналитику больших данных, высокие этические нормы, обоснованное профессиональное суждение, а также потребует компетенций в области информационной безопасности, противодействия финансированию терроризма и экстремизма, технологий оказания дистанционных услуг [12].

Список использованных источников:

1. Петренко С.А., Петренко А.С. Новая доктрина информационной безопасности Российской Федерации // Защита информации. Инсайд. 2017. № 1 (73). С. 33-39.
2. Казакова Н.А. Концепции контроллинга экономической безопасности компании: анализ российского и зарубежного подходов.// Фундаментальные исследования. 2016. № 12-2. С. 416-421.
3. Глобальное исследование утечек конфиденциальной информации в 2020 году // InfoWatch. – 2021. – URL: InfoWatch_Мир_Утечки_2020_v.1.17.pdf (дата обращения 15.08.2021)

4. Утечки данных. Россия. 2020 год // InfoWatch. – 2021. – URL: с IW_Россия_2020_утечки_v 1 7 1пп (2).pdf (дата обращения 16.08.2021)
5. Международные рейтинги стран по развитию ИКТ // Институт развития информационного общества. – 2021. – URL: <http://eregion.ru/mezhdunarodnye-ryeitingi> (дата обращения 27.08.2021)
6. Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed \$150 Billion in 2021 // Gartner Inc. – 2021. – URL: <https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem> (дата обращения 20.08.2021)
7. Drew R., Top Cybersecurity Companies for 2021 // eSecurity Planet. – 2021. – URL: <https://www.esecurityplanet.com/products/top-cybersecurity-companies/#fortinet> (дата обращения 21.08.2021)
8. The National Initiative for Cybersecurity Careers and Studies. – 2021. – URL: <https://niccs.cisa.gov/> (дата обращения 17.09.2021)
9. Казакова Н.А. Влияние цифровой экономики на образование и профессиональное развитие специалистов финансового рынка // Национальные интересы: приоритеты и безопасность. – 2019. – Т. 15, № 8. – С. 1394 – 1405.
10. Бровкина Н.Д., Казакова Н.А. Оценка компетенций и профессиональных навыков аудитора в цифровой среде: наиболее значимые аспекты использования информационных технологий в аудите // Аудитор. 2020. Т. 6. № 8. С. 20-24.
11. Казакова Н.А. Развитие национальной системы квалификационной аттестации аудиторских кадров как фактор повышения качества аудита и востребованности профессии. // Аудитор. 2021. Т. 7. № 8. С. 24-28.
12. Сайт АНО «ЕАК» <http://www.eak-rus.ru/> .

Мошенничество с криптовалютой

П.М. Аскерко

студент 3 курса ФФБД БГЭУ, Минск

E-mail: polina.askerko@mail.ru

И.Д. Шикунец

студент 3 курса ФФБД БГЭУ, Минск

E-mail: innashikunets123@gmail.com

научный руководитель: В.В. Позняков

к.э.н., доцент кафедры банковского дела БГЭУ, Минск

E-mail: Pozniakov@bseu.by

Аннотация: Статья посвящена исследованию криптовалюты, видам мошенничества на фоне роста популярности виртуальных денег. Авторами предоставлены пути решения и разработаны предложения, направленные на минимизацию преступлений с криптовалютой.

Ключевые слова: криптовалюта, блокчейн, биткоины, мошенничество, майнинг, криптокошелек, криптоинвестор.

Cryptocurrency Fraud

Abstract: The article is devoted to the study of cryptocurrencies, types of fraud against the background of the growing popularity of virtual money. The authors have provided solutions and developed proposals aimed at minimizing crimes with cryptocurrency.

Keywords: cryptocurrency, blockchain, bitcoins, fraud, mining, crypto wallet, crypto investor.

Криптовалюты — это вид наиболее распространённых альтернативных валют. В отличие от различных электронных денег и финансовых инструментов, этот вид валюты децентрализован, и таким образом он не поддается правительственному контролю какого-либо государства. В свою очередь криптовалюты не имеют иерархической структуры, то есть представлены в качестве однорангового инструмента, в таком случае отдельные пользователи могут купить и продать товар друг другу напрямую, без участия каких-либо посредников сторонних организаций, например, банков. Вдобавок некоторые криптовалюты являются анонимными, но это самая часть их характеристики.

Рассматривая основные криптовалюты, можно заметить, что они включают в себя набор базовых технологий и концепций, с помощью которых существует возможность брать на себя ответственность и имеется возможность отслеживать транзакции между банками и иными пользователями.[3]

Все операции, связанные с криптовалютой реализуются посредством блокчейна. Блокчейн — распределенный реестр, состоящий из цепочки блоков, внутри каждого из которых записаны транзакции. Все блоки связаны между собой цепочкой и являются зависимыми друг от друга. Данная последовательность не подлежит нарушению или же видоизменению, таким образом данные в сети криптовалюты будут считаться действительными.

Вся криптовалюта хранится на электронных кошельках. А для того чтобы получить доступ к электронному кошельку используется ключ. Существует два вида ключей. Публичный, который является адресом, позволяющий просматривать содержимое кошелька любому желающему. Приватный — ключ является необходимым для списания средств с электронного кошелька [4].

Причины, благодаря которым виртуальные деньги получили популярность следующие:

- Высокая популяризация, универсальность, доступность. Кошелек достаточно просто создать на любом из электронных носителей: смартфон или планшет, компьютер на различных операционных системах.

- Простота и открытость различных расчетных операций. Полная история всех входящих и исходящих транзакций хранится не имея какого-либо ограничения по времени, а также обеспечивается полный контроль.

- Каждый узел системы генерации криптовалюты равноправен, не имея объединенного центра, что исключает возможность блокировки электронных кошельков, отмены и контроля платежей.

- Увеличение независимости платежной системы происходит при помощи максимальной анонимности. При совершении платежей существует возможность указывать адрес, номер счета по желанию владельца электронного кошелька, с которого будет осуществляться платеж.

Для защиты проводимых пользователями транзакций используется криптографический метод. По этой причине провести финансовую операцию не получится без её подтверждения специальным проверочным кодом. Если код введен верно, то ни один человек не сможет отменить подтвержденный кодом перевод денег, что исключает мошенничество при оплате криптовалютой различные услуги или товары.

В результате довольно высокой надежности электронных кошельков, которые защищены закрытым ключом, криптовалюта может быть использована в качестве созданных сбережений. Данные накопления пригодятся для универсального средства обмена, способа расчета в интернет-магазинах или на биржах фрилансеров. За счет значительного роста курса относительно доллара США многие пользователи накапливают биткоины для дальнейшего увеличения своих сбережений.

Технология блокчейн, используемая в производстве монет криптовалюты, дает возможность для создания неограниченного количества видов цифровых денег. Для того чтобы добиться высокой популярности цифровых денег и подключить к майнингу (процессу производства) большое количество пользователей могут не все. Без развитой сети количество «монет» будет минимальным и заинтересованности для общественности такая «валюта» представлять не сможет.

Во многих европейских странах, включая Россию, допускается возможность выпуска «государственной» криптовалюты.

Популярность принято считать по величине курса к доллару США:

- Bitcoin. Первый вариант криптовалюты, появился в 2009 году.
- Ethereum. Создание началось в 2015 году. Технология используется в регистрации сделок, передаче ресурсов/авторских прав.
- Litecoin. Считается производной от биткоина. Запуск генерации состоялся в 2011 г.
- Dash. Ранее название валюты было Darkcoin. Требуется минимум ресурсов для майнинга.

Остальные цифровые деньги не воспринимаются общественностью, а также часто относят к электронным финансовым пирамидам, способным прекратить существование в любой промежуток времени. Этот риск присущ для всех типов криптовалюты. На практике прекратить свое существование может даже биткоин (пока отсутствует законодательно принятый способ урегулирования подобных ситуаций).

Для всех видов криптовалют применяют открытый алгоритм производства, поэтому подключение к общей сети любой из них является добровольным делом. Передача информации об электронном кошельке совершенно безопасна, никаких персональных данных при этом не разглашается. Отчасти это является тормозом для признания коинов государством, ведь законодательство требует полного контроля над движением денежных средств в стране, а криптовалюта изначально защищена от этого [5].

Когда пользователь начинает разбираться, что такое криптовалюта и как ее использовать, тогда нужно обратить внимание на ряд недостатков в

данной платежной системе. Они являются общими для множества онлайн-ресурсов и просто игнорируются при отсутствии должного внимания к безопасности своего компьютера, смартфона или планшета.

Рекомендуется обратить особое внимание на следующие моменты:

- Сохранность пароля. Опасность исходит как и от его утраты (забыл, не имеешь возможности заменить из-за смены сим-карты или же электронной почты), так и от кражи учетных данных. Второе несет в себе угрозу потерять все средства на электронном кошельке.

- Высокая волатильность. На смене курса криптовалюты можно как заработать, так и получить от этого убытки. Все зависит от колебаний курса после покупки «монет», а также от решения владельца сразу тратить валюту или же стремление создать накопления.

Все криптовалюты подвержены аналогичным рискам, что и онлайн-счета с абсолютно реальными деньгами.

С появлением криптовалюты, появились и новые виды мошенничества. Интернет — это прекрасная возможность для мошенников, в которой даже биржи криптовалют не застрахованы от мошеннических схем.

Разберем основные виды мошенничества с криптовалютой. Так, например:

1. Поддельные веб-сайты

В мире множество мошенников, которым ничего не стоит создать точную копию сайта, на котором вы будете или приобретать криптовалюту или майнить ее. Киберпреступники могут спокойно создать идентичный сайт, но заменив одну букву так, что вы даже не заметите подделки. Перейдя на такие сайты и регистрируя свои данные, вы спокойно передадите их в руки мошенникам, которые потом будут спокойно располагаться ими.

2. Поддельные мобильные приложения

Еще одним распространённым видом мошенничества являются поддельные мобильные приложения, на которые чаще всего попадают пользователи. Такие приложения в свободном доступе размещаются на платформах Google Play и Apple App Store. Да, такие приложения быстро распознаются или совсем не проходят проверку, но если же сервер пропустил приложение, то на эту уловку достаточно легко попасться.

3. Социальные сети

Социальные сети-самая легкодоступная платформа для мошенничества. Создать там страницы не составляет труда, чем и пользуются злоумышленники. Профили популярных блогеров, бизнесменов и других людей, связанных в криптовалютой, могут оказаться фальшивками или ботами. Они могут просить поделиться криптовалютой или помочь майнить. Не видите на эти уловки.

4. Письмо-спам

Мошенники часто обманывают письмами. Так, например, вам может поступить письмо, якобы от реальной компании с идентично выглядящим почтовым ящиком. В письме может быть призыв на первичное размещение уже имеющихся монет или их покупку- с помощью этого способа у вас могут быть украдены как монеты, так и личные денежные средства.[1]

5. Хакерские атаки

С помощью кибератаки, хакеры могут получить доступ к уже известному сайту по криптовалюте, на котором имеются данные пользователей, в ходе чего, доступ к личным данным будет открыт.[2]

Для того чтобы не стать жертвой мошенников, следует всего лишь соблюдать бдительность. Не доверяйте сайтам, которые не являются безопасными по мнению поисковых площадок и в которых вы не уверены ; не передавайте свои личные данные другим лицам или регистрируйтесь на малоизвестных сайтах; не переходите по странным ссылкам и не отвечайте на смс от незнакомцев с просьбами по пересылке криптовалюты или помощи работы с ней.

Поскольку криптовалюта стала «ценной добычей» для хакера, то приведем статистические данные по краже криптовалюты по итогам 2020 года.

Мошенники при помощи скама(обмана) за 2020 год совершили порядка 54% от всех видов криптомошенничества, что в долларовом эквиваленте составляет 2,6 млрд.. Вторым по величине способом стал рынок даркнета, его сумма составляет 1,7 млрд. долл.. Что касаясь программ-вымогателей и краж посредством атак на программы и биржи 350 млн.долл и 20 млрд.долл. соответственно.[6]

Криптовалюта — это сектор, который нуждается в нормативно-правовом регулировании из-за рисков, связанных с неустойчивыми рынками, колебаниями цен и возможностью ее использования для отмывания денег и мошенничества.

Для перевода средств и выполнения платежей платформы криптоактивов полагаются на сложные инфраструктуры и объекты, которые разбросаны по многим странам. Информация о клиенте будет находиться в различных организациях этих разных странах и юрисдикциях. Это открывает возможности для совершения противоправных действий и затрудняет доступ регулирующих органов и любых правоохранительных органов к этой информации.

На законодательном уровне устранить криптомошенничество очень проблематично, из-за специфики работы криптокошельков и децентрализованных сервисов. Также влияет тот факт, что сервисы автономные и это затрудняет отслеживание транзакций, в особенности сомнительные. Единственное, что может совершаться при обнаружении

транзакции с ворованной криптовалютой — это временное закрытие счета. Впрочем даже это достаточно затруднительно, поскольку существуют разнообразные мошеннические способы, которые помогают провести транзакции без угрозы для обнаружения незаконной деятельности.

Одним из радикальных способов считается ввести запрет на инвестирование в криптовалюту и пользование приложениями для ее реализации. Принято, что самым лояльным и правильным способом защиты людей от криптомошенничества является не запрет на деятельность, а наоборот легализация. То есть достаточно начать формировать законодательную базу для контроля и научить криптовалютчиков распознавать мошенников. На данный момент разрабатывается улучшенная версия платформы DeFi, эксперты полагают, что новинка ProFi обязана сотрудничать с регуляторами, так они смогут защитить пользователей. К тому же, лишение регулирования крипторынка причиняет вред самой экосистеме децентрализованных финансов. Большую долю ликвидности составляют «отмытые» деньги, отчего юзеры несут дополнительные убытки или же недополучают прибыль из пула ликвидности.7]

Без нормативно-правового регулирования невозможно будет избавиться от рисков, создаваемых криптовалютой. Это означает, что многие будут обвиняться в использовании этого средства для совершения преступления, а многие другие — страдать от опасности совершения такого преступления. В любой из этих ситуаций невозможно переоценить значение правильного юридического представительства.

Список использованных источников:

1. Распространенные виды мошенничества с криптовалютами URL:<https://www.kaspersky.ru/resource-center/definitions/cryptocurrency-scams> (дата обращения: 18.11.2021).
2. 10 проблем и рисков криптовалют URL:<https://www.garant.ru/article/1150927/>(дата обращения: 18.11.2021).
3. Доступно о том, как работают криптовалюты URL:<https://habr.com/ru/company/jincor/blog/407949/>(дата обращения: 18.11.2021).
4. Все что важно знать о криптовалюте. Словарь терминов URL:<https://www.rbc.ru/crypto/news/5f95b6d79a7947d04d2375e0>(дата обращения: 18.11.2021).
5. Криптовалюта.URL:<https://alpariforex.online/ru/beginner/glossary/cryptocurrency/>(дата обращения: 18.11.2021).
6. Итоги преступлений с криптовалютами в 2020: скам, даркнет и вымогательство URL:<https://hub.forklog.com/itogi-prestuplenij-s-kriptova>

- lyutami-v-2020-skam-darknet-i-vymogatelstvo/(дата обращения:
18.11.2021).
7. Мошеннические схемы с криптовалютой URL:<https://vc.ru/crypto/204779-moshennicheskie-shemy-s-kriptovalyutoy>(дата обращения:
18.11.2021).

Налоговое бремя и его влияние на экономику государства

А.П. Николаева

студент 3 курса НИЯУ МИФИ, Москва

E-mail: nikolaevaanna161084@gmail.com

А.Н. Майорова

к.э.н., доцент кафедры бухгалтерского учета и аудита НИЯУ МИФИ

E-mail: ANMaiorova@mephi.ru

Аннотация: В данной статье рассмотрены основные теоретические положения по теме налогового бремени: его трактования, уровни, направления применения на макроэкономическом и микроэкономическом уровнях. Результаты исследования могут использоваться для более глубокого понимания мероприятий и методов налоговой оптимизации в Российской Федерации, а также основных трендов и тенденций налоговой политики в области налогового бремени в РФ.

Ключевые слова: налоги, налоговое бремя, налоговая нагрузка, налоговая оптимизация.

Tax burden and its impact on the economy of the state

Abstract: This paper examines the main theoretical provisions on the topic of the tax burden: its interpretation, levels, directions of application at the macroeconomic and microeconomic levels. The research results can be used for a deeper understanding of the measures and methods of tax optimization in the Russian Federation, as well as the main trends and tendencies of tax policy in the field of the tax burden in the Russian Federation.

Keywords: taxes, tax burden, tax load, tax optimization.

Налоговое бремя – это тот аспект экономической, финансовой, налоговой систем, который влияет коренным образом на экономические процессы как на макроуровне, так и на микроуровне. Сегодня мы наблюдаем весьма значимые успехи в трансформировании системы налогообложения в разных странах мира, но это не отменяет необходимости системно и постоянно задумываться о стратегии, будущих действиях законодательных и исполнительных органах государственной власти, а также более совершенной концепции процесса взимания налогов.

Цель данного исследования заключается в том, чтобы выявить и описать основные направления налоговой политики в области налогового бремени, в частности Министерства финансов Российской Федерации. Также считаю важным затронуть темы налоговой оптимизации на уровне юридического лица, описать ее задачи, цели, методы и основные мероприятия. Для этого будут даны описания основных направлений применения показателя налогового бремени, его экономической сущности, уровней налоговой нагрузки.

Разберемся с терминологией затронутой в этом исследовании темы. Термин «налоговое бремя» имеет большое множество различных определений от разных источников, авторов, словарей и др.

Например, современный экономический словарь дает такое описание: «Налоговое бремя – это мера, степень, уровень экономических ограничений, создаваемых отчислением средств на уплату налогов, отвлечением их от других возможных направлений использования».

А.В. Брызгалин, автор более 180 научных работ по экономике, в частности по вопросам налогообложения и роли государства в процессе деятельности хозяйствующих субъектов, в своей работе «Налоговая оптимизация» отмечает, что «налоговое бремя (или налоговый гнет иными словами) - - это обобщающий показатель, характеризующий роль налогов в жизни общества и определяемый как отношение общей суммы налоговых сборов к совокупному национальному продукту» [5, с 272].

Налоговое бремя возникает в связи с наличием двух ключевых компонентов: наличия объекта налогообложения и обязанности по уплате налога. До тех пор, пока существуют обстоятельства, которые вынуждают производить уплату налога, налоговое бремя существует и не исчезает. Особенность процесса заключается в том, что мы рассматриваем целую совокупность обязанностей, так как субъект налога (налогоплательщик) уплачивает сразу несколько различных налогов.

Таким образом, понятие «налоговое бремя» имеет множество разных оттенков значений и является комплексным системным явлением, имеющее место в любом государстве, например, в виде регулятора экономики и фискальной (бюджетно-налоговой) политики.

Экономическая сущность налогового бремени выражается в том, что оно выражается не только суммой уплаченных в бюджет разных уровней налогов, но и иных затрат, связанных с необходимостью выполнения обязанности правильно, в срок и в полном объеме уплачивать установленные законом налоги. Например, затраты, связанные с изучением налогового законодательства, с уплатой пени и штрафных санкций за несвоевременную уплату налога или из-за нарушения налогового законодательства, а также затраты на содержание штата специалистов по

вопросам обжалования действий налоговых органов, правильности начисления данных обязательных платежей. Еще в экономическую сущность налогов стоит включить факт мобилизации денежных средств на момент уплаты налогов, требующий уплаты процентов за кредит или заем.

Учитывая данные последних исследований и собственные наблюдения, можно рассмотреть налоговую нагрузку с точки зрения пяти уровней.

1) Уровень государства в целом или его субъектов, регионов. На нем государственные органы принимают решения о проведении налоговых реформ, как правило основываясь на данных сравнительного анализа налоговой нагрузки в других странах со схожей системой налогообложения.

2) Уровень конкретных отраслей хозяйства страны или ее регионов. Государство может вводить меры поддержки для ключевых отраслей своей национальной экономики, а также для тех отраслей, которым необходимы дополнительные льготы в кризисный период.

3) Уровень группы сходных предприятий.

4) Уровень отдельных хозяйствующих субъектов.

5) Уровень конкретного человека.

«Эти уровни можно объединить в две группы: налоговое бремя на макроуровне (общегосударственный и территориальный уровни) и на микроуровне (уровне субъекта)» [6, с. 48]

Проведя анализ деятельности налогового механизма, были выявлены главные векторы развития, связанные с налоговой нагрузкой:

1) Формирование налоговой политики.

2) Сопоставление налоговой нагрузки в разных отраслях экономики, а также на различных масштабах (федеральном, региональном и местном).

3) Планирование, реализация и анализ результатов проведенной социальной политики.

4) Показатель экономической активности хозяйствующих субъектов.

То, насколько большой процент всех доходов физическое или юридическое лицо обязано отчуждать в качестве обязательных безвозмездных платежей в государственный бюджет, то есть налогов, является очень значимой информацией прежде всего для Министерства финансов РФ, Федеральной налоговой службы РФ, а также для иных органов, связанных с финансовой и налоговой деятельностью хозяйствующих субъектов РФ и налоговых резидентов РФ.

Министерство финансов Российской Федерации занимается анализом, планированием и прогнозированием экономических ситуаций, процессов в стране и ее регионах. Это позволяет оперативно и своевременно реагировать на новые вызовы и решать существующие проблемы. Федеральная налоговая служба Российской Федерации проводит выездные и камеральные налоговые проверки, а также совместно с Министерством

финансов РФ осуществляет деятельность по совершенствованию системы налогового контроля. В свою очередь налогоплательщик может заниматься анализом текущей и перспективной деятельности, оценкой рисков проведения налоговых проверок с учетом новых нормальных правовых актов в сфере налогообложения и возможных методах оптимизации налогового бремени.

Перспективные направления оптимизации налогового бремени для хозяйствующих субъектов на 2021-2022 гг. можно условно разделить на мероприятия и методы. В качестве мероприятий для оптимизации налогового бремени можно предложить следующие: подбор методов оптимизации налогов для конкретного бизнеса компетентными специалистами самой организацией или через аутсорсинг, налоговое планирование, управление рисками (риск-менеджмент) и другие. К методам оптимизации налоговой нагрузки относятся дробление бизнеса, использование договорных отношений, возможных налоговых льгот, перечень которых указан в Налоговом кодексе РФ, освобождений от уплаты конкретных налогов (по НК РФ), метод отсрочки налогового платежа и иные.

Уровень налоговой нагрузки с 2007 г. является одним из показателей для контроля ФНС России за поступлениями в бюджет. Дело в том, что налоговая нагрузка может свидетельствовать об уклонении от уплаты налогов, а это имеет важное значение для определения вероятности назначения налоговой проверки и создает ситуацию недополучения денежных средств в федеральный, региональный и местный бюджеты. Такова позиция налоговых органов на текущий момент. При детальном изучении структуры налоговых поступлений в консолидированные бюджеты субъектов Российской Федерации можно заметить ярко выраженную большую долю налога на доходы физических лиц (НДФЛ), на втором месте по объему доходных статей бюджета находится налог на прибыль организаций. Еще можно отметить значимую для консолидированных бюджетов субъектов РФ долю налогов на имущество (на которые приходится 11,3% всех поступлений по результатам 2018 г.).

Выездная налоговая проверка как инструмент контроля налоговых поступлений может быть назначена в том случае, если уровень налоговой нагрузки у конкретного налогоплательщика ниже его среднего уровня по определенной отрасли (то есть по виду экономической деятельности).

Безопасные значения налоговой нагрузки в 2021 году по итогам 2020 года установлены Приказом ФНС России от 30.05.2007 N ММ-3-06/333@ "Об утверждении Концепции системы планирования выездных налоговых проверок".

Сегодня, в эпоху цифровизации, компьютеризации, глобализации как мировой экономической системы, так и региональных отраслей постоянно возникают различные конкретные задачи, цели, формирующие более значимые задачи по основным векторам развития налоговой политики, которые требуют рассмотрения и работы над ними уже в текущем периоде. Поэтому Министерство финансов ставит следующие центральные направления развития на 2021 и плановый 2022 и 2023 годы:

1. Борьба с пандемией коронавирусной инфекции (Covid-19) и содействие восстановлению экономики в целом, отдельным отраслям хозяйства и конкретным домохозяйствам.
2. Развитие межбюджетных отношений.
3. Повышение операционной эффективности использования бюджетных средств и усиление контроля за их расходованием.
4. Структурная трансформация налоговых отношений как области экономической деятельности в РФ.

Список использованных источников:

1. Налоговый кодекс Российской Федерации (НК РФ)
2. Приказ ФНС России от 30.05.2007 N ММ-3-06/333@ (ред. от 10.05.2012) "Об утверждении Концепции системы планирования выездных налоговых проверок"
3. Барташевич, С.В. Налоговое бремя как правовая категория [Текст] / С.В. Барташевич // Налоги и налогообложение. 2019, № 6.
4. Барулин, С.В. Налоговый менеджмент [Текст] учебное пособие / С.В. Барулин. – М.: Омега-Л, 2018.
5. Брызгалин, А.В. Налоговая оптимизация [Текст] / А.В. Брызгалин. – М.: Налоги, 2018.
6. Катушина, М. В. Методы расчета налоговой нагрузки [Текст] / М.В. Катушина // Студенческий научный форум - 2018. - №10.
7. Корнийчук, Д.В. Налоговая нагрузка предприятия и способы ее оптимизации [Текст] / Д.В. Корнийчук // Молодой ученый. - 2018. - №15.
8. Пелькова, С.В. Анализ методик расчета налоговой нагрузки организации [Текст] / С. В. Пелькова // Современная налоговая система: состояние, проблемы и перспективы развития: межвузовский сб. науч. тр. с междунар. участием. / М. К. Аристархова. - Вып.3.– Уфа: УГАТУ, 2018
9. Пименов, Н. А. Управление финансовыми рисками в системе экономической безопасности [Текст] учебник и практикум для академического бакалавриата / Н. А. Пименов. — М.: Юрайт, 2019.
10. <https://rosstat.gov.ru/folder/11192> (14.09.2021)

Новые способы отмывания денег в сфере медицины в период COVID-19

Д.Ю. Елкина

студент 1 курса НИЯУ МИФИ, Москва

E-mail: dasha-15.15@yandex.ru

Д.С. Павлов

студент 2 курса НИЯУ МИФИ, Москва

E-mail: denpav98@yandex.ru

Аннотация: В статье анализируется ситуация, связанная с отмыванием денег в сфере медицины, как наиболее уязвимая в период пандемии COVID-19. На основе изучения международных отчетов, научных статей и СМИ, авторами выделяются основные угрозы, рассматриваются схемы мошенничества в данной области, а также предлагаются пути решения.

Ключевые слова: отмывание денег, COVID-19, пандемия, мошенничество, медицина, финансовая уязвимость.

New ways of money laundering in the medical field during COVID-19

Abstract: The article analyzes the situation related to money laundering in the field of medicine, as the most vulnerable in the current COVID-19 pandemic. On the basis of international reports, scientific articles and the media, the authors highlight the main threats, consider fraud schemes in this area, and also propose solutions.

Keywords: money laundering, COVID-19, pandemic, fraud, medicine, financial vulnerability.

Отмывание денег определяется как процесс сознательного преобразования или передачи такого имущества, которое является доходом от преступлений, с целью его сокрытия или сокрытия его незаконного происхождения [1]. Хотя пандемия COVID-19 остановила мир, она одновременно расширила возможности криминальной экономики.

Другими словами, пандемия COVID-19 привела к определенным беспрецедентным обстоятельствам, таким как рост удаленной работы и онлайн-транзакций, которые могут выявить или еще больше усугубить

финансовую уязвимость. Поэтому, чтобы понять потенциальное влияние этих угроз, финансовые учреждения и организации по всему миру проводят исследования в областях, подверженных риску отмыwania денег вследствие COVID-19. В данной статье проводится анализ основных тенденций в области противодействия отмыwania денег.

Для начала стоит отметить, что в сентябре 2020 года MONEYVAL [2] показал, что «многие страны сообщили о резком росте числа определенных преступлений, особенно с транснациональными элементами, такими как мошенничество (с использованием электронных средств) и киберпреступность, создающих новые источники доходов для целей отмыwania денег» [3]. Комитет определил пять основных категорий потенциальных угроз отмыwania денег:

- мошенничество;
- медицинские преступления;
- коррупция;
- киберпреступления;
- несвоевременный спрос на перевозку незаконных товаров [3].

В рамках более широкой категории мошенничества как угрозы отмыwania денег были выделены различные подкатегории мошенничества, связанного с COVID-19. Особое внимание стоит уделить следующему факту, что пандемия привела к значительному спросу на медицинское оборудование и материалы, а это, в свою очередь, привело к завышению цен и низкому качеству товаров. В СМИ отмечалось, что за последние два года наблюдался рост преступлений в сфере медицины более чем в 4 раза в среднем по всему миру. Как следствие, медицинские преступления являются одними из ключевых в ходе распространения пандемии, а схемы, используемые преступниками, требуют тщательного анализа.

Анализ официальных отчетов и СМИ показал, что ПФР по всему миру сообщили об умеренном увеличении количества инцидентов, потенциально связанных с поставками небезопасных и/или ненадежных импортных товаров, удвоенных поддельными или отсутствующими сертификатами соответствия товаров медицинского назначения.

В свою очередь, ФАТФ выделила подделку медицинских товаров, таких как лекарства и средства индивидуальной защиты, как серьезную форму мошенничества с медицинским оборудованием [4]. Также было отмечено увеличение случаев мошенничества с доставкой, когда недобросовестные агенты требовали предоплату за доставку медицинских товаров, но, получив предоплату, не доставляли товар. Более того, были сообщения о мошеннической рекламе компаний, разрабатывающих «чудодейственные лекарства» от COVID-19, и обещающих огромную прибыль от любых вложений [5].

Отметим, что факты мошенничества, связанные с медицинским оборудованием, прослеживались в сфере государственных закупок. Так, по сообщению одной юрисдикции, организованные преступные группы продавали «гарантии» (вид финансового инструмента), необходимые для участия в государственных тендерах. Стоимость таких поддельных документов оставалась низкой, и, как правило, требовалась предоплата наличными средствами. Всем известно, если гарантированное юридическое лицо становится неплатежеспособным или не выполняет свои обязательства (гарантии не выполняются), то это приводит к потере государственных средств.

Данную ситуацию можно проиллюстрировать следующим примером.

Представим, что в ответ на пандемию COVID-19 страна А решила снизить нормативные требования в сфере государственных закупок, т. е. постановление предусматривает, что определенным государственным объектам (например, стационарным лечебным учреждениям) разрешено не применять государственные требования в данной сфере при закупке товаров и услуг, необходимых для борьбы с COVID-19.

В результате хирургические маски и респираторы были закуплены в Восточной Азии в рамках упрощенных процедур государственных закупок. Когда была получена первая поставка товаров, сертификаты, приложенные к контракту, были признаны несуществующими, недействительными или поддельными, а лаборатория, которая их выдала, не была включена в официальный список аккредитованных лабораторий по испытанию масок в экспортной юрисдикции.

Как следствие, данная продукция не может быть использована в качестве средств индивидуальной защиты, а государство теряет свои средства.

Основной причиной, которая может вызвать приведенную выше ситуацию, является стремление государства создать условия для борьбы с пандемией. Упрощение доступа к медицинским препаратам и оборудованию, популяризация веб-приложений, программы медицинского страхования создают дополнительные возможности для отмывания денег.

В подтверждении данного факта рассмотрим следующую ситуацию. В середине 2020 года двое граждан США были привлечены к ответственности по одному пункту обвинения в сговоре с целью совершения мошенничества в сфере здравоохранения и мошенничества с использованием электронных средств, а также по одному пункту обвинения в сговоре с целью отмывания денег. Обвиняемые использовали коды экстренной помощи и правки в системе Medicare (национальная программа медицинского страхования США), которые вступили в силу должным образом в связи с пандемией COVID-19, чтобы подать претензии

в отношении дорогостоящих онкологических препаратов, которые никогда не предоставлялись, не заказывались и не разрешались медицинскими работниками. Эти действия проводились в периоды, когда аптеки не работали и указанные ранее лица могли использовать имена врачей в рецептах без их разрешения.

Мошенники приобрели контроль над десятками аптек Нью-Йорка, заплатив другим за то, чтобы они выдавали себя за владельцев аптек, и, наняв фармацевтов, которые притворялись надзирающими за фармацевтами в аптеках, с целью получения аптечных лицензий и подтверждения страхового плана. Обвиняемые использовали пандемию COVID-19 как возможность извлечь выгоду из чрезвычайной ситуации с помощью выставления счетов для подачи мошеннических претензий в отношении Targetin Gel 1%, средняя оптовая цена которого составляет приблизительно 34 000 долларов США за каждую 60-граммовую тубу.

Рассмотрим действия мошенников поэтапно. На подготовительном этапе обвиняемые граждане создали фиктивные оптовые компании аптек, названные ими в честь ранее существовавших оптовых продавцов аптек, и сфабриковали счета, чтобы создать впечатление, что переводимые средства из аптек в фиктивные оптовые компании предназначались для законных закупок фармацевтических препаратов.

На первом этапе обвиняемые вступили в сговор с международным агентом по отмыванию денег, который организовал перевод денежных средств от фиктивных оптовых аптек компаниям в Китае для распределения среди физических лиц в Узбекистане. В обмен на это обвиняемые получили денежные средства, предоставленные членами иммигрантской общины Узбекистана нелегализованному бизнесу по переводу денег их родственникам, за вычетом комиссии.

На втором этапе заговора по отмыванию денег, когда сумма мошеннических доходов превышала сумму наличных денег, имеющихся в узбекском иммигрантском сообществе, ответчики приказали международному агенту перевести средства обратно от фиктивных оптовых компаний к ответчикам, их родственникам. Вырученные от схемы средства ответчики использовали для покупки недвижимости и других предметов роскоши. В результате им удалось легализовать около 30 миллионов долларов США.

Начиная с 2019 года, национальная страховая компания Medicare потеряла более 19 миллиардов долларов США за счет действий мошенников по аналогичным схемам.

Данная мошенническая схема, а также приведенные ранее способы отмывания денег через медицинскую сферу, создают реальную угрозу международному сообществу в период COVID-19. В связи с этим, на

основе изученных документов, можно обозначить следующие рекомендации. Во-первых, чтобы предотвратить подобные прецеденты, сократить рост активности по отмыванию денег после COVID-19 и справиться с изменившимся финансовым ландшафтом, правительственные и финансовые учреждения, банки и поставщики услуг должны разработать гибкие механизмы, которые должны развиваться с изменяющимися угрозами, чтобы преступники не могли использовать так называемые уязвимые места, на которые не обращают внимания учреждения [5].

Во-вторых, ФАТФ рекомендует уделять приоритетное внимание точным механизмам распознавания личности и повышению качества онлайн-услуг для защиты менее опытных пользователей. Компании также должны быть оснащены для оценки программ оперативного контроля и управления рисками в связи с постоянно развивающимися и быстрорастущими новыми угрозами.

Также важно повышать осведомленность общественности об этих угрозах, поскольку преступники, в основном, преследовали невинных людей и использовали коллективные беды, вызванные пандемией.

Таким образом, преступления в сфере отмывания денег в медицине являются одними из ключевых в современных реалиях, постоянный мониторинг и анализ схем преступников, а также соблюдение рекомендаций международных организаций поможет государствам минимизировать угрозы, вызванные текущей ситуацией.

Список использованных источников:

1. Конвенция Организации Объединенных Наций против транснациональной организованной преступности. URL: https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml (дата обращения 12.10.2021).
2. Комитет экспертов по оценке мер по борьбе с отмыванием денег и финансированием терроризма (Совет Европы). URL: <https://www.fedsfm.ru/activity/moneyval> (дата обращения 22.10.2021).
3. МАНИВЭЛ, «Тенденции отмывания денег и финансирования терроризма в юрисдикциях МАНИВЭЛ во время кризиса COVID-19» (Совет Европы, 2 сентября 2020 г.) URL: <https://rm.coe.int/moneyval-2020-18rev-covid19/16809f66c3> (дата обращения 10.11.2021).
4. Заявление президента ФАТФ: COVID-19 и меры по борьбе с незаконными финансовыми операциями. URL: <https://www.fedsfm.ru/covid19/4489> (дата обращения 10.11.2021).
5. ФАТФ Обновление: Отмывание денег и финансирование терроризма, связанные с пандемией COVID-19 Риски и политические меры реагирования (Декабрь 2020). URL:

https://eurasiangroup.org/files/uploads/files/%D0%9C%D0%B5%D1%80%D1%8B_%D0%B2_%D1%81%D0%B2%D1%8F%D0%B7%D0%B8_%D1%81_COVID-19/Update-COVID19Related%20Money%20Laundering%20and%20Terrorist%20Financing%20Risks_rus_1.pdf (дата обращения 11.11.2021).

6. Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 N 115-ФЗ.
7. ФАТФ Отмывание денег и финансирование терроризма, связанные с пандемией COVID-19 Риски и политические меры реагирования (Май 2020). URL: https://nbt.tj/files/monitoring/fatf_recomendations/2020/informacionnyj-bulleten-otmyvanie-deneg-i-finansirovanie-terrorizma-svazannye-s-pandemiej-covid-19-maj-2020%20-2.pdf (дата обращения 11.11.2021).
8. Financier Worldwide, «COVID-19: переосмысление борьбы с отмыванием денег (AML) и управления рисками мошенничества» (май 2021 г.) URL: <https://www.financierworldwide.com/covid-19-rethinking-anti-money-laundering-aml-and-fraud-risk-management#.YKtlgZMzZAd> (дата обращения 11.11.2021).

О специфических особенностях государственного финансового контроля в условиях пандемии COVID-19

А.Е. Сорокин

студент 2 курса магистратуры ФГАОУ ВО
«Севастопольский государственный университет»,

Юридический институт

E-mail: zlexz@mail.ru

А.С. Кропачева

студент 2 курса магистратуры ФГАОУ ВО
«Севастопольский государственный университет»,

Юридический институт

научный руководитель: Е.В. Скребец

д.полит.н., доцент, зав. кафедрой «Гражданское право и процесс»

ФГАОУ ВО «Севастопольский государственный университет»

E-mail: evskrebets@sevsu.ru

Аннотация: В условиях пандемии COVID-19 изменились приоритеты и способы государственного контроля. Ограничены непосредственные контакты сотрудников контрольно-надзорных органов и контролируемых лиц. Надзорная деятельность строится на основе риск-ориентированного подхода. В план проверок попадают только субъекты с высоким уровнем риска незаконопослушности. Актуальной задачей является предотвращение киберпреступлений.

Ключевые слова: экономические преступления, антикризисные меры, риск-ориентированный подход, риск незаконопослушности, надзорное сопровождение, мошенничество, киберпреступность.

On the specific features of state financial control in the context of the COVID-19 pandemic

Abstract: In the context of the COVID-19 pandemic, priorities and methods of state control have changed. Direct contacts of employees of Effective Environmental Enforcement Authorities and controlled persons are limited. The supervisory activity is based on a risk-based approach. Only subjects with a high risk of lawlessness are included in the inspection plan. An urgent modern task is to prevent not only financial offenses, but also cybercrimes.

Keywords: economic crimes, anti-crisis measures, risk-oriented approach, risk of lawlessness, supervisory support, fraud, cybercrime.

Пандемия COVID-19 не только нанесла тяжелейший удар мировой экономике, но и бросила серьезный вызов национальным системам государственного финансового надзора. В Российской Федерации количество преступлений экономической направленности за семь месяцев 2021 года выросло почти на 10% по сравнению с тем же периодом 2020 года, следует из данных МВД России. Так, с января по июль прошлого года было зафиксировано 71 384 преступления, связанных с экономической деятельностью, а за то же время в 2021 году — уже 78 290 преступлений. По подсчетам Генпрокуратуры, за январь-июнь 2021-го ущерб от экономических преступлений превысил 142 млрд рублей [1]. В соответствии с УК РФ к преступлениям экономической направленности относятся незаконная банковская деятельность, лжепредпринимательство, легализация (отмывание) денежных средств или иного нелегального имущества, незаконное получение кредита, злостное уклонение от погашения кредиторской задолженности, преднамеренное банкротство, коммерческий подкуп, уклонение от уплаты налогов, контрабанда и ряд других деяний [2]. Помимо экономических, растет число киберпреступлений и увеличивается число случаев коррупции. Мошенники совершенствуют механизмы отъема денег у людей и государства, и задача органов финансового контроля — не просто остановить рост экономической преступности, но и минимизировать причиняемый преступниками денежный ущерб.

Пандемия началась внезапно, и а перед аппаратом государственной власти встал ряд проблем, требующих оперативного решения. С одной стороны, встали новые финансовые задачи и сместились приоритеты финансирования, с другой — эффективно применявшиеся ранее способы государственного контроля (например, выездные проверки), стали недоступными. Пошатнулся малый и средний бизнес, и стало ясно, что без поддержки государства этот сектор совершит откат назад в своем развитии.

С началом эпидемии был разработан комплекс антикризисных мер, предназначенных для поддержки бизнеса и некоммерческих организаций:

- Принято Постановление Правительства РФ № 438 от 3 апреля 2020 года «Об особенностях осуществления в 2020 году государственного контроля (надзора), муниципального контроля и о внесении изменения в пункт 7 Правил подготовки органами государственного контроля (надзора) и органами муниципального контроля ежегодных планов проведения плановых проверок юридических лиц и индивидуальных предпринимателей" с последующими изменениями.

– Начали действовать рекомендации, обозначенные в ФЗ от 21 декабря 1994 г. № 68-ФЗ.

– Вступили в силу требования ФЗ от 30 марта 1999 г. № 52-ФЗ.

Карантин 2020 года поставил задачу – ограничить непосредственные контакты сотрудников контрольно-надзорных органов и контролируемых лиц. Никогда ранее социальное дистанцирование не применялось в таких масштабах. Правительство ввело ограничения на проверки надзорных органов, таких как: Ростехнадзор, Инспекция труда, Пожарная инспекция, Роскомнадзор, Счетная палата, Таможенная служба, Налоговая служба, Росприроднадзор, во исполнение постановления Правительства Российской Федерации от 3 апреля 2020 г. № 438. Росфинмониторингом было отменено проведение проверок соблюдения требований законодательства в сфере ПОД/ФТ поднадзорными организациями, за исключением отдельных случаев. Цель данного документа – снизить административную нагрузку на хозяйствующие субъекты. И тут возникает некая дилемма: с одной стороны, налицо два явных «плюса»: частично снижено административное давление на субъекты предпринимательства, а также предприняты меры противодействия распространению COVID-19. Но в то же время никто не отменял обязанности поднадзорных субъектов соблюдать требования законодательства о ПОД/ФТ, а в условиях последовавшего за началом пандемии экономического кризиса контроль денежных потоков в указанной сфере стал еще более значимым. Главным инструментом финансового надзора стал Личный кабинет. Через него Служба продолжила осуществлять дистанционный мониторинг деятельности поднадзорных организаций на предмет соблюдения требований 115-ФЗ и оценку рисков незаконопослушности. Можно констатировать, что надзорная деятельность оказалась эффективной. Основываясь на статистических данных контрольно-надзорной деятельности МРУ Росфинмониторинга по Крыму и Севастополю по итогам прошедшего года наблюдалась положительная динамика законопослушности поднадзорных субъектов. На начало 2020 года процент законопослушных субъектов составлял 84%, а по состоянию на начало 2021 года данный показатель превысил 90%.

В Российской Федерации в 2020-2021 гг. применялись беспрецедентные меры государственной поддержки бизнеса и граждан в период пандемии. Так называемый «локдаун» существенно сократил уровень доходов как предпринимателей, так и наемных работников, что, безусловно, повлияло на уровень совокупного предложения. К мерам поддержки организаций и индивидуальных предпринимателей можно отнести продление сроков сдачи отчетности и уплаты ряда платежей в 2020 году, мораторий на проверки, беспроцентные кредиты на выплату зарплаты, мораторий на

возбуждение дел о банкротстве, кредитные каникулы, упрощенную процедуру госзакупок, а для граждан – многочисленные социальные выплаты разным категориям населения, изменение порядка оформления и оплаты листков нетрудоспособности и т.п. [3]. На данном этапе усилия государства сосредоточены, с одной стороны, на том, чтобы направить больше ресурсов в систему здравоохранения и медицинскую промышленность, а с другой - на поддержке совокупного предложения, сохранении трудового и производственного потенциала, стимулировании спроса. Следует отметить, что при увеличении общих расходов федерального бюджета в Российской Федерации не были сокращены инвестиционные планы. В этих условиях расход каждого бюджетного рубля, связанного с реализацией национальных проектов, находится на жестком контроле. По словам генерального прокурора России И.Краснова, "за девять месяцев текущего года в этой сфере прокурорами выявлено более 45 тыс. нарушений законов. Две основные беды - несвоевременное доведение до получателей бюджетных средств и их незаконное расходование. По результатам надзорных проверок к административной и дисциплинарной ответственности привлечено свыше 12 тыс. лиц, инициировано возбуждение 495 уголовных дел» [4]. Также генеральный прокурор отметил, что при надзорном сопровождении реализации национальных проектов «налажен непрерывный обмен информацией с федеральным казначейством, Счетной палатой и Росфинмониторингом».

Если говорить о коррупционных правонарушениях в условиях пандемии, нельзя не заметить появление нового вида преступления – продажу «липовых» сертификатов о вакцинации против коронавируса, но пока эта тема требует более глубокого и детального изучения и выходит за рамки данного исследования.

Не менее серьезной проблемой контрольно-надзорных органов является противодействие преступдениям в цифровой среде. Перемещение преступников с улиц за компьютерные мониторы – тренд последних двух-трех лет, главной предпосылкой которого является цифровизация (диджитализация) всех сфер жизни. По данным McKinsey Global Institute общий рост бизнеса, обусловленный цифровой трансформацией, может составлять более \$13 трлн. Мировые расходы компаний на цифровую трансформацию продолжают расти в среднем на 16–18% в год. По итогам 2017 года их объем превысил \$1,3 трлн, а к 2021 году увеличился до \$2,1 трлн.[5]. Еще до COVID-2019 контрольно-надзорные органы готовились к цифровой трансформации, но именно пандемия подтолкнула их к массовой цифровизации процессов сбора и анализа данных. Так, для автоматизации контрольно-надзорной деятельности разработали высокотехнологичные виртуальные сервисы, к которым можно отнести:

1. Государственную информационную систему «Типовое облачное решение по автоматизации контрольной (надзорной) деятельности».

2. Государственную информационную платформу, предназначенную для контроля оборота драгоценных металлов, камней и изделий из них (ГИИС ДМДК).

3. Цифровой сервис для обработки жалоб предпринимателей на незаконные действия правоохранительных органов.

Более 50 онлайн-сервисов предлагает Федеральная налоговая служба. Мониторинг-контроль в сфере противодействия отмыванию доходов и финансированию терроризма осуществляется через Личный кабинет на официальном сайте Росфинмониторинга, использование которого дает возможность получить доступ ко всему спектру информации, отражающей ключевые индикаторы взаимодействия со службой.

Цифровизация не только дает новые возможности, но и генерирует новые риски: ее обратной стороной является увеличение количества киберпреступлений.

Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства. К киберпреступлениям, например, можно отнести кражу финансовых данных или данных банковских карт, мошенничество с электронной почтой, кибершантаж, интернет-мошенничество, использование сайтов-двойников, мошенничество с использованием личных данных, кражу и продажу корпоративных данных, криптоджекинг, кибершпионаж.

Основная причина роста количества киберпреступлений в условиях пандемии - перевод персонала на удаленную работу и вход в корпоративные сети компаний из дома. Корпорации тратят огромные ресурсы на защиту финансово-экономической информации, контролируют информационные потоки. А домашние маршрутизаторы обычно плохо защищены, пароли на домашних ПК слабые, системы часто заражены вирусами. Так и создаются благоприятные условия для информационных утечек. Первоначальным вектором заражения чаще всего является электронная почта, подверженная массированным фишинговым атакам.

Наиболее привлекательным для киберпреступников является финансовый сектор. О росте числа киберпреступлений свидетельствует статистика МВД. Так, в январе-июне 2021 года IT-преступлений было совершено на 20,3% больше, чем в аналогичный период прошлого года [1]. По словам Г.Грефа, к 2030 году убытки от кибератак могут достигнуть 30 триллионов долларов, и сейчас фактор хакерского взлома находится на девятом месте среди вероятных мощнейших потрясений для мира. К примеру, в России в 2020 году из-за атак потеряно уже 3,5 триллиона

рублей. При этом 90 процентов успешных атак осуществляется с помощью метода социальной инженерии [7].

С одной стороны, кибератаки не только наносят экономический ущерб, но и, в целом, снижают уровень доверия к сети Интернет. С другой стороны, вызовы, брошенные киберпреступниками, стимулируют развитие системы методов и технологий противодействия киберпреступности. Создаются новые антивирусные программы, развивается социальная реклама, расширяется образовательная деятельность в сфере финансовой грамотности и финансовой безопасности.

Сфера преступлений становится интеллектуальной, снижается количество злодеяний, связанных с физическим насилием. Этот факт, который можно считать условно-положительным, безусловно, является особенностью периода пандемии.

Поскольку COVID-19 и угрозы киберпреступности, связанные с этим кризисом, являются глобальными, ответные меры также должны быть глобальными: решить данную проблему в одиночку ни одному государству не под силу. В связи с этим тревогу вызывает тот факт, что в настоящее время с некоторыми государствами все еще осложнена коммуникация по раскрытию электронных адресов киберпреступников. В качестве примера можно привести расследование хакерских атак на сайт Бессмертного полка – это преступление хоть и не является экономическим, красноречиво отражает интернациональный характер преступной деятельности и недостаточный уровень межстранового взаимодействия. Сотрудничество же в сфере противодействия киберпреступности может осуществляться посредством обмена информацией, передовыми практиками, учениями на государственном и межгосударственном уровне.

Список использованных источников:

1. Кулакова В. Диффузия обмана: экономических преступлений стало больше на 10%. Почему на улице стали грабить меньше, а в интернете — больше — <https://iz.ru/1209294/veronika-kulakova/diffuziia-obmana-ekonomicheskikh-prestuplenii-stalo-bolshe-na-10> .
2. Перечень N 2 преступлений экономической направленности по уголовным делам, предварительное расследование по которым производится в форме предварительного следствия - <https://sudact.ru/law/ukazanie-genprokuratury-rossii-n-48711-mvd-rossii/prilozhenie/perechen-n-2-prestuplenii-ekonomicheskoi/>
3. Меры государственной поддержки бизнеса и граждан в период пандемии (подготовлено экспертами компании "Гарант") - <https://base.garant.ru/77398919/> .

4. В 2021 году при реализации нацпроектов выявили более 45 тыс. нарушений закона. - <https://www.fedsfm.ru/mediaaboutus/5427>
5. Что нужно знать о цифровизации промышленности. - https://www.cnews.ru/articles/cto_nuzhno_znat_o_tsifrovizatsii_promyshlennosti
6. «Один неверный клик может изменить все» Пандемия коронавируса сделала хакеров опаснее и быстрее. Как им противостоять? - https://lenta.ru/articles/2020/07/09/cyber_trends/

Обеспечение безопасности банкоматов в условиях цифровизации

Т.И. Карабчук
студентка 1 курса магистратуры
ФГАОУ ВО «КФУ им. В. И. Вернадского», г. Симферополь
E-mail: tanya_karabchuk@mail.ua
научный руководитель: О.Г. Блажевич
к.э.н., доцент кафедры финансов и кредита
ФГАОУ ВО «КФУ им. В. И. Вернадского», г. Симферополь
E-mail: blolge@rambler.ru

Аннотация: Преступность, связанная с банкоматами, продолжает расти и распространяться по всему миру, несмотря на региональные различия в частоте совершения преступлений. Поэтому в статье рассмотрены традиционные и новые преступления, связанные с банкоматами, а также разработаны рекомендации обеспечению безопасности банкоматов.

Ключевые слова: банкомат, мошенничество, безопасность, скимминг.

Ensuring ATM security in the context of digitalization

Abstract: ATM-related crime continues to grow and spread around the world, despite regional differences in the frequency of crimes. Therefore, the article discusses traditional and new crimes related to ATMs, as well as recommendations for ensuring the security of ATMs.

Keywords: ATM, fraud, security, skimming.

Мошенничество с банкоматами стало глобальной проблемой, с которой сталкиваются не только клиенты, но и банковские операторы. Методы мошенничества, используемые киберпреступниками, стали более совершенными, и управление рисками, связанными с мошенничеством в банкоматах, является важной проблемой, с которой сталкиваются финансовые учреждения по всему миру. С появлением новых атак на банкоматы перед владельцами банкоматов стоит задача обеспечить их кибер-готовность к этим новым угрозам.

Угрозы/атаки банкоматов можно разделить на физические и логические атаки. Физические атаки включают в себя физическое нападение на банкомат, киберпреступники используют такие методы, как твердые и

газовые взрывчатые вещества. Другие физические атаки включают размещение гаджетов в банкомате киберпреступниками, которые копируют данные карты банкомата и воспроизводят их на другой карте, которую можно использовать для снятия денег со счета владельца карты. Логические атаки включают использование вредоносных программ для указания банкомату выдавать деньги. Такие атаки могут быть осуществлены путем получения физического доступа к банкомату для установки этой вредоносной программы на ядро ПК банкомата, либо вредоносная программа может быть внедрена через сеть [5]. Рассмотрим распространённые виды атак на банкоматы:

1. Скимминг банковских карт.

Атака на скимминг банковских карт — это физическая угроза, которая в прошлом была угрозой номер один для банкоматов во всем мире. Скимминг банкоматов относится к краже данных электронной карты, помогая преступнику подделать карту. Скиммер — это устройство, установленное на считывателе карт, заставляющее клиента поверить, что он вставляет свою карту в считыватель карт банкомата. Скиммер считывает данные с магнитной полосы карты или чипа EMV (Europay + MasterCard + VISA), когда клиент вставляет карту в банкомат. Некоторые скиммеры имеют возможность считывать данные с чипа карты на расстоянии. Однако атаки на скимминг банкоматов сокращаются благодаря внедрению решений для защиты от скимминга, стандарта безопасности данных индустрии платежных карт, технологии EMV и функциональности бесконтактных банкоматов [1].

2. Скимминг подслушивания.

Новый тип скимминг-атаки, называемый «скиммингом подслушивания», появился и распространился преимущественно в Соединенном Королевстве. Атака нацелена на моторизованные считыватели карт банкоматов на более старой модели банкоматов под названием *personas*. Злоумышленник проникает в банкомат, чтобы получить доступ к считывателю карт банкомата. Затем скиммер устанавливается непосредственно на электрический узел, который переносит данные карты на устройство считывания карт. В банкоматах *Personas* злоумышленник нацеливается на электронную панель управления считывателем карт, создавая отверстие за окном ориентации карты банкомата.

3. Блокировка карты банкомата.

Атака на блокировку карту банкомата — это атака, в ходе которой киберпреступник вставляет устройство в устройство считывания карт банкомата, которое перехватывает и записывает данные, передаваемые между чипом EMV и устройством считывания карт банкомата. Затем эти

данные могут быть повторно использованы для клонирования карты с магнитной полосой. Данные чипа EMV и данные магнитной полосы имеют разные контрольные значения (CVV), и поэтому данные, полученные с карты чипа EMV, нельзя использовать для клонирования магнитной полосы. Блокировка карты не является уязвимостью ни для чиповой карты, ни для банкомата. Поэтому нет необходимости добавлять в банкомат механизмы защиты от этой формы атаки. Если во время транзакции в банкомате соблюдается надлежащая процедура авторизации, поддельные карты могут быть немедленно обнаружены. Эта атака может быть успешной только в том случае, если эмитент пренебрегает проверкой CVV при авторизации транзакции. Поэтому все эмитенты должны проводить эти базовые проверки, чтобы предотвратить эту категорию мошенничества.

4. Перехват карт банкомата.

Перехват карты банкомата крадет саму физическую карту через устройство, подключенное к банкомату. Киберпреступники помещают устройство непосредственно над или в слот для считывания карт банкомата. Эти устройства предназначены для захвата карт после того, как клиенты вставляют их в банкомат. Возможность бесконтактной связи помогает в борьбе с этим мошенничеством.

5. Перехват наличных в банкоматах.

Перехват наличных — это когда киберпреступник использует устройство для физического захвата выдаваемых наличных и приходит за ними, как только клиент покинул место расположения банкомата. Это мошенничество включает в себя размещение денежных ловушек или фальшивых предъявителей перед банкоматом. При обработке транзакции банкомат выдает банкноты в ловушку, установленную киберпреступниками вместо того, чтобы передать деньги клиенту. Клиент предполагает, что банкомат неисправен, и уходит. Затем киберпреступник возвращается, удаляет денежную ловушку или фальшивого предъявителя и уходит с наличными, предназначенными для клиента.

6. Мошенничество с отменой транзакций.

Мошенничество с отменой транзакций включает в себя создание ошибки, из-за которой создается впечатление, что наличные деньги не были выданы. На счет повторно зачисляется сумма, (снятая), но эти деньги преступник забирает. Это может быть физический захват (аналогичный захвату наличных денег) или искажение сообщения о транзакции. Счет не будет списан, хотя преступник снимет наличные из банкомата [4].

7. Социальная инженерия/Фишинговые атаки.

Жертву обманом заставляют раскрыть свою идентификационную информацию (PIN-код). Это может быть физически или с помощью электронных средств. например, злоумышленники создают

мошеннические веб-сайты для сбора аутентификационной информации от ничего не подозревающих клиентов во имя необходимых обновлений или изменений, проводимых их "банкирами". Пользователь в конечном итоге разглашает конфиденциальные данные своей карты мошенническому сайту [2].

8. Операционное мошенничество.

При этом виде мошенничества банкоматом манипулируют. Банкомат сконфигурирован так, чтобы выдавать большие купюры как меньшие, вследствие чего выдает больше денег, чем следует выдавать. Это может быть достигнуто либо путем загрузки банкнот неправильного номинала в неправильные кассеты с деньгами, либо путем внесения неправильной конфигурации в программное обеспечение.

9. Атаки вредоносных программ.

Атаки вредоносного ПО обычно проще проводить при участии инсайдера, поскольку для развертывания вируса необходим физический доступ. Тем не менее, сегодня эта атака возможна онлайн. Вредоносный файл или устройство помещается в банкомат, затем его управляющее устройство запускается, чтобы предоставить злоумышленнику дистанционное управление через пользовательский интерфейс, который позволяет записывать номера карт и ПИН-коды через личное пространство памяти приложений для обработки транзакций, установленных на взломанном банкомате. Развертывание эффективного антивирусного программного обеспечения может помочь смягчить этот класс атак.

10. Атаки вымогателей.

Серьезная вредоносная программа под названием «WannaCry» затронула многие организации по всему миру. Она была запущена 12 мая 2017 года и предназначалась для компьютеров под управлением Windows 7 или более ранних версий в более чем 150 странах. «WannaCry» шифрует файлы на конечных точках, на которых запущено программное обеспечение операционной системы Microsoft, делая их недоступными. Файлы расшифровываются только после выплаты денежной суммы, известной как выкуп. Эта вредоносная программа пытается заразить другие конечные точки в той же сети. Вредоносная программа не нацелена специально на банковские и розничные системы или их функциональные возможности, но банкоматы, как и любая другая система на базе Windows, также подвержены риску этой атаки [3].

Многие организации по всему миру пострадали от другой вредоносной программы под названием «Petya». Эта вредоносная программа шифрует файлы на конечных точках, работающих под управлением программного обеспечения операционной системы Microsoft, делая их недоступными. Банкоматы подвержены риску этой атаки, поскольку они работают в

операционной системе Microsoft. Все банкоматы, работающие под управлением любой операционной системы Windows, которые не были исправлены с помощью обновления безопасности Microsoft MS17-010, подвергаются риску. Если какие-либо банкоматы заражены/заблокированы программой-вымогателем, то все остальные банкоматы и конечные точки в той же сети также должны быть проверены на наличие вирусов. Как только вредоносная программа заразит одну конечную точку в сети, она будет реплицироваться в другие уязвимые системы.

11. «Банкоматный джекпот».

Термин «Банкоматный джекпот» происходит от термина «Джекпот». При таком типе атаки киберпреступники сразу получают огромные суммы денег из банкомата. Киберпреступники используют два метода для выполнения этой атаки:

- Атака черного ящика: Киберпреступнику необходим физический доступ к верхнему шкафу банкомата, в котором размещается ядро ПК банкомата, а затем он переводит банкомат в режим супервизора. Злоумышленник удаляет сетевой кабель банкомата, чтобы банкомат не мог контролироваться службой мониторинга банкоматов. Затем злоумышленник устанавливает черный ящик, который представляет собой специальное устройство, запрограммированное для управления банкоматом. Банкомат переходит в режим супервизора для клиента банкомата, но банкомат все еще работает. Черным ящиком можно управлять по беспроводной сети с помощью обычного смартфона. Злоумышленник использует смартфон для выдачи команд банкомату для выдачи наличных. Команда может выдаваться непрерывно до тех пор, пока в банкомате не закончатся деньги. Затем злоумышленники удаляют устройство черного ящика и не оставляют никаких следов его установки на банкомате.

- Вредоносная атака: Вредоносное ПО может быть доставлено физически с помощью USB-портов банкомата или удаленно через взломанную банковскую сеть. Используя клавиатуру и командную строку, злоумышленник запускает вредоносную программу. Эти действия можно даже автоматизировать, чтобы вредоносная программа работала автономно. Атака может быть проведена через сеть без физического доступа к банкомату и возможна, когда отсутствуют система защиты банкомата от вредоносных программ, белый список программного обеспечения для банкомата, аутентификация для обмена данными между аппаратными блоками банкомата и его основным приложением.

Владельцы банкоматов должны внедрять решения для предотвращения несанкционированного развертывания вредоносных программ на

банкоматах [4]. В целом, все владельцы банкоматов должны выполнять следующие действия для обеспечения безопасности своих банкоматов:

- следовать всем рекомендациям в стандарт безопасности индустрии платёжных карт;
- система обнаружения вторжений должна быть настроена так, чтобы отслеживать весь трафик и предупреждать о любых подозрительных действиях;
- брандмауэр должен быть настроен так, чтобы обновлять и пропускать только известный трафик приложений внутрь и наружу;
- программа управления исправлениями для операционной системы и приложений должна быть на месте, чтобы гарантировать, что программное обеспечение банкоматов хорошо исправлено;
- должно быть разработано программное решение для внесения банкоматов в белый список, а также должен быть установлен и постоянно обновляться антивирус;
- необходимо внедрить систему управления рисками и подготовить план реагирования на эти риски, чтобы сообщения о мошенничестве с банкоматами поступали в режиме реального времени;
- программное обеспечение банкомата должно регулярно обновляться;
- всем операторам банкоматов следует перейти на чип EMV и PIN-карту и исключить откат магнитной полосы, это снизит риск скимминга карт;
- отделить сеть банкоматов от остальной сети банка с помощью брандмауэра и виртуальных локальных сетей;
- должна быть разработана политика паролей, чтобы гарантировать, что в банкоматах используются только надежные пароли, и у каждого пользователя есть свой собственный уникальный пароль;
- все коммуникации в банкомате должны быть зашифрованы, включая связь между ядром ПК и банкоматом;
- неиспользуемые сервисы и приложения должны быть удалены из банкомата, чтобы уменьшить поверхность атаки;
- необходимо развернуть эффективное программное обеспечение для защиты от вредоносных программ;
- операционная система ядра ПК должна быть закалена;
- тестирование на проникновение должно проводиться на банкомате ежегодно;
- обеспечить физическую безопасность банкомата, такую как видеонаблюдение и сигнализация, при его установке;

– установить инструмент, который обеспечит конфиденциальность, целостность и доступность банкомата.

Таким образом, для предотвращения рассмотренных рисков владельцы банкоматов должны убедиться, что они применяют рекомендуемые меры противодействия для обеспечения безопасности среды банкомата для пользователя. Предлагаемые средства управления должны быть проверены путем их внедрения в банкомате, а затем выполнение теста на проникновение. Это должно быть сделано в разных географических регионах, чтобы обеспечить работу средств контроля во всех регионах мира. На основе предлагаемых средств контроля будет разработана структура, способствующая повышению безопасности банкоматов.

Список использованных источников:

1. Антонов А. Как злоумышленники используют уязвимости АТМ // Расчеты и операционная работа в коммерческом банке. М.: Регламент, – 2018. – № 2 (144). – С. 47–59.
2. Архипов А. Проблемы определения места совершения мошенничества в отношении безналичных денежных средств // Уголовное право. – 2016. – № 3. – С. 4–10
3. Блажевич О. Г. Особенности развития финансового рынка в условиях цифровизации / О. Г. Блажевич, Н.С. Сафонова // Научный вестник: финансы, банки, инвестиции – 2021. – №1 (54). – С. 106-124.
4. Буркальцева Д. Д., Управление финансово-экономической безопасностью: институциональные основы в условиях цифровизации / Д. Д. Буркальцева Р.А. Овчинников // Методологические основы и научно-практические положения институционального прогнозирования и планирования в системе государственного регулирования экономики: Материалы Международного научно-практического круглого стола. – 2018. – С. 21-24.
5. Норец Н.К. Цифровая безопасность банковской сферы / Н.К. Норец // Развитие Российской экономики и ее финансовая безопасность в условиях современных вызовов и угроз: международная научно-практическая онлайн конференция, г. Ростов, 22-23 октября 2020 г. – С. 183-186.

Обеспечение кибербезопасности в банковской сфере в условиях цифровой трансформации

К.Ю. Мяделец

студентка 4 курса БГЭУ, Минск

E-mail: mu.karinka@mail.ru

научный руководитель: В.В. Позняков

к.э.н., доцент кафедры банковского дела БГЭУ, Минск

E-mail: pozniakov@bseu.by

Аннотация: В статье обосновывается необходимость обеспечения кибербезопасности в банковской сфере для преодоления порождаемых цифровой трансформацией киберрисков, определяются приоритеты развития информационной безопасности, направления и перспективы ее совершенствования.

Ключевые слова: киберриски, обеспечение кибербезопасности, цифровая трансформация, безопасность банковских услуг.

Ensuring cybersecurity in banking in the context of digital transformation

Abstract: The article substantiates the necessity to ensure cybersecurity in the banking to overcome the cyber risks generated by digital transformation, identifies the priorities for the development of information security, directions and prospects for its improvement.

Keywords: cyber risks, cyber security, digital transformation, security of banking services.

В современных условиях формирования открытого рынка цифровых финансовых услуг одним из важнейших вопросов обеспечения безопасности деятельности в банковской сфере является обеспечение защиты ее информационной инфраструктуры и определение в связи с этим основополагающих подходов к обеспечению кибербезопасности банковской сферы.

Поскольку банковская сфера занимает одно из ведущих мест в реализации национальных стратегий и планов создания цифровой экономики, координация деятельности ее субъектов в процессах обеспечения кибербезопасности является необходимым условием проведения государственной политики в этой области.

Актуальность вопроса повышения кибербезопасности в банковской сфере обусловлена главным образом существенным увеличением в последние годы объемов предоставляемых банками цифровых финансовых услуг и нарастанием присущего такой деятельности риска, в том числе ростом количества кибератак, в первую очередь ставящих целью хищение денежных средств [1].

Особенностью финансовых мошенников, орудующих в условиях цифровой трансформации экономики, является умение быстро адаптироваться к глобальным переменам и наживаться на уязвимостях, связанных с растущей популярностью Интернет-банкинга, SMS-банкинга, Мобильного банкинга, PC-banking, WAP-banking и т.п.

Развитие систем дистанционного банковского обслуживания наряду с такими преимуществами, как рост качества, скорости, доступности банковских услуг, несет в себе и дополнительные риски, а именно – предоставление киберпреступникам возможности использования для мошеннических целей вредоносных программ, под которыми понимаются зловреды, атакующие пользователей финансовых сервисов и вредоносные программы, пытающиеся получить доступ к финансовым организациям и их инфраструктуре.

Анализ международной практики показывает, что на мировом уровне можно выделить следующие наиболее характерные для банковской сферы виды киберугроз:

1. воздействие через аппаратные уязвимости – уязвимости, присутствующие в микропроцессорах разных производителей, открывающие новые возможности для злоумышленников, неустраняемые при помощи программных обновлений;

2. компьютерный шпионаж – направлен на долговременное присутствие в сетях объектов критической информационной инфраструктуры с целью саботажа и шпионажа за деятельностью финансовых организаций;

3. целенаправленные кибератаки – атаки, направленные на конкретные финансовые организации и позволяющие злоумышленникам проникать в сеть организаций и далее к изолированным финансовым системам для вывода денежных средств;

4. клиент-ориентированные кибератаки – направлены непосредственно на клиентов банков, а именно на хищение их личных денежных средств [2].

На сегодняшний день наиболее распространенными путями реализации киберпреступлений в банковской сфере являются финансовый фишинг, использование вредоносных программ для персональных компьютеров (ПК) и мобильных приложений, что подтверждается результатами

проведенного в 2021 году «Лабораторией Касперского» исследования, направленного на изучение финансовых угроз [3].

Финансовый фишинг – один из главных инструментов хищения денег, применяемых киберпреступниками, при котором злоумышленники выдают себя за банки или другие финансовые учреждения, чтобы заставить жертву заполнить фальшивую форму и получить данные учетных записей. Похищенные данные, как правило, используются для кражи средств с банковских счетов или продаются в Интернете. Подобные атаки осуществляются также через телефонные звонки (vishing) и SMS-сообщения (smishing).

Финансовый фишинг помимо банковского включает в себя и другие типы атак. Например, атаки на пользователей платежных систем с использованием маскировки под широко известные сервисы.

Наиболее часто используемыми брендами платежных систем в финансовом фишинге выступают Visa, PayPal, Mastercard и American Express (рисунок 1).

Как видно на рисунке, главной мишенью в 2019 году были пользователи Visa (37,6%). Второе место у PayPal с показателем 26,8%, а замыкает тройку лидеров MasterCard (16,3%). В 2020 году бренд PayPal использовался мошенниками чаще, чем бренды других известных платежных систем (в 38,7% случаев), а его доля увеличилась на 12 п. п.

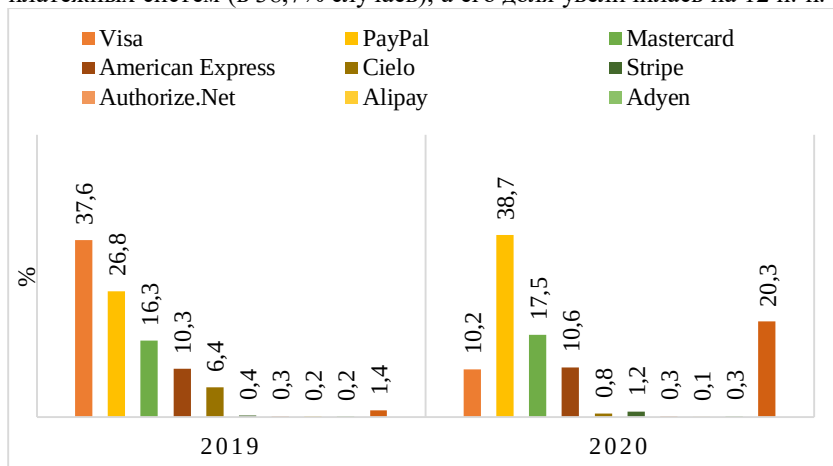


Рисунок 1 – Бренды платежных систем, чаще всего используемых в финансовом фишинге

Примечание – Источник: собственная разработка на основе [3].

Второе место досталось Mastercard, чья доля выросла незначительно: с 16,3% до 17,5%. Третье и четвертое места с минимальным отрывом друг от

друга заняли American Express (10,6%) и Visa (10,2%). В 2020 году мошенники маскировались под Visa в 3,5 раза реже, чем в 2019 году (37,6%).

Второй по популярности в банковской сфере путь реализации киберпреступлений – банковские вредоносные программы для ПК, задачей которых является похищение учетных данных для входа в системы интернет-банкинга или в платежные системы, а также перехват одноразовых паролей.

Наибольший всплеск активности вредоносных программ наблюдался в октябре 2016 года, когда было затронуто свыше 1,5 млн пользователей банковских услуг по всему миру. Далее наблюдается постепенное сокращения числа клиентов банков, ставших жертвами вредоносных программ. К 2020 году их число сократилось до 0,5 млн пользователей (рисунок 2). Однако, такое снижение атак объясняется приобретением ими целенаправленного характера, т.е. переориентация с банковского сектора на крупный бизнес, что, как и прежде, оказывает негативное влияние на финансовую безопасность государства в целом.

Самыми активными семействами банковских вредоносных программ выступают Zbot, RTM, Emotet, CliptoShuffler, Trickster, Ramnit, Neurevt, SpyEye и др. На первые четыре приходится более половины атакованных пользователей.

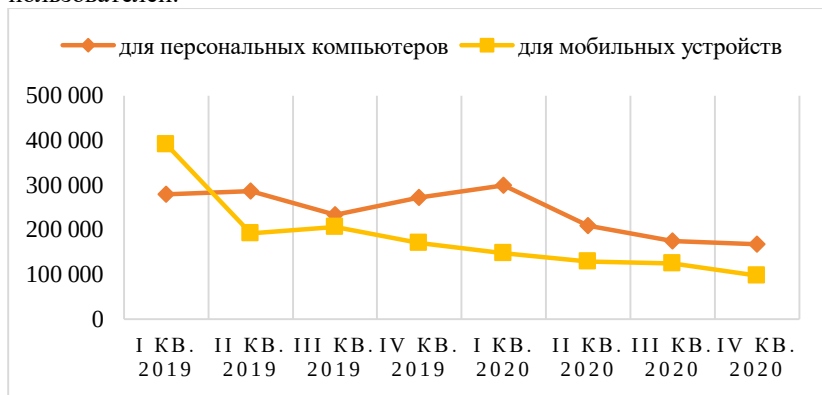


Рисунок 2 – Изменение числа уникальных пользователей, атакованных банковскими вредоносными программами

Примечание – Источник: собственная разработка на основе [3].

Третий по популярности вид вредоносных программ – банковские вредоносные программы для мобильных устройств, цель функционирования которых практически ничем не отличается от целей соответствующих программ для ПК. Число пользователей, атакованных

банковскими вредоносными программами, резко снижается. Если в октябре 2018 года данный показатель был зафиксирован на уровне 600 тыс. пользователей, что в 2020 году он не превышает 200 тыс. (рисунок 2).

Самыми распространенными банковскими вредоносными программами являются Asacub, Agent, Svpeng, Rotexy. 2020 год характеризуется появлением особо агрессивных программ, реализующих ряд принципиально новых возможностей, к числу которых относятся Trojan-Banker.AndroidOS.Knobot.a, Trojan-Banker.AndroidOS.Gorgona.a и Trojan-Banker.AndroidOS.Ghimob.a.

Таким образом, в результате исследования выявлено, что киберпреступники способны адаптироваться к новым реалиям и переменам в мире, продолжая развивать вредоносные программы и методы обхода защитных алгоритмов. Такое положение требует принятия мер, способных обезопасить от угроз, вызванных цифровой трансформацией, как банки, так и клиентов.

С целью предотвращения реализации кибератак пользователям банковских программных продуктов необходимо соблюдать следующие рекомендации:

1. установка приложений только из надежных источников, таких как официальные веб-сайты;
2. проверка разрешений и прав доступа, запрашиваемых приложением, и отказ в их предоставлении, если они фактически не требуются для работы приложения;
3. установка надежного защитного решения, способного обезопасить от широкого спектра финансовых киберугроз.

К корпоративным пользователям, которые одновременно выступают и объектом, и инструментом реализации угроз, необходимо применение наиболее действенных мер, в число которых обязательно должно входить обучения основам кибербезопасности сотрудников; проведение вебинаров, направленных на повышение финансовой и компьютерной грамотности; по возможности установка актуальных обновлений и исправлений для всех используемых программ. Для обеспечения защиты данных будут актуальны следующие действия: предотвращение физического вторжения и защита рабочих мест от несанкционированного доступа к конфиденциальной информации; шифрование всех данных, хранящихся на компьютерах в финансовом учреждении и передаваемых во внешний мир, выбор надежных внутренних средств коммуникации в организации; запрет на использование социальных сетей или публичных медиаинструментов; реализация многоуровневой системы защиты почтовых ящиков сотрудников для предотвращения фишинга; внедрение системы

мониторинга, в которой любая финансовая операция должна пройти серию проверок, прежде чем будет одобрена.

Противостоянием стремительно совершенствующимся приемам киберпреступников в дальнейшем может послужить модификация системы обнаружения мошенничества на основе больших данных, которые помогут отслеживать необычные изменения привычных моделей поведения пользователей, использование новых биометрических технологий и аутентификации на основе оценки риска, инвестирование банков в разработку защищенных механизмов.

В целом ключевые направления развития кибербезопасности банковской сферы в условиях цифровой трансформации можно сформировать в виде трех блоков (таблица 1).

Таблица 1 – Ключевые направления развития кибербезопасности

Цель на сегодня	Цель на будущее
Защищенность	
1. Защита ключевых информационных активов. 2. Создание эффективной системы управления кибербезопасностью.	1. Оценка киберрисков в момент принятия решения об использовании новейших технологий. 2. Акцент на управлении киберрисками, а не на отказе от новейших технологий. 3. Защита данных от утечек и искажения.
Бдительность	
1. Осведомленность о нарушении кибербезопасности в банке. 2. Акцент на всей экосистеме. 3. Тестирование на проникновение, оценка защищенности.	1. Применение передовых технологий для проактивного выявления угроз кибербезопасности. 2. Понимание экспоненциальных угроз кибербезопасности и подготовка к ним.
Устойчивость	
1. Планирование восстановления в случае реализации киберинцидентов. 2. Регулярная проверка способности банка к восстановлению.	1. Разработка сценариев реагирования, специфичных для различных категорий угроз и инцидентов. 2. Разработка интегрированного плана реагирования, охватывающего все ключевые подразделения.

Примечание – Источник: собственная разработка на основе [4].

В последние годы ведется активная разработка и применение ряда документов, направленных на формирование системных подходов к обеспечению кибербезопасности, управлению киберриском и распространению на него режима надзора с учетом специфики этого риска: документ Комитета по платежам и рыночной инфраструктуре и Совета

Международной организации комиссий по ценным бумагам «Руководство по киберустойчивости для инфраструктур финансового рынка»; документ Института финансовой стабильности «Регуляторные подходы к усилению системы обеспечения кибербезопасности в банках»; документ Всемирного банка «Кибербезопасность финансового сектора: дайджест для регуляторов»; документ Базельского Комитета по банковскому надзору «Киберустойчивость: обзор практик» и др.

Надзорными органами Австралийского союза, Канады, Великобритании, Европейского союза, Соединенных Штатов Америки, Швейцарии, Сингапура, Гонконга разрабатываются требования и принципы обеспечения кибербезопасности в банковской сфере и подходы к управлению киберриском.

Отдельными государствами утверждаются собственные Концепции обеспечения кибербезопасности в банковской сфере [1].

Определенно, вопрос повышения уровня кибербезопасности и в дальнейшем не собирается игнорироваться как отдельными государствами, так и мировым сообществом в целом.

Список использованных источников:

1. Концепция обеспечения кибербезопасности в банковской сфере / Постановление Правления Национального банка Республики Беларусь от 20.11.2019 № 466, – 15 с.
2. Бозиева З.А. Роль цифровизации в развитии финансового сектора // Вестник КЭУ, № 2(47), Бишкек, 2019.
3. Финансовые киберугрозы в 2020 году [Электронный ресурс] / Securelist by Kaspersky. – Режим доступа: <https://securelist.ru/financial-cyberthreats-in-2020/101160/>. – Дата доступа: 17.11.2021.
4. Кибербезопасность, цифровые риски и угрозы [Электронный ресурс] / «Делойт». – Режим доступа: <https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/russian/kiberbezopasnost-cifrovye-riski-i-ugrozy.pdf>. – Дата доступа: 17.11.2021.

Обзор биометрических криптосистем и отменяемой биометрии

А.А. Новопавловский

аспирант 1 курса НИЯУ МИФИ, Москва

E-mail: mr.novopavlovskiy@mail.ru

К. Верейкин

аспирант 1 курса ИАТЭ НИЯУ МИФИ, Обнинск

E-mail: kirill_vereikin@mail.ru

Аннотация. С точки зрения конфиденциальности, большинство опасений по поводу обычного использования биометрии возникает из-за хранения и неправомерного использования биометрических данных. Биометрические криптосистемы и отменяемая биометрия представляют собой новые технологии защиты биометрических шаблонов, которые решают эти проблемы и повышают общественное доверие и признание биометрии. Кроме того, биометрические криптосистемы предоставляют механизмы для освобождения ключей в зависимости от биометрических данных. В последние годы опубликовано значительное количество подходов к обеим технологиям. Представлен всесторонний обзор биометрических криптосистем и аннулируемой биометрии. Рассматриваются современные подходы, на основе которых дается подробное обсуждение и взгляд на будущие перспективы.

Ключевые слова: биометрия, биометрическая криптосистема, конфиденциальность, криптография, аннулируемая биометрия, защита биометрических шаблонов.

A survey on biometric cryptosystems and cancelable biometrics

Abstract. From a privacy perspective most concerns against the common use of biometrics arise from the storage and misuse of biometric data. Biometric cryptosystems and cancelable biometrics represent emerging technologies of biometric template protection addressing these concerns and improving public confidence and acceptance of biometrics. In addition, biometric cryptosystems provide mechanisms for biometric-dependent key-release. In the last years a significant amount of approaches to both technologies have been published. A comprehensive survey of biometric cryptosystems and cancelable biometrics is presented. State-of-the-art approaches are reviewed based on which an in-depth discussion and an outlook to future prospects are given.

Keywords: *biometrics, biometric cryptosystem, privacy, cryptography, canceled biometrics, protection of biometric templates*

Введение

Термин биометрия определяется как «автоматическое распознавание людей на основе их поведенческих и биологических характеристик». Физиологические, а также поведенческие биометрические характеристики получают с помощью соответствующих датчиков, а отличительные черты извлекаются для формирования биометрического шаблона в процессе регистрации. Во время проверки или идентификации (идентификация может быть обработана как последовательность проверок и проверок) система обрабатывает другой биометрический ввод, который сравнивается с сохраненным шаблоном, обеспечивая принятие или отклонение. Обычно признается, что замены биометрии для положительной идентификации в интегрированных приложениях безопасности не существует. В то время как отрасль давно заявляла, что одним из основных преимуществ биометрических шаблонов является то, что исходные биометрические сигналы, полученные для регистрации субъекта данных, не могут быть восстановлены из сохраненных шаблонов, несколько подходов доказали, что это утверждение неверно. Поскольку биометрические характеристики в значительной степени неизменны, компромисс с биометрическими шаблонами приводит к безвозвратной потере биометрических данных объекта. Стандартные алгоритмы шифрования не поддерживают сравнение биометрических шаблонов в зашифрованном домене и, таким образом, оставляют биометрические шаблоны открытыми при каждой попытке аутентификации. Гомоморфно и асимметричное шифрование, например, в работах, которые позволяют биометрическое сравнение в зашифрованном домене представляет собой исключение. Обычные криптосистемы предоставляют множество алгоритмов для защиты любой важной информации. В то время как аутентификация пользователя основана на владении секретными ключами, управление ключами осуществляется путем введения второго уровня аутентификации (например, паролей). Как следствие, зашифрованные данные наследуют безопасность соответствующих паролей, применяемых для выпуска правильных ключей дешифрования. Схемы защиты биометрических шаблонов, которые обычно классифицируются как биометрические криптосистемы (также называемые схемами на основе вспомогательных данных) и отменяемые биометрические данные (также называемые преобразованием функций), разработаны для удовлетворения двух основных требований защиты биометрической информации:

Необратимость: восстановление исходного биометрического шаблона из сохраненных справочных данных, т.е. защищенного шаблона, должно быть трудным в вычислительном отношении, в то время как создание защищенного биометрического шаблона должно быть простым.

Несвязность: разные версии защищенных биометрических шаблонов могут быть созданы на основе одних и тех же биометрических данных (возможность обновления), в то время как защищенные шаблоны не должны допускать перекрестного сопоставления (разнообразия).

«Биометрические криптосистемы (BCS) предназначены для надежной привязки цифрового ключа к биометрическому или для генерации цифрового ключа из биометрического», предлагая решения для биометрической защиты от выпуска ключа и защиты биометрических шаблонов. BCS, заменяющие выпуск ключей на основе пароля, дают существенные преимущества в плане безопасности. Подделывать, копировать, делиться и распространять биометрические данные значительно сложнее, чем пароли. Большинство биометрических характеристик обеспечивают одинаковый уровень безопасности для группы пользователей (физиологические биометрические характеристики не выбираются пользователем). Из-за биометрической дисперсии, обычные биометрические системы выполняют «нечеткие сравнения», применяя пороги принятия решения, которые устанавливаются на основе распределения баллов между подлинными и не подлинными субъектами. Напротив, BCS предназначены для вывода стабильных ключей, которые должны соответствовать 100% при аутентификации. Оригинальные биометрические шаблоны заменяются общедоступной информацией, зависящей от биометрических данных, которая помогает процессу выпуска ключей.

Биометрические криптосистемы

Для большинства BCS требуется хранение общедоступной информации, зависящей от биометрических данных, которая применяется для извлечения или генерации ключей и называется вспомогательными данными. Из-за биометрической дисперсии для большинства биометрических характеристик невозможно извлечь ключи напрямую. Вспомогательные данные, которые не должны раскрывать важную информацию об исходных биометрических шаблонах, помогают в восстановлении ключей. Биометрические сравнения выполняются косвенно, путем проверки достоверности ключей, где результатом процесса аутентификации является либо ключ, либо сообщение об ошибке. Поскольку проверка ключей представляет собой биометрическое сравнение в зашифрованном домене, BCS применяются как средство защиты биометрических шаблонов, в дополнение к возможности

разблокировки ключа, зависящей от биометрических данных. В зависимости от того, как получены вспомогательные данные, BCS классифицируются как системы привязки или генерации ключей.

Отменяемые биометрические данные

Отменяемые биометрические преобразования разработаны таким образом, что восстановление исходных биометрических данных должно быть трудным с вычислительной точки зрения. Внутренняя сила (индивидуальность) биометрических характеристик не должна снижаться с применением преобразований (ограничение на FAR), в то время как, с другой стороны, преобразования должны быть устойчивыми к вариациям внутри класса (ограничение на FRR). Кроме того, корреляция нескольких преобразованных шаблонов не должна раскрывать никакой информации об исходной биометрии (несвязность). В случае компрометации преобразованных биометрических данных изменяются параметры преобразования, т. е. Обновляется биометрический шаблон. Чтобы мошенники не отслеживали субъектов посредством перекрестного сопоставления баз данных, предлагается применять разные преобразования для разных приложений. Выделяют две основные категории КБ:

1) Необратимые преобразования: в этих подходах биометрические данные преобразуются с применением необратимой функции. Для предоставления обновляемых шаблонов изменяются параметры применяемых преобразований. Преимущество применения необратимых преобразований заключается в том, что потенциальные мошенники не могут восстановить все биометрические данные, даже если преобразования скомпрометированы. Однако применение необратимых преобразований в большинстве случаев подразумевает потерю точности. Снижение производительности вызвано тем, что преобразованные биометрические шаблоны трудно согласовать (как в BCS), чтобы выполнить правильное сравнение, и, кроме того, уменьшается информация. Для нескольких подходов эти эффекты наблюдались;

2) Биометрическое «засаливание»: Биометрическое «засоление» обычно означает преобразование биометрических шаблонов, которые выбираются как обратимые. Любое обратимое преобразование элементов вектора биометрических признаков представляет собой подход к биометрическому засолению, даже если биометрические шаблоны были извлечены таким образом, что невозможно восстановить исходный биометрический сигнал. Как следствие, параметры преобразования должны храниться в секрете.

Заключение

На основе представленных ключевых концепций BCS и СВ проводится заключительное обсуждение, включая преимущества и приложения,

потенциальные атаки на обе технологии, текущее состояние дел, коммерческих поставщиков, а также открытые вопросы и проблемы.

Наиболее очевидное применение BCS - это биометрический зависимый выпуск ключей в традиционных криптосистемах, заменяющий незащищенное освобождение ключей на основе пароля или PIN-кода. Устранение этого слабого звена в криптосистемах, биометрический зависимый выпуск ключей приводит к существенным преимуществам безопасности, делая криптографические системы более подходящими для приложений с высоким уровнем безопасности.

Современное состояние BCS и СВ оценивается по нескольким параметрам, т.е. по заявленным показателям производительности, биометрическим модальностям, прикладным тестам и т.д., а также сравниваются и обобщаются наиболее эффективные и оцененные подходы.

Что касается целей проектирования, BCS и СВ предлагают значительные преимущества для повышения конфиденциальности и безопасности биометрических систем, обеспечивая надежную биометрическую аутентификацию на высоком уровне безопасности. Методы, которые обеспечивают доказуемую безопасность/конфиденциальность, при достижении практических показателей распознавания, остаются труднодостижимыми (даже для небольших наборов данных). Кроме того, при развертывании этих технологий возникает несколько новых проблем и проблем. Одна фундаментальная проблема, касающаяся обеих технологий, представляет собой проблему согласования, которая значительно влияет на производительность распознавания. Биометрические шаблоны скрыты в рамках обеих технологий, т.е. выравнивание скрытых шаблонов без утечки очень нетривиально. Хотя для некоторых биометрических характеристик (например, радужной оболочки глаза) все еще возможно выравнивание, для других (например, отпечатков пальцев) необходимо сохранять дополнительную информацию, которая не должна приводить к реконструкции шаблона. В рамках обычных биометрических систем были предложены подходы, инвариантные к выравниванию, для нескольких биометрических характеристик. До сих пор почти не было сделано никаких предложений по созданию согласованно-инвариантных BCS или СВ, позволяя биометрическое слияние в форме, подходящей для различных схем защиты шаблонов.

Список использованных источников:

1. Jain AK, Ross A, Prabhakar S: An introduction to biometric recognition. IEEE Trans Circ Syst Video Technol 2004, 14: 4-20.

2. appelli R, Lumini A, Maio D, Maltoni D: Fingerprint image reconstruction from standard templates. *IEEE Trans Pattern Anal Mach Intell* 2007, 29(9):1489-1503.
3. Ross A, Shah J, Jain AK: From template to image: reconstructing fingerprints from minutiae points. *IEEE Trans Pattern Anal Mach Intell* 2007, 29(4):544-560.
4. Jain AK, Nandakumar K, Nagar A: Biometric template security. *EURASIP J Adv Signal Process* 2008, 1-17.
5. Luo Y, Cheung SS, Ye S: Anonymous biometric access control based on homomorphic encryption. *ICME'09: Proc of the 2009 IEEE Int Conf on Multimedia and Expo 2009*, 1046-1049.
6. Upmanyu M, Namboodiri AM, Srinathan K, Jawahar CV: Efficient biometric verification in encrypted domain. *ICB '09: Proc of the Third Int Conf on Biometrics 2009*, 899-908.
7. Uludag U, Pankanti S, Prabhakar S, Jain AK: Biometric cryptosystems: issues and challenges. *Proc IEEE* 2004, 92(6):948-960.
8. Cavoukian A, Stoianov A: Biometric encryption. In *Encyclopedia of Biometrics*. Springer; 2009.
9. Ratha NK, Connell JH, Bolle RM: Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst J* 2001, 40: 614-634.

Обзор ERP-систем в контексте повышения прозрачности деятельности крупных компаний

А.В. Михеева

студентка 1 курса аспирантуры НИЯУ МИФИ, Москва

E-mail: stacy1510@yandex.ru

П.Ю. Леонов

к.э.н., доцент кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: p.u.leonov@gmail.com

Аннотация: Вопросы использования цифровых технологий для автоматизации бизнес-процессов, а также для улучшения прозрачности деятельности – достаточно актуальны сегодня. В статье рассмотрены внедренные ERP-системы у разных крупных компаний России для своих собственных целей, в том числе для повышения прозрачности ценообразования, прозрачности работы складских сотрудников, прозрачности цепочки поставок и управления и т.д.

Ключевые слова: ERP-система, SAP, коррупция, предикатное преступление, бизнес-процессы.

Overview of ERP systems in the context of increasing transparency of the activities of large companies

Abstract: The issues of using digital technologies to automate business processes, as well as to improve the transparency of activities, are quite relevant today. The article discusses the implemented ERP systems of various large companies in Russia for their own purposes, including increase the transparency of pricing, transparency of warehouse employees, transparency of the supply chain and management, etc.

Keywords: ERP system, SAP, corruption, predicate crime, business processes.

Основная часть

Стоит отметить, что ERP-системы были разработаны в 60-е годы XX века в виде MRP систем. Данная система отвечала за производственную планировку материалов. Однако термин «ERP» впервые появился в 1990 году благодаря финансовому аналитику Ли Уайли.

ERP-системы с момента своего появления на рынке позиционировались как комплекс мер, позволяющих оптимизировать не только производственную часть бизнеса. Ведение бухгалтерского учета, ценообразование, организация данных, управление продажами и запасами — все это сегодня возможно реализовать в новых ERP-системах.

Сегодня одной из самых популярных в мире ERP-систем является SAP. Был замечен дефицит научной отечественной литературы, теоретических и практических статей по теме внедрения, реализации, использования ERP системы SAP. Есть предположение, что это связано с тем, что ERP-система SAP имеет большую популярность за рубежом, в то время как компании России отдают предпочтения российскому аналогу «1С: ERP», а также обычным системам учета «1С». Данное предпочтение делается, так как компании на территории России должны соблюдать законодательство РФ в сфере ведения бухгалтерского и налогового учета. В свою очередь «1С» является российской разработкой, которая формирует различные отчетные документы (баланс, управленческие формы, справки по ФСС РФ и т.д.) сразу в соответствии с законодательством РФ. Зарубежные ERP-системы, такие как SAP, необходимо адаптировать под стандарты, принятые для предприятий РФ.

Незаконные действия менеджеров, а также коррупция на предприятии — являются предикатным преступлением. Предикатным преступлением является виновно-совершенные общественно-опасные деяния, запрещенные уголовным законодательством государства, предшествующие легализации доходов от таких деяний. В этой связи решение по ведению учета в системе, позволяющей проверять данные контролирующими и надзорными органами — позволяет компании не терять деловую репутацию в рамках усиления прозрачности деятельности, а также позволяет усилить инвестиционную привлекательность для потенциальных инвесторов.

Несмотря на достаточную привлекательность ведения бухгалтерского, налогового, управленческого и статистического учета в российской программе для упрощения процедуры аудита, а также процедуры подачи отчетности в налоговый орган, фонды и т.п. — некоторые крупные предприятия в России внедряют SAP систему в свою деятельность. Это связано, во-первых, с тем, что материнская компания (как правило иностранная компания) утверждает систему, в которой дочерние предприятия должны вести бухгалтерский и управленческий учет; во-вторых, компания самолично нуждается в автоматизации процессов за счет использования иностранной ERP-системы.

На основе информации, выложенной в публичном пространстве (пресс-релизы, премии и т.д.) была собрана информация по внедренным ERP-

системам, в частности SAP- систем. В исследовании участвовало 23 компании, данные по которым представлены ниже в таблице.

Таблица 1 – Информация по компаниям, которые внедрили SAP системы

Номер	Наименование предприятия	Отрасль предприятия	Год проекта	Продукт SAP
1	АО «Фаберлик»	Сетевой маркетинг	2018-2021	SAP Commerce Cloud,
2	ПАО «Северсталь»	Металлургия	2020-2021	SAP Marketing Cloud
3	ООО «Сеть Связной»	Ритейл	2016 - 2018	SAP Commerce Cloud
4	ООО «Рив Гош»	Ритейл	2021	SAP BPC
5	ПАО «Аптечная сеть 36,6»	Ритейл	2017	SAP Commerce Cloud
6	ЗАО «Биокад»	Фармацевтика и биотехнологии	2020	SAP Commerce Cloud
7	Группа компаний «Дамате»	Агро промышленность	2021	SAP Customer Experience
8	ООО «Гиперглобус»	Ритейл	2015-2018	SAP Process Orchestration
9	ООО «Объединенные Пивоварни Хейнекен»	FMCG (Товары повседневного спроса)	2017-2019	SAP EWM Embedded
10	ТПО «Комус»	Ритейл	2017	SAP EWM
11	АО «Мегафон Ритейл»	Телекоммуникации	2010-2011	SAP TM
12	ПАО «МТС»	Телекоммуникации	2020-2021	SAP for Retail
13	Группа «М.Видео Эльдорадо»	Ритейл	2019-2020	SAP F&R
14	S Group	Ритейл	2018-2019	SAP Promotion Management
15	ООО «Воздушные Ворота Северной Столицы»	Транспорт	2019-2020	SAP EWM
16	ООО «МОЛЛ»	Ритейл	2020	SAP ERP
17	ЗАО «Талосто»	FMCG (Товары повседневного спроса)	2006-2007	SAP PI
18	ООО «Восток Запад»	Оптовая торговля	2016-2018	SAP Customer Experience B2B
19	ООО «Лента»	Ритейл	2019	SAP Customer Experience B2C
20	ООО «Группа Мегаполис»	Управляющая организация	2018	SAP for Retail
21	ООО «Охапка»	Ритейл	2021	SAP F&R
22	ООО «Посуда Центр сервис»	Ритейл	2020	SAP Promotion Management
23	ООО «Утконос»	Ритейл	2017-2020	SAP CAR

Из указанного для анализа перечня компаний 2 предприятия внедряла систему SAP до 2015 года (АО «Мегафон Ритейл»; ЗАО «Талосто»); 6 компаний внедряло SAP с 2015 года до 2018 года (ООО «Сеть Связной»; ПАО «Аптечная сеть 36,6»; ООО «Гиперглобус»; ТПО «Комус»; ООО «Восток Запад»; ООО «Группа Мегаполис»), с 2019 по 2021 год внедряли SAP оставшиеся 15 компаний. Таким образом, спрос на использование ERP-системы SAP растет с каждым годом.

Стоит отметить, что среди указанных выше компаний есть предприятия, в которых проект внедрения ERP-системы SAP занял достаточно мало времени. Ниже таблица, в которой представлены данные.

Таблица 2 – Информация по компаниям, которые внедрили SAP системы за короткий срок

Наименование предприятия	Отрасль предприятия	Год проекта	Требования заказчика	Период внедрения проекта
ООО «Рив Гош»	Ритейл	2021	Снижение затрат на поддержку e-commerce платформы с миграцией на SAP Commerce Cloud	Реализация проекта за 6 месяцев
ЗАО «Биокад»	Фармацевтика и биотехнологии	2020	Автоматизация управления складом на базе решения SAP EWM в интеграции с роботизированной системой хранения, системой маркировки и отслеживания лекарственных препаратов, контролем качества.	Реализация проекта за 7 месяцев;
ООО «МОЛЛ»	Ритейл	2020	Создание цифровой платформы для поддержания интенсивного роста компании и расширения присутствия в регионе.	Всего за 10 месяцев были внедрены система SAP S/4HANA и преднастроенное решение

				NOVARDIS Retail
ЗАО «Талосто»	FMCG (Товары повседневного спроса)	2006-2007	Повышение качества управления и автоматизации основных бизнес процессов предприятия.	Внедрение проекта за 12 месяцев
ООО «Группа Мегаполис»	Управляющая организация	2018	Увеличение пропускной способности логистической сети, повышение мощности склада и снижение ресурсных издержек за счет внедрения нового складского оборудования и его интеграции с промышленной WMS системой.	5,5 месяцев осуществлялось внедрение преднастроенного решения NOVARDIS EWM на базе SAP EWM
ООО «Охапка»	Ритейл	2021	Увеличение скорости и точности выполнения складских операций путем автоматизации основных бизнес процессов с интеграцией в существующую ERP систему.	Реализация проекта за 5,5 месяцев

В таблице 2 выведены цели заказчика к проекту. При сборе и обработке данных по компаниям были проанализированы проектные решения для конкретных требований предприятий- заказчиков. Нельзя сказать, что каждая компания решила внедрить систему SAP для одной цели. Например, для роста выручки, для роста спроса на товар, для улучшения прозрачности бизнеса. У каждой компании была индивидуальная цель в зависимости от масштабов деятельности и миссии компании. Все требования и желания заказчиков были выполнены в рамках проектов внедрения.

Для более детального анализа все цели и требования каждой компании были выявлены и преобразованы в единый вид. Была создана таблица, в

которой были зафиксированы 7 основных требований, которые были выдвинуты компаниями. Напротив, каждой цели для компаний были проставлены 0 (не зафиксирована цель) или 1 (цель была зафиксирована). Ниже представлена таблица с данными.

Таблица 3 – Данные для анализа компаний, которые внедрили SAP

Наименование предприятия	Отрасль предприятия	Цели и требования заказчиков						
		X1	X2	X3	X4	X5	X6	X7
АО «Фаберлик»	Сетевой маркетинг	0	1	1	0	0	0	0
ПАО «Северсталь»	Металлургия	1	0	1	0	0	0	1
ООО «Сеть Связной»	Ритейл	0	0	0	1	0	0	0
ООО «Рив Гош»	Ритейл	0	0	0	0	1	0	0
ПАО «Аптечная сеть 36,6»	Ритейл	1	0	0	0	0	0	0
ЗАО «Биокад»	Фармацевтика и биотехнологии	0	0	1	0	0	0	0
Группа компаний «Дамате»	Агро промышленность	1	0	0	1	1	0	0
ООО «Гиперглобус»	Ритейл	0	0	0	1	0	0	1
ООО «Объединенные Пивоварни Хейнекен»	FMCG (Товары повседневного спроса)	1	0	0	0	1	1	1
ТПО «Комус»	Ритейл	0	1	0	0	0	1	1
АО «Мегафон Ритейл»	Телекоммуникации	0	1	0	1	1	0	0
ПАО «МТС»	Телекоммуникации	1	1	0	0	0	0	0
Группа «М.Видео Эльдorado»	Ритейл	0	1	0	0	0	1	0
S Group	Ритейл	1	0	1	0	0	0	0
ООО «Воздушные Ворота Северной Столицы»	Транспорт	0	1	1	0	1	1	1
ООО «МОЛЛ»	Ритейл	0	1	0	0	0	1	0
ЗАО «Талосто»	FMCG (Товары повседневного спроса)	1	0	0	1	0	0	0
ООО «Восток Запад»	Оптовая торговля	0	1	0	1	1	0	0
ООО «Лента»	Ритейл	1	0	0	0	0	1	0

ООО «Группа Мегapolis»	Управляющая организация	0	1	0	0	1	1	0
ООО «Охалка»	Ритейл	1	1	0	0	0	0	0
ООО «Посуда Центр сервис»	Ритейл	1	1	0	0	0	1	0
ООО «Утконос»	Ритейл	1	1	0	0	0	0	0

При этом X1- Автоматизация бизнес-процессов, в том числе товарных позиций на интернет-магазине; X2 - Рост продаж; X3 - Рост объема заказов через интернет-магазин; X4 - Сокращение времени на бюджетирование, планирование; X5- Снижение затрат на производство; X6- Расширение доли рынка; X7- Прозрачность бизнеса.

Если осуществить суммирование 1 по каждому столбцу, то есть по каждому требованию, получатся следующие данные, представленные ниже в таблице.

Таблица 4 – Данные для анализа компаний, которые внедрили SAP

	X1	X2	X3	X4	X5	X6	X7
Итого	11	12	5	6	7	8	5

За счет расчетов по каждой цели, можно сказать, что приоритетной целью для многих компаний является X2 (рост продаж). Самый низкий приоритет в выборке отведен для X3 (Рост объема заказов через интернет-магазин) и X7 (Прозрачность бизнеса). Данный факт подтверждает индивидуальность требований для каждой компании.

Несмотря на то, что компании стараются минимизировать затраты для максимизации прибыли, при сборе и обработке данных по компаниям было выявлено, что требованием к новым ERP-системам SAP является улучшение прозрачности деятельности. В частности, при внедрении продукта SAP Commerce Cloud ПАО «Северсталь» отметила в качестве результата наличие прозрачного ценообразования. При внедрении в компанию ООО «Гиперглобус» продуктов SAP for Retail в качестве результата отмечалось повышение прозрачности всех бизнес-процессов. ООО «Объединенные Пивоварни Хейнекен» в качестве требований к новым ERP-системам выдвигало следующее: «Достижение прозрачности и повышение эффективности работы складов и сотрудников». Для АО «Мегафон Ритейл» результатом использования продуктов SAP стало оптимизация уровня товарных запасов и кардинальное повышение прозрачности цепочки поставок. Последним примером является компания ООО «Воздушные Ворота Северной Столицы», которое в качестве требований предъявило обеспечить прозрачность управления движимым и недвижимым имуществом.

Можно сказать, что требование прозрачности деятельности компании является актуальным для множества предприятий крупного бизнеса.

Вышеуказанные примеры говорят о том, что даже в рамках цели прозрачности бизнеса каждая компания может индивидуально определять цель, в зависимости от отрасли, миссии и стратегии компании.

Заключение

Проведенное исследование выявило дефицит отечественных исследований по проектному решению внедрения SAP-систем для компаний. Несмотря на то, что с каждым годом все больше крупных компаний начинает использовать ERP-систему SAP, данная система не является популярной в Российской Федерации из-за достаточно специфичного законодательства.

В статье описаны некоторые компании, которые уже внедрили ERP-систему в виде различных продуктов SAP. Было выявлено, что компании преследуют экономические цели, в виде роста продаж, сокращения затрат по основной деятельности. Однако такая цель, как улучшение прозрачности бизнеса, что является достаточно актуальной целью сегодня, также имеет популярность у крупных компаний.

Зарубежная ERP-система SAP, как показано в статье, является универсальным средством для различных целей предприятий. Внедрение продуктов системы SAP может обеспечить не только рост прибыли в рамках экономических целей, но и отсутствие пристальных проверок со стороны контрольных органов в рамках правовой цели.

Список использованных источников:

1. Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ (последняя редакция)
2. Савенкова Е.А., Горбунова О. Н. Особенности выбора ERP-системы для предприятия: статья. Социально – экономические явления и процессы Т. 13, № 1, 2018, стр. 117-121
3. Черненко В. А. Антикризисное управление: учебник / В.А. Черненко, Н. Ю. Шведова - С-П.: Гриф УМО СПО 2-е изд., 2019. - 410 с.
4. Shuyang Li, Fei Xing, Guo Chao Peng. (2019) Barriers of embedding big data solutions in smart factories: insights from SAP consultants. *Industrial Management & Data Systems* 119(5):P: 1147-1164
5. Madhavi Latha Nandi, Jacob Vakkayil (2018). Absorptive Capacity and ERP Assimilation: The Influence of Company-Ownership. *Business Process Management Journal* 24(3) DOI:10.1108/BPMJ-11-2016-0228
6. Sung J. Shim, Minsuk K. Shim (2020). Effects of User Perceptions of SAP ERP System on User Learning and Skills. *Journal of Computing in Higher Education* 32(2) P: 41-56

УДК 004.451.84:005.934

© Н.М. Мусин, П.Ю. Леонов, 2021

Обзор ERP-систем в контексте экономической безопасности бизнеса

Н.М. Мусин

аспирант 1 курса НИЯУ МИФИ, Москва

E-mail: polka.ru@mail.ru

П.Ю. Леонов

к.э.н., доцент кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: p.u.leonov@gmail.com

Аннотация: Что такое ERP-система и как внедрение данной системы в деятельность предприятия способно улучшить экономические аспекты общества, в том числе уровень экономической безопасности компании? Для того, чтобы разобраться в данном вопросе, необходимо изучить суть ERP-систем, а также их особенности и преимущества над другими системами.

Ключевые слова: ERP-система, оптимизация, информационные ресурсы.

Overview of ERP systems in the context of economic security of business

Abstract: What is an ERP system and how can the implementation of this system in the company's activities improve the economic aspects of society, including the level of economic security of the company? In order to understand this issue, it is necessary to examine the substance of ERP systems, as well as their features and advantages over other systems.

Keywords: ERP system, optimization, information resources.

Основная часть

В научной литературе можно найти расшифровку «ERP» как «планирование ресурсов предприятия». ERP-система является корпоративной информационной системой, которая содержит информацию о всех аспектах деятельности компании для повышения эффективности деятельности. Ресурсами выступает все, что подлежит учету, обработке и анализу.

Существует несколько теорий развития ERP-систем. В основном полагают, что развитие ERP началось в 1950-е годы, с появлением систем ROP (reorder point, точка заказа) и BOM (bill of materials, спецификация

изделия) с дальнейшей трансформацией в MRP (material requirement planning. планирование потребности в материалах). Ниже представлена наглядная схема развития ERP-систем.

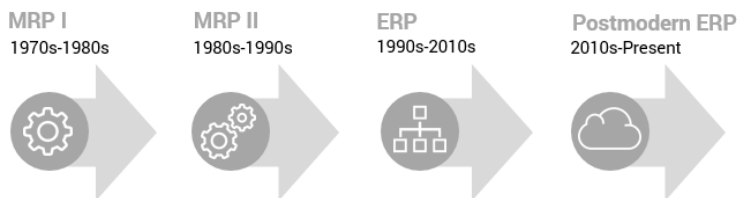


Рисунок 1 – История развития ERP-систем

ERP-система нужна, в основном, для сокращения «ручной» работы и транзакционных издержек за счет создания единого пространства для планирования и управления. Данное решение по внедрению и использованию ERP-систем актуально для предприятий, которые имеют несколько удаленных друг от друга филиалов или подразделений, с которыми центральному офису требуется вести оперативный обмен информацией.

Мировым лидером на рынке корпоративных приложений является SAP. У компании насчитывается более 440 000 клиентов в 180 странах мира. Однако SAP является международной системой, что требует адаптации различных систем, форм отчетности и единиц измерения к специфике конкретного рынка. Это является достаточно серьезным недостатком системы и требует дополнительных финансовых, трудовых и временных затрат.

Так же в списке лидеров находится Microsoft Dynamics AX (Ахapta) и Oracle ERP. Естественно, все указанные системы являются зарубежными системами, которые требуют доработок по реализации рыночной ситуации разных стран. Стоит отметить, что разработка дополнительных мер адаптации зарубежной ERP-системы требуется ввиду особенностей законодательства в каждой стране. У пользователей таких систем на территории России нередко встречаются трудности в связи с динамичным изменением законодательства. Например, Microsoft выпустила обновление для своей ERP-системы Ахapta только спустя 3 месяца после того, как уже была введена в действие ставка НДС 20%. Это создает определенные финансовые и налоговые риски. Поэтому чаще всего, отечественные организации выбирают ERP-системы Российских компаний.

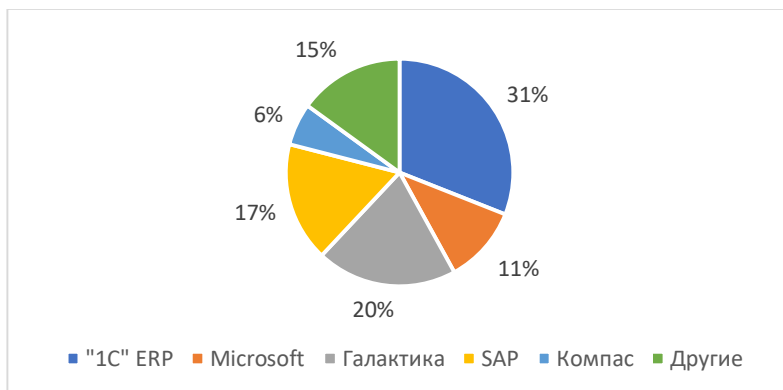


Рисунок 2 – Популярность ERP-систем

Выше представлены данные по ERP-системам которые используются в компаниях России. Безусловным лидером здесь являются различные ERP продукты фирмы «1С». Программа «1С» была разработана братьями Нуралиевыми в 1991 году. В те годы в России уже существовал ряд программ, которые отвечали бухгалтерским требованиям (как «Инфобухгалтер», «Парус», «Финансы без проблем» и т.п.). Однако система «1С» отличалась на тот момент достаточно мощной сбытовой сетью, что обеспечило лидерство программы на рынке.

В 1997 году был выпущен новый продукт «1С Предприятие». Данный продукт охватывал не только сферу бухгалтерского учета, но и другие сферы деятельности предприятий. Система «1С Предприятие» является достаточно универсальным средством автоматизации различных по смыслу задач.

Продукты фирмы ««1С»» предлагают полный функционал по шести основным модулям:

- Бухгалтерия;
- Управление проектами;
- Казначейство;
- Управление персоналом;
- Логистика;
- Производство.

Среди преимуществ использования ««1С»» стоит отметить наличие подробной документации о продукте с полным описанием функций подсистем и более низкие цены лицензий по сравнению с зарубежными аналогами. Однако существует ряд проблем, которые связаны с внедрением, интеграцией и использованием зарубежных ERP-систем:

- высокая стоимость внедрения и обслуживания;
- большая длительность сроков внедрения;
- высокая стоимость специалистов для поддержки, дополнительных разработок в программе;
- некачественное внедрение из-за нехватки специалистов;
- риски информационной и экономической безопасности;
- слабая адаптация и отсроченная реакция на изменения в местном законодательстве.

Сегодня спрос на программирование «1С» достаточно велик в России, а также в других странах мира возрастает интерес к данной ERP-системе. Например, «1С» на текущий момент в процессе внедрения в Европе, а в Африке достаточно долгий срок осваивают программу и успешно удаленно работают над ней программисты, адаптируя под собственные нужды. У «1С: Предприятия» есть два основных отличительных качества: функциональность и приемлемая цена на рынке.

В современных условиях экономическая безопасность организации приобретает первостепенное значение, так как она дает ориентир для принятия основных экономических решений. Экономическая безопасность - состояние защищенности экономики предприятия от внешних и внутренних угроз, при котором обеспечиваются экономическая независимость и условия для реализации стратегических приоритетов. В свою очередь экономическая безопасность организации – это обеспечение наиболее эффективного использования корпоративных ресурсов для предотвращения угроз и обеспечения устойчивого функционирования хозяйствующего субъекта в настоящее время и в будущем.

Использование в повседневной жизни инновационных технологий привело к ускорению товарно-денежного обращения, а также к увеличению масштабов переливов капиталов. Данные процессы, безусловно, оказывают положительное влияние на экономический рост. Однако, с другой стороны, данные процессы способны увеличить риски деятельности, а также расширить зону опасности для компаний и страны в целом.

Структура системы экономической безопасности состоит из следующих элементов:

- Концепция и стратегия безопасности – определяет приоритеты, интересы организации, которые реализуются посредством стратегий
- Угрозы в сфере экономики- внутренние и внешние, для определения угроз и степени реализации этих угроз вводятся индикаторы;
- Индикаторы экономической безопасности – это вероятность наступления внешних или внутренних угроз;

– Пороговые значения индикаторов экономической безопасности – используются, чтобы определить приоритеты в угрозах и свидетельствуют о том, что есть определенные изменения;

– Меры по обеспечению экономической безопасности.

Для оценки уровня экономической безопасности можно использовать различные инструменты и методики. Определение конкурентоспособности, как фактора роста экономической безопасности компании по методу М. Портера является достаточно информативным методом оценки экономической безопасности. М. Портер определил конкурентоспособность в виде способности определенной компании успешно конкурировать в конкретной бизнес-среде [3].

Стоит отметить, что метод пяти сил конкуренции М. Портера позволяет за короткое время понять уровень экономической конкуренции в том числе для проведения экспресс-анализа компании. Пять сил Портера включают в себя:

1. угроза появления продуктов-заменителей;
2. угроза появления новых игроков;
3. рыночная власть поставщиков;
4. рыночная власть потребителей;
5. уровень конкурентной борьбы.

Чтобы обеспечить экономическую безопасность, подкорректировав свою стратегию в зависимости от рассчитанного уровня экономической безопасности, компания может воздействовать на силы конкуренции путем эффективного использования своих корпоративных ресурсов. Ниже представлены виды корпоративных ресурсов:

- а) Капитал (позволяет поддерживать остальные корпоративные ресурсы);
- б) Персонал;
- в) Информация;
- г) Техника и технологии;
- д) Права.

Для повышения уровня экономической безопасности – обществу следует осуществлять мониторинг за обеспечением максимальной безопасности основных функциональных составляющих. Ниже приведены функциональные составляющие:

1. Финансовый аспект (зависит от учетной системы организации, связана с механизмами выявления угроз, методами снижения угроз, мониторинг среды, посредством которой осуществляется управление финансовыми показателями деятельности организации);

2. Интеллектуально-кадровый аспект (характеризует кадровую обеспеченность. На кадровую обеспеченность влияет отток кадров,

текучка кадров, низкая квалификация кадров, старение кадров, старение знаний и квалификации);

3. Техничко-технологический аспект (технологический потенциал и степень защищенности. Подрыв технологического потенциала, нарушение технологической дисциплины, моральное старение используемых технологий);

4. Политико-правовой аспект (недостаточная правовая защищенность интересов организации, договорной и прочей деловой документации)

5. Экологический аспект (угроза здоровью работников)

6. Информационный аспект (на уровень ЭБ влияет доля информации, которая является неполной и неточной или противоречивой, которая чувствует при принятии управленческих решений).

Эффективное использование корпоративных ресурсов, которые нужны для достижения целей и реализации миссии бизнеса, можно достигнуть путем предотвращения угроз негативного воздействия на экономическую безопасность организации, а также за счет достижения следующих целей экономической безопасности:

1. Обеспечение высокой финансовой эффективности работы предприятия, а также достижение финансовой устойчивости и независимости;

2. Обеспечение технологической независимости компании и достижение высокой конкурентоспособности технологического потенциала организации;

3. Высокая эффективность менеджмента в организации, оптимальность корпоративной структуры;

4. Высокий уровень квалификации персонала и эффективность корпоративных НИОКР;

5. Достижение высокого уровня экологичности работы компании (минимизация разрушительного влияния на окружающую среду);

6. Обеспечение качественной правовой защищенности всех аспектов деятельности компании;

7. Обеспечение защиты информационной среды организации, коммерческой тайны и высокий уровень информационного обеспечения всех её служб;

8. Обеспечение безопасности персонала организации, капитала, имущества и коммерческих интересов;

9. Экспертное структурирование;

10. Определение целей мониторинга;

11. Выбор постоянных индикаторов;

12. Сбор и обработка информации;

13. Предварительная формализация аналитических материалов;

14. Фильтрация и обработка информации, графическая визуализация данных;

15. Выявление закономерностей и устойчивых тенденций.

Стоит отметить, что проведение анализа состояния экономической безопасности осуществляется с учетом взаимосвязи экономических противоречий, угроз и потерь, к которым может привести реализация бизнес-стратегии.

ERP-системы позволяют реализовать компаниями различные цели, начиная с минимизации затрат, заканчивая улучшением уровня экономической безопасности и улучшением прозрачности бизнеса. Если на предприятии ведется учет не в автоматизированной системе, например, в Excel, возникает риск недостоверного ведения бухгалтерского учета, утечки информации, а также намеренное искажение финансовых показателей в целях личной выгоды. Также в данной ситуации возникает риск слабой системы внутреннего контроля, что позволяет увеличить количество выездных, налоговых и аудиторских проверок для подтверждения достоверности отчетности.

За счет сведения к минимуму участие человека в процессе ведения учета компании в системе ERP – происходит снижение различных рисков. При этом обеспечивается качество данных ввиду отсутствия человеческого фактора как со стороны наличия ошибок из-за невнимательности, так и со стороны отсутствия объективности и злоупотреблением служебным положением для своих целей (завышение или занижение каких-либо финансовых показателей в личных целях).

ERP-системы непосредственно влияют на информационные ресурсы, как элемент экономической безопасности. Это связано с тем, что при ведении учета в ERP-системах конечный пользователь может точно определить микро и макропоказатели для учета планирования и текущих бизнес-процессов. В этой связи, увеличение числа компаний, которые пользуются ERP-системами, позволяет улучшать уровень экономической безопасности, в общем и целом, на уровне страны.

Несмотря на достаточное количество ERP-систем и схожий принцип работы ERP-систем, каждая компания использует или внедряет ERP-системы в рамках индивидуального подхода, преследуя собственные цели в рамках стратегии компании. Ведение бухгалтерского, налогового, статистического учета в ERP-системах позволяет компании оптимизировать затраты, автоматизировать ряд процессов (на складе, в сфере закупок, логистике и т.д.), а также, как итоговая цель, позволить компании получить больше прибыли, сохраняя непрерывность деятельности.

Заключение

Вопрос автоматизации и оптимизации бизнес-процессов может решить внедрение ERP-системы в компании. При использовании автоматизированной системы для ведения различных видов учета на предприятии повышается качество отчетности; улучшается прозрачность бизнеса; сокращаются проверки со стороны надзорных органов; улучшается инвестиционная привлекательность общества; сокращаются затраты на производство. Все это позволяет улучшить экономическую безопасность, как на предприятии, так и в стране за счет экономических единиц – предприятий.

Список использованных источников:

1. Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ (последняя редакция)
2. А. А. Борькина, А. К. Конищева. История возникновения «1С: ПРЕДПРИЯТИЕ» // Кузбасский государственный технический университет имени Т. Ф. Горбачева» г. Кемерово, 2016 г. VIII Всероссийская научно-практическая конференция молодых ученых с международным участием «Россия молодая»
3. Портер М. Конкурентная стратегия: Методика анализа отраслей и конкурентов / Пер. с англ. 2018, С 198.
4. Степанов Д.Ю., Бикашов И.Д. Evolution of russian ERP-systems market // Фундаментальные проблемы радиоэлектронного приборостроения. – 2016. – т.16, №1. – с.244-247
5. Савенкова Е.А., Горбунова О.Н. Особенности выбора ERP-системы для предприятия // Текст научной статьи по специальности «Экономика и бизнес» - 2018 г. – 15-19
6. Практика применения ERP-систем. – М.: «Альпина – паблишер», - 2017 г. – с. 4.

Обнаружение поддельных и не поддельных DDoS-атак и их отличие от слэшдот-эффекта

В.А. Рычков

старший преподаватель кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: VARychkov@mephi.ru

Д.М. Якупов

студент 2 курса НИЯУ МИФИ, Москва

E-mail: dante2597@mail.ru

В. Давыденко

старший преподаватель кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: VIDavydenko@mephi.ru

Аннотация: Технология распределенных вычислений широко используется бизнес-приложениями на базе Интернета. Управление цепочками поставок (SCM), управление взаимоотношениями с клиентами (CRM), электронная коммерция и банковское дело - приложения, которые используют распределенные вычисления. Эти приложения являются основной мишенью для массовых атак, известных как распределенный отказ в обслуживании (DDoS), которые приводят к отказу в обслуживании или ухудшению качества предоставляемых услуг. Серверы, предоставляющие надежные услуги подлинным пользователям в распределенной среде, становятся жертвами таких атак, которые выдают появляющиеся поддельные запросы за подлинные. Слэшдот-эффект, с другой стороны, - это огромное количество трафика, вызванного определенными флэш-событиями (FES), которые имитируют DDoS-атаки. Обнаружение DDoS-атак - сложная проблема, требующая решения. Существующие решения, как правило, предназначены либо для слэшдот-эффекта, либо для DDoS-атак, и необходимы дополнительные исследования, чтобы разработать комплексный подход для удовлетворения потребностей в обнаружении поддельных и не поддельных вариантов DDoS-атак.

Ключевые слова: DDoS -атаки, флэш-событие, энтропия, обнаружение DDoS -атаки, распознавание ddos-атак по флэш-событию.

Detection of counterfeit and non-counterfeit DDoS attacks and how they differ from flash crowds

Abstract: Distributed computing technology is widely used by Internet-based business applications. Supply Chain Management (SCM), customer relationship management (CRM), e-commerce and banking are applications that use distributed computing. These applications are the main target for mass attacks known as distributed denial of service (DDoS), which lead to denial of service or deterioration of the quality of services provided. Servers that provide reliable services to genuine users in a distributed environment become victims of such attacks that pass off fake requests that appear as genuine. The flash crowds, on the other hand, is a huge amount of traffic caused by certain flash events (FES) that simulate DDoS attacks. Detecting DDoS attacks as a result of a crowd of people is a complex problem that needs to be solved. Existing solutions are usually designed for either a flash crowds or DDoS attacks, and more research is needed to develop a comprehensive approach to meet the needs for detecting fake and non-fake DDoS attack variants.

Keywords: DDoS attacks, flash event, entropy, detection of a ddos attack, discrimination of DDoS from a flash event.

Интернет стал основой многих приложений, где расположение серверов не имеет значения с точки зрения пользователя. В последнее десятилетие многие серверы в распределенной среде подверглись массовой атаке на отказ в обслуживании, известной как распределенный отказ в обслуживании (DDoS-атака). DDoS-атаки происходят, когда большое количество скомпрометированных систем направляет запросы на один или несколько веб-серверов в распределенной среде. Flash crowd - это еще один сценарий трафика в распределенной среде, который напоминает DDoS движение. Тем не менее, слэшдот-эффект - это подлинный трафик из законных систем, но трафик в большей степени обусловлен событием вспышки [1]. Оба трафика выглядят одинаково, за исключением таких случаев, как цели доступа, скорость уменьшенного или увеличенного трафика и распределение IP-адреса источника.

Цель доступа в этих двух случаях различна, поскольку слэшдот-эффекты являются естественными потоками последних новостей, в то время как трафик DDoS является результатом массовой атаки типа "отказ в обслуживании" (DOS). Распределение исходного IP-адреса с реальным DDoS-атака ограничена только скомпрометированными узлами.

Что касается слэшдот-эффекта, увеличение или уменьшение скорости движения происходит постепенно, поскольку распространение происходит медленно. С другой стороны, DDoS-атака вызывает интенсивный трафик,

который поступает очередями. Увеличение трафика происходит в короткие сроки.

Очень большое количество людей внесли свой вклад в обнаружение DDoS- атак и их отличие от слэшдот-эффекта. В атаках на основе веб-прокси действуют от имени реальных источников атаки, распределенный характер атаки все еще существует, поскольку в большинстве реальных сетевых сценариев используется архитектура среднего прокси-сервера, которым злоупотребляют. В исследовании обнаруживают аномальное поведение прокси-сервера путем сравнения его текущего поведения с его историческим профилем поведения без учета других прокси-серверов, участвующих в той же атаке, обнаружение распределенных HTTP-атак на основе веб-прокси может быть преобразовано в ряд относительно независимых задач. Таким образом, в реальном сетевом сценарии система обнаружения может работать параллельно для повышения эффективности обнаружения. [2]. DDoS-атаки на уровне приложений были обнаружены и предотвращены, были использованы обученный алгоритм искусственной нейронной сети для обнаружения DDoS-атак TCP; UDP и ICMP на основе характерных признаков, которые отделяют подлинный трафик от DDoS-атак. Процесс был начат с воспроизведения сетевой среды, которая является зеркальным отражением реальной жизненной среды. Затем были запущены различные DDOS-атаки, в то время как обычный трафик проходил через сеть. Наборы данных были собраны, предварительно обработаны и подготовлены для обучения алгоритма. Затем механизм обнаружения был интегрирован с помощью Snort-AI, где он был протестирован на известных и неизвестных DDoS-атаках.[3]. Метод частичной ранговой корреляции используется для обнаружения как низкоскоростных, так и высокоскоростных DDoS-атак. Как только вредоносный трафик обнаружен на основе значения ранга, полученного в результате оценки, происходит запрос пограничного маршрутизатора прекратить перенаправление трафика на нижестоящие маршрутизаторы.

Подход, основанный на фильтрации, где маршрутизаторы выполняют фильтрацию нежелательного трафика с понятием распространения фильтра. Фильтрация использует количество горячих точек, доступность ресурсов маршрутизатора и степень связи маршрутизатора. Это означает, что маршрутизатор, который находится близко к злоумышленникам, действительно имеет больше ресурсов и демонстрирует больше соединений с соседями. Поскольку фильтры работают совместно друг с другом в распределенной среде, этот метод демонстрирует более высокий коэффициент блокировки атак.[5]

У всех этих методов есть свои плюсы в том, то они решают задачу выявления атак различными способами, но минусы в том, что ни один из

методов не показывает, как выявить отличия DDos – атак от слэшот-эффекта. Необходим системный подход к выявлению различий. Нужно разработать методологию, которая будет учитывать множественную динамику трафика, включая энтропию источника, энтропию трафика и различные пороговые значения для хорошего понимания и обнаружения DDos – атак и отличия их от слэшдот – эффекта.

Список использованных источников:

1. Прасад, К.М., Редди, АРМ, Рао, К.В. (2010). Дискриминация трафика DDoS-атак из флеш-толпы на мониторах интернет-угроз (ITM) с использованием энтропии вариации. IEEE., 6, 1–10.
2. С.Ж.Хмылев. Распределенные атаки типа DDoS. Анализ, метод обнаружения и защиты. – М.:LAP, 2015.- 65 с.
3. Щерба Е. В., Щерба М. В. Разработка архитектуры системы обнаружения распределенных сетевых атак типа «отказ в обслуживании» // Омский научный вестник. Сер. Приборы, машины и технологии. 2012. № 3 (113). С. 280–283.
4. Wang H., Zhang D., and Shin K. G. Detecting SYN flooding attacks // Proc. IEEE INFOCOM'2002. New York City, 2002. P. 1530–1539.
5. Seo, D, Lee, H, Perrig, A. (2013). APFS: Adaptive Probabilistic Filter Scheduling against distributed denial-of-service attacks. Comput. Secur., 39(part B), 366–385 Elsevier.

**Описание проведения оценки рисков финансирования
распространения оружия массового уничтожения и предложение мер
по их минимизации**

Д.Д. Жусупов

студент 6 курса НИЯУ МИФИ, Москва

E-mail: jusupov.daniar.98@gmail.com

Аннотация: Выявление, оценка и понимание рисков ФРОМУ на регулярной основе имеет важное значение для укрепления способности страны предотвращать сбор, хранение, перемещение и использование средств, а, следовательно, и других финансовых активов лицами и организациями, причастными к распространению оружия массового уничтожения.

Ключевые слова: ФРОМУ, оценка рисков, целевые финансовые санкции, угрозы и уязвимости, ФАТФ.

**Description of the assessment of the risks of financing the proliferation
of weapons of mass destruction and the proposal of measures to minimize
them**

Abstract: Identifying, assessing and understanding the risks of FPWMD on a regular basis is essential to strengthen a country's ability to prevent the raising, storing, moving, and using funds, and thus other financial assets, by individuals and organizations involved in the proliferation of weapons of mass destruction.

Keywords: FPWMD, risk assessment, targeted financial sanctions, threats and vulnerabilities, FATF.

Введение

В октябре 2020 года ФАТФ внесла изменения в Рекомендацию 1 и Пояснительную записку к Рекомендации 1, включив в них требование, согласно которому страны, финансовые учреждения и УНФПП должны проводить оценки рисков финансирования распространения оружия массового уничтожения (далее - ФРОМУ), как они определены в Рекомендациях ФАТФ [1, с.11]. Это означает, что теперь надзорные органы обязаны рассматривать, в какой степени субъекты, в отношении которых они осуществляют мониторинг, подвержены рискам ФРОМУ, и как они обеспечивают эффективное применение целевых финансовых санкций

(ЦФС). Однако, не все государства завершили свои оценки отмыwania денежных средств и финансирования терроризма (далее – ОД/ФТ). Соответственно, возникают вопросы об алгоритме проведения национальной оценки рисков (далее – НОР) ФРОМУ. В данной статье будет описана методика проведения оценки рисков финансирования распространения (далее – ФР), а также меры по их минимизации.

Риски

Стоит отметить, что риск ФРОМУ аналогичен риску ОД/ФТ и его можно рассматривать как функцию трех факторов: угрозы, уязвимости и последствий.

Еще одна концепция, актуальная для любого процесса оценки риска, - это понимание присущего (неотъемлемого) и остаточного рисков и применение этих концепций конкретно к ФРОМУ аналогично тому, как страны/сектора уже сделали это для рисков ОД/ФТ [2, с.13].

Под присущим риском понимается естественный уровень риска до введения каких-либо мер по минимизации. Понимание присущего риска, хотя оно и не требуется и не указано в Рекомендациях, важно и полезно, поскольку оно может способствовать соответствующему пониманию и оценке эффективности мер контроля, а в случае, если меры контроля не вводятся, влияние такого риска на государство/сектор.

Остаточный риск относится к уровню риска, который остается после процесса применения мер по его смягчению. Понимание остаточного риска позволяет государству/сектору определить, эффективно ли они управляют рисками ФР в рамках своей юрисдикции или деловых операций. Высокая степень остаточного риска может указывать на то, что меры контроля неэффективны.

Угрозы, уязвимости и последствия

Под угрозой в контексте ФРОМУ понимаются лица или организации, которые имеют потенциал нанести вред государству, обществу, экономике и т.д. В качестве угрозы может выступать существование организованных преступных группировок, которые ведут деятельность по распространению/финансированию ОМУ.

Под уязвимостью понимаются факторы, которые способствуют реализации угрозы. Для страны эти уязвимости могут включать недостатки в законах или нормативных актах, или контекстуальные особенности, которые могут предоставить злоумышленникам возможности для сбора или перемещения средств. Например, юрисдикция со слабым контролем ПОД/ФТ или государство, которое не собирает информацию о бенефициарных владельцах, и имеет высокий уровень преступности, контрабанды, мошенничества или другой незаконной деятельности.

Последствия относятся к результату, когда средства или активы становятся доступными для нарушителей, что в конечном итоге может позволить им, например, получить необходимые материалы, предметы или системы для разработки и обслуживания систем незаконного ядерного, химического или биологического оружия (или средства их доставки).

Этапы оценки рисков

Определившись с терминологией, наступает этап проведения оценки рисков. В целом, можно сказать, что оценка рисков ФРОМУ – это процесс, основанный на методологии, согласованной вовлеченными сторонами, которая пытается идентифицировать, анализировать и понимать соответствующие риски с целью разработки превентивных мер. Подобно процессу оценки рисков ОД/ФТ, здесь должны быть обоснованные суждения об угрозах, уязвимостях и последствиях на основе тщательного анализа информации, доступной государству/сектору. Что касается НОР ФР, то она должна быть достаточно всеобъемлющей, чтобы в дальнейшем способствовать разработке национальной стратегии борьбы с распространением ОМУ и эффективному применению мер противодействия. Конечная цель проведения оценки риска финансирования распространения - обеспечить полное выполнение требований ФАТФ с соответствующими резолюциями Совета Безопасности ООН [3, с.2]. С точки зрения масштабов, оценка ФРОМУ может быть более целенаправленной, чем у ОД/ФТ (например, потому что масштаб оцениваемого риска более узкий, чем у ОД/ФТ).

Поскольку в процессе оценки риска участвует ряд агентств и заинтересованных сторон и часто он растягивается на определенный период времени, в целом было бы полезно разделить процесс на схожие с ОД/ФТ этапы: (1) предварительная оценка; (2) планирование и организация; (3) выявление угроз и уязвимостей; (4) анализ; (5) оценка; (6) разработка и имплементация мер противодействия.

Предварительное исследование

Странам/секторам настоятельно рекомендуется сначала провести предварительное исследование, чтобы определить цели, объем и направленность оценки до ее начала. В этом же пункте рассматриваются различные методологии оценивания и вопрос их применения. Государство/сектор может принимать во внимание свои внутренние обстоятельства, включая уникальный профиль национальных угроз и уязвимостей, национальный контекст противодействия ФРОМУ и стратегии развития.

Планирование и организация

Систематический и последовательный процесс имеет решающее значение для содержательной оценки рисков. До проведения оценки

рисков государство/сектор могут подготовить план проекта и определить членов комиссии из различных ведомств/департаментов. К тому же очень важным шагом будет включение в план и представителей частных организаций, так как они непосредственно имеют дело с злоумышленниками. Государство/сектор может также разработать механизм для сбора и последующего анализа и обновления данных и для документирования результатов. Так как большая часть данных будет конфиденциального характера, можно разработать протокол по обмену информацией через закрытые сессии-брифинги. Кроме того, страны могут рассмотреть вопрос о том, чтобы сделать общедоступными результаты своей оценки рисков ФРОМУ, где это возможно, а также разработать защищенную платформу для постоянного взаимодействия, консультаций и обмена информацией с финансовыми и нефинансовыми предприятиями. Публикация и обмен такой информацией будет способствовать пониманию рисков ФР и соблюдению требований ФАТФ.

Идентификация угрозы

Хорошей основой для процесса идентификации как для национальных, так и для секториальных оценок рисков ФР является составление списка известных или предполагаемых угроз; ключевые секторы, продукты или услуги, которые использовались; виды деятельности, подверженные ФРОМУ; и основные причины, по которым указанные лица и организации не лишаются своих активов или не идентифицируются. Это особенно полезно, поскольку требования Рекомендации 7 и касаются не только определенных физических и юридических лиц, но также лиц, действующих от их имени.

Хотя методология выявления угроз ФРОМУ может быть аналогична методологии ОД/ФТ, государства/секторы должны учитывать, что природа их угроз значительно отличается. В отличие от угроз ОД и ФТ, угрозы ФР могут исходить от физических и юридических лиц, обозначенных согласно соответствующим резолюциям Совета Безопасности ООН (например, КНДР и Иран) [4, с. 65], и от международных сетей, созданных ими для сокрытия своей деятельности; а также могут быть косвенно связаны с указанными лицами и организациями. В результате финансовые потребности и методы обозначенных физических и юридических лиц могут не обязательно совпадать с потребностями отмывателей денег и террористов. Также необходимо учитывать, что ФР может быть получено как в результате законной, так и незаконной. Примеры использования законной деятельности могут включать закупку или торговлю товарами двойного назначения, подлежащими экспортному контролю, или торговлю природными ресурсами в нарушение соответствующих резолюций Совета Безопасности ООН. Что касается незаконной деятельности, примеры могут

включать контрабанду наличных денег, золота и других ценных товаров, киберпреступления, незаконный оборот наркотиков, экспорт оружия и природных ресурсов, таких как песок, и т. д. Эти действия могут происходить в нескольких юрисдикциях. Часто в данных схемах используются подставные лица и компании.

Стране/сектору необходимо понимать, что профиль рисков и масштабы угроз ФР будут отличаться от соседних государств. Поэтому рекомендуется применять целостный подход при сборе информации об угрозах и использовать доступные источники информации, относящиеся к внутренним, региональным и международным угрозам ФРОМУ. Отсутствие прецедентов, связанных с ФР, не обязательно означает, что риски имеют низкий уровень.

Идентификация уязвимости

После составления списка угроз следующим шагом является составление списка основных уязвимостей. Подобно ОД/ФТ, эти уязвимости могут быть основаны на ряде факторов, таких как структурные, отраслевые, продукт или сервис, клиенты и транзакции.

Под структурными уязвимостями понимаются слабые места в национальной системе борьбы с распространением, которые делают страну или сектор привлекательными для злоумышленников. Сюда входит:

1. Слабое управление, неэффективный надзор, экспортный контроль и/или режимы регулирования, слабая осведомленность о рисках;
2. Отсутствие законодательной базы противодействия ФРОМУ, а также проблемы с реализацией Резолюции Совета Безопасности ООН и Рекомендаций ФАТФ;
3. Наличие значительного уровня организованной преступности, коррупции или другой противоправной деятельности;
4. Неэффективный внутренний контроль;
5. Отсутствие межведомственного сотрудничества.

Отраслевые уязвимости относятся к контекстуальным особенностям конкретного сектора. Слабые стороны, такие как низкий уровень осведомленности о рисках ФР, понимание требований ЦФС и общая слабая культура соблюдения требований в секторе, представляют собой уязвимые места.

Основываясь на имеющемся опыте оценки рисков ОД/ФТ, страны склонны уделять больше внимания банковскому сектору или сектору денежных переводов или ценностей, поскольку преступникам необходим доступ к международной финансовой системе для обработки платежей за компоненты или материалы из-за рубежа. Однако недавние типологии подчеркнули [5, с. 42], как другие секторы сталкиваются с эксплуатацией со стороны преступников, с целью осуществления ФР. Таким образом,

страны должны знать, какие части экономики подпадают могут подвергаться ФРОМУ. Примером могут служить:

1. Поставщики трастовых и корпоративных услуг;
2. Торговцы драгоценными металлами и камнями: предоставление преступникам альтернативного метода тайного перемещения финансовых ресурсов через международные границы;
3. Поставщики услуг виртуальных активов: предоставление продуктов определенным лицам и организациям, которые были добыты и украдены, и предоставление платформы для мгновенного перемещения денежных сумм через международные границы [6, с. 35];
4. Морской сектор: указанные лица и организации также эксплуатируют морской сектор, который предоставляет им средства для доставки компонентов и материалов для использования в ОМУ.

Уязвимости продукта или услуги означают является ли продукция или услуга, предоставляемая финансовым учреждением или УНФПП, сложной по своей природе, имеет ли трансграничный охват, легко ли доступен для клиентов.

Выявление уязвимостей клиентов и транзакций имеет решающее значение для оценки рисков, проводимой финансовым учреждением или УНФПП. В качестве отправной точки они могут рассмотреть возможность пересмотра количества клиентов, которые уже определены как группы высокого риска, особенно тех, которые часто осуществляют трансграничные операции с участием юридических лиц и образований, или нескольких подставных компаний. Информация о типе и личности клиента, а также о характере, происхождении и цели взаимоотношений также имеет значение. Другие соображения включают: количество, сумму (особенно наличными) и частоту транзакций: (1) исходящие, проходящие транзитом или предназначенные для зарубежной юрисдикции, которая плохо выполняет соответствующие обязательства Резолюции Совета Безопасности ООН и Рекомендации ФАТФ, слабое управление, закон; (2) с участием лиц, действующих от имени юридического лица или образования (например, уполномоченного лица с подписью, директора); (3) которые не связаны с заявленным профилем бизнеса частной фирмы.

Источниками информации при определении угроз и уязвимостей служат типологии, национальные оценки рисков, наднациональные оценки рисков, соответствующие отраслевые отчеты, надзорные отчеты, результаты внутреннего аудита, отчеты о взаимных оценках.

Стоит отметить, что уже на данном этапе можно составить соответствующие индикаторы риска.

Индикаторы риска профиля клиента:

- При приеме на обслуживание клиент предоставляет расплывчатую или неполную информацию о предполагаемой торговой деятельности. Клиент неохотно предоставляет дополнительную информацию о своей деятельности при запросе;

- Клиент включен в Санкционные перечни или имеется информация в СМИ, где раскрываются его прошлые схемы ОД, мошенничества, другая преступная деятельность или текущие или прошлые расследования или обвинительные приговоры;

- Клиент - это лицо, имеющее дело с товарами двойного назначения или товарами, подлежащими экспортному контролю, или он имеет сложное оборудование, для работы с которыми у него нет технической подготовки или которые несовместимы с заявленным направлением его деятельности;

- Клиент, связан с университетом или исследовательским учреждением и участвует в торговле товарами двойного назначения или товарами, подлежащими экспортному контролю.

Индикаторы риска активности счета и транзакции

- Отправитель или получатель транзакции - это физическое или юридическое лицо, проживающее в стране, вызывающей озабоченность в связи с распространением ОМУ (например, КНДР и Иран);

- Операции по счету или транзакции, в которых отправитель или получатель находится в стране со слабым выполнением соответствующих обязательств Резолюции Совета Безопасности ООН и Рекомендаций ФАТФ или со слабым режимом экспортного контроля (также имеет отношение к корреспондентским банковским услугам);

- Клиент использует личную учетную запись для покупки промышленных товаров, находящихся под экспортным контролем или иным образом не связанных с корпоративной деятельностью или соответствующими направлениями бизнеса.

Индикаторы риска морского сектора:

- Торговая организация регистрируется по адресу, который может быть адресом массовой регистрации, например, жилые дома с высокой плотностью населения, адреса почтовых ящиков, коммерческие здания или промышленные комплексы, особенно когда нет ссылки на конкретную единицу;

- Физическое или юридическое лицо, готовящее отгрузку, указывает транспортно-экспедиторскую фирму в качестве конечного пункта назначения продукта;

- Пункт назначения поставки отличается от местонахождения импортера;

- Несоответствия выявляются в контрактах, счетах-фактурах или других торговых документах, например, противоречия между названием экспортирующей организации и названием получателя платежа; разные цены в счетах-фактурах и соответствующих контрактах; или несоответствия между количеством, качеством, объемом или стоимостью реальных товаров и их описанием;

- Отгрузка товаров имеет низкую заявленную стоимость по сравнению со стоимостью доставки;

- Отгрузка товара несовместима с техническими возможностями страны, в которую он направляется (например, отправка оборудования для производства полупроводников в страну, не имеющую электронной промышленности)

- Отгрузка товаров несовместима с обычными географическими моделями торговли, например, страна назначения обычно не экспортирует и не импортирует товары, перечисленные в документах торговых сделок;

- Доставка товаров осуществляется через страну со слабым выполнением соответствующих обязательств по Резолюции Совета Безопасности ООН и Рекомендаций ФАТФ, законов об экспортном контроле;

Другие индикаторы:

- Клиент просит выставить аккредитив для осуществления операции, ожидая признания нового счета правильным.

- Поручения по платежу или оплата от, или в адрес сторон, не указанных в исходном аккредитиве или другой документации.

Анализ

На этом этапе страны, финансовые учреждения, УНФПП и ПУВА должны стремиться понять природу, источники, вероятность и последствия идентифицированного риска. В рамках этого процесса им следует присвоить относительную ценность или важность каждому из этих рисков и расставить приоритеты между идентифицированными рисками.

Оценка

В результате анализа рисков необходимо классифицировать их по одной из следующих категорий: низкий, средний или высокий, с возможными комбинациями между различными категориями (например, умеренный, повышенный). Эта классификация призвана помочь в понимании и расстановке приоритетов рисков ФР. Результаты оценки риска должны быть доведены до сведения компетентных органов (включая надзорные органы) и соответствующего персонала соответствующих фирм частного сектора.

На национальном уровне компетентные органы должны создать и внедрить национальную законодательную базу, а также политику по

устранению выявленных рисков. Они могут также рассмотреть возможность публикации результатов оценки по мере необходимости, чтобы способствовать более широкому пониманию субъектами первичного финансового мониторинга.

Рекомендации ФАТФ требуют, чтобы юрисдикции поддерживали актуальную оценку своих рисков ФР. Подобно ОД/ФТ, оценка рисков ФРОМУ должна регулярно обновляться и быть развивающимся процессом с учетом текущих угроз и требований санкций в отношении потенциального нарушения.

Меры по смягчению, принимаемые странами

– Меры по минимизации рисков включают в себя следующие элементы:

– НОР: оценки рисков на национальном уровне могут быть полезны для информирования и укрепления системы ПОД/ФТ в стране.

– Секториальные оценки: финансовые учреждения, УНФПП и ПУВА должны предпринимать соответствующие шаги для выявления и оценки своих рисков ФРОМУ. Они обязаны документировать эти оценки, чтобы иметь возможность продемонстрировать их основу, поддерживать в актуальном состоянии и иметь соответствующие механизмы противодействия. Степень любой оценки рисков ФРОМУ должна соответствовать характеру и размеру бизнеса.

– Эффективная правовая база: странам необходимо эффективные правовые рамки для безотлагательного введения ЦФС за распространение ОМУ в соответствии с Рекомендацией 7. Им следует создать и определить соответствующие компетентные органы, ответственные за применение и обеспечение соблюдения требований ФАТФ в отношении ФРОМУ. Четкие институциональные механизмы, процессы и обязанности помогут властям сосредоточить внимание на уязвимых областях и выявить средства, с помощью которых указанные лица и организации могут уклоняться от санкций в различных секторах. Это помогло бы им применять соответствующие меры (например, обеспечение отказа в финансировании, замораживания средств и активов и наказания за нарушения).

– Страны также должны иметь соответствующие базы данных и поддерживать их обновления.

– Внутреннее сотрудничество, координация и обмен информацией: в соответствии с Рекомендацией 2 и Пояснительной запиской к ней, страны должны иметь межведомственную структуру для более эффективного снижения рисков финансирования распространения. Тесное сотрудничество и координация между компетентными органами будет способствовать обмену соответствующей информацией. Это могло бы

помочь инициировать и продолжить параллельные финансовые расследования.

- Финансовые учреждения, УНФПП и ПУВА должны подлежать надзору или мониторингу для обеспечения полного соблюдения ими своих обязательств. Несоблюдение должно повлечь за собой соответствующие гражданские, административные или уголовные санкции, если это необходимо. Частота, глубина и интенсивность таких механизмов надзора или мониторинга, а также уровень санкций, применяемых в случае несоблюдения требований, следует периодически пересматривать, чтобы гарантировать, что риски адекватно рассматриваются и смягчаются.

- Регулярное и углубленное обучение (проводимое как государственным, так и частным сектором).

При наличии низких рисков финансовые учреждения и УНФПП, не должны тратить значительное количество времени и ресурсов на их снижение.

Надзор за оценкой и снижением рисков фр

ФАТФ разработала отдельное руководство по риск-ориентированному надзору [7, с.15], чтобы объяснить, как проверяющие органы должны применять риск-ориентированный подход при проверке финансовых учреждений, УНФПП и ПУВА. Хотя это Руководство сосредоточено на ПОД/ФТ, органам следует рассмотреть возможность учета соответствующих аспектов этого документа при разработке своих надзорных подходов при смягчении рисков финансирования распространения ОМУ. Исходя из данного Руководства, можно построить следующие соображения:

1. Надзорные органы должны систематически выявлять и оценивать уровень риска в различных секторах и отдельных организациях, принимая во внимание их подверженность рискам ФРОМУ и эффективность их внутреннего контроля;

2. Классификация субъектов первичного финансового мониторинга по риску ФРОМУ должна приниматься во внимание наряду с другими параметрами, используемыми надзорными органами, при определении интенсивности и частоты надзора. Например, учреждения с более низким уровнем риска должны привлекать меньше внимания надзорных органов;

3. Компетентные органы должны поддерживать динамичный процесс оценки рисков, используя доступную информацию и данные как из внутренних, так и из внешних источников, в рамках своего постоянного надзора и мониторинга организаций;

4. Компетентные органы должны проверить, адекватно ли учреждения применяют меры НПК, идентификации/верификации, понимают ли они характер и цели взаимоотношений с клиентами, так как

необходимо разработать профили рисков клиентов и проводить постоянный мониторинг, на этой основе.

5. Надзорные органы должны предпринять шаги (например, разъяснительная работа, руководство, обмен информацией) для обеспечения того, чтобы их поднадзорные учреждения понимали свои риски и применяли соразмерные меры;

6. Надзорным органам следует учитывать возможности и опыт финансирования противодействия распространению ОМУ поднадзорных учреждений и отдельных секторов, а также их понимание обязательств при разработке своих надзорных программ;

7. На основе оценки рисков проверяющие органы должны определить методологию и процедуры надзорной деятельности, включая типы используемых инструментов (например, анкеты, внешняя отчетность, интервью, выборочное тестирование, выездные визиты);

8. В частности, для УНФПП надзорные и саморегулирующие органы должны учитывать уязвимости, связанные с услугами по регистрации компаний, которые обычно предоставляются поставщиками услуг, юристами и бухгалтерами;

9. При выявлении слабых мест надзорные органы должны отслеживать и оценивать надежность мер, предпринятых для исправления недостатков;

10. В случае нарушений нормативных требований, возникающих в результате их несоблюдения, надзорные органы должны иметь в наличии широкий спектр мер: административные санкции, отзыв лицензий и т. д. Надлежащее правоприменение может стимулировать культуру соблюдения среди поднадзорных организаций.

Заключение

Таким образом, несмотря на то, что понятие финансирования распространения оружия массового уничтожения существовал с момента внедрения 40 Рекомендаций ФАТФ, особое внимание он получил именно после пересмотра 1-й Рекомендации в 2020 году. Если же раньше необходимо было проводить НОР в части ОД и ФТ, то сейчас растет актуальность в проведении подобной процедуры в отношении ФРОМУ. Такое положение обуславливает необходимость проведения постоянного мониторинга факторов и условий, определяющих состояние режима нераспространения ОМУ, а также поддержания системы ПОД/ФТ на должном уровне в целях обеспечения безопасности государств.

Список использованных источников:

1. Рекомендаций, ФАТФ, октябрь 2020 г. [Электронный ресурс] – Режим доступа. URL: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>
2. Руководство по оценке рисков финансирования терроризма, ФАТФ, 2019 г. [Электронный ресурс] – Режим доступа. URL: <https://eurasiangroup.org/files/uploads/files/otcet-fatf-rukovodstvo-po-ocenke-riskov-finansirovania-terrorizma-iul-2019.pdf>
3. Резолюция Совета Безопасности ООН 1540, Совет Безопасности, 2004 г. [Электронный ресурс] – Режим доступа. URL: <https://undocs.org/ru/S/RES/1540%282004%29>
4. Окончательный доклад группы экспертов во исполнение Резолюции 2276, ООН, 2017 г. [Электронный ресурс] – Режим доступа. URL: https://www.un.org/ga/search/view_doc.asp?symbol=S/2017/150
5. Отмывание денег посредством торговой деятельности, ФАТФ, 2020 г. [Электронный ресурс] – Режим доступа. URL: https://eurasiangroup.org/files/uploads/files/other_docs/FATF%20docs/Tra-de-Based-Money-Laundering-Trends-and-Developments_rus.pdf
6. Второй 12-месячный анализ выполнения пересмотренных Стандартов ФАТФ, касающихся виртуальных активов и провайдеров услуг в сфере виртуальных активов, ФАТФ, 2021 г. [Электронный ресурс] – Режим доступа. URL: <https://mumcfm.ru/storage/mediateka/K3ZerFusUq0gmdsSU5qZML2fHJNl oxWFcjOPu6W6.pdf>
7. Руководство по применению риск-ориентированного подхода в надзорной деятельности, ФАТФ, 2021 г. [Электронный ресурс] – Режим доступа. URL: https://www.fedsfm.ru/content/files/documents/fatf/2021/nadzor_web.pdf

Основные тенденции развития FinTech в Российской Федерации

Н.С. Колпакова
к.э.н., доцент кафедры финансов и кредита
ИЭУ ФГАОУ ВО «КФУ им. В. И. Вернадского»,
Симферополь
E-mail: instoc.crimea@bk.ru

Аннотация: В статье отражены результаты исследования перспектив и приоритетов развития FinTech в России, приведены ключевые достоинства и недостатки внедрения инновационных технологий на национальном и международном финансовых рынках, выявлены микро- и макрориски объективного процесса цифровизации предоставления финансовых услуг.

Ключевые слова: финансовые технологии, инновации, финансовый рынок, Россия, цифровизация.

The main trends in the development of FinTech in the Russian Federation

Abstract: The article reflects the results of a study of the prospects and priorities for the development of FinTech in Russia, presents the key advantages and disadvantages of introducing innovative technologies in the national and international financial markets, identifies micro and macro risks of an objective process of digitalization of the provision of financial services.

Keywords: financial technology, innovation, financial market, Russia, digitalization.

Объективной тенденцией развития современного общества является цифровизация всех социально-экономических процессов, включая операции на финансовом рынке. Инновационные технологии, продукты и услуги, предоставляемые современным потребителям, коренным образом меняют сущность и содержание финансовых потоков и формируют цифровую модель бизнеса. В результате трансформации традиционной концепции денежных переводов, кредитования и инвестирования была сформирована новая финансовая ниша – FinTech, динамичное развитие которой обуславливает актуальность ее научного исследования.

Несмотря на достаточно короткий период истории цифровых технологических инноваций в финансовом секторе, они являются объектом

многочисленных публикаций как отечественных [1, 2, 3, 5, 6], так и зарубежных авторов [7, 8, 9]. При этом единого мнения в понятийно-категориальном аппарате FinTech пока не достигнуто, а их основные концепции базируются на следующих постулатах:

- FinTech – это отрасль экономики, включающая компании, которые используют технологии для оказания финансовых услуг более эффективным способом, нежели классические банковские, страховые и другие организации финансового рынка. Компании этой отрасли являются преимущественно стартапами, созданными для осуществления прорыва в имеющихся финансовых системах и организациях, не использующих программные продукты;

- FinTech – это организации, объединяющие инновационные бизнес-модели и технологии для оказания и распространения финансовых услуг;

- FinTech – это сфера действия технических стартапов, осуществляющих трансформацию таких финансовых направлений, как мобильные платежи, переводы денежных средств, управление активами, кредитные и депозитные операции;

- FinTech – это компьютерные программы и прочие технологии, используемые для поддержки либо обеспечения банковских и финансовых услуг.

Таким образом, термин «FinTech», являющийся аббревиатурой словосочетания «финансовые технологии», применяется для описания широкого спектра инноваций в финансовой сфере и связанных с ними участников финансового рынка. По мнению А. Мазараки и С. Волосович, FinTech одновременно следует рассматривать и как систему, включающую подсистемы технологий в таких сферах, как:

- расчетно-платежные операции;
- кредитование;
- инвестиционная деятельность банков и рынков капитала (Investment Banking / Capital Market);
- личные финансы (Personal Finance);
- институциональные финансы (Institutional Finance);
- страхование (InsurTech);
- регулятивные технологии (RegTech).

Структура основных сфер применения FinTech на мировом рынке представлена на рисунке 1.

По оценкам М. Н. Поддубной и Е. Я. Волкова, объемы внедрения FinTech в России ниже, чем в странах Европейского союза и США, однако, отечественные потребители гораздо более открыты для новых технологий в области как личных, так и корпоративных финансов. Исследования консалтинговой компании EY показали, что доля проникновения FinTech в

крупных городах Российской Федерации составляет порядка 35,0 %, в то время как средний общемировой показатель не превышает 16,0 %. По оценкам Deloitte, в 2017 году российский рынок FinTech оценивался в 48 млрд. руб., в 2018 году показатель вырос до 54 млрд. руб. (на 12,5 %), в 2019 году – до 60 млрд. руб., соответственно [5].



Рисунок 1 – Структура основных сфер применения FinTech на мировом финансовом рынке

В значительной степени Россия опережает другие страны мира по уровню пользовательской культуры и кибербезопасности при работе с сервисами FinTech (63,4 % против 32,8 %), однако, отстает по показателям объема инвестиций в их развитие (10,4 млрд. долл. США по сравнению с 82,4 млрд. долл. США) и динамике роста их деловой активности (3,9 % против 19,5 %) [2].

Основным национальным драйвером развития FinTech в России является вовлечение финансового сектора экономики в цифровые реформы через реализацию Национальной программы «Цифровая экономика», в том числе федеральный проект «Цифровое государственное управление» [4]. Ключевыми стейкхолдерами данного процесса выступают государственные органы власти (Министерство цифрового развития, связи и массовых коммуникаций РФ, Министерство экономического развития РФ, Центральный Банк РФ); крупнейшие банки страны (ПАО «Сбербанк России», АО «Тинькофф Банк»); государственные корпорации развития (ГКР «ВЭБ.РФ», АО «РВК»).

Количество участников рынка FinTech в Российской Федерации за период 2016-2020 гг. увеличилось с 91 до 198, то есть на 107 субъектов или

117,6 %. Несмотря на утверждения ряда ученых о неготовности консервативного банковского сектора к инновациям в сфере FinTech, в России 97 организаций, формирующих рынок финансовых инноваций или 49,0 % от общего их количества, относится к банкам и их дочерним структурам. На втором месте, с удельным весом в 24,7 %, находятся венчурные компании, реализующие финтех-сервисы «под ключ» на продажу, на третьем, с долей рынка в 14,6 % – фонды. В целом, численность профессиональных участников отечественного рынка FinTech на начало 2021 года составляла 127 или 64,1 %, нефинансовых организаций-участников – 71 или 35,9 %.

С точки зрения Р. Г. Ганиева, можно выделить следующие тренды развития рынка FinTech в России [1]:

1) Синергетическое усиление сотрудничества всех стейкхолдеров (финансового рынка, бизнеса, государства и потребителей финансовых услуг), последовательное формирование эффективной экосистемы цифровых платежей.

2) Финансовый мониторинг и формирование условий для развития различных моделей финансовых услуг в рамках «регуляторной песочницы», позволяющей государству и бизнесу работать над развитием FinTech совместно с агентами финансового рынка.

3) Защита информации, обрабатываемой в рамках использования FinTech, больших данных, искусственного интеллекта и машинного обучения, а также необходимости интеграции пула финансовых технологий.

Как видно из приведенного перечня перспективных направлений развития отечественного рынка FinTech, каждое из них сопряжено с определенными рисками. Обобщенно их можно сгруппировать по признаку влияния на национальную экономику в две группы: микрориски и макрориски. К первому типу относятся несоответствие сроков погашения кредитов, риск ликвидности, кибер-риск, зависимость от третьих сторон, регулятивный риск, бизнес-риск критически важных объектов инфраструктуры финансового рынка. Вторая группа рисков внедрения FinTech включает системный риск, процикличность, превышение волатильности и риск вытеснения.

В последние пять лет в России наблюдается устойчивый рост кибератак именно на объекты финансовой инфраструктуры (83,0 % в 2016 году по сравнению с 39,0 % в 2020 году), при этом в части атакуемых бизнесов наибольший удельный вес занимают компании, функционирующие в сфере FinTech. Системное негативное влияние на процесс предоставления критически необходимых микрофинансовых услуг влечет за собой соответствующие последствия на макроэкономическом уровне всей

страны, поэтому комплексный мониторинг и эффективное управление одинаково важны для обеих групп выделенных рисков.

Полностью устранить отрицательные факторы развития FinTech в России, как и на уровне мирового финансового рынка, невозможно. Как невозможно остановить и объективный процесс цифровизации, в связи с чем основной задачей участников финансового рынка становится максимальное использование достоинств FinTech, имеющих комплиментарный характер. Распределенные вычисления используют большие данные, искусственный интеллект и криптографию для эффективных распределенных сетевых технологий, например, цифровых кошельков, мобильных телефонов или планшетов в качестве торговых точек для осуществления платежей. Это усиливает активизацию трансформационных процессов в финансовой системе государства. Внедрение новых приложений в информационной экономике растет нелинейно, учитывая сетевые эффекты (чем больше людей связано сетью, тем ценнее сеть для каждого члена), общие для финансирования, а также для коммуникационных технологий. В частности, технология распределенной бухгалтерии (DLT) может стимулировать изменения в финансовом секторе. Эта концепция заключается в том, что учетные записи операций или собственности на активы и обязательства могут сохраняться и обновляться надежно для всей сети пользователей самими пользователями, а не центральным органом управления.

По результатам научных исследований и экспертных опросов, доминирующими направлениями развития FinTech в России в ближайшие годы должны стать: решения для осуществления платежей в режиме реального времени – 43,0 % экспертных оценок; рост автоматизации – 35,0 %; применение блокчейн-технологий – 33,0 %; FinTech M&A банков – 29,0 %; возникновение новой банковской бизнес-модели – 29,0 %; FinTech как поставщик услуг для банков – 28,0 %; безналичные платежи – 24,0 % [6]. Таким образом, FinTech является фундаментом слияния инновационных финансовых технологий с традиционными финансовыми услугами. В то же время FinTech продуцирует целый ряд вызовов для традиционных финансовых институтов и создает основу для трансформационных возможностей как для участников рынка финансовых услуг, так и для других субъектов национальной экономики.

В целом, можно утверждать, что драйвером развития FinTech в России станут не революционные, а эволюционные изменения финансового рынка, и, прежде всего, сектора финансовых услуг. Традиционные финансовые институты адаптируются к новым условиям, а новые участники рынка будут вливаться в финансовую экосистему цифровых отношений. Направленные на удовлетворение потребностей сначала ограниченного

числа клиентов, а затем – на все группы населения, FinTech адаптируются под запросы рынка, решая вновь возникающие проблемы в движении национальных и мировых финансовых потоков. Задача участников рынка FinTech – найти баланс между его преимуществами и возможными рисками и угрозами цифрового характера.

Список использованных источников:

1. Ганиев, Р. Г. Тенденции и тренды развития технологий FinTech / Р. Г. Ганиев // Вестник Таджикского государственного университета права, бизнеса и политики. Серия общественных наук. – 2021. – № 2(87). – С. 15-20. – Текст: непосредственный.
2. Ештокин, С. В. Российский Финтех в национальной финансовой системе: защитник интересов или скрытая угроза? / С. В. Ештокин // Экономика, предпринимательство и право. – 2021. – Т. 11. – № 8. – С. 1915-1944. – Текст: непосредственный.
3. Матвеевский, С. С. FinTech-компании и их взаимодействие с банками: международный и российский опыт / С. С. Матвеевский, А. В. Бердышев // Вестник университета. – 2020. – № 11. – С. 174-180. – Текст: непосредственный.
4. Паспорт Национальной программы «Цифровая экономика Российской Федерации»: утвержден президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам 24.12.2018 г. № 16 [Электронный ресурс]. – Режим доступа: [http://base.garant.ru/72190282 /#ixzz72gR8FrCt](http://base.garant.ru/72190282/#ixzz72gR8FrCt) (дата обращения: 05.10.2021).
5. Поддубная, М. Н. Основные характеристики и анализ состояния отрасли Финтех в России / М. Н. Поддубная, Е. Я. Волков // Международный журнал гуманитарных и естественных наук. – 2020. – № 7-1(46). – С. 156-159. – Текст: непосредственный.
6. Таланова, М. И. Финансовые технологии (FinTech): проблемы и перспективы развития / М. И. Таланова // E-SCIO. – 2021. – № 6(57). – С. 323-333. – Текст: непосредственный.
7. Kuchina, Ya. O. Regulating fintech in russia: the issues raised from the absence of legal definition / Ya. O. Kuchina // JUSTICE. – 2021. – Т. 3. – № 2. – С. 80-102. – Текст: непосредственный.
8. Mazaraki, A. FinTech in the systym of social transformations / A. Mazaraki, S. Volosovych // Herald KNUTE. – 2018. – No 2. – p. 5-18.
9. Wójcik D. Financial Geography I: Exploring FinTech – Maps and concepts / D. Wójcik // Progress in Human Geography. – 2021. – № 45(3). – p. 566-576. – Text: direct.

**Основы повышения эффективности производства на примере
ООО «ЮГСТРОЙИНВЕСТ-КУБАНЬ» в условиях цифровой
трансформации**

О.Д. Ермоленко

к.э.н., доцент кафедры экономики региона, отраслей и предприятий

РГЭУ (РИНХ), Ростов-на-Дону

E-mail: Olenka_er@mail.ru

М.Н. Мурзинова

студентка факультета экономики и финансов

РГЭУ (РИНХ), Ростов-на-Дону

E-mail: marina.murzinova2001@yandex.ru

Аннотация: В статье рассматривается процесс повышения эффективности производства на примере российского предприятия строительной отрасли. Выявлены тенденции в уровне повышения эффективности предприятия ООО «ЮГСТРОЙИНВЕСТ-КУБАНЬ». Следуя инструментам управления эффективности предприятия, мы стремимся к адекватной и равноправной рыночной экономике. Эффективность любого предприятия, вне зависимости от специфики производимых им товаров и услуг, включает в себя такие параметры, как: экономичность, результативность, продуктивность

Ключевые слова: эффективность производства; российские производители; предприятия и организации; строительство; экономические показатели; российские предприятия.

**Fundamentals of increasing production efficiency on the example of
YUGSTROYINVEST-KUBAN llc in the context of digital transformation**

Abstract: The article discusses the process of increasing production efficiency on the example of a Russian enterprise in the construction industry. Trends in the level of increasing the efficiency of the enterprise LLC "YUGSTROYINVEST-KUBAN" are revealed. Following the company's efficiency management tools, we strive for an adequate and equitable market economy. The efficiency of any enterprise, regardless of the specifics of the goods and services it produces, includes such parameters as: efficiency, efficiency, productivity

Keywords: production efficiency; Russian manufacturers; enterprises and organizations; construction; economic indicators; Russian enterprises.

В современных условиях, предприятиям необходимо извлекать максимальную возможную прибыль. В первую очередь, это связано с условиями рыночной экономики, ведь не зря существующий принцип Дарвинизма в экономике гласит: «выживает сильнейший».

Предприятиям необходимо снижать расходы на производственную деятельность и направлять силы на достижение научно-технического прогресса.

Рыночная экономика не может не диктовать производителям товаров и покупателям свои специфические условия. Это касается, прежде всего, производственных отношений, которые построены на принципах жесточайшей конкуренции, когда огромное количество продавцов буквально сражаются за своих покупателей, стараясь предложить более выгодный во всех планах товар, не обходя стороной закон стоимости, закон спроса и предложения.

Экономическая эффективность как объект управления является одним из решающих факторов производства товаров и услуг в современном мире.

В современных рыночных условиях эффективность предприятия, его экономические показатели являются решающими показателями социального, экономического и научного прогресса нашей страны.

Эффективность, как ни странно, зависит от свободной конкуренции, которая является основой нашей экономики.

Благодаря её показателям отечественные производители с каждым разом повышают свою конкурентоспособность, как на внутренних рынках, для отечественных потребителей товаров и услуг, так и внешних рынках, в мировом хозяйстве.

Следуя инструментам управления эффективности предприятия, мы стремимся к адекватной и равноправной рыночной экономике. Эффективность любого предприятия, вне зависимости от специфики производимых им товаров и услуг, включает в себя такие параметры, как: экономичность, результативность, продуктивность.[2]

Со всех сторон учитывается интерес покупателя, к которому и прислушивается продавец, идя на его условия. И благодаря сложившейся ситуации на рынке, предприятия различных форм собственности они обязаны повышать свою самостоятельность, должны нести ответственность перед покупателями. [3]

И для того, чтобы получать максимальную выгоду от своей деятельности, должны вырабатывать максимально верные управленческие решения для обеспечения эффективности их экономической деятельности, производственных показателей, которые, безусловно, должны быть действенными во всех смыслах.

Из века в век повышение экономической эффективности предприятия и его показателей характеризуется определенными трудностями в их достижении, но это довольно важная задача, которая должна быть выполнена.

В современных реалиях огромное количество предприятий работает с довольно низкой эффективностью, их рентабельность стремится к нулю или в принципе отсутствует.

Эффективность использования собственного капитала, имеет большое значение для каждого предприятия страны, поскольку определяет финансовых результаты деятельности данного предприятия, помогает найти пути увеличения этих показателей, проработку внутренних проблем различного характера. Экономическая эффективность отличается от всех остальных тем, что затраты, необходимые для её выполнения, выражаются в стоимостном виде, а также полезные результаты в виде стоимости эффективности предприятия в себе заключает 4 основных подхода.

В рамках первого подхода эффективность рассматривается в качестве степени достижения целей, которые предприятие ставит перед собой, в виде какого-либо плана.

В рамках второго подхода эффективность организации выражается в качестве внешнего использования предприятием своих возможностей для извлечения из нее редких ресурсов необходимых для полноценного и всеохватывающего развития всех её субъектов.

В рамках третьего подхода эффективность характеризуется в том, что у предприятия есть определенный набор способностей, с помощью которых он достигает качественных результатов благодаря минимальным затратам.

В четвертом подходе эффективность является уровнем удовлетворенности потребителя конечными товарами и услугами, которые произвел производитель и смог продать.

Строительная отрасль в Российской Федерации за последние годы испытывает рост. Это можно связать с длительным лаговым эффектом (2-4года) реализации строительных проектов, запущенных до начала пандемии коронавируса.

За 11 лет своего существования строительная фирма ООО «ЮГСТРОЙИНВЕСТ-КУБАНЬ» с другими дочерними компании фирмы «ЮгСтройИнвест» построила и сдала рекордные 4 миллиона квадратных метров жилья. [2]

Она стала компанией на первом месте в России по количеству открытых эскроу-счетов. А также заняла 3 место в России по объему вводимого жилья. Основываясь на данных показателях уже можно смело сказать, что компания довольно эффективна в отрасли строительного бизнеса страны.

Для того, что предприятие достигало эффективности своей работы, необходимо, конечно же, эффективно и продуктивно использовать материальные, трудовые и финансовые ресурсы. Обобщающим показателем эффективности жизнедеятельности предприятия является рентабельность. [1]

Рентабельность представляет собой степень доходности того или иного предприятия. В нашем случае, для показания рентабельности строительной компании ООО «ЮГСТРОЙИНВЕСТ-КУБАНЬ» есть определенная система относительных показателей, оценивающих эффективность работы для каждого вида деятельности организации по отдельности и в целом.

Анализируя показатели рентабельности предприятия, основанные на бухгалтерской отчетности предприятия, можно сказать, что эффективность использования предприятием ООО «ЮГСТРОЙИНВЕСТ-КУБАНЬ» своих основных фондов повысилась, так все важнейшие показатели рентабельности значительно возросли.

Наибольший рост показала рентабельность продукции – за период с 2019 по 2020 годы она возросла на 28,18% и составила 88,54%.

Также значительно увеличились показатели рентабельности продаж. По сравнению с предыдущим 2019 годом она увеличилась на 25,03 % и составила 81,35%, что говорит нам об отношении полученной прибыли от продаж к выручке за 2020 год, которая, несомненно, возросла.

Небольшую динамику проявили рентабельность активов и заемного капиталов, которые увеличились лишь на 1,27 и 2,14%. Такие низкие значения говорят нам о том, что наблюдаемый рост объема чистой прибыли чересчур быстрый для роста показателей основных средств и активов предприятия ООО «ЮГСТРОЙИНВЕСТ-КУБАНЬ».

Вывод по предприятию гласит о том, что предприятие на экстенсивном пути развития, учитывая увеличившийся объем выручки и постоянно растущий спрос на строительство недвижимости юга России.

Деятельность предприятия эффективна, поскольку она эффективно использует имеющиеся ресурсы. [2]

В условиях современной макроэкономической нестабильности это очень хороший знак, который гласит нам о том, что в будущем объем прибыли компании будет лишь расти, включая и объем выручки.

Компания имеет стабильный и довольно крупный доход. [7]

Рентабельность собственного капитала показала отрицательный результат для деятельности предприятия. Она упала на рекордные 43,34%, не исключая валовую рентабельность и затратноотдачу, которые упали, соответственно на 1,05 и 26,8%.

Низкую динамику проявили рентабельность активов и заемного капиталов, которые увеличились лишь на 1,27 и 2,14%. Такие низкие

значения говорят нам о том, что наблюдаемый рост объема чистой прибыли чересчур быстрый для роста показателей основных средств и активов предприятия ООО «ЮГСТРОЙИНВЕСТ-КУБАНЬ».

Вывод по предприятию гласит о том, что на экстенсивном пути развития, учитывая увеличившийся объем выручки и постоянно растущий спрос на строительство недвижимости юга России.

Основными факторами, влияющими на прибыль, являются ценовые изменения на строительные материалы, которые лишь с начала апреля 2021 года выросли на 60-80%. [4]

Одним из по-настоящему действенных способов снижения себестоимости в материалоемком производстве, а именно строительстве, является экономия материальных ресурсов. [3]

Можно было бы предложить совершенствовать технологический процесс строительных сооружений настолько, чтобы в результате на каждую единицу ресурсов добиваться существенного увеличения объема производства продукции.

В целом, наблюдается долгосрочная рентабельность продукции, которая свидетельствует нам о том, что с каждым годом компания увеличивает объем продаж и работает намного эффективнее, формируя и увеличивая свою прибыль.

Также за счет рационализации процессов хранения и расходования строительных материалов можно будет снизить себестоимость сооружений и тем самым повысить эффективность порядка 5%.

Наблюдается долгосрочная рентабельность продукции, которая свидетельствует нам о том, что с каждым годом компания увеличивает объем продаж и работает намного эффективнее, формируя и увеличивая свою прибыль. [5]

Это говорит нам о существовании хороших возможностей: производственные мощности в долгосрочной перспективе могут расширить нам круг потенциальных потребителей, поэтому необходимо усилить мероприятия по продвижению продукции.

Деятельность предприятия эффективна, поскольку она эффективно использует имеющиеся ресурсы. В условиях современной макроэкономической нестабильности это очень хороший знак, который гласит нам о том, что в будущем объем прибыли компании будет лишь расти, включая и объем выручки. Эффективность каждого предприятия нашей страны всегда включает в себя экономичность, результативность и продуктивность. Система управления эффективностью производства безумно важна на предприятии, поскольку помогает ему функционировать на равных с конкурентами того или иного рынка.

Список использованных источников:

1. Бухгалтерская отчетность компании ООО «ЮГСТРОЙИНВЕСТ-КУБАНЬ» [Электр. ресурс]. Режим доступа: https://www.audit-it.ru/buh_otchet/2311176106_ooo-stroitelnoe-upravlenie-5-yugstroyinvest-kuban
2. Официальный сайт строительной компании ЮгСтройИнвест. [Электр. ресурс]. Режим доступа: <https://gk-usi.ru/novosti/>
3. Шифрин, М.Б. Стратегический менеджмент [Текст]: учебник для академического бакалавриата / М.Б. Шифрин. – 3-е изд., испр. и доп. – М.: Издательство Юрайт, 2017. – 321 с Бухгалтерская отчетность компании ООО «ЮГСТРОЙИНВЕСТ-КУБАНЬ» [Электр. ресурс]. Режим доступа: https://www.audit-it.ru/buh_otchet/2311176106_ooo-stroitelnoe-upravlenie-5-yugstroyinvest-kuban
4. Интерфакс. Рейтинг фундаментальной эффективности предприятий [Электр. ресурс]. Режим доступа: <https://www.interfax.ru/russia/678840>
5. Официальный сайт строительной компании ЮгСтройИнвест. [Электр. ресурс]. Режим доступа: <https://gk-usi.ru/novosti/>
6. Официальный сайт Федеральной службы государственной статистики. [Электр. ресурс]. Режим доступа: <http://www.gks.ru/>
7. Шифрин, М.Б. Стратегический менеджмент [Текст]: учебник для академического бакалавриата / М.Б. Шифрин. – 3-е изд., испр. и доп. – М.: Издательство Юрайт, 2017. – 321 с.

Оценка и управление финансовыми рисками компании ПАО «НОВАТЭК»

Д.С. Журавлёв
студент 2 курса НИЯУ МИФИ, Москва
E-mail: danila_13_100@mail.com

Аннотация: в статье рассматриваются анализ и управление финансовыми рисками на примере ПАО «НОВАТЭК». Риск неизбежно сопутствует всем сферам деятельности компании, работающей в рыночных условиях.

Ключевые слова: финансовые риски, ПАО «НОВАТЭК», страхование, корпоративное управление.

Assessment and management of financial risks of PJSC "NOVATEK"

Abstract: the article discusses the analysis and management of financial risks on the example of PJSC NOVATEK. Risk inevitably accompanies all areas of activity of a company operating in market conditions.

Keywords: financial risks, PJSC NOVATEK, insurance, corporate governance.

Риск сопровождает все области бизнеса, который работает в рыночных условиях. Основным критерием устойчивости развития компании является способность высшего руководства управлять и контролировать риски.

Как и любая компания, ПАО «Новатэк» имеет достаточное количество рисков, которые может понести компания, поэтому необходимо их выявить, затем провести качественную и количественную оценку, а затем приложить все усилия для их минимизации.

Наиболее значимые для компании риски:

1. Кредитный риск

Кредитный риск связан с риском возникновения финансового убытка в случае невыполнения контрагентами своих обязательств.

Торговая и прочая дебиторская задолженность распределена между различными отраслями и географическими территориями. Основная часть природного газа и СПГ на международных рынках реализуется клиентам с независимым внешним рейтингом, а также на основе 100%-ной предоплаты.

Таблица 1 – Динамика капитальных вложений, млрд рублей

Год	Размер вложений
2017	26,8
2018	56,2
2019	110,4
2020	142,6
1п2021	136,7

Продажа СПГ на внутреннем рынке подвержена риску неплатежей со стороны мелких и средних промышленных потребителей. Новые контрагенты проходят обязательную процедуру идентификации клиента и оценку кредитоспособности. Все действующие контрагенты регулярно предоставляют обновленную информацию по предприятию, в том числе и в отношении статуса кредитоспособности.

2. Процентный риск

Компания является крупным заемщиком, поэтому подвержена воздействию рисков, которые связаны с повышением процентных ставок. Процентные ставки могут быть привязаны к плавающим международным и российским базовым ставкам. Неустойчивость процентных ставок может ограничить использование заемного капитала в качестве источника финансирования инвестиционной деятельности. При этом компания придерживается сбалансированной политики в области привлечения заемных средств, а также стремится к максимизации доли долгосрочных обязательств с фиксированными ставками в своем долговом портфеле.

3. Инфляционный риск

Изменение индекса потребительских цен оказывает влияние на уровень рентабельности эмитента и финансовое состояние компании. Существенное обесценение рубля может стать причиной роста темпов инфляции. Предсказать критический уровень инфляции невозможно, так как помимо уровня потребительских цен необходимо учитывать изменение реальной покупательной способности рубля, конъюнктуру экспортных рынков жидких углеводородов и СПГ, а также политику правительства в отношении тарифов на природный газ.

4. Валютные риски

Часть обязательств Компании выражена в иностранной валюте, что может привести к убыткам в случае девальвации рубля. При этом, часть выручки компании также выражена в иностранной валюте, что может привести к убыткам в случае укрепления рубля. В целом это компенсирует друг друга. «НОВАТЭК» покупает иностранное оборудование для своих производств, также получает в валюте часть выручки. Таким образом, метод управления валютными рисками – внутреннее хеджирование.

5. Риск ликвидности

В процессе управления риском ликвидности компания поддерживает адекватный баланс денежных средств и заемных ресурсов, отслеживает прогнозируемые и фактические денежные потоки и коррелирует сроки погашения финансовых активов и обязательств.

Для привлечения средств с рынков капитала на выгодных условиях и увеличения числа потенциальных инвесторов компания имеет кредитные рейтинги инвестиционного уровня от трех ведущих международных рейтинговых агентств (Moody's, Standard & Poor's и Fitch) и российского рейтингового агентства «Эксперт РА».

Деятельность ПАО «НОВАТЭК» подвержена рискам, присущим нефтегазовой отрасли. В ПАО «НОВАТЭК» действует и постоянно развивается многоуровневая система управления рисками и внутреннего контроля.

Выполненный спрасе-анализ позволил оценить конкурентное положение компании, таблицы 1-5.

Таблица 2 – Внутренняя среда (оценка по данным компании)

Показатель	значение в отчетном году	оценка от 6 до 0	вес (равный)	итог
Чистая рентабельность продаж, % (Чистая прибыль / Выручка)	11,04	3,00	0,25	0,75
Отношение CAPEX к выручке, % (Инвестиции ОДДС / Выручка)	28,09	6,00	0,25	1,5
Коэффициент дивидендных выплат, % (Дивиденды / Чистая прибыль)	15,09	6,00	0,25	1,5
Рентабельность инвестированного капитала, % (EBI / Инвестированный капитал)	48,23	6,00	0,25	1,5
Итог	х	х	х	5,25

Исходя из данных таблицы 1, мы можем сделать вывод, что показатель внутренней среды составляет 5,25. Данный показатель является значением выше среднего. Компани нацелена на сохранение комфортной долговой нагрузки, а также на поддержание надежного финансового положения, которое открывает возможность для реализации инвестиционных проектов.

Выручка достигла рекордного уровня, превысила показатели докризисного, а чистая прибыль компании увеличилась более в 9 раз относительно прошлого года.

Таблица 3 – Внешняя среда (привлекательность отрасли)

Показатель	значение в отчетном году	оценка от 6 до 0	вес (равный)	итог
1. CAGR суммарной выручки крупнейших компаний за 2016-2020 год	1,26	2,00	0,33	0,67
2. Чистая рентабельность продаж крупнейших компаний (2020 год) (Чистая прибыль/ Выручка)	9,89	2,00	0,33	0,67
3. Сектор экономики	первичный + вторичный	1,00	0,33	0,33
Итого	х	х	х	1,67

По второй таблице мы можем сделать вывод, что привлекательность отрасли оценена в значение – 1,67. Показатель ниже среднего. Первичный сектор экономики (добывающая отрасль) – очень трудоемкая, требует дорогостоящего оборудования, многие ресурсы не возобновляемые, что влияет на значение показателя.

Таблица 4 – Динамика продаж природного газа по рынкам, млрд м3

Год	Россия	Международные	Общие
2017	46,08	-	47,01
2018	47,64	3,45	51,24
2019	47,66	10,21	57,54
2020	47,09	7,28	54,26
2021	49,81	5,67	55,69

Цены на газ на крупных газовых месторождениях в Европе начали стремительно расти и превысили 1900 \$ за 1000 кубометров на фоне сообщений о недостаточной заполненности европейских газовых хранилищ в преддверии отопительного сезона. Причина - холодный и продолжительный зимний сезон 2020—2021, что повлекло за собой потребление природного газа выше нормы. Также погода была практически безветренной, что повлекло за собой падение объемов ветрогенерации.

Таблица 5 – Оценка показателей компании

Показатель	значение	оценка от 6 до 0	вес (равный)	итог
Относительная доля по выручке в 2020 г.	11,01	-5	0,14	-0,71
Изменение относительной рыночной доли по активам (2020/2016)	1,69	0	0,14	0,00
Изменение относительной рыночной доли по выручке (2020/2016)	1,16	-2	0,14	-0,29
Изменение относительной доли по чистой прибыли (2020/ 2016)	0,60	-5	0,14	-0,71
Изменение относительной доли по CAPEX (2020/ 2016)	1,26	-2	0,14	-0,29
Изменение относительной доли по дивидендам (2020/ 2016)	0,00	-2	0,14	-0,29
Изменение относительной доли по денежному потоку (2019/ 2016)	0,939	-3	0,14	-0,43
Итог	х	х	х	-2,71

В третьей таблице указаны конкурентные преимущества самой компании. Конкурентные преимущества выше среднего. При этом потенциал у компании хороший, так как на данный момент развиваются проекты с СПГ – «Ямал СПГ», «Арктик СПГ 2», «Криогаз-Высоцк».

Таблица 6 – Оценка компании и среды

	Характеристика	Оценка в баллах
Financial Strength	Финансовый потенциал компании	5,25
Industry Attractiveness	Привлекательность отрасли	1,67
Environment Stability	Стабильность рыночной среды	-0,50
Competitive Advantage	Конкурентные преимущества компании	-2,71

Компания придерживается стратегии диверсифицированного роста. Это состояние наблюдается на стабильных рынках с низкими темпами роста. В этом случае повышается концентрация на финансовой стабилизации. Данная стратегия направлена на диверсификацию и выход на более перспективные рынки, снижение себестоимости при увеличении качества товара и разработка новой продукции.

Для оценки финансовой деятельности компании выполнен анализ чистого долга и дивидендной политики, таблицы 7, 8.

Таблица 7 – Динамика чистого долга, млрд рублей

Год	Размер чистого долга
2017	88,7
2018	101,8
2019	14,125
2020	38,648
2021	15,128

В декабре 2020 года была утверждена новая дивидендная политика-направление на дивиденды не менее 50% от скорректированной прибыли по МСФО. По прогнозам у компании будут рекордные дивиденды по итогам всего 2021 года.

Таблица 8 – Размер дивидендов на акцию,руб.

Год	Размер дивидендов
2015	13,6
2016	14,8
2017	15,55
2018	25,01
2019	31,28
2020	34,38
1п2021	27,67

У НОВАТЭК наблюдается падение экспортных продаж, это вызвано переходом на долгосрочные прямые контракты проекта «Ямал СПГ», что в дальнейшем позволит компании снизить риски, которые связаны с волатильностью спроса и цен на международном рынке СПГ.

В сфере управления рисками страхование - один из самых эффективных подходов. В 2020 году страховая защита обеспечила достаточную защиту от потенциальных рисков повреждения деятельности НОВАТЭК.

В целях снижения риска финансовых потерь компания осуществляет следующие виды добровольного страхования:

- страхование имущества на случай утраты (гибели) и/или повреждения, в том числе страхование машин и механизмов от поломок;
- страхование убытков от перерыва в производстве (предпринимательских рисков);
- страхование строительно-монтажных рисков;
- страхование рисков при поиске, разведке и разработке месторождений (рисков потери контроля над скважиной);
- страхование транспорта;
- страхование грузов;
- страхование ответственности директоров, должностных лиц и компаний (D&O);
- страхование ответственности фрахтователей;

– добровольное медицинское страхование работников в составе социального пакета.

Общая страховая сумма рисков имущественного ущерба и перерывам производственной деятельности на конец 2020 года составила 910 млрд рублей. Реализуемая программа рассматривается менеджментом компании как одна из эффективных мер по снижению последствий возможных аварий и позволяет получить дополнительные гарантии достижения ожидаемого размера чистой прибыли и ключевых показателей деятельности общества.

Благоприятная для нефтегазодобывающей отрасли ситуация на рынке углеводородов позволила бизнесу показать сильные финансовые результаты по итогам первых 9 месяцев и обновить рекорды по размеру выручки и скорректированной чистой прибыли, тем самым превысить результаты докризисного 2019 года.

На данный момент экономическая ситуация позволяет рассчитывать, что по итогам второго полугодия НОВАТЭК сможет выплатить акционерам больше дивидендов, чем по итогам первого полугодия, а общая сумма годовых выплат за 2021 год может стать для компании рекордной.

Ближе к зимнему сезону цены на газ на мировых рынках увеличились. Высокие цены на природный газ и жидкие углеводороды совокупно с рекордными производственными результатами «Новатэка» прогнозируют хорошие финансовые результаты по итогам всего 2021 года.

У компании почти отсутствует долговая нагрузка, несмотря на инвестиционную программу, которая связана с развитием СПГ-проектов и запуском новых месторождений. Таким образом, способность эффективно влиять на риски позволяет предприятию успешно функционировать, иметь финансовую устойчивость, высокую конкурентоспособность и стабильную прибыльность.

Список использованных источников:

1. Федеральный закон от 26.12.1995 N 208-ФЗ (ред. от 29.07.2017) "Об акционерных обществах".
2. Методические указания по проведению анализа финансового состояния организации. Утверждены Приказом ФСФО РФ от 23.01.2001 №16.
3. Когденко В.Г. Управление финансами и рисками. М.: Юнити Дана, 2019г.
4. Митрова Н., Грушевенко Е., Капитонов С. Коронакризис: влияние COVID-19 на ТЭК в мире и в России: Центр энергетики Московской школы управления СКОЛКОВО. 2020 г.
5. Отчеты об устойчивом развитии ПАО «НОВАТЭК» 2020 г.

Оценка риска наличия скрытых доходов в российских домашних хозяйствах на основе модели Писсаридеса-Вебера

Л.И. Ниворожкина

д.э.н, профессор, зав. каф. статистики, эконометрики и оценки рисков

РГЭУ (РИНХ), Ростов-на-Дону

E-mail: lin45@mail.ru

А.А. Трегубова

к.э.н., доцент, доцент каф. статистики, эконометрики и оценки рисков

РГЭУ (РИНХ), Ростов-на-Дону

E-mail: alexandra_a_t@mail.ru

Аннотация: В работе представлены результаты оценки доли скрытых доходов в располагаемых ресурсах домохозяйств на панельных данных RLMS-HSE за 2000-2018 гг. на основе модифицированной модели Писсаридеса-Вебера. Сформулированы предложения для органов власти в целях принятия решений по сокращению неравенства и бедности и, как результат, снижению социальной напряженности в обществе.

Ключевые слова: скрытые доходы, домашние хозяйства, модель Писсаридеса-Вебера.

Russian households hidden incomes risk assessment based on Pissarides-Weber model

Abstract: The paper presents the results of estimating the share of hidden income in household disposable resources on the panel data of RLMS-HSE for 2000-2018 based on the modified Pissarides-Weber model. We formulated suggestions for the authorities to make decisions to reduce inequality and poverty and, as a result, reduce social tension in society.

Keywords: hidden incomes, households, Pissarides-Weber model.

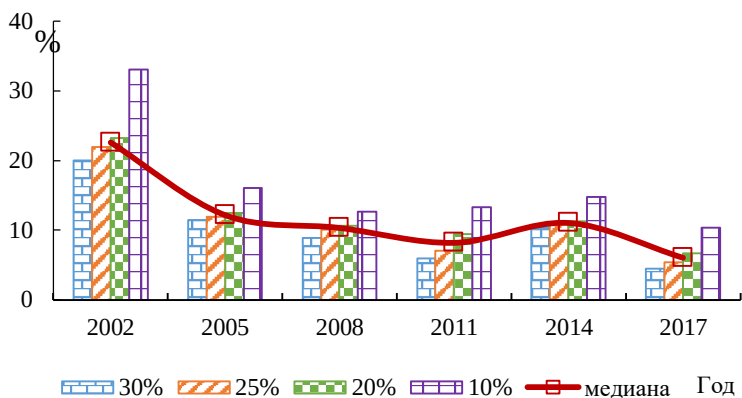
В свете указаний президента РФ по усилению мер по сокращению уровня бедности населения страны, Федеральной службой государственной статистики (Росстат) начата разработка усовершенствованной методики оценки финансового положения россиян, в частности многодетных семей и пожилых. При измерении доходов населения планируется учитывать активы разного рода, а также социальную помощь в натуральном виде. Росстат планирует до конца 2021 года выполнение научно-исследовательской работы по теме «Разработка

рекомендаций по совершенствованию программ и методов проведения выборочных наблюдений по социально-демографическим проблемам в целях развития системы статистических показателей, характеризующих финансовое положение и условия жизни различных целевых демографических групп населения» [1], в которой представлен широкий спектр подходов по определению доходов населения, однако оценка скрытых доходов не уточняется. Важность же выделения именно скрытых доходов обусловлена тем, что оценка распространения и объемов скрытых доходов российских домашних хозяйств позволит уточнить реальные масштабы бедности и неравенства, что особенно актуально, когда обязательства государства по поддержке малообеспеченных слоев населения резко возрастают.

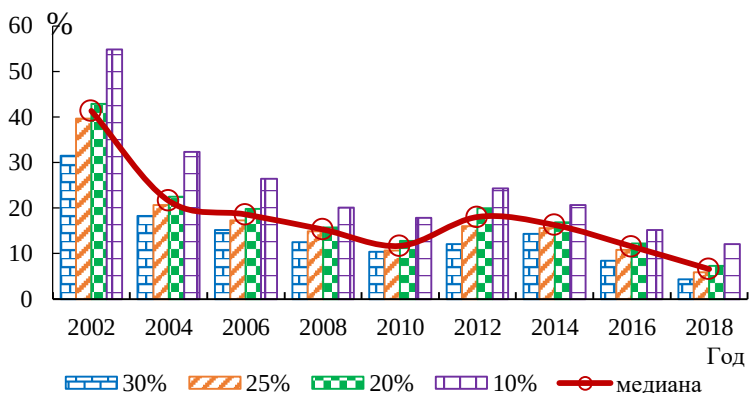
Один из важных аспектов измерения неравенства и бедности в России – «присутствие устойчивого смещения, состоящего в том, что в структуре доходов российских домохозяйств велика доля скрытых доходов, недооценка которых осуществляется официальной статистикой на макроуровне» [2]. Исследование того, как влияют скрытые доходы на сглаживание доходного неравенства и бедности домохозяйств, дает важную информацию для структур любого уровня, принимающих решения в сфере социальной политики, поскольку скрытые доходы участвуют в формировании латентного механизма выравнивания уровня жизни и элиминирования социальной напряженности.

В качестве источника информации об уровне жизни населения на микроуровне были использованы данные «The Russia Longitudinal Monitoring Survey – Higher School of Economics» (RLMS-HSE) [3]. Объектом анализа выступали домохозяйства. В качестве индикатора благосостояния домохозяйства был сформирован показатель ежемесячных располагаемых ресурсов домохозяйства. Структура выборки репрезентативно представляет основную часть населения страны, в том числе реципиентов социальной помощи.

Согласно авторскому подходу группой домохозяйств, в которых в течение двух / трех последовательных периодов текущие расходы превышали располагаемые ресурсы не менее чем на 10% (или, например, на 20%, 25%, 30%). Исходные данные с 2000 г. по 2018 г. включительно были преобразованы в панели по двум / трем последовательным годам, все последующие расчеты осуществлены на данных завершающего панель года. Методология и эмпирическая оценка размера компоненты скрытых доходов россиян, осуществленная на основе модели Писсаридеса-Вебера [4], подробно представлена в работах [5], [6]. Результаты оценки доли скрытых доходов представлены на рис. 1 (более подробно в [7]).



(а) панели по трем годам



(б) панели по двум годам

Рисунок 1 – Доля скрываемых доходов для 10, 20, 25, 30%-го превышения расходов над располагаемыми ресурсами

В течение рассматриваемого периода происходило постепенное снижение доли скрываемых доходов. В панели 2000-2002 года доля скрытых доходов превышала 33,0%, что можно расценить как отклик кризисных 90-х, когда активно функционировала челночная торговля, процветала неформальная занятость. Одна из черт этого периода – преобладание относительно мелких заработков. Кризис 2014 года стал толчком к новому росту скрытых доходов, причем основная часть скрытых доходов сконцентрировалась в домохозяйствах, где их превышение составляло 25-

30%. Однако этот рост был относительно небольшим и, начиная с 2015 года, вновь началось их сокращение.

Инкорпорирование предложенного подхода к оценке скрытых доходов населения в новую методику оценки финансового положения россиян поможет уточнить как общий уровень бедности населения, так и выделить социально-демографические группы населения, в которых преимущественно концентрируются скрытые доходы и оценить их роль в уменьшении бедности и неравенства. Аргументом в пользу целесообразности данного предложения служит то, что скрытые доходы преимущественно распространены в домохозяйствах, находящихся за чертой бедности. Как результат, с учетом относительной малочисленности этой группы, влияние скрытых доходов на общий уровень бедности и неравенство не велико. Однако непосредственно для домохозяйств со скрытыми доходами эта компонента представляется существенным фактором, воздействующим на выход из бедности и элиминирование неравенства.

В процессе совершенствования мер адресной социальной политики в отношении домохозяйств, находящихся за чертой бедности, необходима дифференциация этих мер с учетом источников доходов, что и предусмотрено предложениями, озвученными Росстатом, однако необходимо обратить пристальное внимание на тот факт, что по результатам проведенного анализа [7] социальные трансферты в бедных домохозяйствах не способствовали снижению неравенства, что свидетельствует о необходимости более пристального внимания к этому феномену при принятии решений в области социальных выплат.

Перспективным научным направлением оценки распространенности и объемов скрытых доходов населения на принципиально ином концептуальном уровне является широкое внедрение цифровых информационных технологий, которое позволяет упростить доступ к респондентам по сети Интернет и указывает новый путь развития методологии получения данных от населения. Современные возможности цифровизации, работы с большими данными позволяют начать организацию оперативного формирования данных о характеристиках индивидов и домохозяйств из всех возможных источников, включающих сведения о доходах и расходах. Повсеместный переход на электронные деньги, который уже начался и набирает скорость, позволит дополнительно оценивать риски извлечения скрытых доходов и их воздействия на уровень бедности и неравенства домохозяйств в режиме реального времени и тем самым повысить эффективность социальной политики государства.

«Развитие и внедрение методов многомерной статистики, эконометрики, основанное на растущей мощности вычислительных

средств и наличии пакетов прикладных программ, реализующих эти методы, открыло новый этап в исследованиях в области изучения факторов благосостояния населения, в том числе и структуры доходов, включая их скрытую составляющую» [2]. Ускорение цифровизации денежных расчетов населения позволит в ближайшие годы вывести из тени многие виды скрытых доходов, но этот процесс только набирает силу и по-прежнему актуальным остается вопрос: где и у кого преимущественно концентрируются скрытые доходы и каков их объем? Результаты представленного анализа подтвердили, что скрываемые доходы домашних хозяйств формируют латентный механизм выравнивания уровня жизни и являются «подушкой безопасности» в периоды экономических кризисов, фактором, элиминирующим социальную напряженность в обществе. Выявленная тенденция, характеризующая распространенность и объемы скрытых доходов среди российских домашних хозяйств, позволяет предположить, что концентрация именно теневых, криминальных доходов происходит за границами сектора домашних хозяйств. Способность населения к самоорганизации, устойчивость к внешним шокам свидетельствуют о том, что снятие ряда запретительных мер, жестких налоговых режимов на неформальную активность населения, уход от модели патернализма позволит облегчить груз социальных обязательств государства в период восстановления экономики после кризиса, вызванного падением цен на энергоносители, коронавирусом.

Благодарность. Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-010-00009.

Список использованных источников:

1. РБК. – Режим доступа: <https://www.rbc.ru/economics/19/10/2021/616d78a09a7947fb8d296050>
2. Ниворожкина Л.И. Скрытые доходы российских домашних хозяйств: у кого они? // Известия вузов. Северо-Кавказский регион. Общественные науки. № 3 – 2020. - С. 91-98.
3. RLMS-HSE. – Режим доступа: <http://www.cpc.unc.edu/projects/rlms>, <http://www.hse.ru/rlms>
4. Pissarides C., Weber G. (1989). An Expenditure-Based Estimate of Britain's Black Economy // Journal of Public Economics, vol. 39. pp. 17–32.
5. Ниворожкина Л.И., Арженовский С.В. Оценка скрытых доходов домохозяйств с учетом длительности периода измерения // Финансовые исследования, 2020. - №3 (68). – С.27-39.
6. Nivorozhikina L., Arzhenovskiy S., Galazova S. (2020) International Journal of Economics and Business Administration, Volume VIII, Issue 4, 635-646, 2020. DOI: 10.35808/ijeba/614.

7. Ниворожкина Л.И., Арженовский С.В., Трегубова А.А., Торопова Т.В., Войнова В.И. Неравенство и бедность в постсоветской России: динамика и факторы формирования с учетом скрытых доходов домохозяйств. Монография. – Ростов-на-Дону: Издательско-полиграфический комплекс РГЭУ (РИНХ), 2021. – 286 с.

Оценка финансовых рисков компаний нефтегазового сектора на примере группы компаний «Татнефть»

В.В. Жорова
студент 2 курса НИЯУ МИФИ, Москва
E-mail: zhorovavv@mail.ru

Аннотация: В статье рассматривается ситуация на российском и мировом рынках, которая сложилась в последний год. Также уделено внимание комплексной оценки рисков на примере ПАО «Татнефть».

Ключевые слова: Мировая экономика, нефтегазовый сектор, внутренний рынок, ОПЕК, экономические риски.

Financial and risk management of organizations in an pandemics in the oil and gas sector on the example of PJSC "Tatneft"

Abstract: The article examines the situation on the Russian and world markets, which has developed over the past year. Attention is also paid to a comprehensive risk assessment using the example PJSC "Tatneft".

Keywords: World economy, pandemic, oil and gas sector, domestic market, OPEC, economic risks.

Рыночная экономика характеризуется постоянными изменениями современного мира. Возникновение и распространение коронавируса по всему миру, а также введение мер ограничительного характера оказали негативное влияние на экономику, а именно: стремительное падение объемов продаж, снижение инвестиционной активности, угрозы финансовой безопасности – это факторы определенных рисков, которые влечет за собой нестабильная критическая ситуация.

Известно, что рынок нефти оказывает значительное влияние на экономику страны в целом. Данная отрасль сильнее всего пострадала в период пандемии, в том числе из-за снижения спроса со стороны транспортного сектора.

В связи с этим возникли существенные ограничения на экспорт и импорт. Так как произошло снижение спроса и закрытие границ, хранилища нефти начали переполняться. А так как большая часть

добываемых ресурсов реализуется на экспорт, экономика стран и, в частности, России терпит существенное недополучение прибыли.

Страна имеет высокую зависимость от нефтегазового сектора экономики, так как около 40% доходов федерального бюджета формируются за счет выручки рассматриваемой отрасли, любые колебания в этой сфере незамедлительно влияют на российский рубль и состояние экономики в целом.

Складывается следующая ситуация:

- Мировая экономика переживает самый глубокий и резкий спад экономической активности с 1930-х годов, но восстановление также может быть динамичным.
- Снижение мирового спроса 16–25%.
- Власти по всему миру вводят беспрецедентные бюджетные и монетарные стимулы.
- Суммарное снижение цен на нефть за 2020 год составило 60%.
- Происходит заполнение хранилищ нефти. 21 апреля 2020 г. цены на нефть пережили крупнейший обвал за всю историю
- Снижение ВВП на 3–5%.
- Рост безработицы вырос на максимальный процент с 2011 года – до 5,7%.
- Снижение реальных располагаемых доходов на 3,8%
- Спад промышленного производства на 5,4%.
- Резкое снижение курса рубля.
- Спад объемов экспорта на 21%.

Китай является одним из основных рыночных партнеров и крупных импортеров России. В связи с пандемией в феврале этого года спрос нефти в Китай снизился с 13 млн баррелей в сутки до 10 млн. В марте появляется множество ограничений, связанных со снижением спроса и соответственно экспорта другими странами партнерами.

Коронавирус также оказал прямое влияние на сделку ОПЕК. Так как страны ОПЕК обеспечивают добычу 40% нефти, мировой рынок нефти связан с соглашением ОПЕК.

Суммарное снижение цен на нефть за 2020 год составило 60%.

Данная отрасль начинает постепенное восстановление. К концу 2020 года цена на нефть Brent закрепляет свое положение на 50 долл. за баррель и продолжает устойчивый рост. Данной цены достаточно для поддержания рентабельности работы российских нефтяных компаний. Спрос на топливо также продолжает восстанавливаться.

Государство в свою очередь также вводит поддержку для нефтегазовой отрасли в виде согласования и введения нового законопроекта. Благодаря

данному законопроекту к 2024 году бюджет потратит в поддержку более 50 млрд рублей.

В связи с пандемией и последующие годы восстановления нефтегазовой отрасли нефтяным компаниям необходимо обратить особое внимание на финансовую устойчивость и риски.

Далее рассмотрена группа компаний Татнефть. «Татнефть» - одна из крупнейших российских нефтяных компаний, которая занимает пятое место в рейтинге нефтегазовых компаний России.

Первая половина 2020 года оказалась непростой для группы Татнефть. Добыча нефти из-за сделки ОПЕК+ сократилась по итогам 2020 года на 14,6%. Под воздействием внешних факторов финансовые результаты компании значительно снизились, а риски увеличились.

Итак, группа компаний Татнефть подвержена следующим видам риска, а именно:

– Рыночному риску, который состоит из:

- 1) ценового риска (риск изменения цен на товары, в частности, цен на нефть);
- 2) валютного риска как следствие колебания курсов валют;
- 3) риска изменения процентных ставок в связи с привлечением кредитов и займов под плавающие ставки процента.

– Кредитному риску – риск неисполнения контрагентами своих обязательств и снижение финансовой устойчивости кредитных организаций-контрагентов.

– Риск ликвидности – финансовый риск, связанный с неспособностью расплатиться по обязательствам без существенных убытков, заключающийся в риске неподдержания достаточных резервов, банковских кредитных линий и резервных заемных средств для покрытия обязательств.

На рисунке 1 отражена динамика финансовых результатов группы.

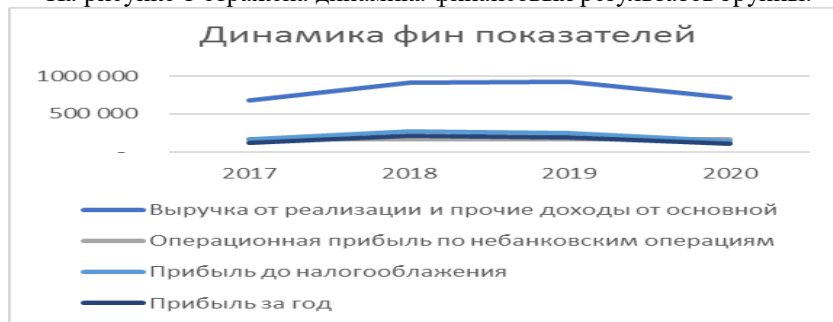


Рисунок 1 – Финансовые показатели компаний ПАО Татнефть

Заметен рост показателей с 2017 года, однако к 2020 году происходит резкий спад. Так, например, чистая прибыль Татнефть падает с 252 млрд рублей в 2019 году до 137 в 2020 году (46%).

Данные снижения крайне негативно сказываются как на финансовой устойчивости компании, так и на инвестиционной привлекательности. Однако в сравнении с компаниями нефтегазовой отрасли ПАО «Татнефть» имеет один из наименьших спадов. Например, чистая прибыль ПАО «Лукойл» упала на 97%, а НК «Роснефть» на 67%.

Что касается кредитного риска – рассматриваемая компания имеет высокое количество контрагентов. Кроме того, дебиторская задолженность занимает более 30% от оборотных активов, что задает необходимость контролировать подверженность кредитному риску. Особенно важным это становится в условиях экономического кризиса 2020 года.

С точки зрения оценки кредитоспособности контрагентов, ПАО «Татнефть» систематически оценивает финансовое состояние контрагентов, а также их кредитные рейтинги в мировых и национальных рейтинговых агентствах.

При анализе крупных контрагентов за 2020 год было выявлено, что все компании имеют достаточно высокие кредитные рейтинги по шкалам Российских рейтинговых агентств. Исходя из этого, что положительно влияет на управление кредитным риском компаний.

С точки зрения анализа дебиторской задолженности, были проанализированы период оборачиваемости задолженности, а также проведено сравнение с кредиторской задолженностью и с выручкой за период 2017–2020 гг.

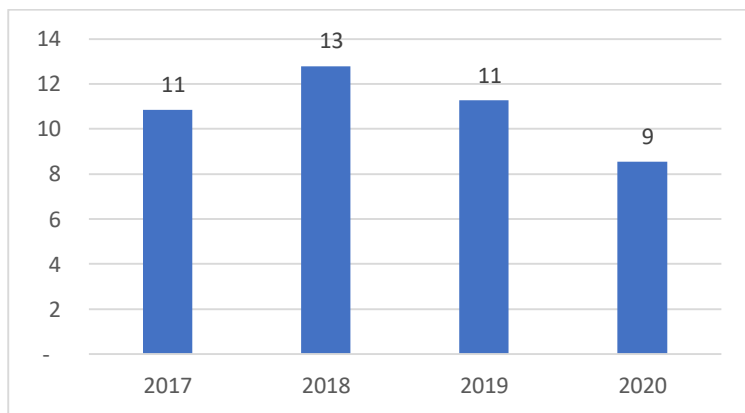


Рисунок 2 – Коэффициент оборачиваемости дебиторской задолженности

При рассмотрении коэффициента оборачиваемости можно сделать вывод, что Татнефть придерживаются жесткой кредитной политики, так как срок оборачиваемости дебиторской задолженности не превышает 20 дней. Даже во время пандемии и неизбежного снижения финансовой устойчивости всех нефтяных компаний удалось улучшить данный показатель (рисунок 2).

При сравнении с темпом прироста выручки, заметно, что выручка растет медленнее дебиторской задолженности, что снижает качество управления как дебиторской задолженностью, так и кредитным риском в целом.

В то же время, просроченная дебиторская задолженность имеет значение ниже 5% (около 1%), что классифицирует группу компаний Татнефть неподверженной кредитному риску в значительной мере как в предыдущих годах, так и во время 2020 года.

По риску ликвидности необходимо отметить, что высокая волатильность цен на углеводороды и продукты их переработки, курсов мировых валют, рост тарифов и цен поставщиков, а также прочие внешние факторы могут привести к разбалансированности показателей планов, бюджетов и инвестиционных программ, и, как следствие, к возникновению дефицита ликвидности и источников финансирования.

В современных экономических условиях хозяйствующий субъект постоянно находится в ситуации риска, связанной с выбором альтернативных решений, обладающих разными вероятностями их осуществления.

Была рассмотрена доля денежных средств и дебиторской задолженности в валюте баланса в динамике (рисунок 4).

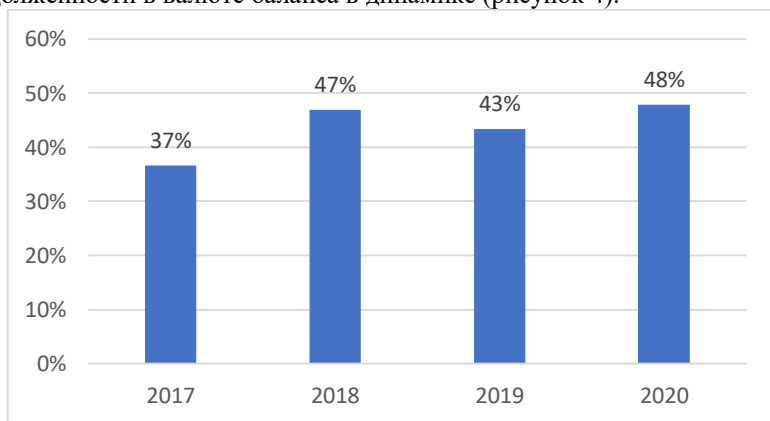


Рисунок 3 – Доля некоторых активов в балансе

Денежные средства и дебиторская задолженность занимают в среднем 43% в активах. Кроме того, наблюдается тенденция к существенному увеличению дебиторской задолженности, из-за снижения покупательской способности контрагентов.

Далее были проанализированы показатели, которые позволяют наиболее точно сделать вывод о подверженности группы Татнефть риску ликвидности.

Для оценки вероятности банкротства ПАО Татнефть рассчитан коэффициент Бивера, который позволит выявить риск неплатежеспособности (рис. 5).

При анализе коэффициента в динамике заметно, что до 2019 года данный показатель имеет крайне высокие значения и положительную динамику до 2020 года. При нормальном диапазоне коэффициента 0,4 – 0,45 ПАО «Татнефть» имеет значение данного показателя в 2-3 раза выше. Даже при кризисном 2020 году ПАО Татнефть сохраняет данный показатель значительно выше среднего.

Однако высокое значение коэффициента Бивера также отрицательно сказывается на получении дополнительного дохода группой, а также возможных инфляционных потерях.

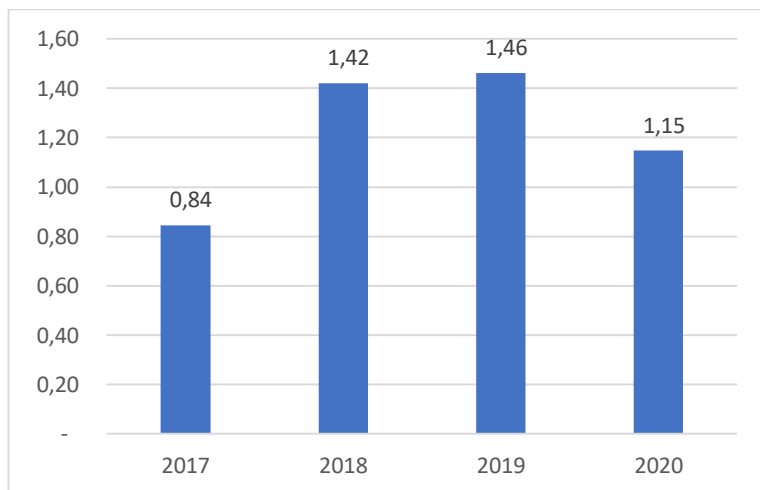


Рисунок 4 – Коэффициент Бивера

Для оценки платежеспособности проанализированы коэффициенты ликвидности.

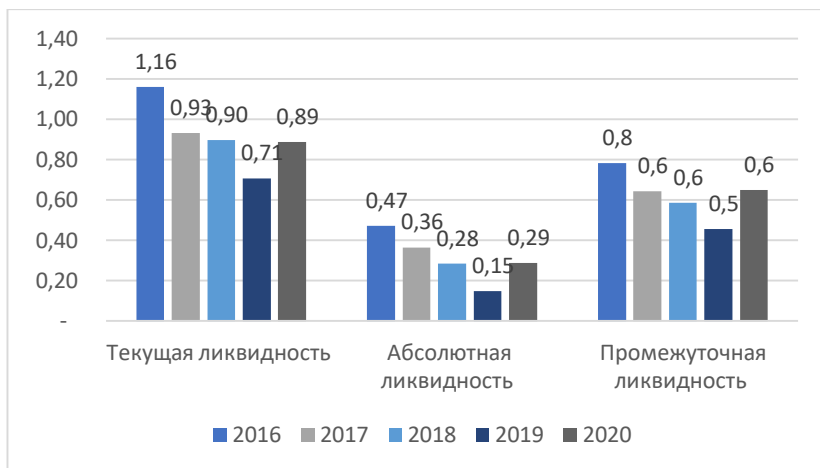


Рисунок 5 – Коэффициенты ликвидности

При изучении графика можно сделать вывод, что Татнефть не имеет проблем с мгновенной платежеспособностью наиболее ликвидными активами. Однако показатели текущей и промежуточной ликвидности ниже нормативных значений, а также имеют тенденцию к снижению до 2020 года, что связано как с увеличением краткосрочных обязательств, так и снижением активов в 2017 и 2019 годах.

При анализе рыночного риска, выявлено, что группа компаний успешно справляется с управлением валютным риском, риском изменения процентных ставок и риску изменения цен на финансовые инструменты.

ПАО Татнефть регулярно проводят анализ подверженности ценовому риску, включая моделирование возможного поведения цены на нефть и нефтепродукты, маржи экспорта и внутреннего рынка. Кроме того, риск изменения цен на финансовые инструменты управляется путем диверсификации портфелей, а также установления лимитов как на содержание советующих активов в портфелях, так и на срок удержания долговых финансовых инструментов.

Что касается валютного риска, группа осуществляет деятельность в международном масштабе, а также имеет финансовые активы в иностранной валюте, что подвергает группу риску вследствие колебания обменных курсов.

Стратегия управления валютным риском, связанным с изменениями денежных потоков по будущим поступлениям в иностранной валюте, предполагает хеджирование экспортной выручки в размере чистой монетарной позиции.

На заключительном этапе была проведена комплексная оценка рисков данной компании.



Рисунок 6 – Комплексный анализ финансовых рисков

При комплексном анализе рисков группы можно сделать следующий вывод: группа компаний Татнефть эффективно управляет финансовыми рисками, однако в 2020 году финансовая устойчивость снижается, а подверженность рискам увеличивается. В наибольшей мере данная группа компаний подвержена кредитному риску.

Список использованных источников:

1. Официальный сайт. URL: <https://www.tatneft.ru>
2. Бадалова, А. Г. Управление рисками деятельности предприятия: Учебное пособие / А. Г. Бадалова, А. В. Пантелеев. – Москва : Вузовская книга, 2016. – 234 с.
3. Гурнович Т. Г., Остапенко Е. А., Молчаненко С. А. Оценка и анализ рисков : учебник / Т. Г. Гурнович, Е. А. Остапенко, С. А. Молчаненко ; под общ. ред. Т. Г. Гурнович. — Москва : КНОРУС, 2019. — 252 с. — (Бакалавриат). ISBN 978-5-406-05701-8.
4. Когденко, В. Г. Управление финансами и рисками: монография./ Когденко В. Г. – М. : ЮНИТИ-ДАНА, 2019 г. – 527 с.
5. Назарова А. Н., Хан А. Г. Анализ в оценке риска потери платежеспособности организации // Молодой ученый. – 2017. — № 2. – С. 461-465.

Оценка ESG стратегии ОАО «РЖД»

В.С. Книга

студент 2 курса НИЯУ МИФИ, Москва

E-mail: kniga.vika@mail.com

Аннотация: в статье рассматривается раскрытие принципов управления ESG российскими компаниями на примере ОАО «РЖД». В настоящее время инвесторы сталкиваются с недостатком качественного раскрытия эмитентами данных об ESG-факторах.

Ключевые слова: ESG стратегия, ОАО «РЖД», экология, социальная сфера, корпоративное управление.

Evaluation of the ESG strategy of JSC "Russian Railways"

Abstract: the article discusses the disclosure of the principles of ESG management by Russian companies on the example of JSC "Russian Railways". Currently, investors are faced with a lack of high-quality disclosure by issuers of data on ESG factors.

Keywords: ESG strategy, JSC "Russian Railways", ecology, social sphere, corporate governance.

На сегодняшний день принципы управления компаниями ESG получают всё большее распространение в России.

ESG представляет собой перечень требований к экологической, социальной и корпоративной ответственности компаний. Соблюдение данных принципов является основой для управления устойчивым развитием компаний. Таким образом, если компания придерживается принципов ESG, то она занимается регулированием своего влияния на окружающую среду, практикует бережливое производственные процессы, а также стремится к углеродной нейтральности, является открытой для стейкхолдеров и общества в целом. Рассмотрим каждый критерий подробнее:

1. Экологические критерии (Е — англ. environmental) определяют, с помощью каких средств и с какой эффективностью компания заботится об окружающей среде. К данному критерию можно отнести вопросы, связанные с выбросами углекислых газов, степень загрязнения

окружающей среды и использование природных ресурсов, а также соблюдение экологических законов.

2. Социальные критерии (S — англ. social) характеризуют отношение организаций к сотрудникам, контрагентам, клиентам и партнерам. Также к данному критерию можно отнести заботу о состоянии работников и их безопасность на рабочем месте, отказ от рабского и детского труда, профессиональные компетенции сотрудников, условия труда, соблюдение прав человека, а также ответственность перед контрагентами за качество товаров.

3. Критерии корпоративного управления (G — англ. governance). К данному критерию можно отнести раскрытие информации об работе менеджмента, прозрачностью отчетности, целесообразности выплаты руководителям, правами акционеров, качеством внутренних и внешних проверок, борьбу с коррупционными действиями.



Рисунок 1 – Критерии ESG

Компании, которые придерживаются принципов ESG, могут привлекать «зелёные» инвестиции с дисконтом относительно действующих ставок и связанные с реализацией экологических проектов.

На постоянной основе независимые исследовательские агентства формируют рейтинги компаний, соответствующих принципам ESG. Они оценивают развитие компаний по трем критериям — E, S и G — и присваивают баллы по определенной шкале. Независимое кредитное рейтинговое агентство RAEX-Europe на ежемесячной основе обновляет

ESG-рэнкинг. По состоянию на 16 сентября 2021 года, следующие 10 российских компаний возглавили рейтинг.

Таблица 1 – Топ 10 компаний по рейтингу RAEX-Europe

Место	Название	Отрасль	Е	S	G
1	«Полиметалл»	Золотодобыча	1	3	22
2	«Сибур»	Нефтехимия	2	6	20
3	«Лукойл»	Нефть и газ	4	16	3
4	«Энел Россия»	Электроэнергетика	16	1	10
5	РЖД	Ж/д транспорт	13	10	5
6	МТС	Телекоммуникации	24	7	4
7	НЛМК	Черная металлургия	7	4	31
8	«Интер РАО»	Электроэнергетика	5	8	39
9	«Полус»	Золотодобыча	3	20	24
10	«Вымпелком»	Телекоммуникации	19	11	18

ОАО «РЖД» (далее – Компания) заняла 5 место в данном рейтинге. Компания получила высокие баллы по критериям «Экологическая ответственность» и «Социальная ответственность». Холдинг в Годовом отчете подробно раскрывает соответствие ESG-принципам. Компания по праву является одним из первопроходцев и лидеров внедрения новых корпоративных ценностей. Рассмотрим информацию детально.

ОАО «РЖД» считается единственной компанией в России, которая представляет страну на международном рынке зеленых облигаций, а также является крупнейшим ESG-заемщиком на местном рынке. Компания размещает зеленые и социальные облигации в соответствии с локальными и международными принципами в области ответственного финансирования. Деньги, полученные от данных операций, идут в качестве инвестиций в проекты. Направленные на реализацию устойчивого развития Холдинга.

В первом квартале 2020 года Компания выпустила зеленые еврооблигации в швейцарских франках сроком на 6 лет. Также в сентябре 2020 года Компания закрыла сделку по первому в истории России выпуску зеленых бессрочных облигаций, которые получили подтверждение о соответствии российским и международным стандартам зеленого финансирования.

Рассмотрим соответствие Компании экологическим критериям. Деятельность Холдинга реализуется на территории 77 субъектов России. Главной задачей Компании является непрерывный рост уровня экологической безвредности, целесообразного использования природных ресурсов и забота о природной системе.

Компания активно занимается реализацией природоохранных мероприятий, а также ежегодно наращивает инвестиционные затраты на охрану окружающей среды (около 4 млрд рублей в 2020 году).

К основным природоохранным мероприятиям ОАО «РЖД» в 2020 году относятся:

- Применение экологических технологий на 138 объектах в разных субъектах РФ (применение экологических видов топлива, замена пылегазоочистного оборудования);

- За отчетный период построено и введено в эксплуатацию 11 сооружений для очистки сточных вод, внедрена технологическая линия по переработке отработанных резинотехнических изделий и автомобильных шин;

- В 4 квартале отчетного года Компания совместно с Министерством природных ресурсов и экологии ратифицировали План мероприятий по защите окружающей среды на территории Байкальской зоны при строительстве и реконструкции основных объектов железнодорожной инфраструктуры.

Холдинг является лидером по энергоэффективности и экологичности грузовых и пассажирских перевозок среди железнодорожных компаний мира. На ежегодной основе в Холдинге действует Программа энергосбережения и повышения энергетической эффективности в рамках реализации Энергетической стратегии на период до 2020 года и на перспективу до 2030 года.

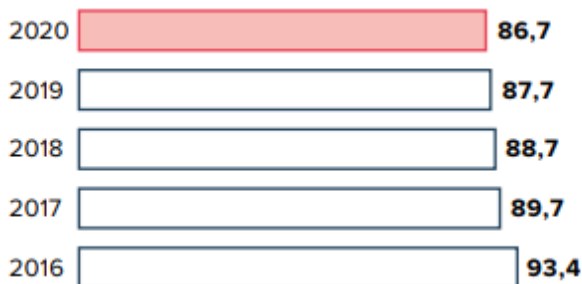


Рисунок 2 – Динамика изменения энергоемкости производственной деятельности ОАО «РЖД», кДЖ/прив. тмк

Согласно Рисунку 2 наблюдается тенденция снижения потребления топлива и энергии, что положительно характеризует Компанию с точки зрения заботы об окружающей среде. В 2020 году Компания реализовала все обязательные энергосберегающие мероприятия как на тягу поездов, так и на стационарные нужды, что позволило выполнить целевые показатели в области энергосбережения и повышения энергетической эффективности, определенные долгосрочной программой развития.

Таблица 2 – Показатели энергоэффективности и энергоемкости производственной деятельности

Цели	Целевые показатели	Фактические показатели 2020
Снижение энергоемкости производственной деятельности, %	-0,6	-1,0
Повышение энергоэффективности производственной деятельности, %	0,6	1,0

Большая часть экономии связана с успешной реализацией реализации комплекса мероприятий по совершенствованию технологических процессов управления движением поездов.

Так же, большая часть отходов, образованных в результате производственной деятельности, обезвреживается и вовлекается во вторичный оборот. При этом доля утилизированных отходов растет с каждым годом, что видно на рисунке 3.

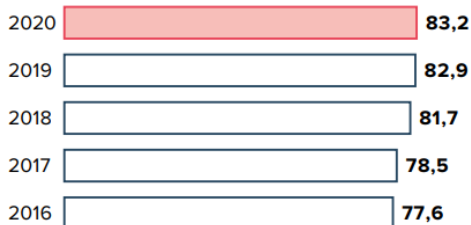


Рисунок 3 – Доля обезвреживания и вовлечения отходов во вторичный оборот %

Следующей составляющей ESG-стратегии являются социальные критерии.

На территории Российской Федерации Холдинг является одним из самых крупных работодателей. Компания заботится о своих сотрудниках и обеспечивает безопасность и комфортные условия работы. Главной задачей социально-кадровой политики является формирование человеческого капитала. Данная задача выполняется с помощью

проведения набора мероприятий, которые направлены на непрерывное обучение, мотивацию, сохранение здоровья сотрудников.

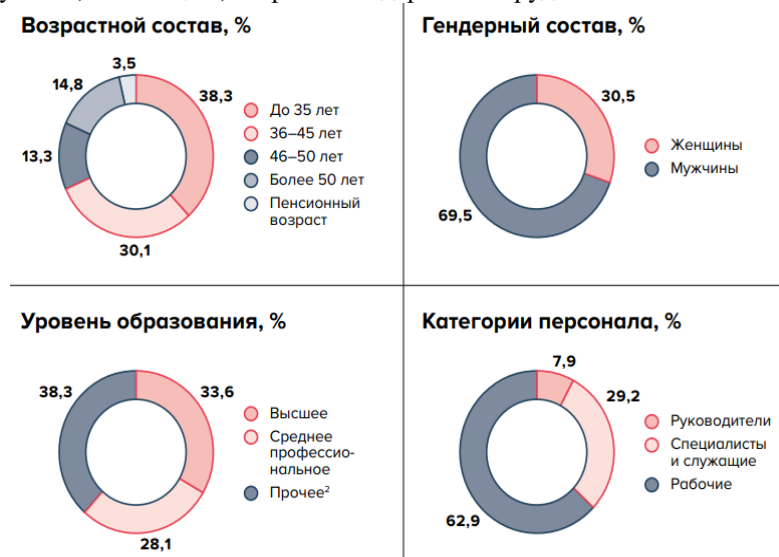


Рисунок 4 – Состав персонала ОАО «РЖД»

Как видно из рисунка 4, Компания активно привлекает к работе молодых специалистов, возрастом до 35 лет, это делает особенно важной социальную поддержку данной категории. Так же, важным событием в 202 году стал образовательный онлайн-форум «ПРОмолодежь», который проводился для вовлечения молодых сотрудников в обсуждение и реализацию программы «Молодежь ОАО «РЖД» (2021–2025 годы)».

Так же с каждым годом растет доля женщин в составе работников. Члены Координационного совета ОАО «РЖД» по совершенствованию условий труда, отдыха и социальной поддержки женщин постоянно проводят выездные встречи с работницами Компании и видеоконференции, которые позволяют получить обратную связь от работниц и обсудить возникающие вопросы. Немаловажным событием в истории компании стало то, что в 2020 году женщины получили возможность работать помощниками машиниста на некоторых типах тягового подвижного состава.

ОАО «РЖД» активно занимается развитием и обучением персонала. Основой корпоративной системы профессионального обучения являются 15 учебных центров профессиональных квалификаций.

Таблица 3 – Социальные показатели

Показатель	2017 г.	2018 г.	2019 г.	2020 г.
Среднесписочная численность персонала, тыс. чел., в том числе:	755	752.2	743.1	723.5
Рабочие	477.1	474.5	468.6	455.1
Руководители	57.7	57.4	57.3	57.2
Специалисты и служащие	220.3	220.3	217.3	211.3
Среднемесячная зп, руб/чел	50,404	54,934	58,504	61,375
Среднегодовая зп, тыс. руб./чел.	605	659	702	737
Рост к уровню предыдущего года, %	7.58	8.99	6.50	4.91
Затраты на оплату труда, тыс. руб	456,660	495,856	521,692	532,858
Расходы на безопасность труда, млн руб.	20,121	22,596	23,915	28,542
Коэффициент частоты производственного травматизма	0.25	0.23	0.21	0.17
Количество рабочих мест с вредными условиями труда, тыс. рабочих мест	88	84	81	79
Улучшены условия труда, тыс. рабочих мест	37	41	41	41

Исходя из данных, представленных в таблице 3, можно сделать вывод, что Холдинг каждый год повышает заработную плату сотрудникам, а также проводит индексацию. В исследуемом периоде снижаются показатели производственного травматизма и количество мест с вредными условиями труда, что говорит о заботе со стороны Компании о своих сотрудниках.

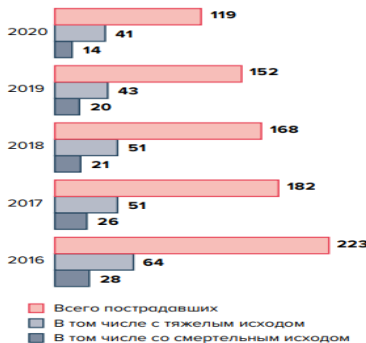


Рисунок 5 – Динамика производственного травматизма, кол-во пострадавших, чел.

Затраты на улучшение условий и охрану труда в 2020 году по категориям, %



Рисунок 6 – Затраты на улучшение условий и охрану труда в 2020 г, %

Одним из главных направлений социальной политики Холдинга является забота о здоровье каждого сотрудника. Холдинг предоставляет своим сотрудникам санитарно-курортное лечение, а также каждый год организует спортивные мероприятия для поддержания и развития физической силы каждого.

Из всего вышесказанного можно сделать вывод, что Компания придерживается своих основных этических принципов, а именно:

- Ставить человека на первое место;
- Работать на совесть;
- Гордиться званием сотрудника ОАО «РЖД»;
- Ориентироваться на результат;
- И многие другие.

Далее перейдем к G-составляющей ESG-стратегии. Сюда можно отнести показатели, связанные с управленческим персоналом и их деятельностью.

Таблица 4 – Совет директоров

Состав Совета директоров	2017	2018	2019	2020
Численность, чел.	14	14	14	14
Число независимых неисполнительных членов совета директоров	3	3	3	3
Доля независимых директоров, %	21.43	21.43	21.43	21.43

Значительную роль в работе совета директоров Холдинга занимают вопросы, связанные с реализацией устойчивого развития Компании.

Компания ежегодно в отчетности раскрывает вознаграждения топ-менеджмента в разбивке на заработную плату и выплаченные премии.

В ОАО «РЖД» на регулярной основе действует Ревизионная комиссия и служба Внутреннего аудита. На ежегодной основе данная служба проводит оценку финансово-хозяйственной деятельности Холдинга.

Немаловажную роль в борьбе с коррупцией играет Антикоррупционная политика, которая направлена на предотвращение и сокращение коррупционных проявлений, а также сокращение рисков. Данная политика дает понять каждому сотруднику, что за любое совершение коррупционных правонарушений последуют непредотвратимые наказания.

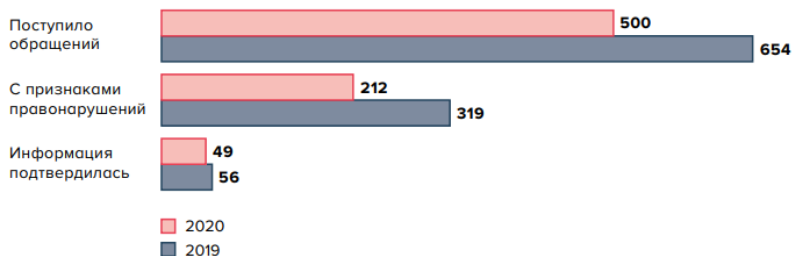


Рисунок 7 – Итоги работы «Горячей антикоррупционной линии»

Одним из методов борьбы с коррупцией в Компании является работа «Горячей антикоррупционной линии». Как видно по рисунку 7, в 2020 году сократилось количество как обращений, так и самих нарушений. По итогу проведенной работы к 39 сотрудникам компании применены дисциплинарные взыскания. При этом, при разбирательстве только по семи сообщениям информация была передана в правоохранительные органы.

Таким образом, из всего вышесказанного можно сделать вывод, что ОАО «РЖД» по праву входит в топ-5 российских компаний, соответствующих принципам ESG. Компания является одним из лидеров в применении принципов ESG среди российских компаний, как оператор самого экологически чистого вида транспорта. Как крупнейший работодатель Холдинг заботится о своих сотрудниках и пресекает меры, связанные с мошенничеством и коррупцией.

Список использованных источников:

1. Через ESG к устойчивому развитию. На железной дороге применяет современные принципы управления | Экономика | Гудок (gudok.ru)
2. ESG-принципы: что это такое и зачем компаниям их соблюдать | РБК Тренды (rbc.ru)
3. Отчетность компании | Компания (rzd.ru)
4. Цели в области устойчивого развития — Устойчивое развитие (un.org)

Первоочередные меры по развитию и обеспечению финансовой безопасности экспортноориентированных малых предприятий торговли в Российской Федерации

Р.М. Богданова

к.э.н., доцент, кафедры Экономики региона,
отраслей и предприятий РГЭУ (РИНХ)

E-mail: raisa.m1975@mail.ru

А.С. Медведева

студентка факультета экономики и финансов РГЭУ(РИНХ) РФ,

E-mail: olenka_er@mail.ru

Аннотация: С развитием малого предпринимательства увязывали разработку новых видов продукции, повышение степени насыщения рынков продукцией и услугами. В многочисленных исследованиях, проведённых отечественными и зарубежными экономистами, предпринимательство рассматривается как негосударственная часть экономики.

Ключевые слова: Малые предприятия, экспортоориентированные предприятия, цифровизация, государственные меры поддержки.

Priority measures for the development and financial security of export-oriented small trade enterprises in the Russian Federation

Abstract: The development of new types of products and an increase in the degree of saturation of markets with products and services were linked with the development of small business. In numerous studies conducted by domestic and foreign economists, entrepreneurship is considered as a non-state part of the economy.

Keywords: Small enterprises, export-oriented enterprises, digitalization, government support measures.

Практически четверть века в России обсуждаются проблемы развития малого бизнеса. В многочисленных публикациях девяностых и начала нулевых с развитием малых предприятий связывались рост ВВП страны и решение многочисленных социальных задач от проблем занятости и роста ВВП до вовлечения населения в предпринимательство. С развитием малого предпринимательства увязывали разработку новых видов продукции, повышение степени насыщения рынков продукцией и услугами. К

сожалению, подобные надежды себя не оправдали. С 2009г., когда произошёл переход от поотраслевого сбора статистических данных к статистике по видам деятельности, по 2018г., последний доковидный период функционирования экономики, обороты малых предприятий в Российской Федерации (доступный в официальной статистике аналог объёма реализации) выросли в 2.835 раза. Т.е. в среднем за год прирост составлял более 20%. Однако в 2019г. обороты малых предприятий сократились по отношению к 2018г. в 2.356 раза. Падение год к году продолжилось в 2021г., нивелировав практически десятилетнее развитие производства в сфере малого бизнеса. Количество работников малых предприятий в 2019г. сократилось по сравнению с 2009г. в 1.715 раза. Столь значительное падение оборотов малых предприятий, как и сокращение численности занятых на них, несмотря на принимавшиеся правительством меры по стимулированию сохранения их численности и поддержанию производства, свидетельствуют о проблемах в малом предпринимательстве и отсутствии у предприятий этой сферы достаточных запасов внутренней прочности. По данным результатов опросов, проведённых РБК в 2020г. почти 10 % предпринимателей из числа владельцев и руководителей малых предприятий готовились к закрытию в 2021г. Можно привести и ряд других эмпирических данных, иллюстрирующих проблемы в развитии малого бизнеса в нашей стране, что вызывает необходимость реформирования экономико-организационного механизма регулирования этой важной сферы деятельности.

В многочисленных исследованиях, проведённых отечественными и зарубежными экономистами, предпринимательство рассматривается как негосударственная часть экономики, некая система, внутренне подразделяемая на подсистемы, отдельные аспекты которых рассмотрены в работах Lewandowska et al. (2015) [1 с.787-792], Pinkovetskaia (2018) [2 с.66-77], Щемелев С.Н. и соав. (2019) [3 с.119-125], и ряда других экономистов.

Системный характер малого предпринимательства крайне важен для понимания проблем его развития и выработки мер по их устранению, относящихся как к малому бизнесу в целом, так и предприятиям отдельных видов деятельности, имеющих свои специфические особенности.

Прежде всего, следует критериально определить собственно сферу малого бизнеса, как объекта государственной политики, направленной на её развитие. В настоящее время к категории малых относятся предприятия с численностью занятых на них работников от 16 до 100 человек и годовым доходом от 120 до 800 млн. руб. Под годовым доходом понимается объём реализации продукции и услуг за прошлый календарный год. Существуют ограничения на участие в капитале малых предприятий государственных, муниципальных и иностранных предприятий. Указанные ограничения, в

основном, связаны с ограничением возможностей по уходу от налогов средних и крупных предприятий и нежелательного увеличения госсектора.

При существующих ограничениях только малые предприятия с численностью до 100 человек и объёмами продаж не более 150 млн. руб. могут применять упрощённые системы налогообложения. Соответственно возникает вопрос о целесообразности нахождения в категории малых предприятий тех из них, объёмы продаж которых превышают в годовом исчислении 150 млн. руб. Оставив пока данное обстоятельство, рассмотрим основополагающий вопрос о принципах включения предприятий в сферу малого бизнеса. Проведённые в последние годы исследования [4], показали, что обороты малых предприятий (доступный аналог объёма реализации), как результирующий показатель, в большей степени коррелирует с факторами, воздействующими на сферу малого бизнеса, чем численность работников предприятий. Незамедлительный отказ от двухкритериальности отнесения предприятий к категории малых в пользу оборотов по их расчётным счетам, позволит решить многие существующие сейчас проблемы. Особенно это актуально для тех малых предприятий, где широко используется ручной труд.

Следующим вопросом, имеющим отношение ко всей сфере малого бизнеса, является количественное определение объёма реализации, превышение которого характеризует переход предприятия в категорию средних и соответствующей потери возможностей упрощённого налогообложения и ведения отчётности. Кроме того, малые предприятия повсеместно рассматриваются как инкубаторы бизнеса и поэтому часто пользуются господдержкой со стороны государства, но размеры средств, выделяемых на эти цели объективно ограничены. Это обстоятельство тоже актуализирует вопрос об обоснованной границе отнесения предприятия к малым.

Укрупнённо решение указанной проблемы можно представить в виде следующей последовательности действий. Определяются объём продаж, характеризующий предприятия, как крупные, исходя из занимаемой ими доли рынка. По оставшимся предприятиям рассчитывается среднее значение годовых объёмов реализации, которые и представляют собой максимальные граничные значения, отделяющие малые предприятия от средних. Все расчёты необходимо проводить по видам деятельности, а в ряде случаев и подвидам, а не как сейчас - по укрупнённым сферам общественного производства. Очевидно, что объёмы продаж и занимаемые предприятиями доли рынков радикально различаются в различных видах деятельности. Происходящая в настоящее время цифровизация производства, как и иных сфер жизнедеятельности, создаёт для этого необходимые условия. Решение общих задач идентификации сферы малого бизнеса позволит повысить адресность и эффективность мер

государственного регулирования и стимулирования малых предприятий, имеющих как общие для данной сферы проблемы, так и связанные с конкретным видом их деятельности.

В 2019г. 3 035,4 тыс. человек были заняты на малых предприятиях (включая микропредприятия), занимавшихся торговлей оптовой и розничной, ремонтом автотранспортных средств и мотоциклов. Без микропредприятий численность занятых на малых предприятиях этого вида деятельности составляла 1 398 тыс. человек, обороты по данным предприятиям составили 16 923.6 млрд. руб. или 58,9% от оборотов всех малых предприятий Российской Федерации. По данным проведённых обследований в Ростовской области, 2,8% от общего числа малых предприятий, занимающихся оптовой и розничной торговлей, осуществляют экспортные операции. Основные проблемы, с которыми сталкиваются малые предприятия торговли-экспортёры имеют как общий для малого бизнеса характер, так и специфический, вытекающий из характера осуществляемых операций. К общим проблемам можно отнести недостаток собственных средств на создание предприятия и формирование необходимого оборотного капитала. Если затраты на создание предприятия, осуществляющего экспортные операции, не столь значимы и покрываются, в большинстве случаев, собственниками бизнеса, то недостаточность оборотного капитала создаёт существенные трудности. Получение кредитов на пополнение оборотных средств затрудняется почти повсеместным отсутствием у предприятий торговли-экспортёров адекватного залогового имущества. В связи с чем, приходится либо прибегать к заимствованиям средств у родственников и знакомых, либо обращаться за получением гарантий и (или) страхованию возврата кредитов в специализированных организациях, оказывающих содействие предприятиям-экспортёрам (Агентство ЭКСАР, организации содействия внешнеэкономической деятельности субъектов РФ и др.). Обращение в указанные организации предполагает опыт работы предприятия-экспортёра, как правило, не менее трёх лет и его хорошую экономику. Другой сложностью является то, что все организации, оказывающие помощь экспортёрам, являющиеся государственными, ведут свою деятельность на принципах коммерческого расчёта и в случае раскрытия гарантии или наступления страхового случая, собственников и руководителей предприятия-экспортёра ждут сложные разбирательства, приводящие, в ряде случаев, к ликвидации предприятия.

Решению отмеченных вопросов мог бы способствовать отказ от коммерциализации государственных организаций, способствующих развитию бизнеса экспортёров и перевод их документооборота с экспортёрами в систему блокчейн с подключением других заинтересованных сторон. Последнее бы повысило транспарентность

деятельности предприятий торговли, осуществляющих экспортные операции, и снизило бы риски организаций, взаимодействующих с ними в финансировании транзакций. Кроме того, внедрение технологии распределённого реестра во взаимодействие торговых предприятий-экспортёров с налоговыми органами могло бы автоматизировать, как уплату налогов, так и возврат последним НДС. Данное обстоятельство весьма важно при осуществлении экспортных операций, особенно при торговле низкомаржинальной продукцией, на пример сельскохозяйственной.

Таким образом, первоочередные меры по развитию малых предприятий торговли, осуществляющих экспорт продукции, должны включать в себя как решение общих для малого предпринимательства задач обоснованной идентификации составляющих эту сферу деятельности предприятий, что повысит адресность и эффективность целевых программ господдержки, позволит разработать адекватную систему налогообложения и отчислений в социальные фонды, так и специфических вопросов для предприятий этого вида деятельности. К последним относятся способы финансирования пополнения оборотного капитала предприятий торговли, осуществляющих экспорт продукции и их взаимодействие, в первую очередь, с налоговыми органами по возврату НДС.

Список использованных источников:

1. Lewandowska, A., Stopa, M. and G. Hummenny (2015). The European Union Structural Funds and Regional Development. The Perspective of SMEs in Eastern Poland. *European Planning Studies*, 23(4), pp. 785-797.
2. Pinkovetskaia I., Slepova V. (2018), "Estimation of fixed capital investment in SMEs: the existing differentiation in the Russian Federation", *Business Systems Research*, Vol.9, No.1, pp. 65-78.
3. Щемелев. С.Н., Шумаева Л.И. Системный характер предпринимательства и его развитие в малых организационно-правовых формах. *Финансовые исследования*. №2., 2019. Издательство РГЭУ(РИНХ), г. Ростов-на – Дону. Стр. 119-125
4. Щемелев С.Н., Шумаева Л.И., Козловский В.А. Идентификация сферы малого предпринимательства, как условие формирования эффективной системы стимулирования его развития. Материалы международной научно-практической онлайн конференции «Развитие российской экономики и её безопасность в условиях современных вызовов и угроз» Ростов-на –Дону, 21-22 апреля 2021г.

Положительные и отрицательные аспекты обращения криптовалют

М.Д. Исмоилова

самостоятельный исследователь, Ташкент

E-mail: malika_bazarova_94@mail.ru

научный руководитель: Р.И. Каюмов

к.э.н., зав. отделом Центра исследований при АУГА РУз, Ташкент

E-mail: Kayumov_1960@mail.ru

Аннотация: В статье на основе анализа раскрыты тенденции развития мировой экономики в условиях цифровизации, показано возрастание роли и уровня капитализации ИТ-компаний. Отражены положительные и негативные аспекты обращения криптовалют, объемы и виды которых в условиях цифровой трансформации экономики растут.

Ключевые слова: цифровая экономика, криптовалюта, биткоин, обеспеченность валюты, финансовая пирамида.

Positive and negative aspects of the circulation of cryptocurrencies

Abstract: Based on the analysis, the article reveals the trends in the development of the world economy in the conditions of digitalization, shows the increasing role and level of capitalization of an IT company. The positive and negative aspects of the circulation of cryptocurrencies are reflected, the volumes and types of which are growing in the conditions of digital transformation of the economy.

Keywords: digital economy, cryptocurrency, bitcoin, currency security, financial pyramid.

В современном мире происходят глобальные трансформации в сфере промышленности, экономики и науки под влиянием инноваций. Сейчас человечество живет в эпоху четвертой промышленной революции именуемая, как «Индустриальная революция 4.0». Основная особенность данного этапа общественного развития – усиление значимости цифровых технологий.

С 2010 года стали появляться киберфизические системы, адаптивные системы, зеленое производство, сетевые информационные системы. Появились 3D принтеры, повсеместно используется искусственный интеллект, роботизированная техника. Происходит цифровизация

промышленности и экономики. Все больше потребителей желают не приобретать физические объекты, а платить за предоставление услуг, к которым они получают доступ через цифровую платформу. В результате видоизменяются бизнес-процессы, трансформируются корпоративные бизнес-модели. Если во время предыдущих этапов развития общества передовыми компаниями считались нефтегазодобывающие, машиностроительные, металлургические, горнодобывающие, то сейчас рейтинги рыночной капитализации возглавляют IT-компании (Табл.1).

Таблица 1 – Рыночная капитализация компаний на март 2021 года

Rank	Company name	Location	Sector	31 March 2021		31 March 2020	
				Rank +/- (VS Mar 2020)	Market capitalisation (\$bn)	Rank	Market capitalisation (\$bn)
1	APPLE INC	United States	Technology	2	2,051	3	1,113
2	SAUDI ARAMCO	Saudi Arabia	Energy	-1	1,920	1	1,602
3	MICROSOFT CORP	United States	Technology	-1	1,778	2	1,200
4	AMAZON.COM INC	United States	Consumer Discretionary	0	1,558	4	971
5	ALPHABET INC	United States	Technology	0	1,393	5	799
6	FACEBOOK INC	United States	Technology	1	839	7	475
7	TENCENT	China	Technology	1	753	8	469
8	TESLA INC	United States	Consumer Discretionary	75	641	83	96
9	ALIBABA GRP	China	Consumer Discretionary	-3	615	6	522
10	BERKSHIRE HATHAWAY	United States	Financials	-1	588	9	443

Источник: Bloomberg with PwC analysis, PwC | Global Top 100 companies by market capitalization (May 2021).

В 2021 году компания Apple сместила Saudi Aramco с первого места, поднявшись с третьего места относительно 2020 года. Как можно заметить из 10 компаний возглавляющих рейтинг по рыночной капитализации, пять работают сфере IT-технологий. [1]

Согласно вышеизложенным данным наибольшее влияние на мировую экономику оказывают компании в сфере IT-индустрии и телекоммуникации.

Вместе с цифровой трансформации экономики происходит трансформация платежей за товары и услуги. Научные открытия и промышленные инновации способствовали развитию финансовых систем. Во время каждого этапа общественного развития появлялись новые формы и виды финансовых средств. Сначала это были акции, облигации, развитие фондовых бирж, появление электронных денег, дебетовых и пластиковых карт. Сегодня абсолютно новой формой платежей считается криптовалюта. Они выпускаются децентрализованно, независимо от государства и их стоимость обеспечивается спросом людей.

В 2018 году резко вырос спрос на криптовалюты, в результате произошел скачок их стоимости. Ниже приведена статистика общей рыночной капитализации криптовалют с 01.01.2016 года по 01.11.2021 в млрд. долл. США.



Рисунок 1 – Общая рыночная капитализация криптовалют

Источник: <https://coinmarketcap.com/ru/charts/>

Криптовалюты, как и обычные деньги выполняют схожие функции: выражают стоимость, являются средством обмена, накопления и сбережения. Но у них есть свои особенности, которые привлекают пользователей.

Криптовалюты обладают высокой степенью защиты. Развитие криптографии в настоящее время обеспечивает максимальное шифрование и конфиденциальность информации. Транзакции с использованием криптовалют проводятся без посредников, что обеспечивает низкую стоимость и высокую скорость проводимых операций. Высокая волатильность криптовалют привлекает спекулятивных инвесторов.

Многие люди желают увеличить свой капитал в виде фиатных валют, занимаясь покупкой и продажей криптовалют на криптовалютных биржах. Криптовалюта не повержена инфляции и подчиняется закону спроса и предложения среди пользователей и «майнеров» (люди, занимающиеся добычей криптовалют). Более того, предложение первой криптовалюты биткоина ограничена объемом в размере 21 млн. монет. [2]

То есть эта монета всегда будет дорожать, что является преимуществом перед обычными деньгами.

Криптовалюты децентрализованы, что предполагает их дефляционную природу. Правительства и центральные банки крупных стран не могут контролировать эмиссию, обращение и соответственно стоимость криптовалют. Это является одним из ключевых отличий криптовалютных средств. Это достигается благодаря технологии блокчейн. Блокчейн - совместно используемый и неизменный реестр, упрощающий процесс записей транзакций и учета активов в бизнес-сети. Принцип работы блокчейна заключается в том, что каждая транзакция записывается в виде блока данных. При этом каждый блок связан с предыдущим и последующим блоком. Таким образом, транзакции образуют неизменную цепочку блоков – блокчейн. При обновлении реестра и образовании нового блока, он уже не может быть изменен. [3]

Все это защищает транзакции и не дает возможность подделать блокчейн. К нему можно только добавлять новые записи. Важно учесть то, что реестр обновляется на всех компьютерах в сети одновременно. Взломать шифровальный код одного блока и заменить его на другой невозможно, так как для этого необходимо получить доступ одновременно к копиям базы данных на всех компьютерах в сети. [4]

В настоящее время, криптовалюты не участвуют в производстве добавленной стоимости и не могут служить его мерилom. Добавленная стоимость денег возникает при производстве товаров и услуг. Например, фермер, который выращивает овощи, мясо, хлеб, создает добавленную стоимость. Работник на заводе, делающий комплектующие части для производства машин, техники, оборудования, также создает добавленную стоимость. Майнер, занимаясь производством биктоина путем расходования электроэнергии, не создает добавленную стоимость. У криптовалют нет обеспечения, в современном его понимании. С принятием Ямайской валютной системы, национальные валюты перестали иметь золотое обеспечение, их курсы устанавливаются не государством, а рынком. Обеспечением национальной валюты являются экономическая значимость страны, ее авторитет, размер и темпы роста ВВП, природные ресурсы и полезные ископаемые.

За биткоином стоит потраченная энергия, которая не имеет полезного эффекта, поэтому эта криптовалюта не может использоваться в качестве капитала, даже фиктивного, т.к. не является производным от другого финансового инструмента. Эмитент криптовалюты не несет никакой ответственности ни за стабильность курса, ни за возможные махинации с ними.

Исходя из этих критериев обращение криптовалют схоже с функционированием финансовых пирамид, которые рано или поздно обязательно рухнут. Все это приводит к тому, что нет достаточных оснований считать криптовалюты настоящими деньгами. Все современные криптовалюты несут определенные угрозы при их использовании.

Анонимность участников сделок с помощью криптовалют позволяет некоторым пользователям покупать запрещенные товары, оплачивать или заказывать преступления в сети «даркнет». Данная глобальная сеть никаким образом не контролируется государством. Все совершаемые сделки практически невозможно выявить, отследить, заблокировать и соответственно наказать участников преступной деятельности. Сделки с криптовалютами необратимы. Операции не могут быть отменены, заблокированы, возвращены. Поэтому необходимо быть предельно осторожными при использовании криптовалют для оплаты или переводов.

Сооснователь майнинг-компании BitCluster Сергей Арестов назвал базовые принципы безопасности, которые необходимо соблюдать как при использовании криптовалют, так и при работе с фиатными активами:

- записывать и сохранять пароли и коды восстановления. При этом места хранения должны быть недоступны посторонним лицам;
- не использовать простые и легко запоминающиеся пароли;
- записывать доверенные IP-адреса;
- не хранить ключевую фразу (необходима для аутентификации) в одном месте, а разбить на две части и спрятать в разных местах;
- внимательно относиться к обновлениям кошельков, так как это может быть уловкой мошенников;
- прежде чем начинать активно пользоваться счетом, стоит попробовать его удалить и восстановить через фразу. [5]

Пока единого решения по дальнейшей стратегии развития криптовалют в мире не существует, нам представляется важным, что конкурентное развитие платежных систем электронных денег с большим количеством эмитентов должно находиться под обязательным контролем регуляторов финансовых рынков.

Учитывая, что платежные системы, как правило, преследуют цели достижения определенной операционной и экономической эффективности,

обращение криптовалют будет менее рисковым, если этот процесс содержать следующие основные элементы:

1. формальные договоренности между участниками системы;
2. согласованные и принятые технические стандарты и методы пересылки платежных распоряжений между участниками;
3. согласованные способы зачета взаимных требований участников и урегулирования проблемы с ликвидностью;
4. общие процедуры и правила работы, включая график работы, критерии участия, уровень комиссии и др. [6, с. 146-152]

В странах с развитой экономикой и устойчивой денежно-кредитной системой, со сложившейся традицией расчетных операций, криптовалюты возможно займут свою нишу, в которой их использование будет эффективно. В развивающихся же странах с молодой и пока неустойчивой денежно-кредитной системой необходим жесткий контроль при их внедрении.

В целом можно сделать вывод: обращение криптовалют - это новое явление, - прообраз принципиально новой системы денежного обращения. Поэтому важно активнее осуществлять исследования оценить потенциал криптовалют с точки зрения развития общества и государства, экономики страны, её информационно-технологического и финансового секторов, функционирования всех и каждого субъекта экономики (включая финансово-кредитные институты) и населения в новых экономических реалиях. Необходима объективная оценка положительных и отрицательных сторон криптовалют, выявление факторов, повышающих риски их использования и разработка механизмов по предотвращению или снижению таких рисков.

В настоящее время все больше число специалистов отмечает, что Ямайская валютная система устарела, не отвечает требованиям современной экономики, и поэтому необходимо разработать новую международную валютную систему. Однако, на наш взгляд, это система будет эффективной, если при ее реализации будут учтены и согласованы основные аспекты функционирования криптовалют.

Список использованных источников:

1. PwC | Global Top 100 companies by market capitalization (May 2021).
2. <https://rbc.ru/crypto/news/>
3. Куприяновский В.П., Синягов С.А., Климов А.А., Петров А.В., Намиот Д.Е. Цифровые цепи поставок и технологии на базе блокчейн в совместной экономике // International Journal of Open Information Technologies. 2017. №8.

4. Кочергин Д.А. Место и роль виртуальных валют в современной платежной системе // Вестник СПбГУ. Серия 5: Экономика. 2017. №1.
5. <https://www.rbc.ru/crypto/news/6062d39c9a79477265df81f4>
6. Панова Г.С., Валетдинова Э.Н. Ограничение наличного денежного обращения в борьбе с теневой экономикой/ Вестник МГИМО-Университета. - 2014. - № 1.

Постпандемическое восстановление мирового рынка прямых иностранных инвестиций и цифровизация в экономике

А.Л. Сапунцов

профессор кафедры финансового мониторинга НИЯУ МИФИ, Москва

E-mail: andrew@sapuntsov.ru

Аннотация: Проведено исследование конъюнктуры глобального рынка прямых иностранных инвестиций (ПИИ) в 2020-2021 гг. Изложены и анализированы данные о движении ПИИ в представлении по их формам, регионам и отраслям экономики. Автор приходит к выводу о запаздывающем характере восстановления глобального потока ПИИ и необходимости внедрения цифровых технологий в деятельности агентств по поддержке инвестиций (АПИ).

Ключевые слова: Африка, КОВИД-19, многонациональных предприятия (МНП), прямые иностранные инвестиции (ПИИ), цифровизация, агентство по поощрению инвестиций (АПИ).

Post-pandemic recovery of the global market of foreign direct investments and economic digitalization

Abstract: The study covers market research of the global foreign direct investment (FDI) flows in 2020-2021. Analysis of collected data on FDI flows represents its modalities, form, regions, and industries. The author concludes that it will take longer for the FDI flows to recover. It is necessary, to further implement digital technology into the work of investment promotion agencies (IPA).

Keywords: Africa, COVID-19, foreign direct investment (FDI), multinational enterprise (MNE), digitalization, investment promotion agency (IPA).

Вызванные пандемией КОВИД-19 негативные явления в мировой экономике представлялись весной 2020 г. в апокалиптических тонах. Имело место резкое снижение цен на сырье, индексов фондовых рынков, нарушение в работе международного транспорта. Трудности в лечении граждан и в оказании им медицинской помощи, нехватка коечного фонда и медицинского оборудования еще больше усугубляли паникерские настроения. Исследователи выдвигали гипотезы о грядущей кардинальной перестройке мировой экономики, необратимых сдвигах в центрах

экономической власти и выгодных для извлечения прибыли инвестиционных источниках, указывая: «Сквозь недужную хмарь пандемии и грозовые тучи экономического кризиса сегодня невозможно разглядеть конечную конфигурацию будущего миропорядка и правил экономических, политических и военно-силовых взаимоотношений между членами мирового сообщества» [4, с. 5].

Появление в середине 2021 г. новых штаммов коронавируса требует от мировой системы здравоохранения проведения масштабной вакцинации населения, а также разработки новых лекарственных препаратов и методов лечения коронавируса. Введение новых карантинных и разрешительных мероприятий посещения общественных мест вносит коррективы в прогнозирование выхода мировой экономики из состояния кризиса, постепенно затягивая его и делая возвращение к прежней жизни как бы невозможным. В условиях колоссальной эмиссии долларов США, принявших форму «вертолетных денег», наблюдается рост индексов мирового фондового рынка. Резкое повышение мировых цен на черные металлы и древесину, а также скачки цен на природный газ, имевшие место на европейских биржах осенью в 2021 г., свидетельствует о том, что после окончания пандемии КОВИД-19 расстановка сил в мировой экономике станет иной, так как «происходит борьба между глобальными игроками, надеющимися на коренное изменение соотношения сил в мире в свою пользу, и теми, кто в целом был бы удовлетворен сохранением „докоронавирусного“ баланса сил и интересов» [3, с. 5].

Помимо резкого спада в объемах глобального производства и обороте мировой торговли, коронакризис оказал существенно пагубное воздействие на конъюнктуру глобального рынка прямых иностранных инвестиций (ПИИ) и внес коррективы в экономические программы многонациональных предприятий (МНП). Тем не менее рассматриваемые явления не являются принципиально новыми, так как показатели инвестиционной активности имеют большую амплитуду колебаний в условиях кризиса.

Согласно обзорам Конференции ООН по торговле и развитию (ЮНКТАД), общемировой объем поступления ПИИ в 2020 г. составил один 957 млрд долл., сократившись на 35% относительно 1481 трлн долл. в 2019 г. [9; р. x]. Рассматриваемый спад оказался крайне глубоким, так как глобальные потоки ПИИ находились на уровне одного трлн долл. только 15 лет тому назад, и в условиях предыдущего экономического кризиса (получившего название мирового финансового кризиса) значение показателя все равно было выше – 1,2 трлн долл. (2009 г.).

В большей степени снижение объемов поступления ПИИ затронуло развитые страны (290 млрд долл. и 749 млрд долл. в 2020 г. и 2019 г., спад

на 58%), нежели чем развивающиеся страны (667 млрд долл. и 732 млрд долл. соответственно, спад на 8%), при этом в странах с переходной экономикой снижение также было значительным (58 млрд долл. и 24 млрд долл. соответственно, спад на 58%) [9, р. 4]. Объемы поступления ПИИ в беднейшие страны напротив увеличились с 23 млрд долл. до 24 млрд долл. соответственно, что было обусловлено необходимостью продолжения и окончания работ по отдельным относительно крупным инвестиционным проектам.

Своего рода «инвестиционный крах» наступил в странах ЕС, куда в 2020 г. поступило лишь 70 млрд долл. ПИИ против 378 млрд долл. годом ранее. Российская Федерация поставила антирекорд, получив лишь 10 млрд долл. ПИИ в 2020 г. против 32 млрд долл. в 2019 г, причем эксперты ЮНКТАД дают ясную оценку результатам экономического строительства в Российской Федерации: ее «экономика существенным образом зависит от инвестиций в добычу полезных ископаемых» [9, р. 4]. Спад в объемах поступления ПИИ по регионам в 2020 г. представлен следующим: Европа – 80%, Северная Америка – 42%, Африка – 16%, Южная Америка – 45%; только в развивающихся странах Азии показатель увеличился на 4% [9, р. 4-6].

Введение локдаунов как меры борьбы с распространением пандемии КОВИД-19 привело как к снижению темпов реализации текущих инвестиционных проектов, так и к отмене анонсированных МНП проектов в условиях преобладания пессимистических ожиданий экономической конъюнктуры. Проводя анализ данных ЮНКТАД по анонсированным проектам в «зеленом поле» на мировом уровне, в 2020 г. наибольшее замедление инвестиционной активности наблюдалось в строительстве, автомобилестроении, на транспорте и в услугах хранения. В указанном году объемы поступления ПИИ в пищевую, фармацевтическую промышленность и торговлю сохранили свои значения, а поступления ПИИ в информационные технологии и связь увеличились. Анализ массива данных по 36-ти странам, проведенный за декабрь 2020 г. – октябрь 2020 г., позволил прийти к выводу о крайне пагубном воздействии кризиса на общество, причем «нельзя недооценивать такое воздействие на экономические отношения» [10, р. 1610].

Воздействие экономического кризиса на мировые потоки ПИИ особенно выражено наблюдалось в первом полугодии 2020 г., тогда как во втором полугодии – произошло оживление в заключении трансграничных слияний и приобретений компаний (СиП), а также сделок по международному проектному финансированию [8, р. 15-16]. В свою очередь поступление ПИИ в создание новых мощностей и производств (СНМП) сохранялось на низком уровне во второй половине 2020 г. и в

первом полугодии 2021 г. Это еще в большей степени усилило экономический кризис в развивающихся странах, так как для этих стран инвестиции в СПМП представляют особую значимость за счет поступления новых технологий и ценного импортного оборудования.

Пандемия КОВИД-19 вызвала целую серию экономических потрясений в странах Глобального Юга, не обойдя стороной Африку. «Важными социальными последствиями вспышки коронавируса для африканских граждан стал рост социальной тревожности и напряженности среди семей и граждан» [1, с. 32]. В 2020 г. объемы поступления ПИИ в страны Африки составили 40 млрд долл., уменьшившись на 16% относительно прошлого года [9, р. 40]. Спад инвестиционной деятельности в Африке оказался несколько более глубоким, чем в целом по развивающимся странам. Более того, Африка впервые за последние 25 лет вошла в фазу экономической рецессии, вызванной замедлением деловой активности и ограничениями на передвижение людей и грузов, что отрицательно сказалось на инвестициях.

В 2020 г. поступление в страны Африки ПИИ в СНМП сократилось на 62% до 29 млрд долл., объемы международного проектного финансирования – 74% до 32 млрд долл., ПИИ с СиП – 45% до 3,2 млрд долл. [9, р. 40]. Наибольшая стагнация в притоке ПИИ имела место в странах Африки, где экономике доминируют отрасли добывающей промышленности, что было обусловлено резким спадом мировых цен на энергоносители. В крупнейшей экономике Африки – Нигерии короавирусный локдаун в экспорте нефти вызвал шок в финансовой сфере (воздействие на валютный курс, темп инфляции, состояние платежного баланса) [7; р. 132-133]. Напротив, в Замбии были внесены коррективы в меры государственного регулирования экономики, за счет которых стало возможным извлечь выгоды из повышения мировых цен на медь в 2021 г. и привлечь ПИИ в большем объеме [5; р. 35].

По последним данным за первое полугодие 2021 г., глобальные потоки ПИИ составили 852 млрд долл., что на 78% больше аналогичного периода прошлого года и превосходит оптимистические прогнозы. Подробные данные о движении ПИИ в представлении по регионам и группам стран (в том числе по анонсированным проектам в «зеленом поле»), а также данные в представлении по секторам мировой экономики и десяти видам экономической деятельности [6, р. 3-5]. Развитые страны смогли привлечь 424 млрд долл. ПИИ, что на 193% превосходит показатель первого квартала 2020 г., развивающиеся – 427 млрд долл., на 28% больше; показатель для наименее развитых стран уменьшился на 9% до 11 млрд долл. [6, р. 3].

Кризисные явления, имевшие место в мировой экономике за 2020-2021 гг., включили в себя стагнацию глобального рынка ПИИ и замедление в

хозяйственной деятельности МНП. Ожидается, что в ближайшее время мировой рынок ПИИ пройдет перигей своей конъюнктуры, и за второе полугодие 2021 г. объемы поступающих инвестиций, вероятно, увеличатся на 15-20% по отношению к первому полугодью. Столь скромное восстановление определяется появлением новых штаммов коронавируса, неопределенностью доступа населения мира к вакцинам и вопросам к их эффективности, а также сохранением локдаунов и ограничений в отдельных видах экономической деятельности.

Посткризисное восстановление рынка ПИИ происходит крайне неравномерно по странам и регионам мира. Лидерами по оживлению инвестиционной деятельности в Глобальном Юге выступают страны Восточной и Юго-Восточной Азии. Представляется целесообразным разработать в странах Африки правительственные меры, «которые позволят „перезагрузить“ экономику после окончания коронавируса, таки[е] как снижение цен на энергоносители..., предоставление помощи малому бизнесу..., программы сохранения рабочих мест во время кризиса и входе последующего восстановления экономики» [2, с. 372].

Для оживления на рынке ПИИ представляется важным улучшить работу агентств по привлечению инвестиций (АПИ) на основе внедрения цифровых технологий. Проведенное исследование показало востребованность услуг АПИ при вложении капитала в сельское хозяйство, сферу информационных технологий и связь, фармацевтику, электроэнергетику и коммунальное хозяйство, а также горно-шахтное дело [9; р. 20]. Ожидается, что в условиях посткризисного восстановления мировой экономики АПИ проведут дальнейшую цифровизацию условий оказания своих услуг и мероприятий по росту охвата своей клиентской базы, включая расширение своего присутствия в Интернете, проведение вебинаров и виртуальных конференций, а также налаживание сотрудничества с некоммерческими организациями.

Список использованных источников:

1. Дробот Е.В., Макаров И.Н., Сапунцов А.Л. Распространение коронавируса в Африке: региональные паттерны и экономические последствия // Экономические отношения. 2021. № 1. С. 13-38. DOI: 10.18334/ео.11.1.111816
2. Дробот Е.В., Макаров И.Н., Сапунцов А.Л. Трансформация отраслевой структуры инновационного бизнеса в Африке и вызовы пандемии коронавируса // Вопросы инновационной экономики. 2021. № 1. С. 351-378. DOI: 10.18334/vinec.11.1.111858

3. Фитуни Л.Л. Коронавирус и «конец истории» // Ученые записки Института Африки РАН. 2020. № 2. С. 5-13. DOI: 10.31132/2412-5717-2020-51-2-5-13
4. Фитуни Л.Л., Абрамова И.О. Развивающиеся страны в политической экономике посткоронавирусного мира // Мировая экономика и международные отношения. 2020. Т. 64. № 9. С. 5-14. DOI: 10.20542/0131-2227-2020-64-9-5-14
5. Africa's Pulse. An Analysis of Issues Shaping Africa's Economic Future / No. 24, Oct. International Bank for Reconstruction and Development. Wash. D.C.: World Bank Group, 2021. III, 102 p. DOI: 10.1596/978-1-4648-1805-9
6. Investment Trends Monitor / UNCTAD. 2020. I. 39. Oct.
7. Nwosa P.I. Oil price, exchange rate and stock market performance during the COVID-19 pandemic: implications for TNCs and FDI inflow in Nigeria. Transnational Corporations Review. 2021. Vol. 13. I. 1. P. 125-137. DOI: 10.1080/19186444.2020.1855957
8. World Investment Report. International Production Beyond the Pandemic / UNCTAD. N.Y.; Geneva: UN, 2020. XVII, 247 p. ISBN 978-92-1-112985-4.
9. World Investment Report. Investing in Sustainable Recovery / UNCTAD. N.Y.; Geneva: UN, 2021. XVI, 267 p. ISBN 978-92-1-113017-1
10. Zhang H., Ding Y., Li J. Impact of the COVID-19 Pandemic on Economic Sentiment: A Cross-Country Study // Emerging Markets Finance and Trade. 2021. Vol. 57. I. 6. P. 1603-1612. DOI: 10.1080/1540496X.2021.1897005

Практические аспекты оценки соответствия требованиям защиты информации Банка России

А.В. Глазков

Акционерное общество «Перспективный мониторинг»

E-mail: Aleksey.Glazkov@amonitoring.ru

О.А. Иванов

Акционерное общество «Перспективный мониторинг»

E-mail: Oleg.Ivanov@amonitoring.ru

И.Ю. Червяков

Акционерное общество «Перспективный мониторинг»

E-mail: Ivan.Chervyakov@amonitoring.ru

Аннотация: Целью данной работы является показать практические аспекты оценки соответствия требованиям защиты информации Банка России. Отражены основные уровни соответствия защиты информации и основные пункты которые аудитор должен затрагивать при выполнении аудиторской проверки.

Ключевые слова: требования защиты информации, аудит, информация.

Practical aspects of assessing compliance with the information security requirements of the Bank of Russia

Abstract: The purpose of this work is to show the practical aspects of assessing of compliance with the requirements of the Bank of Russia. Reflected the main levels of compliance with information security and the main points that the auditor should touch upon when performing an audit.

Keywords: information security requirements, audit, information.

Введение

Не так давно Банк России перешёл на нормативные акты нового типа, в части требований по защите информации которых, они ссылаются на требования ГОСТ Р 57580.1 [1]. Также ими установлены требуемые уровни защиты информации и уровни соответствия защиты информации.

В этих двух почти одинаково звучащих понятиях многие зачастую путаются. Уровень защиты информации определяет состав организационных и технических мер защиты информации. В ГОСТ Р

57580.1 определены три уровня защиты информации: минимальный (уровень 3), стандартный (уровень 2) и усиленный (уровень 1).

Уровень соответствия защиты информации определяет, в какой степени финансовая организация реализовала организационные и технические меры защиты информации. В ГОСТ Р 57580.2 [2] установлено пять уровней соответствия. В соответствии с требованиями нормативных актов Банка России в итоге финансовые организации должны обеспечить уровень соответствия не ниже четвёртого.

Актуальные нормативные акты Банка России по защите информации:

№683-П от 17 апреля 2019;

№719-П от 4 июня 2020;

№747-П от 23 декабря 2020;

№757-П от 20 апреля 2021.

Соответствие требованиям Банка России

Одни из распространенных вопросов во многих организациях возникают: когда же надо соответствовать. При этом зачастую ссылаются на письма Банка России в которых определены сроки проведения оценки соответствия. Здесь важно различать два аспекта: когда соответствовать и когда проводить оценку. В своих разъяснениях Банк России определяет допустимые сроки проведения оценки соответствия, но сроки обеспечения Банком того или иного уровня соответствия остаются неизменными относительно требований его нормативных актов. Например, уже сейчас кредитные организации должны обеспечивать третий уровень соответствия. В рамках комплексных или тематических проверок Банк России может проверить реализацию отдельных требований и при их невыполнении выдать предписания по устранению несоответствий. Однако с оценкой соответствия лучше не затягивать, поскольку к установленному сроку все аудиторы на рынке будут перегружены работой, так как многие организации будут делать всё в последний день, из-за чего может возникнуть длительное ожидание своей очереди или получить некачественную оценку. Кроме того, представляется целесообразным сначала выполнить предварительную оценку, понять своё состояние защищённости. Далее реализовать недостающие меры и уже после этого провести оценку соответствия, результаты которой потом предоставить Банку России.

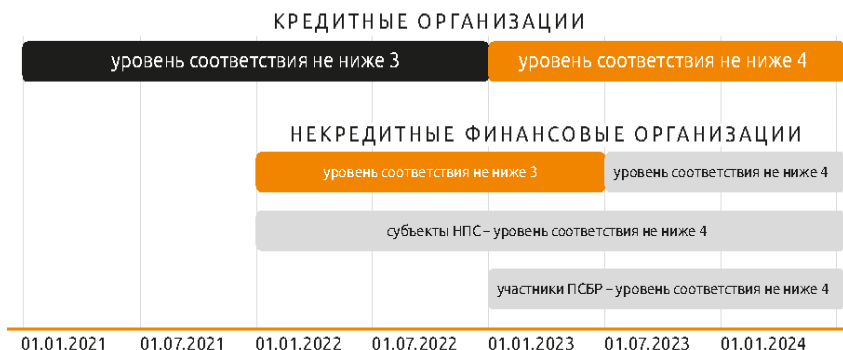


Рисунок 1 – Даты соответствия требованиям

Перед заключением договора на оценку соответствия требованиям стоит обратить внимание на ряд аспектов, которые могут повлиять на состав заказываемых работ.

На начало 2022 года, например, для кредитных организаций, будет действовать несколько нормативных актов, которые требуют соответствия стандарту Банка России. Рассмотрим минимальную область оценки ГОСТ Р 57580.1:

683-П, 719-П:

АБС и ДБО;

АРМ пользователей АБС и ДБО;

АРМ администрирование АБС и ДБО;

сетевое оборудование;

контроллер домена.

747-П:

АРМ КБР-Н;

АБС.

Правила платёжных систем, отличных от платёжной системы Банка России (при включении их владельцами в них соответствующих требований):

АРМ взаимодействия с платёжными системами.

Приказ Минкомсвязи России от 25.06.2018 №321:

инфраструктура ЕБС.

Как видим, для кредитных организаций область оценки требованиям ГОСТ Р 57580.1 в области действия №683-П и №719-П, как правило, одинакова.

Опережая дальнейшие наши рассуждения хочется пояснить, что ряд мер ГОСТ Р 57580.1 ориентированы на конкретный объект (систему),

например, требования управления доступом должны быть реализованы и, в ходе оценки соответствия, проверены в каждой, входящей в объект оценки, системе, а ряд мер ориентирован на организацию процесса в рамках всей организации, например, управление инцидентами защиты информации. Исходя из этого, при небольшом объекте оценки, например, объект положения № 747-П, много трудозатрат всё равно уйдёт на оценку мер, ориентированных на организацию процесса в рамках всей организации. Потому оценку требованиям ГОСТ Р 57580.1 в области действия, например, Положения №747-П отдельно проводить экономически нецелесообразно.

Исходя из опыта, целесообразно заказывать комплексную оценку требованиям ГОСТ Р 57580.1 сразу в области действия №683-П, №719-П, №747-П, Приказа Минкомсвязи России от 25.06.2018 №321, что позволит снизить затраты на оценку соответствия по сравнению с заключением отдельных договоров по каждому из этих нормативных актов. Результаты такой оценки соответствия могут быть предъявлены в рамках отчётности перед Банком России.

Что ещё следует включить в состав работ.

В состав работ целесообразно включить оценку реализации технологических мер защиты информации и требований к применению СКЗИ.



Рисунок 2 – Состав защиты информации

Большинство банков уже 2 года получают сообщения от Банка России с требованием представить результаты самооценки по положению № 683-

П. Для этих мер не установлены требования проводить оценку соответствия силами сторонних организаций. Однако, если у вас нет собственных ресурсов провести подобную оценку, вы можете заказать данную услугу у нас.

Банки привыкли, что требования положения № 382-П можно было реализовать на бумаге. Однако такой подход неприемлем для требований ГОСТ Р 57580.1.

В отличие от положения № 382-П, ГОСТ регламентирует способ реализации меры защиты информации (технический и организационный) и аудитор должен проверить, внедрены ли средства защиты информации, реализующие соответствующие технические меры защиты информации.

Какие системы в идеале необходимы для обеспечения четвёртого уровня защиты информации:

- Система управления доступом.

- Система учёта информационных активов.

- Антивирусные средства.

- Средства межсетевого экранирования.

- Средства обнаружения (предотвращения) вторжений.

- Система мониторинга событий защиты информации.

- Система управления инцидентами.

- Система защиты платформ виртуализации.

- Сканер уязвимостей.

- Система управления мобильными устройствами.

После прослушивания вебинаров ряда консультантов по вопросам соответствия требованиям ГОСТ Р 57580.1 у банков возникает ощущение, что технические меры защиты информации можно заменить компенсирующими организационными мерами, либо исключить их, разработав соответствующую модель угроз.

Хотелось бы отметить, что состав мер защиты информации ГОСТ Р 57580.1 сформирован исходя из типового ландшафта угроз, характерных для финансовых организаций. Можно с высокой степенью вероятности утверждать, что исключение каких-либо мер защиты информации или замена на организационные, приведёт к возрастанию риска информационной безопасности относительно ситуации, когда эта мера была бы реализована с применением технических средств. Такая ситуация противоречит методологии ГОСТ Р 57580.1.

Давайте рассмотрим простой вариант. Типовое рассуждение: «внедрение SIEM дорогое удовольствие, и я буду вручную просматривать журналы событий, мне этого будет достаточно». Однако, просмотр событий вручную, во-первых, будет делаться не в режиме on-line, во-

вторых, просмотр журнала событий вручную - очень трудоёмкая задача, требующая большой концентрации внимания и высокой компетенции. Такой подход не позволит коррелировать события из журналов различных средств.

Таким образом, второй вариант никак не сможет в той же мере минимизировать риски информационной безопасности, как вариант с применением SIEM, т.к. SIEM при должной настройке позволит выявлять атаки практически в режиме on-line. То есть, условие, что компенсирующая мера должна минимизировать риски в той же мере, что и основная, не выполняется.

Другой способ попытки соответствия, к которому пытаются прибегнуть компании – создание модели угроз. Они делают это в надежде получить перечень актуальных и неактуальных угроз, дабы сэкономить при введении средств защиты информации, сосредоточившись только на самых важных проблемах. То есть такая модель угроз, фактически, определяет остаточные риски после применения неких средств защиты информации.

Однако здесь кроется много подводных камней. Как правило, неактуальность угрозы обосновывается наличием тех или иных защитных мер. И здесь возникает вопрос тот же, что и при выборе компенсирующих мер. Обеспечивается ли применяемыми мерами тот же уровень рисков защиты информации, что и при применении мер ГОСТ Р 57580.1.

Банковский ГОСТ Р нацелен на оснащение организации «джентельменским набором» технических средств, необходимыми для защиты от угроз, как внутренних, так и внешних.

Учитывая, что внедрение мер защиты информации вносит только 50% в значение оценки соответствия (в соответствии с методикой ГОСТ Р 57580.2), только внедрение технических средств без организации должного управления процессами защиты информации не позволит достичь требуемого уровня соответствия. Не стоит забывать о документировании процессов защиты информации и всех применяемых мер, полноценном охвате защитными мерами всех объектов информационной инфраструктуры, входящих в регулируемые области, организации контроля и совершенствования защиты информации.

Таким образом, одним из недорогих приёмов с помощью которого можно повысить оценку соответствия является приведение внутренней нормативной базы в соответствие с требованиями нормативных актов Банка России по обеспечению защиты информации и ГОСТ Р 57580.2.

Какие же действия необходимо выполнить с внутренними нормативными документами для достижения необходимого уровня требований:

Разработать и ввести в действие внутренние нормативные документы для всех процессов защиты информации ГОСТ Р 57580.1.

Определить область действия документов.

Регламентировать все организационные и технические меры защиты информации.

Определить в документах соответствие нормативным актам Банка России в области защиты информации и ГОСТ Р 57580.1.

Дополнительные организационные аспекты, на которые необходимо обратить внимание:

Высокий уровень интеграции деятельности подразделений информационных технологий и информационной безопасности.

Усиление контрольных функций службы информационной безопасности, в том числе, в области мониторинга защиты информации.

Повышение квалификации персонала по всем процессам защиты информации.

Повышение осведомлённости сотрудников по всем процессам защиты информации.

Документальная фиксация всех решений по улучшению защиты информации.

Приобретение «коробочных» АБС и ДБО не отменяет требований к жизненному циклу автоматизированных систем.

Аутсорсинг информационных технологий или защиты информации.

Использование аутсорсинга информационных технологий или защиты информации не снимает с кредитных организаций ответственности за ущерб, причинённый клиентам банка от действий со стороны злоумышленника.

Поэтому при выборе поставщика услуг важно понимать насколько хорошо у поставщика услуг организована деятельность по защите информации.

Перед заключением договора целесообразно тем или иным образом выяснить насколько качественно этот поставщик обеспечивает защиту информации как в отношении своих информационных активов, так и информационных активов своих клиентов. Для этого могут быть применены способы от опросного листа до независимого аудита поставщика услуг.

Перед оформлением договора важно продумать все моменты, связанные с предоставлением вам поставщиком услуг информации как относительно качества предоставляемой услуги, включая обеспечение защиты информации, так и относительно предоставления поставщиком информации, необходимой вам для выполнения регуляторных требований.

С точки зрения выполнения регуляторных требований, в договор можно включить как требование выполнения поставщиком услуг периодической независимой оценки соответствия, так и детальные требования защиты информации, требование об участии поставщика услуг в процессе оценки соответствия и предоставлении оценщику всей необходимой информации.

В первом случае при проведении оценки соответствия вы предоставляете отчёт проверяющей организации, отчёт от поставщика услуги, а во втором привлекаете его специалистов к проводимой вами оценке соответствия.

Заключение

В данной работе рассмотрены практические основы соответствия требованиям защиты информации Банка России. Описана процедура действий и проверка соответствия регламентирующим документам перед заключением договора.

В статье так же показаны риски привлечения аутсорсинга для использования информационных технологий и защиты информации.

Так же необходимо отметить, что для соответствия требованиям защиты информации Банка России придется изучить большое количество нормативных актов, поэтому большинство компаний для соответствия описанным ранее требованиям привлекают компетентные компании для выстраивания бизнес процессов и процессов разработки документов для прохождения аккредитации на соответствие требований.

Список использованных источников:

1. ГОСТ Р 57580.1 Защита информации финансовых организаций. Базовый состав организационных и технических мер.
2. ГОСТ Р 57580.2 Защита информации финансовых организаций. Методика оценки соответствия.

Применение анализа голоса и речи в защите от социальной инженерии

В.А. Рычков

старший преподаватель кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: VARychkov@mephi.ru

В. Давыденко

старший преподаватель кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: VIDavydenko@mephi.ru

А.В. Перепечаев

студент 2 курса НИЯУ МИФИ, Москва

E-mail: alexanderperepechaev@mail.ru

Аннотация: В работе представлен обзор текущих проблем, связанных с применением злоумышленниками методов социальной инженерии для атак на крупные компании. А также предложены идеи по применению технологий анализа голоса и речи человека для защиты от атак злоумышленников, использующих методы социальной инженерии.

Ключевые слова: социальная инженерия, голос, речь, идентификация, текст, распознавание.

Application of voice and speech analysis in defense against social engineering

Abstract: This paper provides an overview of the current problems associated with the use of social engineering techniques by cybercriminals to attack large companies. Also, ideas were proposed for using technologies for analyzing human voice and speech to protect against attacks by malefactors using social engineering methods.

Keywords: social engineering, voice, speech, identification, text, recognition.

Основной проблемой в сфере информационной безопасности остаётся социальная инженерия. Злоумышленники часто звонят сотрудникам компаний по телефону, чтобы, например, представиться специалистом техподдержки и получить важные данные или заставить собеседника

совершить нужное действие (например, установить вредоносное программное обеспечение).

Accenture Security сообщает, что 85% организаций в настоящее время сталкиваются с фишингом и социальной инженерией, что на 16% больше, чем год назад [1]. Также отчет Positive Technologies сообщает, что 38% организаций вообще не проводят тренинги для сотрудников по вопросам информационной безопасности, а 37% делают это формально, без какой-либо проверки эффективности [2]. По результатам исследований Positive Technologies [3] 44% сотрудников в результате телефонного взаимодействия выдавали свои пароли, рассказывали об установленном ПО, переходили по требуемой ссылке.

Статистики насколько часто злоумышленники используют голосовой фишинг не найдено, так как достаточно сложно собрать подобную информацию, да и многие компании, которые подверглись социальной инженерии, не обнародуют данную информацию, так как боятся репутационного ущерба. Но если говорить о голосовом фишинге в целом, то он служит скорее вспомогательным инструментом при атаке, нежели основным. Злоумышленнику в любом случае изначально нужно составить сценарий атаки, подготовиться технически (фишинговый сайт, вредоносный файл и тд), а голосовой фишинг он может использовать как один из этапов для достижения цели.

Пример из практики одной компании, который мне рассказал один из сотрудников:

“Заказчик хотел проведение социальной инженерии любыми методами в своей компании. Была подготовлена легенда, разосланы письма с фишинговыми ссылками. Некоторое количество сотрудников перешли по ссылке/ввели свои доменные учетные данные, соответственно были получены доступ к почте сотрудников и возможность развивать атаку дальше. Через 10–15 минут после начала атаки, ИТ отдел начал бить тревогу и разослал письма всем сотрудникам, что компания подверглась атаке, и чтобы никто не переходил по данным ссылкам. Учитывая то, что нужно было получить больше учетных записей, было решено прибегнуть к голосовому фишингу. По найденным рабочим номерам некоторых сотрудников, были осуществлены звонки, «злоумышленники» представлялись именем, которое было указана в письмах от ИТ отдела.

Разговор был примерно следующим:

– Марина Ивановна, добрый день, я Иванов Иван из ИТ отдела, мы только что вам и всем сотрудникам присылали письма об атаке, вы его читали?

– Да, читала.

– А само фишинговое письмо открывали?

– Да, но куда по ссылке не переходила.

– Это хорошо, но нам нужно, чтобы вы запустили антивирус на своем компьютере, чтобы мы убедились

– Хорошо, что мне нужно сделать?

Соответственно сотруднику был отправлен вредоносный exe-файл, при запуске которого появлялся доступ к shell.»

И таких ситуаций можно привести очень много: просьба рассказать об установленных программах, дать удаленный доступ, пароли и логины, перейти на определенный сайт.

Для защиты от подобных атак по телефону нужно хорошо подготовить сотрудников компании, но также можно прибегнуть к созданию технических средств защиты.

Анализировать разговор на предмет применения методов социальной инженерии можно с помощью технологий машинного обучения и нейронных сетей.

Для работы системы, определяющей социального инженера по телефону, можно использовать следующие подходы:

1. Идентификация злоумышленника по голосу, сравнение с существующей базой голосов злоумышленников;
2. Перевод речи в текст;
3. Поиск в полученном тексте речевых конструкций, указывающих на злоумышленника.

Также можно использовать дополнительные параметры для определения злоумышленника, использующего методы социальной инженерии:

1. Пол говорящего: мужчины и женщины по-разному испытывают стресс и лгут;

2. Возрастная группа: от возраста же зависят голосовые характеристики и уровень знаний, так как с возрастом на человеке отражается все прожитое им, увеличивается его багаж знаний. Для определения возраста по голосу может быть разработана отдельная нейронная сеть;

3. Процентное содержание каждой из 6-ти базовых эмоций: вполне возможно, что у социального инженера будет больше преобладать нейтральные эмоции без негатива;

4. Изменение эмоций во времени: Поллом Экманом предлагалась теория микровыражений на лице для определения лжи [4] (когда на лице на долю секунды проступает другая эмоция), вполне возможно, что в голосе также можно определить подобные изменения;

5. Паузы, тембр, скорость речи и тому подобное: данные параметры скорее всего не позволят определить социального инженера, так как в

отличии от спонтанной лжи – социальный инженер основательно готовится к предстоящему разговору, однако их все равно стоит рассмотреть, так как возможно в них будет полезная информация;

6. Наличие определенных слов в разговоре и тема разговора: вполне вероятно, что если звонящий спрашивает про пароли или предлагает открыть письмо, которое пришло на почту, то он может быть социальным инженером.

Применение вышеописанных подходов позволит при наличии аудиозаписи разговора определить применение злоумышленником методов социальной инженерии.

Для получения лучшего эффекта предлагается анализировать аудиозапись в режиме реального времени и сообщать службе безопасности о возможных атаках. Таким образом возможно предотвратить атаку в реальном времени или хотя бы оперативно отреагировать на атаку.

Основываясь на вышеизложенной информации, можно отметить, что и по сегодняшний день многие компании испытывают проблемы при применении злоумышленниками методов социальной инженерии. Таким образом интеллектуальная система, основанной на анализе голоса и речи человека, может оказать существенную поддержку компаниям, которые сталкиваются с атаками социальных инженеров.

Список использованных источников:

1. Навигация в океане социальной инженерии [Электронный ресурс]. – URL: <https://www.securitylab.ru/contest/499701.php>
2. Отчет Positive Technologies: социальная инженерия открывает хакерам двери вашей компании [Электронный ресурс]. – URL: <https://www.securitylab.ru/news/492267.php>
3. Как социальная инженерия открывает хакеру двери в вашу организацию [Электронный ресурс]. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/social-engineering/>
4. Экман Пол - Психология лжи [Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage] / Пер. с англ. Н. Исуповой, Н. Мальгиной, Н. Миронова, О. Тереховой. — СПб.: Питер, 2010. — 270 с.

**Применение искусственных нейронных сетей для
прогнозирования девиантной деятельности кредитных
организаций как субъектов финансового мониторинга**

А.С. Приказчикова

Главный специалист-эксперт Управления развития информационных
технологий финансового мониторинга Федеральной службы по
финансовому мониторингу, Москва

E-mail: aska4.92@mail.ru

Научный руководитель: В.В. Иванов

д.ф.-м.н., профессор кафедры прикладной математики
№ 31 института лазерных и плазменных технологий

НИЯУ МИФИ, Москва

E-mail: ivanov@jinr.ru

Аннотация: В статье обсуждаются вопросы применения искусственных нейронных сетей для идентификации девиантной деятельности кредитных организаций, потенциально вовлеченных в противоправную деятельность по легализации преступных денежных средств и финансированию терроризма.

Ключевые слова: машинное обучение; нейронные сети; кредитные организации; девиантная деятельность; легализация денежных средств; финансирование терроризма.

**The artificial neural networks application for forecasting the deviant
activity of credit institutions as financial monitoring subjects**

Abstract: The article presents the artificial neural networks applying results in order to identify the deviant activities of credit institutions potentially involved in illegal activities for the criminal funds legalization and terrorism financing.

Keywords: machine learning; neural networks; credit organizations; deviant activity; money laundering; terrorist financing.

Как известно, важнейшим условием обеспечения национальной безопасности государства является стабильность его экономической системы. Одним из элементов такой системы являются кредитные организации, репутационные риски которых необходимо оценивать [1].

Современные технологии анализа финансового состояния кредитных организаций базируются на накоплении, систематизации и обработке большого количества информационных ресурсов, одним из которых является официальная финансовая отчетность, публикуемая на сайте Центрального банка Российской Федерации. Используемые методики расчетов экономических показателей не всегда очевидны, а результаты – интерпретируемы [2]. В связи с чем с целью увеличения скорости реакции на изменение внешней среды представляется целесообразным использовать отдельные математические алгоритмы, в частности методы нейронных сетей.

В настоящем исследовании в качестве исходных данных использовались сведения из банковской отчетной формы № 101 за период с января 2013 года по декабрь 2020 года включительно. Актуальные данные за 2021 год использовались для проверки корректности прогнозных значений.

Целью исследования являлось повышение эффективности выявления кредитных организаций с высокой степенью финансовых рисков, которые при этом могут быть вовлечены в деятельность по отмыванию денег и финансированию терроризма (далее – ОД/ФТ).

Актуальность настоящей работы обуславливается необходимостью разработки новых методик и алгоритмов обнаружения потенциально проблемных кредитных организаций, использующих финансовую систему России для легализации полученных преступным путем денежных средств.

Обработка информации о деятельности кредитных организаций начинается с представления анализируемых объектов векторами показателей $x^{(1)}, x^{(2)}, \dots, x^{(p)}$, для которых отношение «больше – меньше» не определено. Эта неопределенность носит фундаментальный характер и для своего преодоления требует изыскания и разработки адекватных оценок объектов векторной природы.

Реализация этих методик в информационной системе Росфинмониторинга позволит осуществлять оперативную автоматизированную классификацию кредитных организаций в целях установления факта их вовлеченности в противоправную деятельность по легализации денежных, полученных преступным путем.

Для целей настоящей работы были использованы наиболее распространенные методы нейронных сетей, как разновидности машинного обучения.

Искусственные нейронные сети являются одним из основных направлений современной теории искусственного интеллекта. Первые нейронные сети были разработаны У. Маккалоком и У. Питтсом. После разработки алгоритмов обучения получаемые модели стали использовать в

практических целях: в задачах прогнозирования, для распознавания образов, в задачах управления и др.

Базовый уровень сети, перцептрон, является по сути математическим аналогом биологического нейрона в головном мозге человека (см. рис. 1).

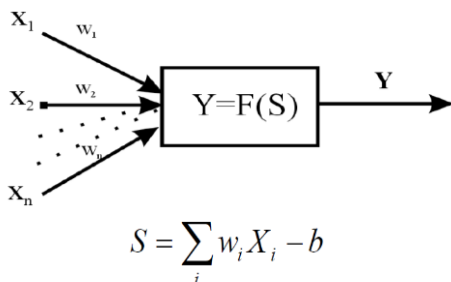


Рисунок 1 – Имитация нейрона

Первый слой нейросети называется входным. Каждый узел этого слоя получает на вход какую-либо информацию и передает ее на последующие узлы в других слоях. Чаще всего между узлами одного слоя нет связей, а последний узел цепочки выводит результат работы нейросети (см. рис 2). Узлы посередине нейросети называются скрытыми [3]. Как правило, нейронные сети классифицируются на 2 основных типа: нейросети с учителем и нейросети без учителя. Первый вариант подразумевает наличие заранее известных исходов обработки нейросети.

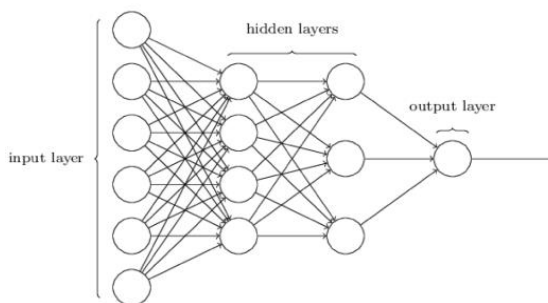


Рисунок 2 – Структура нейронной сети

Для каждого элемента сети (нейрона) существует определенное правило, в соответствии с которым рассчитывается его выходное значение. Это правило называется функцией активацией. Например, пороговая

функция, линейный порог, сигмоидальная функция, гиперболический тангенс (см. рис. 3).

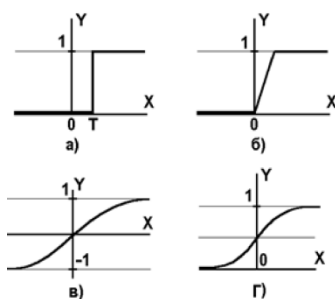


Рисунок 3 – Примеры функций активации

Вес связи определяет будет ли усилен или ослаблен сигнал, передаваемый по рассматриваемой сети.

Если для вычисления комбинированного ввода в нейросети использовать правило суммирования взвешенных связей, а в качестве функции активации – пороговую функцию, то тогда, если ввод меньше нуля, то активность нейрона будет равна нулю; а если ввод больше нуля, то активность нейрона будет равна единице [4].

В общем алгоритм нейросети можно представить следующим образом (см. рис. 4):

1. Задается шаг обучения $\alpha \in [0, 1]$ и желаемая средняя ошибка сети E_m ;
2. Случайно инициализируются веса w_i и пороговые значения нейронов b_j ;
3. Подаются последовательно образы из обучающей выборки на вход нейронной сети. Вычисляются выходные значения нейронов;
4. Вычисляются ошибки нейронов выходного и скрытого слоев;
5. Производится изменение весовых коэффициентов и порогов нейронных элементов для каждого слоя нейронной сети;
6. Вычисляется суммарная ошибка нейронной сети E ;
7. Если $E > E_m$, то вновь переходим к этапу обучения, иначе – выполнение алгоритма завершается.

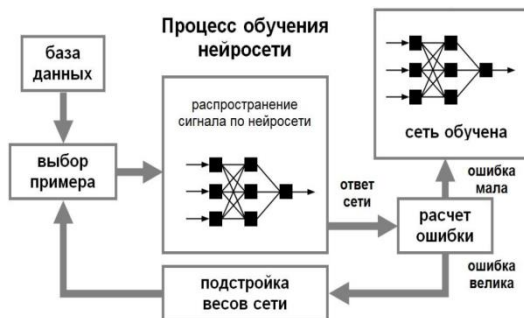


Рисунок 4 – Алгоритм обучения нейронной сети

Таким образом, нейронные сети не программируются в привычном смысле этого слова, они обучаются. Возможность обучения – одно из главных преимуществ нейронных сетей перед традиционными алгоритмами. Технически обучение заключается в нахождении коэффициентов связей между нейронами. В процессе обучения нейронная сеть способна выявлять сложные зависимости между входными данными и выходными, а также выполнять обобщение. Это значит, что в случае успешного обучения сеть сможет вернуть верный результат на основании данных, которые отсутствовали в обучающей выборке, а также неполных и/или «зашумленных», частично искажённых данных.

С использованием высокоуровневого языка программирования Python были проанализированы показатели 101 формы банковской отчетности (целевой показатель – отзыв лицензии) за период с января 2013 года по декабрь 2020 года включительно.

Используемые предикторы для моделирования:

1. Население региона регистрации банка;
2. Уставный капитал;
3. Кредиты другим банкам (МБК);
4. Учтённые векселя;
5. Прибыль (убыток) до налогообложения;
6. Коррсчета (ЛОРО);
7. Коррсчета (НОСТРО);
8. Средства организаций на расчетных счетах;
9. Облигации;
10. Векселя;
11. Капитал;
12. Ценные бумаги;

13. Чистые активы;
14. Основные средства;
15. Длительность существования банка (возраст банка);
16. Кредиты;
17. Прирост вышеуказанных показателей.

Рассмотрим результаты применения искусственных нейронных сетей к исследуемым данным (рис. 5): значение показателя «precision» = 80% и 68%, значение показателя «recall» = 76% и 73%, значение показателя «f1-score» = 78% и 70% для благонадежных и высокорисковых банков соответственно. Модель – многослойный перцептрон. Общая точность построенной модели нейронной сети «ассигасу» = 75%.

С учетом того, что большинство благонадежных банков, которые были отнесены моделью к ненадежным, лишись лицензии в будущих периодах, можно заключить, что модель нейронных сетей успешно справилась с задачей классификации.

	precision	recall	f1-score	support
0.0	0.80	0.76	0.78	11821
4.0	0.68	0.73	0.70	8434
accuracy			0.75	20255
macro avg	0.74	0.74	0.74	20255
weighted avg	0.75	0.75	0.75	20255

Рисунок 5 – Результаты применения нейронных сетей

Теперь рассмотрим результаты кросс-валидации, расчета медианных значений, то есть устойчивой оценки, не зависящей от разбиения. Код реализации кросс-валидации представлен на рис. 6.

```
In [55]: for metric_name, metric_array in metrics.items():
          med, mean, std = np.round((np.median(metric_array), np.mean(metric_array), np.std(metric_array, ddof=1)), 4)
          print(metric_name, med, mean, std)

precision 0.6776 0.6743 0.0695
recall 0.6688 0.6612 0.0622
auc 0.7367 0.7302 0.0461
```

Рисунок 6 – Код реализации кросс-валидации

Таким образом, устойчивое значение показателя «precision» = 68% и 67%, устойчивое значение показателя «recall» = 67% и 66% для

благонадежных и высокорисковых банков соответственно. Общая устойчивая точность построенной модели нейронной сети = 74%.

На рис. 7 представлен график кривой «Precision-recall». Из графика видно, что с увеличением значения показателя precision значение показателя recall уменьшается. Аналитик вправе выбрать и установить их оптимальное соотношение самостоятельно.

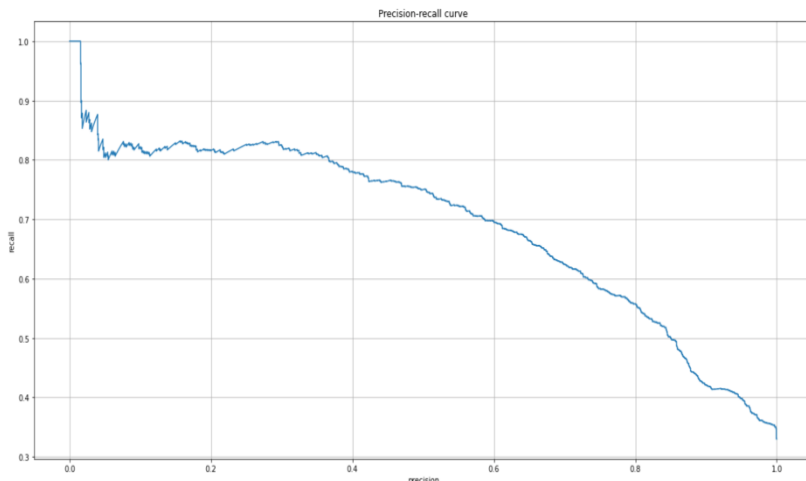


Рисунок 7 – График кривой «Precision-recall»

И, наконец, рассмотрим оценку важности входных предикторов согласно построенной модели нейронных сетей.

Наиболее важными показателями для оценки финансовой устойчивости и законопослушности банка оказались:

1. Прибыль (убыток) до налогообложения;
2. Возраст банка;
3. Уставный капитал;
4. Капитал;
5. Векселя.

Выбор данных показателей в качестве наиболее влиятельных для оценки банков можно интерпретировать следующим образом.

Прибыль (убыток) банка до налогообложения характеризует его профессиональную активность. Цель любого банка – заработать денежные средства. Прибыль формируется в виде дельты от заработанных банком на финансовом рынке денежных средств и выплаченных денежных им средств в виде процентов физическим и юридическим лицам.

Возраст банка характеризует период, в течение которого он функционировал, и может служить косвенным критерием его благонадежности. Банк, который открывается с целью организовать теневой финансовый оборот, как правило, существует относительно недолго. Однако возможна ситуация, когда руководители благонадежного банка осознанно идут на риск и нарушают банковское законодательство в своих интересах.

Уставный капитал – сумма, зафиксированная в учредительных документах банка, прошедшего государственную регистрацию. Уставный капитал определяет минимальный размер имущества банка, гарантирующего интересы его кредиторов. Если банк был создан для преступных целей, то логично предположить, что размер уставного капитала этого банка будет незначительным.

Капитал характеризует итог финансовой деятельности банка, его результат работы.

Векселя являются денежным документом, своего рода письменным обязательством уплатить кому-либо определенную сумму денег в определенный срок. Наличие в обороте подобных документов является критерием осуществления банком финансовой деятельности и проведения профильной работы.

В данной работе решена актуальная научно-экономическая задача классификации кредитных организаций и прогнозирования девиантной деятельности объектов исследования, что позволило повысить эффективность обработки данных и обеспечило высокую эффективность аналитической работы финансового мониторинга в условиях ограниченных ресурсов. Основные результаты научной работы заключаются в следующем:

1. применение искусственных нейронных сетей для прогнозирования девиантной деятельности кредитных организаций позволяет получить новые количественные оценки финансовой безопасности и на их основе спрогнозировать риск отзыва лицензии;
2. предложенное решение имеет прикладное значение, так как позволяет выявлять потенциально проблемные кредитные организации;
3. место субъективных экспертных оценок заменяют точные объективные количественные оценки.

Список использованных источников:

1. Приказчикова А.С., Бекетнова Ю.М., Крылов Г.О. «Системный анализ признакового пространства деятельности кредитных организаций в целях выявления рисков их финансовой устойчивости» / Орёл: Информационные системы и технологии, 2017 №1(97) / с. 125-129.

2. Приказчикова А.С., Бекетнова Ю.М., Крылов Г.О., Р.Э. Асланов «Об эффективности анализа кредитных организаций методом главных компонент в целях выявления рисков информационной и финансовой безопасности» / М.: Информатизация и связь, 2017, № 4.
3. Нейронные сети и нейроконтроллеры: учеб. пособие/ М. В. Бураков. – СПб.: ГУАП, 2013. – 284 с.: ил. ISBN 978-5-8088-0812-6.
4. Искусственные нейронные сети и приложения: учеб. пособие / Ф.М. Гафаров, А.Ф. Галимянов. – Казань: Изд-во Казан. ун-та, 2018. – 121 с.

Применение методов интеллектуального анализа данных для управления финансовыми рисками компании

Ж.Д. Даулетханова
доктор по профилю Финансы, Евразийский гуманитарный институт
г. Нур-Султан, Республика Казахстан
E-mail: Zhanar021@mail.ru

Аннотация: За последние несколько десятилетий мир стал свидетелем резкого роста зависимости от финансовых услуг, что привело к резкому росту числа онлайн-транзакций. Данный фактор способствуют росту распространенности финансового мошенничества, что вызывает необходимость в новом подходе к выявлению финансовых рисков и управлению ими. В статье рассматривается использование интеллектуального анализа данных для выявления и снижения финансовых рисков, возникающих в результате финансовых махинаций.

Ключевые слова: цифровые технологий, интеллектуальный анализ данных, финансовый риск, кредитный риск, операционный риск, корпоративный риск.

Application of data mining methods for financial risk management of the company

Abstract: Over the past few decades, the world has witnessed a sharp increase in dependence on financial services, which has led to a sharp increase in the number of online transactions. This factor contributes to the increase in the prevalence of financial fraud, which necessitates a new approach to identifying and managing financial risks. The article discusses the use of data mining to identify and reduce financial risks arising from financial fraud.

Keywords: digital technologies, data mining, financial risk, credit risk, operational risk, corporate risk.

В последнее время большинство инноваций во всем мире связано с развитием цифровых технологий. Цифровизация финансов относится к развитию цифровых инструментов и услуг в финансовой сфере. Количество новых разнообразных приложений для мобильных, бесконтактных и мгновенных платежей, управления активами, инвестиционного консалтинга, предоставления информации об учетной

записи и услуг по инициированию платежей, управления данными и хранения информации и тому подобного увеличивается с каждым годом.

Развитие цифровых инструментов и услуг в финансовой сфере, где инструменты и услуги отвечают потребностям клиентов и инвесторов, способствуют росту производительности и повышению конкурентоспособности экономики. Однако развитие цифровизации также может привести к нежелательным последствиям, например, снизить безопасность транзакций или способствовать отмыванию денег и финансированию терроризма. Важно подчеркнуть риски, которые цифровые технологии вносят в финансовую систему.

Компании используют большие наборы данных для установления закономерностей, необходимых для оперативной, ликвидной, снижение рыночных, юридических и кредитных рисков [1, с.11]. Однако для использования выводов, основанных на данных, и автоматизации необходимо разработать модели для решения задач в реальном времени [2, с.126]. Интеллектуальный анализ данных предполагает интеграцию методов моделирования со статистикой, искусственным интеллектом и машинным обучением [3, с.73]. Сочетание этих инструментов гарантирует, что компании могут решать различные ситуации на основе знаний, полученных в результате обучения без присмотра и под наблюдением, а также принятия решений. В связи с этим были предложены алгоритмы обучения и обработки данных разработан для достижения целей финансовой организации, особенно в области сбора и сбора информации [4, с.3]. Одним из которых выступает интеллектуальный анализ данных

Интеллектуальный анализ данных - это процесс извлечения информации или обнаружения скрытых и ценных знаний на основе некоторых закономерностей из больших данных. Интеллектуальный анализ данных выгоден для различных предприятий, например, производства, рекламы, управления рисками и так далее.

Процесс проведения интеллектуального анализа данных продемонстрирован в таблице 1.

Таблица 1 – Процесс реализации интеллектуального анализа данных

Этап	Наименование	Содержание
Первый	подготовка данных/предварительная обработка данных	Процесс подготовки данных включает очистку данных, интеграцию данных, выбор данных и преобразование данных
Второй	Процесс реализации интеллектуального анализа данных	включает интеллектуальный анализ данных, оценку шаблонов и представление знаний

Примечание: составлено на основе источника [5]

Применение интеллектуального анализа данных способствует обрабатывать информацию с нескольких платформ, а также баз данных при достижении желаемых результатов. Людям может потребоваться больше времени для обработки такой информации и достижения эффективности, полученной в результате глубокого и машинного обучения [5, с.31]. Следовательно, интеллектуальный анализ данных можно использовать в управлении финансовыми рисками для определения профилей, тенденций и анализа в реальном времени.

Интеллектуальный анализ данных используется в управлении финансовыми рисками, в результате чего соответствующие модели широко изучаются и применяются. Рассмотрим разновидности интеллектуального анализа данных.

1. Интеллектуальный анализ данных для управления кредитными рисками

Использование кредитных карт становится нормой в финансовом мире. Банки и эмитенты кредитных карт используют кредитную историю клиентов для оценки кредитоспособности клиентов и создания кредитного рейтинга. Модели кредитных рейтингов и оценки кредитных рисков используют интеллектуальный анализ данных. Технология интеллектуального анализа данных, связанная с интуитивной количественной оценкой, используется для оценки кредитоспособности банковского счета [6, с.40]. Кредитные баллы используют модели интеллектуального анализа данных для получения показателей рейтингов клиента. Следовательно, финансовое учреждение решает, предоставить ли заявителю желаемый лимит или отклонить заявку. Кроме того, интеллектуальный анализ данных использует другую важную информацию для клиента, такую как необычное использование кредитной карты, незаконная потеря денег, мошенничество или чрезмерные расходы. Знания и знания, полученные в результате обширных процессов интеллектуального анализа данных, предоставляют финансовой компании соответствующий обзор клиента, который становится определяющим фактором для одобрения или неодобрения кредитования

2. Интеллектуальный анализ данных для управления операционными и корпоративными рисками.

Крупные и малые организации, могут использовать инструменты интеллектуального анализа данных, большие данные и инструменты бизнес-аналитики для получения информации, а также улучшения бизнес-операций [7, с.41]. Интеллектуальный анализ данных может быть применен в управлении для установления закономерностей, которые могут быть использованы при анализе поведения и тенденций. Следовательно, полученные результаты используются для разработки устойчивой стратегии.

Для дальнейшего снижения корпоративных рисков интеллектуальный анализ данных используется для выявления операционных и отраслевых тенденций, а также проблем, что повышает конкурентоспособность бизнеса и долю рынка предприятия.

Компании сталкиваются с многочисленными рисками, для управления которыми требуются автоматизированные системы обнаружения. Финансовые учреждения используют алгоритмы для интеллектуального анализа данных, а также машинного обучения и искусственного интеллекта, чтобы снизить многочисленные риски, которые могут произойти без обнаружения. В связи с этим интеллектуальный анализ данных используется для разработки механизмов финансового контроля для защиты данных, систем и клиентов. Возможность машинного обучения и искусственного интеллекта для улучшения моделей интеллектуального анализа данных увеличивает скорость выполнения рутинных задач, а неструктурированные данные обрабатываются для выявить риск [8, с.81]. Эти методологии способствуют автоматизации во многих аспектах, тем самым снижая риски, связанные с человеческими ошибками. В связи с этим оценка сетей и клиентов становится проще. За сотрудниками и трейдерами также можно следить с помощью этого анализа данных. Что касается поведения, кластеризация и классификация являются важными инструментами для разработки профилей, в которых данные электронной, торговой и голосовой связи используются для установления закономерностей, а также скрытых рисков. Предупреждения также устанавливаются с использованием данных с приоритетом информации для определения подозрительных деятельности. Основные инструменты искусственного интеллекта, используемые для обнаружения финансовых мошенничеств, используют интеллектуальный анализ данных при выборе соответствующих наборов данных.

3. Интеллектуальный анализ данных для управления рыночными рисками.

На финансовых рынках доступны многочисленные наборы данных для торговли и инвестиций. Стратегии управления рыночными рисками направлены на снижение подверженности негативным последствиям соответствующих изменений в портфелях. Интеллектуальный анализ и обработка данных с использованием машинного обучения полезны в управлении рыночными рисками. Уместно отметить, что соответствующие методы и систематические методы являются основополагающими для проверки и моделирования, и важно установить роль рыночных моделей в торговле.

Каждый механизм подходит для определенной цели. Один одним из фундаментальных аспектов, требующих интеллектуального анализа данных и механизмов машинного языка, является стресс-тестирование

рыночных моделей [9, с.119]. Роль интеллектуального анализа данных в данном случае заключается в сборе, а также обработке данных для определения возникающего риска в отношении торгового поведения.

4. Интеллектуальный анализ данных для управления юридическими рисками

Соблюдение требований является важнейшим компонентом для финансовых учреждений, учитывая принятые меры контроля, особенно после финансового кризиса. Процессы управления рисками считаются несовместимыми с бюрократическими функциями по соблюдению нормативных требований, но они связаны тем, что они связаны с системами управления рисками [10, с.27]. Таким образом, соблюдение требований связано с различными последствиями для управления корпоративными рисками. Аналогичным образом, операционные, рыночные и кредитные риски рассматриваются в управлении рисками соответствия. Интеллектуальный анализ данных, машинное обучение, а также поскольку искусственный интеллект используется для обеспечения оценки больших наборов данных, чтобы гарантировать их соответствие законодательным положениям. Кроме того, интеллектуальный анализ данных имеет решающее значение для определения нетрадиционных данных, которые нарушают нормативные рамки и положения. В большинстве случаев интеллектуальный анализ данных постоянно используется для мониторинга деятельности и кредитных аспектов компании.

Однако отслеживание в режиме реального времени имеет решающее значение для предотвращения нарушений, связанных с соблюдением требований.

В заключение отметим что, интеллектуальный анализ данных является важной технологией, используемой в качестве инструмента для разработки современных моделей управления финансовыми рисками. Эта технология вместе со статистической регрессией, машинным обучением и искусственным интеллектом используется в обширных областях для оценки и управления финансовыми рисками, при этом основными подходами являются кластерный анализ, дерево решений.

Интеллектуальный анализ данных в основном использовался для моделирования оценки кредитного риска и профилирования клиентов путем определения кредитных рейтингов. Различные методы, а также алгоритмы, в том числе гибридная модель, в основном использовались для повышения точности классификации. В управлении операционными рисками интеллектуальный анализ данных использовался для разработки финансовых средств контроля за мошенничеством и другими критическими проблемами, такими как банкротство и финансовые кризисы.

Управление рыночными рисками применялось при разработке моделей, учитывающих модели финансовых рынков в реальном времени. Эти модели также используются для оповещения трейдеров, а также крупных предприятий о количественных последствиях вливания активов на рынок.

Таким образом, интеллектуальный анализ данных может быть использован для устранения алгоритмов и моделей кредитных, рыночных и бизнес-операций, которые увековечивают социальной несправедливости путем разработки инструментов для расшифровки негативных последствий существующих моделей, а также устранения потенциальных угроз для нарушений законодательства.

Список использованных источников:

1. Leo, M., Sharma, S., & Maddulety, K. (2019). Machine learning in banking risk management: A literature review. *Risks*, 7(1), 29. doi: 10.3390/risks7010029.
2. Zhong, X., & Enke, D. (2017). Forecasting daily stock market return using dimensionality reduction. *Expert Systems with Applications*, 67, 126-139. doi: 10.1016/j.eswa.2016.09.027.
3. Davenport, T. (2018). From analytics to artificial intelligence. *Journal of Business Analytics*, 1(2), 73-80. doi: 10.1080/2573234x.2018.1543535.
4. Alloghani, M., Al-Jumeily, D., Mustafina, J., Hussain, A., & Aljaaf, A. (2019). A systematic review on supervised and unsupervised machine learning algorithms for data science. *Unsupervised and Semi-Supervised Learning*, 3-21. doi: 10.1007/978-3-030-22475-2_1.
5. Heaton, J., & Polson, N. (2016). Deep learning for finance: Deep portfolios. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2838013.
6. Dicuonzo, G., Galeone, G., Zappimbulso, E., & Dell'Atti, V. (2019). Risk management 4.0: The role of big data analytics in the bank sector. *International Journal of Economics and Financial Issues*, 9(6), 40-47. doi: 10.32479/ijefi.8556
7. Moradi, S., & Mokhtab Rafiei, F. (2019). A dynamic credit risk assessment model with data mining techniques: evidence from Iranian banks. *Financial Innovation*, 5(1). doi: 10.1186/s40854-019-0121-9
8. Choi, T., Chan, H., & Yue, X. (2017). Recent development in big data analytics for business operations and risk management. *IEEE Transactions on Cybernetics*, 47(1), 81-92. doi: 10.1109/tyb.2015.2507599
9. Olson, D., & Wu, D. (2017). Data mining models and enterprise risk management. *Springer Texts in Business and Economics*, 119-132. doi: 10.1007/978-3-662-53785-5_9
10. Arner, D., Barberis, J., & Buckley, R. (2016). The emergence of Regtech 2.0: from know your customer to know your data. *SSRN Electronic Journal*. doi: 10.2139/ssrn.3044280.

Применение методов машинного обучения в целях выявления мошеннических транзакций

А.В. Кирина
студентка 5-го курса НИЯУ МИФИ, Москва
E-mail: nstkirina@yandex.ru

Д.В. Домашова
к.э.н., доцент кафедры финансового мониторинга
НИЯУ МИФИ, Москва
E-mail: janedom@mail.ru

Аннотация: Решение проблемы выявления мошеннических транзакций является одной из приоритетных задач для банковской отрасли. В работе были смоделированы и реализованы некоторые из алгоритмов машинного обучения для набора исторических данных о транзакциях – логистическая регрессия, случайный лес, XGBoost, изолирующий лес. Был проведен анализ качества работы моделей, построенных на базе данных алгоритмов.

Ключевые слова: машинное обучение, логистическая регрессия, транзакционное мошенничество, случайный лес, XGBoost.

Application of machine learning techniques in detecting fraudulent transactions

Abstract: Solving the problem of detecting fraudulent transactions is one of the priorities for the banking sector. In this paper, some of the machine learning algorithms for a set of historical transaction data were modeled and implemented – logistic regression, random forest, XGBoost, isolating forest. An analysis of the quality of the models was made.

Keywords: machine learning, logistic regression, transactional fraud, random forest, XGBoost

Стремительное развитие и трансформация сферы осуществления банковских переводов, роботизации ряда банковских услуг требует совершенствования системы противодействия осуществлению мошеннических транзакций.

С ростом количества осуществляемых транзакций значительно возрастает число совершаемых в данной сфере преступлений. По данным Банка России[1], в 2020 году количество мошеннических операций с

использованием электронных средств платежа увеличилось на 34%, а их объем возрос на 52,2%. Также на основании информации, полученной от кредитных организаций информации Банком России было установлено, что потери физических лиц в результате проведения одной мошеннической транзакции в среднем составили 11,4 тыс. руб., для юридических лиц данный показатель находится на уровне около 347,8 тыс. рублей. Наибольшее количество краж было среди операций по оплате товаров и услуг в интернете - российские банки зафиксировали 585,3 тыс. таких инцидентов. Объем краж через банкоматы и терминалы по сравнению с 2019 годом возрос на 40,3%, а через системы дистанционного банковского обслуживания — на 70%. Подобная тенденция вынуждает банковские организации регулярно пересматривать системы обнаружения транзакционного мошенничества.

Финансовые учреждения с каждым годом увеличивают количество затрачиваемых средств на развитие и внедрение инновационных технологий, автоматизированных инструментов анализа структурированных и неструктурированных данных, направленных на защиту банковского сектора от мошеннических операций. Основной целью является снижение роста числа несанкционированных операций и предотвращение потерь средств с банковских счетов кредитных организаций а также их клиентов – физических и юридических лиц.

Из-за больших объемов, информация об осуществленных банковских транзакциях тяжело поддается анализу. Банковские организации имеют большое преимущество в использовании методов анализа данных, так как обладают большим количеством достоверной информации как о клиентах, так и о совершаемых ими транзакциях, однако обработка информации о транзакциях затрудняется большими объемами представленных данных а также несбалансированностью объемов легальных операций по отношению к мошенническим.

Для выявления мошеннических транзакций используется информация об операциях, поступающая от платежной системы. По непосредственно информации о совершенной транзакции невозможно сказать – является она мошеннической или нет. Для принятия решения необходимо использовать исторические данные. Такими могут быть, например, информация о сумме, снятой с некоторого счета за определенный период времени или информация о количестве проведенных транзакций для данного клиента также за некоторый период времени.

Таким образом, перед принятием решения по транзакции необходимо «обогащать» информацию об операции рядом признаков, которые могут быть вычислены на основе информации, полученной ранее.

Единообразие стандартов значительно влияет на эффективность финансовой системы в целом, позволяет снизить затраты и предотвращать ошибки. Шагом на пути к единообразию стандартов передачи информации о финансовых операциях стала разработка ISO 20022. ISO 20022 был опубликован в 2014 году и представляет глобальный стандарт для обмена финансовыми сообщениями, обеспечивающий стандартную модель в различных областях.

Преимуществами данного стандарта является открытость и высокая пропускная способность данных, которая позволяет улучшить идентификацию участников взаимодействия. Данный стандарт является более универсальным для интеграции (по сравнению с ISO 8583 или ISO 15022), что значительно упрощает получение и передачу данных. Однако, для реализации преимуществ единообразия стандартов необходимы значительные средства со стороны организации. Кроме того, предполагается, что стандарт должен быть принят всеми участниками взаимодействия, что является одним из основных вызовов.

Многие авторы занимались проблемой обнаружения мошеннических операций. В исследованиях [2], [3] были представлены методики и алгоритм извлечения признаков из данных пользовательских активностей для двухклассовой классификации. В [4] в качестве моделей обнаружения были использованы наивный байесовский классификатор, C4.5 дерево решений и бэггинг с деревом решений C4.5 в качестве базового классификатора. В [5] использовались такие алгоритмы как stacking классификатор, случайный лес и градиентный бустинг. Наилучший результат показал stacking классификатор с логической регрессией в качестве мета-классификатора. В исследовании [6] были использованы искусственные нейронные сети и логистическая регрессия на реальном наборе данных. Проведенный анализ показал, что классификаторы, основанные на нейронных сетях превосходят по качеству те, что основаны на логистической регрессии.

В качестве исходных данных для анализа и обучения использовался набор данных Credit Card Fraud Detection, размещенный на платформе Kaggle. Данный датасет представлен 284 807 транзакциями, проведенными по кредитным картам за два дня. Данные описаны такими признаками как сумма транзакции, количество секунд с начала наблюдения, а также еще 28 признаков, полученных в результате преобразования методом главных компонент. Каждой транзакции соответствует значение класса (0 – мошенническая, 1 – не мошенническая). Доля мошеннических транзакций составляет 0,17%, таким образом выборка является несбалансированной относительно целевой переменной.

Для целей обучения с учителем данные были разбиты на тренировочную и тестовую выборку в отношении 3 к 1 с помощью метода StratifiedKFold. Это позволило сохранить соотношение числа мошеннических и немошеннических транзакций. В процессе работы также проводился подбор параметров модели путем анализа roc_auc кривых в рамках перебора различных параметров моделей.

Были обучены следующие модели: логистическая регрессия, случайный лес, XGBoost (градиентный бустинг на деревьях), изолирующий лес.

Результаты обучения моделей обучения с учителем представлены ниже (табл.1,2).

Таблица 1 – Результаты обучения на несбалансированной выборке

model	precision	TPR	FPR	roc_auc_score
Logistic Regression (l2, C =1)	0.835	0.699	2.39e-04	0.8495
Random Forest (n_est=5)	0.968	0.748	4.22e-05	0.8739
Random Forest (n_est=10)	0.920	0.748	1.12e-04	0.8739
Random Forest (n_est=20)	0.933	0.789	9.84e-05	0.8943
Random Forest (n_est=100)	0.960	0.772	5.62e-05	0.8862
XGBoost	0.962	0.821	5.62e-05	0.9105

Таблица 2 – Результаты обучения на сбалансированной выборке

model	precision	TPR	FPR	roc_auc_score
Logistic Regression (l2, C =1)	0.042	0.943	3.678e-02	0.9532
Random Forest (n_est=5)	0.039	0.992	4.177e-02	0.9750
Random Forest (n_est=10)	0.062	0.976	2.569e-02	0.9750
Random Forest (n_est=20)	0.066	0.992	2.437e-02	0.9835
Random Forest (n_est=100)	0.058	1.000	2.825e-02	0.9858
XGBoost	0.046	1.000	3.588e-02	0.9821

Изолирующий лес в настоящее время является одним из алгоритмов, наиболее часто используемых для обнаружения выбросов. Его применимость к задаче выявления фрода связана с линейной временной сложностью, что важно в случае анализа больших объемов данных. Однако важно отметить, что алгоритм не подходит для данных с большой размерностью, поскольку для каждого дерева в целях разделения пространства, признак выбирается случайно, что в случае большого количества признаков ведет к снижению качества выборки. По этой причине перед использованием изолирующего леса необходимо провести снижение размерности.

Обучение модели изолирующего леса было проведено в несколько этапов. Без снижения размерности, а также со снижением количества признаков методом главных компонент до 10. Помимо этого,

изолирующий лес был обучен без указания количества мошеннических транзакций в наборе данных и с ним (однако, такой метод уже нельзя назвать методом обучения без учителя).

Ниже представлены результаты обучения.

- 1) Без снижения размерности (с указанием в качестве параметров количества мошеннических транзакций, $\text{contamination} = N_{\text{фрод}}/N$) (Рис.1).

Для удобства рассмотрения графического представления выборка не мошеннических операций была сокращена до 70000 объектов. Выборка мошеннических сохранена в отображении полностью.

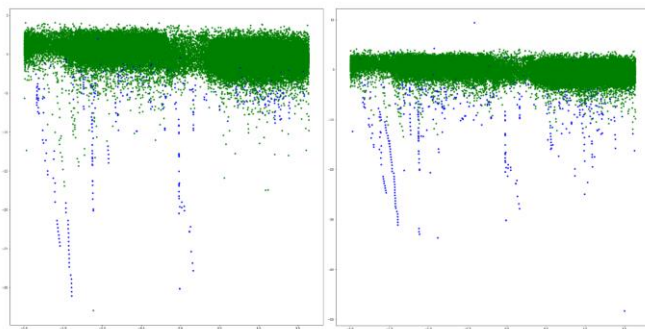


Рисунок 1 – Визуализация мошеннических операций (слева - разметка датасета, справа – изолирующий лес)

- 2) Без снижения размерности (без указания в качестве параметра числа объектов целевого класса, $\text{contamination} = 0.0009$) (Рис.2).

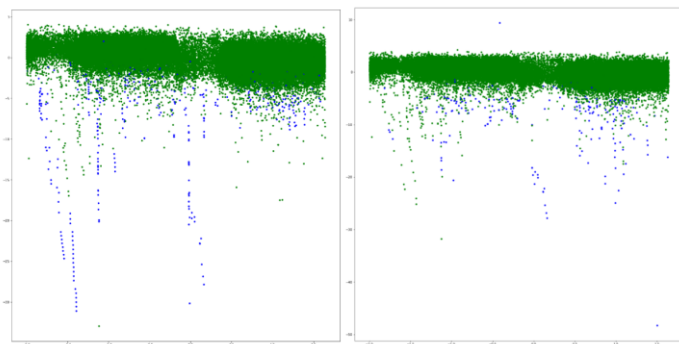


Рисунок 2 – Визуализация мошеннических операций (слева -разметка датасета, справа – изолирующий лес)

- 3) Со снижением размерности (без указания в качестве параметра количества мошеннических транзакций) (Рис. 3).

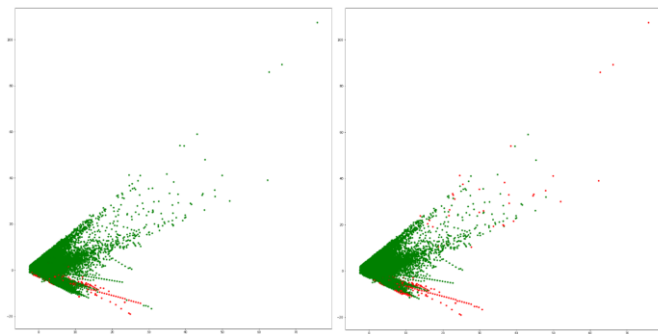


Рисунок 3 – Визуализация мошеннических операций (слева - разметка датасета, справа – изолирующий лес)

Анализ результатов

Обучение на сбалансированной выборке в целом показало более высокие значения ROC AUC, однако все модели, обученные подобным образом имели слишком высокое значение ошибки 1 рода. Применение подобной модели может негативно сказаться на лояльности клиентов по отношению к банковской организации, поскольку частые ошибочные блокировки транзакций являются негативным фактором. Однако, возможно, увеличение обучающей выборки позволило бы снизить ошибку первого рода. Также, возможным решением может быть изменение методики балансировки обучающей выборки. В данном случае, это может быть не отсеивание части наблюдений, а синтез дополнительных объектов мошеннических транзакций.

Среди моделей, обученных на несбалансированной выборке наилучший результат показал алгоритм XGBoost, ROC AUC = 0.9105.

Обучение без учителя также показало хорошие результаты. Было исследовано расположение точек фродовых операций по различным парам координат и проведено сравнение с исходной классификацией. Расположение и плотность мошеннических операций является очень схожей для исходной разметки датасета и результатов работы изолирующего леса.

Список использованных источников:

1. Банк России [Электронный ресурс]: Обзор операций, совершенных без согласия клиентов финансовых организаций за 2020 год. – Режим

доступа: https://www.cbr.ru/Collection/Collection/File/32190/Review_of_transactions_2020.pdf (Дата обращения: 17.04.2021)

2. Крылов П. Схемы хищений в системах ДБО и пять уровней противодействия им // Расчеты и операционная работа в коммерческом банке. 2018. №3 (145). С. 46 – 59.
3. Слипенчук, П. В. Алгоритм извлечения характерных признаков из данных пользовательских активностей // Вопросы кибербезопасности. 2019. №1 (29). – С. 53 – 58.
4. Husejinovic A. Credit card fraud detection using naive Bayesian and c4. 5 decision tree classifiers //Husejinovic, A.(2020). Credit card fraud detection using naive Bayesian and C. – 2020. – Т. 4. – С. 1-5.
5. Dhankhad S., Mohammed E., Far B. Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study //2018 IEEE International Conference on Information Reuse and Integration (IRI). – IEEE, 2018. – С. 122-125.
6. Sahin Y., Duman E. Detecting credit card fraud by ANN and logistic regression //2011 International Symposium on Innovations in Intelligent Systems and Applications. – IEEE, 2011. – С. 315-319.

Применение методов машинного обучения и глубокого обучения при решении задачи защиты информации в сфере облачных технологий

В.А. Рычков

старший преподаватель кафедры финансового мониторинга
НИЯУ МИФИ, Москва

E-mail: VARychkov@mephi.ru

В. Давыденко

старший преподаватель кафедры финансового мониторинга
НИЯУ МИФИ, Москва

E-mail: VIDavydenko@mephi.ru

И.П. Чурилов

студент 2 курса НИЯУ МИФИ, Москва

E-mail: mrchurilov@mail.ru

Аннотация: В данной статье рассмотрено применение алгоритмов машинного обучения и глубокого обучения в области защиты информации при использовании облачных технологий. Акцент сделан на исследование подходов обнаружения вредоносной активности, использующих информацию о системных вызовах.

Ключевые слова: машинное обучение, нейронные сети, информационная безопасность, облачные технологии, контейнеризация.

Application of machine learning and deep learning methods in solving the problem of information security in the field of cloud technologies

Abstract: This article discusses the application of machine learning and deep learning algorithms in the field of information security when using cloud technologies. The emphasis is placed on the study of approaches to detecting malicious activity using information about system calls.

Keywords: machine learning, neural networks, information security, cloud technologies, containerization.

Информационная безопасность является фундаментальной и неотъемлемой частью современной жизни. За последние несколько лет популярность облачных вычислений в ИТ-индустрии резко возросла. Интерес к облачным технологиям наблюдается не только в промышленной

сфере, но и в государственном секторе. Однако, учитывая строгие требования к конфиденциальности и безопасности, активному использованию этой технологии по-прежнему препятствуют многие проблемы безопасности, связанные с функциями облачных вычислений, а именно общими ресурсами, виртуализацией и многопользовательской арендой.

Эти проблемы варьируются от угроз конфиденциальности и отсутствия прозрачности работы таких систем до вторжений. Вторжений как внутри, так и за пределами облачной инфраструктуры. Для активного развития и использования облачных технологий необходима разработка адекватных механизмов безопасности, способных эффективно реагировать и устранять возникающие угрозы. Одним из механизмов являются системы обнаружения вторжений, COB (англ. Intrusion Detection System IDS). Существует много разновидностей подобных систем (сетевые, узловые, гибридные). В статье более подробно остановимся на рассмотрении хостовых COB (англ. Host-based intrusion detection system, HIDS), точнее, на одном из методов, используемых в таких системах для обнаружения вредоносной активности.

Такие системы используют различные методы для обнаружения вредоносной активности, среди которых мониторинг действий пользователей, использования различных участков памяти, логов системы и т.д. Одним из важных индикаторов поведения системы, активно используемых в хостовых COB, являются системные вызовы (англ. syscalls).

Что касается методов обработки индикаторов вредоносного поведения для выявления по ним вредоносной активности, то их также существует очень много, в рамках данной статьи рассматриваются методы машинного обучения, МО (англ. Machine Learning, ML) и глубокого обучения, ГО (англ. Deep Learning, DL) используемые для детектирования вредоносной активности.

Потенциальная успешность применения этих методов обусловлена следующими вещами:

1. Бурное развитие и широкое использование методов машинного обучения в последние десятилетие, вызванное:

- а) Ростом вычислительных мощностей;
- б) Объёмом накапливаемой информации;
- в) Развитием математической базы, используемой в этих алгоритмах;

2. Успешное применение этих методов в других областях науки и в производстве;

3. Попытки применения этих методов в области ИБ, в настоящий момент сложно понять, насколько эффективными являются эти попытки, поскольку эта информация является интеллектуальной собственностью и не разглашается.

В статье сделан обзор и сравнительный анализ последних научных работ, исследовавших возможность применения алгоритмов МО и ГО в хостовых СОВ.

Особенностью применения всех алгоритмов МО и ГО являются следующие ограничения:

1. Необходимость в качественных данных. Недостаточно просто иметь много данных, необходимо также, чтобы они не были зашумлены и данные отражали зависимость, которую необходимо выучить для дальнейшего прогнозирования;

2. Вычислительные мощности, необходимые для обучения алгоритмов и в момент прогнозирования;

3. Время работы, необходимое для прогнозирования. Этот пункт особенно важно учитывать, поскольку время отклика в хостовых СОВ является критическим параметром.

Таким образом, успешность применения алгоритмов МО и ГО зависит не только от качества работы самих алгоритмов, но ещё от ряда факторов и ограничений. В последних научных работах исследования проводились в следующих направлениях:

- достижение высокого качества моделями МО и ГО в задаче обнаружения вредоносной активности;

- исследование существующих датасетов (наборов данных), выявление недочетов существующих, создание новых датасетов, необходимых для обучения моделей МО и ГО;

- Основными исследуемыми алгоритмами являлись следующие:

- Скрытые Марковские Модели (англ. Hidden Markov Model, HMM) [2];

- Многослойный перцептрон, (англ. Multilayer Perceptron, MLP) [2];

1. Метод опорных векторов (англ. Support Vector Machine, SVM) [2, 4];

2. Метод k-ближайших соседей (англ. k-nearest neighbors algorithm, k-NN) [2, 3];

3. Алгоритмы кластеризации [2];

4. Дерево решений [4];

5. Случайный лес [4];

6. Градиентный бустинг [4];

7. Логистическая регрессия [4];

Подходы с использованием этих алгоритмов показали очень хорошее качество. Доля обнаруженных случаев вредоносной активности (англ.

Detection Rate) на уровне выше 95% и в некоторых случаях близка к 100%. В то время как доля ложных срабатываний (англ. False Alarm Rate) на уровне долей процентов. Но необходимо сказать, что большинство представленных алгоритмов являются алгоритмами классификации, поэтому они обучались классифицировать определённые типы вредоносной активности. При этом обобщающая способность таких алгоритмов очень низкая, они не смогут обнаружить типы вредоносной активности, которые не встречались в тренировочной выборке.

Также были применены некоторые нестандартные подходы. В [2] авторы попробовали “семантический подход”, который состоит в том, чтобы относиться к системным вызовам как к буквам, формирующим слова, фразы. Затем формируются фразы, сигнализирующие о вредоносном поведении системы. Этот подход был опробован на двух датасетах. на одном из которых показал качество в районе 100% по метрике Detection Rate. В другом результаты были меньше 90%.

В работе [5] для того, чтобы охарактеризовать трейс системных вызовов был применён подход “мешка слов” (англ. Bag of system calls), это позволило авторам добиться 100% доли обнаружения вредоносной активности. Тем не менее, этому подходу также принадлежат все недостатки, перечисленные выше.

Часть работ [3, 6, 7, 8, 9] посвящена анализу датасетов (наборов данных), используемых для обучения, поскольку, этот компонент является критически важным, как говорилось выше.

В работах [3, 6, 7] сделано детальное описание датасетов, причин, по которым они создавались, недостатков, которые они были призваны исправить.

Самыми известными датасетами на сегодняшний день являются CIDD [6], KDD, ADFA-LD, ISOT-CID. В большей части работ эксперименты проводились именно с ними.

В работах [8, 9] дан исчерпывающий сравнительный анализ существующих на момент публикации датасетов (2018 г. и 2019 г. соответственно). Общие выводы работ следующие:

1. На данный момент наблюдается нехватка общедоступных датасетов, в последние несколько лет было опубликовано несколько датасетов, но проблема всё ещё остаётся актуальной;
2. Существующие датасеты охватывают лишь небольшую часть различных типов атак;
3. Отсутствие сопровождающей документации в части датасетов.

Частично описываемые недостатки были исправлены в датасете ISOT-CID [10].

Отдельного внимания заслуживают работы [11, 4]. Поскольку в них детектирование вредоносного поведения происходит не при помощи классификации, а с использованием подхода обнаружения аномалий. Его преимущество над методом классификации заключается в том, что работа происходит в парадигме поиска любой активности, по своим признакам отличающейся от легитимной. Поэтому данный метод способен обнаружить типы вредоносной активности, которые не встречались в обучающей выборке. Таким образом нивелируется недостаток, принадлежащий большинству существующих на сегодняшний день датасетов.

Реализуется этот метод при помощи нейронных сетей с архитектурой, называемой Автокодировщик (англ. autoencoder). Отсюда следует важное ограничение (которое необходимо учитывать при технической реализации) – время работы нейронных сетей существенно больше, чем у большинства перечисленных выше алгоритмов.

Качество работы, достигнутое в работе 11, отражено в таблице 1.

Таблица 1 – Метрики качества системы обнаружения вредоносной активности [11]

Название датасета	F мера	Доля верных срабатываний
Wisconsin	94.29%	94.36%
Ionosphere	92.00%	90.74%
Musk	41.93%	67.76%
Biomed	55.67%	54.25%
Shape1	95.24%	95.00%
Shape2	51.28%	52.50%

В работе [4] пошли ещё более хитрым путём и использовали автокодировщик для создания признаков, на которых уже затем обучали стандартные алгоритмы классификации. Результаты представлены в таблице 2.

Таблица 2 – Метрики качества системы обнаружения вредоносной активности [4]

	Дерево решений	Случайный лес	Логистическая регрессия	Метод опорных векторов	Градиентный бустинг
Доля правильных ответов	0,94	0,96	0,91	0,94	0,95
Точность	0.87	0.95	0.83	0.88	0.94
Полнота	0.86	0.89	0.69	0.83	0.84
F мера	0.86	0.92	0.74	0.86	0.88

Эти результаты вызывают доверие, поскольку видно, что на разных датасетах алгоритм показывает разное качество, нигде не достигнуто качество в 100%.

Обобщая вышесказанное, можно заключить, что на данный момент существуют исследования и попытки применить методы МО и ГО для обеспечения защиты информации в сфере облачных технологий, для обеспечения безопасности контейнеров. Исследования можно считать успешными, в некоторых работах исследователи заявляют об очень хорошем достигнутом качестве. Особенно перспективными выглядят подходы с использованием автокодировщиков. Но нужно понимать, что успешность использования заявленных результатов работы в реальных системах безопасности подлежит перепроверке с учетом ограничений, накладываемых на использование методов МО и ГО.

Список использованных источников:

1. Host-based intrusion detection system [Электронный ресурс] – URL: https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system
2. A Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguous and Discontiguous System Call Patterns [Электронный ресурс] – URL: https://www.researchgate.net/publication/260946457_A_Semantic_Approach_h_to_Host-

- Based_Intrusion_Detection_Systems_Using_Contiguousand_Discontiguous_System_Call_Patterns
3. Statistical analysis of CIDDs-001 dataset for Network Intrusion Detection Systems using Distance-based Machine Learning [Электронный ресурс] – URL: https://www.researchgate.net/publication/321715580_Statistical_analysis_of_CIDDs-001_dataset_for_Network_Intrusion_Detection_Systems_using_Distance-based_Machine_Learning
 4. A MACHINE LEARNING FRAMEWORK FOR HOST BASED INTRUSION DETECTION USING SYSTEM CALL ABSTRACTION [Электронный ресурс] – URL: <https://dalspace.library.dal.ca/handle/10222/78469>
 5. Applying Bag of System Calls for Anomalous Behavior Detection of Applications in Linux Containers [Электронный ресурс] – URL: <https://arxiv.org/abs/1611.03053v1>
 6. CIDD: A Cloud Intrusion Detection Dataset For Cloud Computing and Masquerade Attacks [Электронный ресурс] – URL: https://www.researchgate.net/publication/236854663_CIDD_A_Cloud_Intrusion_Detection_Dataset_for_Cloud_Computing_and_Masquerade_Attacks
 7. Generation of a new IDS Test Dataset: Time to Retire the KDD Collection [Электронный ресурс] – URL: https://www.researchgate.net/publication/261418008_Generation_of_a_new_IDS_test_dataset_Time_to_retire_the_KDD_collection
 8. Data Sources and Datasets for Cloud Intrusion Detection Modeling and Evaluation [Электронный ресурс] – URL: https://link.springer.com/chapter/10.1007/978-3-319-73676-1_13?error=cookies_not_supported&code=0639305e-2d93-4edc-8e0f-4a38a10346e9
 9. A Survey of Network-based Intrusion Detection Data Sets [Электронный ресурс] – URL: <https://arxiv.org/abs/1903.02460v2>
 10. Набор данных ISOT-CD Dataset, University of Victoria [Электронный ресурс] – URL: <https://www.uvic.ca/ecs/ece/isot/datasets/cloud-security/index.php>
 11. Securing Cloud Containers through Intrusion Detection and Remediation [Электронный ресурс] – URL: https://vtechworks.lib.vt.edu/bitstream/handle/10919/87730/Abed_AS_D_2017.pdf

Проблемы безопасности бесконтактных платежей

Э.Р. Аблитаров

студент 2 курса бакалавриата ИЭиУ, Симферополь

E-mail: ablitaroff@mail.ru

Аннотация: В данной статье рассмотрены вопросы, связанные с бесконтактной оплатой и выявлены основные ее негативные составляющие. Определены меры по предупреждению и устранению основных негативных составляющих бесконтактной оплаты.

Ключевые слова: бесконтактная оплата, NFC, безопасность, информационное пространство.

Security problems of contactless payments

Abstract: This article discusses issues related to contactless payment and identifies its main negative components. Measures have been identified to prevent and eliminate the main negative components of contactless payment.

Keywords: macroeconomics, economic growth, inflation, balance of payments, GDP.

Совершенствование и усиление информационной безопасности на данный момент требует внедрения инновационных технологий и наиболее современных электронных платежных инструментов, которые по своей сущности должны удовлетворять нуждам граждан и прочим рыночным субъектам. Также, они требуют разработки современных подходов к улучшению их регулирования и качественного применения с целью наращивания эффективности воздействия платежных инструментов для поддержания стабильного экономического роста как отдельных государств, так и мирового хозяйства. Современные исследования по вопросам функционирования платежных инструментов позволяют говорить о том, что финансовые составляющие экономик стран мира крайне чувствительны любым изменениям в финансовом обороте.

В силу того, что многие страны, в частности, Россия постепенно переходят к инновационной форме развития экономики, крайне необходимым аспектом выступает модернизация и совершенствование механизма ведения безналичных расчетов. Толчком к усиленному внедрению и использованию банковских карт могут послужить изменения,

касающиеся совершения финансовых операций на основе Интернет-банкинга. Данный интерфейс управления банковским счетом подразумевает то, что людям нет нужды идти в банк для совершения финансовых операций (оплаты счета, снятия наличных, переводы и т.д.). Отсюда можно сделать вывод, что качественная трансформация в области ведения безналичных расчетов является приоритетным направлением для многих государств, в частности, России в силу того, что данная составляющая финансовых изменений является неотъемлемой частью перехода к инновационной форме развития.

В современном мире почти каждый человек пользуется банковской картой за счет ее надежности, удобства и простоты использования, а также она является технологией, которая развивается и модернизируется с течением времени.

Платежные карты впервые были затронуты Эдвардом Беллами в 1887 г. в его знаменитой работе «Взгляд назад», при этом, вошли в реальность в 1921 г. Вскоре многие универсальные магазины, станции технического обслуживания и отели стали рекомендовать покупателям платежные карты для комфорта и простоты транзакции [1].

Первой банковской картой с технологией PayPass в России, выпущенной Московским индустриальным банком, были обеспечены преподаватели и студенты учебных заведений. Для студентов такая карта была не только средством накопления, позволяющей осуществлять повседневные покупки, но и действовала в роли студенческого билета, и даже зачетной книжки. Банковские карты активно распространяются в современном мире, особенно в условиях пандемии COVID-19. В 2020 году банки выдали 19,2 млн. расчетных и кредитных карт - это максимум за все время ведения статистики ЦБ по текущей методологии [2].

Для передачи данных используется NFC - разновидность RFID. На карте размещены чип и антенна, которые откликаются на запрос платежного терминала на определенной радиочастоте. NFC надёжна и проста в использовании. Бесконтактные чипы NFC обеспечивают хранение и обмен данными со специальными считывающими устройствами, например, валидаторами на турникетах или POS-терминалами на кассах магазинов.

В настоящее время остается острым вопрос о угрозах и вызовах бесконтактных платежей в связи с наличием мошенников как среди граждан, так и среди сотрудников финансовых учреждений, подрывающих экономическую безопасность как граждан, так и государства. Обобщенно проблемы бесконтактных платежей можно представить в следующем виде (рисунок 1):

Проблемы бесконтактных платежей

- 1 Кража данных по NFC - каналу
- 2 Концет Android-троянца
- 3 Перехват ключа транзакции

Рисунок 1 – Обобщенная систематизация проблем бесконтактных платежей
Источник: составлено автором на основе [3, с. 53-56]

Особо острой проблемой выступает возможность считывания данных по NFC каналу. Среднее расстояние для считывания денежных средств со считывателей составляет порядка несколько сантиметров (но не больше 10 см). Однако, исследователям удалось собрать комплект, позволявший просматривать данные транзакции и красть данные карты на расстоянии до 45 см. Набор, правда, включал в себя рюкзак и тележку из супермаркета, в котором, собственно, и проводился опыт. В общем, с нестандартным считывателем шанс получить данные карты сильно возрастает, но требуется крупногабаритное оборудование. Отличным решением в данной ситуации выступает использование приложения Google Pay. Благодаря использованию данного приложения можно оплатить покупку без карты, достаточно открыть приложение платежного сервиса и поднести телефон к терминалу бесконтактной оплаты на расстоянии 5 - 10 см. Оплата проходит моментально. Несмотря на то, что на многих смартфонах программа установлена разработчиками, некоторые модели смартфонов не поддерживает технических характеристик для использования данного приложения.

Отсюда следует, что разработчикам данного платежного сервиса необходимо усовершенствовать приложение, чтобы им смогли пользоваться люди, не имеющие на данный момент смартфона, который поддерживал бы такое приложение. Выполнение данного аспекта позволит избежать в дальнейшем кражи данным злоумышленниками по NFC-каналу и сохранит денежные средства жертв.

Компьютерные вирусы, которые вначале своего существования приносили лишь мелкие неприятности, теперь являются настоящей разрушительной силой нашего общества и наносят огромный ущерб мировой экономике, экономике отдельных государств и гражданам.

Одним из способов мошенничества, выступает Android-троянец, распространяющийся не только на компьютеры с операционной системой Windows, но и на компьютеры с операционной системой Mac и мобильные устройства. Вредоносные программы чаще всего появляются посредством зараженных файлов, сообщений текстового характера с манипулятивным содержимым или нелегальных веб-сайтов. [4]. Из этого можно сделать вывод, что не следует при использовании компьютера, мобильных устройств и других технологий, доверять ложному чувству безопасности, исключая факт защиты специализированных приложений от подобных вредоносных программ.

Наиболее часто встречаются банковские трояны. Повседневное распространение онлайн-банкинга и невнимательность пользователей банковских карт делают банковские трояны перспективным способом для кражи мошенниками чужих денег. Цель таких программ – получить учетные данные пользователей банковских карт для доступа к банковским счетам. В соответствии с данной целью используется фишинг: предполагаемые жертвы перенаправляются на страницу, контролируемую мошенниками для ввода учетных данных [4]. Затем телефон человека становится жертвой и своеобразным ретранслятором NFC сигнала: едва лишь телефон оказывается рядом возле бесконтактной карты, он направляет через Интернет мошеннику сообщение о доступности транзакции. После получения данного сообщения, предполагаемый мошенник подносит к считывающему устройству телефон, и таким образом создается некий мост между банковской картой и терминалом, который может реализовываться на абсолютно любом расстоянии.

Таким образом, для онлайн-банкинга необходимо использовать безопасные методы входа в систему: приложение банка, а не ввод данных в веб-интерфейсе. Следует пользоваться доверенными антивирусными приложениями, не переходить на подозрительные ссылки, не скачивать всесторонние приложения с недоверенных источников и т. д. Со стороны государства необходимо усилить контроль за мошенничеством в сети, т. к. параллельно с развитием инновационных технологий развивается механизм обхода системы данных технологий, в результате чего люди претерпевают финансовые траты и кражу личных данных.

Действующим способом мошенничества является перехват ключа транзакции. В силу того, что некоторые данные могут храниться незашифрованным виде в памяти чипа карты (номер карты, данные недавних совершенных операций и др.), перехват ключа транзакции злоумышленниками не влечет за собой угрозы для пользователей. Код запрашивается для одной транзакции и будет активирован только для ее оплаты. Например, если человек совершил платеж через NFC модуль,

после чего транзакция была отменена, для повторения транзакции считывающее устройство запросит новый ключ от пользователя. За счет факта существования данных сложностей перехват злоумышленниками таких данных, как ключей транзакций является действительно сложной задачей. Что выполнить ее и остаться незамеченными, им необходимо взломать банковскую систему с целью получения кода, сгенерированного мобильным устройством [5]. Стоит отметить, что эти данные можно получить с помощью NFC смартфона, установив необходимое приложение (в т.ч. легальное), и этих данных будет достаточно злоумышленнику, а также, администратору приложения, чтобы выполнить платеж на основе данных карты. Также, воспользоваться данным способом мошенничества могут и финансовые учреждения, которые являются хранителем информации обо всех операциях пользователей данного финансового учреждения.

Решение данной проблемы заключается в добросовестном поведении банков и других финансовых учреждений, а также усиленный финансовый контроль со стороны государства, что будет способствовать устранению и предотвращению подобного рода проблем.

Обеспечение безопасности бесконтактных платежей можно представить в следующем виде (рисунок 2).

Обеспечение безопасности бесконтактных платежей

- 1 Добросовестность финансовых учреждений
- 2 Внимательность граждан к своим мобильным устройствам
- 3 Усовершенствовании приложений, производимых покупки без использования банковской карты
- 4 Усиление государственного контроля и мониторинга мошенников
- 5 Перевод крупных сумм на дополнительные (накопительные) счета

Рисунок 2 – Обобщенная систематизация обеспечения безопасности бесконтактных платежей

Источник: составлено автором

Степень добросовестности финансовых учреждений отражает степень вовлеченности в мошенничество. Т. е. чем более добросовестно финансовое учреждение будет функционировать, тем меньше шансов быть вовлеченным в мошенничество.

Внимательность граждан к своим мобильным устройствам крайне необходима, т. к. от них зависит сохранность финансовых средств и самих пользователей бесконтактных платежей.

Усовершенствование приложений, производимых покупки без использования банковской карты, а именно, создание мер, направленных на поддержание устройствами приложений, производимых покупки удаленно от банковской карты позволит людям не опасаться кражи личных данных путем считывания данных через NFC-канал, т. к. это будет невозможно для мошенников.

Усиление государственного контроля и мониторинга мошенников будет способствовать улучшению финансового климата граждан, а также непосредственному наказанию мошенников.

Стоит отметить, что распространенным способом защиты является перевод крупных сумм на дополнительные (накопительные) счета.

Из всего вышесказанного можно сделать вывод, что действительно, технология бесконтактных платежей закрыта хорошей многофакторной защитой, но и это стопроцентной гарантии пользователям бесконтактных платежей не дает. Т.к. большинство банковских карт связаны с устаревшими технологиями, такими как магнитная полоса, платеж без дополнительной аутентификации и т.д., мошенники выработали слаженный механизм хищения денежных средств, подрывающий финансовую безопасность как страны, так и государства.

Список использованных источников:

1. Хрипунов, Д. Эволюция мобильных платежей / Д. Хрипунов // Хабр. - URL: <https://habr.com/ru/post/305910/> (дата обращения: 16.11.2021)
2. Банки в год пандемии увеличили выдачи карт до рекорда за семь лет // РБК. - URL: <https://www.rbc.ru/finances/06/03/2021/60422c739a79471a7> (дата обращения: 16.11.2021)
3. Гурьянов К. В. Современные риски бесконтактных платежей с использованием RFID-технологий / К.В. Гурьянов // КиберЛенинка // Базис. 2019. №1 (5). - URL: <https://cyberleninka.ru/article/n/sovremennyye-riski-beskontaktnyh-platezhey-s-ispolzovaniem-rfid-tehnologii> (дата обращения: 19.11.2021).
4. Что такое троянские программы и какой ущерб они могут нанести? // «Лаборатория Касперского». - URL: <https://www.kaspersky.ru/resource-center/threats/trojans> (дата обращения: 18.11.2021)
5. Могут ли через NFC украсть деньги? // Пикабу. - URL: https://pikabu.ru/story/mogut_li_cherez_nfc_ukrast_dengi_6682830 (дата обращения: 17.11.2021)

Проблемы идентификации финансовых вложений в учетно-аналитических целях

Д.И. Норкина

студентка 4 курса НИЯУ МИФИ, Москва

E-mail: nice.diank@mail.ru

Н.С. Белогина

к.э.н., доцент кафедры бухгалтерского учета и аудита

НИЯУ МИФИ, Москва

E-mail: nsbelogina@mephi.ru

Аннотация: В данной статье на основе сравнительного анализа дефиниций, используемых в нормативно-правовом поле, а также изучения и группировки мнений авторов публикаций предложены подходы к систематизации терминологической основы данной области бухгалтерского учета.

Ключевые слова: деривативы, долевого инструмента, инвестиции, финансовый актив, финансовые вложения; финансовый инструмент; финансовое обязательство.

Problems of identification of financial investments for accounting and analytical purposes

Abstract: Based on a comparative analysis of the definitions used in the regulatory field, as well as studying and grouping the opinions of the authors of publications, the article proposes approaches to systematizing the terminological basis of this area of accounting.

Keywords: derivatives, equity instrument, investments, financial asset, financial investments; financial instrument; financial liability

Финансовый рынок – важнейший инфраструктурный элемент экономики и многие российские компании активно работают на этом рынке. Наличие в отчетности таких компаний полной и точной информации об используемых ими финансовых инструментах может способствовать расширению масштабов привлечения инвестиций. Этому препятствует недостаточная согласованность нормативного регулирования, выражающаяся в том числе в отсутствии единой терминологии и единообразного подхода к пониманию сущности основных

категорий. Проанализируем и сопоставим трактовки содержания категории финансовых вложений, установленные международными и российскими учетными стандартами, а также используемые в специальной литературе, для разработки подходов к их гармонизации в учетно-аналитических целях.

Вместо категории «финансовые вложения» МСФО оперируют определениями «financial instrument», «financial assets», «financial liability», «equity instrument». Понятие финансовый инструмент регулируется IAS 32 «Финансовые инструменты: представление информации» [3]. В IAS 32 п. 11 даны важные определения, которые входят в состав финансовых вложений, такие как «финансовый инструмент», «финансовое обязательство», «финансовый актив» и др. И более точно раскрываются остальные понятия в Приложении А IFRS 9 «Финансовые инструменты» [5] или п. 9 IAS 39 «Финансовые инструменты: признание и оценка» [4].

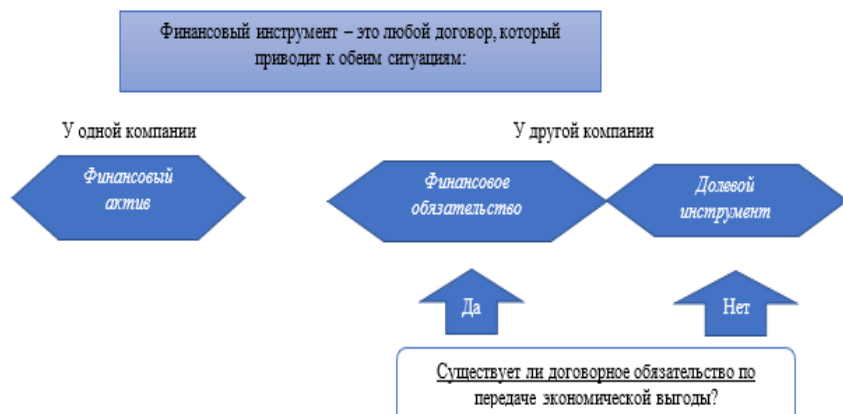


Рисунок 1 – Определение финансового инструмента по МСФО

Как видно на рис. 1, МСФО дают определение непривычного для российского нормативно-правового поля термина «финансового инструмента», определяя его как сопутствующий финансовым инвестициям тип договора. Помимо этого, международные стандарты не дают определения той категории актива, которая появляется в бухгалтерском учете у организации-инвестора.

В отечественном бухгалтерском учете, пока что применяется ПБУ 19/02 «Учет финансовых вложений», которое введено в действие Приказом Минфина РФ N 126н (далее ПБУ 19/02) [6]. В ПБУ 19/02 не приведены определения ни финансовых вложений, ни финансового инструмента.

Вместо этого дается перечень требований, соответствие которым позволяет признать в бухгалтерском учете актив в форме финансовых вложений. Это заставляет авторов публикаций в специальной литературе в вопросе идентификации категории полагаться только на собственное понимание изложенного в учетных стандартах и в тех правовых актах, которые затрагивают вопросы идентификации финансовых вложений. Так Гражданский кодекс Российской Федерации косвенно дает определение таких терминов, как ценные бумаги, обязательство - которые являются частью понятия финансовых вложений и, соответственно, попадают под их нормативно-правовое регулирование из других документов. Однако можно заметить, упоминание не всех видов финансовых вложений приведено в Гражданском кодексе. Что тоже подразумевает под собой неполное раскрытие информации [1].

В Налоговом законодательстве России имеют оборот такие слова и выражения, как: финансовые вложения, ценные бумаги, дивиденды и проценты. Они рассматриваются с позиции налогообложения. Раскрытие данных понятий и связанных с ними операций в данном документе не приводится [2].

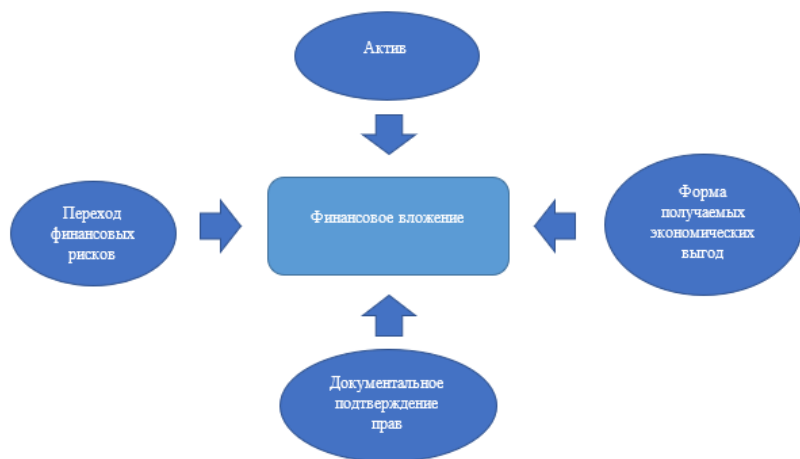


Рисунок 2 – Требования к идентификации финансовых вложений по РСБУ

Имеет смысл упомянуть 39-ФЗ «О рынке ценных бумаг». Данный закон посвящен объектам финансовых вложений – акциям, облигациям, связанной с рынком ценных бумаг деятельностью и др. Данный нормативно-правовой документ (в разрезе объекта исследования данной статьи) рассматривает следующие позиции: процедуру эмиссии, переход

прав на ценные бумаги, раскрытие информации по ценным бумагам, а также множество других позиций, необходимых для полноценной деятельности рынка ценных бумаг [10, 134].

В специальной литературе также можно отметить отсутствие единообразия позиций авторов. Данная ситуация обусловлена отсутствием определения финансовых вложений в их основополагающем регламентирующем документе - ПБУ 19/02. Исходя из вышеизложенного, можно столкнуться с тем, что раскрытие данного термина зависит от видения автора. Для примера, приведу несколько понятий разных авторов.

Согласно, изложенному материалу в книге «Бухгалтерский учет», изданной под научным руководством А.Д. Ларионова [8,211], финансовые вложения преимущественно представляют собой активы организации, которые используются с целью наращивания ее капитала или достижения иных целей, направленных на экономическое развитие организации.

Костева Н.Н., Гвоздевская А.Е. и Плякина А.С. в своей статье «Сущность и виды финансовых вложений» представили понятие финансовых вложений в виде вкладов организации в различные ценные бумаги и/или в виде займов, предоставленных организацией. [7, 33].

Ремизова О. Н. в своей монографии «Финансовые вложения: понятие, бухгалтерский учет» рассматривает суть финансовые вложения в виде вложений финансовых ресурсов организации в другие организации с помощью процессов покупки их ценных бумаг, предоставлении заемных средств и др.

Ганеса К. О., автор книги «Финансовые вложения, виды и учет», сформировала понимание финансовых вложений, в виде вкладов финансовых ресурсов в ценные бумаги других организаций и государства, выдачу займов для получения денежных средств [9,73].

Миллер Д.П. дал определение финансовым вложениям как инвестициям денежных средств организации в ценные бумаги государства, ценные бумаги других организаций, выдачу займов контрагентам и иным участникам финансовых отношений, финансовые вклады в совместные активы в рамках договоров о совместной деятельности [10,90].

Широбоков В. Г. пишет, что финансовые вложения – представляют собой вклады денежных средств в активы других компаний. При этом, подобные вклады не должны иметь общие начала с основным видом деятельности организации, а еще, помимо вышеизложенного [11,45].

Рассмотрев вышеуказанные определения, выделим два основных подхода к пониманию категории «финансовые вложения». Первый подход заключается в определении финансового вложения как инвестиций в другие организации (в форме займов или взносов в уставный капитал и т. п.) или в государственные ценные бумаги с целью получения прибыли.

Второй подход имеет более расплывчатое понимание, и состоит в раскрытии понятия финансового вложения в виде определенного списка активов, планируемая роль которых, заключается в доставке организации экономической выгоды, смысл которой заключается не только в получении денежных средств.

Таблица 1 – Требования нормативно-правовых документов к финансовым вложениям

Область сравнения	Источники нормативно-правового регулирования			
	МСФО (IAS 32, IAS 39, IFRS 9)	ПБУ 19/02	ГК РФ, 39-ФЗ	НК РФ
Сфера регулирования	Учет финансовых инструментов в концепции МСФО	Учет финансовых вложений по РСБУ	Правовое регулирование ценных бумаг и обязательств	Налогообложение операций и дохода (убытка), получаемого от сделок с финансовыми вложениями
Понятие финансовых вложений (финансовых активов)	Финансовый актив представляет собой актив, который является средством обмена или правом, позволяющим получить какой-либо актив	Отсутствует	Отсутствует, так как регулирует узкое направление ценных бумаг и обязательств по ним	Отсутствует
Критерии отнесения к финансовым вложениям	Право получения актива по итогам погашения	- Наличие надлежаще оформленных документов	Отсутствуют в ГК, дан четкий перечень	Отсутствуют

	финансового актива	- Переход вместе с финансовыми вложениями рисков, по этим вложениям - Способность финансовых вложений приносить организации доход в будущем - Отсутствие материально-вещественной формы	ь признак ов в 39-ФЗ	
Ограничения в отнесении актива к финансовым вложениям	К финансовым активам НЕ относятся: 1) физические активы 2) активы, которые в дальнейшем принесут получение товаров и услуг 3) активы недоговорного характера	Финансовыми вложениями не являются: 1) собственные акции компании; 2) векселя, выписанные поставщикам 3) вклады в материальное имущество с целью получения дохода от его сдачи пользование за плату 4) специализированные активы (драг металлы, культурные ценности и т. п.), не предназначенные для обычных видов деятельности	Отсутствуют	Отсутствуют

Авторы обоих подходов имеют одинаковое мнение, что финансовое вложение — это актив, который должен в будущем принести организации экономическую выгоду. Однако сторонники первого подхода видят эту выгоду преимущественно в денежной форме, что существенно сужает диапазон активов, квалифицируемых в качестве финансовых вложений. Например, в состав финансовых вложений не будут включены предоставленный заем или приобретенная ценная бумага, если по ним предусмотрена возможность погашения должником обязательств не денежными средствами, а другим видом актива. Такое ограничение

является недостатком данного подхода. Второй подход этого недостатка лишен.

Но оба подхода совершенно не затрагивают финансовые вложения, целью которых не является получение прибыли. Наиболее распространенным примером подобных финансовых вложений будет являться инвестирование (вклады, приобретение ценных бумаг) малых организаций их более крупными партнерами в составе групп компаний (холдинг или других объединений).

Финансовые вложения, находящиеся на учете организации, могут представлять собой следующие варианты: государственные и муниципальные ценные бумаги (как правило, подобные ценные бумаги представлены облигациями), ценные бумаги, выпущенные иными компаниями (наиболее распространены в данном направлении – акции); финансовые вложения в другие компании (уставный капитал); финансовые фидуциарии, выданные организациям-заемщикам (исключение – беспроцентное заимствование денежных средств); банковские (деPOSITные) вклады, созданные с целью сохранения и увеличения положенных на них денежных сумм; приобретение дебиторской задолженности по договору уступки права требования (цессия); инвестиции в рамках договоренностей по ведению совместной деятельности (например, на основе товарищества); и иные финансовые вклады компании.

С ростом экономического рынка РФ стали расти и экономические возможности компаний. У них появилась возможность вести более активно инвестиционную деятельность, что вызвало повышение интереса потенциальных вкладчиков к производным финансовым инструментам (далее - ПФИ) или деривативам. На текущий момент ПФИ представлены следующими типами производных ценных бумаг: фьючерс, форвардный контракт, опцион, варрантам и др. Такие понятия как «финансовый инструмент», «финансовый актив», «долевой инструмент», «финансовое обязательство», «производный финансовый инструмент» или «дериватив» особенно актуально используются инвестиционными площадками с целью повышения интереса к биржевым торгам. В современных условиях информатизации экономических процессов одним из перспективных направлений является представления достоверной информации в бухгалтерской и управленческой отчетности. Ситуация осложняется тем, что финансовые инструменты не могут учитываться из-за отсутствия необходимых элементов правовой основы, потенциально способной грамотно регламентировать учет подобных финансовых вложений, включая рассмотренные ранее ПФИ. Рынок ценных бумаг находится в фазе динамичного развития, предлагая инвесторам новые виды продуктов,

вызывая тем самым, необходимость в постоянном обновлении нормативно-правовой базы по учету финансовых вложений. В специализированной литературе и других источниках по данной теме, встречается понятие финансовых инвестиций. Данной понятие по своему смыслу соответствует идее финансовых вложений, однако, большинство пользователей подразумевает под ним именно приобретённые ценные бумаги других организаций. Понятие финансовой инвестиции имеет более узкий смысл вложения денежных средств, который ставит собой цель в виде получения прибыли с потраченных средств. В связи с этим, данное понятие имеет смысл дифференцировать, чтобы не путать пользователей информации. Очень распространены случаи, когда денежные средства инвестируются в финансовые вложения, которые представляют собой ценные бумаги, нормативно-правовое регулирование которых исходит из Гражданского кодекса РФ и Федерального закона «О рынке ценных бумаг» № 39-ФЗ от 22.04.1996. Смысл определений «финансовые вложения» и «ценные бумаги» зачастую могут быть очень близки по смыслу, однако не все ценные бумаги будут являться объектом финансовых вложений, как и не все финансовые вложения попадают под нормативно-правовое регулирование ценных бумаг.

В качестве наиболее важных направлений совершенствования правил идентификации финансовых вложений и систематизации терминологической основы данной области бухгалтерского учета могут быть выделены следующие.

1) Дополнение действующих нормативно-правовых актов, регулирующих как учет финансовых вложений, так и порядок проведения операций с ними, с целью выработки единой позиции. Например, ввести в ПБУ19/02 следующее определение категории финансовых вложений. «Финансовые вложения – это финансовые активы, позволяющие признать финансовое обязательство контрагента или могут быть использованы в качестве долевого инструмента». Данное или аналогичное по смыслу определение позволит исключить из перечня финансовых вложений такие драгоценные металлы и валюту. Исчезают также проблемы со включением в состав финансовых инструментов как уже применяемых, так и вновь разрабатываемых участниками фондового рынка производных финансовых инструментов.

2) Актуализация требований нормативно-правовых актов, регулирующих учет финансовых вложений, а также порядок проведения и налогообложения операций с ними, с целью гармонизации трактовки используемых в них категорий с определений, декларируемых в учетных стандартах. Таким образом будет решена проблема обеспечения новых

видов финансовых инструментов сопутствующим нормативно-правовым и методическим регулированием.

Данные направления представляют собой минимум, который необходимо поддерживать в действующем законодательстве для корректного учета и отображения финансовых вложений и операций с ними. Дальнейшее совершенствование будет проходить в направлении максимального сближения регламентов российского бухгалтерского учета с международными учетными стандартами.

Список использованных источников:

1. "Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ (ред. от 28.06.2021, с изм. от 08.07.2021) [Электронный ресурс] // СПС КонсультантПлюс: Студент – URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения 01.11.2021);
2. "Налоговый кодекс Российской Федерации (часть первая)" от 31.07.1998 N 146-ФЗ (ред. от 02.07.2021) [Электронный ресурс] // СПС КонсультантПлюс: Студент – URL: http://www.consultant.ru/document/cons_doc_LAW_19671/ (дата обращения 01.11.2021);
3. "Международный стандарт финансовой отчетности (IAS) 32 "Финансовые инструменты: представление" (введен в действие на территории Российской Федерации Приказом Минфина России от 28.12.2015 N 217н) (ред. от 14.12.2020) [Электронный ресурс] // СПС КонсультантПлюс: Студент – URL: http://www.consultant.ru/document/cons_doc_LAW_193676/ (дата обращения 01.11.2021);
4. "Международный стандарт финансовой отчетности (IAS) 39 "Финансовые инструменты: признание и оценка" (введен в действие на территории Российской Федерации Приказом Минфина России от 28.12.2015 N 217н) (ред. от 17.02.2021) [Электронный ресурс] // СПС КонсультантПлюс: Студент – URL: http://www.consultant.ru/document/cons_doc_LAW_193673/ (дата обращения 01.11.2021);
5. "Международный стандарт финансовой отчетности (IFRS) 9 "Финансовые инструменты" (введен в действие на территории Российской Федерации в редакции 2014 года Приказом Минфина России от 27.06.2016 N 98н) (ред. от 17.02.2021) [Электронный ресурс] // СПС КонсультантПлюс: Студент – URL: http://www.consultant.ru/document/cons_doc_LAW_202060/ (дата обращения 01.11.2021);

6. Приказ Минфина России от 10.12.2002 N 126н (ред. от 06.04.2015) "Об утверждении Положения по бухгалтерскому учету "Учет финансовых вложений" ПБУ 19/02" (Зарегистрировано в Минюсте России 27.12.2002 N 4085);
7. Костева Н.Н. Гвоздевская А.Е. и Плякина А.С. Сущность и виды финансовых вложений / Н.Н. Костева // Colloquium–journal. – 2020. – № 8(32). – С. 33–34. [Электронный ресурс] // URL: <https://cyberleninka.ru/article/n/74284993> (дата обращения 16.11.2021)
8. Ларионов А.Д. Бухгалтерский учет / А.Д. Ларионов – Москва: Учебное пособие, 2020. - 368 с. [Электронный ресурс] // URL: https://primo.nl.ru/primo-explore/fulldisplay?docid=07NLR_LMS001702931 (дата обращения 16.11.2021)
9. Едророва В. Н., Мизиковский Е. А. Учет, оценка доходности и анализ финансовых вложений / В. Н. Едророва, Е. А. Мизиковский – Москва: Учебное пособие, 2021. – 368 с. [Электронный ресурс] // URL: https://primo.nl.ru/primo-explore/fulldisplay?docid=07NLR_LMS001123483 (дата обращения 16.11.2021)
10. Миллер Д.П. Учет ценных бумаг и финансовых вложений: Учебно-практическое пособие / Д.П. Миллер, Е.Н. Макарова. - М.: Дашков и К, 2020. - 264 с. [Электронный ресурс] //URL: <https://urait.ru/book/436911> (дата обращения 16.11.2021)
11. Широбоков В. Г. Бухгалтерский учет в организациях АПК: учебник для студентов вузов, обучающихся по специальности «Бухгалтерский учет, анализ и аудит» / В. Г. Широбоков. - Москва: Финансы и статистика, 2019. - 687 с. [Электронный ресурс] // URL: <https://cyberleninka.ru/article/n/42183240> (дата обращения 16.11.2021)

Проблемы обеспечения финансовой безопасности хозяйствующего субъекта в условиях аутсорсинга бухгалтерских услуг

А.Н. Кизилов

д.э.н., профессор, заведующий кафедрой аудита РГЭУ (РИНХ),

Ростов-на-Дону

E-mail: akizilov@inbox.ru

Аннотация: В статье рассматриваются ключевые положения о месте и роли аутсорсинга бухгалтерских услуг в системе финансовой безопасности хозяйствующих субъектов. Предложены основные подходы к определению аутсорсинга как экономического инструмента и одного из методов оптимизации затрат для повышения эффективности функционирования организаций. Определена необходимость предварительного оценивания рисков от использования стратегии аутсорсинга для финансовой безопасности субъектов хозяйствования.

Ключевые слова: финансовая безопасность, риски, аутсорсинг.

Problems of ensuring financial security of an economic entity in terms of outsourcing accounting services

Abstract: The article discusses the key provisions on the place and role of outsourcing accounting services in the financial security system of economic entities. The main approaches to the definition of outsourcing as an economic tool and one of the methods of cost optimization to improve the efficiency of organizations are proposed. The necessity of preliminary risk assessment from the use of outsourcing strategy for the financial security of business entities is determined.

Keywords: financial security, risks, outsourcing.

Финансовая безопасность на уровне субъекта хозяйственной деятельности предполагает устранение рисков потери устойчивости на рынках, как на внутреннем, так и на внешнем, причин снижения объема производства ниже отраслевых или запланированных и т.д. Такую информацию, достоверную и систематизированную стандартами бухгалтерского учета на государственном уровне, предоставляет бухгалтерская (финансовая) отчетность. Эта информация позволяет дать адекватную оценку состояния экономической системы локального уровня,

сопоставить контролируемые параметры управляемого объекта до и после принятия управленческого решения, оценить его эффективность, ожидаемые результаты, либо выявить проблемы для дальнейшего поиска альтернативных решений.

Основной, если не единственной, информационной системой для принятия управленческих решений выступают данные, формируемые в бухгалтерской (финансовой) отчетности субъекта хозяйствования. Принципы бухгалтерского учета, систематический и хронологический порядок учета фактов хозяйственной жизни позволяют получать информацию об объектах учета, принимать обоснованные и эффективные управленческие решения.

Устанавливая единые требования к бухгалтерской (финансовой) отчетности ФЗ «О бухгалтерском учете», федеральные стандарты бухгалтерского учета, в частности Положение по ведению бухгалтерского учета и бухгалтерской отчетности в РФ, в зависимости от объема учетных работ, определяют варианты организации ведения бухгалтерского учета экономического субъекта:

- «а) учредить бухгалтерскую службу как структурное подразделение, возглавляемое главным бухгалтером;

- б) ввести в штат должность бухгалтера;

- в) передать на договорных началах ведение бухгалтерского учета централизованной бухгалтерии, специализированной организации или бухгалтеру-специалисту;

- г) вести бухгалтерский учет лично» [4].

Одним из способов оптимизации деятельности предприятий путем уменьшения количества выполняемых ими функций и снижение дополнительных расходов в процессе хозяйственной деятельности является использование аутсорсинговых операций бухгалтерского учета (передать на договорных началах ведение бухгалтерского учета специализированной организации).

Услугами по ведению бухгалтерского учета внешними субъектами все чаще пользуются предприниматели малого и среднего бизнеса и вновь созданные компании. А учитывая тот факт, что в России в последние годы наблюдается положительная динамика количества как малых, так и средних предприятий, а также увеличение их доли в общем количестве предприятий, практика внедрения аутсорсинга, в том числе бухгалтерского, в современном бизнесе будет получать все большее распространение.

Другими словами, сам термин «аутсорсинг бухгалтерских услуг» в российском законодательстве отсутствует, но такого рода деятельность осуществляется.

По данным российской справочно-информационной системы СПАРК-Интерфакс [5] из действующих в России в 2020 г. юридических лиц – 3.44 млн. ЮЛ и 3.22 млн. ИП услугами бухгалтерского аутсорсинга, согласно исследованию компании «NeoAnalytics», пользуются около 1 млн. компаний и индивидуальных предпринимателей [6].

По утверждению аналитиков рынок аутсорсинга бухгалтерских услуг динамично развивается и является одним из наиболее перспективных в России. Этому способствует ряд причин: со стороны государства – ужесточение контроля за сбором налогов; со стороны организаций, штатные сотрудники которых не обладают требуемой квалификацией или должны сдавать отчетность по МСФО – привлекают специалистов более высокого уровня; со стороны собственников бизнеса – застраховаться от ошибок персонала и минимизировать фискальную нагрузку в виде штрафов и начислений.

В мировой практике аутсорсинг считается эффективным инструментом делового сотрудничества, его развитие рынка позволяет компаниям спокойно заниматься основной деятельностью, отдавая формирование налоговой отчетности и другие сегменты бухгалтерского учета профессионалам. В развитых странах услугами аутсорсеров в сфере ведения бухгалтерского учета по оценкам пользуются от 86 до 92 % предприятий малого и среднего бизнеса. Так в европейских странах, согласно исследований ученых, в сегменте малых компаний услугами бухгалтерских бюро пользовалось около 63 %, а в сегменте средних и крупных предприятий их доля составляла до 70%.

Зарубежный опыт свидетельствует о возможности значительного увеличения доходов предприятий с помощью применения этого метода. Однако, как и любой новый способ повышения эффективности хозяйственной деятельности, аутсорсинг бухгалтерских услуг имеет свои особенности, предпосылки, преимущества и недостатки.

Поэтому, прежде чем использовать аутсорсинг бухгалтерских услуг, целесообразно провести анализ рисков, связанных с его применением и разработать стратегию управления ими. Контракты с высокой степенью риска требуют более серьезного и тщательного контроля, с более низким – периодического мониторинга. Под рисками будем понимать экономическую категорию в деятельности субъектов хозяйствования, связанную с преодолением неопределенности и конфликтности в ситуациях оценивания, управления и выбора. Оценка риска является многомерной величиной, характеризующей возможные отклонения от целей, а также от желаемого результата с учетом влияния контролируемых и неконтролируемых факторов.

По мнению ученых-экономистов, наиболее характерными рисками использования бухгалтерского аутсорсинга является: снижение эффективности труда собственного персонала и потеря им необходимых знаний и опыта реализации функции, которая передается в аутсорсинг; недобросовестности аутсорсера, возникновения форс-мажорных обстоятельств или его банкротства; виток информации – угроза информационной безопасности компании, что обуславливает необходимость сотрудничества только с проверенными организациями с отличной репутацией; потеря контроля над собственными ресурсами, отстранение руководства от определенной сферы деятельности компании, что может привести к неадекватным управленческим решениям; в случае повышения цен на услуги, стоимость функции, передана на аутсорсинг может превысить ее внутреннюю себестоимость, что влечет за собой неэффективность использования такой концепции.

Также необходимо отметить, что каждое преимущество может представлять угрозу для предприятия при учете отдельных ключевых моментов использования бухгалтерского аутсорсинга, в то же время и потенциальные риски его применения в долгосрочной перспективе могут стать преимуществом. В частности, снижение риска махинаций (аутсорсер не имеет доступа к имуществу и денежным средствам заказчика) в долгосрочной перспективе имеет риск убытков из-за низкого качества получаемых услуг. При этом, возможность оптимизировать налоги (исполнитель имеет опыт большого количества клиентов из разных сфер бизнеса) не учитывает риск отсутствия индивидуального подхода к заказчику.

Как представлено на рис. 1, аутсорсинг бухгалтерских услуг могут оказывать аудиторские и консалтинговые организации.

Оказывая услуги субъектам хозяйственной деятельности в области бухгалтерского аутсорсинга аудиторские и консалтинговые организации должны оценивать риски легализации (отмывания) денег и финансирования терроризма для понимания рисков и угроз финансовой системе и экономике.

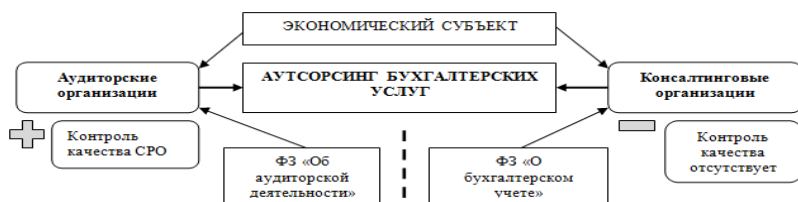


Рисунок 1 – Варианты организации аутсорсинга бухгалтерских услуг экономическим субъектом

Основным законодательным актом, регламентирующим вопросы финансовой безопасности России, выступает Федеральный закон РФ от 7 августа 2001 г. №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [7].

Публичная версия отчета о проведении Национальной оценки рисков легализации (отмывания) преступных доходов 2017-2018 размещена на официальном сайте Росфинмониторинга в сети Интернет и свидетельствует о том, что одним из основных уязвимых мест национальной системы противодействия отмыванию доходов (ПОД) с которым сталкиваются учетные работники и аудиторы в своей профессиональной деятельности является отсутствие регулирования и государственного надзора за выпуском и обращением виртуальных валют.

Как показано на рис.2, исходя из оценки национальных рисков отмывания доходов Росфинмониторингом риск использования виртуальных валют (типа «биткоин» и пр.) в схемах легализации преступных доходов оценен как максимальный или «группа высокого риска». По результатам отчета Росфинмониторинга виртуальные валюты «могут использоваться на различных этапах движения наркодоходов, включая расчеты наркопотребителей за наркотики, легализацию полученного преступного дохода и распределение денежных средств между организаторами ОПГ, а также выплату вознаграждений закладчикам, наркокурьерам, работникам нарколабораторий».

Риск использования других финансовых секторов и установленных нефинансовых предприятий и профессий (УНФПП), к которым в частности отнесены аудиторы, адвокаты, юристы, бухгалтеры включены в IV группу, группу низкого риска.

Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и ст.13 Федерального закона «Об аудиторской деятельности» [8] обязывает аудиторские и консалтинговые организации уведомлять уполномоченный орган (Росфинмониторинг) о любых основаниях полагать, что сделки или финансовые операции заказчика услуг или аудируемого лица связаны с легализацией (отмыванием) доходов, полученных преступным путем, или финансированием терроризма. Разглашать факт передачи данной информации, а также информировать руководство аудируемого лица о возникновении названных предположений аудиторы не вправе. Порядок передачи сведений определяет Правительство РФ. На сайте Росфинмониторинга предусмотрены личные кабинеты для взаимодействия аудиторских и консалтинговых организаций с ведомством.

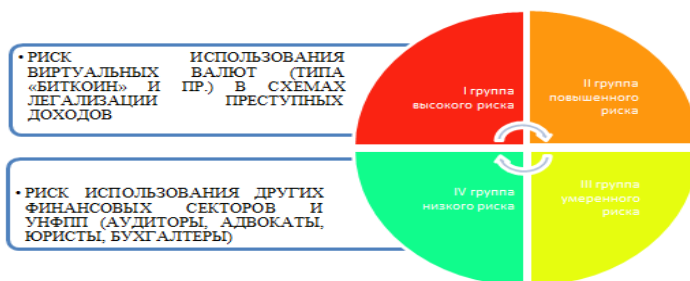


Рисунок 2 – Ранжирование рисков легализации (отмывания) преступных доходов связанных с аудиторской деятельностью и деятельностью в сфере оказания бухгалтерских услуг

Особенности оказания аутсорсинга бухгалтерских услуг аудиторами и бухгалтерами в рамках предпринимательской деятельности, при осуществлении которой применяются технологии и методики по выявлению противоправных действий субъектов хозяйствования и перечня экономических правонарушений формируют новые возможности для оптимизации производства и экономии затрат, создают конкурентные преимущества и позволяют организации быть более гибкой в отношении внешней среды что, в свою очередь, повышает уровень ее финансовой безопасности.

Список использованных источников:

1. Указ Президента РФ от 13.05.2017 №208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года»
2. Миронова О.А. Развитие экономической безопасности как науки: проблемы и перспективы // Инновационное развитие экономики, 2019. - №2 (50). – С. 332-338.
3. Дементьев Н.В. Экономическая безопасность в структуре национальной безопасности современной России // Социально-экономические явления и процессы. – 2011. - №5-6.
4. Приказ Минфина России от 29.07.1998 №34н «Об утверждении Положения по ведению бухгалтерского учета и бухгалтерской отчетности в Российской Федерации»
5. <https://www.spark-interfax.ru/statistics>
6. <https://marketing.rbc.ru/articles/12281/>
7. Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 №115-ФЗ
8. Федеральный закон «Об аудиторской деятельности» от 30.12.2008 №307-ФЗ

Проблемы цифровизации национальных валют

М.А. Лынный

студент 3 курса бакалавриата КФУ им. В.И. Вернадского, Симферополь

E-mail: marina.lynnick@mail.ru

научный руководитель: В.В. Ворошило

к.э.н., доцент кафедры финансов и кредита КФУ им. В.И. Вернадского,

Симферополь

E-mail: mivik06@mail.ru

Аннотация: В статье анализируются причины и последствия внедрения цифровых валют центральных банков ведущих стран мира в платежную систему. На основе проведенного анализа автором статьи были систематизированы сведения о проектах по внедрению CBDC, инициированные центральными банками, и определены основные проблемы, возникающие с введением цифровых национальных валют.

Ключевые слова: цифровизация, цифровые валюты, CBDC, центральный банк, токен, проблемы.

Problems of digitalization of national currencies

Abstract: The article analyzes the reasons and consequences of the introduction of digital currencies of the central banks of the world's leading countries into the payment system. Based on the analysis, the author of the article systematized information about CBDC implementation projects initiated by central banks, and identified the main problems arising with the introduction of digital national currencies.

Keywords: digitalization, digital currencies, CBDC, central bank, token, problems.

Деньги имеют огромное значение в экономической жизни любого государства. С экономическим развитием менялись и формы денег. На современном этапе по всему миру, и в Российской Федерации, в частности, все больше граждан используют безналичную оплату. При таком спросе на электронный расчет и хранение денежных средств государством, банками и отдельными организациями активно внедряются цифровые финансовые технологии.

Актуальность данной темы заключается в том, что цифровизация национальных валюты позволяет противостоять всемирным финансовым вызовам. Банки мировых стран обращены на то, чтобы денежная система отвечала быстро изменяющимся потребностям граждан и предприятий, содействовала внедрению инноваций на финансовый рынок. Поэтому, на сегодняшний день важно изучить проблемы, препятствующие созданию цифровой валюты в качестве дополнительной формы денег.

Банк международных расчетов (BIS) в 2019 г. опубликовал отчет, в котором отмечалось, что 80% всех центральных банков занимаются анализом и созданием государственных цифровых валют – CBDC (Central Bank Digital Currency). На сегодняшний день не существует единственного, общепринятого в мировой практике определения CBDC. Как отмечает Банк международных расчетов (BIS), CBDC не является четко определенным термином. Все определения сходятся в том, что CBDC является новой формой цифровых денег, сочетающая возможности наличных и электронных денег и являющаяся законным платежным средством [1,2].

С внедрением CBDC платежные операции смогут стать более быстрыми, дешевыми и эффективными как внутри страны, так и на международном уровне. Введение CBDC также предполагает большую безопасность и меньший риск мошенничества с использованием

т
е
х

В настоящее время центральные банки всех развитых стран мира обсуждают две модели CBDC: розничная модель CBDC и оптовая модель CBDC. По результатам проведенного исследования процессов разработки и внедрения цифровых валют центральных банков в ведущих странах мира была составлена таблица 1.

и
и

Таблица 1 – Проекты по внедрению CBDC, инициированные центральными банками (Источник: составлено автором на основе [2])

б
л
о
к
ч
е
й
н
.

Организация	Вид CBDC	Статус
Центральный Банк Франции	Оптовая модель	Пилотный проект
Фонд для разработки цифрового доллара (США)	Оптовая и розничная модель	5 пилотных проектов
Народный Банк Китая	Розничная модель	Пилотный проект

Б
л
о
к
ч
е
й

Валютное управление Сингапура	Оптовая модель	Разработка пилотного проекта
Центральный Банк России	Розничная модель	В состоянии исследования и возможного применения

Розничные платежи обычно представляют собой платежи между физическими и юридическими лицами. Как правило, они имеют низкую стоимость, но больший объем сделок, и осуществляются с помощью различных платежных инструментов. Розничная цифровая валюта центрального банка – это электронные деньги центрального банка, которые, как и наличные, напрямую доступны физическим и юридическим лицам.

Розничные CBDC могут предлагаться населению в двух различных формах:

- депозитные счета в центральном банке;
- токены, выпущенные в цифровом виде.

В случае депозитных счетов физические и юридические лица смогут открывать счета в своих центральных банках и пользоваться теми же услугами, которые предоставляют коммерческие банки.

CBDC, выпущенные в форме токенов, представляют собой электронную альтернативу банкнотам и монетам. Они будут выпускаться только центральным банком для распространения между коммерческими банками.

Оптовая модель CBDC, предполагает осуществление платежей и расчетов по транзакциям между финансовыми учреждениями. Эта модель может повысить эффективность управления рисками процесса расчетов, потенциально усиливая эти преимущества за счет расширения доступности оптовых CBDC для участников финансового рынка, которым в настоящее время не разрешено иметь счета в центральном банке [4].

В 2020 г. пандемия привела к повышению темпов цифровизации экономики, тем самым создав основу для более ускоренного формирования рынка цифровых валют центральных банков. Нельзя не согласиться с высказыванием в докладе Deutsche Bank о том, что «новая реальность», вызванная COVID-19, окончательно сделала замену наличных денег на цифровые неизбежной [1].

В своем исследовании аналитики The Block отметили факторы, которые стимулируют страны заниматься разработкой CBDC. Одними из них являются:

- новые инструменты денежно-кредитной политики;
- увеличение доступа к финансовым услугам;

– уменьшение затрат в финансовой сфере.

Бесспорным лидером в развитии национальных цифровых валют остается Китай. Экономика данной страны готова к цифровизации своей национальной валюты – китайский юань. В 2018 году число пользователей таким платежным приложением, как WeChat Pay приблизилось к цифре 1,1 млрд человек, а у следующего за ним приложением Alipay число клиентов составило 900 млн. В тоже время CBDC может заменить формально запрещенные в КНР криптовалюты.

В качестве причин выпуска цифрового юаня отмечены: совершенствование качества предоставляемых финансовых услуг и снижение издержек на поддержание денег в обращении.

В июне 2021 г. в рамках пилотного проекта в 6 городах Китая было совершено 1,32 млн операций по оплате товаров и услуг цифровым юанем (DCEP), открыто для граждан более 20 млн кошельков и 3,5 млн кошельков для юридических лиц. По мнению экспертов, DCEP сможет показать свои достоинства только после внедрения его во все сферы экономической деятельности государства. Народный банк Китая в отчетных документах упоминает, что цифровой юань будет еще тестироваться во время проведения зимней Олимпиады 2022 в Пекине [1, 5].

Руководство Федеральной резервной системы (ФРС) США задумалось о разработке национальной криптовалюты позже, чем центробанки других развитых стран: к примеру, китайское правительство начало подготовку к запуску цифрового юаня еще в 2014 году, как только курс биткоина подскочил с \$13,4 до \$1000.

Федеральная резервная система в августе 2020 г. выпустила информационные данные, в которых сообщила о начале работы технической платформы для создания цифрового доллара. Первый эксперимент должен пройти на базе Федерального резервного банка Бостона совместно с учеными из Массачусетского технологического института. При этом финансовым регулятором было подчеркнуто, что проект направлен на исследование сильных и слабых сторон технологии, а не на создание конкретного прототипа [1].

Мировым экономическим центром, который находится ближе к выпуску государственных цифровых валют по сравнению с США, но дальше, чем Китай, является Европейский Союз. Там процесс разработки цифрового евро к осени этого года перешел от теоретических вопросов к определению конкретных сроков начала тестирования. Кристин Лагард, глава Европейского центрального банка (ЕЦБ), в сентябре 2020 г. заявила, что благодаря пандемии создание цифрового евро также ускорила пандемия: в первые полгода продажи в сфере электронной коммерции в ЕС выросли на 20%.

Европейский центральный банк в октябре 2020 г. выпустил документ, посвященный цифровому евро. В нем ЕЦБ отметил, что CBDC не заменит денежные купюры и монеты, а станет дополнительной формой денег. Впрочем уже в ноябре глава Европейского центрального банка заявила, что власти ЕС не спешат быть первыми в запуске цифровых национальных валют. Данное решение должно быть принято коллективно, с участием всех стран-участников союза, а с момента его принятия и до запуска пройдет от 2 до 4 лет [1,6].

Долгое время Банк России отказывался от идеи введения российской цифровой валюты, но в октябре 2020 г. неожиданно выпустил подробный доклад, в котором рассматривались характеристики цифрового рубля. Цифровой рубль станет современной формой российской национальной валюты, будет эмитироваться ЦБ РФ и использоваться на всей территории государства наравне с наличными и безналичными рублями. Внедрение данной инновации позволит цифровому рублю иметь дополнительные преимущества повышающие его привлекательность как средства платежа. Планируется доступ к своему цифровому кошельку в офлайн-режиме, без доступа к сети Интернет. Это позволит гражданам и предпринимателям иметь доступ к финансовой организации, в которой обслуживаются и совершать операции 24/7.

Цифровой рубль в отечественной экономике окажет значительное воздействие на доходность и ликвидность банковского сектора, финансовую стабильность, а также на трансмиссионный механизм ДКП нашего государства в целом.

В тоже время, Национальный банк Украины (НБУ) провел пробное испытание «электронной гривны» еще в 2018 году. Итоги тестирования «электронной гривны» были представлены на большой конференции НБУ, которая проходила с участием представителей других центробанков в феврале 2020 г.

Национальный банк Украины дал следующее определение электронной гривны – это фиатная валюта в электронном виде, которая в будущем должна обмениваться на наличные или безналичные деньги в отношении 1:1. Стоит подчеркнуть, что украинская цифровая валюта не обязательно будет построена на технологии блокчейн [1, 7].

Несмотря на то что выпуском цифровых национальных валюты занимаются центральные банки, такая форма денег несет определенные проблемы для пользователей, банковской системы, государства и финансового регулятора. Проблемы, связанные с цифровизацией национальных валют, предложены на рисунке 1.



Рисунок 1 – Проблемы СВ
(Источник: составлено автором на основе [2,4])

Для пользователей основными проблемами могут стать кибернетические – угроза потери денег из-за взломов системы злоумышленниками. И операционные – сбои в системе, приводящие к потере сведений пользователей. В остальном деньги центробанка для потребителей безопасны: они не подвержены колебаниям, происходящим на рынке и по ним отсутствует кредитный риск.

Второй значительной проблемой является потенциальное уменьшение прибыльности коммерческих банков за счет потери клиентов, так как часть из них отдаст предпочтение услугам центрального банка, а не частных кредитных организаций. Это повлечет за собой утрату банками части комиссионных доходов.

Весьма вероятно, что цифровые деньги центральных банков будут конкурировать с депозитами физических и юридических лиц в коммерческих банках. Если для граждан и организаций появится возможность открывать счета в центральном банке, то в условиях финансовой нестабильности это будет приводить к оттоку средств из коммерческих банков на счета (или токены) центробанка. Отток средств будет ухудшать ликвидность коммерческих банков и препятствовать им выполнять функции финансовых посредников. В этой ситуации пострадает сфера кредитования, а также инвестиционная отрасль [2,4].

Рискам, связанным с цифровыми деньгами центральных банков, была посвящена большая часть выступления Ива Мерша на конференции Consensus в мае 2020 г. Хотя член правления Европейского центрального банка (ЕЦБ) говорил о цифровом евро, его высказывания актуальны и для

CBDC любой другой страны. Одной из основных проблем Ива Мерш видел в ликвидации анонимности при платежах. Помимо этого он также озадачен вопросом о том, кто будет создавать счета цифрового евро и управлять ими – центральные или коммерческие банки [4].

Первый вариант, по мнению Ива Мерша, неэффективный, так как сосредоточение значительных финансовых ресурсов в руках центробанка нерентабельно. Центробанки исторически не предназначены для размещения в них индивидуальных депозитов, выдачи кредитов и оказания других коммерческих услуг. Выходом из сложившейся ситуации было бы обязательное применение коммерческих банков, как второго уровня между центробанком и экономической сферой при распространении CBDC. Как это было сделано в Китае.

Государство и финансовый регулятор также имеют определенные проблемы в области CBDC: стратегические и репутационные. Расширение сфер влияния и ответственности в части увеличения клиентской базы повлечет за собой необходимость организационного изменения штатной работы центробанков, а возможные неполадки в системе могут повлечь за собой репутационные издержки как для регулятора, так и государства в целом [4].

Таким образом, мы выяснили, что на сегодняшний день для центральных банков существуют необходимые ресурсы для обеспечения эмиссионных операций, предусматривающие выпуск собственных цифровых денег. Однако существующие проблемы для клиентов, банковской и финансовой системы, а также государства пока удерживают центробанки от этого шага.

Список использованных источников:

1. CBDC в 2021 году: насколько центробанки близки к выпуску цифровой валюты [Электронный ресурс]. – URL: <https://media.sigen.pro/articles/1223> (дата обращения 13.11.2021)
2. Некрасова, И.В. Причины и последствия внедрения цифровых валют центральных банков в платежную систему ведущих стран мира / И. В. Некрасова // Государственное и муниципальное управление. Ученые записки. – 2021. – № 3. – с. 141-145. – Текст: электронный // Лань: электронно-библиотечная система. – URL: <https://e.lanbook.com/journal/issue/315335> (дата обращения: 13.11.2021).
3. Мамонтова С. В., Муродзода У. Эволюция денег и современные тенденции их преобразований // РСЭУ. – 2020. – №1 (48). URL: <https://cyberleninka.ru/article/n/evolyutsiya-deneg-i-sovremennye-tendentsii-ih-preobrazovaniy> (дата обращения: 13.11.2021).

4. Ларина О.И., Акимов О. М. Цифровые деньги на современном этапе: ключевые риски и направления развития // Финансы: теория и практика. – 2020. – №24 (4). – с.18-30. . – URL: <http://www.fa.ru/org/div/edition/vestnik/SiteAssets/Pages/now/18-30.pdf> (дата обращения: 13.11.2021).
5. Цифровой юань: подробный обзор китайской валюты будущего [Электронный ресурс]. – URL: <https://www.rbc.ru/crypto/news/6127c1cb9a7947396479f560> (дата обращения 13.11.2021).
6. Доклад ЕЦБ о разработке цифрового евро. 4 условия запуска криптовалюты [Электронный ресурс]. – URL: <https://www.rbc.ru/crypto/news/5f770c519a79470c9f50b798> (дата обращения 14.11.2021).
7. Доклад для общественных консультаций «Цифровой рубль», октябрь 2020 г. – [Электронный ресурс]. – URL: https://cbr.ru/StaticHtml/File/112957/Consultation_Paper_201013.pdf (дата обращения 14.11.2021).

Пути обнаружения и предотвращения киберугроз

В.М. Гапанович

студент 3 курса НИЯУ МИФИ, Москва

E-mail: walik.smille@mail.ru

В.Н. Чернова

студент 3 курса НИЯУ МИФИ, Москва

E-mail: chernova.vn@mail.ru

А.С. Деревенская

студент 3 курса НИЯУ МИФИ, Москва

E-mail: derenbka46@mail.ru

С.Е. Климова

к.э.н., доцент кафедры финансового мониторинга НИЯУ МИФИ, Москва

E-mail: seklimova@mephi.ru

Аннотация: Целью работы было исследование киберугрозы как проблемы и поиск путей её предотвращения. Были проанализированы отчеты и статьи, касающиеся области кибератак. В результате сформулированы рекомендации для решения проблемы нарушения кибербезопасности.

Ключевые слова: кибератака, киберугроза, кибербезопасность.

Ways to detect and prevent cyber threats

Abstract: The purpose of the work was to study cyber threats as a problem and to find ways to prevent it. Reports and articles related to the field of cyber attacks were analyzed. As a result, recommendations are formulated to solve the problem of cybersecurity violations.

Keywords: cyberattacks, cyber threats, cybersecurity.

Кибербезопасность — это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Цель кибератак заключается в получении доступа к конфиденциальной информации, ее изменении или уничтожении, получении денег незаконным путем.

В отношении финансового сектора имеют смысл кибератаки в целях возврата криминально нажитых средств обратно в законную финансовую систему для последующего использования, то есть осуществление схем отмыwania доходов, полученных преступным путем.

Процесс отмыwania денег при помощи кибератак состоит из трех этапов:

1. Размещение – первый перевод денег со счета жертвы на счет мошенников или размещение украденных наличных средств на счете мошенников;
2. Наслоение - серия транзакций, помогающих скрыть происхождение средств и их настоящего владельца;
3. Интеграция – вложение отмытых денег в легальный или криминальный бизнес.

Киберпреступники открывают множество счетов, принадлежащих физическим и юридическим лицам, с помощью поддельных или украденных документов. Для этого существует такое понятие, как "денежный мул" - жертва взлома. Им принадлежат счета, созданные мошенниками.

Не так давно криптовалюты присоединились к инструментам отмыwania денег. Киберпреступников привлекает этот мошеннический метод, поскольку для проведения виртуальных транзакций пользователям не нужно предоставлять персональные данные, что упрощает реализацию планов по отмыwанию денег. Но использование криптовалюты остаётся пока не идеальным и отчасти сложным, так как для вывода средств из мошеннической схемы требуется довольно много операций.

Статистика кибератак за последнее время

Согласно данным Всемирного экономического форума, в прошлом году мировая экономика понесла убытки из-за кибератак в размере 2,5 трлн долларов США, а к 2022 году они могут достичь 8 трлн долларов США.

Group-IB — одна из ведущих компаний-разработчиков решений для предотвращения кибератак. На основе данных, предоставленных этой компанией, был проведен анализ статистики преступлений, который показал, что мошенничество стало основным киберпреступлением в интернете. Суммарно на мошенничество приходится 73% всех киберпреступлений в Интернете.

Скам – обман с добровольным платежом и раскрытием своих данных.

Фишинг – кража данных банковских карт.



Рисунок 1 – Мошенничество как киберпреступление в интернете

Основными видами мошенничества можно выделить (по сумме транзакций):

- через мобильные приложения (43%);
- с использованием банковских карт (42%).



Рисунок 2 – Каналы вывода похищенных средств



Рисунок 3 – Каналы вывода похищенных средств на 2019 г.

Согласно агрегированной статистике *Positive Technologies*, международной компании, специализирующейся на разработке инновационных решений в области информационной безопасности, в первом квартале 2020 года было зафиксировано на 22,5 % больше, чем в последнем квартале 2019 года.

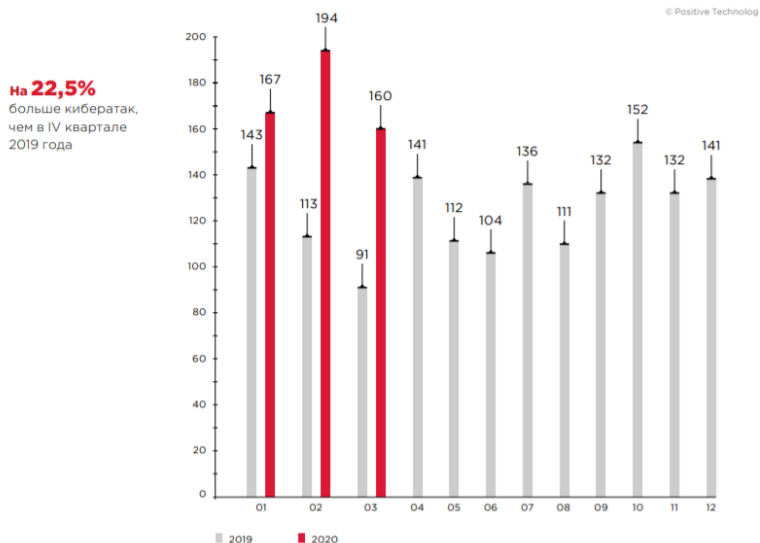


Рисунок 4 – Количество атак в 2019 и 2020 годах по месяцам (на первый квартал 2020 года)

По сравнению с первым кварталом 2021 года количество атак увеличилось на 0,3%. Также увеличилась доля атак, мотивированных финансовой выгодой (с 43 % до 59 %). В большинстве случаев злоумышленники нападали на медицинские и государственные учреждения, а также на промышленный сектор. В атаках на частных лиц злоумышленники в основном руководствуются мотивом получения данных. Его доля по сравнению с первым кварталом 2021 года увеличилась на 9 % и составляет до 78 %, в то время как количество украденных платежных данных в два раза увеличилось.

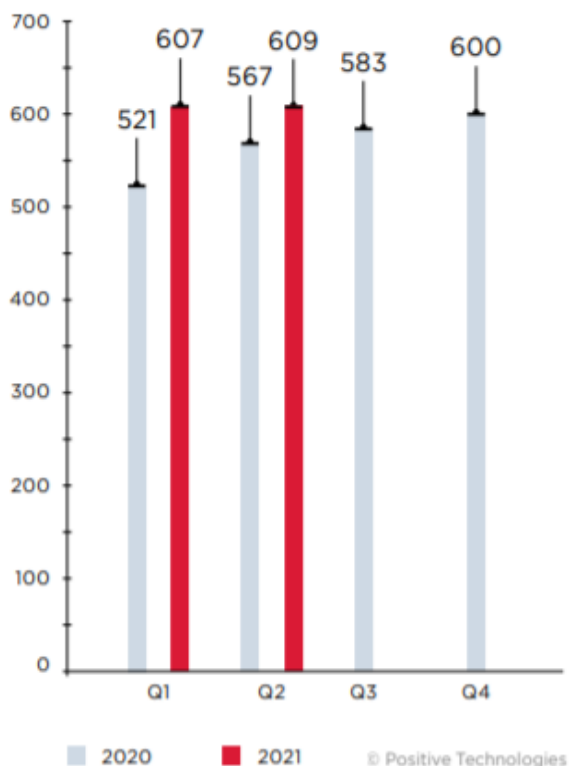


Рисунок 5 – Количество атак в 2020 и 2021 годах по кварталам (на второй квартал 2021 года)

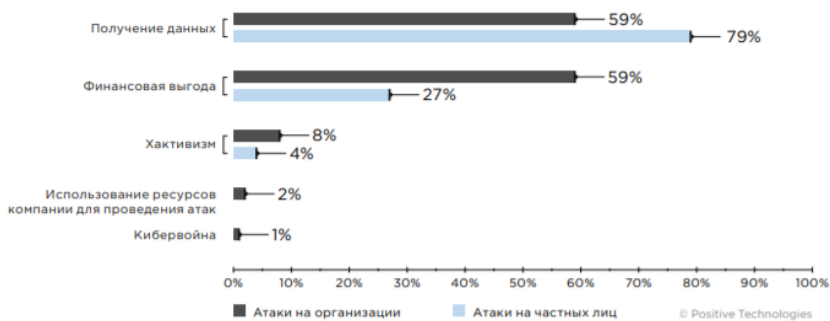


Рисунок 2. Мотивы злоумышленников (доля атак)

77% атак носили целенаправленный характер

Рисунок 6 – Мотивы злоумышленников (доля атак)

В конце 2019 и 2020 годов произошел новый раунд атак с использованием программ шифрования. Большинство вымогателей нападают на компании в коммерческом и государственном секторах.

В общей сложности в 2020 году шифровальщики атаковали компании более чем в 45 странах в более чем 500 странах мира. Нижний предел общего ущерба, причиненного актом вымогательства, превышает 1 миллиард долларов США (1 005 186 000 долларов США). Однако реальный ущерб намного выше: обычно пострадавшие компании стараются скрыть инцидент, выплачивая вымогателям, иначе атака не сопровождается публикацией данных из сети жертвы.

Согласно статистике *Group-IB*, объем транзакций российского рынка киберпреступности со второй половины 2018 года по первую половину 2019 года достиг почти 510 миллионов рублей. Согласно отчету МВД России "Состояние преступности в России", с января по октябрь 2019 года в стране было зарегистрировано 2376 преступлений в сфере компьютерной безопасности.

Компьютерные злоумышленники сегодня совсем не похожи на тинейджеров, получивших первоначальные знания с хакерских веб-сайтов, а представляют собой экспертов, получивших значительную подготовку в области информационных технологий и финансов. Кроме того, большинство из них входят в состав организованных преступных группировок. Сегодня доходы от компьютерных преступлений значительно превышают доходы от продажи оружия и наркотиков.

Угрозы в будущем не станут легче. Сегодня многие атаки представляют собой комбинацию различных техник. Кредитные учреждения, которые защищают себя только от известных угроз, всегда подвергаются риску, поскольку злоумышленники продолжают создавать новые методы атаки.

Пути решения проблемы киберугроз

Нормативно-правовая база

Для достижения цели обеспечения защиты от киберугроз необходимо сформулировать комплекс мер, направленных на выявление, пресечение и устранение результатов кибератак. Для достижения этих целей в первую очередь необходимо создать соответствующую нормативную базу. В настоящее время вступили в силу некоторые законы, нормативно-правовые акты и профессиональные стандарты, касающиеся информационной безопасности. Их необходимо своевременно редактировать, вносить соответствующие изменения и, самое главное, применять на практике - только так можно добиться максимальных результатов в борьбе с киберугрозами. Для экспертов, работающих в области информационной безопасности предприятия, необходимо ввести эти требования в нормативную базу, чтобы сотрудники могли выявлять и предотвращать новые виды кибератак.

Одним из действий, которое следует предпринять в отношении нормативно-правовой базы, является внесение в ГОСТ Р 50922-2006 “Защита информации. Основные термины и определения” терминов “кибербезопасность”, “киберугроза”, “кибератака”. Их не хватает для объяснения актуальной терминологии данной предметной области.

Другим шагом на пути к решению проблемы угроз кибербезопасности является внесение в Профстандарт: 06.033 “Специалист по защите информации в автоматизированных системах” в раздел “Группы занятий” деятельность, связанную с обеспечением безопасности от киберугроз, написать профессиональный стандарт и сформулировать требования для специалиста, который будет осуществлять данную деятельность на предприятиях. Также можно создать отдельный профессиональный стандарт, описывающий квалификационные требования для ряда различных специалистов, которые будут заниматься вопросами пресечения кибератак и устранения их последствий.

Системы анализа поведения пользователей и мониторинга финансовых операций

Множество сложных многоуровневых схем создается киберпреступниками для отмывания средств, они манипулируют счетами, компаниями, правовыми формами, валютами, а также юрисдикцией в течение нескольких дней. Определенные фирмы даже не успевают заподозрить, что на них было совершено нападение. Именно по этой

причине компании должны взять дело в свои руки, чтобы устранить риски и угрозы, и создать инфраструктуру сетевой безопасности для минимизации хакерских атак или атак на финансовую систему.

Также важно использовать системы, предназначенные для банков и других финансовых учреждений. Эти системы не только обеспечивают анализ поведения пользователей и мониторинг финансовых транзакций, но и отслеживают попытки отмыwania денег через различные компании.

Динамика развития киберпреступности показывает, что большинство угроз следует научиться отражать автоматически, чтобы сосредоточить внимание экспертов на выявлении новых и более сложных методов мошенничества. Злоумышленники со временем приобретают новые навыки и учатся обходить автоматизированные системы. Следует быть готовым к этому, используя специальные инструменты анализа данных, чтобы постепенно набираться опыта в мониторинге и сборе информации об угрозах.

Примеры решений по обнаружению новых видов угроз компании *Group-IB*

Компания *Group-IB Threat Hunting Framework* создала множество решений для обнаружения новых типов киберугроз.

Основной целью этого продукта является обнаружение ранее неизвестных угроз и атак, блокирование угроз и предоставление автоматизированных инструментов для обнаружения угроз внутри и за пределами защищенных зон компании, а также для расследования и реагирования на кибератаки.

Group-IB также создала технологию анализа файлов *Polygon*. Платформа нацелена на поиск и устранение угроз во вредоносном коде. Она использует поведенческий анализ электронных писем, файлов и связанного контента для обнаружения угроз, запускает вредоносный код в изолированной среде, приводит к его наиболее полному выполнению и позволяет получать индикаторы атак и идентифицировать выявленные угрозы.

Group-IB также представила защиту рабочих станций пользователей - *Huntpoint*. Он записывает полную хронологию событий на компьютерах сотрудников, делает их доступными в режиме реального времени и отслеживаемыми, обеспечивает обнаружение нестандартного поведения, блокирует вредоносные файлы, мгновенно изолирует атакованные хосты и собирает важные криминальные данные для дальнейшего исследования.

Служба *Hunbox* отвечает за автоматический анализ. Он дает полную картину того, что происходит внутри и за пределами сети, помогает находить угрозы и определяет поведение киберпреступников, которые специально нацелены на компании.

Список использованных источников:

1. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
2. Профстандарт: 06.033 Специалист по защите информации в автоматизированных системах
3. WORLD ECONOMIC FORUM - Digital Currency Governance Consortium White Paper Series COMPENDIUM REPORT NOVEMBER 2021https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf
4. Threat Zone 2020 — исследование трендов кибератак и их влияния на мировую экономику и бизнес.
https://icc.moscow/upload/iblock/2ef/Threat_Zone_Report_2020_RU.pdf
5. Отчет «Актуальные киберугрозы I квартал 2020 года» от 16.06.2020 компании Positive Technologies
6. Отчет «Актуальные киберугрозы II квартал 2021 года» от 30.08.2021 компании Positive Technologies

**Разработка аналитических индикаторов на основе дерева решений
для выявления признаков манипуляций в финансовой отчетности на
примере строительного сектора**

А.К. Завалишина
ассистент кафедры финансового менеджмента
НИЯУ МИФИ, Москва
E-mail: akzavalishina@gmail.com

Аннотация: В текущей экономической ситуации на фоне ужесточения требований международных организаций и заинтересованных лиц к достоверности и прозрачности финансовой отчетности возникает необходимость в определении риска совершения недобросовестных действий со стороны руководящего состава анализируемой организации. При достаточно большом количестве инструментария для выявления манипуляций в отчетности в научной среде нет единого мнения об эффективности применения существующих инструментов.

Ключевые слова: манипуляции в финансовой отчетности, финансовые индикаторы, экономическая безопасность, аналитические индикаторы.

**Development of analytical indicators based on a decision tree to identify
signs of manipulation in financial statements using the example of the
construction sector**

Abstract: In the current economic situation, against the background of the tightening of the requirements of international organizations and stakeholders for the reliability and transparency of financial statements, there is a need to determine the risk of fraud on the part of the management of the analyzed organization. With a sufficiently large number of tools for detecting manipulations in reporting, there is no consensus in the scientific community about the effectiveness of the use of existing tools.

Keywords: manipulations in financial statements, financial indicators, economic security, analytical indicators.

В текущем исследовании обоснован состав и рассчитаны значения аналитических коэффициентов, характеризующих финансово-хозяйственную деятельность организаций. Для этой цели была осуществлена выборка строительных организаций, в которую вошли

организации с видом деятельности по ОКВЭД 42.11 (Строительство автомобильных дорог и автомагистралей) и периодом выборки 2016 – 2020 гг., количество организаций 6162.

Аналитические процедуры по обоснованию и оценке типичных значений коэффициентов, рассчитанных по данным финансовой отчетности для добросовестных и недобросовестных организаций, представлены на рисунке 1.



Рисунок 1 – Последовательность аналитических процедур по обоснованию и оценке типичных значений аналитических коэффициентов

Выгрузка данных из информационной системы СПАРК-Интерфакс осуществлялась по критериям, представленным в таблице 1. Отчетным годом для сформированной выборки является 2020 год. Выборка включает 3 группы организаций:

- добросовестные поставщики, участвующие в государственных закупках; всего 3 919 организаций;
- недобросовестные поставщики, включенные в реестр недобросовестных поставщиков; всего 63 организации;
- организации, не участвующие в государственных закупках, всего 2 180 организаций.

Очистка базы данных была проведена по следующему алгоритму: были отсечены организации с пустыми ячейками значений абсолютного большинства показателей финансовой отчетности.

Система коэффициентов была сформирована на основе следующих положений:

- включение в систему показателей, позволяющих дать всестороннюю характеристику финансового состояния организации: ликвидность, финансовая устойчивость, оборачиваемость, рентабельность;
- включение коэффициентов, рассчитываемых на основе показателей с высокой вероятностью искажения;
- включение индикаторов динамики ключевых показателей отчетности, а именно выручки, чистой прибыли, прочих доходов и расходов, основных средств, запасов, финансовых вложений, денежных средств, дебиторской и кредиторской задолженностей, прочих внеоборотных и оборотных активов;
- включение в систему показателей, используемых в общепризнанных моделях выявления мошенничества (модель М. Бениша).

Таблица 1 – Характеристики тестовой выборки

Показатель	Характеристика
Отрасль	Строительство автомобильных дорог и автомагистралей
Код вида деятельности (ОКВЭД)	42.11 (Строительство автомобильных дорог и автомагистралей) основной в отчетном году
Регион	Любой
Форма собственности	Любая
Организационно-правовая форма	Любая
Возраст, лет	От 0,5
Предмет поставки	Любой
Реестры СПАРКа	Без фильтра
Выручка, руб.	От 1 000 000 в отчетном году
Периоды выборки	2016, 2017, 2018, 2019, 2020

Коэффициенты были рассчитаны для совокупностей добросовестных организаций и недобросовестных поставщиков строительной отрасли, в частности по виду ОКВЭД 42.11 «Строительство автомобильных дорог и автомагистралей».

Полученные данные были проанализированы с помощью описательной статистики, такой как: среднее значение, медиана. Следует отметить, что 2020 год выделяется из общей тенденции характеристик деятельности организаций в отрицательную сторону, что обусловлено коронавирусной инфекцией.

По результатам расчетов, следует отметить, что почти все показатели, входящие в модель М. Бениша, показывают существенные отклонения значений недобросовестных поставщиков от значений добросовестных организаций. Таким образом, подтверждается эффективность данных

индикаторов в выявлении манипуляций в финансовой отчетности. Однако учитывая специфичность расчетов показателей и необходимость их сравнения между собой, в дальнейших расчетах они будут участвовать частично.

Помимо этого, показатели динамики статей бухгалтерского баланса и отчета о финансовых результатах, также вошли в состав коэффициентов, свидетельствующих об отклонениях средних значений недобросовестных поставщиков от значений добросовестных организаций.

Из протестированной системы были изъяты следующие группы показателей:

1. Коэффициенты ликвидности, коэффициенты оборачиваемости дебиторской и кредиторской задолженности, поскольку они и в числителе, и в знаменателе включают статьи финансовой отчетности с высокой степенью вероятности искажения (выручка, кредиторская и дебиторская задолженности);
2. Показатели, использующие данные из отчета о движении денежных средств, поскольку в исследуемой совокупности организаций по этому отчету доля пропусков превышает 50%;
3. Коэффициенты, для расчета которых необходима амортизация, в частности коэффициенты долга, поскольку данные об амортизации по организациям могут не раскрываться организациями в финансовой отчетности.

В связи с этим, предлагается новый подход к выявлению недобросовестных организаций. Особенность данного подхода заключается в том, чтобы сопоставлять между собой некачественные показатели финансовой отчетности с качественными. Именно такой алгоритм построения аналитических показателей обеспечивает выявление недобросовестных организаций, поскольку они существенно отличаются от показателей добросовестных организаций.

В результате для разработки комплекса аналитических процедур с помощью использования дерева принятия решений выбраны следующие показатели:

1. Соотношение некачественных активов и численности персонала. При ее отклонении (превышении) относительно медианного уровня вероятность манипуляций увеличивается, что связано с фиктивной выручкой организаций манипуляторов.

$$R_{LA} = \frac{LA}{S}$$

где R_{LA} – low-rank ratio (соотношение некачественных активов к численности персонала), тыс. руб./чел.);

LA – low-rank assets (некачественные активы, тыс. руб.);

S – stuff (среднесписочная численность персонала, чел).

2. Доля некачественных активов. При ее отклонении (превышении) относительно медианного уровня вероятность манипуляций увеличивается, что связано с наличием у организаций-манипуляторов производственных активов (нематериальных активов, финансовых вложений, дебиторской задолженности, прочих оборотных активов) низкого качества.

$$f_{LA} = \frac{LA}{A}$$

где f_{LA} – fraction low-rank assets (доля некачественных активов);

A – assets (активы, тыс. руб.).

3. Темп прироста некачественных активов. При его отклонении (превышении) относительно медианного уровня вероятность манипуляций увеличивается.

$$AR_{LA} = \left(\frac{LA_1}{LA_0} - 1 \right) \times 100\%$$

где AR_{LA} – accession rate low-rank assets (темп прироста некачественных активов);

LA_1 – low-rank assets current period (некачественные активы отчетного периода, тыс. руб.);

LA_0 – low-rank assets previous period (некачественные активы предыдущего периода, тыс. руб.).

4. Темп прироста некачественных пассивов. При его отклонении (превышении) относительно медианного уровня вероятность манипуляций увеличивается.

$$AR_{LL} = \left(\frac{LL_1}{LL_0} - 1 \right) \times 100\%$$

где AR_{LL} – accession rate low-rank liabilities, (темп прироста некачественных пассивов);

LL_1 – low-rank assets current period (некачественные активы отчетного периода, тыс. руб.);

LL_0 – low-rank assets previous period (некачественные активы предыдущего периода, тыс. руб.).

Предложенные показатели и их интервальные значения (ограничения) были протестированы на выборке, характеристики которой представлены в таблице 1, результаты расчетов представлены в таблице 2.

В результате тестирования выборки задача была решена с помощью дерева принятия решений (рисунок 2). Деревья регрессии и классификации, известные также под общим названием как деревья

решений (Decision Tree – DT), представляют собой структуры данных, позволяющие интерпретировать шаблоны данных с целью их распознавания. Деревья решений организованы в виде иерархической структуры, состоящей из узлов принятия решений по оценке значений определенных переменных для прогнозирования результирующего значения.

Следует отметить, что эксперты в области больших данных, в частности, Эрик Сигел [119] отмечает простоту, точность алгоритма дерева решений в прогнозной аналитике.

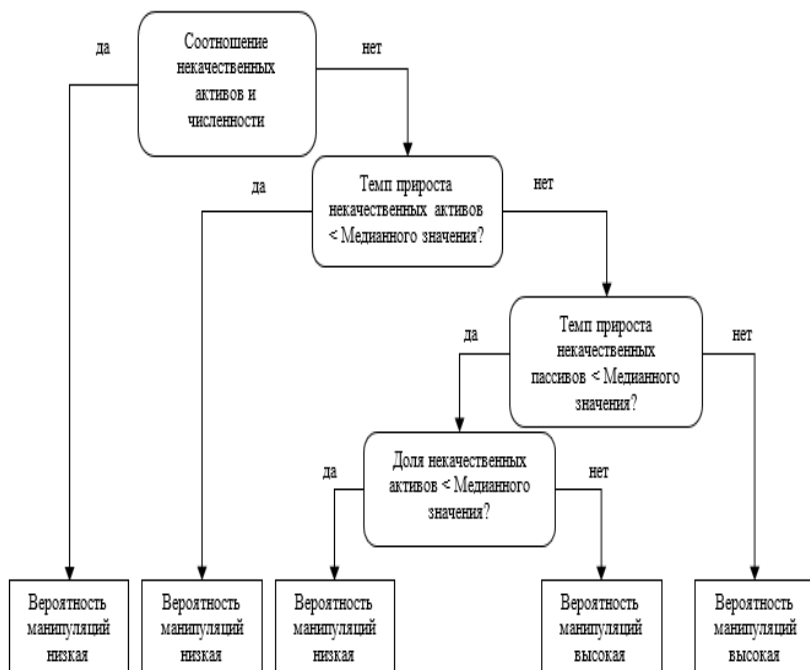


Рисунок 2 – Дерево принятия решений для выявления признаков манипуляций

С помощью программы RStudio в качестве корневого узла определен показатель «соотношение некачественных активов к численности персонала» и его медианное значение 2,2 млн руб./чел.

Следующие узлы дерева – это темп прироста некачественных активов с медианным значением выше 8,49%, темп прироста некачественных пассивов с медианным значением выше 11,04%, доля некачественных активов с медианным значением выше 0,67.

Таблица 2 – Индикаторы, позволяющие выявлять признаки манипуляций в финансовой отчетности строительной организации

Показатель	Добросовестные организации	Недобросовестные организации	Отклонения значений недобросовестных организаций от значений добросовестных, %
Соотношение некачественных активов и численности персонала, тыс. руб. / чел.	1 755	2 681	52,80
Доля некачественных активов в активах	0,48	0,86	79,17
Темп прироста некачественных активов, %	4,42	12,57	184,39
Темп прироста некачественных пассивов, %	5,99	16,10	62,80

Таким образом, соблюдении четырех критериев дерева принятия решений, вероятность манипуляций в финансовой отчетности исследуемой организации признается высокой и далее требует более детального углубленного исследования.

Список использованных источников:

1. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : Федеральный закон от 07.08.2001 г. № 115-ФЗ (последняя редакция) // СПС «Консультант Плюс». – URL: <http://www.consultant.ru/>
2. Волошин Д.А. Искажение корпоративной отчетности: выявление, противодействие и профилактика: Монография / Д.А. Волошин – Москва : ИЦ РИОР, НИЦ ИНФРА-М, 2016. – 156 с.
3. Когденко В.Г. Управление финансами и рисками: Монография. / В.Г. Когденко. – Москва : ЮНИТИ-ДАНА, 2019 г. – 527 с.
4. Система проверки контрагентов «СПАРК» [Электронный ресурс] URL: <http://www.spark-interfax.ru;>
5. Beneish M. The Detection of Earning Manipulation. Financial Analysts Journal. – 1999. – № 55(5). – pp. 24–36.
6. Hugh Grove, Mac Clouse Due Diligence Procedures and Principles for Financial Analysis and Corporate Governance // Journal of Corporate Finance Research / Корпоративные финансы 2018. – Vol. 15– № 1. – P. 107–114.

Разработка финансовой структуры торговой организации (в рамках разработки системы бюджетирования)

А.Б. Романенко

студентка 5 курса НИЯУ МИФИ, Москва

E-mail: anastasiaromanenko@yandex.ru

И.П. Комиссарова

доктор экономических наук, профессор кафедры бухгалтерского учета и аудита НИЯУ МИФИ

E-mail: ipkomissarova@mephi.ru

Аннотация: В данной статье рассматривается формирование финансовой структуры торговой организации в рамках разработки системы бюджетирования.

Ключевые слова: бюджетирование, финансовая структура, торговая организация, методики бюджетирования.

Development of the financial structure of a trade organization (as part of the development of a budgeting system)

Abstract: The article is about the formation of the financial structure of a trade organization in the framework of the development of a budgeting system.

Keywords: budgeting, financial structure, trade organization, budgeting techniques.

1. Описание компании

Компания «Принтер» является участником рынка полиграфии с начала 2000-х годов. Компания ведет свою деятельность в сфере производства полиграфической продукции и продажи оборудования. Миссия ООО «Принтер» - непрерывное совершенствование методов и технологий для производства рекламной продукции.

Своих целей организация достигает благодаря компетентным сотрудникам, помощи и поддержки каждого клиента, высоким требованиям к качеству оборудования и сопутствующих услуг, а также многолетнему опыту успешной работы.

Организация занимается не только закупкой и продажей оборудования, но и имеет собственные производственные мощности. В качестве НМА используется ряд товарных знаков.

В сентябре 2021 года руководством компании в рамках концепции непрерывного совершенствования бизнеса было принято решение о постановке системы бюджетирования как элемента управления.

В качестве консультантов по проекту была привлечена компания ООО «А-УНИВЕРСАЛ КОНСАЛТИНГ». В ходе согласования проекта консультантом были переданы Заказчику ряд методик и шаблонов:

- 1) Методика подготовки «Положения о бюджетном планировании»;
- 2) Методика подготовки бюджета продаж;
- 3) Методика разработки стандарта «Положение о финансовой структуре»;
- 4) Методика разработки стандарта «Классификатор Затрат».

В качестве первого шага проекта был составлен регламент «Устав проекта», составной частью которого стал «План постановки системы бюджетирования».

Кроме того, в качестве ключевых этапов проекта были обозначены следующие этапы разработки:

1. Анализ структуры доходов и расходов, выбор перечня операционных бюджетов;
2. Определение финансовой структуры компании;
3. Определение технологии бюджетирования;
4. Определение форматов основных финансовых бюджетов;
5. Регламент бюджетирования;
6. Организация бюджетного процесса.

Среднесписочная численность компании составляет 16 сотрудников. Организационная структура организации представлена на рисунке 1.



Рисунок 1 – Организационная структура

Представленная организационная структура является отражением реализуемых в компании бизнес-процессов. При этом, в целях реализации процесса бюджетирования были выделены следующие основные бизнес-процессы:

- 1) Общее управление;
- 2) Процесс «Закупка»;
- 3) Процесс «Продажа»;
- 4) Процесс «Склад»;
- 5) Процесс «Техническая поддержка».

2. Подготовка реализации процесса бюджетирования

Частью структуры реализации бюджетного процесса является «Положение о бюджетировании».

«Положение о бюджетировании» – это основной документ, в котором отражаются базовые принципы, сфера применения, процессы разработки, утверждения, редакции и контроль исполнения бюджетов организации. Кроме того, в документе приводится описание бюджетной структуры, включая операционные бюджеты, финансовые бюджеты и бюджеты центров финансовой ответственности (ЦФО). Таким образом «Положение о бюджетировании» раскрывает схему бюджетной организации и регламенты бюджетирования.

Структура бюджетного планирования представляет собой следующее:

1. Цели и задачи ООО «Принтер»;
2. Порядок формирования бюджетов;
3. Состав участников бюджетного процесса:
 - 3.1 Генеральный директор;
 - 3.2 Главный бухгалтер;
 - 3.3 Финансовый директор;
 - 3.4 Начальник отдела закупки;
 - 3.5 Начальник службы персонала;
 - 3.6 Начальник отдела маркетинга;
 - 3.7 Начальник отдела продаж;
 - 3.8 Начальник службы технической поддержки;
 - 3.9 Начальник склада.
4. Функции и ответственность лиц, принимающих участие в бюджетном процессе;
5. Делегирование права участников бюджетного процесса;
 - 5.1 Перечень документов бюджета;
 - 5.2 Порядок проверки заполнения, корректировки и утверждения бюджетной документации.
6. Порядок и методика пересмотра и корректировки бюджетов при значительных отклонениях плана от факта;
7. Анализ исполнения бюджета;
8. Порядок утверждения отчета об исполнении бюджета.

Для составления бюджета организации необходимо определить цели, для достижения которых проводится процедура бюджетирования.

Для начала формируются принципы разделения ответственности между центрами ответственности, а также составляются формы планов и годовой отчетности.

Определяется срок, на который будут составлены финансовые бюджеты. Оптимальным является помесечный бюджет, но некоторые компании определяют отчетным периодом квартал.

Составляются сроки разработки, согласования, утверждения, консолидации и анализа бюджетов всех имеющихся уровней, назначить ответственных.

В заключительный этап входит контроль исполнения и непосредственная корректировка составленных бюджетов.

Методику подготовки «Положения о бюджетном планировании» можно описать следующим образом:

- Общие правила бюджетной деятельности

Необходимо определить цель внедрения бюджетирования, целевые показатели, на основе которых будут формироваться доходные и расходные статьи бюджетов. Это необходимо для того, чтобы установить правила формирования отчетов о работе экономического субъекта, порядок анализа и корректировки бюджетов.

- Описание центров ответственности (ЦО)

Необходимо описать принципы разделения ЦО на ЦФО, ЦФУ и МВЗ, определить формы планов и годовой отчетности, которые представляет каждый центр ответственности, а также правила консолидации этой документации в общефирменную отчетность.

- Определение бюджетного периода

Бюджетный период – это тот срок, на который составляются основные финансовые бюджеты. Из-за того, что в процессе сбора и представления отчетности возникают некоторые сложности, большинство отечественных компаний в качестве бюджетного периода выбирают квартал. Как показывает опыт и практика, оптимальным периодом является помесечный бюджет.

- Составление бюджетного графика

В регламенте необходимо отразить сроки разработки, согласования, утверждения, консолидации и анализа бюджетов всех уровней. Сроки должны быть достаточными для формирования бюджетной документации и утверждения их на бюджетном комитете экономического субъекта, назначить ответственных.

- Контроль исполнения и правила корректировки бюджетов

Необходимо утвердить методики и сроки проведения анализа бюджета, регламентировать порядок корректировки бюджетных документов и определить перечень тех сотрудников, которые отвечают за анализ.

Методика может содержать правила анализа отклонений фактических показателей от плановых, анализа структуры производства и динамики реализации продукции.

Учитывая специфику деятельности торговой организации в настоящей работе пристальное внимание помимо основных финансовых бюджетов уделено бюджетам продаж и коммерческих (административных) расходов.

В структуру бюджета продаж входят следующие показатели:

- 1) Объем продаж;
- 2) Средневзвешенная цена;
- 3) Выручка от реализации;
- 4) Оборачиваемость товара;
- 5) Маржинальная прибыль;
- 6) Маржинальная рентабельность;
- 7) Доля товаров ниже заданного уровня рентабельности и прибыльности;
- 8) Коммерческая прибыль;
- 9) Дебиторская задолженность на конец периода;
- 10) Оборачиваемость дебиторской задолженности;
- 11) Поступление денежных средств.

От корректности планирования бюджета продаж и достоверности его показателей зависит качество прогнозируемых показателей взаимосвязанных с ним бюджетов. Чтобы обеспечить наибольшую корректность бюджета продаж, организации следует соблюдать алгоритм его формирования: прогноз количества реализации, прогноз цены реализации.

3. Бизнес-модель ООО «Принтер»

Безусловно, планирование любого вида бюджета необходимо производить на основании бизнес-модели предприятия (см. рис.2).

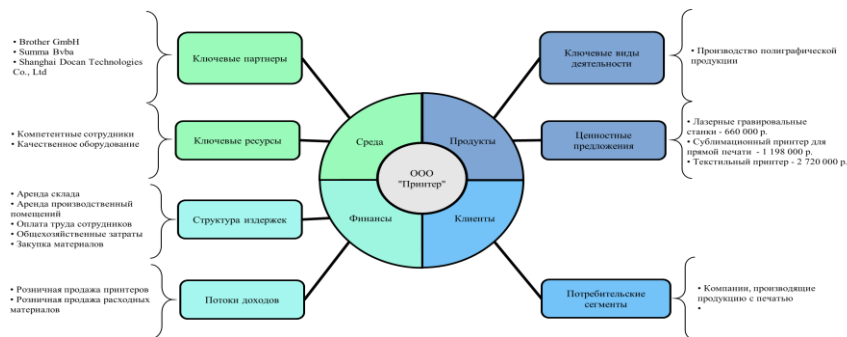


Рисунок 2 – Бизнес-модель организации

ОО «Принтер» занимается производством и продажей печатных устройств, а также продажей полиграфической продукции. Основным потребительским сегментом компании являются организации, производящие продукцию с печатью, рекламные агентства, размещающие баннеры, вывески и плакаты. Основными доходными потоками являются розничная продажа принтеров и расходных материалов. Издержками компании являются аренда склада и производственных помещений, оплата труда сотрудников, общехозяйственные затраты, закупка материалов. В качестве своих ключевых ресурсов компания выделяет компетенции сотрудников и высокое качество оборудования как продаваемого, так и того, на котором происходит производство продукции для продажи.

Brother GmbH, Summa Bvba, Shanghai Docan Technologies Co., Ltd – являются ключевыми партнерами ООО «Принтер».

4. Составление бюджетов

При составлении бюджетов любой организации необходимо проанализировать затраты конкретной компании. Относительно ООО «Принтер» можно выделить следующие затраты:

- Материалы;
- Услуги сторонних организаций;
- Затраты на оплату труда;
- Налоговые платежи;
- Амортизация;
- ОС;
- НМА;
- Погашение кредитов и займов;
- Прочие платежи.

Каждый вид затрат, перечисленный выше можно, в свою очередь, классифицировать более подробно (см. табл. 1).

Таблица 1 – Классификация затрат

Наименование статьи затрат	Раздел статьи затрат	Детализация статей
Материалы	В интересах производства	Покупные комплектующие изделия
		Спецодежда
		Запчасти для ремонта
		Текущие расходы на хозяйственные нужды
		Копировальные работы для проектной деятельности
		Потери от брака

Наименование статьи затрат	Раздел статьи затрат	Детализация статей
	Для целей офиса	Прочие производственные расходы
		Техническая литература и подписные издания
		Канцтовары
		Копировальные работы
		Транспортные расходы
		Прочие офисные расходы
Услуги сторонних организаций	Производственные заказы	Соисполнители
		Производственные заказы (печатные платы)
		Авансы
	Услуги связи	Международные и междугородние переговоры, интернет
		Сотовая связь
		Спецсвязь
	Услуги охраны	Охрана территории и помещений п/п
		Охранная сигнализация
		Пожарная безопасность
		Прочие выплаты
	Аренда	Аренда земли и помещений
		Аренда оборудования
		Прочая аренда
	Техобслуживание	Обслуживание оргтехники
		Обслуживание станков и оборудования
		Обслуживание прочего технического оснащения п/п
		Авансы
	Услуги банков	Инкассация
	Коммунальные услуги	Газ
		Вода
		Электроэнергия
		Дератизация
		Вывоз ТБО
		Работы по водоотведению

Наименование статьи затрат	Раздел статьи затрат	Детализация статей
		Прочие
Затраты на оплату труда	ФОТ к выдаче	
Налоговые платежи	Платежи в бюджет	Налог на прибыль
		Налог на имущество
		Налог на землю
		Налог на загрязнение окружающей среды
		Транспортный налог
		НДС
		НДФЛ
	Отчисления в фонды	ПФР
		ФОМС
		ФСС
Амортизация	Износ ОС	
	Износ НМА	
ОС	ОС	Станки и инструменты
		Оргтехника и оборудование
		Мебель
НМА	Программное обеспечение	IC Предприятие
		Консультант +
		Программное обеспечение для проектной деятельности
	Документы подтверждающие правообладание	Сертификаты
Погашение кредитов и займов	Платежи по кредитам и займам	
	Проценты по кредитам и займам	
Прочие платежи	Командировочные расходы	
	Представительские расходы	
	Страхование	
	Подготовка кадров и аттестация рабочих мест	
	Пени и штрафы	
	Погашение задолженности по платежам	
	Прочие расходы	

Уже исходя из вероятных затрат можно составить проекты бюджета движения денежных средств, характеризующего притоки и оттоки денежных средств по текущей, инвестиционной и финансовой деятельности, и бюджета доходов и расходов, в котором отражены расходы и доходы организации.

Ни одно крупное предприятие не может обойтись без оптимизации показателей деятельности (производительности труда, торговой наценки, объемов продаж, активов предприятия, прибыли). Руководителям жизненно важно понимать, что относится к этим ключевым показателям. Важно знать, какие оптимальные и минимально допустимые значения на данном этапе деятельности компании, какие ресурсы и когда понадобятся предприятию, чтобы предвидеть неблагоприятные ситуации, анализировать и упреждать возможные риски, добиваться эффективного использования привлеченных, заемных средств. Бюджетирование — система комплексного, «сквозного» планирования, анализа и контроля деятельности предприятия, поставленная на регулярную основу

В целом бюджетный процесс можно разделить на 4 крупных блока:

1. Аналитический блок
 - Методология сводного бюджета;
 - Методики по отдельным бюджетам, входящим в сводный бюджет;
 - Квалифицированный персонал.
2. Учетный блок
 - Бухгалтерский учет;
 - Управленческий учет;
 - Маркетинговые исследования.
3. Организационный блок
 - Организационно-финансовая структура со всеми подразделениями;
 - Регламенты взаимодействия;
 - Система ответственности и мотивации.
4. Программно-технический блок
 - Технические средства;
 - Программное обеспечение.

Торговые организации ведут два вида бюджета: операционный и финансовый. Для ООО «Принтер» были выделены следующие бюджеты:

- 1) операционный бюджет:
 - Бюджет продаж;
 - Бюджет на закупки;
 - Бюджет затрат на оплату труда;
 - Бюджет административных затрат и расходов на сбыт.
- 2) финансовый бюджет:
 - Бюджет доходов и расходов;
 - Бюджет по балансовому листу;
 - Бюджет движения денежных средств.

Постановка системы управленческого учета и бюджетирования необходима для упорядочения процессов управления, создания стройной системы планирования и контроля. Фундаментом этой системы является финансовая структура.

Финансовая структура – это система центров финансовой ответственности, выстроенная по иерархии. Основная функция финансовой структуры – это определение порядка формирования финансовых результатов и распределение ответственности за достижение общего результата компании.

Наличие финансовой структуры позволяет руководству экономического субъекта видеть зоны ответственности каждого сотрудника, оценивать, контролировать и координировать деятельность подразделений, помогает разрабатывать действенную систему мотивации сотрудников.

Типы ЦФО:

1. Центры инвестиций — верхний уровень финансовой структуры. Они управляют не только оборотным капиталом, но и внеоборотными активами (основными средствами), в том числе инвестициями.

2. Центры прибыли. Величина прибыли — доходы и затраты не одного направления, а всего предприятия в целом. Если речь идет об одном предприятии, то на этих центрах система финансовой ответственности заканчивается.

3. Центры маржинального дохода. Отвечают за эффективность деятельности, контролируя доходную и расходную часть своего направления в плане покрытия прямых расходов, связанных с деятельностью направления (бизнес-направления). Это обособленная производственная единица, у которой есть и затраты, и себестоимость. В принципе, коммерческий директор, под началом которого находится производство, является руководителем центра маржинального дохода. Производственник сам по себе — это кост-центр, который может входить в маржинальный центр. То же касается и отдела продаж.

4. Центры дохода. Отвечают за доходную часть бюджета: реализацию готовой продукции, товаров и услуг, то есть выручку (отдел продаж, оптовая база, сеть). Например, в отделах продаж не обращают внимание на себестоимость товара, а работают в рамках данных им регламентов. И руководителя подразделения не интересует, как сформировалась стоимость товара, его себестоимость, маржинальность бизнеса, какой суммой можно поступить. Его задача — объем доходов и скидок.

5. Центры затрат. Они только потребляют ресурсы. Это производственные подразделения и функциональные службы (цех, склад,

бухгалтерия, реклама и маркетинг, охрана). Являются нижним уровнем ЦФО, который чаще всего фигурирует в явном виде в операционной деятельности (накладные расходы и общехозяйственные результаты).

Таблица 2 – Построение финансовой структуры организации

Подразделение	Функции	Показатель деятельности	Управлен и е доходами	Управлен не затратами	Тип ЦФО
1	2	3	4	5	6
Административны й отдел	Обеспечение жизнедеятельности компании	Общие затраты	НЕТ	ДА	ЦЗ
Финансовая служба	Управление финансами и учет	Чистая прибыль	ДА	ДА	ЦЗ
Служба персонала	Управление персоналом	Затраты Списочная численность	ДА	ДА	ЦЗ
Отдел маркетинга	Управление продажами и развитием	Маржинальная прибыль	НЕТ	ДА	ЦЗ
Отдел закупок	Процесс «Закупки»	Затраты	НЕТ	ДА	ЦЗ
Отдел продаж	Процесс «Продажа»	Доход	ДА	ДА	ЦП
Склад	Процесс «Складское хранение»	Затраты	НЕТ	ДА	ЦЗ
Служба технической поддержки	Доход	Доход	ДА	ДА	ЦД

Анализируя организационную структуру организации, была сформирована финансовая структура.

Были выделены следующие типы ЦФО:

1. Центр затрат:

- Административный отдел;
- Финансовая служба;
- Служба персонала;
- Отдел маркетинга;
- Отдел закупок;
- Склад.

2. Центр прибыли:

- Отдел продаж.

3. Центр дохода:

- Служба технической поддержки.

На наш взгляд, разработанная финансовая структура станет полноценной составляющей системы бюджетирования ООО «Принтер».

Список использованных источников:

1. Как построить финансовую структуру // Корпоративный менеджмент URL: https://www.cfin.ru/management/finance/financial_structure_building.shtml
2. Положение о бюджетировании // Финансовый директор URL: <https://www.fd.ru/articles/36624-polojenie-o-byudjetirovanii>
3. Положение о финансовой структуре // Business Studio URL: https://www.businessstudio.ru/articles/article/polozhenie_o_finansovoy_strukture/
4. Бюджет продаж // Budgeting Technology URL: https://budget-tech.ru/budget_sales.html
5. Положение о бюджетировании // Aktiv URL: <https://finacademy.net/materials/article/polozhenie-o-byudzhetrovanii-na-predpriyatii>
6. Классификатор затрат // Wise Advice IT URL: <https://wiseadvice-it.ru/o-kompanii/blog/articles/klassifikaciya-zatrat/>
7. Анализ бюджетирования на примере: как провести оценку системы и что влияет на ее эффективность // Financial academy URL: <https://finacademy.net/materials/article/analiz-byudzhetrovaniya>
8. Александр Карпов Бюджетирование как инструмент управления. 6 изд. М.: 2021.

Риски использования анонимных виртуальных активов и виртуальных валют для легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма

С.А. Бойко

студент 4 курса НИЯУ МИФИ, Москва

E-mail: sophia.boiko@yandex.ru

И.В. Кольца

студент 4 курса НИЯУ МИФИ, Москва

E-mail: koltsaiv@yandex.ru

М.А. Степаненкова

студент 4 курса НИЯУ МИФИ, Москва

E-mail: stepanenkovam@gmail.com

В.А. Корчинская

преподаватель кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: viktoriya_shvarc@mail.ru

Аннотация: Сфера виртуальных активов и виртуальных валют (ВАВВ) быстро развивается, создавая новые возможности как для законопослушных граждан, так и для преступников. Свойства, присущие ВАВВ, обеспеченные инновационными технологиями, делают их привлекательным инструментом для субъектов, занимающихся незаконной деятельностью. Целью исследования является анализ рынка криптовалют и возможностей их использования в незаконной деятельности.

Ключевые слова: виртуальные активы и виртуальные валюты, легализация денежных средств, финансирование терроризма.

Risks of using anonymous virtual assets and virtual currencies for the legalization (laundering) of proceeds from crime and the financing of terrorism

Abstract: The sphere of virtual assets and virtual currencies (VAVC) is rapidly developing, creating new opportunities for both law-abiding citizens and criminals. The properties inherent in VAVC, provided with innovative technologies, make them an attractive tool for entities engaged in illegal

activities. The purpose of the study is to analyze the cryptocurrency market and the possibilities of their use in illegal activities.

Keywords: virtual assets and virtual currencies, money laundering, terrorist financing.

Введение. Появление новых технологий, продуктов и связанных с ними услуг за последнее десятилетие стало одним из основных изменений в мировой финансовой системе. Эти новые технологии, продукты и связанные с ними услуги обладают потенциалом для стимулирования финансовых инноваций, повышения эффективности и расширения доступа к финансовым услугам, но они также создают новые возможности для преступников и террористов отмывать свои доходы или финансировать свою незаконную деятельность. В соответствии с подходом, основанным на оценке рисков, который лежит в основе стандартов Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), понимание и реагирование на выявленные риски отмывания денег и финансирования терроризма (ОД/ФТ) лежат в основе деятельности ФАТФ и ее государств-членов.

Виртуальные активы и виртуальные валюты, которые включают криптовалюты, такие как биткойн (Bitcoin), а также ряд других методов передачи цифровых ценностей, являются инновационными технологиями, которые позволяют осуществлять цифровые транзакции и предоставлять финансовые продукты и услуги в новых онлайн-сетях, средах и на рынках.

Как и другие финансовые продукты и услуги, виртуальные валюты обладают функциями, которые представляют риски для содействия преступности, включая ОД/ ФТ. Безграничный, одноранговый (P2P) характер некоторых виртуальных активов открывает перед террористическими субъектами перспективы перевода средств за пределы регулируемого сектора и за пределы компетенции органов по противодействию отмыванию доходов и финансированию терроризма (ПОД / ФТ). Виртуальные активы и виртуальные валюты также имеют различные уровни анонимности и псевдоанонимности, что может способствовать сокрытию незаконной деятельности.

Поскольку в последние годы виртуальные валюты, и, в частности, криптовалюты, такие как биткойн, набирают всю большую популярность, а их капитализация сравнима или превышает капитализацию крупнейших в мире компаний, проблема использования виртуальных активов и виртуальных валют для совершения незаконной деятельности становится особо актуальной.

Проблемы, возникающие в результате использования виртуальных активов и виртуальных валют, поднимались в работах исследователей

Группы разработки финансовых мер с отмытием денег ФАТФ, Всемирного банка, Международной организации уголовной полиции Интерпол, а также в работах Г.Ю. Негляда, П.М. Шуста, Д.Л. Достова, К.В. Гурьянова, Я.С. Шатило.

Основная часть. Не существует единого определения таких терминов как «виртуальные активы», «виртуальные валюты», «поставщики услуг виртуальных активов». Среди специалистов в сфере экономической теории ведутся дискуссии в отношении данных терминов. Приведем определение этих терминов, данные в нормативных документах Группы разработки финансовых мер борьбы с отмытием денег (ФАТФ) [5].

Виртуальный актив (ВА) — это цифровое представление стоимости, которое может быть продано или передано в цифровом виде и может использоваться для оплаты или инвестиционных целей. Виртуальные активы не включают цифровые представления фиатных валют, ценных бумаг и других финансовых активов.

Поставщик услуг виртуальных активов (ПУВА) — физической или юридическое лицо, которое осуществляет одну или несколько перечисленных ниже видов деятельности или операций для или от имени другого физического или юридического лица:

- обмен между виртуальными активами и фиатными валютами;
- обмен между одной или несколькими формами виртуальных активов;
- передача виртуальных активов;
- хранение и/или администрирование виртуальных активов или инструментов, позволяющих распоряжаться виртуальными активами;
- участие и предоставление финансовых услуг, связанных эмиссией и/или продажей виртуального актива.

Виртуальная валюта (ВВ) - цифровое представление стоимости, которое не эмитировано или не гарантировано центральным банком или государственным органом, не обязательно привязано к официально установленной валюте и не имеет юридического статуса валюты или денег, но принимается физическими или юридическими лицами в качестве средства обмена и может передаваться, храниться и продаваться в электронном виде.

В зависимости от архитектуры сети, в которой распространяются виртуальные активы и виртуальные валюты (BABB), их принято делить на децентрализованные и централизованные.

Децентрализованные BABB не требуют наличия центрального эмитента или органа власти для согласования действительности транзакций в сети или для создания и выпуска новых единиц. Термин "децентрализованный виртуальные валюты", как правило, является

синонимом популярного термина "криптовалюта", первоначально использовавшегося для обозначения криптовалюты Bitcoin.

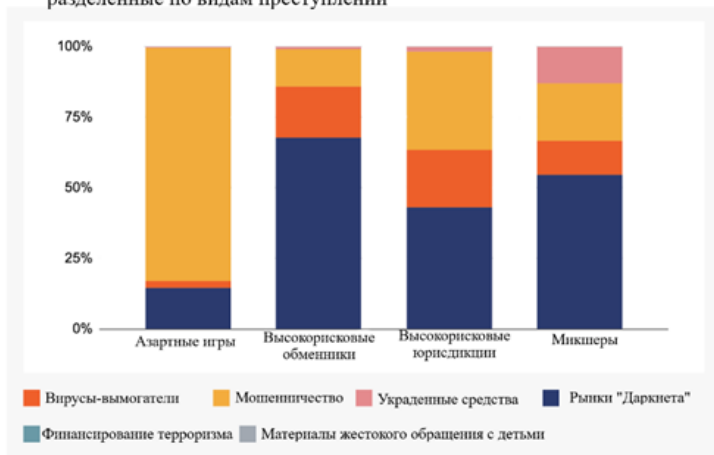
Криптовалюты — это сети передачи ценностей P2P с открытым исходным кодом, которые полагаются на криптографическое доказательство для проверки транзакций и обеспечения консенсуса в отношении сетевой активности без опоры на доверенную третью сторону, такую как банк или другое финансовое учреждение. Криптовалюты функционируют как форма "цифровых денег", позволяя P2P, прямые переводы между двумя сторонами, подобно тому, как два человека могут обмениваться физической фиатной валютой, но без тех же ограничений пространства и расстояния.

Отмывание денег является частью любого преступления, связанного с виртуальными активами, и, в частности, с криптовалютами. Основная цель киберпреступников, которые крадут криптовалюту или принимают ее в качестве оплаты незаконных товаров, заключается в том, чтобы скрыть источник своих средств и конвертировать криптовалюту в наличные деньги, чтобы ее можно было потратить или хранить в банке.

Благодаря работе правоохранительных органов и специалистов по соблюдению требований по всему миру, преступники не могут просто отправить свою незаконно полученную криптовалюту на биржу и обналичить ее, как это сделал бы обычный пользователь. Вместо этого они полагаются на удивительно небольшую группу поставщиков услуг для обмена своих виртуальных активов. Некоторые из этих поставщиков специализируются на услугах по отмыванию денег, в то время как другие являются просто крупными компаниями по предоставлению криптовалютных и денежных услуг со слабым уровнем соответствия требованиям законодательства в области ПОД/ФТ.

Также можно заметить, что значительный объем перемещается с незаконных адресов на высокорискованных поставщиков услуг, таких как высоко рисковые биржи, платформы для азартных игр, микшеры и сервисы со штаб-квартирами в юрисдикциях с высоким уровнем риска. Интересные тенденции возникают, когда мы смотрим на конкретные рискованные сервисы, получающие средства от различных видов преступлений, основанных на криптовалютах (рис. 9) [6].

Незаконные средства, полученные рискованными поставщиками услуг, разделенные по видам преступлений



Включенные валюты: BCH, BTC, ETH, LTC, OMG, PAX, USDC, USDT

Рисунок 1 – Незаконные средства, полученные рискованными поставщиками услуг, разделенные по видам преступлений

Наиболее популярные категории рискованных услуг для отмыwania денег одинаковы для каждой категории преступлений, за исключением мошенничества. Мошенники гораздо чаще, чем другие киберпреступники, переводят средства на игровые платформы и в сервисы, расположенные в юрисдикциях с высоким уровнем риска.

Мы также можем увидеть интересные тенденции, когда смотрим на отмыwanie в зависимости от географического положения (рис. 2) [14].

Географическое место назначения средств, отправленных незаконными поставщиками услуг (2020).



Включенные валюты: BAT, BCH, BTC, ETH, LTC, MKR, OMG, PAX, TUSD, USDC, USDT

Рисунок 2 – Географическое место назначения средств, отправленных незаконными поставщиками услуг (2020)

Следующие страны получают наибольший объем криптовалюты с незаконных адресов, основываясь на разбиение географических местоположений пользователей незаконных услуг, поставщики которых получающих эти средства: США, Россия, Китай, Южная Африка, Великобритания, Украина.

Незаконные средства, полученные пятью странами, наиболее популярными с точки зрения незаконного использования криптовалют, разделенные по видам преступлений.

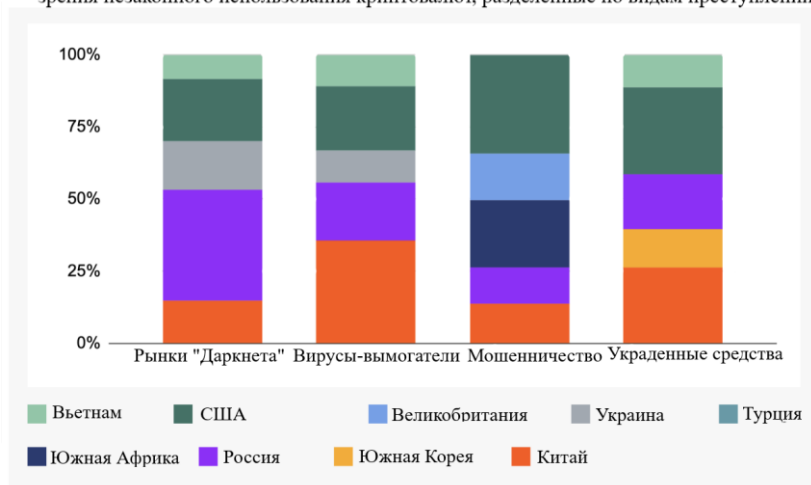


Рисунок 3 – Незаконные средства, полученные пятью странами, наиболее популярными с точки зрения незаконного использования криптовалют, разделенные по видам преступлений

Однако закономерности проявляются сильнее, когда мы анализируем географическое местоположение средств по категориям преступлений (рис. 3). Первая тенденция, которая сильно выделяется, — это получение Россией непропорционально большой доли средств на рынке «Даркнет», что в основном связано с Hydra. Hydra является крупнейшим в мире рынком даркнета по выручке и обслуживает исключительно Россию и другие русскоязычные страны Восточной Европы. Китай также выделяется тем, что получает непропорционально большую долю средств, отправленных с адресов, связанных с украденными средствами и программами-вымогателями. Отчасти это может быть объяснено кражей криптовалют и деятельностью вымогателей, связанной с Lazarus Group, киберпреступным синдикатом, связанным с правительством Северной Кореи [12]. Наконец, Соединенные Штаты несколько чрезмерно представлены в средствах, полученных с адресов, связанных с мошенничеством и кражей средств.

Криптовалюта, отправленная с незаконных адресов, как правило, оказывается всего в нескольких сервисах. Ниже показана доля всех незаконных средств, поступающих в пять поставщиков услуг, получающих наибольшее количество незаконных средств каждый год с 2017 года в целом. Два наиболее популярных сервиса, получающие незаконные средства, оставались неизменными в течение трех лет, с некоторыми изменениями в третьем, четвертом и пятом местах. Вместе взятые, первые два принимают больше, чем остальные три, вместе взятые, в любой данный год. В целом в 2020 году эти пять ведущих сервисов получили 55% всех средств, переведенных с незаконных адресов (рис. 4) [13].

Доля всех незаконных средства, полученных пятью наиболее популярными поставщиками незаконных услуг.

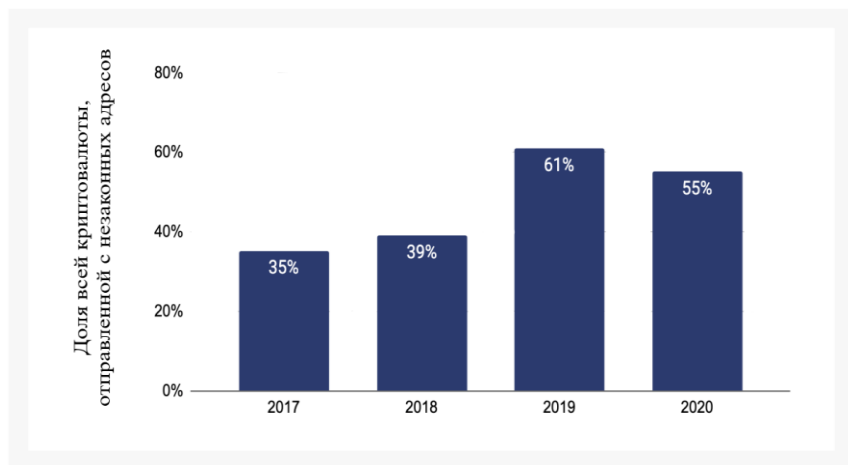


Рисунок 4 – Доля незаконных средств, полученных пятью наиболее популярными поставщиками незаконных услуг

Такая высокая концентрация незаконных средств свидетельствует о том, что существует несколько центральных поставщиков услуг, обслуживающих преступников. Правоохранительные органы могут значительно ограничить возможность преступников конвертировать криптовалюту в наличные деньги, вычислив этих поставщиков, и затем идентифицировать их клиентов. В силу особенностей криптовалют, обеспеченных архитектурой блокчейн-сетей, таких как псевдонимность и трансграничный характер, компетентным органам следует

сосредоточиться на обменниках, тем самым расправившись с самыми злостными нарушителями.

Как было показано в предыдущем пункте, виртуальные активы, и, в частности, криптовалюты, активно используются преступниками и являются составной частью преступления различных видов. То же самое справедливо и для ФТ. В данный момент нельзя сказать, является ли использование виртуальных активов террористическими группами единичными инцидентами или предвещает глобальную и более пагубную тенденцию.

В то время как BAVB имеют много очень важных законных применений, некоторые характеристики также делают их восприимчивыми к злоупотреблениям. Многие, особенно криптовалюты, защищают или скрывают личность, тем самым затрудняя правоохранительным органам выявление и отслеживание этих личностей по сравнению с традиционными механизмами передачи ценностей. Поэтому, если террористы начнут использовать BAVB массово, их будет гораздо труднее отслеживать и уничтожать.

Вторая причина, из-за которой террористические группы могут пожелать использовать BAVB массово, — это географический охват таких валют. С помощью определенных BAVB можно мгновенно переводить деньги по всему миру без использования таких учреждений, как банки, которые требуют большей прозрачности и обязаны сообщать о подозрительных операциях. Даже централизованные BAVB могут быть доступны онлайн в любой точке мира, поэтому террористы и преступники могут воспользоваться преимуществами этих валют, которые были созданы в юрисдикциях с недостаточно эффективной системой ПОД/ФТ. Потенциально такие характеристики могут быть эффективно использованы для создания цифровой платформы поверх существующих систем, которая в настоящее время позволяет террористам и другим лицам переводить наличные деньги в международном масштабе.

Наконец, новизна и некоторые особые атрибуты BAVB, такие как децентрализация, делают их особой проблемой для регуляторов. Децентрализованные криптовалюты, такие как Bitcoin, не имеют концентрированных хранилищ идентифицирующей информации о владельцах счетов, которые правоохранительные органы обычно используют в расследованиях финансовых преступлений и борьбы с терроризмом, но которые недоступны при работе со многими BAVB.

Сообщения в прессе и многочисленные научные исследования часто описывают перспективы использования BAVB террористами в общих терминах. Однако террористы являются сложными субъектами, представляющими широкий спектр идеологий, мотиваций, возможностей,

тактики и поведения. Они также сильно различаются по структуре. Примеры различных террористических субъектов включают:

- неорганизованные (индивидуальные) субъекты, которые, как правило, вдохновляются центральной террористической группой, но могут не иметь официальных связей с ней;
- небольшие ячейки и сети содействия, которые могут быть либо вдохновлены основной группой, либо связаны с ней;
- командно-контрольные организации без единой установленной базы (такие как «Аль-Каида»);
- контролирующие территорию группировки (такие как ИГИЛ или "Аш-Шабааб").

Что касается методов ФТ, то они могут принимать несколько форм, в том числе:

- сбор средств, например, за счет пожертвований или преступной деятельности;
- перемещение средств, например, путем перевода средств через банки из Европы в страны, расположенные вблизи зон военных действий, или просто путем перевозки наличных денег;
- хранение средств, например, путем поддержания резервов наличности, которые впоследствии могут быть потрачены на нападения, военные операции, поездки или другую деятельность по содействию.

Если рассматривать неорганизованные субъекты и небольшие ячейки, то финансовые ресурсы, необходимые для совершения атаки, часто довольно низки. Например, во время нападения в День взятия Бастилии в 2016 году в Ницце, Франция, злоумышленнику потребовались средства лишь для аренды грузовика. Британская супружеская пара, которые были осуждены за планирование неудачного заговора с бомбой в 2015 году, собрали 14 000 фунтов стерлингов за счет займов в день зарплаты. Упреждающая идентификация таких лиц финансовыми учреждениями представляет собой огромную проблему, если не почти невозможную.

Таким образом, ВАВВ могут не предоставлять неорганизованным субъектам и небольшим ячейкам существенных преимуществ, которые можно легко финансировать с помощью обычных методов, таких как наличные деньги или кредитные карты, а также за счет самофинансирования. Действительно, виртуальные активы не являются ни необходимым, ни практичным способом оплаты аренды транспортных средств в Европе. Нынешние ограниченные возможности для их повседневного практического использования могут ограничить полезность ВАВВ для большинства террористических субъектов.

Тем не менее, ВАВВ могут иногда оказаться привлекательными для некоторых неорганизованных субъектов и небольших ячеек, работающих

в Интернете. В июне 2015 года подросток из Вирджинии Али Шукри Амин был осужден в США за оказание материальной поддержки ИГИЛ через социальные сети. Амин признался, что использовал Twitter, чтобы консультировать других о том, как Биткоин может быть использован для маскировки предоставления средств в поддержку ИГИЛ. В то время как Амин, похоже, не добился успеха в сборе биткоинов для ИГИЛ, его случай дает предупреждение: он отражает молодую демографию джихадистов, которые выросли в Интернете и могут комфортно использовать новые финансовые технологии.

Когда дело доходит до финансирования текущих операций более крупных групп, таких как "Аль-Каида" и ИГИЛ, ВАВВ вряд ли будут необходимы или полезны им для многих их текущих операций. Финансирование ИГИЛ своей деятельности в Сирии и Ираке, например, в основном осуществлялось за счет принудительного налогообложения физических и юридических лиц, находящихся под его контролем. Более того, нынешние характеристики многих ВАВВ – особенно волатильность и проблемы с удобством использования – скорее всего, сделают их ненадежными методами перевода или перемещения средств в значительных объемах.

Поэтому вместо того, чтобы рассматривать ВАВВ как методы постоянного и устойчивого финансирования, террористические группы могут найти в них большую полезность для случайных и запланированных международных P2P-переводов между членами группы в качестве метода перемещения средств или для использования в целевых кампаниях краудфандинга, предназначенных для сбора средств в Интернете. Средства, собранные с помощью краудфандинга, могут использоваться для самых разных целей, таких как приобретение оружия, облегчение поездок, оплата пропагандистских кампаний или приобретение повседневных товаров и услуг. Террористы часто действуют под предлогом сбора пожертвований на гуманитарную деятельность или другое благородное дело.

В 2020 году правительственные учреждения по всему миру раскрыли, расследовали и преследовали в судебном порядке больше схем финансирования терроризма, связанных с криптовалютой, чем когда-либо прежде. Наиболее заметный пример произошел в августе, когда Министерство юстиции США объявило о крупнейшем в истории изъятии криптовалюты у террористической группы. После расследования нескольких различных кампаний по пожертвованию криптовалют правительственные учреждения США изъяли биткоины на сумму более 1 миллиона долларов из кошельков, контролируемых террористическими группами и их финансовыми посредниками [15].

Приведенные выше примеры относятся к религиозно мотивированной и, в частности, джихадистской деятельности, но политическая экстремистская деятельность также заслуживает рассмотрения. Данные свидетельствуют о росте политической экстремистской активности в Европе и США. Исследование, проведенное Королевский объединённый институт оборонных исследований в 2016 году по Борьбе с Терроризмом Неорганизованных Субъектов, показывает, что 33% сговоров в период с 2000 по 2014 год были связаны с правыми экстремистами [6]. Конечно, определенная политическая экстремистская деятельность, такая как распространение пропаганды, не всегда может подпадать под определение "терроризм", данное ЕС, которое включает в себя такую деятельность, как запугивание населения и дестабилизация или разрушение политических, экономических и социальных структур [11]. Тем не менее изучение глобальных моделей использования ВАВВ экстремистами может помочь понять, как ВАВВ могут использоваться теми экстремистами, которые действительно занимаются терроризмом.

Таким образом, можно сделать вывод, что схемы финансирования террористических и экстремистских групп становятся все сложнее, соединяя в себе глобальные сети посредников, спонсоров и инновационные технологии, которые затрудняют финансовые расследования, проводимые правоохранительными органами. Компетентные органы всех стран должны объединить свои усилия для предотвращения массового использования данных технологий в незаконной деятельности и принять соответствующие превентивные меры для ограничения возможностей преступников.

Заключение. Рынок криптовалют активно расширяется, но при этом расширяются и теневые рынки, поставляющие незаконные товары и услуги. Доля от всего объема транзакций с криптовалютами, связанная с незаконной деятельностью, невелика и в 2020 году составила всего 0.34%, что говорит о том, что основной объем на рынке составляют законные транзакции. Таким образом можно сделать вывод, что криптовалюты – альтернативное средство платежа, которым в основном пользуются субъекты, не нарушающие закон, а не только инструмент, который используют преступники.

На сегодняшний день подтвержденных и документально зафиксированных случаев использования ВАВВ, и, в частности, криптовалют, для финансирования терроризма и экстремизма крайне мало, поэтому нельзя дать полную и достоверную оценку соответствующего риска. Однако существует риск адаптации террористов к новым технологиям, и их массового использования для создания новых каналов финансирования своей деятельности.

Список использованных источников:

1. Гурьянов К.В. Оценка возможности легализации доходов, полученных преступным путем и финансирования терроризма при использовании электронных денег / К.В. Гурьянов, Я.С. Шатило // Научно-практический журнал «Базис». ISSN 2587-8042.
2. Достов В.Л. Влияние финансовых технологий на практику борьбы с отмытием денег и финансированием терроризма / В.Л. Достов, Г.Ю. Негляд, П.М. Шуст // Журнал «Финансовые исследования» №4 (61) 2018.
3. Негляд Г.Ю. Виртуальные валюты и проблемы противодействия отмытию доходов, полученных преступным путем, и финансированию терроризма / Г.Ю. Негляд // Журнал «Имущественные отношения в Российской Федерации» №5 (200) 2018.
4. Сведения об организациях и физических лицах, причастных к террористической деятельности, 2021, ФСТЭК России [электронный ресурс]. URL: <https://fstec.ru/normotvorcheskaya/eksportnyj-kontrol/283-reestry-perechni/14-72-spisok-2> (дата обращения: 26.05.2021)
5. 12-month Review Virtual Assets and VASPs, 2020 FATF/OECD, Paris, France [электронный ресурс]. URL: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html> (дата обращения: 01.05.2021)
6. Chainalysis in Action: Department of Justice Announces Takedown of Two Terrorism Financing Campaigns with Help from Blockchain Analysis, August 13, 2020, Chainalysis [электронный ресурс]. URL: <https://blog.chainalysis.com/reports/cryptocurrency-terrorism-financing-al-qaeda-al-qassam-brigades-bitcointransfer> (дата обращения: 01.05.2021)
7. FATF Report to the G20, 2020 FATF/OECD, France [электронный ресурс]. URL: <http://www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html> (дата обращения: 01.05.2021)
8. Geographic Distinctions in Darknet Market Activity: U.S. and Western Europe Have the Most Vendors, Eastern Europe and China Lead in Money Laundering, 2021, Chainalysis [электронный ресурс]. URL: <https://blog.chainalysis.com/reports/darknet-markets-2021-geographic-breakdown> (дата обращения: 01.05.2021)
9. Goldman Z.K., Maruyama E., Rosenberg E., Saravalle E., Solomon-Strauss J. Terrorist Use of Virtual Currencies, 2017, CNAS [электронный ресурс]. URL: <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNASReport-TerroristFinancing-Final.pdf?mtime=20170502033819&focal=none> (дата обращения: 01.05.2021)

10. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2019 FATF/OECD, Paris [электронный ресурс]. URL: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html> (дата обращения: 01.05.2021)
11. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Recommendation 15, FATF, Paris, France [электронный ресурс]. URL: <http://www.fatf-gafi.org/recommendations.html> (дата обращения: 01.05.2021)
12. Lazarus Group Pulled Off 2020's Biggest Exchange Hack and Appears to be Exploring New Money Laundering Options, 2021, Chainalysis [электронный ресурс]. URL: <https://blog.chainalysis.com/reports/lazarus-group-kucoin-exchange-hack> (дата обращения: 01.05.2021)
13. Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, 2020 FATF/OECD, Paris, France [электронный ресурс]. URL: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html> (дата обращения: 01.05.2021)
14. The 2021 Crypto Crime Report, 2021, Chainalysis [электронный ресурс]. URL: <https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf> (дата обращения: 01.05.2021)
15. Virtual currencies and terrorist financing: assessing the risks and evaluating responses, INTERPOL, PE 604.970 - May 2018 [электронный ресурс]. URL: [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU\(2018\)604970_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf) (дата обращения: 01.05.2021)

**Риски ОД/ФТ/ПРОМУ и инструменты управления ими
на уровне субъектов первичного финансового мониторинга
Российской Федерации**

С.Е. Климова

доцент кафедры финансового мониторинга НИЯУ МИФИ, Москва

E-mail: SEKlimova@mephi.ru

Аннотация: В течение последних 10 лет основным вектором развития национальных систем ПОД/ФТ/ПРОМУ стало внедрение риск-ориентированного подхода с целью повышения эффективности их функционирования. Так, с февраля 2012 года в соответствии с 1 Рекомендацией ФАТФ странам-участницам предписано выявлять риски ОД/ФТ и создать систему управления ими. А с октября 2020 года данное требование распространилось и на риск ПРОМУ (финансирование оружия распространение оружия массового уничтожения). В статье рассматриваются подходы к исследованию рисков ОД/ФТ/ ПРОМУ, инструменты управления ими (на примере деятельности коммерческих банков), а также исторические аспекты внедрения в практику субъектов первичного финансового мониторинга в Российской Федерации

Ключевые слова: ПОД/ФТ, коммерческий банк, риск ориентированный подход, распространение оружия массового уничтожения.

**ML/FT/FMT risks and their management Tools
at the level of subjects of primary financial monitoring of the Russian
Federation**

Abstract: Over the last 10 years a risk-based approach has come to the forefront in the AML/CTF sphere. Since the February of 2012 countries are to identify and manage both money laundering risk and terrorism financing risk. As to the proliferation of weapon of mass distraction risk, the recommendation to reveal, monitor and asses this kind of risk appeared at the end of 2020. These article is devoted to the nature of these risks, specifies the instruments of their management in practice of russian commercial banks, and describes the history of their implementation into the national AML/CTF system of Russian Federation.

Keywords: *AML/CTF, commercial banks, risk-oriented approach, proliferation of weapon of mass distraction.*

Существуют разные подходы к исследованию рисков ОД/ФТ/ФРОМУ. В частности, в методологических документах ФАТФ, Банка России риск легализации доходов, полученных преступным путем, риск финансирования терроризма и риск финансирования оружия массового уничтожения объединены в совокупный риск. Одна из причин возникновения такого подхода – историческая. Далее рассмотрим наиболее значимые в контексте данной статьи этапы развития Рекомендаций ФАТФ и их влияния на российскую нормативно-правовую базу в данной области (рис.1) .

Первоначально мировым сообществом было признано существование глобальной проблемы вовлечения банков в схемы легализации преступных доходов. Так, в декабре 1988 года Базельским комитетом по банковскому надзору был принят документ «Предотвращение криминального использования банковской системы для целей отмывания денег». В следующем году была создана международная рабочая группа ФАТФ, которая выпустила «40 Рекомендаций по противодействию отмыванию денег» в 1990 году. В этот же период ряд европейских стран, такие как Австралия, Бельгия, Великобритания, США, Швейцария, принимают законодательные акты, направленные на предотвращение использования финансово-кредитного сектора исключительно в целях отмывания преступных доходов

В 2001 году на фоне усиления угрозы международного терроризма в международную систему противодействия отмывания доходов, полученных преступным путем, был интегрирован аспект противодействия финансированию терроризма и финансированию распространения оружия массового уничтожения: ФАТФ выпускает «9 специальных Рекомендаций».

Следует отметить, что именно в этот период в Российской Федерации проводилась активная работа по обеспечению соответствия требованиями ФАТФ в целях исключения из «черного» списка. Что и послужило одной из причин объединения в Федеральном законе от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма» основ противодействия данным видам преступлений.

Итак, к 2001 году ФАТФ сформирован перечень рекомендаций, касающихся противодействия трем видам преступлений: отмывание

доходов, полученных преступным путем, финансирование терроризма и финансирование распространения оружия массового уничтожения.

В 2012 году в свет выходит обновлённая 1-ая Рекомендация ФАТФ, которая в том числе предписывает странам-участницам: определить и оценить риски ОД/ФТ; назначить орган или создать механизм взаимодействия по оценке рисков ОД/ФТ; распределять ресурсы финансового мониторинга в зависимости от уровня риска (т.е. реализовать риск-ориентированный подход). Следует обратить внимание, что в тот период данный подход не включал требования по выявлению и управлению риском ФРОМУ. Такого рода рекомендации появились осенью 2020 года в связи с обновлением Рекомендаций ФАТФ. Так, в Рекомендацию 1 и Пояснительную записку к ней внесено изменение, требующее от стран, финансовых учреждений и УНФПП выявления и оценки рисков потенциальных нарушений, невыполнения или уклонения от целевых финансовых санкций, связанных с финансированием распространения оружия массового уничтожения, содержащихся в Рекомендации 7 ФАТФ, и принятия мер по снижению этих рисков.



Рисунок 1 – Этапы изменений Рекомендаций ФАТФ

В российской экономической литературе отдельными авторами риск легализации рассматривается как самостоятельная категория, в отдельности от риска финансирования терроризма. Так, например, Каратаев М.В. дает следующее толкование указанному риску: «риск вовлечения банка в процессы легализации доходов, полученных преступным путем, представляет собою вероятность понесения кредитной организацией потерь в результате вовлечения в процессы придания

правомерного вида владению, пользованию или распоряжению денежными средствами, полученными в результате совершения преступления, через оказание услуг клиентам с непрозрачной структурой собственности и/или неясными источниками происхождения капитала» [4].

Применение указанного подхода в рамках рассмотрения вопроса управления рисками кредитных организаций представляется вполне оправданным вследствие различия признаков преступлений, связанных с отмыванием нелегальных доходов и финансированием терроризма, и, как следствие, связанных с ними финансовых операций. Во-первых, в процессе легализации происходит оперирование доходами, полученными исключительно от преступной деятельности (укрывательство от налогов, «серый» импорт, взяточничество и пр.). Вместе с тем, как подтверждается исследованиями ФАТФ [6], в целях финансирования терроризма используются комбинированные источники денежных средств: как полученные вследствие осуществления незаконной деятельности, так и законные источники, например, сбор некоммерческими организациями средств в виде пожертвований и благотворительных взносов.

Во-вторых, транзакции, осуществляемые в целях финансирования терроризма, как правило, совершаются относительно небольшими (дробными) суммами, что не требует предоставления расширенного перечня сведений в отношении перевододателя и получателя денежных средств. Вместе с тем, финансовые операции, проводимые в целях легализации преступных доходов, зачастую характеризуются сравнительно большими объемами и частотой совершения, так как в данном случае основная цель преступников – в максимально короткие сроки разместить и распылить в финансовой системе доходы, полученные в результате совершения преступления. Например, таким способом мошенники стараются «вывести» незаконно полученные средства в государства с низким уровнем налогов и дополнительного финансового контроля. Вместе с тем, направление средств в целях финансирования терроризма зачастую не связано с такими экономическими зонами.

Как показывают результаты исследований типологий преступлений, связанных с ОД/ФТ в Российской Федерации и отдельных зарубежных странах (Австралия, Бельгия, Япония, Китай, Польша и др.), для совершения транзакций в целях отмывания преступных доходов, как правило, используются такие финансовые инструменты, как ценные бумаги, страховые и сберегательные продукты, банковские карты, в то время как для финансирования терроризма - переводы денежных средств

без открытия счета, или же услуги небанковских организаций в виде предоплаченных карт, электронных кошельков, мобильных платежей и пр.

Следует отметить, что в соответствии с Методологией Росфинмониторинга указанные риски рассматриваются также как отдельные категории. Их толкование приведено в следующих документах: «Публичный отчет о национальной оценке рисков легализации (отмывания) преступных доходов 2017-2018» и «Публичный отчет о национальной оценке рисков финансирования терроризма 2017-2018».

Таким образом, указанными различиями обусловлена необходимость выработки процедур выявления, мониторинга и оценки в отдельности для риска легализации преступных доходов и риска финансирования терроризма. На основании изложенного считаем обоснованным придерживаться второго подхода к исследованию указанных рисков, т.е. как самостоятельных категорий – риска ОД и риска ФТ.

Вопрос толкования указанных рисков уже долгое время остается дискуссионным как с точки зрения теоретического, так и практического осмысления. В частности, в российском законодательства на сегодняшний день толкование таких рисков отсутствует. Так, в п.1.1) ст. 7 Федерального закона от 07.08.2001 № 115-ФЗ указано на необходимость ранжировать объем требований по получению в отношении клиентов дополнительных сведений (о целях установления и предполагаемом характере их деловых отношений, целях финансово-хозяйственной деятельности, финансового положения и деловой репутации, источников происхождения денежных средств и иного имущества) в зависимости от присвоенного клиенту уровня риска легализации. При этом несколькими годами раньше, в 2012 году Банком России было дано опосредованное толкование риска ОД/ФТ, через программу его управления. Исследование видов и сущности риска легализации подробнее изложено в других работах автора.

Далее рассмотрим инструменты управления рисками ОД/ФТ/ПРОМУ в Российской Федерации. Предрасполагаясь подхода раздельного исследования данных рисков, данный вопрос изложен отдельно для каждого из рисков: риска легализации, риска финансирования терроризма и риска финансирования распространения оружия массового уничтожения.

Дополнительно считаем целесообразным определиться с понятийным аппаратом. Согласно общей теории рисков, целью управления рисками является снижение их уровня (вероятности наступления рискового события) или смягчений последствий их реализации (если рисковое событие состоялось). Таким образом, под инструментами

управления рисками ОД/ФТ/ФРОМУ в первую очередь мы рассматриваем перечень мер, направленных на снижение их уровня.

Инструменты управления риском легализации можно условно разделить на две группы: законодательные и экономические. К законодательным инструментам относятся предусмотренные ст. 7 Федерального закона от 07.08.2001 № 115-ФЗ права:

1. *отказ в заключении договорных отношений с клиентом* (за исключением физических лиц), в случае возникновения подозрений, что целью заключения такого договора является совершение операций в целях легализации (отмывания) преступных доходов (в соответствии с п. 5.2 указанной статьи);

2. *отказ в выполнении распоряжения клиента о совершении операции* в случае возникновения подозрений, что она совершается в целях легализации (отмывания) преступных доходов (в соответствии с п. 11 указанной статьи);

3. *отказ в дальнейшем обслуживании*, расторгнув договор банковского счета в случае принятия в течение календарного года двух и более решений об отказе в выполнении распоряжения клиента (в соответствии с п. 5.2 указанной статьи).

Дополнительным законодательным инструментом управления риском легализации, проявляющемся в вероятном совершении операций по незаконному выводу денежных средств за рубеж, является исполнение коммерческими банками функций агентов валютного контроля в соответствии с Федеральным законом от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле». Согласно ст. 23 гл. 4 данного нормативного акта коммерческие банки обязаны осуществлять контроль за соответствием исходящих платежей документам, подтверждающим факт поставки товаров и услуг на территорию Российской Федерации. Выполняя функции агентов валютного контроля, коммерческие банки взимают тарифы за проведение платежей, сопровождающих внешнеэкономическую деятельность своих клиентов.

Что касается экономических инструментов, то в отдельных случаях, введение повышенных индивидуальных тарифов за такое обслуживание позволяет пресечь подозрительную финансовую активность клиентов по выводу денежных средств за рубеж. Анализ динамики объемов вывода денежных средств за рубеж через банковский сектор РФ за период с 2015 по 2020 гг. свидетельствует о результативности выработанных инструментов, а также совместной работы коммерческих банков и Банка России. Так в указанный период, в абсолютном выражении объем таких

операций снизился почти в 10 раз: с 501 млрд. руб. в 2020 г. до 53 млрд. руб. в 2020 году (см. Рис. 1). При этом, важным является тот факт, что за последние три года (в период с 2018 по 2020 гг.) достигнутый показатель держится на стабильном уровне в 0,05-0,07% ВВП (см. Рис. 2) с тенденцией к понижению.

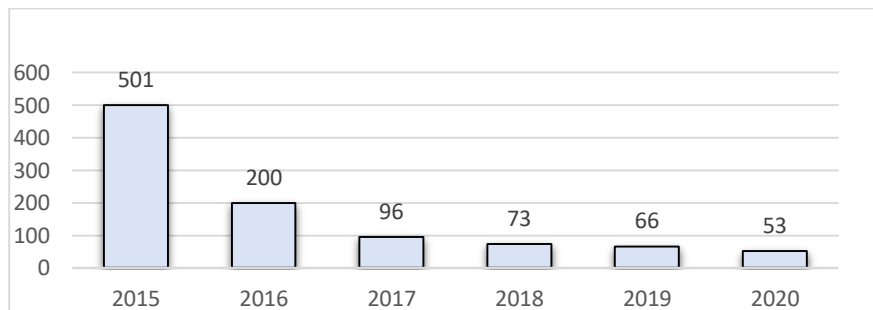


Рисунок 2 – Объем операций по незаконному выводу денежных средств за рубеж (в млрд.руб)

(Источник: составлено автором на основании данных официального сайта Банка России)

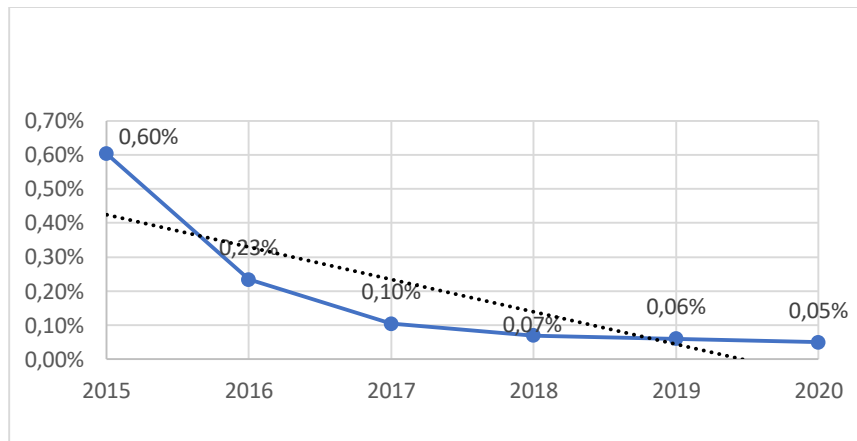


Рисунок 3 – Соотношение объема вывода денежных средств за рубеж к реальному ВВП (%)

(Источник: составлено автором на основании данных официального сайта и Госкомстата Банка России)

Инструменты управления риском легализации, проявляющемся в незаконном обналичивании денежных средств, включают в себя рассмотренные нами выше законодательные инструменты, а также экономические в виде установления комиссий и лимитов за снятие денежных средств в наличной форме со счетов физических и юридических лиц. Обзор комиссий российских коммерческих банков показал, что среднесуточная комиссия за снятие наличных в банкоматах первой и второй десятки банков составляет 1%, а для третьей десятки – 2%. Размер среднесуточных лимитов со снятия денежных средств со счетов физических лиц составляет: для банков первой десятки - 167 тыс.рублей, для банков второй десятки - 253 тыс.рублей, третьей десятки - 255 тыс.рублей.

Также следует отметить, что в части объемов незаконного обналичивая денежных средств в российском банковском секторе в периоде с 2014 по 2020 гг. также наблюдается устойчивое снижение (Рис. 3).

Объемы обналичивания денежных средств в банковском секторе, в млрд. руб

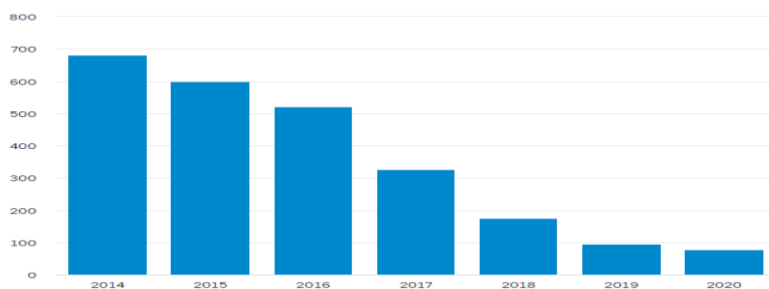


Рисунок 4 – Объемы обналичивания денежных средств в банковском секторе (Источник: Официальный сайт Банка России (www.cbr.ru)).

Инструменты управления риском финансирования терроризма в соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ (далее – Закон) включают в себя:

1) *обязательный контроль* операций с участием фигурантов Перечня и подконтрольных, действующих от их имени лиц (в соответствии с п. 2 ст. 6 Закона);

2) *блокирование денежных средств и иного имущества* (согласно пп. 6 п. 1 ст. 7 Закона) в отношении фигурантов Перечня либо лиц, в отношении которых имеются достаточные основания подозревать их

причастность к террористической деятельности (в т.ч. к финансированию терроризма);

3) *регулярная сверка клиентской базы* с Перечнем и списком лиц, отношении которых имеются достаточные основания подозревать их причастность к террористической деятельности (согласно пп. 6 п. 1 ст. 7 Закона) ;

4) *приостановление расходных операций клиентов* с участием лиц, в отношении которых принято решение о блокировании (в соответствии с п.10 ст. 7 Закона);

5) *право отказа в открытии счета*, в совершении операции при наличии подозрений в том, что их целью является финансирование терроризма (на основании п. 5.2 , п. 11 ст.7 Закона), а также право расторгнуть договора банковского счета в случае принятия в течение календарного года двух и более решений об отказе в проведении операции.

Формирование вышеуказанного комплекса инструментов управления риском финансирования терроризма происходило последовательно. Так, требование об обязательном контроле было включено в Закон в 2010 году, а блокирование (сверка клиентской базы) – в 2013 году, а права «отказов» - в 2015 году.

В 2018 году в российское законодательство был внедрены меры противодействия финансированию распространения оружия массового уничтожения. В соответствии со ст. 7.5 Закона субъектам первичного финансового мониторинга надлежит осуществлять: обязательный контроль операций с участием фигурантов Перечня ФРОМУ (п. 1 ст. 7.5 Закона), блокирование денежных средств и имущества фигурантам (п. 5 ст. 7.5 Закона), регулярную сверку клиентской базы с Перечнем ФРОМУ (п. 6 ст. 7.5 Закона), приостанавливать операции с участием лиц из Перечня ФРОМУ на 5 рабочих дней (п. 8 ст. 7.5). С формальной точки зрения их нельзя назвать инструментами управления риском ФРОМУ, ввиду того, что такая категория и дефиниция как риск ФРОМУ на текущий момент отсутствует в российской нормативно-правовой базе. Тем не менее, с точки зрения содержания данный перечень мер вполне обоснованно может быть рассмотрен как комплекс инструментов управления риском ФРОМУ (см. Таблица 1).

Таким образом, практические аспекты управления рисками ФТ и ФРОМУ в Российской Федерации могут быть объединены ввиду идентичности инструментария. При этом единство природы операций, связанных с финансированием такого рода преступлений (терроризм и распространение оружия массового уничтожения) может служить

дополнительным аргументом объединения и дальнейшего исследования данных рисков как риск совокупного риска ФТ/ФРОМУ.

Таблица 1 – Перечень законодательных инструментов управления риском легализации, риском финансирования терроризма и распространения оружия массового уничтожения в РФ
(Источник: составлено автором)

ИНСТРУМЕНТЫ	ВИД РИСКА		
	РИСК ОД	РИСК ФТ	РИСК ФРОМУ
1) обязательный контроль	+	+	+
2) приостановление расходных операций клиентов	-	+	+
3) блокирование денежных средств и иного имущества	-	+	+
4) регулярная сверка клиентской базы с Перечнями	-	+	+
5) отказ в открытии счета / совершении операции / дальнейшем обслуживании	+	+	-

На основании изложенного можно сделать вывод о том, что субъекты первичного финансового мониторинга прошли динамичный путь по внедрению и реализации риск-ориентированного подхода в области ПОД/ФТ/ФРОМУ. С 2012 года удалось сформировать подходы к управлению риском легализации и риском финансирования терроризма. Научное осмысление сущности этих рисков, их толкование также нашло свое отражение и в экономической литературе.

При этом представляется перспективным закрепить полученные достижения и на законодательном уровне, включив в понятийный аппарат Федерального закона от 07.08.2001 № 115-ФЗ понятия «риск легализации», риск «финансирования терроризма», «риск финансирования распространения оружия массового уничтожения», а в подзаконных нормативных актах – внести уточнения в данные термины учитывая уровень, на котором они реализуются: национальный, секторальный, частный.

Учитывая содержание обновленных рекомендаций ФАТФ (в ред. от октября 2020 года) перед национальной системой ПОД/ФТ и ее участниками стоит новая задача – разработать и внедрить процедуры выявления, мониторинга и оценки риска финансирования оружием массового уничтожения.

Список использованных источников:

1. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма»
2. Федеральный закон от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле»
3. Положение Банка России от 2 марта 2012 г. N 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (с изменениями и дополнениями)
4. Каратаев М.В. Управление риском вовлечения российских банков в процессы легализации преступных доходов. Диссертация на соискание ученой степени кандидата экономических наук: 08.00.10. – Москва, 2011. - 234 с.
5. ФАТФ/ ГМФД. Руководство по применению подхода, основанного на оценке риска в целях противодействия отмыванию денег и финансированию терроризма. –Июнь, 2007. [Электронный ресурс] / Официальный сайт Группы разработки финансовых мер. – Режим доступа:<http://www.fatf-gafi.org>
6. ФАТФ/ ОЭСР. Глобальная оценка угроз отмывания денег и финансирования терроризма. Обзор способов и причин финансового злоупотребления со стороны преступников и террористов, последствий и мер по смягчению данных угроз. - июль 2010. - [Электронный ресурс] / Официальный сайт Группы разработки финансовых мер. – Режим доступа:<http://www.fatf-gafi.org>.

Риски финансирования экспортной деятельности многонациональных предприятий ЮАР

С.В. Ефименко

соискатель аспирантуры Института Африки РАН, Москва

E-mail: sergej.efimenko2014@yandex.ru

научный руководитель: А.Л. Сапунцов

д.э.н., доцент центра глобальных и стратегических исследований

Института Африки РАН, Москва

E-mail: andrew@sapuntsov.ru

Аннотация: Данная статья рассматривает риски финансирования экспортной деятельности, которые испытывают МНП ЮАР. Эта область исследования, оценивает перспективы экспортных рисков с точки зрения взаимоотношений кредитора и потенциальной компании МНП. Даны выводы, в которых предложен пакет в виде набора принципов, как МНП могут снизить риски и повысить свои шансы на получение финансовой помощи.

Ключевые слова: МНП (многонациональные предприятия), интернационализация, экспортное финансирование, снижение рисков, экспортные рынки.

Risks of financing export activities of multinational enterprises of South Africa

Abstract: This article examines the risks of export financing experienced by South African MNEs. This area of research, evaluates the prospects of export risks from the point of view of the relationship of creditor and potential companies of MNEs. Conclusions are given, in which a package in the form of a set of principles is proposed, how MNEs can reduce risks and increase their chances of receiving financial assistance.

Keywords: MNEs (multinational enterprises), internationalization, export Finance, risk reduction, export markets.

Несмотря на доступность внешних рынков, большинство МНП в состоянии сделать переход от местного рынка к международному, но рискованные экономические барьеры все же присутствуют. Общеизвестно, что многие финансовые учреждения предпочитают сделки с надежными,

проверенными крупными МНП. Предоставление экспортного финансирования МНП рассматривается как высокий риск. Основная причина, опасение банков в этом отношении: высокие операционные издержки, связанные сделки с МНП, ограниченное обеспечение и высокий риск дефолта.[5]

Следует признать, что финансовые учреждения имеют политику управления рисками и практики для минимизации риска дефолта своих заемщиков. Еще многие МНП не могут найти пути для решения своих проблем как кредитозависимые предприятия. В результате скептицизм кредиторов усиливается, что еще больше ограничивает доступ МНП к финансированию.[3, 4]

В ходе проведенных исследований были выявлены экспортные барьеры в деятельности МНП в развивающихся странах. При их анализе обнаружено отсутствие экспорта финансирования, которое является вторым по величине барьером для расширения внешнего рынка, после недостаточного изучения рынка. Несколько удивительно, но плохая инфраструктура и коррупция не рассматривалась как серьезное препятствие для успешного экспорта.[5]

Все формы бизнеса содержат элементы риска, но когда дело доходит до международных торгов, профиль риска переходит в новое измерение.

Различные виды рисков приведены в таблице 1.[13]

Таблица 1 – Риски, оцениваемые финансовыми учреждениями при рассмотрении экспортного финансирования МНП ЮАР

Рыночный риск	Риски производительности	Риски бизнеса
Риск изменения цен на сырьевые товары Валютный риск Суверенный риск	Операционный риск Производство и принятие риска Риск поставщика Риск покупателя Расчетный риск Экологический риск Риск качества	Риск конкуренции Риск спроса Отраслевой риск Риск концентрации Риск инвентаризации Транзитные риски

Риски, приведенные в таблице 1 и методы их снижения, рассматриваемые в настоящей статье, были исследованы на примере МНП и двух финансовых учреждений ЮАР в период с 2010 по 2020 гг., два из которых специализируются в структурированной торговле и товарном финансировании. Все два финансовых учреждения используют контрольный список оцениваемых компаний на предмет предоставления им денежных средств или нет.

Рыночный риск, включает в себя ценовой риск, валютный риск и процентный риск. Ценовой риск относится к вероятности того, что цена товара будет двигаться в направлении, которое негативно повлияет на МНП. Даже в тех случаях, когда МНП используют сырьевые товары, цены на такие сырьевые товары, как нефть, металлы и другие полезные ископаемые будут неизменно влиять на деятельность компаний.

Все МНП имеют прямой или косвенный опыт валютного риска. Фирмы-экспортеры, например, учитывают риск своей национальной валюты, оценивая момент вступления договора в силу и окончание платежа. В южноафриканском контексте это очень правдоподобно из-за его ярко выраженной волатильности.

Суверенный (страновой) риск связан с политической стабильностью государства и экономической стабильности импортера страны. Например, политические потрясения могут затруднить выполнение контрактов, в то время как экономические условия в стране могут побудить правительство ввести валютный контроль, изменение конвертируемости национальной валюты или замораживание переводов денежных средств. Как и валютный риск, политическая нестабильность и трудовые беспорядки, серьезная проблема ЮАР.[6]

Риски производительности представлены в настоящей статье как: операционный риск, риск поставщика, риск покупателя, расчетный риск, экологический риск и риск качества. Операционный риск связан с риском экспортера и импортера, их способности успешно выполнять свои обязанности по договору. Кроме того для оценки операционной эффективности фирмы финансовое учреждение обязано иметь качественный менеджмент, а также стабильную управленческую команду (или ключевой персонал) достаточно компетентный в отрасли в которой они работают.

В целом, производственный риск и риск поглощения относится к адекватности и эффективности компаний по обработке, уровня квалификации рабочей силы и непрерывности снабжения производства водой и энергоресурсами.[7] Экологический риск и потенциальные проблемы качества, как правило, связаны с неоптимальным производством.

Риск поставщика относится к степени вероятности, что партия не отвечает установленным техническим требованиям, уровень качества которой соответствует определенной величине AQL (допустимый предел качества) в плане выборочного контроля. Риск покупателя (также известный как коммерческий риск) относится к потенциальной неспособности совершать плату. При желании оплата труда является отражением деловой этики, платежеспособность же связана с

доступностью средств. Даже если импортер готов и способен заплатить, есть еще мера расчетного риска. Это касается возможности, что банк выплачивает средства, причитающиеся при совершении сделки но не получает средства, которые он должен от своего контрагента.[7]

Хотя эти риски также присутствуют в контексте Южной Африки, они не более выражены. МНП ЮАР сталкиваются с теми же проблемами, что и МНП в других странах. Однако южноафриканские компании сталкиваются с дополнительными вызовами на политическом и макроэкономическом фронтах, с изменением курса валют, трудовыми волнениями и политической нестабильностью.

Существует ряд других рисков, которые, хотя и не являются такими особыми для МНП ЮАР, но особенно остро ощущаемы этими фирмами из-за их ограниченных ресурсов. Например, чем больше МНП ЮАР сталкиваются с конкуренцией на рынке, тем больше трудностей испытывают в своем бизнесе, способности генерировать продажи и соблюдать свои финансовые обязательства. Уровень спроса и предложения на продукцию МНП ЮАР напрямую влияет на денежный поток и общую эффективность бизнеса.[7]

Отрасли, в которых задействованы МНП ЮАР, являются все без исключения источником повышенного риска. Например, в то время как производители сырьевых товаров подвержены непредсказуемым мировым тенденциям ценообразования, различным техническим спецификациям и стандартам экспортных рынков, эффективность работы МНП ЮАР является их главной целью.[6]

Внешняя торговля ЮАР очень сильно диверсифицирована — ни одна страна по состоянию на 2018 год не контролирует более 15% ни экспорта, ни импорта африканского государства. Основные партнёры по экспорту и импорту за 2020 год, приведены на рисунке 1.[3, 4]

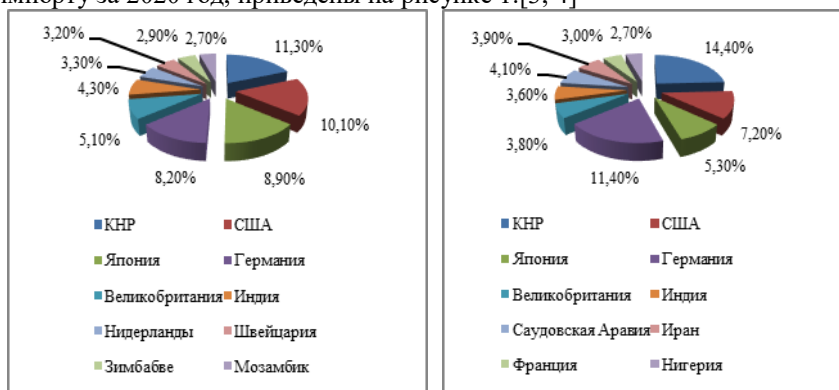


Рисунок 1 – Основные партнёры по экспорту и импорту в 2020 году

Ниже приведены некоторые общие рекомендации, которые помогут МНП ЮАР снизить вышеуказанные риски и улучшить свои шансы обеспечить получение финансовых средств.

Страхование экспортных кредитов является лучшим способом хеджирования риска, который может проявляться, в частности: конфискации, экспортирования товаров, войн, актов терроризма, нанесение ударов стихий природы, невозможность оплаты консигнаций и непостоянство валюты. Альтернативой к приему вне страхования экспортного кредита для МНП ЮАР может служить использование подтвержденного аккредитива, где Банк обслуживающий компанию страхует кредитный риск иностранного банка, выдавшего аккредитив.

Чтобы снизить операционный риск, МНП ЮАР в первую очередь должны быть платежеспособными. Если МНП ЮАР имеют отрицательный денежный поток, следует уведомить об этом кредитора, что это объясняется неустойчивым торговым циклом, а не неустойчивостью компании или завышением расходов. Финансовые коэффициенты и качество оборотных средств (товарно-материальных запасов и дебиторов) также будет предметом тщательного изучения. Если МНП ЮАР в состоянии поддерживать активы в актуальном состоянии, своевременно и надлежащим образом поддерживают низкий уровень запасов, это большая вероятность, иметь возможность получить заимствование значительно большее, чем стоимость своего капитала.

Во-вторых, МНП ЮАР не должны быть новичками в бизнесе. Они должны иметь хорошую репутацию и послужной список в своей конкретной отрасли, и быть способными продемонстрировать свою компетентность в ведении бизнеса на международном уровне. В-третьих, МНП ЮАР необходимо иметь хороший бизнес-план, который отражает приверженность компании сильному корпоративному управлению и включает реалистичную стратегию развития бизнеса.[3]

Некоторые из рисков, которые являются особым бременем для МНП ЮАР, составляют конкурентные угрозы и изменение спроса, которые мешают фирме зарабатывать. Эти риски лучше всего решать, участвуя в регулярных сессиях бизнес-планирования, чтобы показать кредиторам, что риски воспринимаются серьезно и что руководство МНП ЮАР готовы предпринять корректирующие действия, если их бизнес находится под угрозой. Риски, связанные с высокой концентрацией рынка, могут быть снижены, если МНП ЮАР диверсифицируют свою продуктовую базу или, по крайней мере, характеристики своего вида продукции. Инвентарный риск, в свою очередь, может быть снижен путем оформления страховки от возможности потерь или повреждений. Транзитный риск можно контролировать, даже если МСП проводят небольшие логистические

операции, исходя из тщательного выбора вида (видов) транспорта, налаживание прочных отношений с фактическими перевозчиками и обеспечение покрытия каждой сделки страховкой грузов. То же касается и МНП ввиду способности уделять внимание крупным логистическим операциям [4].

Таким образом, экспортное финансирование рассматривалось как важное звено в цепи развития рынка МНП ЮАР, в частности, в обеспечении такого финансирования от банков и других финансовых организаций [4]. Проведено исследование отдельных финансовых учреждений по вопросам финансирования экспорта для МНП ЮАР, и определены ключевые риски, которые обычно оцениваются с точки зрения кредиторов. Результатом является ценный набор руководящих принципов, которыми указанные компании могут следовать при подготовке своего бухгалтерского досье при обращении за финансовой помощью. Это в большинстве своем смягчает риски, которые в противном случае отстраняют заявителя от финансирования [6].

Список использованных источников:

1. Абрамова И.О., Фитуни Л.Л. Экономическая привлекательность и инвестиционный потенциал региона Африки к югу от Сахары // Экономическая глобализация и проблемы национальной и международной безопасности. 2015. №3 –167-173.
2. Сапунцов А.Л. Атрибутивность инвестиционной деятельности многонациональных предприятий ЮАР // Мировая экономика. 2015. – 4(125). –202-209.
3. Шубин В.Г. ЮАР в БРИКС: последняя по очереди, но не по важности // Вестник международных организаций, т.10, №2, 2015.- С. 229 -246.
4. SADC. [Официальный сайт Южноафриканского сообщества развития]. 1992. URL: <http://www.sadc.int/> (дата обращения: 12.11.2021).
5. Департамент инвестиционной и торговой политики ЮАР. [Официальный сайт Департамента инвестиционной и торговой политики ЮАР] // Правительство ЮАР. 2018. URL: <http://www.thedti.gov.za/> (дата обращения: 12.11.2021).
6. UNCTADStat – Table view – Foreign direct investment: Inward and outward flows and stock, annual, 1970–2018 [Electronic resource]. – URL: <http://unctadstat.unctad.org/wds/TableView/tableView.aspx> (accessed: 04.11.2021).
7. Where we are. MNT Group [Electronic resource]. – URL: <https://www.mtn.com/en/mtn-group/about-us/our-story/Pages/where-we-are.aspx> (accessed: 06.11.2021).
8. West Africa Region. Gold fields [Electronic Resource]. – URL: <https://www.goldfields.com/west-africa-region.php> (accessed: 13.11.2021).

Роботизация бизнес-процессов предприятия, как инструмент информационной логистики

А.Р. Азизова

студентка 4 курса НИЯУ МИФИ, Москва

E-mail: a2izowa.a@yandex.ru

научный руководитель: А.Н. Норкина

к.э.н., заместитель директора ИФТЭБ НИЯУ МИФИ, Москва

E-mail: ANNorkina@mephi.ru

Аннотация: Данная статья посвящена анализу, выявлению преимуществ и недостатков и оценке эффективности оптимизации информационной логистики предприятия, посредством внедрения технологий автоматизации бизнес-процессов, то есть роботизации бизнес-процессов.

Ключевые слова: роботизация бизнес-процессов, информационная логистика, автоматизация, оптимизация, искусственный интеллект.

Robotic Process Automation as an information logistics tool

Abstract: This article is devoted to analysis, identification of advantages and disadvantages and evaluation of the efficiency of optimization of information logistics of enterprise by means of robotic process automation.

Keywords: RPA, information logistics, automation, optimization, artificial intelligence.

Роботизация бизнес-процессов на предприятии является трендом сегодня во всем мире, а также и в России. Впервые она зародилась в начале 2000-х годов, но более широкое распространение получила в 2015 году.

RPA (Robotic Process Automation) - это технологии в области автоматизации сервисов управления офисными операциями.

На сегодняшний день, данные системы позволяет частично или даже полностью автоматизировать ручную работу на предприятии.

Что же лежит в основе технологий RPA? В их основе лежит программное обеспечение, которое легко адаптируется под нужды пользователя. Принцип работы ПО заключается в следовании установленному списку действий с использованием API, то есть программных интерфейсов или языка сценария. То есть, данное ПО

подключается через API и выполняет требуемые действия вместо человека. RPA является координирующей платформой, состоящей из множества модулей, каждый из которых является самостоятельным продуктом.

Другими словами, RPA - это современная технология автоматизации бизнес-процессов предприятия, основанная на использовании программных роботов. А робот в данном случае выполняет роль виртуального сотрудника.

Для полного рассмотрения данной темы необходимо провести анализ технологий роботизации бизнес-процессов и эффективности от их внедрения в организацию.

При рассмотрении вышеперечисленного будут решены главные вопросы этой темы, а именно:

- Исследование показателей эффективности внедрения RPA,
- Выявление преимуществ и недостатков, а также рисков RPA.
- В процессе исследования будут применены такие методы, как:
- Сбор статистики и отчетов аналитический предприятий по RPA,
- Сравнение имеющихся показателей.

По данным компании KPMG в России в период с 2017 по 2019 года количество компаний, тестирующих или уже внедривших RPA возросло в 2 раза. Среди них чаще всего фигурируют следующие области:



Рисунок 1 – Процент использования технологий RPA в различных индустриях

Данная диаграмма иллюстрирует, что лидерами в использовании технологий RPA являются телекоммуникационная (100%) и металлургическая (83%) индустрии, далее следует нефтегазовая индустрия (60%) и банки и финансовые институты (53%). И наименьший процент использования RPA наблюдается в розничной торговле (40%).

Какие же процессы на предприятии доверяются роботу? Чаще всего это следующие работы:

- Часто повторяющиеся процессы,
- Процессы, основанные на строгих правилах,
- Процессы с небольшим процентом исключения,
- Процессы с большим объемом информации, но при этом с невысокой сложностью,
- Стабильные процессы.

Одними из ключевых процессов автоматизации в организациях являются агрегирование отчетов, документооборот, сбор и обработка информации, подготовка отчетов. То есть все те процессы, за которые непосредственно и отвечает информационная логистика.

Главное правило информационной логистики: релевантная информации в нужном объеме, в нужное время, в нужном месте. Как раз-таки на этом правиле и строятся технологии RPA.

Стоит отметить, что роботизация и искусственный интеллект тесно связаны между собой, так как правильная автоматизация бизнес-процессов может быть достигнута только при слиянии машинного обучения и искусственного интеллекта. Но при этом, между этими двумя понятиями существует и различие. Если провести сравнение робота и искусственного интеллекта с человеком, то можно отметить следующее. Робот - это руки, а ИИ – интеллект человека. Однако сейчас технологии RPA активно развиваются. Современные RPA уже обладают аналитическими решениями тоже.

Функционал роботов крайне велик на сегодняшний день. Основные функции:

- Парсинг данных, то есть сбор и обработка информации,
- Рассылка запросов или необходимой информации,
- Агрегация ответов, то есть объединение данных в единую систему,
- Выдача результатов,
- Регистрация данных.

Такие решения зачастую строятся на основе Open Source продуктов. Open source - принцип разработки, который заключается в предоставлении свободного и открытого доступа к программному обеспечению и материалам, которые были использованным для его создания.

Рассмотрим подробнее риски при RPA и как их избежать.

Таблица 1 – Риски, сопровождающие RPA и способы из избегания

Риски	Как избежать
Ошибки при разработке сценария действий	Необходимо писать код, чтобы он был хорошо читаем; После разработки сценария необходимо неоднократно протестировать его, а также отслеживать его работу регулярно.
Ошибки при предъявлении требований	При наличии возможности привлекать экспертов для написания требований.
Сбой работы платформы	Постоянный контроль.
Невнесение актуальных изменений	При внедрении изменений в бизнес-процессы предприятия, нужно вносить необходимые изменения в работу роботов.

Помимо прочего, при внедрении и использовании роботов на предприятии стоит позаботиться о информационной безопасности.

При использовании технологий RPA выделяются 2 вида рисков, связанных с кражей информации:

1. Данную систему могут взломать злоумышленники и неправомерно использовать хранящуюся в системе информацию.

2. Уязвимые места системы, где пользователи также могут неправомерно авторизоваться и украсть информацию. Чаще всего данный риск наиболее осуществим при сбоях работы системы.

Поэтому при работе с данными системами необходимо позаботиться о кибербезопасности, а именно:

- Во-первых, необходимо проанализировать все возможные риски и слабые места.

- Построить структуру управления доступа к системе на основе проанализированных рисков, использовать шифрование в системе.

- И наконец, постоянных мониторинг и отслеживание за действиями робота.

Приобретение роботизированного программного обеспечения в организацию рекомендуется выполнять следующим образом:

1. В начале воспользоваться пробным периодом в течение ограниченного срока.

2. Подробно ознакомиться с документацией, форумами и различными видео-уроками по работе с ПО.

3. Обучение сотрудников работе с данным ПО.

4. Выполнение пилотного проекта.

5. Непосредственная покупка ПО.

При рассмотрении технологий RPA были выявлены следующие преимущества:

- Экономия времени на выполнение рутинных процессов. С помощью роботизации обыденных процессов можно делать больше, при этом не привлекая дополнительный персонал.

- Улучшение качества обслуживания, а именно сокращение ошибок, повышение точности работ, исключение влияния человеческого фактора.

- Сокращение числа рабочих на рутинных заданиях. Появляется возможность обучения и перевода работников на более сложные задачи предприятия.

- Сокращение затрат на оснащение рабочих мест и амортизацию оборудования.

Стоит отметить еще один положительный аспект от внедрения технологий RPA, который затрагивает мотивацию сотрудников. Для многих рабочих - это хорошая возможность найти себя в новом деле.

Однако не стоит забывать и о недостатках:

- Для поддержания таких технологий нужна техническая поддержка (а это дополнительные расходы для организации).

- Необходимо понимать, что недостаточно просто роботизировать бизнес-процессы, особенно если они находятся в хаосе. Также необходимо провести аудит бизнес-процессов и формализовать их. Поэтому для RPA необходимо иметь хорошо и точно документированные алгоритмы работы бизнес-процессов и в целом системы.

- Также стоит подумать о том, что даже если полностью роботизировать бизнес-процессы предприятия, то все равно необходимо иметь в запасе возможность поддержки работы системы при сбое роботизированного процесса.

- Недостаточно просто внедрить RPA и оставить это на самотек. Нужно постоянно контролировать и анализировать его деятельность, чтобы вовремя выявлять неточности и находить пути для улучшения его работы. Все это поможет минимизировать финансовые и репутационные риски и потери.

Помимо всего вышеперечисленного, существует также весомый недостаток, который не позволяет внедрить RPA на каждое предприятие - это стоимость.

Рассмотрим затраты на работа:

- Покупка лицензии,

- Покупка услуги разработки, а также технической поддержки системы.

Очевидно, что самое дорогостоящее - это приобретение лицензий и непосредственное внедрение работа на предприятие. А прочие затраты, характеризующиеся дальнейшей поддержкой работы системы, выходят гораздо дешевле.

Стоит отметить, что некоторые решения не требуют затрат на их поддержание. Это может быть связано с тем, что никаких изменений в программе в данное или ближайшее время не предвидется.

Если сравнить различные средства, применяемые для автоматизации различных бизнес-процессов, был сделан вывод, что самые значительные инвестиции идут на RPA.

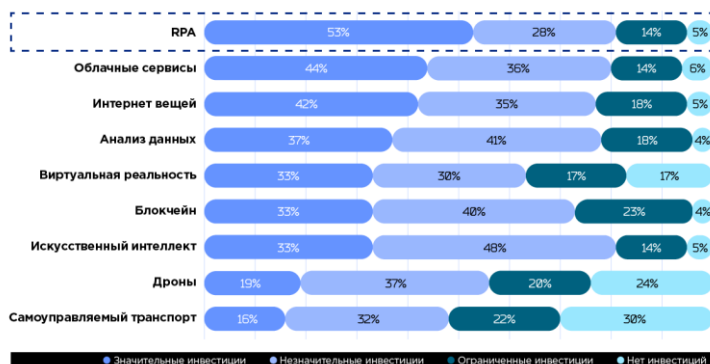


Рисунок 2 – Инвестиции в различные области, Grand View Research

По данным GVR (Grand View Research), ожидается совокупный годовой темп роста в 32,8% с 2021 по 2028 года. Это связано с текущей эпидемиологической ситуацией во всем мире, которая способствовала перенесению работы на дом и, следовательно, изменению работы бизнес-процессов на предприятии.

Что же тормозит организации от внедрения RPA?

- Во-первых, это непонимание или неведение преимуществ, консервативный взгляд на вещи;
- Высокая затратность данного процесса, не каждая организация может себе это позволить.

Чтобы оценить эффективность RPA необходимо прибегнуть к статистике. Рассмотрим результаты опроса HFS Research, которые проанализировали большое число компаний, внедривших технологии RPA. Исходя из результатов анализа был сделан вывод, что данные компании получили значительные выгоды и конкурентные преимущества.

Первый и наиболее значимый улучшенный показатель - это повышение качества (уменьшение количества ошибок и повышение качества исполнения рутинных задач), доля оптимизации которого составила 21%. Следом за ним оптимизировалась скорость работы (сокращение временных затрат бизнес-процессов) - 19%. Далее оптимизировалась функциональность (сокращение количества систем/окон, необходимых для

выполнения работ - 14%, автоматизация процесса (сквозная автоматическая обработка задач) – 11%). А также повысилась эффективность (сбор исторических данных для улучшения процесса, оптимизация бизнес-процесса за счет устранения лишних действий) - 7%.

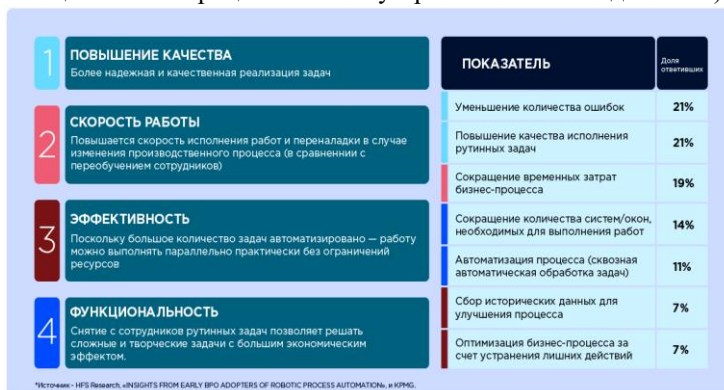


Рисунок 3 – Данные компании HFS Research

Следующий критерий рассмотрения эффективности - эффективность для бизнеса. Рассмотрим результаты анализа компании ABBYY, которые показывают, что внедрение решений RPA позволило многим компаниям уменьшить дополнительные расходы значительно.



Рисунок 4 – Данные компании ABBYY

Подводя итог, хочется затронуть перспективы развития данного направления.

Как уже было упомянуто выше технологиям RPA активно внедряются аналитические способности. Поэтому самой главной перспективой развития можно выделить слияние роботизированных технологий и искусственного интеллекта. В будущем, роботы будут способны самостоятельно принимать аналитические решения, а не просто выполнять рутинные и механические процессы.

В ходе работы были проанализированы анализ работы RPA, выявлены преимущества и недостатки, а также эффективность внедрения. Несомненно, процесс внедрения RPA на предприятие содержит сложную работу, требующую серьезного и детального анализа. Но необходимо отметить, что все сделанные мероприятия будут оправданы.

Список использованных источников:

1. Джон Будро, Р. Д. (2019). Реинжиниринг бизнеса: Как грамотно внедрить автоматизацию и искусственный интеллект. Москва: альпина публшер.
2. Бьёрн, А. (2003). . Бизнес-процессы. Инструменты совершенствования. Москва: РИА «Стандарты и качество».
3. Т.А., Р. (2001). Информационная логистика. Экзамен.
4. (2021). Автоматизация Роботизированных Процессов Объем Рынка, Доля И Анализ Тенденций Отчет По Типу, По Услугам, По Приложениям, По Развертыванию, По Организациям, По Регионам И Сегментам Прогнозы, 2021-2028. Grand View Research. Получено из <https://www.grandviewresearch.com/industry-analysis/robotic-process-automation-rpa-market>
5. Хенкель. (2 сентябрь 2019 г.). Непрерывное управление изменениями должно лежать в основе процессов автоматизации предприятия. Получено из HFS Research: <https://www.hfsresearch.com/research/continuous-change-management-must-underpin-enterprise-automation-journeys/>
6. Андреев, А. (18 августа 2020 г.). Первая система. Получено из Роботизация (RPA) давно пора или мы ещё не готовы?: <https://1-sys.ru/robotizatsiya-ili-rpa/>

Санкционный комплаенс как новый элемент KYC

В.Н. Морозова

студент 3 курса НИЯУ МИФИ, Москва

E-mail: varya.morozova@bk.ru

А.А. Хоченко

студент 3 курса НИЯУ МИФИ, Москва

E-mail: nastja.ho4enko@yandex.ru

Н.В. Морозов

к.э.н., доцент кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: nvmorozov@mephi.ru

Аннотация: В данной статье рассматривается санкционный комплаенс как главный инструмент защиты перед односторонними ограничительными мерами, исходящие от отдельных субъектов, таких как государства и организации. Необходимость обеспечить компетентное ведение внешне- и внутриэкономической деятельности становится ключевой при управлении в сложных геополитической ситуации, при постоянно существующих ограничениях. Делается вывод, что санкционный комплаенс становится фактором предотвращения рисков в бизнесе, обеспечивая клиентов качественными услугами на основе принципа «Знай своего клиента», в результате которого происходит тщательный анализ информации, проверка поступления денежных средств и истории проводимых сделок, что помогает выявить финансовые преступления и соблюдать правила ПОД/ФТ.

Ключевые слова: ПОД/ФТ, санкционный комплаенс, принцип «знай своего клиента».

Sanctions compliance as a new element of KYC

Abstract: This article examines sanctions compliance as the main instrument of protection against unilateral restrictive measures emanating from individual actors, such as states and organizations. The need to ensure the competent conduct of foreign and domestic economic activities becomes key when managing in a difficult geopolitical situation, with constantly existing restrictions. It is concluded that sanctioned compliance becomes a risk prevention factor in business, providing customers with quality services based

on the “Know your customer” principle, which results in a thorough analysis of information, verification of cash flows and the history of transactions, which helps to identify financial crimes and comply with AML / CFT rules.

Keywords: *AML / CFT, sanctioned compliance, “know your customer” principle.*

В рамках социально-политических отношений внимание мировой арены приковано к санкциям, то есть императивным нормам, запретам на установленную деятельность, которые вводятся различными государствами и международными субъектами, словно последняя попытка отстоять собственное мнение в сложной политической ситуации. Стоит отметить, что результатом данных действий является не только ухудшение отношений, складывающихся в сфере управления и политики, но и в частности, фиксируется негативное влияние на международные и российские экономические рынки. Под страхом наказания в результате несоблюдения санкций находятся даже те предприятия, которые не имеют внешних, то есть иностранных представительств, но имеют дело с контрагентами, которые попадают под запреты ряда стран, но не предоставляют информации об этом.

Вследствие данной напряженной ситуации последние годы наблюдается активный рост участия органов регулирования в осуществлении преследования и предупреждения финансовых преступлений по причине несоблюдения нормативно-правовых актов в области отмыwania денежных средств, финансирования терроризма и противоправных действий, выраженных в нарушении существующих санкций. Для защиты компаний от рисков необходим ряд систем и механизмов, эффективных в своем использовании, то есть качественном соблюдении норм ПОД/ФТ и санкций на местном и международном уровне. Таковым является санкционный комплаенс, который со временем стал важной частью системы соблюдения правовых требований к бизнесу, или способом защиты от незаконного взаимодействия с любыми компаниями, юридическими или физическими лицами, на которые распространяются санкции. В дополнение к проверке клиентов фирмам рекомендуется совершить проверку транзакций для выявления любых платежей, связанных с указанными физическими или юридическими лицами, то есть осуществлять качественную идентификацию клиентов, соответствовать основам процедуры «знай своего клиента».

Таким образом, чтобы соответствовать международным нормам по борьбе с отмыwанием денег и финансированием терроризма, что является ключевым и **актуальным** в финансовой системе, необходимо внедрить данные усиленные процедуры на первом этапе любых деловых отношений

при регистрации нового клиента, проверять санкционные списки и удостоверять личность, то есть соединять два понятия «санкционный комплаенс» и политику «знай своего клиента». Стоит обозначить *гипотезу* о том, что отсутствие или малоразвитость комплаенс-системы приведет к росту финансовых потерь и невозможности проведения результативного внутреннего контроля.

Однако важным будет обратить внимание на значение слова «санкция», поскольку единого мнения о значении данной категории не существует в научных кругах, хотя приводятся различные понятия в международном праве, включая Устав ООН, и в российском праве. Так создатель Института исследований мира, норвежский основательно дисциплины конфликтов, Й. Галтунг, сформулировал наиболее полное четкое мнение, утверждая, что санкция есть ни что иное, как «действия одного или нескольких других акторов, предпринятые по одной или обоим из следующих целей: наказать их, лишив чего-то ценного, заставить подчиняться определенным нормам.» Действительно, ученый делает акцент не на вопросе взыскания, а на подчинении, как ключевым аспектом существования данной системы порицания, причем исключительно в экономической сфере как приоритетной. На ряду с зарубежным опытом рассмотрим взгляды советского и российского правоведа в области международного права, профессора, И. И. Лукашука, которые имели отличительную особенность, заключаемая в наличии разграничений между терминами «санкция», источником которой служат международные субъекты, или акторы, и «ограничительные меры» со стороны отдельных государств, как индивидуальных методов принуждения. [6] Де-факто в жизни общества стирается невидимая граница определений, поскольку вопросами применения санкций в современном мире, на последних стадиях процессов занимают конкретные страны, а не Организация Объединенных Наций, как первоисточник и законный владелец термина «санкции». На основе сравнительного анализа разграничивать сущности нецелесообразно, поскольку остается вопросом юридической грамотности и деликатности, но по-прежнему носит обязательный характер для всех субъектов на мировой арене.

Возрастающая сложность, строгость регулирования и непредсказуемый характер глобальных режимов поднимают планку соблюдения санкций, которые становятся связанными с рынками. Аппарат управления каждой страны используют первое, как фактор воздействия и проникновения в деятельность отдельных игроков, ограничивая экономические возможности глобализации. Ошибки, связанные с нарушением запретов, то есть санкциями обходятся бизнесу очень дорого, при условии постоянно развивающихся нормативных требованиях во всем мире.

Преимуществом категории является ее открытость, поясняя, можно утверждать, что санкционные списки обычно предоставляются в открытом бесплатном доступе, через любой браузер. Таким образом, компании должны обратить свое внимание на них до начала деловых взаимоотношений с новым клиентом, чтобы убедиться, что закон не нарушается. Кроме того, санкционные списки должны быть важной частью стратегии ПОД/ФТ любого финансового учреждения для осуществления задач в рамках политики «знай своего клиента». По статистике, предоставленной Deloitte, отмечает тот факт, что треть сотрудников видит сложность в широком спектре данных, с постоянным расширяющимся списком лиц. [1] Эти проверки обычно используют в первую очередь автоматизированные базы данных, но слишком часто последующий поиск предупреждений, генерируемых с помощью автоматических инструментов, должен проводиться вручную. Этот процесс занимает много времени и может быть дорогостоящим из-за ручного досмотра, но немало важным остается образованность сотрудников. Около половины опрошенных обеспокоены тем, что работники, или человеческий капитал, задействованный в производстве, недостаточно осведомлены о требованиях соблюдения санкций для применения на практике.

На основе данных крупной аудиторской компании KPMG, существующая система проверки способна дать до 95% ложных предупреждений, что случается из-за большого количества платежей, постоянно расширяющегося списка санкций, и как результат наблюдается задержка при проверке клиентов и их финансовых операций.[3]

Несмотря на то, что санкционные списки понятны для восприятия, но на практике это большой объем данных, так как там перечислены не только имена, они также включают возможные местоположения. Учитывая, что большинство организаций связаны с большим количеством клиентов ежедневно, проверка санкционных списков вручную становится практически невозможной задачей. Хотя сторонняя проверка проводится только на основе готовых баз данных, с которыми сравнивается информация и устанавливается факт верности по всем параметрам, все же подрывается корректное выполнение принципа «знай своего клиента», создавая новые сложности.

Обобщая все вышесказанное, можно выделить две фундаментальные проблемы современного бизнеса в условиях санкций, служащие основаниям для возникновения рисков. Во-первых, это отсутствие в компаниях четкой политики по соблюдению санкций. Во-вторых, недостаточное количество существующих образовательных программ и курсов, повышающих квалификацию в области нормотворческих знаний. Анализируя первую проблему, важно уточнить, что у многих компаний,

которые попадают под санкционные штрафы, система комплаенса либо не была предусмотрена и отсутствовала в структуре контроля, либо находилась на ранних стадиях развития, что повлекло к ряду нарушений, негативно сказавшихся на эффективности управления. В связи с этим, необходимо контролировать в организациях развитие санкционного комплаенса, в соответствии с этим, необходимо начать надо с руководства компаний, повышения их правовой культуры, то есть прививания важности соответствия нормативно-правовым требованиям законодательства и регуляторов. Необходимо уделять должное внимание такому важному элементу, как принципу «знай своего клиента», учитывая сложный характер санкционных списков. Для решения второй обозначенной проблемы существует такой путь, как обязать бизнес сроком один раз в шесть месяцев давать сотрудникам возможность, а иногда изменять характер с рекомендательного на обязывающий, повышения квалификации в знаниях по правовой базе, а также организовывать тренинги для сотрудников по данной тематике и разрабатывать различные методологические пояснения в области санкционного комплаенса.

Для того чтобы оценить важность внедрения санкционного комплаенса в организации лучше всего рассмотреть реальную историю с российской судоходной компанией «Гудзон», которая была включена в санкционный список США из-за недостаточного развития, или отсутствия санкционного комплаенса в организации. [5] «Гудзон» нарушила санкции, введенные Советом безопасности ООН против Северной Кореи, суть которых заключалась в том, чтобы не допустить поставок из-за рубежа сырья, валюты и металлов. Компания вела сотрудничество с КНДР по поставкам нефти, перекачивала ее с российского судна на северокорейские в открытом море. Северокорейское судно, на которое с российского была осуществлена перекачка нефти, ранее было включено в санкционный список США и ООН. Таким образом, вследствие некомпетентности сотрудников компании и их безответственного отношения к такой значимой системе как комплаенс, компания потеряла возможность для ведения своего бизнеса, ведь все средства на ее счетах были заморожены и ни один порт больше не сможет принять корабли компании «Гудзон». История этой компании показывает важность и необходимость наличия системы санкционного комплаенса в организациях.

Таким образом, хотелось бы отметить, что политика меняется, и бизнес всегда должен быть в состоянии адаптироваться к определенным условиям, чтобы сохранить свою стабильность. Благодаря имеющимся ресурсам,

компетенциям и накопленному опыту крупные компании должны понимать важность внедрения санкционного комплаенса в свои организации. Это позволит рассматривать долгосрочные выгоды для бизнеса и приведет к тому, что руководство сможет принимать аргументированные решения на счет предстоящих сделок и исключать риски, связанные с ведением бизнеса с клиентами, которые указаны в санкционных списках.

Список использованных источников:

1. Facing the sanctions challenge in financial services. A global sanctions compliance study / авт. Deloitte. - [б.м.] : Deloitte, 2009 г..
2. Know Your Customer in banking [В Интернете] / авт. Group Thales // Digital Identity and Security. - 2020 г..
3. Sanctions compliance: Plotting a new course for sanctions compliance with technology solutions that drive efficiency and effectiveness. [В Интернете] / авт. International KPMG // KPMG. - 2020 г..
4. We've all heard of sanctions, but how could they impact your business? Here's all you need to know about sanctions. [В Интернете] / авт. KYC-Chain // Sanctions 101. - 5 февраль 2020 г..
5. Международные санкции: что следует учитывать российским компаниям? [Конференция] / авт. С.В. Гландин // «Санкционный комплаенс как способ минимизации рисков для бизнеса».. - 31 марта 2021.
6. Санкции и односторонние ограничительные меры: проблема различия терминов и тождественности явлений [Статья] / авт. Пятибратов И.С. // Вестник Финансового университета. - 2020 г..
7. Санкционный комплаенс в 2019 г.: тенденции и новые веяния [Журнал] / авт. INSIGHT LEGAL. - 2019 г..

Сервисы веб-аналитики как инструмент маркетинга

М.М. Джураев

студент 4 курса НИЯУ МИФИ, Москва

E-mail: matindzhuraev@gmail.com

Е.Р. Мысева

заместитель начальника отдела правового и методического
обеспечения учебного процесса ИФТЭБ НИЯУ МИФИ, Москва

E-mail: ERMyseva@mephi.ru

Аннотация: В статье рассмотрена актуальность использования сервисов веб - аналитики как инструмент маркетинга. Проведен сравнительный анализ функциональности двух сервисов - Яндекс.Метрика и Google Analytics. Рассмотрено преимущество сквозной аналитики. Был сделан вывод о недостаточности использования только сервисов веб – аналитики для отслеживания полного пути потребителя до совершения им покупки.

Ключевые слова: веб-аналитика, сквозная аналитика, конверсия, глубина просмотра, источники трафика, электронная коммерция, CRM – система, система колтрекинга, Яндекс.Метрика, Google Analytics, ROMI.

Web analytics services as a marketing tool

Abstract: In the article the relevance of using web analytics services as a marketing tool is discussed. The functionality of two services - Yandex.Metrica and Google Analytics is analysed and compared. The advantage of end-to-end analytics is considered. Concluded insufficiency of usage of only web analytics services to track the full path of the consumer before he making a purchase.

Keywords: web analytics, end-to-end analytics, conversion, page depth, traffic sources, e-commerce, CRM system, call tracking system, Yandex.Metrica, Google Analytics, ROMI.

Привлечение потребителей и продвижение бренда (товаров или услуг) сейчас не проходят без использования интернет – технологий. Сегодня успешное ведение бизнеса предполагает непрерывную борьбу за потенциальных клиентов, активно пользующихся сетью. Ведь все больше потенциальных покупателей ежедневно получают необходимую им информацию по интернету. Наличие сайта – это базовая необходимость для

любой компании, претендующей на успех. Однако, для того, чтобы конкретно понимать, как заинтересовать клиента и повысить онлайн-присутствие, мало просто создать сайт и наполнить его интересным контентом. Чаще всего компании идут простыми путями, просто запуская контекстную, либо таргетированную рекламу, не исследуя целевую аудиторию и маркетинговые показатели. В итоге рекламный бюджет расходуется, а заметного эффекта от продвижения не наблюдается.

Ведение рекламной кампании всегда подразумевает под собой развитие, постоянные тесты гипотез, каналов и выявление наиболее-profitных. Без аналитики невозможно узнать сколько вам стоит заявка, откуда она пришла и вообще какой у вас возврат инвестиций в рекламу. Просто настроить что-то и ждать результата - самая большая ошибка в интернет-маркетинге, ведь он полностью строится на сборе статистики и оптимизации. Поэтому веб-аналитика является важной частью аналитической функции маркетинга. Анализ статистических данных посещений и просмотра страниц сайта даёт богатую информацию для улучшения корпоративного веб-ресурса, изучения поведения пользователей, а также оценки результативности каждого канала привлечения клиентов.

Актуальность темы объясняется и положительной динамикой объема как глобального, так и российского рынка e-commerce. Агентство E – Promo в своем отчете «E – commerce 2021» дала прогноз, что в период с 2020 по 2025 год со средним ежегодным приростом 10,5% объем мирового рынка e-commerce в 2025 году составит 7 трлн. долларов. А объем российского рынка e-commerce - 7,5 трлн руб. со средним приростом 22,8% ежегодно в периоде 2020 – 2025 гг.

Соответственно, растет и объем рынка интернет - рекламы. Согласно отчету PWC, в 2020 году объем рынка интернет – рекламы в России увеличился на 5%, а к 2024 году при среднегодовых темпах роста 8%, составит 5,4 млрд. долларов (диаграмма 1).

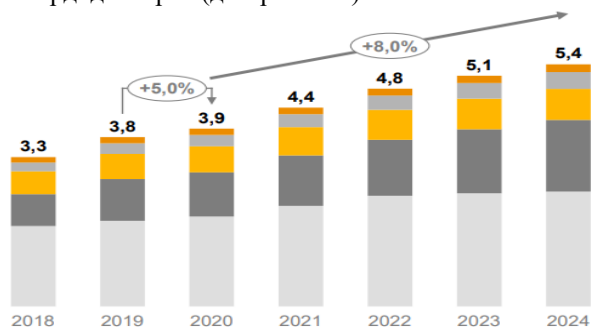


Диаграмма 1 – Динамика объема российского рынка интернет-рекламы

В том же отчете «Е – commerce 2021» Е – Promo, используя данные Ассоциации Коммуникационных Агентств России (АКАР), спрогнозировала, что доля интернет-рекламы в общем объеме российского рекламного рынка на 2021 год будет составлять 55%.

Сейчас, по результатам первого полугодия 2021 года, согласно данным АКАР, доля интернет-рекламы составила 53,44% (диаграмма 2), динамика к аналогичному периоду 2020 года – +27%.

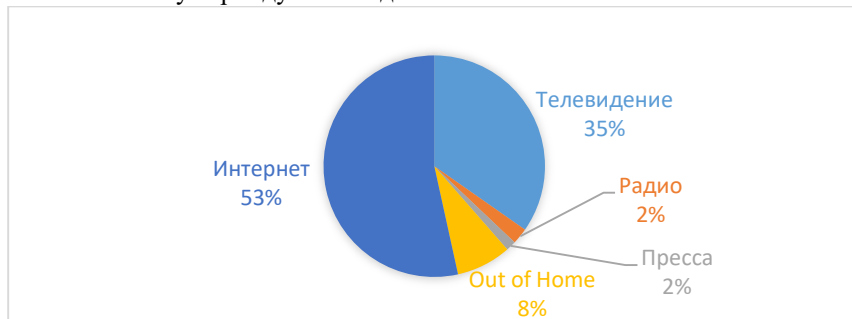


Диаграмма 2 – Доля сегментов рекламы в общем объеме российского рекламного рынка

Следовательно, сегодня, когда большая часть ресурсов для продвижения инвестируются в интернет, сервисы веб-аналитики являются необходимым инструментом маркетинга.

Для полного определения роли и места сервисов веб-аналитики как инструмент маркетинга, в статье будут рассмотрены их задачи и функции, а также сравнительный анализ двух таких сервисов. Благодаря этому можно решить один из главных вопросов данной проблематики, а именно определение возможностей систем веб-аналитики как маркетинговый инструмент.

Веб-аналитика – это измерение, сбор и анализ информации о посещениях веб-ресурса, на основании которой принимаются решения по улучшению стратегии продвижения.

Для сбора статистики и формирования необходимых для анализа отчетов используются сервисы веб-аналитики. Основные задачи, которые решаются с применением сервисов веб-аналитики:

- Определение целевой аудитории
- Сегментирование аудитории по разным признакам
- Оптимизация бюджета для рекламы
- Оптимизация контента
- Поиск оптимальной стратегии продвижения

Наиболее популярными сервисами веб-аналитики в России являются Яндекс.Метрика и Google Analytics. Они обладают достаточно широким функционалом, чтобы формировать отчеты по основным показателям (таблица 1) для выполнения вышеперечисленных задач.

Таблица 1 – Сравнение функционала сервисов

Функциональность/Показатель	Яндекс.Метрика	Google Analytics
Анализ посещаемости (общий трафик, число новых посетителей, количество просмотров и т.д.)	+	+
Источники трафика (ресурсы, с которых был совершен переход)	+	+
Отказы	+ отказом считается визит, длительностью менее 15 секунд	+ отказом считается посещение пользователем только одной страницы без выполнения каких-либо действий
Конверсии	+	+
Глубина просмотра (число просмотренных страниц)	+	+
Карта поведения пользователей	+	+
Вебвизор	+	-
Проведенное время на сайте	+	+
География посетителей и их демографические характеристики	+	+
Электронная коммерция (определение популярных товаров, категорий, количество совершенных заказов, доход от заказов)	+	+
Возможность интеграции с рекламными системы	+ Яндекс.Директ, Facebook, Google Ads	+ Google Ads
Сквозная аналитика внутри самого сервиса	+	-
Сбор данных из мобильного приложения	-	+

Как видно из таблицы, основные функции есть у обоих сервисов. Важным преимуществом Google Analytics является возможность сбора данных не только из сайтов, но и из мобильных приложений. В Яндекс.Метрике нет такой возможности, для этого у компании Яндекс есть отдельный сервис - AppMetrica.

Стоит отметить функцию «Вебвизор» Яндекс.Метрики. Она позволяет анализировать поведение пользователя, фиксируя его действия в виде краткого описания и видеофайла. Основной целью просмотра вебвизора является повышение конверсии страниц. Видеозапись посещения показывает:

- движение курсора мыши
- клики
- нажатия на клавиатуру и заполнение форм
- выделение и копирование текста
- прокрутка страницы
- перемещение между страницами.

Просмотрев поведение пользователя, можно решить следующие задачи:

- тестирование дизайна
- выявление ошибок в структуре веб-ресурса
- улучшение юзабилити (удобство пользования веб-ресурсом и его элементами)
- улучшение контента веб-ресурса.

Кроме различий, представленных в таблице, есть различия по стоимости использования данных сервисов. Яндекс.Метрика предоставляется полностью бесплатно, а в Google Analytics есть и платный, бесплатный варианты. Для пользователей бесплатного тарифа устанавливается квота в 10 млн. событий. Риск использования бесплатного тарифа в том, что отчеты могут формироваться не из 100% имеющихся данных, если размер запроса превышает квоту. Поэтому для полноты картины часто используются оба сервиса.

Обычно потребитель не сразу совершает покупку. Например, он может зайти на сайт, изучить информацию о продукте, не сделав заказ или покупку покинуть сайт. В этом случае, с точки зрения веб-аналитики можно сделать разные выводы, например, контент сайта нерелевантный запросу пользователя.

Однако этот посетитель через некоторое время может вернуться на сайт и решиться на покупку. Сервисы веб-аналитики сами по себе не имеют возможности отследить такого рода сложный маршрут потребителя. Для таких целей используется сквозная аналитика. Принцип сквозной аналитики заключается в том, чтобы отследить путь потребителя от нажатия на объявление до совершения покупки.

Интегрируя сервисы веб-аналитики, рекламные системы, CRM – системы и системы коллтрекинга, создаются решения для сквозной аналитики. При первом посещении потребителя на сайт в CRM – системе ему присваивается индивидуальный идентификатор. При каждом последующем посещении сайта система распознает пользователя и фиксирует его действия под ранее присвоенным ему уникальным аккаунтом.

Система сквозной аналитики в едином окне собирает данные (рисунок 1) по затратам на рекламные каналы (из рекламных систем), звонкам (из системы коллтрекинга), источникам трафика, посещаемости, целям и транзакциям (из сервисов веб-аналитики), продажам (из CRM) и показывает, сколько денег тратится на каждый рекламный канал и какая отдача от каждого из них. На основании этих данных можно отслеживать один из важных показателей – ROMI (рентабельность вложений в маркетинг) и эффективно управлять рекламным бюджетом.

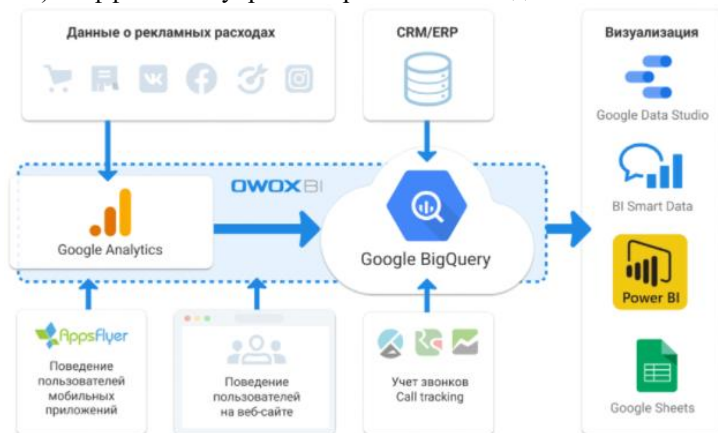


Рисунок 1 – Схема объединения данных для сквозной аналитики на примере аналитической платформы OWOX BI

В этом году (2021 г.) в Яндекс.Метрике появились возможности для сквозной аналитики внутри самого сервиса. То есть можно формировать отчеты, используя данные с разных интегрированных систем прямо в Метрике.

Ниже приведена схема воронки продаж, которую позволяет отслеживать функция «Сквозная аналитика» Яндекс.Метрики (рисунок 2).



Рисунок 2 – Воронка продаж, которую позволяет отслеживать функция «Сквозная аналитика»

Подводя итоги, можно сделать следующие выводы:

- Сервисы веб-аналитики являются необходимым инструментом маркетинга. С применением таких сервисов можно решать разные маркетинговые задачи, от определения и сегментации аудитории до оптимизации маркетингового бюджета. Тем самым, повышая конкурентоспособность компании.

- Недостаточно использовать только сервисы веб-аналитики для полного отслеживания от первого клика на объявления до совершения покупки. Для этого используется система сквозной аналитики, где сервисы веб-аналитики являются частью этой системы.

В связи с развитием технологий машинного обучения и больших данных, которые внедряются в компаниях, системы веб-аналитики становятся все более актуальными для повышения эффективности инициатив маркетинга.

Список использованных источников:

1. E-Promo Аналитический отчет по результатам исследования "E commerce 2021". - 2021 г..
2. PWC Исследование российского рынка programmatic buying. - 2021 г..
3. Демкина О.В. Шаламова Н.Г. Исследование роли веб-аналитики в повышении эффективности деятельности организации [Журнал]. - [б.м.] : / О.В.Демкина, Н.Г. Шаламова // Вестник университета., 2019 г.. - №5, -С. 56-61.
4. Кошик Авинаш Веб-аналитика 2.0 на практике. Тонкости и лучшие методики (+ CDRом) [Книга]. - [б.м.] : М.: Диалектика.
5. Объем рекламы в средствах ее распространения в январе-июне 2021 года [В Интернете] // Ассоциация Коммуникационных Агенств России.-

2021г.-ноябрь2021г.

https://www.akarussia.ru/knowledge/market_size/id9802.

6. Сквозная аналитика: система, примеры и инструменты [В Интернете] // Центр развития компетенций в маркетинге НИУ ВШЭ. - 2020 г.. - ноябрь 2021 г.. - <https://marketing.hse.ru/news/397981286.html>.
7. Справка - Google Analytics [В Интернете].-ноябрь 2021 г. <https://support.google.com/analytics/?hl=ru>.
8. Яндекс.Метрика [В Интернете] // Яндекс справка. - ноябрь 2021 г.. - <https://yandex.ru/support/metrika/>.

Современные инструменты по выявлению подозрительных клиентов

А.А. Суркова

аспирант 1 курса НИЯУ МИФИ, Москва

E-mail: aleksandra270198@mail.ru

Д.В. Домашова

к.э.н., доцент кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: janedom@mail.ru

Аннотация: В статье рассматриваются вопросы обнаружения мошенничества или действия, связанные с ОД/ФТ. Проведен анализ имеющихся на рынке систем, которые позволяют улучшить процессы ПОД/ФТ в коммерческих организациях. Инструменты мониторинга подозрительных клиентов позволяют реализовать безопасность систем и хранилищ данных. Проанализирован функционал данных систем на примере Palantir и SAS и запросов API.

Ключевые слова: ПОД/ФТ, машинное обучение, отслеживание клиентов, подозрительные операции.

Modern tools for identifying suspicious customers

Abstract: The article discusses the issues of fraud detection or actions related to ML/FT. The analysis of the systems available on the market that allow improving AML/CFT processes in commercial organizations is carried out. Monitoring tools of suspicious clients allow you to implement the security of systems and data warehouses. The functionality of these systems is analyzed on the example of Palantir and SAS and API requests.

Keywords: AML/CFT, machine learning, customer tracking, suspicious transactions.

Введение

В современном мире с развитием технологий коммерческие и кредитные организации сталкиваются со случаями мошенничества и отмывания денежных средств. Поэтому они вынуждены создавать внутренние подразделения для отслеживания подозрительных действий и должной защиты персональных данных клиентов и компании.

Рынок технологий с каждым годом стремится упростить работу своих заказчиков и создает различные аналитические технологии, основанные на машинном обучении и мобильном мониторинге, которые будут соблюдать требованиям по противодействию отмыванию денежных средств.

Машинное обучение в сфере ПОД/ФТ

Машинное обучение давно облегчает деятельность всех компаний и банков, и ему было найдено применение в борьбе с отмыванием денежных средств. Благодаря особым алгоритмам можно внедрять технологии по: исследованию клиентов, их покупки, периоды, затраты и источникам происхождения денег клиента, а также отслеживанию транзакций.

На данный момент сложно создать стопроцентный автоматизированный продукт и обучить программу на выявление всех особенностей, поэтому важно развивать проекты с возможностью для адаптации.

По последним данным Sanction Scanner [1] машинное обучение позволит сократить затраты компании на мониторинг всех транзакций и заявок клиентов, так как искусственный интеллект отклонит 98% некорректных случаев выявления подозрительных операций и позволит специалистам сконцентрироваться на 2%, которые будут тщательно изучены и предотвращены.

Искусственный интеллект достигнет такого результата благодаря применению таких методов:

- Статистический анализ персональных данных клиентов для составления рейтинга вероятных преступников, что позволит сократить временные затраты
- Обработка данных с целью очищения от информационного мусора в анкетах клиентов, что также сэкономит производительность.

Обнаружение изменений в поведении клиентов

Модели машинного обучения могут быть разработаны, чтобы помочь обнаруживать изменения в поведении клиентов путем анализа их транзакций. Этот метод может быть реализован для обогащения существующих устройств, основанных на мониторинге с помощью правил. Это позволит выявлять клиентов с подозрительной активностью на этапе расследования. Действительно, в традиционных устройствах поведенческого анализа не хватает новых шаблонов, которые могут возникнуть, потому что отмыватели денег, как правило, на шаг впереди.

Рассмотрим основные особенности систем AML, представленных на рынке.

Palantir

Данная система создает продукты для анализа реальных данных на основе машинного обучения, и передовые сетевые модели рисков

позволяют легко и точно связывать клиентов, сети и неизвестных контрагентов. Это дает компании прочную основу для мониторинга. Клиент получает отчет - файл клиента, который может динамически обновляться в рамках функций ПОД/ФТ.

Palantir использует гибридный подход [2], предоставляя комплексные готовые модули, сценарии и модели, обеспечивая при этом гибкость, необходимую для удовлетворения нормативных требований, определяемых вашей конкретной клиентской базой и устойчивостью к рискам. В конечном счете это повышает точность и эффективность оповещения, обеспечивая при этом более качественные автоматизированные отчеты для регулирующих органов.

Изначально построенный для использования правительственными разведывательными и оборонными ведомствами, с учетом соображений конфиденциальности и гражданских свобод, Palantir Foundry включает в себя беспрецедентные, детализированные средства контроля безопасности.

Все данные шифруются как при передаче, так и в состоянии покоя, и Palantir предлагает точность проверки системы управления доступом на основе ролей, чтобы все команды могли получать доступ к необходимым данным и обмениваться ими без ущерба для безопасности.

Palantir решает такие задачи как:

- Мониторинг транзакций;
- Расследований и финансовой разведки;
- Оценка рисков клиентов и транзакций;
- Проверка санкций;
- Расширенная и комплексная проверка клиентов;

Palantir является ведущей в отрасли инфраструктурой коммерческих данных и обеспечивает основу для решения финансовых преступлений следующего поколения в качестве готового решения. Он включает в себя стабильную, масштабируемую серверную часть, созданную для сложных сред обработки данных.

Решение по мониторингу может быть быстро внедрено и удовлетворить потребности в ускоренные сроки в несколько недель, а не лет. Palantir обеспечивает базу данных для продолжения цифровой трансформации. По мере того, как мир меняется, инфраструктура данных предназначена для адаптации и масштабирования в соответствии с меняющимися потребностями организации.

Данная система — это полностью интегрированное решение с высокой скоростью и множеством функций для оптимизации общей стоимости владения, даже при локальном развертывании. Благодаря упаковке набора универсальных приложений организации экономят на рабочей силе, техническом обслуживании, поддержке и эксплуатационных расходах.

Все данные могут быть безопасно экспортированы в отраслевые стандарты, открытые форматы для использования в других системах, и вся логика, используемая для интеграции данных наших клиентов, доступна и может использоваться в любой среде.

SAS

Данный сервис быстро выявляет возникающие сложные угрозы ПОД/ФТ с помощью алгоритмов и методов, которые автоматически строят сетевые диаграммы и выявляют скрытые взаимосвязи. Расширенная аналитика позволяет изучать клиентов, просматривая несколько источников данных, а затем учитывает несоответствия, ошибки, сокращения и неполные записи, чтобы помочь определить, относятся ли они к одной и той же сущности.

В системе реализован гибридный подход к мониторингу транзакций [3], который сочетает проверенные правила обнаружения известных рисков с передовыми аналитическими методами, включая машинное обучение, глубокое обучение и искусственный интеллект, для выявления неизвестных рисков и скрытых взаимосвязей. Пользователи с правами администратора могут создавать, управлять и обновлять определяемые программой правила мониторинга с помощью пользовательского встроеного конструктора сценариев.

SAS помогает компаниям достичь точности модели более чем на 90%, снизить количество ложных срабатываний до 80%.

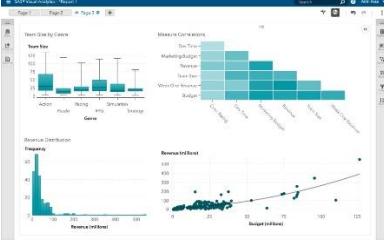
Проект позволяет просматривать транзакции и клиентов в пакетном режиме по широкому спектру списков наблюдения. Алгоритм подсчета очков – с правилами фильтрации для конкретной организации, уникальной аналитикой сопоставления имен, возможностью многоязычного скрининга и консолидацией предупреждений – генерирует высококачественные попадания с низким уровнем ложных срабатываний.

SAS по борьбе с отмыванием денег обеспечивает полную наглядность сценариев, которые вызывают красные флажки, и предоставляет четкие объяснения относительно генерации предупреждений для аудита результатов.

Сравнительный анализ Palantir против SAS

Таблица 1 – Palantir против SAS

 Palantir	 SAS

Разработано для таких отраслей, как автомобилестроение, управление делами, киберзащита, финансы, комплаенс, инсайдерские угрозы, страхование, правоохранительные органы и юридическая разведка.	SAS Visual Analytics подходит для малого и среднего бизнеса или крупных организаций во всех отраслях. Нацелен на использование небольшой команды, отдела, нескольких бизнес-единиц или корпоративного уровня.
	
Интеграции	
	Hadoop
	Импала
	Microsoft 365
	Microsoft Power BI
Microsoft Power Query	
Палантир Аполлон	
Палантир Готэм	
	SAS Analytics для Интернета вещей
	SAS по борьбе с отмыванием денег
	SAS Business Intelligence
Развертывание	
SaaS	SaaS
Служба поддержки	
	Электронная почта / Служба поддержки
	FAQ / Форум
База знаний	База знаний
	Поддержка по телефону

	24/7 (Live Rep)
	Чат
Обучение	
Документация	Документация
	Онлайн
	Лично

Сравнительная таблица 1 показывает, что SAS более доступная и открытая система, которая предоставляет учебные материалы пользователям, сотрудничает с другим проектами. В Palantir есть только внутренние продукты, что дает понять, что данная система закрытая и не готова делиться своими алгоритмами. Именно эта уникальность и интересует их целевую аудиторию.

По данным Cuspera [6] рейтинг обеих систем идентичен и составляет 4.1. Платформа SAS предлагает лучшее корпоративное решение, а Palantir техническое. А именно: в Palantir преобладают функционал по поддержке, визуализации и работе с данными, тогда, когда SAS предлагает лучшие отчетности и аналитику сетей.

API

Acuris Risk Intelligence Search API 3.0 позволяет запрашивать отдельных лиц и компании по собственной базе данных ПОД/ФТ. API обеспечивает доступ к следующим наборам данных: список политически важных лиц, санкции, списки нормативных требований, профили интересов, несостоятельность, дисквалифицированный директор, список нормативных требований.

Система позволяет запрашивать наборы данных в базе, используя набор параметров поиска. Он доставляется через HTTP, соответствует принципам RESTful и возвращает объекты JSON.

Сейчас реализована новая улучшенная модель данных с более детальным содержанием и более строгими типами данных. Превосходный алгоритм сопоставления, который был обучен с помощью машинного обучения и может похвастаться такими функциями, как сокращения, псевдонимы, отчества, устранение шумовых слов, синонимы, опечатки, похожее по звучанию имена и транслитерации, и это лишь некоторые из них. Было показано, что новый алгоритм снижает количество ложных срабатываний на 50%.

Заключение

Были рассмотрены технологии нового поколения, реализованные для ПОД / ФТ, такие как алгоритмы анализа поведенческих данных, которые обнаруживают слабые сигналы об отмывании денег или финансировании терроризма. С увеличением риска несоблюдения некоторые

технологические компании предлагают новые технологически сложные подходы, чтобы соответствовать действующим нормам. Упомянутые выше системы применили эти подходы для улучшения своего уникального программного решения.

Создаются платформы для интеграции, управления и защиты данных, поверх которых накладываются приложения для полностью интерактивного управляемого человеком и машинным анализом.

Мы на пороге будущего, в котором коммерческие и кредитные организации могут использовать данные для работы в соответствии с их задумкой - для выполнения возложенных на них поручений, для предоставления ценности клиентам и для защиты данных.

Список использованных источников:

1. Sanction Scanner. How AI and Machine Learning Help Prevent Money Laundering? – [Электронный ресурс]. – URL: <https://sanctionscanner.com/blog/how-ai-and-machine-learning-help-prevent-money-laundering-64> (Дата обращения 18.11.2021)
2. Palantir – [Электронный ресурс]. – URL: <https://www.palantir.com/about/>
3. SAS. Analytics Software & Solutions – [Электронный ресурс]. – URL: https://www.sas.com/en_us/home.html
4. Sanction Scanner. AML Transaction Monitoring Software – [Электронный ресурс] – URL: <https://sanctionscanner.com/aml-transaction-monitoring>
5. Acuris Risk Intelligence Search API 3.0 – [Электронный ресурс] – URL: <https://iongroup.com/analytics/data-portal/apis-data-feeds/acuris-aml-api/documentation/>
6. Compare SAS® Analytics for IoT vs Palantir Foundry – [Электронный ресурс] – URL: <https://www.cuspera.com/compare/sas-analytics-for-iot-vs-palantir-foundry/1791/15600>

Современные информационные технологии в обеспечении информационной безопасности логистических процессов

В.Г. Гредычан

студент 4 курса НИЯУ МИФИ, Москва

E-mail: vikagredychian@gmail.com

научный руководитель: А.Н. Норкина

к.э.н., заместитель директора ИФТЭБ НИЯУ МИФИ, Москва

E-mail: annorkina@mephi.ru

Аннотация: В данной статье рассмотрены понятия и актуальность информационной безопасности в логистических процессах, рассмотрены основные информационные технологии для обеспечения этой безопасности. Рассмотрена система менеджмента безопасности в логистике как основа обеспечения информационной безопасности в организации.

Ключевые слова: информация, информационная безопасность логистических процессов, информационные технологии, риски, угрозы.

Modern information technologies for information security in logistics

Abstract: This article describes notions of information security in logistics and explores basic information technologies aimed at maintaining of information security. In addition, article reviews implementation of security management system within organization.

Keywords: information, information security of logistics, information technologies, risks, threats.

Сегодня, в век информационных технологий, данные людей и организаций продолжают оставаться уязвимыми и требующими контроля. Ущерб от потери данных или нарушения процесса работы предприятия могут нанести миллионные убытки организации. По этой причине необходимость специалистов в области информационной безопасности растёт с каждым годом. Данная проблема остаётся актуальной и для логистики, поскольку в данной сфере также замечен бурный рост информационных и логистических технологий. Для полного понимания проблематики статьи будут даны определения.

Под информацией подразумевается актив, который имеет ценность и должен быть надлежащим образом защищён. Информационная безопасность – это защита информации от широкого диапазона угроз с целью обеспечения уверенности в непрерывности бизнеса, минимизации ущерба, получения максимальной отдачи от инвестиций и реализация потенциальных возможностей бизнеса (ГОС1).

Под информационной безопасностью логистических процессов подразумевается защита информации и поддержка логистической инфраструктуры (производственные предприятия, транспортные компании, складское хозяйство и другое (Детлеф Венде Франк, 2014)) от внутренних и внешних угроз. Основным условием для обеспечения безопасности логистической системы является сохранение её целостности.

Логистика является неотъемлемым и ключевым составляющим бизнеса, поскольку благодаря грамотной организации поставок и хранения грузов можно совершенствовать свой бизнес и иметь высокое преимущество перед конкурентами. По этой причине данная сфера постоянно развивается. Следует отметить, что цифровизация логистических процессов ведёт к их уязвимости перед угрозами информационной безопасности.

Под информационным потоком подразумевается движение информации по потоку создания ценности (2021). Иными словами, это данные, объединённых общими признаками, которые перемещаются в логистических системах, между ними и внешней средой, и служат для управления и контроля логистических и информационных процессов. Данное понятие приводится здесь по той причине, что сама информация может рассматриваться как двигатель системы логистики, она сопровождает материальный поток на протяжении всех этапов его продвижения.

Сегодня информационный поток играет особую роль, поскольку наличие достоверной и точной информации позволяет снизить неопределённости в спросе, что в свою очередь снижает необходимость в запасах и трудозатратах; благодаря информации можно определять время, место и способ использования ресурсов для того, чтобы превзойти конкурентов, другими словами, информация делает логистическую систему более гибкой; потребители предпочитают оперативно получать достоверную информацию о сроках и статусе их доставки.

В логистической системе возможны угрозы информационной безопасности. Причиной тому являются устаревшие стандарты и способы регулирования в области информационных технологий; широкое использование операционных технологий, коммуникационных и беспроводных каналов, которые делают компанию уязвимой; дефицит

квалифицированных специалистов в области информационной безопасности.

В логистике для снижения рисков от угроз информационной безопасности применяется система менеджмента безопасности, которая позволяет повысить безопасность организации с использованием основных элементов (рис. 1).

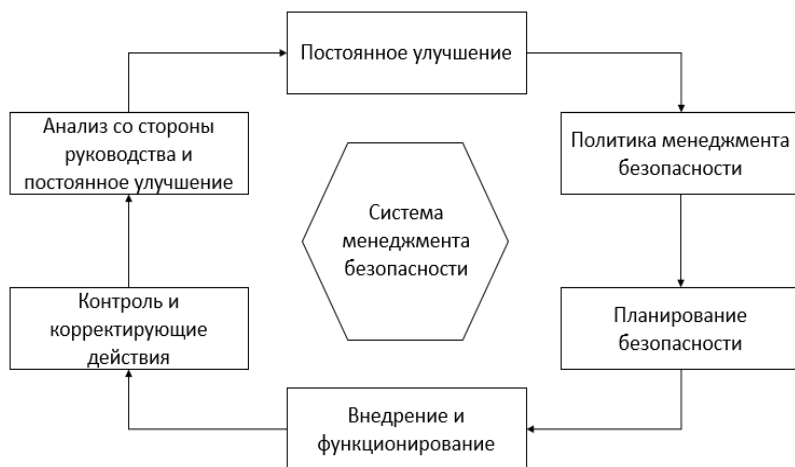


Рисунок 1 – Базовые элементы системы менеджмента безопасности

Политика формирует обязательства высшего руководства по обеспечению безопасности деятельности организации и требования к информационной безопасности логистических процессов.

Планирование представляет собой разработку установок и мероприятий по определению целей безопасности для достижения целей по управлению информационной безопасностью логистических процессов.

Внедрение и функционирование подразумевает определение обязанностей и полномочия тех лиц, на которых будет возложена ответственность в системе менеджмента безопасности, то есть это создание организационной структуры, которая обеспечивает информационную безопасность логистических процессов.

Контроль и корректирующие действия обеспечивают поддержку системы менеджмента безопасности за счёт мониторинга показателей информационной безопасности логистических процессов.

Анализ со стороны руководства предложений по улучшению безопасности логистических процессов проводится для обеспечения пригодности, адекватности и результативности системы менеджмента.

В результате обеспечивается информационная безопасность логистических процессов со стороны менеджмента. Однако, существуют и информационные технологии для этого, речь о которых будет ниже.

Информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (Фед). Сегодня информационные технологии являются неотъемлемой частью человеческой жизни, поскольку благодаря современным средствам коммуникации и программного обеспечения можно повысить эффективность работы организации, снизив при этом затраты труда, времени, материальных и финансовых ресурсов. Вместе с вышеперечисленным, современные технологии позволяют обрабатывать растущие объёмы данных гораздо быстрее человека.

В логистике информационные технологии позволяют повысить качество организационно-управленческой инфраструктуры предприятия за счёт построения эффективных схем планирования и поддержки принятия коммерческих решений. Для того, чтобы информация обеспечивала процесс управления логистическими системами, она должна быть доступной, точной, своевременной, оперативной в реагировании на сбои, гибкой и наглядной.

Информационные технологии, которые создаются на сегодняшний день, связаны с безопасностью, чтобы иметь преимущества перед конкурентами и не была испорчена репутация компании. По этой причине стоит делать акцент на информационной безопасности информационных технологий в логистике.

EDI (Electronic Data Interchange) или электронный обмен данными представляет собой информационную технологию, позволяющую производить обмен документами в электронном формате. Данная технология является как внутренней, так и межотраслевой. Основным отличием EDI от электронного документооборота в том, что здесь не просто переводят документ в цифровой формат, но и осуществляют их обмен между компаниями. Благодаря такой автоматизации бумажных транзакций экономится время и средства организации, что является основным преимуществом данной технологии.

За счёт того, что процесс документооборота становится полностью автоматизированным, повышается скорость оформления и обработки документом. Следует отметить, что существует такое понятие, как «человеческий» фактор, которому сопутствуют множественные ошибки при работе с документацией. Электронный обмен данными снижает число как самих ошибок, так и время на их поиск и исправление. За счёт

стандартов используется единый способ идентификации товаров, и используются технологии, которые гарантируют доставку сообщений.

Если рассматривать данную технологию со стороны информационной безопасности, то она обеспечивает конфиденциальность передаваемой информации, поскольку все данные шифруются, обеспечивается аутентификация за счёт проверки электронной подписи отправителя, а также исключается попытка изменения сообщения без ведома получателя, можно быть уверенным в достоверности сообщения.

EDI может функционировать на различных платформах: «облако», мэйнфрейм, клиент-сервер или на персональном компьютере, всё зависит от потребностей компании. Передача сообщений может осуществляться через подключение двух компьютеров или систем друг к другу через Интернет или за счёт VAN (Value-added Network) – сеть с дополнительными услугами, где сторонняя сеть отвечает за передачу данных.

Однако, нет необходимости внедрять данное решение в своё предприятие и сразу рассчитывать на быструю экономию средств. Дело в том, что электронный обмен данными, его внедрение также имеет свои затраты. Нужно рассчитать и проанализировать, а есть ли смысл использовать эту информационную технологию. В основном ею пользуются крупные предприятия, в которых большое количество документации и компаний. Малым же предприятиям не всегда выгодно использование EDI.

Следует отметить, что вместе с вышенаписанным необходимо обучение сотрудников данной информационной технологии, нужны специалисты, которые разбирается в этой системе и могут помочь персоналу. Всё это влечёт за собой потерю финансовых и временных ресурсов.

EDI подразумевает под собой двухточечную связь, а значит, что каждая «точка», с которой будет осуществляться контакт, должна иметь необходимое оборудование и программное обеспечение для взаимосвязи.

Помимо этого, существует проблема зависимости работы от стабильности работы серверов. При отсутствии Интернета или других технических проблем в организации, использование электронного документооборота становится невозможным. В данном случае нужно повышать организации работу серверов и приобретать более современное оборудование.

Таким образом, перед внедрением данной информационной технологии, организации стоит проанализировать, на сколько это будет эффективно и необходимо. Существенных преимуществ можно добиться, если в организации имеются большие объёмы данных.

Ещё одной современной информационной технологией служит CALS (Continuous Acquisition and Lifecycle Support) или непрерывная информационная поддержка поставок и жизненного цикла изделий, которая представляет собой поддержку, отслеживание и контроль изделия на всех этапах его жизненного цикла.

CALS-технологии предназначены для повышения эффективности и упрощения этапов жизненного цикла продукта. Достигается это за счёт унификации и стандартизации описания этапов, используемых на всех стадиях продукта, например, на стадии проектирования унифицируется формат работы при описании оборудования, узлов, агрегатов и прочего. Унификация и интеграция процессов в рамках общей многофункциональной системы, доступной всем вовлечённым в работу с продуктом лицам, значительно сокращает сроки и объём работ на всех стадиях жизненного цикла.

Благодаря автоматизации процессов производства и формирования электронной документации несколько рабочих групп могут одновременно работать над несколькими сложными проектами, уменьшая тем самым время разработок, уменьшается количество совершаемых ошибок и времени на их исправление, повышается качество выпускаемой продукции. Таким образом сокращаются сроки работы, финансовые затраты, растёт качество продукции и конкурентоспособность компании.

Среди CALS-технологий есть PDM-технологии (Product Data Management) или технологии управления данными, которые в свою очередь интегрируют все данные в логическую единую модель и предоставляет необходимую информацию определённому сотруднику. Для реализации таких технологий существуют специальные PDM-системы, которые хранят данные в специальном хранилище данных, обеспечивая их целостность, и предоставляют их сотрудникам в зависимости от их прав доступа. Тем самым осуществляется информационная безопасность этих данных.

Проблемами с внедрением CALS-технологий считаются необходимость в приобретении современного оборудования, обучение и переподготовка кадров. Помимо этого, сотрудники могут уйти на другое предприятие в связи с трудностями освоения новых информационных технологий, поэтому нужно использовать методы по удержанию их в организации за счёт повышения заработной платы и премий.

Таким образом, в настоящее время существуют разнообразные информационные технологии, применяемых в логистике, которые помимо повышения эффективности самого логистического процесса повышают конкурентоспособность предприятия. Вместе с тем была рассмотрена система менеджмента безопасности, которая позволяет повысить безопасность логистического процесса на организационном уровне.

Список использованных источников:

1. ГОСТ Р ИСО/МЭК 17799-2005 "Практические правила управления информационной безопасностью» [В Интернете]. Available: <https://docs.cntd.ru/document/1200044724>.
2. Р. О. С. В. Деглеф Венде Франк, «Определение понятия и содержания инфраструктуры логистики» 2014. [В Интернете]. Available: <https://elibrary.ru/item.asp?id=22744028>.
3. «ГОСТ Р 56020-2020 "Бережливое производство. Основные положения и словарь"» 2021. [В Интернете]. Available: <https://docs.cntd.ru/document/1200174885>.
4. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 02.07.2021) "Об информации, информационных технологиях и о защите информации".
5. ГОСТ Р ИСО 28004-1-2019 "Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ИСО 28000. Часть 1. Общие принципы"» 2020.
6. А. П. В.А. Медведев, Информационные системы и технологии в логистике и управление цепями поставок, Санкт-Петербург: Университет ИТМО, 2016.
7. К. Балинская, «Преимущества и недостатки использования CALS-технологий на современных предприятиях» 2017. [В Интернете]. Available: <https://www.elibrary.ru/item.asp?id=28179259&>.

Современные проблемы информационной безопасности в разработке программного обеспечения

А.А. Тулеубаева

студентка 4 курса НИЯУ МИФИ, Москва

E-mail: aigerim.tuleubayeva@yandex.ru

научный руководитель: А.Н. Норкина

к.э.н., заместитель директора ИФТЭБ НИЯУ МИФИ, Москва

E-mail: annorkina@mephi.ru

Аннотация: В статье рассмотрены современные проблемы информационной безопасности в разработке программного обеспечения. Описаны основные уязвимости и приведены примеры самых часто используемых в настоящее время подходов для решения проблем информационной безопасности в процессе разработки ПО. Приведен список рекомендаций для разработки ПО с минимальным количеством уязвимостей.

Ключевые слова: информационная безопасность, разработка ПО, безопасная разработка, динамический анализ кода, статический анализ кода, DevSecOps.

Modern problems of information security in software development

Abstract: The article deals with modern problems of information security in software development. The main vulnerabilities and examples of the most commonly used approaches to solving information security problems in the software development process are described. A list of recommendations for developing software with minimal vulnerabilities is provided.

Keywords: information security, software development, secure development, dynamic code analysis, static code analysis, DevSecOps.

В современном мире, где каждое предприятие стремится к обладанию наиболее эффективным инструментом для конкурентного преимущества, использование информационных технологий, систем и программного обеспечения стало крайне необходимым, так как автоматизация процессов оказывает огромное влияние на производительность труда; а сами информационные технологии сегодня являются основным ускорителем инноваций, который обеспечивает экономический рост не только в рамках

одной конкретной организации, так и глобально – всего мирового пространства. Разработка программного обеспечения – растущая и развивающаяся отрасль, влияние которой на мировую экономику значительно превосходит ее долю во всемирном производстве.

Однако развитие информационных технологий имеет не только положительный эффект, но и обратную сторону: количество уязвимостей постоянно растет, появляются новые способы реализации вроде бы уже известных угроз информационной безопасности. С точки зрения изобилия угроз для программного обеспечения, информационная среда является беспрецедентной в последние несколько десятков лет. Новые угрозы возникают с внедрением новых систем и средств защиты. Вопрос безопасности программного обеспечения всегда заботил, заботит и будет заботить все мировое сообщество всегда, пока существует программное обеспечение, что и обуславливает актуальность выбранной темы.

Данная работа освещает проблемы информационной безопасности в процессе разработки программного обеспечения.

Безопасное программное обеспечение — программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы.

Уязвимости могут возникать из-за недостатков:

а) требований, т.е. продукт ИТ может обладать требуемыми от него функциями и свойствами, но все же содержать уязвимости, которые делают его непригодным или неэффективным в части безопасности;

б) проектирования, т.е. продукт ИТ не отвечает спецификации, и/или уязвимости являются следствием некачественных стандартов проектирования или неправильных проектных решений;

в) эксплуатации, т.е. продукт ИТ разработан в полном соответствии с корректной спецификацией, но уязвимости возникают как результат неадекватного управления при эксплуатации.

В сути, безопасность программного обеспечения – это ничто иное, как одно из свойств программного обеспечения функционировать без негативных последствий для пользователя и системы. Причины негативных последствий — это не только баги и логические ошибки, но и преднамеренные и непреднамеренные дефекты, а также сбои в самой компьютерной системе.

На сегодняшний день во всем мире практикуются самые разные методы для обеспечения безопасности разрабатываемого ПО. Наиболее широкое практическое применение для обеспечения информационной безопасности при разработке программного обеспечения получили такие решения, как безопасная разработка; DevSecOps; антиотладочные приемы и всевозможные методы тестирования ПО; методы защиты кода как

обфускация и шифрование; а также динамический и статический анализ кода.

Безопасная разработка ПО — это практика, при которой разработчики пытаются учесть ошибки в коде программы и возможные сбои, добавляют вспомогательный код, предотвращающий введение уязвимостей, а также обеспечивающий защиту от несанкционированного доступа и вредоносного ПО.

Несмотря на огромное количество разных технологий разработки безопасного ПО, существуют основные принципы, учитываемые везде:

1. работоспособность и полезность (usability) — свойство функционирования в заданных условиях;
2. безопасность (security) - свойство защищенности от атак и сохранения работоспособного состояния после отражения;
3. надежность (reliability) — свойство обеспечения долговечности, безотказности и приспособленности к восстановлению и поддержанию;
4. конфиденциальность (privacy) — свойство необходимости корректного использования и защиты персональных данных, а также любой информации, используемой предприятием в своей деятельности;
5. обеспечение целостности и корректности бизнеса (business integrity) — свойство, которое подразумевает под собой контроль законности и прозрачности бизнеса пользователя, а также возможность оперативного исправления ошибок за счет организации сопровождения программного обеспечения.

Самыми распространенными проблемами современности в области безопасности разработки ПО являются вирусы, трояны, черви, логические бомбы, а также уязвимости, введенные разработчиками случайно или преднамеренно.

Предупреждение и предотвращение уязвимостей - лучшая стратегия для обеспечения безопасности ПО. Это требует постоянной проверки входных данных. Но излишнее количество проверок усложняет процесс разработки и может привести к появлению новых ошибок. Лучшее решение — комбинация разных методов обеспечения безопасности ПО.

Статический и динамический анализ кода — это две наиболее распространенные формы тестирования безопасности программного обеспечения, которые используют различные подходы к выявлению уязвимостей и часто дополняются друг другом в процессе разработки ПО.

Динамический анализ кода — динамическое тестирование безопасности приложений (DAST) — анализ программного обеспечения, запущенного на реальном или виртуальном процессоре для выявления потенциальных уязвимостей. Динамический анализ производится с целью проверки функционала программного обеспечения по уже готовым наборам тестов.

Для эффективного использования данного вида тестирования, необходимо обеспечить достаточное количество входных данных ради максимального возможного покрытия кода. Этот вид анализа кода использует вредоносные входные данные для имитации настоящих атак на ПО. Метод стал востребован при тестировании методом «черного ящика», при котором тестируемому доступен только внешний интерфейс ПО. DAST имеет минимальное количество ложных срабатываний за счет того, что при обнаружении ошибки во время тестирования, можно сразу увидеть, где и при каких входных эта ошибка появляется. Примерами являются модульное, интеграционное и приемочное тестирование.

Статический анализ кода – статическое тестирование безопасности приложений (SAST) - анализ программного обеспечения, проверяющий исходный код ПО на наличие уязвимостей, который часто является автоматизированным процессом. Статический анализатор – инструмент SAST, который помогает в минимизации количества ложных срабатываний и дает дополнительные возможности в работе с предупреждениями.

В результате автоматического статического тестирования получаются рекомендации для ручной проверки потенциальных ошибок.

Преимущества:

1. Тестирование проводится высококвалифицированными экспертами;
2. Обеспечивает скорость и гибкость поиска ошибок;
3. Инструменты автоматизации повышают качество и скорость;
4. Раннее обнаружение проблем;

Недостатки:

1. Сканируется только код;
2. Ручной метод очень затратен по времени;
3. Инструменты автоматизации иногда могут предоставлять ложные положительные и отрицательные случаи.

В качестве примеров статического тестирования выступают обзоры (code review), аудиты, сквозные просмотры, а также тестирование требований и документации. Свое широкое применение технология получила в верификации свойств ПО для систем высокой надежности, как медицинские устройства, атомные станции, автомобильный транспорт и авиация.

В силу того, что динамический анализ применяется для скомпилированных файлов, а статический анализ работает с исходным кодом, они обнаруживают разные виды уязвимости и применяются на разных этапах жизненного цикла разработки ПО.

Как правило, специалисты по информационной безопасности уделяют особое внимание и сосредотачивают свои силы на защите

конфиденциальности, целостности и доступности информации. Следует также рассматривать уязвимости в используемых методологиях организации и контроля процесса разработки для обеспечения того, чтобы конечные пользователи получили функциональное ПО, максимально удовлетворяющее их требованиям.

DevSecOps — это естественное и логическое развитие методик по обеспечению безопасности программного обеспечения. Данная методология автоматизирует задачи обеспечения безопасности на всех стадиях жизненного цикла разработки, начиная с проектирования до развертывания и доставки ПО.

До появления DevSecOps, задачи безопасности решались лишь в конце разработки ПО и за тестирование отвечали отдельные команды. Однако, с популярностью использования Agile и DevOps, которые сокращали время на разработку, такой подход стал не эффективным. DevSecOps интегрирует задачи по обеспечению безопасности приложений и инфраструктуры в процессы и инструменты Agile и DevOps. DevSecOps позволяет решать проблемы безопасности по мере их появления, когда это можно сделать с меньшими затратами времени и средств - до развертывания функций в рабочей среде. Кроме того, DevSecOps позволяет разделить ответственность за безопасность приложений и инфраструктуры между специалистами по разработке, безопасности и эксплуатации ИТ-систем.

Несмотря на существование огромного количества инструментов для обеспечения безопасности и качества ПО, уязвимостей и угроз становится не меньше. Ущерб от возникающих рисков в информационной безопасности, способен обойтись в разы дороже, чем внедрение мер защиты. Снижение рисков, очевидно, является одним из самых необходимых процессов.

Одной из наиболее частых проблем, с которыми сталкиваются при разработке безопасного приложения является то, что программисты не мотивированы выполнять дополнительную работу по обеспечению безопасности, а рамки бюджета проекта не всегда имеют возможность выделения достаточных ресурсов для привлечения квалифицированных специалистов по информационной безопасности для постоянного и своевременного обеспечения необходимого контроля безопасности ПО.

Для решения этой задачи были созданы каркасы - фреймворки, помогающие программным инженерам в конструировании безопасных ПО. Применение готовых решений облегчает работу разработчиков от предоставления возможности не производить бесчётные проверки входящих данных и HTTP-запросов до обеспечения защиты от CSRF - угроз. Также применение DevSecOps там, где это возможно, дает

преимущество не только в безопасности разрабатываемого ПО, но и повышается скорость разработки и качество кода, а затраты снижаются.

Сообщество специалистов в области информационной безопасности находится в постоянном поиске решений задач обеспечения безопасности ПО. Создаются новые стандарты, рекомендации, методики, инструменты и сервисы по анализу и тестированию кода. Однако, стоит помнить, что информационная безопасность — это не только технологическая, но и человеческая проблема. Самым слабым звеном в информационной безопасности, без сомнений, является человеческий фактор. Первым делом, для обеспечения безопасности разрабатываемого ПО от уязвимостей, необходимо повышение осведомленности об информационной безопасности. Чтобы защитить среду разработки, подход к безопасности должен быть комплексным.

Для того, чтобы разработать ПО с минимальным возможным количеством уязвимостей, рекомендуется начиная с самого начала разработки программного обеспечения безопасность обеспечивать с помощью:

1. применения практик безопасного программирования;
2. проведения автотестов;
3. динамического и статического анализа кода;
4. организации испытаний на проникновение (пентестов);
5. функционального тестирования;
6. тестирования протоколов;
7. мониторинга угроз, реагирования на инциденты (после развертывания, в ходе эксплуатации);
8. автоматизации рутинных процессов;
9. документирования политики безопасности;
10. внешнего аудита безопасности;
11. применения подходящих методологий разработки ПО.

Список использованных источников:

1. ГОСТ Р 56939-2016. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования - www.consultant.ru
2. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности" - <http://ivo.garant.ru>

3. Аветисян А. И., Белеванцев А. А., Чукляев И. И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. № 3 (4). С. 20-28.
4. Воротникова, Т. Ю. Надежный код: статический анализ программного кода как средство повышения надежности программного обеспечения информационных систем / Т. Ю. Воротникова // Информационные технологии в УИС. – 2020. – № 2. – С. 22-27. - <http://elibrary.ru>
5. Рагозин, Юрий Николаевич диссертация ... кандидата экономических наук : 08.00.13 Москва 2011 - <http://dlib.rsl.ru>
6. Сафонов, В. О. Современные технологии разработки надежных и безопасных программ (trustworthy computing) / В. О. Сафонов // Компьютерные инструменты в образовании. – 2008. – № 6. – С. 25-33. - <https://elibrary.ru>
7. DevSecOps [Электронный ресурс] / IBM Cloud Education / IBM - <https://www.ibm.com/ru-ru/cloud/learn/devsecops>

Создание цифровой среды взаимодействия банка и корпоративных клиентов

Н.Н. Корсунова

аспирант 3 курса РГЭУ(РИНХ), г. Ростов-на-Дону,

E-mail: nadegdacorsunova2@gmail.com

научный руководитель: С.А. Уразова

д.э.н., профессор кафедры «банковское дело» РГЭУ(РИНХ),

г. Ростов-на-Дону,

E-mail: urazova@inbox.ru

Аннотация: Статья посвящена исследованию цифровой среды взаимодействия банка и корпоративных клиентов в условиях процесса цифровизации. Сделан обзор ключевых изменений на банковском рынке в условиях перехода к цифровой экономике; изучен успешный опыт российских банков в области развития цифровых каналов обслуживания юридических лиц; выделены современные тренды развития каналов коммуникации с клиентами; выделены существенные черты организации процесса цифрового взаимодействия банка и корпоративных клиентов; определены элементы цифрового взаимодействия банка с корпоративными клиентами.

Ключевые слова: банк, корпоративные клиенты, цифровая среда взаимодействия, тренды развития.

Creation of a digital environment for interaction between the bank and corporate clients

Abstract: The article is devoted to the study of the digital environment of interaction between the bank and corporate clients in the context of the digitalization process. An overview of the key changes in the banking market in the context of the transition to the digital economy is made; studied the successful experience of Russian banks in the development of digital channels for servicing legal entities; highlighted modern trends in the development of communication channels with clients; the essential features of the organization of the process of digital interaction between the bank and corporate clients are highlighted; the elements of the digital interaction of the bank with corporate clients have been determined.

Keywords: *bank, corporate clients, digital interaction environment, development trends.*

На сегодняшний день отмечается цифровизация и ускоренная трансформация деятельности банков, которая направлена на развитие дистанционных каналов банковского обслуживания корпоративных клиентов.

Отличительной особенностью банковского рынка РФ в настоящее время является участие банков в создании цифровых экосистем, а процесс их регулирования основан на риск-ориентированном и пропорциональном подходах [1].

Рассмотрим ключевые источники изменений на банковском рынке, которые были отмечены в рамках Международного финансового конгресса (МФК), проводимого Банком России с 28 июня по 2 июля 2021 г. (см. рис.1).

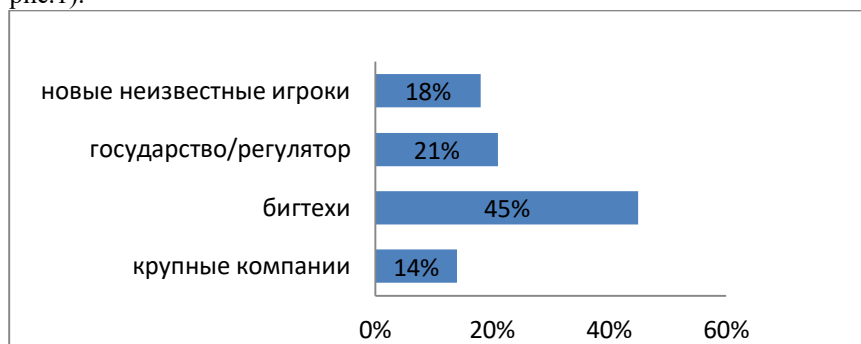


Рисунок 1 – Ключевые источники изменений на банковском рынке, которые были отмечены в рамках Международного финансового конгресса, проводимого летом 2021 г. [2].

Согласно данным рисунка 1, ключевую роль в организации работы банковского сектора нашей страны окажут бигтехи. Данные были получены на основе голосования представителей крупных банков, приглашенных на конгресс.

Как отмечает Г.В. Семяко, отличие бигтеха от финтеха состоит в том, что центральное место в бигтехе занимают цифровые технологии, а финансовые продукты являются лишь частью их деятельности. Бигтехи владеют сетевыми данными и, как следствие, имеют доступ к обширной базе данных, а их услуги не имеют конкурентов. В своей деятельности бигтехи используют стратегию расширения, где от оказания платежных услуг они переходят к кредитным, сберегательным, страховым,

инвестиционным и услугам по управлению капиталом представителей малого бизнеса[3,с.77-78].

Яркими представителями бигтех являются такие компании, как Facebook, Apple, Microsoft, Google и Amazon. За 2016-2020 г.г. отмечается рост инвестиций со стороны бигтех-компаний в пять раз, равный \$12.36 млрд. [4].

В свою очередь, представители Центрального банка Индии видят риски в результате развития финансовых сервисов со стороны бигтех-компаний, поскольку они составляют неравную конкуренцию классическим финансовым организациям, а инструменты бигтех превосходят решения традиционных банков. Кроме того, бигтех-компании могут преодолевать ограничения в области масштабирования финансовых услуг, за счет использования сетевых эффектов[5].

Организация деятельности бигтех-компаний составляет конкуренцию банкам и предполагает формирование цифровой среды взаимодействия с клиентами, в результате формирования которой осуществляется переход в облако и осуществляется внедрение BI-решений.

Согласно отчёту Economist Intelligence Unit , представленному в 2021 г. почти три четверти ИТ-руководителей зарубежных банков считают, что переход в облако поможет их компаниям достичь своих бизнес-приоритетов. В числе главных стимулов они видят внедрение облачных технологий для уменьшения издержек (43%), внедрение ИИ (34%) и улучшение качества обслуживания клиентов (21%). Гибкость, эластичность и масштабируемость бизнеса отмечены 40% респондентов в качестве основных факторов внедрения облачных решений [6].

Как показало исследование IDC, в 2020 г. отечественный рынок облачных услуг продемонстрировал рост на 29,9% по сравнению с предыдущим годом. Его объем составил \$1,21 млрд. До 2025 г., среднегодовой рост данного рынка в нашей стране составит порядка 18,6% [7].

По данным исследования Accenture, в 2020 г. облачные решения удалось внедрить 95% европейским банкам и банкам США. Размер инвестиций в облачные проекты в банках увеличился за несколько лет на 30%. Ежегодный объем инвестиций будет продолжать расти в среднем на 15%, а к 2022 г. составит \$411 млрд. [8].

По данным обзора «Аналитика 3.0- 2021», проведенного CNews Analytics, выручка 15 лидеров отечественного и зарубежного рынков, занимающихся разработкой средств анализа данных, в 2020 г. выросла на 15%, до \$24,9 млрд. Число участников рейтинга осталось на уровне 2020 г., при этом состав участников обновился на четверть. Один из новых

участников рынка, Parma TG, вошел в топ-5 рейтинга, еще один, ГКС, замкнул топ-15 участников рейтинга[9].

Переход к цифровым каналам коммуникации банка и корпоративных клиентов предполагает повышение качества и скорости передачи информации; рост требований к вычислительным мощностям и ИТ-архитектуре банка.

Согласно данным исследования Frank Media , определены тренды в области развития технологий в организации работы отечественных банков в 2021 г.(см.рис.2).

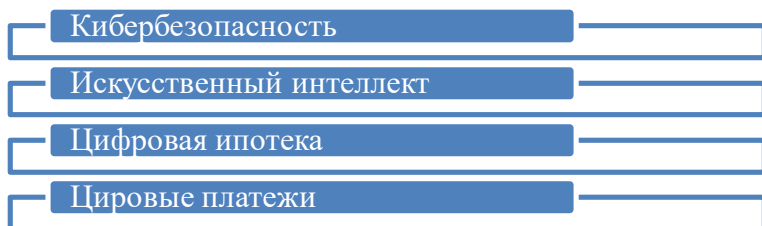


Рисунок 2 – Тренды развития банковских технологий в 2021 г. [10]

Согласно данным опроса Accenture, которое проводилось в 2019 г. среди 240 топ-менеджеров ,отвечающих за развитие банковских платежных операций из 22 стран, установлено, что 71% опрошенных банковских руководителей в мире и 93% в Европе убеждены, что платежные услуги становятся бесплатными; 73% считают, что большинство платежей уже «невидимы» или станут такими в течение следующих 12 месяцев; 78% заявили, что платежи либо уже мгновенные, либо станут мгновенными в ближайший год. В результате мировой рынок платежных услуг будет расти в среднем на 5,5% в год, то есть с 1,5 трлн. долларов в 2019 г. и до 2 трлн. долларов к 2025 г. [11].

В результате повышения роли цифровых сервисов и услуг под влиянием пандемии коронавирусной инфекции произошла цифровая трансформация бизнеса, которая требует перевод предприятий к онлайн-каналам, организацию финансовой поддержки со стороны банков, а также проведение обучения сотрудников предприятий цифровым навыкам [12], которые могут быть полезны при получении банковских услуг в режиме онлайн.

Проведенное исследование НАФИ в феврале-марте 2021 г, показало, что индекс цифровизации МСБ увеличился по сравнению с аналогичным периодом годом ранее – с 50 до 51 пункта (по шкале от 0 до 100)[12].

Рассмотрим успешный опыт развития цифровизации российских банков. Например, ПАО «Сбербанк» при формировании собственной цифровой экосистемы использует гибкую модель разработки технологий,

которая помогла ему перестроить весь производственный процесс, сформировать самоуправляемые команды, произвести отказ от устаревшей «водопадной модели». В результате банк внедряет банковские продукты на рынок в семь раз быстрее. В ближайшие годы ПАО «Сбербанк» продолжит поступательное движение к экосистеме, завершив миграцию на облачную платформу PlatformV, встраивая искусственный интеллект во все банковские продукты и процессы для повышения их эффективности, развивая технологические продукты, а также обучая сотрудников. Ключевая цель банка состоит в том, чтобы стать помощником и навигатором для человека, бизнеса и государства. Для предпринимателей банк планирует стать партнером для сохранения и роста бизнеса[13].

В декабре 2019 г. в ПАО «Банке Уралсиб» завершился проект по смене платформы дистанционного банковского обслуживания для юридических лиц. Единую цифровую среду банка для взаимодействия с данной категорией клиентов формируют маркетплейс, интернет-банк и мобильный банк на базе единого кроссплатформенного фреймворка. Принцип работы банка заключается в том, чтобы избавить клиента от лишних трудностей в процессе банковского обслуживания[14].

В 2021 г. совместный проект компании «Диасофт» и ПАО «Росбанка», вышел в финал премии «Banking Tech Awards 2021» в номинации «Лучший IT-проект для поддержки кредитного бизнеса». В рамках развития инновационных IT-решений и сервисов в ПАО «Росбанке» запущена масштабная программа IT-трансформации, включающая отказ от устаревшей монолитной системы и внедрение современных независимых решений для поддержки отдельных направлений бизнеса. Важным этапом IT-трансформации банка стала реализация крупного проекта по замене core-системы для поддержки кредитного обслуживания юридических лиц. В ходе проекта в банке внедрена платформа развития Digital Q.Corporate от «Диасофт». Ключевой технологической инновацией проекта стало внедрение микросервисной архитектуры в бэк-офисной банковской системе, которая отличается высокой масштабируемостью и надежностью, возможностью осуществления гибкой замены компонентов, их развития и доработки. В результате реализации данного проекта, банку удалось сформировать современную цифровую платформу, направленную на технологическую и бизнес-трансформацию корпоративного бизнеса[15].

В 2021 г. ПАО «ВТБ» удалось внедрить уникальную экосистему цифровых продуктов и онлайн-сервисов для клиентов бизнеса с зарубежными партнерами «под ключ». Данное техническое решение предлагается данной категории клиентов в новом интернет-банке «ВТБ Бизнес». Перечень банковских продуктов и сервисов ПАО «ВТБ» для клиентов бизнеса представлен на рисунке 3.

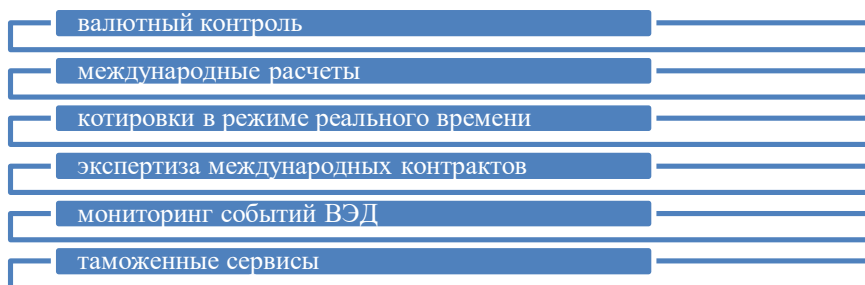


Рисунок 3 – Ключевые сервисы и банковские продукты ПАО «ВТБ» для бизнеса[16]

В результате пандемии коронавирусной инфекции произошли существенные изменения в работе рынка цифровых коммуникационных технологий и каналов передачи данных за счет формирования мультиканальной стратегии, ориентированной на интересы клиентов с учетом ключевых трендов в области развития каналов коммуникаций (см.рис.4).

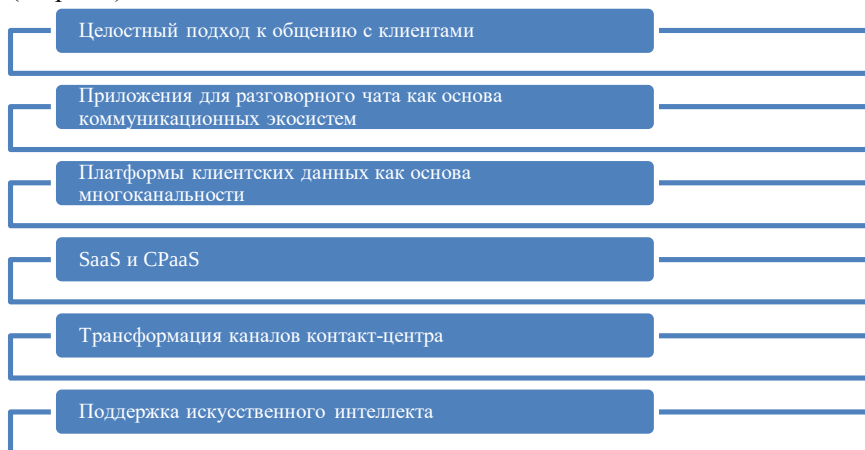


Рисунок 4 – Современные тренды развития каналов коммуникации с клиентами[17]

Тренды развития каналов коммуникации с клиентами, представленные на рисунке 4, оказали влияние на формирование цифровой среды взаимодействия банка и корпоративных клиентов, которая в настоящее время выходит за пределы интернет-банка.

Выход за пределы интернет-банка связан с формированием цифровых каналов взаимодействия банка и корпоративных клиентов, развивающихся согласно требований индустрии 4.0 (см. рис.5).



Рисунок 5 – Элементы Индустрии 4.0 [18]

Как отмечает Б.Кинг, Банк 4.0 даст возможность клиентам воспользоваться банковскими услугами в любом месте в любой момент, в соответствии с определенными привычками клиента. Появление Банка 4.0 означает, что банк либо встраивается в мир клиентов, либо нет [19,с.27].

Банк 4.0 предполагает радикальную трансформацию, которая отражает, как лучшие мировые банки реагируют на существующие изменения, как их конкуренты, работающие на основе первых принципов, заставляют иначе взглянуть на банкинг. Банк 4.0 – это также история о регуляторах, готовых устранить помехи, отказаться от устаревших норм и пересмотреть саму суть регулирования [19,с.28].

Согласно исследованию KPMG, проведенному в 2019 г., отмечается, что к 2030 г. наибольшее влияние на процесс взаимодействия банка с клиентами окажут восемь технологических разработок и решений: квантовые технологии, блокчейн, биометрия, 5 G, облачные вычисления, Интернет-вещей, технологии виртуальной и дополненной реальности, технологии искусственного интеллекта и машинного обучения[20,с.11-12].

Создание цифровой среды взаимодействия банка и корпоративных клиентов предполагает переход банка к разработке цифровой экосистемы, где ключевая роль отводится формированию технологических платформ для организации цифровых коммуникаций с корпоративными клиентами (см. рис.6).



Рисунок 6 – Ключевые компоненты цифровой среды взаимодействия банка и корпоративных клиентов



Рисунок 7 – Этапы создания цифровой среды банка в обслуживании корпоративных клиентов

Формирование цифровой среды банка в обслуживании корпоративных клиентов содержит ряд последовательных этапов (см.рис.7).

Организация процесса цифрового взаимодействия банка и корпоративных клиентов предполагает:

- Формирование коммуникационных приложений;
- Программируемую голосовую связь, которая обеспечивает унифицированное управление звонками и конференциями для разных участников: PSTN, SIP, WebRTC;
- Программируемую видеосвязь, которая обеспечивает эффективные решения для видеоконференций между двумя и более участниками, а также для прямых трансляций;
- Программируемый месседжинг SMS и IP-месседжинг для множества платформ, включая веб и мобильные устройства;
- Serverless-архитектуру, которая обеспечивает вывод банковского продукта на рынок, где инструменты разработки и развертывания встроены в систему;
- Интеграцию с ботами на основе искусственного интеллекта , направленную на создание персонализированного клиентского сервиса;
- Распределенную облачную инфраструктуру, обеспечивающую высокое качество и надежность связи для коммуникаций в режиме реального времени [21];
- Использование инструментов коммуникации с корпоративными клиентами;
- Проведение оценки рабочей атмосферы банка при обслуживании корпоративных клиентов;
- HR-аналитику за счет мониторинга активности сотрудников банка в рабочих приложениях[22];
- Удаленное управление серверами и распределение нагрузки;
- Создание системы, где все инструменты для работы с инфраструктурой объединены на одной платформе: учёт оборудования, мониторинг и статистика, управление серверами и виртуализацией, а также создание пользовательских учетных записей разного уровня доступа;
- Выполнение в автоматическом решении большинства задач и экономии времени;
- Мультивендорность ;
- Проверку состояния серверов и запуск режима восстановления;
- Осуществление удаленного доступа к серверам;
- Управление сетями;
- Гибкую систему API[23].

Создание цифровой среды взаимодействия банка и корпоративных клиентов связано с разработкой новой технологической платформы банка (см.рис.8).



Рисунок 8 – Этапы работы технологической платформы банка в процессе обслуживания корпоративных клиентов при помощи цифровых каналов взаимодействия

Цифровое взаимодействие банка и корпоративных клиентов содержит ряд элементов, сформированных на основе цифровых потребностей банка и корпоративных клиентов с целью создания онлайн-каналов обслуживания данной категории клиентов в условиях перехода к цифровой экономике:

- Развитие клиентской базы при помощи цифровых сервисов, которые могут продавать банковские услуги даже в городах, где нет операционного офиса;

- Снижение нагрузки на филиалы банка за счет автоматизации неплатежного документооборота, где корпоративные клиенты заполняют анкеты, а банк получает готовые заявки;

- Увеличение дохода от агентской сети и продажа нефинансовых сервисов прямо в интернет-банке;

- Формирование сервиса для открытия расчётного счёта юридического лица и передачи необходимых документов без посещения офиса;

- Создание приложений для выездного менеджера;

- Проведение Онлайн-регистрации бизнеса;

- Создание сервиса для агентских продаж;

- Формирование маркетинговых сервисов [24];

- Создание, управление и развертывание приложений в любой точке мира на единой платформе;

- Управление устойчивым развитием за счет повышения эффективности работы на основе применения экологичного подхода;

- Внедрение решений SAP для устойчивого развития, которые помогают оценивать и контролировать влияние предприятий бизнеса на окружающую среду;

- Внедрение отраслевого облака для изучения и развертывания вертикальных решений от SAP и партнеров, применяя ведущие отраслевые практики и дополняя текущие бизнес-процессы;

- Управление опытом корпоративных клиентов, сотрудников и других заинтересованных лиц при помощи решений SAP и Qualtrics для управления впечатлениями корпоративных клиентов;

- Организация работы интеллектуальных бизнес-процессов за счет внедрения быстрой, гибкой и рациональной схемы оптимизации процессов, основанной на аналитической информации реального времени и включающей рекомендации по улучшению и автоматизации банковских бизнес-процессов в обслуживании корпоративных клиентов;

- Формирование банком бизнес-сети SAP Business Network, которая объединяет все точки взаимодействия и интеграции всех партнеров [25];

– Внедрение микросервисного бэкенда, который обеспечивает работу микросервисной архитектуры и позволяет быстро добавлять новый функционал как отдельно стоящий сервис без замены уже имеющихся или внедрения в ядро дистанционного банковского обслуживания корпоративных клиентов;

– Масштабирование платформы банка благодаря микросервисам, API и модулям многократного применения;

– Использование открытой модульной архитектуры, которая расширяет функции платформы с помощью новых цифровых решений и сторонних сервисов банка в обслуживании корпоративных клиентов (страхование, управление личными финансами, осуществление денежных переводов и т. д.);

– Объединение данных о корпоративных клиентах, находящихся в обособленных хранилищах[26].

Таким образом, переход к цифровым каналам банковского обслуживания корпоративных клиентов связан с ростом конкуренции для банков со стороны бихтех-компаний, ключевыми преимуществами которых являются наличие собственной экосистемы, низкие транзакционные издержки, наличие сетевых эффектов, оказание банковских услуг за минимальную плату. Создание цифровой среды взаимодействия банка и корпоративных клиентов основано на ключевых трендах развития банковского рынка и с учетом проявляющейся на нем конкуренции, предполагающих внедрение цифровых платформ и сервисов, направленных на создание единой технологической платформы банка для организации дистанционного взаимодействия с корпоративными клиентами.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-310-90036 «Трансформация банковского обслуживания корпоративных клиентов в условиях перехода к цифровой экономике»

Список использованных источников:

1. Регуляторное уравнение. [Электронный ресурс]. -Режим доступа: <https://iz.ru/1218324/aleksei-voilukov/regulatornoe-uravnenie> (дата обращения 15.11.2021)
2. Банки и бигтехи: в будущее возьмут не всех. [Электронный ресурс]. - Режим доступа: <https://econs.online/articles/mfk-2021/banki-i-bigtekhi-v-budushchee-vozmут-ne-vsekh/> (дата обращения 15.11.2021)
3. Семеко, Г. В. Бигтехи - новые игроки на рынке финансовых услуг / Г. В. Семеко // Социальные и гуманитарные науки. Отечественная и

- зарубежная литература. Серия 2: Экономика. Реферативный журнал. – 2020. – № 2. – С. 76-84
4. Бигтех во время пандемии: кого покупают и во что инвестируют крупнейшие IT-компании мира. [Электронный ресурс]. -Режим доступа: <https://bloomchain.ru/detailed/bigteh-vo-vremja-pandemii-kogo-pokupajut-i-vo-cto-investirujut-krupneishie-it-kompanii-mira> (дата обращения 15.11.2021)
 5. Банк Индии увидел риски в развитии финансовых сервисов со стороны бигтех-компаний. [Электронный ресурс]. -Режим доступа: <https://bloomchain.ru/newsfeed/bank-indii-uvidel-riski-v-razvitii-finansovyh-servisov-so-storony-bigteh-kompanii> (дата обращения 15.11.2021)
 6. Дайджест зарубежных СМИ. [Электронный ресурс]. -Режим доступа: <https://www.fintechru.org/analytics/daydzhest-zarubezhnykh-smi-3-11-poyabrya-2021/> (дата обращения 15.11.2021)
 7. Российский рынок облаков за год вырос на треть. [Электронный ресурс]. -Режим доступа: https://www.cnews.ru/news/top/2021-10-01_obem_rossijskogo_oblachnogo(дата обращения 15.11.2021)
 8. Accenture: банки, использующие облака, растут в два раза быстрее конкурентов.[Электронный ресурс]. -Режим доступа: <https://www.accenture.com/ru-ru/about/newsroom/company-news-release-banks-using-clouds-growing-fast>(дата обращения 15.11.2021)
 9. CNews выпустил рейтинг поставщиков средств аналитики. [Электронный ресурс]. -Режим доступа:https://www.cnews.ru/news/top/2021-06-24_cnews_vypustil_rejting_postavshchikov (дата обращения 15.11.2021)
 10. Топ-5 технологий в банках: эксперты назвали главные тренды 2021 года. [Электронный ресурс]. -Режим доступа: <https://frankrg.com/38577> (дата обращения 15.11.2021)
 11. Исследование Accenture: развитие цифровых платежей ударит по доходности традиционных банков. [Электронный ресурс]. -Режим доступа: <https://www.accenture.com/ru-ru/company-news-release-digital-payments-development> (дата обращения 15.11.2021)
 12. Три кита цифровой трансформации субъектов МСП: перевод бизнеса в онлайн-формат, финансовая поддержка, обучение цифровым навыкам. [Электронный ресурс]. -Режим доступа: <https://www.garant.ru/article/1467601/> (дата обращения 15.11.2021)
 13. Герман Греф: у классических банков не очень радужные перспективы. [Электронный ресурс]. -Режим доступа: <https://ria.ru/20211108/gref-1757966466.html>(дата обращения 15.11.2021)

14. Банк Уралсиб рассказал о построении единой цифровой среды для клиентов. [Электронный ресурс]. -Режим доступа: <https://www.kommersant.ru/doc/5029470> (дата обращения 15.11.2021)
15. Росбанк и Диасофт стали финалистами международной премии Banking Tech Awards 2021. [Электронный ресурс]. -Режим доступа: <https://plusworld.ru/daily/tehnologii/rosbank-i-diasoft-stali-finalistami-mezhdunarodnoj-premii-banking-tech-awards-2021/>(дата обращения 15.11.2021)
16. ВТБ запустил цифровую экосистему для международного бизнеса. [Электронный ресурс]. -Режим доступа: <https://www.vtb.ru/o-banke/press-centr/novosti-i-press-relizy/2021/10/2021-10-21-vtb-zapustil-tsifrovuyu-ekosistemu-dlya-mezhdunarodnogo-biznesa/>(дата обращения 15.11.2021)
17. Коммуникационные технологии изменились навсегда: 7 главных трендов. [Электронный ресурс]. -Режим доступа: https://www.cnews.ru/articles/2021-06-29_kommunikatsionnye_tehnologii_izmenilis (дата обращения 15.11.2021)
18. Четвертая промышленная революция. Популярно о главном технологическом тренде XXI века. [Электронный ресурс]. -Режим доступа:[https://www.tadviser.ru/index.php/Статья:Четвертая_промышленная_революция_\(Industry_Индустрия_4.0\)](https://www.tadviser.ru/index.php/Статья:Четвертая_промышленная_революция_(Industry_Индустрия_4.0)) (дата обращения 15.11.2021)
19. Банк 4.0: Новая финансовая реальность / Б. Кинг — «ОлимпБизнес»,2018
20. The Future of Digital Banking: Banking in 2030. [Электронный ресурс]. -Режим доступа: <https://assets.kpmg/content/dam/kpmg/au/pdf/2019/future-of-digital-banking-in-2030-cba.pdf> (дата обращения 15.11.2021)
21. Коммуникационная платформа нового поколения. [Электронный ресурс]. -Режим доступа: https://voximplant.ru/platform?utm_source=yandex&utm_medium=cpc&utm_campaign=65503213&utm_content=11141879440&utm_term=коммуникационная%20платформа&yclid=6739933857882888902 (дата обращения 15.11.2021)
22. Повышайте вовлеченность и продуктивность в компании с помощью цифровых сервисов VK HR Solutions. [Электронный ресурс]. -Режим доступа: https://tech.mail.ru/product/involving/?utm_source=yandex.direct.DB&utm_medium=cpc&utm_campaign=y_hr_solutions_and_teams_poisk_general_rf_66885055&utm_content=11312495032&utm_term=цифровые%20коммуникационные%20платформы&yclid=6740025746395292304(дата обращения 15.11.2021)
23. Платформа для управления IT-инфраструктурой в ритейле и e-commerce. [Электронный ресурс]. -Режим доступа:

- https://www.ispsystem.ru/industries/retail?yclid=6740152110456824469&utm_source=yandex&utm_medium=dsa&utm_campaign=ISPS-Content-RU-YANDEX-DSA&utm_content=4689519462&utm_term=&roistat=direct1_search_11150688137_Фильтр%20ispmanager&roistat_referrer=none&roistat_pos=premium_1(дата обращения 15.11.2021)
24. Abanking Digital Office. [Электронный ресурс]. -Режим доступа: https://ado.abanking.ru/?utm_source=google&utm_medium=cpc&utm_campaign=ado_poisk&utm_content=digital_ru (дата обращения 15.11.2021)
25. Интеллектуальное предприятие. [Электронный ресурс]. -Режим доступа: https://www.sap.com/cis/products/intelligent-enterprise.html?campaigncode=CRM-RU21-PPC-S4HCLEN&source=ppc-cis-GOO-%25epid!----&DFA=1&gclid=CjwKCAiAm7OMBhAQEiwArvGi3Kxc3Z1UfFDFOrMKGvMikJOiiYrQwewx20_4K3QUvF-Pu2sb8LKcbRoCYFYQAvD_BwE (дата обращения 15.11.2021)
26. DigiWave. Платформа цифрового банкинга. [Электронный ресурс]. - Режим доступа: <https://www.softwaregroup.com/ru/platforma-digiwave>(дата обращения 15.11.2021)

Состояние мирового рынка аудиторских услуг и его тенденции развития

С.В. Сергеев

студент 2 курса НИЯУ МИФИ, Москва

E-mail: SVSergey.sergeev@yandex.ru

П.М. Абдуллаева

студентка 2 курса НИЯУ МИФИ, Москва

E-mail: a.patimat98@yandex.ru

Н.С. Белогина

к. э. н., доцент кафедры бухгалтерского учета и аудита

НИЯУ МИФИ, Москва

E-mail: nsblog@gmail.com

Аннотация: В статье на основе анализа публикаций в периодических изданиях, сайтов аудиторских компаний, исследований и отчетов «Большой четверки», новостных публикаций за период с 2017 по 2021 год рассматривается состояние глобального аудита и его тенденции в ближайшей перспективе.

Ключевые слова: аудиторские торги, большие данные, конфликт интересов, консалтинг, кибербезопасность, мониторинг инфраструктуры, престиж профессии аудитора, многонациональные компании.

The state of the global audit services market and its development trends

Abstract: Based on the analysis of publications in periodicals, websites of audit companies, research and reports of the "Big Four", news publications for the period from 2017 to 2021, the article examines the state of global audit and its trends in the near future.

Keywords: audit trades, big data, conflict of interest, consulting, cybersecurity, infrastructure monitoring, prestige of the auditing profession, multinational companies.

Введение. В последнее время можно все больше наблюдать трансформацию экономики, в том числе большого ряда профессий в связи с глобализацией и цифровизацией. Данные изменения не могут не

коснуться аудиторской профессии, которая, в свою очередь, должна отреагировать на данные факторы, чтобы сохранить востребованность на глобальном рынке. Однако, помимо технологического прорыва, мировой аудит сталкивается с другими вызовами, такими как монополизация рынка, потеря доверия общественности, падение качества услуг, а также падение общего уровня престижа профессии.

Рассмотрим ключевые факторы, отражающие и влияющие на текущие тенденции в индустрии аудита.

Тенденции в доходах и росте компаний. За период с 2017 по 2021 год спрос на консультационные и аудиторские услуги вырос, о чем можно судить по увеличению объемов продаж и количества нанятого персонала «Эрнст энд Янг», «Делойт», «Прайсвотерхаускоперс» и «КПМГ». Так, в компании Делойт с 2017 по 2021 число сотрудников увеличилось на 42% и составило 345 тыс. человек по всему миру (Рис. 1).

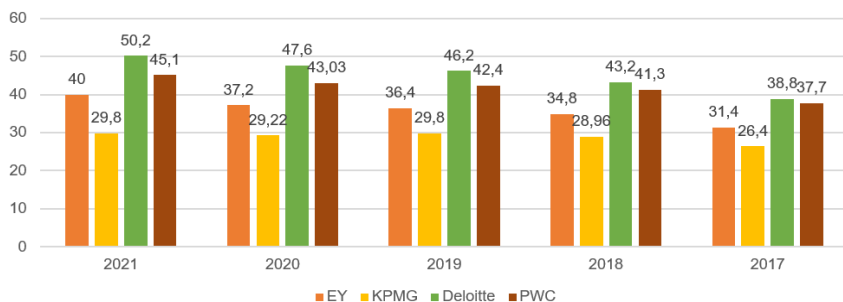


Рисунок 1 – Показатели выручки «Большой четверки» за 2017-2021 года, млрд долл. [1]

Компании «Big 4» обычно предлагают три вида услуг: аудит, налогообложение и консультирование. Хотя организации в основном позиционируются как аудиторы, непосредственно на аудит приходится в среднем всего 40% от выручки. Это вызвано тем, что консультационные услуги помогают компании выстраивать успешный бренд, а также они имеют большую рентабельность по сравнению с аудитом.

В связи с этим в последние годы транснациональные компании в области аудита начали повсеместно осуществлять сделки по покупке консалтинговых организаций, тем самым осуществляя коммерциализацию. Для примера, сегодня можно обратиться в одну из компаний «Большой четверки» с потребностью или запросом совершенно различной направленности, и, с большей вероятностью, у данных компаний найдутся решения от помощи в построении налогового учета до проведения аудита

корпоративной отчетности по новой ESG-стратегии, нормативна база по которой даже еще закреплена в российском законодательстве.

Данный фактор не может не вызывать беспокойство у широкой общественности и регулирующих органов, поскольку с ростом оказания консультирования все сложнее поддерживать независимость и надлежащее качество аудиторских проверок, так как разная специфика консультирования и аудиторских услуг ведет к конфликту интересов внутри организаций.

Необходимо отметить следующие риски:

- Практика предоставления гарантий может оказаться под давлением из-за отставания от роста продаж или прибыли консультирования;

- Возникновения конфликта из-за выбора в пользу реализации коммерческих целей, а не осуществления классических аудиторских услуг;

- При выборе между консультированием или аудитом компании могут выбирать консультационные услуги вместо аудиторских обязательств из-за меньшего риска и большей прибыли;

- По мере роста консалтинговых услуг и увеличения доли продаж руководители компаний и партнеры по аудиту могут уделять больше внимания направлению консалтинга компании, а не практике обеспечения гарантий.

Как уже ранее упоминалось, при изучении проблемы роста консультирования в аудиторских фирмах следует учитывать положительные факторы от их реализации, помимо возрастания рентабельности:

- повышение узнаваемости и престижа бренда компании на рынке аудиторско-консалтинговых услуг;

- создание дополнительных стимулов для привлечения нового персонала (что необходимо «Большой четверке» из-за большого показателя текучести кадров);

- расширение личных контактов с клиентами, в том числе для проведения последующего аудита;

- диверсификация рисков в условиях кризиса путем предоставления услуг разной направленности.

По новостным публикациям «Интерфакс» от 2020 года для минимизации рисков, описанных выше: «Совет по финансовой отчетности (Financial Reporting Council, FRC) предписал аудиторам PwC, KPMG, EY и Deloitte отделить аудиторские операции от остального бизнеса. Financial Times назвала это крупнейшей за несколько десятилетий реформой аудиторской отрасли. Компании должны представить на рассмотрение FRC планы разделения аудиторских и консалтинговых операций до 23

октября текущего года, и на реализацию этих планов им отведено время до июня 2024 года» [5]. FRC 6 июля разъяснил основные цели, которых он планирует достичь за счет реорганизации отрасли. Главной целью он назвал «улучшение качества аудита за счет гарантирования того, что люди, занятые в аудиторской практике, фокусируются, прежде всего, на обеспечении качественного аудита в интересах общества» [5].

Конкуренция на рынке аудита. Несмотря на падения уровня доверия к рынку аудита и снижение качества проверок за последние годы, аудиторы продолжают оставаться необходимыми игроками в глобальной экономике, поскольку, во-первых, проведения внешнего независимого аудита для определенных организаций закреплено законодательством стран, а во-вторых, с точки зрения инвестирования компания считается более привлекательной, если она была проаудирована, в особенности одной из компаний «Big 4». Поэтому спрос на аудит вне зависимости от многих факторов, даже таких как кризисы и пандемия COVID-19 в 2020 году, остается стабильным из-за его неэластичности. Однако проблема данной ситуации в том, что в основном данный спрос удовлетворяют только четыре компании, борьба между которыми разворачивается уже не в ценовом сегменте, а в позиционировании бренда.

В соответствии с данными фактами барьер для входа на рынок слабый малых аудиторских фирм, однако для того, чтобы можно было претендовать на аудит крупных публичных интернациональных корпораций и участвовать в тендерах, необходимо обладать количеством ресурсов, сравнимым с «Большой четверкой», что в современных реалиях практически невозможно. К тому же дополнительные препятствия для новых аудиторов создают следующие факторы со стороны «Big 4»:

- Накопленный опыт и всеобъемлющая практика по всему миру, в том числе знания в применении аудиторских и бухгалтерских стандартов;
- Разная направленность деятельности позволяет при проведении аудита привлекать специалистов из других отделов внутри фирмы;
- Существенные судебные и страховые издержки, которые может не в силах покрыть компания, вне периметра «Большой четверки» и остальных крупных глобальных аудиторов;
- Большие финансовые и нефинансовые издержки для аудируемых лиц при смене аудиторов.

В последние годы во многих странах регулирующими органами началась работа для принятия и внедрения специальных мер по стимулированию конкуренции на рынке аудиторских услуг, что должно укрепить независимость аудиторского рынка в целом. Данные структурные изменения и реформы проводятся с целью поддержки аудиторских компаний среднего размера, которым тяжело входить на рынок,

монополизированный «Большой четверкой». Примерами реализаций специальных мероприятий является, в первую очередь, введение тендерной основы для выбора аудиторского лица и обязательная ротация, а также стимулирование расширенных совместных проверок. В качестве последнего можно сразу вспомнить назначение аудиторами ЦБ РФ PwC и ФБК одновременно.

Также примером изменений может служить сама Великобритания, в которой расширилась практика проведения аудиторских торгов и изменений в аудиторах среди крупных компаний, котирующихся на бирже. Однако изменения, по-видимому, оказали ограниченное влияние на конкуренцию, поскольку большинство крупных компаний продолжали привлекать аудиторскую фирму «Большой четверки» в качестве аудитора. Так данные, опубликованные аудиторским наблюдателем Совета по финансовой отчетности FRC, показали, что EY, KPMG, Делойт и PwC провели аудит всего FTSE 100 в 2019 году, а также доминировали в FTSE 250, и только две фирмы, не входящие в «Большую четверку», провели аудит по меньшей мере 10 компаний в индексе.

Таким образом, монополизация рынка до сих пор остается неразрешимой задачей для регуляторов. В условиях слабой конкуренции меньше стимулов для повышения качества аудита. Об этом также говорит тот факт, что «Большая Четверка» аудиторов сформировала £162 млн резервов в 2020 году на оплату штрафов за недобросовестный аудит, поскольку ранее согласно новостному portalу «Финансовый учет»: «расследование FRC (британского Совета по финансовой отчетности) выявило 30 предполагаемых случаев недобросовестного проведения аудита» [6].

Влияние новых технологий на аудит

Активное развитие технологий в различных областях вносит изменения в «традиционную» деятельность аудиторских компаний и оказывает влияние на представления о профессии аудитора. Во-первых, инновации в части анализа больших данных путем применения алгоритмов в ближайшем в будущем смогут повысить качество аудита, так как появится возможность с меньшей погрешностью выполнять аналитические процедуры и процедуры проверки по существу. Вместо выборочного подхода планируется рассматривать все секции отчетности по 100 процентам бухгалтерских операций. Это позволит на этапе планирования аудита и изучения бизнес-процессов сформировать более полную картину о «слабых» местах учета и системы внутреннего контроля аудируемых лиц с целью акцентирования внимания на этих областях в последующей проверке.

С повышением обоснованной уверенности в достоверности финансовой отчетности должен, как ожидается, повыситься и уровень и общественного доверия к аудиту, в особенности со стороны инвесторов. Однако для достижения данной цели аудитором необходимо производить огромные инвестиции в свои технологии, на что на данный момент способны в основном только монопольные компании «Большой четверки». Так, в данных фирмах за последний год были разработаны курсы тренингов по цифровизации: машинное обучения, создание сайтов, интернет-вещей, блокчейн и т.д. Все это говорит о том, что сейчас возрастает спрос не на просто аудиторов, а на «технических аудиторов».

Однако речь о высоких технологиях в отношении аудита идет в основном только в контексте будущего времени, поскольку в условиях слабой конкуренции наблюдается мало стимулов для повышения качества аудита и практическое внедрение инноваций.

Также в дополнение к вышеперечисленным пунктам следует сказать, что в последнее десятилетие в соответствии с «Концепцией развития аудиторской деятельности в Российской Федерации до 2024 года»: «В последние годы наблюдается падение престижа аудиторской профессии. В определенной степени данное явление порождено влиянием общей экономической ситуации на аудиторский рынок. В то же время не создана действенная система мотивации наиболее профессиональных и опытных работников с целью удержания их в аудиторской профессии. Молодые специалисты демонстрируют крайне низкий уровень заинтересованности в получении аудиторской профессии» [8].

Вектор развития международной аудиторской деятельности в эпоху глобализации экономики. С середины прошлого столетия происходит непрерывная глобализация в мировом пространстве. В частности, одной из сфер, на которые данные процессы оказывают существенное влияние, является экономика. В данном случае аудиторские и консультационные услуги как составная часть экономики не стали исключением.

Создание сетей аудиторских компаний является тому подтверждением. Например, «Большая четверка» в лице Deloitte в РФ представлена следующими организациями: АО «Делойт и Туш СНГ» и ООО «Делойт Аудит». Сети аудиторских организаций в основном формируются для цели обеспечения эффективного взаимодействия входящих в них организаций, а также должного распределения ответственности и должностных функций между ними. В то же время данные компании используют единый бренд, систему контроля качества и профессиональные ресурсы, а также имеют общую стратегию и задачи для ее осуществления.

Трансформация аудита и аудиторской профессии заключается в применении новых интернет-технологий, ПО, технологий блокчейн,

способных в короткое время автоматизировано обрабатывать большой объем данных, которые раньше приходилось анализировать зачастую вручную. Аудит все ближе к переходу от выборочного подхода к повсеместному контролю, что будет приближать «разумную уверенность» в достоверности финансовой отчетности к «абсолютной». Технологии будут способны распознать девиации в бухгалтерских транзакциях, сделанные неавторизованным или недопустимым лицом в праздничный день.

Необходимость обработки больших объемов данных также вызвана фактором глобализации: расширения, объединения компаний по всему миру. В данном ключе аудит сможет справиться с поставленными вызовами только если будет использовать преимущества инноваций: электронный документооборот, цифровые подписи, высокая скорость и небольшая стоимость передачи информации.

Одновременно с достоинствами применения новых технологий появляются и негативные факторы глобализации в виде кибератак на системы баз данных. В данном случае аудиторская тайна представляет собой наибольший интерес, поскольку утечка конфиденциальной информации и нарушения доступа к ней может приводить к различным судебным разбирательствам с аудируемыми лицами, что влечёт за собой риск подрыва имиджа компаний и повышение издержек как с точки зрения самих судебных расходов, так и с точки зрения дополнительной защиты базы данных.

Директор по инновациям Deloitte Джон Рафаэль так оценивает автоматизацию в аудите: «Автоматизация рабочего процесса, средства анализа данных и искусственный интеллект фундаментально меняют процесс аудита» [10]. Сегодня компания Deloitte обладает технологиями Argus. Данная программа очень быстро подбирает из разных документов бухгалтерскую информацию. Вице-президент компании PwC Ричард Секстон также подчеркивает влияние новых технологий на аудит: «Как только начинаешь применять искусственный интеллект и компьютерный анализ данных, эффективность повышается невероятно» [10].

Новые технологии вынуждают компании развивать системы безопасности и увеличивать осведомленность персонала с области цифровизации и работе с данными. В противном случае аудиторские компании будут уязвимы, как минимум, к кибератакам.

В связи с вышеперечисленным есть опасения в сокращении рабочих мест, а также появляется потребность именно в специалистах в области математических наук, базы данных, умеющих создавать алгоритмы. Также будет меньше потребности в выпускниках университетов, которые первое время способны только заменять работу искусственного интеллекта. Даже

«типичные» инвентаризации при присутствии аудиторского лица будут проводиться и уже проводиться с использованием дронов и квадрокоптеров – это позволит сократить фирмам расходы на командировки сотрудников.

Выводы. Как итог, сейчас можно наблюдать трансформацию аудиторской деятельности, которая должна в большинстве случаев закончиться в ближайшем десятилетии. Это с большей вероятностью может повлиять на выборочный подход к аудиту, что может повысить его качество, и, как следствие, доверие со стороны общественности. Однако стоит понимать, что использование инноваций в основном доступно крупным игрокам рынка глобального аудита по причине низкой конкуренции, и данный фактор может только повысить барьеры для входа новых игроков и, как следствие, усилить монополизацию. Также коммерциализация в последние десятилетия стала новой угрозой для качества аудита вследствие большой рентабельности у консультационных услуг.

Список использованных источников:

1. <https://big4accountingfirms.com/>;
2. http://www.consultant.ru/document/cons_doc_LAW_71765/9dbadedfc5ede08e8d9d8713bbd319ebde3409ea/;
3. <https://www.cpajournal.com/2020/01/03/a-2020-global-auditing-forecast/>;
4. <https://www.iaasb.org/publications/iaasb-strategy-2020-2023-and-work-plan-2020-2021>;
5. <https://www.interfax.ru/world/716193>;
6. <https://fin-accounting.ru/financial-news/2020/big-four-accountants-162m-provisions>;
7. https://pcaobus.org/news-events/speeches/speech-detail/remarks-on-the-global-audit_445
8. https://minfin.gov.ru/ru/document/?id_4=132327-kontseptsiya_razvitiya_auditorskoi_dyeyatelnosti_v_rossiiskoi_federatsii_d_o_2024_goda
9. https://minfin.gov.ru/ru/performance/audit/reestr_audit/net/?id_65=116722-poryadok_vedeniya_perechnei_setei_auditorskikh_organizatsii;
10. <https://www.vedomosti.ru/finance/articles/2016/05/11/640538-auditorskim-kompaniyam-ne-nuzhni-auditori>;
11. Федеральный закон от 30 декабря 2008 г. № 307-ФЗ «Об аудиторской деятельности».

Состояние, перспективы и риски развития рынка металлов платиновой группы в постпандемийной экономике

И.А. Степанов
аспирант 1 курса НИЯУ МИФИ, Москва
E-mail: stepanovilya13@gmail.com

Аннотация: В статье выполнен обзор рынка металлов платиновой группы (МПП) в 2020-2021 годах, проведен анализ факторов, ограничивающих рост рынка в текущих условиях, а также оценено влияние последствий пандемии на дальнейшую динамику спроса на металлы. Выявлены и описаны риски происходящих в текущий момент процессов на рынок МПП в среднесрочной и долгосрочной перспективе.

Ключевые слова: металлы платиновой группы, рынок МПП, рыночные риски, пандемия, дефицит чипов.

Situation, prospects and risks of platinum group metals market development in the post-pandemic economy

Abstract: The article presents platinum group metals market overview in 2020-2021, conduct factors analysis which limiting the growth of the market in the current conditions, and also estimates the impact of pandemic consequences on the further demand dynamics for PGM's. The paper identifies and describes the risks of the processes currently taking place on the PGM's market in the medium and long term.

Keywords: platinum group metals, PGM market, market risks, pandemic, chip shortage.

В 2020 году мировая экономика вошла в фазу глубокого кризиса, который, как считают эксперты, продлится не один год, главной причиной которого, несомненно, можно считать пандемию COVID-19. Кризисные явления в разной степени затронули все сферы, включая цепочки поставок, общественные и корпоративные ценности и приоритеты, политику производства и сбыта товаров и услуг по всему миру.

Исключением не стал и рынок металлов платиновой группы. Металлы платиновой группы (МПП) — общее название группы из шести химических элементов (рутений, родий, палладий, осмий, иридий, платина), имеющих схожие физические и химические свойства, являющихся благородными,

драгоценными металлами. Их добыча зачастую заключена в единый производственно-технологический процесс, поэтому на предложение всех металлов платиновой группы оказывают влияние общие факторы. Связаны эти факторы с геологическими запасами МПГ и уровнем их добычи крупными горно-металлургическими компаниями.

Чтобы определить состояние рынка МПГ, необходимо привести данные за доковидный 2019 год, сопоставив их с данными за 2020 год, сравнить эти значения и проанализировать выявленные закономерности. Включать в исследование более ранние периоды не имеет практического значения для исследования.

В целях выявления состояния рынка целесообразно сосредоточить внимание и рассматривать лишь три металла: палладий, платина и родий. В таблице 1 приведена информация по ценам на МПГ, а также объемам рынков в физическом и денежном выражениях в 2019-2020 гг., которая объясняет выделение лишь трех металлов для дальнейшего исследования.

Таблица 1 – Цены и объемы на металлы платиновой группы в 2019-2020 гг.[5]

Металл	Средняя цена \$/Toz		Объем рынка тонн		Объем рынка млн \$	
	2019	2020	2019	2020	2019	2020
Палладий	1 538	2 197	345	302	17 059,11	21 331,33
Платина	863	884	236	202	6 547,93	5 740,96
Родий	3 904	11 231	36	32	4 518,49	11 554,45
Рутений	n/a	n/a	n/a	n/a	1 109,37	1 178,12
Иридий	n/a	n/a	n/a	n/a		
Осмий	n/a	n/a	n/a	n/a		

Из данных таблицы видно, что в 2019 году на рутений, иридий и осмий суммарно пришлось 3,8% всего объема рынка МПГ в денежном выражении, а в 2020 году их доля снизилась до 3%.

Иридий, осмий и рутений не нашли столь широкого промышленного применения, являются нишевыми металлами, используемыми узконаправленно. Данный факт подкрепляет рыночное наблюдение, что спрос в зависимости от металла имеет более выраженную дифференциацию, обуславливая существенные отличия в цене, объемах и условиях торгов на площадках.

Стоит отметить, что пандемия оказала минимальное воздействие на добычную деятельность основных производителей металлов, а падение цен

в марте-апреле 2020 года было быстро перекрыто стремительным ростом во втором полугодии.

Из рисунка 1, на котором представлены цены платины и палладия за 2019-2020 гг., видно, что восходящий тренд несмотря на пандемию продолжился [5].

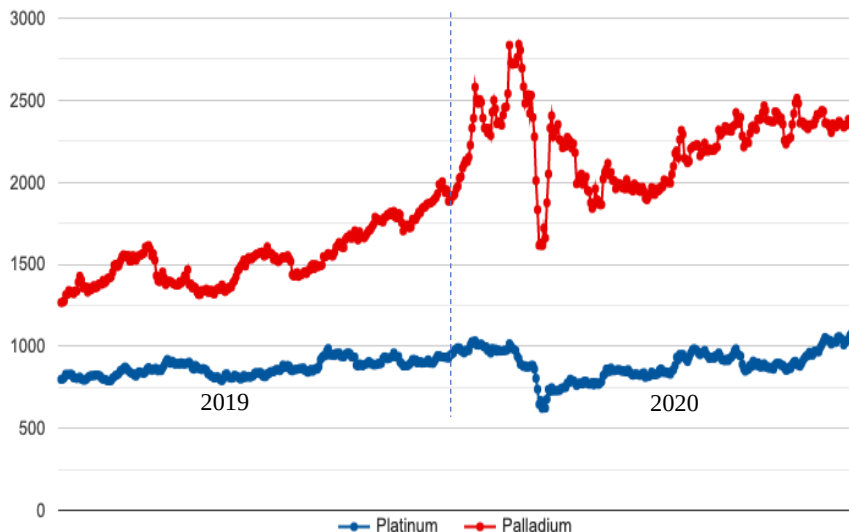


Рисунок 1 – Динамика цен на платину и палладий в 2019-2020 гг.[5]

В начале 2020 года цены на палладий достигли локального исторического максимума в 2795 \$/Toz, сохранив восходящий тренд на фоне высокого промышленного спроса, а также недостатка металла в запасах для спотового покрытия пиков.

Из рисунка 1 видно, что волатильность котировок, вызванная распространением новой коронавирусной инфекции, привела практически к полной остановке конвейеров по сборке автомобилей. Падение спроса привело к резкому снижению цен на палладий в первом полугодии 2020 года, однако, сложившейся v-образный эффект восстановления экономики в ключевых отраслях потребления, обеспечил прирост средней цены на палладий на 42,9% по итогам 2020 относительно предыдущего периода.

Чтобы понимать влияние автороизводителей на палладиевый рынок, на рисунке 2 приведена отраслевая структура потребления металла в 2020 году.



Рисунок 2 – Отраслевая структура потребления палладия в 2020 году [1]

Оживление рынка в мае-июне 2020 года произошло во многом благодаря более быстрого, чем ранее ожидалось, восстановления цепочек поставок автомобильной промышленности, а также из-за приостановки работ на добычных и перерабатывающих мощностях в Южной Африке [4].

Дополнительная поддержка цен на палладий возникла из-за денежно-кредитных и фискальных мер поддержки экономики, выполненных центральными банками и правительствами по всему миру. Комплекс этих мер привел к ослаблению доллара США и отрицательной реальной доходности по казначейским облигациям в ключевых странах.

На рисунке 3 видно, что потребление палладия в промышленности снизилось в 2020 году только на 43 тонны (–14%) по сравнению с предыдущим годом и составило 302 тонны.



Рисунок 3 – Потребление палладия в промышленности в 2019-2020 гг. [1]

Что касается платины, то цена на нее в январе — феврале 2020 года была относительно стабильной и находилась в узком диапазоне 900 – 1000 \$/Toz, прежде чем в марте упала до минимума за десятилетие в 600 \$/Toz. Тем не менее цена быстро восстановилась до уровня в 800–850 \$/Toz.

Во втором полугодии 2020 года рост цены на платину продолжился, и к концу года она достигла показателей августа 2016 года на уровне в 1050\$/Toz, на что повлияли поломки на пирометаллургическом переделе компании Anglo American Platinum и повышенный инвестиционный спрос, выразившийся в притоке в ETF-фонды (+16 тонн) и росте розничных инвестиций (+11 тонн) [4]. Среднегодовые чистые спекулятивные позиции

на Нью-Йоркской товарной бирже снизились на 4%, до уровня в 49 тонн. Резюмируя ценовую динамику по платине, можно сказать, что средняя цена в 2020 году выросла на 2% в сравнении с аналогичным показателем за 2019 год.

У платины, в отличие от палладия более диверсифицирована потребительская структура, на что указывают данные, приведенные на рисунке 4.



Рисунок 4 – Отраслевая структура потребления платины в 2020 году [1]

В ювелирной промышленности (второй по объему потребления платины после автомобильной) потребление платины в 2020 году продолжило сокращаться, что связано с падением спроса на предметы роскоши в связи с пандемией и растущей конкуренцией с золотыми изделиями [4].

Из-за ограниченного объема предложения и влияния пандемии, промышленное потребление платины в 2020 году снизилось на 34 тонны или на 15% до 202 тонн по сравнению с предыдущим годом, что находит отражение на рисунке 5.



Рисунок 5 – Потребление платины в промышленности в 2019-2020 гг.[1]

Таким образом, можно сделать вывод, что рынок платины в 2020 году перешел в состояние баланса — производства металла было даже недостаточным для удовлетворения потребления за счет сильного инвестиционного спроса, который привел рынок платины в состояние дефицита, покрытого из ранее накопленных запасов металла. Источниками

предложения платины из ранее накопленных запасов на рынке являются торговые компании и финансовые организации.

Ситуация, сложившаяся на рынке родия кардинально отличается от всех МПГ. Еще до 2019 года цена на металл колебалась в диапазоне 1000-2000\$/Toz. и ввиду маленького объема рынка, составляющего в среднем около 30 тонн, его следовало включить в группу к иридию, рутению и осмию. Но начиная с середины 2019 года цена на металл начала рост (рисунок 6).



Рисунок 6 – Динамика цен на родий в 2019-2020 гг.[5]

В таблице 2 представлены среднегодовые цены на родий с 2015 по 2020 год с указанием прироста относительно предыдущего периода.

Таблица 2 – Среднегодовые цены на родий в 2015-2020 гг. [5]

Металл	2015	2016	2017	2018	2019	2020
Родий	952	694 (-27% г/г)	1 105 (+37% г/г)	2 220 (+101% г/г)	3 904 (+76% г/г)	11 231 (+188% г/г)

С 2018 года начался бурный рост цены на родий, обусловленный резким повышением спроса на металл за счет целого комплекса факторов, среди которых: небольшой размер рынка, рост потребления металла в автопроме за счет введения новых стандартов контроля выбросов выхлопных газов автомобилей, непрозрачность запасов в Южноафриканском регионе, производство в котором считается наиболее нестабильным.

В марте 2020 цена на родий достигала локального максимума в 13,8 тыс. \$/Toz, однако в связи с распространением коронавирусной инфекции она упала на 60%.

Тем не менее уже в начале апреля котировки находились на уровнях в 8–9 тыс. \$/Toz. Во втором полугодии 2020 года по мере восстановления автомобильной промышленности, смягчения карантинных ограничений, а также в связи с поломками на пирометаллургическом переделе компании Anglo American Platinum цена на родий продолжила рост и в конце декабря достигла нового максимального уровня в 17 тыс. \$/Toz.

В 2021 году цены на палладий, платину и родий находятся в условиях ограниченного роста. Так, средняя цена на палладий за 10 месяцев 2020 года составила 2358 \$/Toz, на платину – 995 \$/Toz, на родий 15769 \$/Toz.

Говоря про ограниченный рост, важно затронуть те риски, реализованные в 2021 году и связанные с последствиями постпандемийной экономики.

Оптимизм на рынке МГП, возникший во втором полугодии 2020, наткнулся в 2021 году на серьезный вызов падения спроса стороны автомобильной промышленности. Производства автомобилей по всему миру оказались вынуждены резко сокращать объемы выпуска вплоть до остановки производств из-за возникшего дефицита чипов (Chip shortage).

На приведенном ниже рисунке 7 показано сравнение прогноза производства легковых автомобилей крупнейшей исследовательской компанией по автомобильному рынку LMC Automotive Limited на декабрь 2020 года с их представлением в октябре 2021 [2]. Различия в прогнозных значениях подчеркивают серьезные последствия нехватки чипов в 2021 и 2022 годах.

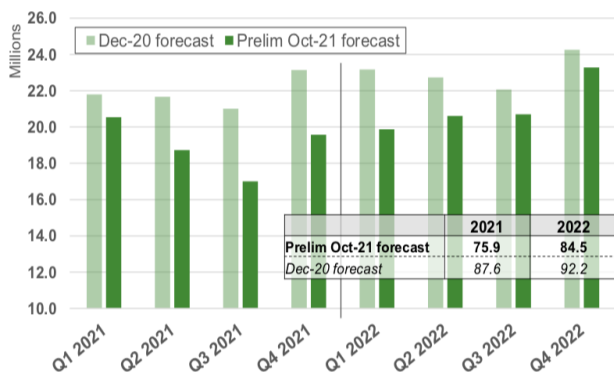


Рисунок 7 – Прогноз производства легковых автомобилей, млн штук [2]

В настоящее время ожидается, что нехватка микросхем повлияет на мировое производство легких транспортных средств на 10 млн автомобилей в 2021 году [3].

Однако в статье не стоит задачи рассмотреть обстоятельства возникновения дефицита микросхем. Важной задачей является классификация и описание групп рисков, способных наряду с дефицитом чипов кардинально изменить состояние рынка МГП в постпандемийной экономике. В таблице 3 представлена классификация рисков на рынке МГП и их проработка.

Таблица 3 – Классификация и анализ рисков на рынке МГП

Группа риска	Описание	Степень влияния	Вероятность возникновения/ Предсказуемость/ Управляемость
Падение спроса на МГП	Переход на более дешевый субститут или риск снижения потребления в ключевых отраслях; экономический спад	высокая на палладий; средняя на платину; низкая на родий	высокая/ средняя/ средняя
Аварии при добыче МГП	Остановка производства, снижения предложения металла	Высокая	средняя/ низкая/ низкая
Преобладание спекулятивных сделок над физическими	Переход металлов из промышленных к инвестиционным, накопление металлов в банках	средняя на палладий; высокая на платину; низкая на родий	высокая/ высокая/ низкая

Таким образом, перспективы развития рынка МПГ остаются неоднозначными. Не беря в расчет дефицит чипов, в долгосрочном периоде уже сейчас появляются мнения, что палладий переоценен, поскольку его применение в электрических автомобилях, чья доля в ежегодном производстве будет неуклонно расти, не требуется. Вызовом для палладия в ближайшем будущем будет поиск альтернативных сфер применения, которые будут готовы к его использованию на текущих ценовых уровнях.

Для платины, наоборот, предсказывают суперцикл, в котором она способна частично заместить палладий в производственном потреблении, а также встать на один уровень с золотом и серебром в качестве инвестиционного металла.

Что касается родия, то из-за его редкости и неотируемости на бирже волатильность цен на металл продолжится в будущем. Благодаря своим

уникальным физико-химическим свойствам поддержка цен на текущих уровнях и дальнейший рост в среднесрочном периоде вполне ожидаемый сценарий поскольку постепенное увеличение предложения микросхем во второй половине 2022 года разогреет производство легковых автомобилей прогнозные значения которых в 2021 и 2022 годах достигнут 75,9 млн (+2% г/г) и 84,5 млн (+11% г/г) соответственно.

Список использованных источников:

1. Годовой отчет ПАО «ГМК «Норильский никель» за 2020 год. URL: <https://ar2020.nornickel.ru>.
2. Global Semiconductor Shortage: Update on Vehicle Production / LMC Automotive Limited, Flash Alert, 27 October 2021. URL: <https://lmc-auto.com/wp-content/uploads/2021/05/LMC-Global-Semiconductor-Shortage-Impact-Assessment-Update-on-Vehicle-Production-12-MAY-2021.pdf>.
3. PGM Supply and Demand Update – Semi-conductor Impact / BASF, October 2021. URL: <https://www.basf.com/global/en/media/news-releases/2021/10/p-21-348.html>
4. Pgm market report / Johnson Matthey, February 2021. URL: <http://www.platinum.matthey.com/documents/new-item/pgm-market-reports/pgm-market-report-february-2021.pdf>.
5. Matthey Precious Metals Management (PMM). URL: <http://www.platinum.matthey.com/prices/price-charts>.

Социальная инженерия и конструирование «несовершенного пользователя» в кибербезопасности

А.А. Новопавловский

аспирант 1 курса НИЯУ МИФИ, Москва

E-mail: mr.novopavlovskiy@mail.ru

К. Верейкин

аспирант 1 курса ИАТЭ НИЯУ МИФИ, Обнинск

E-mail: kirill_vereikin@mail.ru

Аннотация: На сегодняшний день методы социальной инженерии являются наиболее распространенным способом совершения киберпреступлений путем вторжения и заражения компьютерных систем. Первостепенно описывается, как риторическая фигура неполноценного пользователя строится по отношению к понятиям безопасности в социальной инженерии. Во-вторых, исследуется нормативная напряженность, которую создает эта практика. Эмпирически выработанный анализ основывается на этнографии многосетевой кибербезопасности, а также на обширном анализе документов. Результаты, полученные в результате анализа, предполагают перераспределение институциональной ответственности между отдельными пользователями посредством трех различных сюжетных линий социальной инженерии — “забывчивый сотрудник”, “говорящий код и социальные сети” и “исправление человеческих недостатков”.

Ключевые слова: кибербезопасность, социальная инженерия, политика создания дефицита, секьюритизация, устойчивость, критические исследования безопасности.

Social engineering and the construction of the «imperfect user» in cybersecurity

Abstract: Today, social engineering methods are the most common way to commit cybercrimes by invading and infecting computer systems. First, we will show how the rhetorical figure of an inferior user is constructed in relation to the concepts of (b)security in social engineering discourses. Secondly, we investigate the normative tension that this practice creates. Empirically, our analysis is based on the ethnography of a multi-network conference during three

cybersecurity conferences, as well as extensive document analysis. Our results suggest the redistribution of institutional responsibility between individual users through three different social engineering storylines — "forgetful employee", "talking code and social networks" and "correcting human shortcomings". Finally, we propose to open a discussion about social engineering and its inscribed policy of creating scarcity and securitization, and call on companies and politicians to create and develop a culture of collective cybersecurity and corporate responsibility.

Keywords: cybersecurity, social engineering, politics of deficit construction, securitization, resilience, critical security studies.

Введение

Сегодня методы социальной инженерии являются наиболее распространенным способом совершения киберпреступлений путем вторжения и заражения компьютерных систем и инфраструктур информационных технологий. Эксперты по кибербезопасности используют термин “социальная инженерия”, чтобы подчеркнуть “человеческий фактор” в оцифрованных системах. Как набор стратегий атаки, социальная инженерия относится к манипулированию людьми с целью раскрытия конфиденциальной информации. Наиболее известными, возможно, являются фишинговые атаки, когда ничего не подозревающих пользователей просят нажать на ошибочную ссылку и тем самым позволить хакерам установить вредоносное ПО и войти в систему. Во всех случаях атаки социальной инженерии включают в себя сочетание социальных взаимодействий и технологических подвигов, в результате чего специалисты по кибербезопасности в компаниях и правительственных организациях одинаково пытаются разработать эффективные контрмеры.

Теоретический подход

В дальнейшем в первую очередь исследуется социально-политические процессы и онтологические практики, с помощью которых неидеальный пользователь конструируется по отношению к понятиям безопасности в дискурсах социальной инженерии, и определяем соответствующие различия между этими позициями. Во-вторых, исследуется моральные и нормативные проблемы, которые создают эти практики, и подчеркивается, почему различия важны. Для этого теоретическая часть этой статьи связывает концепцию построения дефицита с работой CSS по повышению устойчивости в ответ на растущую секьюритизацию и связанные с ней неопределенности в области кибербезопасности.

Многие эксперты по кибербезопасности рассматривают атаки социальной инженерии как вопрос технической грамотности и знаний. Согласно этой точке зрения, инциденты безопасности происходят из-за

того, что сотрудник не соблюдал общепринятые методы обеспечения безопасности и не обнаруживал манипулятивные методы, используемые хакерами. Этот предполагаемый дефицит знаний считается основным вектором атаки, с помощью которого злоумышленники могут обойти меры безопасности и получить доступ к цифровой инфраструктуре. Такое формирование превращает подразумеваемого «неполноценного пользователя» в угрозу безопасности. Сообщается, что сотрудники, не обладающие надлежащими знаниями, чтобы обнаруживать подозрительные действия и соответствующим образом реагировать на них, нуждаются в дополнительном обучении, чтобы избежать риска для безопасности своего работодателя. Этот рассказ о пользователях как о недостатках, недостатках, или невежественный очень напоминает то, что ученые СС наблюдали в дискурсе вокруг общественного понимания науки и технологий (PUS). Традиционные подходы к PUS продвигают идею о том, что споры вокруг рисков и преимуществ научных достижений могут быть смягчены за счет улучшения научного общения и образования. Эта точка зрения не предполагает, что общественность является разумной группой участников, которые коллективно решают научные вопросы или устанавливают границы, основанные на моральных соображениях. Скорее, ожидается, что неинформированные части общественности действительно будут доверять мнению научного сообщества, если они будут разделять такую же (или достаточную) степень опыта и понимания.

В качестве аналитической линзы концепция секьюритизации позволяет нам проследить, как возникают проблемы безопасности и как субъекты рассматривают и коллективно реагируют на других участников, события и объекты как на угрозу. Кратко говоря, такая перспектива переключает внимание с рассмотрения безопасности как стабильного объекта или нематериального идеального понятия, с одной стороны, на изучение тех практик и субъектов, которые обеспечивают безопасность, с другой. Практики и рассуждения различных специалистов по безопасности придают определенные конструкции и обрамления (не) легитимности безопасности. Недавняя работа на пересечении CSS и STS специально посвящена часто рутинным методам и повседневным физическим действиям, посредством которых строится безопасность, и тому, как эксперты по кибербезопасности формируют процессы стабилизации проблем безопасности; то есть перемещение явлений из невидимой и нематериальной области в область, в которой с ними можно общаться, действовать и управлять ими. Сосредоточение внимания на «создании сетей профессионалов (не) безопасности, систем значений, которые они создают, и производительной силы их практик» помогает нам понять, как

практики и дискурсы социальной инженерии вместе составляют неполноценного пользователя как главную проблему кибербезопасности.

Методологический подход и полевые исследования

Наш анализ основан на исследованиях, материалы которых были взяты из трех международных конференций по кибербезопасности. Одной из конференций была Венская неделя кибербезопасности в январе 2018 года, нацеленная в основном на правительственные учреждения. Двумя другими конференциями были Black Hat и Defcon, которые прошли в Лас-Вегасе в июле 2017 года. Последние две являются ведущими мероприятиями в этой области, ежегодно собирая около 20 000 человек. Black Hat - это в большей степени корпоративная конференция, поскольку она в основном предназначена для ИТ-компаний, различных отраслей и стартапов, а также государственных учреждений, например, правоохранительных органов, финансов и оборонного сектора. Defcon - это более неформальная и творческая конференция, со смешанной аудиторией, от хакеров и ИТ-специалистов до журналистов, неправительственных организаций, занимающихся вопросами конфиденциальности, активистов, исследователей и, в меньшей степени, государственных служащих. В последние годы на обеих конференциях увеличилось количество докладов о «человеческом факторе» в кибербезопасности, и даже на 25-й конференции Defcon в 2017 году появилась, так называемая, «деревня» социальной инженерии (сопоставимая с разделом на академических конференциях).

В дополнение к растущему сообществу хакеров и практиков-самоучек, индустрия консалтинговых фирм определила небезопасность, связанную с социальной инженерией, как очень прибыльный рыночный пробел. Подобные конференции - это сейсмографы дискуссий, ключевых вопросов и социальных взаимодействий соответствующих месторождений и, следовательно, обширные площадки для антропологических исследований.

Мы проанализировали эмпирический материал, опираясь на подход Хаджера (2009) к аргументативному анализу дискурса, который в традиции Фуко понимает дискурс как «совокупность понятий, идей, концепций и категорий, посредством которых значение приписывается социальным и физическим явлениям, и который создается и воспроизводится в идентифицируемом наборе практик». Такой подход исследует и делает видимым, как и при каких условиях конкретный дискурс становится доминирующим. Особенно актуально для нашей статьи понятие сюжетных линий - сжатых ключевых элементов в остальном очень широкого и транснационального дискурса о социальной инженерии - вокруг которых дискурсивные коалиции организуются и навязывают свои взгляды на реальность другим.

Эмпирический анализ

Диагностика проблемы: невнимательный сотрудник

В то время как технологии и люди изображаются как векторы риска в киберфизических системах, именно подверженность человека ошибкам рассматривается как основная проблема в современных дискурсах о кибербезопасности. В ходе наших исследований стало видно, что люди считаются «самым слабым звеном», как, например, представлено в заявлении, что «пользователи - это проблема, не система». Здесь фигура «глупых людей» часто использовалась, чтобы указать на воспринимаемую неспособность пользователей адаптироваться к все более сложным социотехническим вызовам, создаваемым ИКТ, независимо от того, «сколько образования и подготовки им брошено». Эта конкретная цитата уже указывает на то, что пользователи считаются слишком наивными, чтобы позаботиться о каких-либо достаточных мерах защиты, или неспособными адаптировать меры предосторожности, такие как сложные пароли или двойная проверка телефонного звонка от предполагаемого коллеги, который запрашивает конфиденциальную информацию. Большинство экспертов по ИТ-безопасности полностью осознают тот факт, что сотрудники имеют дело с ситуацией, которую они активно не создавали и которая была немыслима несколько десятилетий назад. Интересно, что один из наших собеседников заявил, что бремя обеспечения безопасности своей компании умножилось на количество сотрудников, которые у них есть: «Некоторое время назад у вас был забор, охранник с фонариком и немецкая овчарка у ворот, а ваша помещения в основном охранялись».

Это утверждение прекрасно иллюстрирует вышеупомянутую индивидуализацию дискурса риска: риск в основном рассматривается как индивидуальный риск, который увеличивается с увеличением числа сотрудников. Как заявил этот собеседник, теперь они должны обеспечить безопасность сети, поскольку каждый сотрудник должен быть таким же осторожным и хорошо обученным в обнаружении подозрительной активности, как и охранник у ворот. В то же время собеседник признал, что условия труда и обязанности по деятельности, не связанной с безопасностью, могут ограничивать повседневную осведомленность о социальной инженерии, заявив, что «Конечно, это не основная работа людей. Это офисные работники, бухгалтеры, техники. Как они должны справляться с целенаправленными фишинговыми атаками, специально разработанными для них, при выполнении своих обычных дел?». Это утверждение - один из тех редких моментов, когда собеседники указывали на проблемы, которые возникают у сотрудников, когда им поручены действия, которые обычно выходят за рамки их ответственности, например, выявление вредоносного программного обеспечения. Однако в

большинстве учетных записей хакеров изображали как преступников, которые угрожают организациям, хотя часто с определенным восхищением их смекалкой, бесстрашием и новаторскими методами. Сотрудники, которые не могли предотвратить нападение, в свою очередь, были сочтены наивными и даже более опасными. По словам наших партнеров по интервью и в соответствии с академической литературой в этой области (в большинстве учетных записей хакеров изображали как преступников, которые угрожают организациям, хотя часто с определенным восхищением их смекалкой, бесстрашием и новаторскими методами. Сотрудники, которые не могли предотвратить нападение, в свою очередь, были сочтены наивными и даже более опасными. По словам наших партнеров по интервью и в соответствии с академической литературой в этой области, ключевое объяснение успеха социальной инженерии заключалось в том, что она вызывает эмоциональные предубеждения.

Роль экспертных знаний: разговорный код и общение

В этом разделе описывается, как экспертиза социальной инженерии создается, осуществляется и применяется на практике. Мы начнем с полевой заметки, сделанной в Defcon, о встрече между экспертом по социальной инженерии и группой участников конференции, которая произошла возле популярного бара ранним вечером, после того, как большинство переговоров были завершены.

Участник подошел к группе людей, ожидавших в очереди на сцену по социальной инженерии. Он предложил им небольшую баночку с перцем, по его словам, «очень острый перец, который заставит вас плакать, как младенцев». В конце концов, один из членов группы взял банку, высыпал немного красного порошка на тыльную сторону ладони и слизал ее. Толпа приветствовала его, когда он начал кашлять и рвать. Тот, кто протянул банку, улыбнулся и торжественно вручил ее ему: теперь настала его очередь выбрать кого-нибудь не из его группы для этого испытания. Этот обряд посвящения продолжался несколько раз, и почти все, кто принимал перец, оставались с группой.

Во время более позднего интервью с инициатором этого вызова выяснилось, что он делал это не для развлечения. Скорее, он был владельцем очень успешного бизнеса по «тестированию на проникновение». Он использовал это как способ тренировать свои навыки,

заставляя людей попадать в неудобные ситуации, которые им действительно нравились, благодаря создаваемому им чувству общности, а также для установления новых деловых контактов для своей компании. Его клиенты - в основном бизнес-корпорации, но также и государственные учреждения - нанимают его, чтобы проверить осведомленность своих сотрудников о рисках и тем самым, сознательно или нет, подвергнуть их экстремальному стрессу. После этого его компания сообщает об этих «нарушениях безопасности человека» руководству и предлагает обучение тому, как предотвратить эти «ошибки». По словам этого собеседника, каждый может стать жертвой этих атак, и чем сложнее кого-то «социально спроектировать»,

Эта заметка уже включает в себя некоторые ключевые элементы в конституции опыта социальной инженерии и процессы, посредством которых создается неполноценный пользователь. Во-первых, это показывает нам, что в большинстве случаев эксперты по социальной инженерии сочетают социальные навыки, необходимые для атак социальной инженерии, со своим техническим образованием и опытом. Однако, в отличие от других областей ИТ-безопасности, их эпистемический авторитет не зависит в основном от превосходных технических навыков. Скорее, их роль в качестве экспертов проистекает из того факта, что они могут говорить на обоих языках - «кодовом» и «социальном», - противопоставлении, которое часто использовалось как партнерами по собеседованию, так и ведущими. Таким образом, как утверждают эксперты, можно получить знания и понимание как человеческого поведения, так и технических аспектов. Это саморепрезентация затем создает основу, на которой специалисты по социальной инженерии могут действовать как мощные актеры секьюритизации, как мы часто наблюдали. Чтобы поддерживать свою бизнес-модель, они поддерживают и усиливают нарратив неотъемлемой незащищенности и постоянной угрозы, который говорит как о незащищенности человека, так и рассеивает опасения того, что он несет ответственность за риск для всей компании и делает технологию уязвимой для ошибок. Однако в случае, описанном выше, эксперт по социальной инженерии занимался разработкой своих коллег, тех, кто, возможно, уже несколько часов назад рассказывал о том, как избежать атак социальной инженерии. Хотя это происходило не на основной сцене конференции, а в относительно неформальной обстановке, это привлекло наше внимание к ключевому аспекту этой сюжетной линии, который поднимался во многих выступлениях, а именно, что «никто не в безопасности, Жертвой может стать каждый, даже эксперты». Он служит фундаментальной

предпосылкой для успешного предложения опыта для обучения людей, чтобы сделать их менее уязвимыми.

Заключение

В анализе описывается, как ответственность за кибербезопасность индивидуализируется с помощью трех различных сюжетных линий, а именно: «невнимательный сотрудник», «говорящий код и социальный код» и «исправление человеческих недостатков». Часто упоминаемая фигура «глупого пользователя», который подвержен социальной инженерии, коррелирует с переносом ответственности с коллективной заботы на отдельного сотрудника. Это также перекликается с более общей тенденцией к созданию «гибкой» рабочей среды, например, для работы из дома или политики «принеси свое собственное устройство», которая стирает границы между защищаемой организацией и зачастую менее обслуживаемой и секьюритизированная личная социотехническая среда сотрудников. В то время как тренинги по социальной инженерии предполагают, что пользователь по своей сути не замечает и не осведомлен, Намеренное стирание границ между работой и личной жизнью подвергает пользователей еще большему риску кибератак. Парадигма безопасности оставляет в стороне вопросы о том, почему возникли новые уязвимости, и о том, как коллективно бороться с ними более ответственными способами, а не с помощью технических исправлений или лоскутного одеяла руководств для пользователей, установленных компаний. Более того, эксперты по социальной инженерии редко учитывают более широкие последствия для рабочей силы при принятии мер по защите данных и коммуникаций компании. Напротив, все, что повышает безопасность, кажется законным шагом вперед и не требует дополнительного участия сотрудников компании. Однако, в отличие от сторонников научной грамотности, которые считают «просвещенного гражданина» достижимой целью, Эксперты в области социальной инженерии признают, что безопасность - это очень хрупкое, в лучшем случае временное состояние, предвосхищая известные неизвестные когда-либо новые формы атак. Затем концепция устойчивости используется как способ справиться с динамично изменяющимися социотехническими неопределенностями, возникающими в результате цифровизации, при этом оставаясь достаточно гибким, чтобы указывать на потребность пользователя «стать лучше» без обязательной реорганизации инфраструктур и стратегий ИТ-безопасности в более устойчивый способ.

Решение заключается не в каких-либо новых формах ориентированного на пользователя управления рисками, которые причиняют патологию отдельному пользователю, независимо от того, разбирается он в технологиях или нет. Вместо этого руководители компаний, регулирующие

органы и ИТ-инженеры должны решать проблему социальной инженерии на коллективном уровне, уделяя больше внимания возрастающей неопределенности и непредвиденным последствиям, к которым приводит текущий режим работы. Анализ, который был предложен, подчеркивает, как меняющиеся конфигурации режимов безопасности и неолиберальных режимов работы формируют создание новых социотехнических дефицитов и, в свою очередь, как политика создания дефицита играет в процессах секьюритизации и связанных с ними призывов к устойчивости. Признание неотъемлемой и неизбежной уязвимости киберфизических сетей и взаимодействий может тогда открыть возможности для построения доверия между руководством, ИТ-отделами и сотрудниками, а не защищать пользователя как не имеющего недостатка в очень сложных процессах поддержания кибербезопасности. Это внесло бы большой вклад в нормативную дискуссию, которая в настоящее время зарождается в сообществах ИТ-безопасности, с призывами как к компаниям, так и к политикам укрепить нормативно-правовую базу для устранения нарушений кибербезопасности, допущенных пользователями. Кибербезопасность - это неоднородный, постоянно пересматриваемый процесс, а не объективное условие или статус-кво, которые в конечном итоге должны быть достигнуты. Другими словами, это скорее повод для беспокойства, чем факт, поскольку его онтологический статус является одновременно политическим и открытым для оспаривания.

Взаимодействие с тем, как различные реальности кибербезопасности вводятся в действие и обсуждаются, важно для понимания политики создания дефицита, действующей в оцифрованной (рабочей) среде, и, в конечном итоге, для достижения культуры кибербезопасности, которая признает неизбежную уязвимость социотехнических систем и делает риск коллективным, а не индивидуальным предметом беспокойства.

Список использованных источников:

1. Abell, Sandra K., Lederman, Norman G., eds. 2007. *Handbook of Research on Science Education*. Mahwah, NJ: Lawrence Erlbaum Associates: 346–375.
2. Amoores, Louise, Goede, Marieke de, Eds. 2008. *Risk and the War on Terror*. New York: Routledge.
3. Balzacq, Thierry, Cavelty, Myriam Dunn. 2016. “A Theory of Actor-network for Cyber-security.” *European Journal of International Security*
4. Balzacq, Thierry, Léonard, Sarah, Ruzicka, Jan. 2016. “‘Securitization’ Revisited: Theory and Cases.” *International Relations* 30 (4): 494–531
5. Barnard-Wills, David, Ashenden, Debi. 2012. “Securing Virtual Space.” *Space and Culture* 15 (2): 110–23

6. Chandler, David . 2014. Resilience: The Governance of Complexity. Critical Issues in Global Politics.
7. Edwards, Paul N. 1997. The Closed World: Computers and the Politics of Discourse in Cold War America, First MIT Pr. Paperb ed. Inside Technology.
8. Falzon, Mark-Anthony , ed. 2009. Multi-sited Ethnography: Theory, Praxis and Locality in Contemporary Research.
9. Hajer, Maarten A. 2009. Authoritative Governance: Policy-making in the Age of Mediatization. New York: Oxford University Press.
10. Hommels, Anique, Mesman, Jessica, Bijker, Wiebe E., eds. 2014. Vulnerability in Technological Cultures: New Directions in Research and Governance. Inside Technology.

Социальная инженерия, как угроза экономической безопасности предприятия

А.В. Морозов

студент 3 курса НИЯУ МИФИ, Москва

E-mail: dc-1eX@yandex.ru

В.А. Рычков

старший преподаватель кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: VArYchkov@mephi.ru

В. Давыденко

старший преподаватель кафедры финансового мониторинга

НИЯУ МИФИ, Москва

E-mail: VIDavydenko@mephi.ru

Аннотация: В данной статье будут рассмотрены теоретические основы социальной инженерии, техники и виды атак. Показана прямая связь и зависимость с информационной и, как следствие, экономической безопасностью. Приведены примеры успешных атак на компании финансового сектора. Разработан комплекс рекомендаций по противодействию.

Ключевые слова: социальная инженерия, экономическая безопасность, угроза, ущерб, коммерческая тайна, несанкционированный доступ.

Social engineering in the context of the threat to the economic security of the enterprise

Abstract: This article will discuss the theoretical foundations of social engineering, techniques, and types of attacks. Shows a direct connection and dependence with information and, as a result, economic security. Examples of successful attacks on companies in the financial sector are given. A set of recommendations for counteraction has been developed.

Keywords: social engineering, economic security, threat, damage, commercial secret, unauthorized access.

В современном мире мы окружены автоматизированными системами. Вопрос информационной и, как следствие, экономической безопасности стоит очень остро. Однако даже самая совершенная система защиты будет

бесполезна, если ей управляет психологически неустойчивый человек. Сразу стоит вспомнить анекдот о диссертации на тему: “Зависимость скорости перебора паролей от температуры паяльника (утюга)”? Стоит помнить, что объектом атаки может стать не труднодоступный офис или защищённый сервер, а человек, имеющий доступ к необходимой информации. Причем, такой сотрудник зачастую может оказаться наиболее уязвимым элементом в системе защиты.

В рамках данной статьи термин “Социальная инженерия” применяется, как любое психологическое воздействие на человека или группу лиц с целью получения выгоды, например: введение в заблуждение, шантаж, игра на чувствах, таких как любовь, алчность, самолюбие.

Стоит отметить, что данный метод воздействия на людей берёт своё начало во второй половине XIX века, когда стало ясно, что при помощи средств массовой информации можно внедрять любую идеологию, побуждающую к действию или бездействию. За более чем 100 лет использование социальной инженерии для извлечения личной выгоды упростилось до нелезя. Сегодня, получая письмо по электронной почте от коллеги или смс от родственника, мы даже не задумываемся о настоящем авторе данного сообщения.

Далее хотелось бы ввести понятие **Треугольник мошенничества**. Это схема мотивов мошенничества, которая включает давление, возможность и оправдание. Давайте разберем каждое из понятий поподробнее.

Под давлением можно понимать проблемы с финансами, неудовлетворённость работой (например, если человека не ценят, издеваются на нем) и прочими трудностями.

Под возможностью понимаются все ваши знания о компании, которые могут помочь злоумышленникам в получении несанкционированного доступа к информации или проведению диверсии.

Последним, но не менее важным, является оправдание. Эта часть треугольника является необязательной, так как порой жертва даже не понимает, что передает конфиденциальные данные, иначе позволяет избавиться соучастника от чувства вина, а равно признать его действия более чем справедливыми. Например, когда человеку говорят, что все так делают и ничего страшного не произойдёт.

Таким образом для проведения успешной атаки при помощи социальной инженерии, потенциальному злоумышленнику необходимо определить цель атаки, это может быть как раскрытие конфиденциальной информации, так и необходимое действие или бездействие со стороны жертвы. В зависимости от цели подбирается потенциальный объект атаки, обычно, это сотрудник, имеющий доступ к необходимой информации или ресурсу. Далее атакующий выбирает метод воздействия, который будет

основан на потребностях и слабостях жертвы, это может быть как безобидный подарок, так и шантаж. При правильно выбранной цели и методике атаки, с большой вероятностью атакующий достигнет желаемого.

Для окончательного понимания того, о чем мы с вами будем говорить в рамках данной статьи, необходимо ввести понятие Экономической безопасности.

Будем считать, что это область научного знания об устойчивом развитии компании и эффективности использования ресурсов. Таким образом нарушение экономической безопасности — это любые действия, которые могут подвергнуть положение компании угрозе, начиная от информации о том, как выстроены бизнес-процессы и заканчивая прямыми хищениями денежных средств компании.

Рассматривая данный вопрос с научной точки зрения, можно подумать, что это антиутопия и попасться может кто угодно, но не я.

А давайте каждый из нас с вами вспомнит, испытывал ли он острую потребность в финансах? Под острой потребностью может пониматься не только необходимость срочно оплатить лечение или закрыть проценты по кредиту, но и просто желание жить лучше. Порой так и берёт зависть, когда мимо пролетает новенький Порше.

Только ли потребность в деньгах сотрудника может стать угрозой экономической безопасности предприятия? Конечно нет. Порой мы сами создаем почву для преступления, желая сэкономить время или “не обидеть” коллегу напоминанием о соблюдении требований информационной безопасности.

Таким образом сотрудник может создать угрозу экономической безопасности компании как сознательно, так и по незнанию или не пониманию.

Сознательными мы считаем те действия, которые человек совершает с целью извлечения личной выгоды.

Отдельно стоит рассмотреть ситуации, когда человек не отдает в полной мере отчет своим действиям. Это может быть связано как с физическим состоянием, например под влиянием алкоголя или наркотиков, так и психологическим состоянием. Манипулировать такими людьми гораздо проще, ведь человек не может здраво и в полной мере дать оценку происходящему.

Давайте сразу подкрепим эту информацию примером из жизни. (Так как указанная далее информация является коммерческой тайной реально существующего предприятия, название компании и имена сотрудников будут изменены).

В кредитном отделе банка МоскваКредит работает 5 сотрудников. Так как всем бывает необходимо покинуть рабочее место, например, чтобы

покурить или пообедать; в тайне от руководства было принято решение обменяться индивидуальными паролями от учетных записей, чтобы можно было подменить коллегу. Взаимовыручка в рамках компании – это прекрасно. И клиент останется доволен оперативным обслуживанием, и сотрудник сможет отлучиться при необходимости.

Один из сотрудников по имени Алексей, желая улучшить своё материально положение, начал выпускать кредитные продукты, а именно кредитные карты, на данные клиентов коллег.

Далее деньги с этих карт снимались и тратились, а чтобы клиенты не заподозрили проблем, задолженность по старым картам гасилась за счет новых, при этом с соблюдением беспроцентного периода.

Спустя несколько месяцев таких манипуляций сотрудник смог приобрести новый внедорожник марки Lexus.

Схема вскрылась, когда один из клиентов заметил, что на его имя выпущена кредитная карта без его ведома. Внутреннее расследование затянулось, так как при изучении журнала операций было установлено, что действия производились из-под учетных записей разных сотрудников, однако они сами отрицали какое-либо участие в данном инциденте.

В итоге виновный был найден и уволен, а суммарный долг лег на его плечи.

Давайте посмотрим на эту ситуацию со стороны и выделим ключевые моменты, которые могли бы помочь предотвратить махинации или, как минимум, уменьшить ущерб.

Во-первых, сотрудники дали доступ к своей учетной записи третьим лицам (в данном случае любое лицо, кроме владельца учетной записи, считаем третьим). Это грубое нарушение информационной безопасности, которое повлекло за собой возможность операций со счетами клиентов без их ведома и затруднило дальнейшее расследование.

Во-вторых, коллеги Алексея должны были обратить внимание на дорогостоящую покупку, которая не соотносится с его доходами, и сообщить об этом в службу безопасности.

В-третьих, внутренняя система банка позволяла выпускать банковские продукты без подтверждения и оповещения клиентов, что позволило злоумышленнику совершить данное преступление и достаточно долгое время оставаться безнаказанным.

В данной ситуации мы с вами можем увидеть, как желание помочь коллегам обернулось несколькими десятками не погашенных кредитных карт и подрывом репутации банка, восстановить которую будет весьма проблематично.

В завершении хотелось бы дать рекомендации по предотвращению атак социальных инженеров на сотрудников компании:

– мониторинг финансового положения сотрудников. Тут нас интересует, как необоснованный рост доходов, индикаторами которого могут стать дорогие покупки (машина, квартира, премиальная одежда, элитные часы), так и трудности, например обращение в микрофинансовые организации, не выполнение долговых обязательств;

– выявление сотрудников, имеющих разного рода зависимости. Это может быть как пристрастие к алкоголю или наркотикам, так и чрезмерный интерес к азартным играм. Порой именно этот фактор может стать причиной ситуации, которую можно описать так:” Прошу доверить мне новую государственную тайну, так как старую я разболтал по пьяни.”

– проведение тренингов, направленных на информирование сотрудников о возможных угрозах и действиях в случае их возникновения. Сотрудники должны четко понимать, какая информация не подлежит разглашению;

– разграничение доступа к ресурсам и сервисам компании в соответствии с занимаемой должностью. Например, программисту не нужен доступ к личным делам сотрудников компании. Любой доступ, выходящий за рамки должностных обязанностей, должен согласовываться через службу безопасности;

– соблюдение установленных правил в сфере информационной безопасности вне зависимости от ситуации. Например, передача доступа к своему оборудованию или учетной записи коллеге для безобидной просьбы распечатать отчет, может обернуться серьезными проблемами;

– симуляция действий потенциального злоумышленника. Например, отправка писем с якобы выгодным предложением от партнера с прикрепленной ссылкой. В случае, если сотрудник перейдет по ссылке, никакого вреда компании причинено не будет, однако такая ситуация станет поводом, для повторного проведения обучения по противодействию социальной инженерии и неприятному разговору со службой безопасности.

В рамках рекомендаций существует индикаторы, которые, конечно, не являются прямой причиной для увольнения сотрудника, однако должны стать “первым звоночком” для особого контроля.

К сожалению, данная тема актуальная на сегодняшний день, и порой мы “получаем удар” оттуда, откуда, казалось бы, получить не должны. Новые рекомендации и меры противодействия появляются на основе precedентов, которые принесли ущерб реальным компаниям.

Список использованных источников:

1. Как объяснить мошенничество? [Электронный ресурс]. – URL: <https://ethicontrol.com/ru/blog/fraud%252Fquiz>

2. Как социальная инженерия открывает хакеру двери в вашу организацию [Электронный ресурс]. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/social-engineering/>
3. Социальная инженерия (социология) [Электронный ресурс]. – URL: [https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F_\(%D1%81%D0%BE%D1%86%D0%B8%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F\)](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B8%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B8%D1%8F_(%D1%81%D0%BE%D1%86%D0%B8%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F))

Социальные сети и мессенджеры как площадка для кибервойны с обществом и государством

Д.А. Авдеев

студент 6 курса НИЯУ МИФИ, Москва

E-mail: dmavdeev1111@gmail.com

В.Ю. Радыгин

к.т.н., доцент кафедры финансового мониторинга НИЯУ МИФИ, Москва

E-mail: vyradygin@mephi.ru

Аннотация: В настоящее время социальные сети и мессенджеры имеют небывалую популярность, и применяются практически во всех сферах жизни общества и государства. В данной статье рассматривается вопрос использования социальных площадок, как средства продвижения идей ОД/ФТ, экстремизма и терроризма. Данная проблема крайне актуальна так как социальные сети способны значительно воздействовать на пользователей и от того, какое влияние оказывается, напрямую зависит безопасность государства и общества.

Ключевые слова: ПОД/ФТ, экстремизм, терроризм, манипулирование сознанием, социальные сети, финансирование терроризма.

Social media and messengers as platform for performing cyberwar against society and state

Abstract: Currently, social networks and instant messengers have unprecedented popularity, and are used in almost all spheres of society and the state. This article examines the issue of using social platforms as a means of promoting the ideas of ML / FT, extremism and terrorism. This problem is extremely relevant since social networks are able to significantly influence users and the security of the state and society directly depends on what kind of influence it has.

Keywords: AML/CFT, extremism, terrorism, mind manipulating, social media, terrorism financing.

Введение

В настоящее время социальные сети и мессенджеры очень тесно вошли в нашу жизнь практически во всех сферах. Если каких-то 20 лет назад требовалось провести огромный объем работы, чтобы собрать группу

людей, скоординироваться и начать действовать, то сейчас это возможно осуществить, фактически опубликовав одну запись в течение пяти минут. В свою очередь, наличие такое возможности очень оперативно предпринять действия, отреагировать на ситуацию, влечет за собой как множество положительных моментов, так и угроз безопасности государства и общества. Все это следует из свойств, которыми обладают социальные сети и мессенджеры: доступность, легкость использования, чувство защищенности при общении. Как мне кажется, наличие этих свойств делает социальные сети крайне эффективным инструментом, и стоит очень остро задача отделения представляющего угрозу контента от остального. В своей статье мне хочется рассмотреть вопрос использования социальных площадок, как средства продвижения идей ОД/ФТ, экстремизма и терроризма, который, несомненно, будут подрывать безопасность общества и государства. Для достижения поставленной цели необходимо: оценить насколько популярна изучаемая тематика, какой контент присутствует и как он контролируется, оценить возможные способы влияния на пользователей, а также рассмотреть, какие методологии использует преступное сообщество, враждебно настроенные государства для достижения своих целей и возможные способы борьбы с ними.

Актуальность данной темы не вызывает сомнений, учитывая тот факт, как тесно социальные сети и мессенджеры вошли в нашу жизнь. Практически каждое событие так или иначе имеет свой след в различных группах и переписках. Несомненно, изучаемая проблема поднималась и не раз абсолютно на всех уровнях. Например, в ежегодных отчетах ФАТФ отмечается важность и актуальность вопроса использования социальных сетей, как площадки по сбору средств для финансирования терроризма, и действительно такое явление представляет значимую угрозу безопасности государства. Согласно отчету за 2015 год, финансирование терроризма через социальные сети – это один из самых актуальных и значимых рисков в ближайшие 10 лет [5]. К счастью, сейчас ведется очень активная борьба с нежелательным контентом, и в борьбе с определенными категориями действительно имеются значительные успехи, однако по-прежнему остается много нерешенных вопросов, не исключением является и сфера ОД/ФТ.

Оценка возможностей социальных сетей и состояние системы ПОД/ФТ в РФ

Пожалуй, повествование стоит начать с определения текущей ситуации с социальными сетями и площадками, а также состоянием системы ПОД/ФТ в целом. Итак, на момент начала 2021 года в Российской

Федерации насчитывается более 99 миллионов пользователей (аккаунтов) в социальных сетях, однако стоит отметить, что на каждого пользователя приходится в среднем порядка 7 аккаунтов. Такое может быть связано с тем, что многие создают несколько аккаунтов для работы, общения, используют разные площадки.

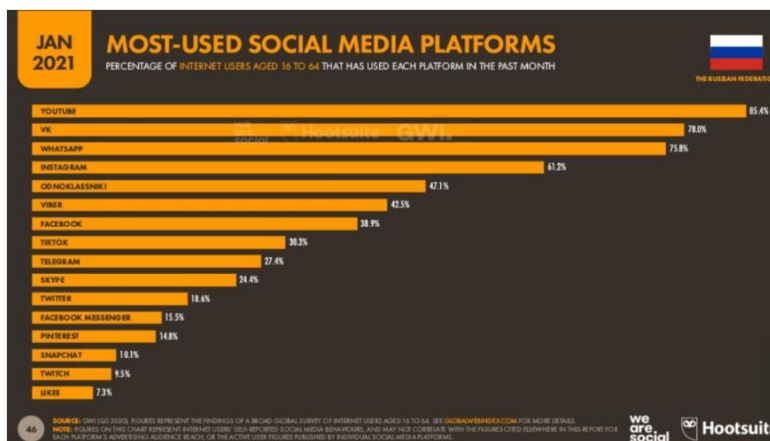


Рисунок 1 – Статистические данные по социальным площадкам за 2021 год

Как можно наблюдать, самыми популярными социальными площадками являются YouTube, VK, WhatsApp. Порядка 80% всех пользователей имеют аккаунты на этих социальных площадках. А, например, Telegram-аккаунт имеется у 30% пользователей [3]. Отсюда можно сделать вывод, что наиболее эффективными путями распространения информация широкому кругу лиц будет платформа YouTube и социальная сеть ВКонтакте. Каждая из платформ имеет свою специфику и предлагает определенный контент, поэтому каждая из них наиболее эффективно может проявить себя в определенных способах воздействия на пользователя, а также методам сбора средств.

Следующим аспектом, которого необходимо коснуться, является оценка состояния ПОД/ФТ в целом в Российской Федерации. Согласно отчету о взаимной оценке в 2019 году суммарно по рейтингам Россия заняла 5-е место по эффективности национальной «антиотмывочной» системы в мире [2]. Суммируя всю информацию, содержащуюся в данном отчете, можно сказать, что в Российской Федерации имеется глубокое понимание существующих в стране рисков ОД и ФТ, в особенности, стоит подчеркнуть, финансовые учреждения имеют наибольший успех в оценке рисков и принятия соответствующих мер, в то время как другими

субъектами успех в борьбе с ОД и ФТ сильно разнится. Для борьбы с финансированием терроризма в России существует надежная правовая база, которая в значительной степени соответствует международным стандартам. В среднем в России ежегодно осуществляется 52 судебных преследований за финансирование терроризма. Однако на фоне всего этого в отчете отмечается, что наблюдается широко распространенная и сохраняющаяся тенденция неисполнения организациями обязательств, касающихся применения предупредительных мер в целях ПОД/ФТ. То есть из вышесказанного можно сделать вывод, что в Российской Федерации система обнаружения, наказания, расследования преступлений по ОД/ФТ находится на довольно высоком уровне, но применяемые превентивные меры недостаточны и не позволяют ограничить возможности осуществления преступления.

Итак, когда определен масштаб охватываемой аудитории социальными площадками и оценено состояние системы ПОД/ФТ, можно переходить к детальному изучению основных подходов и методик по применению определенных социальных площадок в целях ОД/ФТ, экстремизма и терроризма. Для анализа особое внимание будет уделено таким площадкам как YouTube и ВКонтакте, а также мессенджеру Telegram. Необходимо определить роль каждой из площадок, какую информацию они могут предоставить и насколько данная информация будет противоправна в рассматриваемой сфере.

Основными способами использования социальных площадок в целях ОД/ФТ, экстремизма и терроризма может быть:

- Сбор средств для поддержания террористических организаций на территории РФ и за ее пределами;
- Разжигание межнациональной розни;
- Дестабилизация политической обстановки в государстве;
- Координирование террористических акций;
- Призывам к смене политического режима и иных связанных действиях.

Также стоит упомянуть, что популярность социальных площадок среди революционеров объясняется социальным феноменом, так называемым «доминированием слабых связей». Смысл которого заключается в следующем: информация распространяется быстрее через малознакомых, либо вовсе незнакомых людей. Поэтому в случае распространения революционной идеи, наполненной эмоциональной составляющей, социальные площадки, благодаря силе слабых связей за короткий промежуток времени формируют большие массы сторонников и как следствие именно эмоциональная составляющая заставляет участников переходить к конкретным действиям.

ВКонтакте как платформа для размещения объявлений об оказании «услуг»

Социальная сеть ВКонтакте является самой популярной в России и неудивительно, что она активно используется преступным сообществом. Для детального ознакомления с возможными способами работы пользователя с социальной сетью ВКонтакте, было принято решение пойти эмпирическим путем и проверить, какие способами пользователь, интересующийся тематикой ОД/ФТ, способен получить информацию в интересующей его области, и способен ли он вообще это сделать. После недолгих поисков, очень легко найти незаблокированные группы, которые предлагают вот такие «услуги» (рисунок 2):

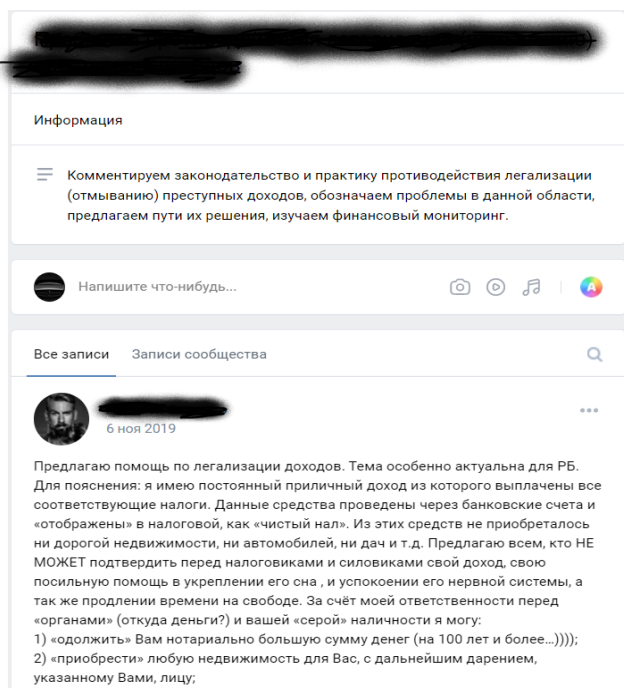


Рисунок 2 – Пример «услуги»

И что удивительно, данной записи уже фактически 2 года, а аккаунт, с которого был опубликован пост, по-прежнему активен. Могу предположить, что это может быть способ правоохранительных органов выхода напрямую на людей, которые хотят «отмыть» свои денежные

средства, а возможно, такая «услуга» будет действительно предоставляться.

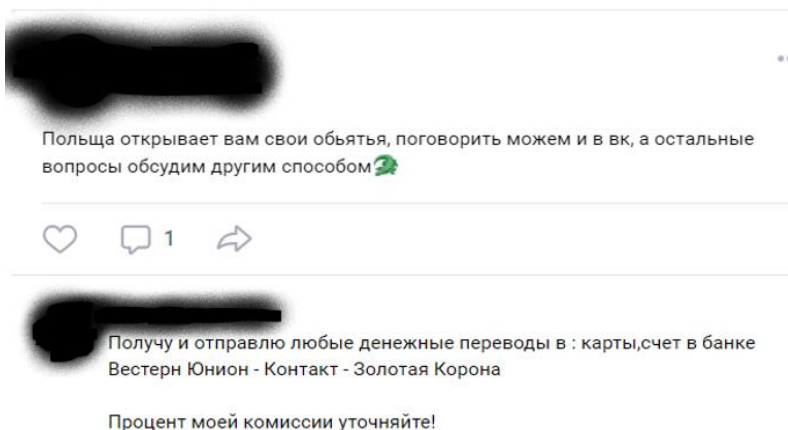


Рисунок 3 – Пример «услуги»

Или же вот еще один пример, когда мы можем наблюдать, что кто-то предлагает свои «услуги», однако тут уже намекают не применение иного способа общения. Таким образом, можно сделать вывод, что с помощью социальной сети вполне реально заявить о себе заинтересованным лицам.

Социальные сети как площадка для социальной инженерии

Однако рассмотренные выше примеры довольно легко найти, в том числе и правоохранительным органам, и скорее всего, они им и известны. Гораздо сложнее обстоят дела с группами, которые на протяжении длительного времени существуют и имеют большое количество подписчиков, но предоставляют информацию, призванную манипулировать мнением и отношением людей к тому или иному событию. Такого рода группы представляют наибольшую опасность, ведь именно за отсутствием видимой угрозы, их довольно тяжело выделить среди остальных групп. И работая с большой группой на протяжении нескольких лет, вполне реально нанести довольно значительный ущерб текущему государственному строю, а также побудить людей к совершению противоправных действий.

Для возможности влиять на огромные группы пользователей, используются обширные средства социальной инженерии:

- Социальные, этнические противоречия;

- Фокусирование внимания на проблемы, накопившиеся в обществе и не решающиеся действующей властью;
- Подлог фактов;
- И иные средства.

Помимо групп в последнее время крайне эффективным способом формирования нужного настроения в обществе являются блоги. Как считается, они являются элементом так называемой «народной журналистики». То есть предполагается, что блоги ведутся абсолютно независимыми людьми близкими ко всему обществу, и невольно население легче принимает таких людей, начинает им доверять, а, следовательно, при помощи этих каналов через некоторое время уже можно будет доносить свою «правду», которая будет наиболее удобной. Основными задачами использования блогов являются: максимальный охват населения и оперативность передачи информации как будто от первого лица, хотя едва ли человек, ведущий блог, обладает большей достоверной информацией, чем кто-либо иной.

Также социальные площадки являются крайне эффективны в процессе сбора денежных средств. Эти средства могут собираться под абсолютно разными предложениями и способами, однако далеко не всегда написанная цель сбора совпадает с реальной. Обычный пользователь может даже и не подозревать, что при переводе благотворительному фонду в конечном итоге эти деньги окажутся у террористов, и в таком случае пользователь может быть привлечен, сам того не подозревая, к уголовной ответственности за финансирование терроризма.

Террористы могут собирать денежные средства под абсолютно любыми предложениями:

- Это могут оказаться благотворительные фонды;
- Сборы на лечение;
- Различного рода стримы;
- Интересные краудфандинговые проекты и т.д.

В связи с чем всем пользователям необходимо быть максимально внимательными, если они собираются финансировать тот или иной проект. Также стоит помнить, что обычно это крайне недолговечные проекты, и страница со сбором средств может исчезнуть буквально за пару часов, а вместо нее появится другая.

Для привлечения внимания к такого рода страницам, ссылки на них рассылаются в личных сообщениях, определенному кругу пользователей (к сожалению, это не является какой-либо проблемой, и такой процесс достаточно легко осуществить). Также в целях привлечения как можно большего количества людей организаторы онлайн-кампаний по сбору средств могут использовать самые разные платежные системы и сервисы

(в том числе могут применяться и системы, которые уже предустановлены в социальной сети), которые популярны среди различных групп потенциальных «спонсоров».

Все вышеперечисленные способы использования социальных площадок представляют довольно серьезную угрозу безопасности Российской Федерации и приведенные ниже несколько примеров тому доказательство:

Пример 1

Группа лиц под руководством г-на «А» (Группа «А») организовала схему по сбору денежных средств через социальные сети и Интернет. Эта группа лиц зарегистрировала множество электронных кошельков, кредитных карт и номеров мобильных телефонов. Реквизиты были размещены в самой популярной социальной сети под предлогом сбора пожертвований для сирийских беженцев, людей, нуждающихся в медицинской и финансовой помощи, а также на строительство мечетей, школ и детских садов. В формулировках содержались косвенные намёки на то, что деньги предназначались в качестве финансовой поддержки террористической деятельности. На самом деле деньги направлялись в качестве помощи террористам и их семьям, а также на поддержку террористической деятельности. Деньги направлялись либо на счета кредитных карт, либо на электронные кошельки. После ряда переводов собранных средств они снимались наличными для дальнейшей перевозки курьерами. Управление платёжными инструментами, а также группами в социальной сети осуществлялось через группы в одном из набирающем обороте мессенджера.

Пример 2

Во время мероприятий по противодействию терроризму ФСБ был обнаружен г-н «Б». Согласно оперативной информации, в феврале 2014 года г-н «Б» прибыл в Сирию для участия в вооруженной группировке «Д», структурно связанной с «ДН». Затем г-н «Б» создал пропагандистские сайты в социальных сетях Facebook и «ВКонтакте», чтобы организовать сбор средств для ФТ. Собранные средства были предоставлены группировке «ДН», в том числе на приобретение оружия, обмундирования, продуктов питания и дорожные расходы для иностранных боевиков-террористов для поездки в Сирию. Для установления того факта, что г-ном «Б» было осуществлено ФТ, ФСБ направила запрос в Межрегиональное управление Росфинмониторинга. В ходе финансового расследования было установлено, что г-жа «Х» предоставила г-ну «Б» следующие финансовые инструменты, зарегистрированные на ее имя: виртуальный кошелек «Q» и банковскую карту, привязанную к этому кошельку для сбора денежных средств в интересах г-на «Б». Общая сумма средств, поступивших на

виртуальный кошелек «Q» в период с октября 2015 года по март 2016 года, составила 284 646,99 руб. (4 000 евро). За тот же период общая сумма исходящих операций составила 164 962,12 руб. (2 262 евро). В то же время г-жа «Х» под псевдонимом «Муслим Абдуллаева» была подписчиком закрытой группы в социальной сети, созданной г-ном «Б», где она представилась как его жена. Выяснилось, что в 2015 году г-н «Н» оказал финансовую поддержку группировке «ДН» путем перевода денежных средств со своей банковской карты, выпущенной банком «С», на банковскую карту, принадлежащую г-же «Х», с использованием информации, опубликованной в Интернете г-ном «Б». В период с ноября 2015 года по декабрь 2015 года г-н «Н» совершил четыре операции на общую сумму 5 200 рублей (71 евро) с использованием банковской карты. Затем г-н «Н» был привлечен к ответственности Генпрокуратурой РФ за ФТ (ст. 205.1), г-жа «Х» — за преступления в сфере ФТ и публичное обращение с призывом осуществлять экстремистскую деятельность (ст. 205.1 и 208), г-н «Б» — за те же два преступления, а также за организацию деятельности террористических организаций (ст. 205.5).

Заключение

Подводя итоги, хочется отметить, что проблема рассмотренная проблема в действительности является крайне актуальной в настоящее время. Современные преступники используют все более и более изощренные методы социальной инженерии, чтобы получить денежные средства для финансирования терроризма, и зачастую жертвы — обычные пользователи, которые даже и не подозревают, что их денежные средства ушли не в благотворительную организацию, а на поддержку боевых формирований. Также методы социальной инженерии широко применяются и в манипулировании сознанием пользователей, подменяя одни понятия и ценности, на другие, напрямую подрывая безопасность общественности и государства. Скорее всего, наиболее действенным способом будут превентивные меры, так как они позволят не допустить воздействие на пользователей социальных площадок: имея опыт и представление о средствах манипуляции, человек сможет им противостоять и не поддаваться их влиянию.

Список использованных источников:

1. Mutual Evaluation Report, Russian Federation // <https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Russian-Federation-2019.pdf>
2. Статья на сайте Россотрудничества // <https://www.fedsfm.ru/preparation-fatf-fourth-round>

3. Интернет и соцсети в 2021 году, статистика // <https://www.web-scanape.ru/business/internet-i-socseti-v-rossii-v-2021-godu-vsya-statistika/>
4. Статья «Социальные сети как инструмент «цветных революций» // <https://catu.su/46-2011-12-12-18-53-21/2011-12-12-18-54-01/170-l-r33>
5. Отчет ФАТФ «Новые риски финансирования терроризма» // <https://fedsfm.ru/content/files/documents/2018/%D0%BE%D1%82%D1%87%D0%B5%D1%82%20%D1%84%D0%B0%D1%82%D1%84.%20%D0%BD%D0%BE%D0%B2%D1%8B%D0%B5%20%D1%80%D0%B8%D1%81%D0%BA%D0%B8%20%D1%84%D0%B8%D0%BD%D0%B0%D0%BD%D1%81%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F%20%D1%82%D0%B5%D1%80%D1%80%D0%BE%D1%80%D0%B8%D0%B7%D0%BC%D0%B0.pdf>
6. Статья в новостном портале Lenta.ru // https://lenta.ru/articles/2020/11/27/social_networks/

Тактические и стратегические цели аудита мирового масштаба

С.В. Сергеев

студент 2 курса НИЯУ МИФИ, Москва

E-mail: SVSergey.sergeev@yandex.ru

Д.В. Сергеев

студент 1 курса МГУ им. Ломоносова, Москва

E-mail: Dmitry.sergeev.v@yandex.ru

Н.С. Белогина

к. э. н., доцент кафедры бухгалтерского учета и аудита

НИЯУ МИФИ, Москва

E-mail: nsbelog@gmail.com

Аннотация: В статье на основе анализа состояния рынка глобального аудита, публикаций в периодических изданиях, отчетов и новостей Международного совета по стандартам аудита и обеспечению уверенности (IAASB), отчетов «Большой четверки» выявлены основные проблемы и задачи, стоящие перед аудитом, стратегии на 2020-2023 года и ключевые факторы, на которые необходимо обратить внимание для повышения качества оказания услуг и общественного доверия во всем мире.

Ключевые слова: дистанционный аудит, глобальные стандарты аудита, обеспечение уверенности, разрыв в ожиданиях от аудита, системные проблемы.

Tactical and strategic objectives of a global audit

Abstract: In the article considers the main problems and tasks facing the audit, strategies for 2020-2023 and key factors that need to be paid attention to improve the quality of services and public trust around the world based on the analysis of the state of the global audit market, publications in periodicals, reports and news of the International Auditing and Assurance Standards Board (IAASB), reports of the "Big Four".

Keywords: remote audit, global auditing standards, assurance, gap in audit expectations, systemic problems.

Введение. Изменения в экономической среде и на рынке аудиторских услуг повлияли на то, как функционирует аудиторская отрасль и как она

воспринимается пользователями и широкой общественностью. Важные проблемы, стоящие перед аудиторской отраслью, включают: коммерциализацию аудита; воспринимаемые ценность и актуальность традиционного аудита, включая ответственность аудитора за выявление мошенничества; влияние повышенного внимания крупных аудиторских фирм к расширению своих неаудиторских услуг с уделением особого внимания консультативным/консультационным услугам; влияние достижений в области технологий и расширение доступности данных. В связи с этим появляется необходимость рассмотрения особенностей развития международного рынка аудиторско-консалтинговых услуг с точки зрения: тактических и стратегических целей, состояния мирового рынка аудита и его структуры, вектора развития международной аудиторской деятельности в эпоху глобализации экономики.

Основная часть. Если рассматривать аудит мирового масштаба, то это следует делать через призму Международного совета по стандартам аудита и обеспечению уверенности (IAASB), который является глобальным независимым органом по установлению стандартов и служит общественным интересам, устанавливая высококачественные международные стандарты, являющиеся общепринятыми во всем мире.

IAASB считает, что высококачественные и надежные международные стандарты способствуют повышению качества взаимодействия и согласованности практики во всем мире, а также укреплению доверия общественности к глобальной профессии аудита и обеспечению уверенности. IAASB устанавливает свои стандарты в общественных интересах с учетом рекомендаций Консультативной группы IAASB (CAG) и под надзором Совета по надзору за общественными интересами.

В данном случае при определении стратегии и целей глобального аудита будет делаться упор на стратегию Совета, которую они сформировали вплоть до 2023 года.

Том Зайденштейн, президент IAASB, заявил, что в ближайшее время аудиторская отрасль столкнется с еще большими вызовами и непростым выбором приоритетов по мере того, как появится потенциал для новых проектов или инициатив. Он подчёркивает важность эффективного внедрения новых и пересмотренных стандартов впервые, и необходимости предоставления достаточного времени для того, чтобы эти изменения были должным образом и эффективно реализованы, а также для того, чтобы были замечены преимущества. Для обеспечения эффективного перехода к этим изменениям также потребуют усилий от бухгалтерских организаций, фирм, регулирующих органов. Следует отметить, что Международная федерация бухгалтеров (IFAC), с которой у Международного совета по стандартам аудита и обеспечению уверенности (IAASB) прочные

отношения сотрудничества, продолжает оставаться лидером в продвижении и мониторинге глобального внедрения стандартов. IFAC по словам Тома Зайденштейна подтверждают свою приверженность поддержке внедрения и образованию в качестве стратегического приоритета [5].

В качестве приоритета, помимо новых задач, в документе обозначается своевременная реализация незавершенных старых проектов с целью создания прочной базы и основы для новой стратегии 2020-2023. Они включают усовершенствования наиболее важных Международных стандартов аудита (МСА) и стандартов контроля качества. «Эти усовершенствования являются ключом к высококачественному аудиту и другим мероприятиям», - заявляет Том Зайденштейн.

Стратегия 2020-2023 уделяет приоритетное внимание решению ключевых возникающих проблем, представляющих общественный интерес:

1. Влияние развивающихся технологий;
2. Требования к отчетности для удовлетворения меняющихся потребностей заинтересованных сторон (включая требования к IAASB рассматривать нефинансовую отчетность);
3. Изменение ожиданий от аудита в отношении таких вопросов, как мошенничество и непрерывная деятельность [5].

Главной целью международного аудита на данный момент по-прежнему остается: «устойчивое доверие к финансовой и иной отчетности, подкрепляемое высококачественными аудитам, гарантиями и соответствующими услугами, предоставляемыми за счет внедрения надежных глобальных стандартов, отвечающих общественным интересам и способных к последовательному и надлежащему внедрению» [5, 6].

В соответствии с установленной целью IAASB выделяет следующий ряд основополагающих принципов:

1. Установка на общественные интересы: установка, которая ставит общественные интересы на первое место, подкрепляя это рабочими планами, процессами и мероприятиями;
2. Подотчетность: укрепление доверия и внушение уверенности посредством коммуникации и прозрачности действий аудиторов;
3. Стандарты: глобально значимые, перспективные, применяемые к организациям всех масштабов и сложности, адаптируемые к меняющейся среде и работоспособные; разработанные и поддерживаемые посредством деятельности, которая является независимой и свободной от ненадлежащего влияния, своевременной и отвечающей потребностям заинтересованных сторон;

4. Методы: строгие и всеобъемлющие, включая привлечение внешних ресурсов, где это возможно; пересмотр и совершенствование с целью выполнения принятых планов работы.

Стоит сказать, что основными драйверами разработки новой стратегии международного аудита явились следующие проблемы, вызовы и изменяющиеся условия:

- Развитие и использование технологий.

Быстро меняющиеся и развивающиеся технологии (например, искусственный интеллект, робототехника, блокчейн, облачные вычисления, социальные сети и цифровые платежные платформы). Разработки в области использования передовых технологий, включая то, как автоматизированные инструменты (включая автоматизированную аналитику данных) используются для выполнения работ по аудиту и обеспечению обязательств, а также то, как такие технологии влияют на структуру и взаимодействие групп по взаимодействию.

- Возрастающая сложность и ее последствия.

Бизнес-среда становится все более сложной, и в результате стандарты финансовой отчетности должны реагировать и становятся все более сложными. Практика бухгалтерского учета развивается, операции становятся все более сложными, а финансовая отчетность продолжает меняться, и требуется больше оценок и управленческих суждений. Темпы изменений приводят к усложнению, усиливая воздействие многих факторов и увеличивая нагрузку на оперативность реагирования и актуальность. Растущее внедрение более сложных стандартов аудита и обеспечения увеличивает проблемы с внедрением и применением.

- Изменение потребностей заинтересованных сторон в отчетности.

Корпоративная отчетность продолжает развиваться, и многие пользователи корпоративных отчетов все больше сосредотачиваются на имеющейся нефинансовой информации и ищут в ней гарантии (например, отчетность об устойчивом развитии, повышенные требования к отчетности для финансовых учреждений или отчеты, касающиеся механизмов управления и внутреннего контроля организации, и другие формы расширенной внешней отчетности).

- Изменение общественного доверия к аудиту.

Колебания доверия и уверенности в аудиторских проверках, вызванные недавними громкими корпоративными неудачами и сообщениями о плохих результатах внешних проверок в некоторых юрисдикциях. Изменения ожиданий заинтересованных сторон относительно того, что стандарты должны требовать от аудитора, например, в отношении выявления и сообщения о мошенничестве, а также рассмотрения вопросов, связанных с непрерывностью деятельности (т. е. "разрыв в ожиданиях" между тем, что

ождается от аудита, и тем, что текущие стандарты требуют от аудитора делать).

Таким образом, основное внимание в действиях аудиторских компаний по всему миру должно уделяться своевременным и соответствующим изменениям, в частности быстрым достижениям в области технологий и другим областям общественных интересов.

Международный совет по стандартам аудита и обеспечению уверенности (IAASB) основой своей деятельности выделяет разработку и поддержание высококачественных международных стандартов аудита, гарантий и сопутствующих услуг. В связи с этим для глобального аудита ставятся следующие задачи:

- усиление внимания к решению возникающих проблем, выявленных в меняющейся среде, в том числе к тому, как технологии влияют на внедрение Международных стандартов - процедуры разработки и пересмотра стандартов и их эффективное внедрение;
- рассмотрение нефинансовой отчетности в свете изменения корпоративной отчетности;
- рассмотрение дальнейших тем для поддержания доверия общественности к аудиту в свете меняющихся общественных интересов (например, в связи с рассмотрением аудитором случаев мошенничества и непрерывности деятельности);
- выполнение функций лидера мысли и созыв заинтересованных сторон по темам, связанным с будущим аудита;
- внедрение инноваций в работу с помощью технологий, новых инструментов совместной работы и других средств для повышения гибкости и максимального эффекта от деятельности;
- проведение более структурированных и надежных мероприятий по сбору информации и проведение исследований для будущих направлений работы, а также обеспечение прозрачности в отношении решений, принимаемых в рамках проводимой работы;
- разработка механизмов для более своевременного решения проблем и задач.

Вывод. В результате сильных и динамичных изменений в технологиях, развития глобальной экономики, внедрения цифровой экономики в повседневную действительность формируются факторы, которые необходимо учитывать всем субъектам экономики, в том числе аудиторской отрасли. Как видно, Международный совет по стандартам аудита и обеспечению уверенности (IAASB) принимает во внимание данные тенденции, делая на них акцент в своей стратегии на 2020-2023 года. Также уделяется внимание снижению доверия общественности к аудиту как таковому вследствие снижения качества проверок и

участившихся крупных скандалов, связанных как с «Большой четверкой», так и с другими компаниями отрасли. Все это говорит, что IAASB обладает достаточной осведомленностью в отношении проблем и вызовов, которые стоят перед глобальным аудитом, что также подтверждает цель, прописанная в документе. Однако, стоит обратить внимание на то, что, за исключением цели, основные положения стратегии представлены достаточно в размытых формулировках, без детально прописанных шагов, действий и задач, что непременно должно усложнять реализацию данной стратегии. К тому же, в обсуждаемых задачах, стоящих перед глобальным аудитом, не упоминается ситуация с монополизацией рынка, поскольку как во всем мире, так и в отдельно взятых странах большую долю оказания аудиторских услуг занимает «Большая четверка». Это негативно влияет в первую очередь на свободу входа в рынок, а также на качество аудита из-за недостатка здоровой конкуренции.

Список использованных источников:

1. https://auditor-sro.org/pc/actions/iaasb-pomogaet-vned/?sphrase_id=85371;
2. <https://big4accountingfirms.com/>;
3. http://www.consultant.ru/document/cons_doc_LAW_71765/9dbadedfc5ede08e8d9d8713bbd319ebde3409ea/;
4. <https://www.cpajournal.com/2020/01/03/a-2020-global-auditing-forecast/>;
5. <https://www.iaasb.org/>;
6. <https://www.iaasb.org/publications/iaasb-strategy-2020-2023-and-work-plan-2020-2021>;
7. <https://auditor-sro.org/events/vebinary/vebinar-ifac-iaasb-i-icaew121121/>;
8. Федеральный закон от 30 декабря 2008 г. № 307-ФЗ «Об аудиторской деятельности».

УДК 339.9(470+430)

© А.В. Анисимова, М.А.Трубачева, А.Н. Майорова, 2021

Торгово-экономические связи России с Германией

А.В. Анисимова

студент 5 курса НИЯУ МИФИ, Москва

E-mail: junioraver1999@mail.ru

М.А. Трубачева

студент 5 курса НИЯУ МИФИ, Москва

E-mail: mariaaleks313243@gmail.ru

А.Н. Майорова

к.э.н., доцент кафедры бухгалтерского учета и аудита

НИЯУ МИФИ, Москва

E-mail: albina_mayorova@mail.ru

Аннотация: В статье раскрываются исторические этапы развития российско-германских экономических отношений анализируются текущие международные отношения России и Германии. Выявляются основные показатели внешнеторговой деятельности двух стран, перспективы сотрудничества в 2021 году.

Ключевые слова: российско-германские отношения, экспорт, импорт, внешнеэкономическая деятельность.

Trade and economic relations of Russia with Germany

Abstract: The article reveals the historical stages of the development of Russian-German economic relations and analyzes the current international relations between Russia and Germany. The main indicators of foreign trade activity of the two countries, prospects of cooperation in 2021 are revealed.

Keywords: Russian-German relations, export, import, foreign economic activity.

Введение

Начавшаяся в России в 1990-х годах глобализация превратила внешнеторговую деятельность в один из самых важных факторов экономического развития нашей страны. В связи с этим международная экономическая деятельность сейчас находится под пристальным контролем и анализом со стороны государственных структур, таких как Росстат, Минэкономразвития, Минпромторг, ФТС, Министерство экономики, а также Правительство РФ.

Также о важности внешнеторговых отношений между Россией и другими странами свидетельствует наличие таких нормативно-правовых актов, как Федеральный закон "Об основах государственного регулирования внешнеторговой деятельности" от 08.12.2003 N 164-ФЗ и Концепция внешней политики Российской Федерации (утв. Президентом РФ 12.02.2013). Данная Концепция определяет одной из ключевых целей укрепление торгово-экономических позиций РФ в системе мировых торговых связей, что позволит России увеличить экспортный потенциал за счет диверсификации поставляемой продукции и оказываемых услуг, в частности предполагается увеличение роли страны не только как поставщика нефтепродуктов, но и других видов готовой продукции.

В рамках данной Концепции особое внимание уделяется укреплению торгово-экономических связей России с Германией, так как это дает возможность активно продвигать национальные интересы РФ в ЕС и мире, а также способствует ускоренному переходу российской экономики на инновационный путь развития.

Выбор Германии в качестве одного из ключевых партнеров России во внешнеторговых связях обуславливается рядом факторов:

- 1) Географическое положение;
- 2) Уверенность в долгосрочных партнерских связях;
- 3) Наличие соглашений между странами, регулирующих базовые правила сотрудничества;
- 4) Созависимость в рамках обмена важнейшими ресурсами для стабильного развития внешнеторгового потенциала.

По данным на 2020 год Германия занимает ведущее положение среди западных партнеров России во внешнеэкономических отношениях с торговым оборотом 41 950 млн. долларов на 2020 год.

Цель работы: определить потенциал торговых отношений между Россией и Германией на 2021 год.

Объект исследования: взаимодействие России и Германии в рамках осуществления внешнеторговой деятельности.

Для осуществления исследования объекта необходимо выполнить следующие задачи:

1. Выявить влияние внешней торговли между Россией и Германией;
2. Определить факторы, влияющие на взаимную торговлю стран;
3. Определить основные инвестиционные проекты российско-германских отношений;
4. Выявить направления и перспективы развития дальнейшего сотрудничества России и Германии в 2021 году.

Теоретическая и практическая значимость настоящей работы заключается в том, что сформулированные в ней выводы и предложения

могут быть использованы в дальнейших исследованиях российско-германских отношений.

История развития внешнеэкономических отношений Российской Федерации и Федеративной Республики Германия

Общее направление развития российско-германских отношений определили в свое время Договор о добрососедстве, партнерстве и сотрудничестве от 9 ноября 1990 г. 4 и Совместное заявление Президента Российской Федерации и Федерального канцлера ФРГ от 21 ноября 1991 г, которые действуют на текущую дату. Именно они положили начало развития экономического сотрудничества Германии и России, перешедшей к рыночному типу экономики.

После становления Российской Федерации в середине 90-х годов появилась тенденция к стабилизации внешнеторговых отношений и товарооборота с Германией. Например, экспорт России вырос на 13,5%, а импорт в свою очередь вырос на 11,3%. Однако стоит отметить, что уже тогда доля ФРГ во внешней торговле РФ была больше, чем РФ во внешней торговле ФРГ (17,5% против 1,5%).

Также стоит отметить, что в конце 20-ого века каркас российского экспорта составляли сырьевые товары, такие, как нефть и природный газ (всего около 90% стоимостного объема), цветные металлы. Плохой тенденцией уже тогда можно было назвать и резкое сокращение экспорта машин и оборудования с 8% до 1,9% за 3 года с 1992 года.

Если говорить об импорте РФ из ФРГ, то 80% его объема составляли машины и оборудование (2/3 от 80%), продовольственные товары. Такая структура экспорта и импорта России явно не могла способствовать росту экономики и технологическому развитию нашей страны. Однако в 1997 году Германия выходит на 1 место по товарообороту среди стран-торговых партнеров РФ, опережая Украину. Тогда объем торговли составил 16,2 млрд. долл. США (рост товарооборота на 18%).

В 1998 году в России происходит страшное экономическое событие – дефолт, в связи с этим произошел резкий спад в развитии торговых отношений между странами.

Но с назначением Владимира Владимировича Путина президентом РФ развитие сотрудничества продолжилось. Проведенные встречи руководителей позволили преодолеть падение в экономических отношениях между Россией и Германией, а также активизировать партнерские отношения в новых отраслях экономики, тем самым обеспечив переход на новый уровень взаимодействия – информационный. Важным событием в этой связи является подписание совместного заявления на высшем уровне о стратегическом партнерстве в области образования, науки и инноваций.



Рисунок 1 – Объем внешней торговли между РФ и ФРГ, млрд.долл. США

Согласно данным, полученным статистическим ведомством ФРГ, в 2006 году товарооборот вырос более чем на 30% (рост на 25 млрд. евро). А в 2008 году товарооборот вырос на 155,8% по сравнению с 2007 годом. Однако структура экспорта и импорта России изменений не претерпела и в период стабилизации и развития внутри страны. По-прежнему 93,4% экспорта составляли природные ресурсы (газ, нефть, каменный уголь), а импорт состоял в основном из готовых товаров и оборудования (товары ФРГ были высоко конкурентноспособными по сравнению с российскими). По итогам 2008 года Германия занимала 1 место среди главных торговых партнеров России, опережая Нидерланды и Китай.

Однако, в 2008 году возникший мировой финансовый кризис пошатнул взаимоотношения двух стран и понизил долю Германии во внешнеторговых отношениях с Россией до 8,1%.

Таблица 1 – Оборот взаимной торговли между странами

	1996 год	2020 год
Оборот	12,3 млрд. долл. США	42 млрд. долл. США
Экспорт	7,1 млрд. долл. США	18,6 млрд. долл. США
Импорт	5,2 млрд. долл. США	23,4 млрд. долл. США
Место Германии во внешнеторговом обороте России	Второе место среди главных партнеров России по рынку экспорта и третье место по импорту	Второе место среди главных партнеров России по рынку экспорта и второе место по импорту
Место России во внешнеторговом обороте Германии	Пятнадцатое место среди главных партнеров Германии по рынку экспорта и двенадцатое место по импорту	Двенадцатое место среди главных партнеров Германии по рынку экспорта и одиннадцатое место по импорту

Оборот взаимной торговли между странами увеличился на 30 млрд. долл. США. Стоит отметить, что на данный показатель оказало влияние изменение курсов валют, а также уровень инфляции и цены на углеводородное сырье. Как мы можем видеть из динамики, роли РФ в экономике ФРГ возросла (выход единственной добытчицы нефти – Великобритании из ЕС и окончание строительства Северного потока 2), так как энергоресурсы необходимы любой стране, особенно с увеличением плотности населения страны. Также можно сказать, что меры, предпринятые канцлером Германии Ангелой Меркель и Путиными В.В., благотворно повлияли на развитие торговых отношений двух стран.

Преимущества двух стран в производстве товаров для экспорта подтверждают выгодность торгового обмена. Данное обстоятельство объясняет теория абсолютных преимуществ. Очевидно, что каждая из стран имеет преимущества в том, что она поставляет на рынок второй, и что им выгодно и необходимо осуществлять такую внешнюю торговлю.

В данной ситуации работает теория абсолютных преимуществ, которая гласит, что торговля между странами будет выгодной, тогда и только тогда, когда страны торгуют между собой продукцией, которую каждая из стран сможет произвести с меньшими издержками, чем их торговый партнер, то есть, экспортируя те товары, в производстве которых имеют абсолютные преимущества.

Внешнеэкономическая деятельность между Россией и ФРГ в цифрах

Так как мы уже говорили ранее о том, что внешняя торговля находится под постоянным контролем и анализом со стороны государства. Это проявляется в том, что на основании данных Федеральной Таможенной Службы постоянно составляются статистические отчеты Министерства экономического развития, которые позволяют оценить динамику и перспективы внешнеторгового сотрудничества России и Германии.

Например, из данного отчета мы можем видеть, что внешнеторговый оборот между РФ и ФРГ 2020 года относительно 2019 года сократился на 21% (сокращение на 11,2 млрд. долларов США). Экспорт сократился на 33,6% (сокращение на 9,5 млрд. долларов США), а импорт на 6,9% (сокращение на 1,7 млрд. долларов США). Также в 2020 году получено отрицательное сальдо по торговле с Германией. Это означает, что наша страна импортирует из ФРГ больше, чем экспортирует туда. Это может быть негативным фактором, указывающим на слаборазвитости и низкоконтурентности нашей продукции на нашем же рынке по сравнению с товарами из Германии.

В структуре экспорта по-прежнему сильно преобладает минеральная продукция (нефть, газ и т.д.) – 78,1%. И так как основу экспорта составляют

минеральное топливо и нефть, то снижение их поставок очень сильно отражается на стоимостной оценке (по итогу 2020 года поставки снизились на 38,9% или на 9 098,2 млн. долл. США, или на 22,3 млн. тонн).

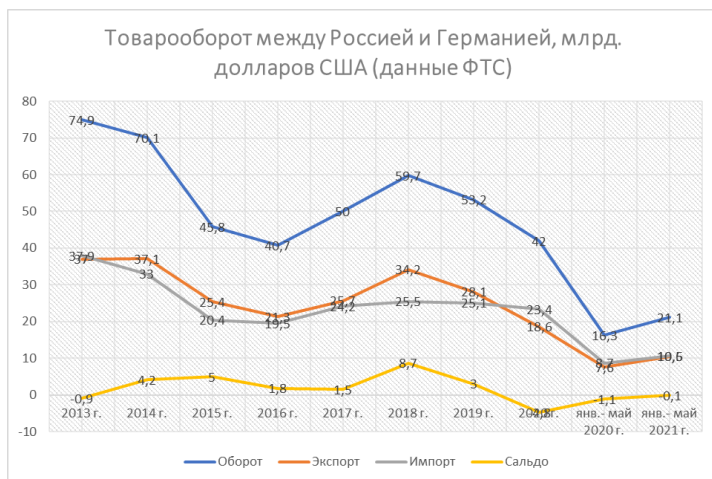


Рисунок 2 – Товарооборот между Россией и Германией, млрд.долл. США (данные ФТС)

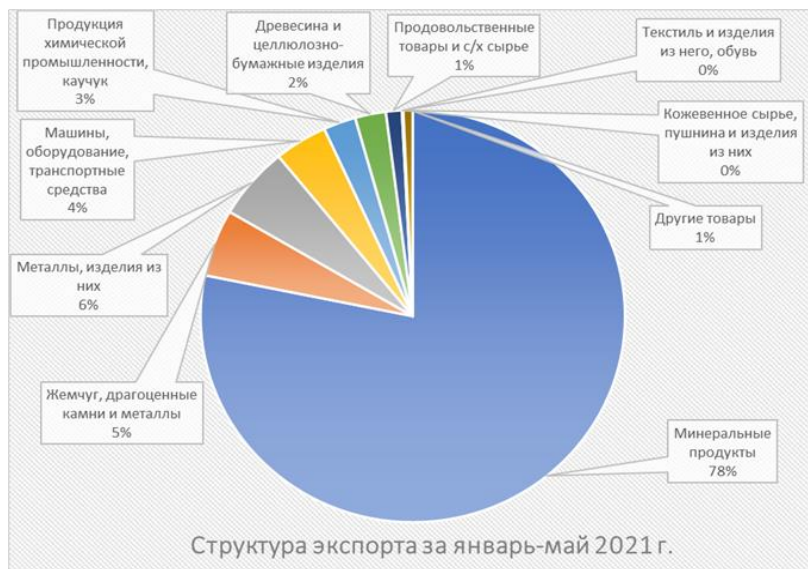


Рисунок 3 – Структура экспорта за январь-май 2021 г.

Так как Германия является высокотехнологичной страной с высококонкурентными товарами, то неудивительно, что Россия импортирует в большей мере машины и оборудование (55% от всего импорта), а также продукцию химической промышленности – 28%. Увеличение импорта по итогам периода с января по апрель 2021 г. (+22,6%, или + 1 962,4 млн долл. США) по сравнению с аналогичным периодом 2020 г. произошло в основном за счет роста импорта по следующим товарным группам:

- «Средства наземного транспорта, кроме железнодорожного или трамвайного подвижного состава, и их части и принадлежности»
- «Реакторы ядерные, котлы, оборудование и механические устройства; их части»
- «Фармацевтическая продукция»



Рисунок 4 – Динамика структуры российского импорта из Германии, млн. долл. США

Внешнеторговые отношения удерживаются на таком высоком уровне во много благодаря институциональным формам сотрудничества между РФ и ФРГ, таким как:

- 1) Российско-Германский экономический совет. Он был создан в 2020 г. как итог встречи первого заместителя Председателя Правительства с представителями германского бизнеса.

Основными целями деятельности данного Совета являются:

- а) Расширение российско-германского инвестиционного сотрудничества
 - б) Повышение инвестиционной привлекательности РФ
 - в) Помощь в продвижении интересов российских деловых кругов на рынке ФРГ
 - г) Изучение проблем, с которыми сталкиваются немецкие бизнесмены, осуществляющие экономическую деятельность на территории России
- 2) Российско-Германская Рабочая группа по стратегическому сотрудничеству в области экономики и финансов (СРГ). Данная группа создана в 2000 году по инициативе Президента Российской Федерации В.В. Путина и Федерального канцлера Германии Г.Шредера.
- 3) Российско-Германская внешнеторговая палата (ВТП). Данная Палата была создана в 2007 году по взаимному решению Президента РФ Путина В.В. и Канцлера ФРГ Меркель А. Палата продвигает интересы действующих в России немецких компаний, а также российских фирм в Германии.

Крупные инвестиционные проекты, реализуемые Германией в России

Инвестиционные отношения между Россией и Германией начали проследиваться уже более 1,5 веков назад. Это очень важная часть международных отношений, так как происходит взаимное переплетение капиталов и развитие предприятий торговли, что имеет особое значение в экономическом развитии стран. Многие зарубежные компании работают на рынке РФ, и Германия не стала исключением.

Однако, жесткие антиковидные ограничения в мировой и российской экономиках коренным образом поменяли ситуацию в негативное русло. Во 2 квартале 2020 года, когда пандемия COVID-19 только начала набирать обороты, немецкие компании вывели из России 1,6 млрд евро – это был рекорд квартального снижения в почти 30-летней истории внешнеторговых отношений между РФ и ФРГ. Также из-за неопределенностей, связанных с временными ограничениями и их беспрецедентным характером, многие немецкие компании отложили или остановили реализации проектов в России. Ситуация пока не исправилась, так как в связи с 4 волной COVID-19 отток немецкого капитала продолжился, хоть и замедлился. Показателем оттока капитала также стало сокращения количества российских юридических лиц с участием немецкого капитала (уменьшение с 4 274 до 3 971) в 2020 году.



Рисунок 5 – Текущие прямые инвестиции компаний Германии в экономику РФ, в млн. евро

Такая же ситуация в 2020 году произошла и с российскими компаниями, которые осуществляют свою деятельность в ФРГ. Во 2 квартале произошел самый крупный вывод отечественных прямых капиталов из Германии. Однако, так как инвестиционная привлекательность Германии все же выше, чем российская, российское годовое сальдо оказалось положительным и составило 450 млн. евро.



Рисунок 6 – Текущие прямые инвестиции компаний в экономику ФРГ, в млн. евро

Несмотря на пандемию COVID-19, немецкие бизнесмены в 2021 году инвестировали в Россию 1,1 млрд. евро.

Инвестиции были сделаны в такие крупные проекты, как:

1) Северный поток 2 (англ. «Nord Stream 2») - магистральный газопровод из России в Германию через Балтийское море. Трубопровод проходит через территориальные воды пяти стран: Германии, Дании, России, Финляндии и Швеции.

2) Газоперерабатывающие комплексы Linde

Linde – ведущая фирма-производитель и поставщик промышленных, пищевых, медицинских и специальных газов в РФ. Также предоставляет в РФ услуги инжиниринга, закупок и строительства в металлургической, нефтехимической, химической и фармацевтической областях.

3) Новейшие железнодорожные технологии Siemens

4) Крупные капиталовложения компании Volkswagen в ее российские заводы

По оценкам экспертов, в 2021 г. будет наблюдаться постепенное восстановление активности немецких прямых инвесторов, которые начнут реализацию ряда отложенных в 2020 г., а также новых проектов.

Вызовы 2020 года и перспективы 2021 года

На сферу внешней торговли в 2020 году наибольшее влияние оказали такие события, как:

1) Пандемия COVID-19, распространившаяся достаточно быстро по миру. Закрытие границ между Евросоюзом и Россией привело к трудностям в деловых поездках бизнесменов, а также к перебоям в работе дочерних компаний, находящихся за рубежом. Помимо этого, из-за жестких ограничений, деятельность многих хозяйствующих субъектов была приостановлена, увеличился уровень банкротств предприятий из-за отрицательных результатов по операционной деятельности.

2) Резкое снижение мировых цен на нефть. Недоговоренность и несогласованность действий стран ОПЕК+ относительно того, сколько стоит добывать нефти на основании прогнозов сокращения ее потребления, привели к обвалу мировых цен на нефть. Ситуацию удалось стабилизировать, однако негативный след все же отразился на итогах года.

Все вышеперечисленные условия стали причиной уменьшения взаимного товарооборота.

Несмотря на данные проблемы мирового масштаба, между Россией и Германией была заключена «Европейская зеленая сделка», которая дала новые пути для взаимных инвестиций и коопераций в сфере водородной энергетики.

Возвращаясь к возможностям развития российско-германским отношений на 2021 и 2022 год необходимо проанализировать также влияние некоторых негативных факторов, проявившихся в течение 2020 года.

Во-первых, стоит проследить изменения в перемещениях капитала между странами. Германия последние три года наращивала прямые капиталовложения в российскую экономику. Но введение карантинных мероприятий, повлиявших на деятельность российских компаний, повлекло за собой рекордный вывод капитала иностранных партнеров. Стоит отметить, что заявлений об отмене намеченного плана наращивания вложений в российские компании от немецкого правительства не поступало. Данное обстоятельство, позволяет строить оптимистические прогнозы по возврату капитала в 2022 году с учетом смягчения ограничительных мер, связанных с распространением новой коронавирусной инфекции.

Во-вторых, совместные проекты не только в сфере энергетики, но и инновационных преобразований, могут быть отменены в соответствии со сменой политической направленности Германии.

Несмотря на негативные факторы, даже в условиях жестких ограничений, страны продолжали сотрудничать, что предполагает взаимную заинтересованность и зависимость в экономической связи. Следовательно, предполагаем, что на 2022 год. В случае улучшения кризисной ситуацией, определяющейся коронавирусом, торговые взаимоотношения между странами должны показать резкое улучшение.

Заключение

Германия – второй по значимости партнер России, что обуславливается рядом факторов: историческим сотрудничеством, географическим положением, а также тем, что Россия и Германия производят продукцию, которая является жизненно необходимой для каждой из них. Россия неизменно на протяжении многих лет является для Германии надежным поставщиком энергоресурсов. В свою очередь, импорт германской продукции, особенно товаров легкой промышленности и технологического оборудования, играет в товарообороте России важнейшую роль.

Для лучшего привлечения инвестиций в Россию от мировых инвесторов необходимо создание конкурентной среды в нашей стране. Для этого нужно использовать заемный капитал немецких партнеров. Всё это возможно только в условиях тесного сотрудничества, которое невозможно в условиях экономических ограничений.

Таким образом, в работе были проанализированы факторы, влияющие на взаимное торговое сотрудничество России и Германии, а также на основе анализа представлен прогноз дальнейшего развития торговой деятельности. Очевидно, что зависимость российской экономической системы от Германии во многом базируется не только на инвестициях ФРГ, но и на импортируемых товарах. Что создает predisposition для развития взаимовыгодных условий сотрудничества.

Список использованных источников:

1. Белов В.Б. «Северный поток – 2» в контексте Мюнхенской конференции по безопасности // Аналитические записки ИЕ РАН. 2020. №4 (187). DOI: 10.15211/analytics42020
2. Белов В.Б. Новые водородные стратегии ФРГ и ЕС: перспективы кооперации с Россией // Современная Европа. 2020. №6. С. 65-76. DOI: 10.15211/soveurope520206576
3. Соболев А., Попцов Д. Цифровизация в 2020 году: опыт Германии и возможности для России. РСМД. 15.03.2021. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovizatsiya-v-2020-godu-opyt-germanii-i-vozmozhnosti-dlya-rossii/>
4. Соболев А. К будущему юбилею: Рапалло и экономический прагматизм. РСМД. 07.09. 2020. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/k-budushchemu-yubileyu-rapallo-i-ekonomicheskij-pragmatizm/>
5. Воробьева А.В. Перспективы развития торговых отношений между Россией и Германией. 2016. URL: <https://nauchkor.ru/uploads/documents/587d36415f1be77c40d58abe.pdf>
6. Тимофеев И.Н. Санкции против России: взгляд в 2021 г. М.: НП РСМД, 2021.
7. Федеральный закон "Об основах государственного регулирования внешнеторговой деятельности" // http://www.consultant.ru/document/cons_doc_LAW_45397/
8. Концепция внешней политики Российской Федерации // Утверждена Президентом Российской Федерации В.В.Путиным 12 февраля 2013 г. // <https://legalacts.ru/doc/kontseptsija-vneshnei-politiki-rossiiskoi-federatsii-utv-prezidentom/>
9. Рейтинг стран дальнего зарубежья по обороту торговли с РФ (источник данных: Росстат) // <https://top-rf.ru/places/530-rejting-stran.html>
10. Анисимов, А. Г. Россия и Германия в поиске путей совершенствования механизмов экономического сотрудничества /А. Г. Анисимов//Внешнеэкономический бюллетень. – 1998. №5. - С.82
11. Международная торговля товарами на основании UN Comtrade // <http://comtrade.un.org/labs/BIS-trade-in-goods/?reporter=276&partner=643&year=2014&flow=2>
12. Россия и страны-члены Европейского союза – 2005 г.: статистический сборник / Федеральная служба государственной статистики. Росстат. 2005 // http://www.gks.ru/bgd/regl/B05_65/main.htm
13. Торгово-экономическое сотрудничество России и Германии // https://www.economy.gov.ru/material/file/b94dd03f74e0648871d5eebd6535d1c0/TEC_Germany_May_2021.pdf

14. Названы главные торговые партнеры Германии Об этом сообщает "Рамблер". // <https://finance.rambler.ru/business/39201302-nazvany-glavnye-torgovye-partnery-germanii/>
15. Мировая экономика и международные экономические отношения: учебник для академического бакалавриата / под ред. А.И. Погорлецкого, С.Ф. Сутырина. – М.: Издательство Юрайт, 2016. – С. 363.
16. Торгово-экономическое сотрудничество России и Германии // https://www.economy.gov.ru/material/file/b94dd03f74e0648871d5eebd6535d1c0/TEC_Germany_May_2021.pdf
17. <https://www.bundesbank.de>.
18. Венкина Е. Число немецких компаний в РФ в 2020 году снизилось на 7 процентов. // <https://p.dw.com/p/3nP23>
19. Немецкий бизнес вкладывает свои финансы в Россию // https://www.ng.ru/world/2021-05-31/100_210531covid.html
20. Северный поток-2 // https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D0%B2%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%BF%D0%BE%D1%82%D0%BE%D0%BA_%E2%80%94%D0%93%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D0%B8%D1%8F_%D0%B8_%D0%90%D0%B2%D1%81%D1%82%D1%80%D0%B8%D1%8F
21. The Linde Group // https://ru.wikipedia.org/wiki/The_Linde_Group#Linde_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8
22. Siemens Mobility // https://ru.wikipedia.org/wiki/Siemens_Mobility

Управление ESG рисками крупных хозяйствующих субъектов на примере компании ПАО «ФосАгро»

А.В. Лукьянченко
студент 2 курса НИЯУ МИФИ, Москва
E-mail: Montopo@yandex.ru

Аннотация: Все больше компаний начинают работать над укреплением развешающихся механизмов корпоративного управления и управления рисками в области устойчивого развития. Правильно выстроенный механизм управления ESG рисками позволит не только сохранить преимущества компаний, но и повисеть эффективность ее деятельности.

Ключевые слова: ESG, риски, компания, стратегия, человеческий капитал, природный капитал, охрана труда, безопасность, экология.

ESG risk management of large business entities on the example of PJSC Phosagro

Abstract: More and more companies are starting to work to strengthen the fluttering governance and risk management frameworks for sustainable development. A properly built ESG risk management mechanism will allow not only to preserve the advantages of companies, but also to increase the efficiency of its activities.

Keywords: ESG, risks, company, strategy, human capital, natural capital, labor protection, safety, ecology.

Введение

На сегодняшний день ESG-повестка становится актуальна для всех стран мира, и Россия не исключение. ESG — это environmental, social and governance (окружающая среда, социальные обязательства и управление). Такие сферы ответственности бизнеса становятся драйвером как доходов, так и расходов. ESG имеет свои принципы базирующиеся на честности, доброй воле, прозрачности и ответственности компаний. В первую очередь это связано с тем, что не многие страны смогли разработать регуляторную базу в данном направлении.

Для российских компаний, работающих на внутреннем рынке, ESG — новое направление, принятие которого может затянуться на годы. Однако для подавляющего большинства компаний-экспортеров и компаний с

международным характером структуры владения данное направление уже не новинка, и они стараются активно внедрять новые ценности, задавая тенденция и направления в раскрытии информации.

Факт раскрытия такой информации безусловно играет положительную роль и делает компании более привлекательными и интересными не только в инвестиционном плане. Отсутствие большого интереса у компаний, занимающихся деятельностью на внутреннем рынке, вполне может быть связан с неготовностью населения платить марк-ап за экологичность.

Таким образом можно сказать, что ESG стратегия – это политика компании, связанная с вложением капитала в положительное и долгосрочное воздействие на общество, окружающую среду и общую эффективность бизнеса. В ESG стратегию входит и такое понятие, как ESG риски – это риски компании, связанные с экологией, климатом, риски в области охраны труда, связанные с управлением и другие. Зачастую компании раскрывают и описывают такого рода риски в своей интегрированной отчетности, но задачей данной работы не продублировать написанное в отчетах, а попытаться определить влияние таких рисков на деятельность компании ПАО «ФосАгро».

Описание и характеристика компании

ПАО «ФосАгро» — один из крупнейших мировых производителей минеральных удобрений. Имеет вертикально интегрированную структуру, которая включает добывающие и перерабатывающие предприятия, логистические компании, а также собственный научно-исследовательский институт.

Вертикальная интегрированность или “От руды до еды” означает, что компания добывает сырье на собственном месторождении, далее перерабатывает добываемое сырье за счет наличия базы нового и модернизированного оборудования. После чего происходит процесс производства удобрений, а затем продажа не только готовой продукции, но и услуг по управлению урожайностью на премиальных зарубежных рынках. Осуществление продаж происходит за счет развитой логистической инфраструктуры, а именно 28 региональных складских комплекса, подвижного состава из 8800 вагонов и перевалочного терминал в порту Усть-Луга.

Ведущим направлением деятельности «ФосАгро» является производство и реализация фосфорсодержащих удобрений, апатитового концентрата, кормовых фосфатов, аммиака и азотных удобрений.

Стоит сказать и про географию присутствия компании. Высокоэффективная и экологичная продукция ФосАгро востребована на всех континентах, кроме Антарктиды. Продажи в более чем 100 стран Европы, Азии, Африки, Северной и Южной Америки ведутся через сеть

собственных трейдинговых офисов, работающих на крупнейших мировых рынках удобрений. Гибкая бизнес-модель производства и продаж позволяет максимально удовлетворять спрос на экологичные и безопасные удобрения со стороны сельхозпроизводителей по всему миру.

2020 год стал первым годом нового стратегического цикла: в 2019 году Компания утвердила Стратегию-2025. Новый стратегический цикл предполагает строительство высокотехнологичных производств и увеличение выпуска удобрений и кормовых фосфатов. Реализация данной задачи невозможна без долгосрочных инвестиций как в расширение производственных мощностей, так и в инфраструктурные проекты, что как раз просматривается и в отчетности компании за 2020 год.

Основными стратегическими направлениями для компании являются:

- Операционная эффективность и рост производства;
- Развитие продаж на приоритетных рынках;
- Повышение эффективности логистики.

Описание и подробный обзор рисков компании

Компания «Фосагро»., как и многие другие компании, занимающиеся добычей и продажей удобрений и не только, сильно подвержена различного рода рискам, например, производственным, операционным, стратегическим, финансовым и др.

Таблица 2 – Классификация рисков ПОА «ФосАгро»

Производственный	Операционный	Стратегический	Финансовый
Экологический	Риски бизнес-процессов и систем	Климатический	Валютный
Риски в области охраны труда и промышленной безопасности	Экономическое безопасности	Санкционный	Кредитный
-	Информационной безопасности	Риск недостижения целей устойчивого развития	Товарно-сырьевой

В вышеперечисленном списке к ESG рискам относятся: Климатические, экологические, санкционные, экономической безопасности и риски в области охраны труда. На официальном сайте компании представлена матрица рисков, где на лидирующих позициях по важности находятся как раз именно те, что перечислены выше. И это не удивительно, ведь производство и сбыт удобрений напрямую зависит от экологической и политической ситуаций в странах.

Климатические риски связаны с изменением в природных процессах и явлениях в процессе изменения климата, а также с принятием экономических, финансовых и политических решений правительствами в области снижения темпов климатических изменений путем снижения выбросов парниковых газов посредством углеродного регулирования. Для минимизации данного риска компания строго контролирует всю цепочку создания ценности, т. е. начиная от проектирования заканчивая транспортировкой готовой продукции. Негативное влияние изменений в климате сказывается на выручке и расходах компании, снижая первое из-за не урожайности и повышая второе из-за сложностей и трудностей при добыче, заготовке и транспортировке готовой продукции. В 2020 году руководством компании была утверждена климатическая стратегия, основанная на анализе климатических рисков и возможностей по сокращению углеродного следа. Эти меры позволили улучшить рейтинг CDP (Carbon Disclosure Project) и рейтинг устойчивого развития (Systainalytics).

Экологические риски связаны с возникновением потенциального ущерба в ходе осуществления своей деятельности компаний. Для предотвращения такого рода рисков в компании утверждена политика в области охраны окружающей среды и иные документы, содержащие требования не только к ведению своей деятельности, но и к поставщикам и покупателям в области экологии. Минимизация негативного экологического влияния достигается путем модернизации складских систем и очистных сооружений. Помимо этого, в рамках проекта «Зеленая химия для жизни» компания вручает гранты, учреждением которых занималось ЮНЕСКО и Международный союз теоретической и прикладной химии. Цель грантов – это защита окружающей среды и здоровья населения.

Под санкционными рисками понимается введение зарубежных стран санкций против компании. Для снижения такого риска компания старается сделать модель производства и продаж гибкой, осуществляя это при помощи тщательной проверки контрагентов, их руководителей, учредителей, а также мест реализации услуг компаний.

Риск экономической безопасности компании – это риск получения убытков или причинения вреда имуществу в результате экономических правонарушений со стороны сотрудников или третьих лиц. В качестве способа предотвращения появления такого рода риска компания делает все возможное начиная с пропускного режима, заканчивая четким разграничением обязанностей и детальной проработкой договоров с поставщиками и покупателями.

Компания Фосагро уделяет особое внимание охране труда и промышленной безопасности, что обусловлено сложностью и опасностью проводимых работ не только под землей, но и снаружи. Данный риск связан в первую очередь с возможностью появления травм, заболеваний или с возникновением неустанных случаев, приводящих к летальному исходу. Чтобы снизить шанс появления такого риска компания действует в соответствии с законодательством РФ и применяет передовые международные практики в этой области. Компания проводит аудит и проверки систем пожарной безопасности, проводит лекции и обучающие семинары в том числе с применением дистанционных технологий.

Оценка ESG показателей компании

Для того, чтобы понять, насколько действия компании соответствуют действительности, необходимо проанализировать отчеты в области экологии, энергоэффективности, социальной ответственности и корпоративного управления.

В экологическом отчете представлены данные о выбросах загрязняющих веществ, парниковых газов, об объемах забираемой и полученной воды, сброса сточных воды, а также об объемах расходов на природоохранную деятельность.

Таблица 2 – Экологические показатели компании

Показатель	Ед. изм.	2015	2016	2017	2018	2019	2020	CA GR, %
Сумма загрязняющих веществ	тыс. т	29	30	32	32	29	30	0,84
Выбросы парниковых газов	тыс. т	3 011	3 644	4 191	4 855	4 656	4 739	9,50
Общее количество забираемой воды	млн м ³	214	221	234	224	190	227	1,13
Общий объем сброса сточных вод	млн м ³	189	200	215	186	152	188	(0,03)
Расходы на охрану окружающей среды	тыс. руб.	3 441 405	4 024 456	5 089 616	8 210 030	9 059 671	8 120 298	18,73

Значение CAGR по всем показателям из таблицы 2 важно и нужно сравнивать с CAGR по объему производства и выручки, а также с отраслевыми бенчмарками, которые пока что в процессе формирования именно по данной отрасли. Стоит отметить, что среднегодовой темп роста выручки компании за период с 2015 по 2020 гг. составляет 5,99%, в то время как расходов на охрану окружающей среды в разы выше – 18,73. Помимо всего прочего, среднегодовой темп роста объемов производства продукции ПАО «ФосАгро» составил 7,09%. Сравнивая данное значение с показателями CAGR по выбросам, можно однозначно сказать, что компания инвестирует в производство, в очистные сооружения, что лишний раз подтверждает важность и значимость экологических рисков.

Таблица 3 – Соотношение затрат на охрану окружающей среды и выручки

Показатель	Ед. изм.	2015	2016	2017	2018	2019	2020	CAGR, %
Коэффициент затрат на охрану окружающей среды	%	1,81	2,14	2,81	3,52	3,65	3,20	4,45

В таблице 3 представлен коэффициент затрат на охрану окружающей среды. Из данной таблицы видно, что компания постепенно увеличивает свои расходы на поддержание стабильной экологической обстановки в регионах пребывания. Причем среднегодовой темп роста не сильно ниже темпа роста выручки, что в целом подтверждает вышесказанное об экологических рисках.

Таблица 4 – Показатели электроэнергии

Показатель	Ед. изм.	2015	2016	2017	2018	2019	2020	CA GR, %
Потребление электроэнергии	тыс. кВт ч/т	0,27	0,25	0,25	0,24	0,23	0,23	(3,6 6)
Самообеспеченность электроэнергией	%	38,17	39,25	37,36	40,42	40,20	39,80	0,84

Потребление компанией электроэнергии с 2015 года не сильно изменилось, а скорее снизилось, даже несмотря на то, что объемы производства готовой продукции ежегодно растут. Такая стабильность невозможна без внедрения передовых технологий и мировых практик. Также немаловажный показатель не только с коммерческой точки зрения,

но и с экологической – это самообеспеченность электроэнергией. ФосАгро активно инвестирует в возобновляемые источники электроэнергии, позволяющие формировать достаточное количество энергии.

В области социальной ответственности немаловажными показателями являются коэффициент лояльности и удовлетворенности персонала, средняя заработная плата (таблица 6), LTIFR (частота травм с потерей трудоспособности), FIFR (частота смертельных случаев) и др.

Таблица 5 – Показатели охраны труда и безопасности

Показатель	2015	2016	2017	2018	2019	2020
Коэффициент частоты травм с потерей трудоспособности (LTIFR, на 200 тыс. часов), сотрудники	0,15	0,11	0,07	0,04	0,15	0,10
Коэффициент частоты смертельных случаев (FIFR, на 200 тыс. часов), сотрудники	0,00	0,01	0,01	0,00	0,03	0,00

Таблица 6 – Социальные показатели

Показатель	Ед. изм.	2015	2016	2017	2018	2019	2020	Прогноз на 2025 г.
Коэффициент лояльности и удовлетворенности персонала	%	43	52	54	62	57	63	65
Средняя заработная плата	Руб.	61 495	74 888	76 526	80 672	87 191	96 401	x

Значение коэффициента LTIFR (Lost Time Injury Frequency Rate) и FIFR (Fatal Injury Frequency Rate) также говорит о количестве случаев травмирования и о возможных рисках компании. В идеальной ситуации данные показатели должны равняться 0, т. е. не должно возникать ни травм, ни смертельных случаев.

Вывод

Правильный подход к управлению рисками устойчивого развития компании может помочь организациям получить конкурентное преимущество не только по причине заботы об окружающей среде и

обществе, но и по причине своей открытости и честности по отношению к заинтересованным сторонам.

Бизнес-ландшафт ESG рисков развивается достаточно быстро. Данный факт заставляет руководителей компаний изучать новые горизонты тенденций не только в области финансовой устойчивости компании.

Компания ПАО «ФосАгро» в лице ее руководства проделывают значимую работу не только для компании, но и в целом для России, показывая то, как это можно и нужно делать – раскрывать информацию, давая исчерпывающие ответы на большинство вопросов.

Целью данной работы было показать подход исследуемой компании к раскрытию информации о рисках, а также проанализировать насколько раскрываемая информация коррелирует с реальными показателями.

В ходе работы были даны основные понятия по теме ESG-рисков, а также разобрана часть показателей, которые можно было оценить на реальных цифрах и сформировать общее представление.

Список использованных источников:

1. Федеральный закон от 26.12.1995 N 208-ФЗ (ред. от 29.07.2017) "Об акционерных обществах".
2. Аналитическое Кредитное Рейтинговое Агентство: Методология оценки ESG от 30.03.2021.
3. Статья Goldman Sachs: If You Ignore Sustainability, You're Going To Be Worth Less, Forbes, ноябрь 2015 года, ссылка: <https://www.forbes.com/sites/jnylander/2015/11/12/goldman-sachs-if-you-ignore-sustainability-youre-going-to-be-/?sh=601e6b005c7c>
4. Когденко В.Г. Управление финансами и рисками. М.: Юнити Дана, 2019 г.
5. Косолапова, М.В. Комплексный экономический анализ хозяйственной деятельности: Учебник / М.В. Косолапова, В.А. Свободин. - М.: Дашков и К, 2016.

Учетно-контрольная среда компании в условиях цифровизации экономики

Ч.А. Нуралиева

д.э.н., профессор кафедры бухгалтерского учета, анализа и аудита

КРСУ им. Б.Н.Ельцина, Бишкек

E-mail: nur-cholpon@mail.ru

О.К. Игликов

аспирант МАУПФиБ, Бишкек

E-mail: kenjebekovich@gmail.com

Аннотация: В статье рассматриваются ключевые направления цифровой трансформации компании и основные признаки формирования цифровой бизнес-модели в ней. Роль цифровой трансформации в учетно-контрольной среде компании и влияние ИТ-новаций на совершенствование учетных и контрольных процедур компании, а также повышение их эффективности и результативности.

Ключевые слова: учетная подсистема, контрольная подсистема, цифровая трансформация, цифровой капитал, цифровая бизнес-модель, смарт-учет, блокчейн, цифровой формат, искусственный интеллект.

Accounting and control environment of the company in the context of the digitalization of the economy

Abstract: The article discusses the key areas of digital transformation of a company and the main features of the formation of a digital business model in it. The role of digital transformation in the accounting and control environment of the company and the impact of IT innovations on improving the accounting and control procedures of the company, as well as increasing their efficiency and effectiveness.

Keywords: accounting subsystem, control subsystem, digital transformation, digital capital, digital business model, smart accounting, blockchain, digital format, artificial intelligence.

Принятая в Кыргызской Республике Концепция цифровой трансформации «Цифровой Кыргызстан» 2019-2023 явилась дополнением Национальной стратегии развития Кыргызской Республики на 2018-2040 в части программы цифровой трансформации страны, определяя основу

процесса цифровизации, ее структуру и систему управления. Основное стратегическое видение цифровой трансформации повысить:

- конкурентоспособность экономики страны за счет технологических перемен, к которым приведет эта трансформация;
- эффективность государства в глобальном мире и уровень жизни граждан.

Процесс реализации цифровой трансформации в Кыргызстане продвигается медленными темпами, что связано с частой сменой правительства и с пересмотром действующего проекта Всемирного банка «Digital CASA-KP», направленного на создание благоприятных условий процесса системной цифровой трансформации страны (объем, выделенной помощи 50 млн. долларов) в сторону обновления программы с учетом последних цифровых трендов.

В контексте проекта «Digital CASA-KP» предполагалось провести 600 км волоконно-оптических линий связи (ВОЛС), что позволило бы обеспечить 60% населения Кыргызстана доступом к интернету, а запланированные к прокладке 400 км ВОЛС регионального значения для стран Центральной Азии и некоторых стран Южной Азии. В конечном итоге, Кыргызская Республика имела бы высокоскоростной и широкополосный доступ к глобальной сети, вариантный внешний канал поставки интернета., выходящий к Индийскому океану. Зарубежными экспертами уровень проникновения Интернета в Кыргызстане в 2020 году оценен как «ниже среднемирового».

Таблица 1 – Уровень проникновения Интернета стран Центральной Азии

№		Доля индивидуальных пользователей интернета (в процентах)	Число абонентов фиксированного широкополосного доступа на 100 жителей
1.	Казахстан	79	13,44
2.	Узбекистан	55	12,7
3.	Кыргызстан	38	5,64
4.	Таджикистан	22	0,07
5.	Туркменистан	21	0,09
6.	Среднемировое значение	54	13,26

Источник: Исследование ООН «Электронное правительство, 2020» [1]

В современных условиях рынка, цифровая трансформация охватила весь мир и очевидной становится необходимость системных преобразований, которые направлены на развитие цифровой экономики в экономических системах всех уровней. Большую значимость приобретает цифровая трансформация и в бизнесе, потому как способствует оптимизации и переходу компаний на электронные платформы. Создание электронных платформ невозможно без использования интернета, в связи с чем, оценка уровня проникновения интернета в стране имеет немаловажное значение в цифровой трансформации. Ключевыми направлениями цифровой трансформации в компаниях являются:

- построение современной цифровой бизнес-модели;
- разработка цифровых товаров и услуг;
- использование цифрового проектирования;
- автоматизированный сбор, хранение и обработка информации;
- управление производственными процессами и сетями поставок;
- выполнение административных функций.

Цифровая бизнес-модель характеризуется наличием в компании двух признаков. Первый, иметь инструмент для быстрого моделирования новых процессов, имеющих связь с получением нового вида нужной информации, из собранных данных и предоставление ее на те или иные рабочие места. Второй, компания может быстро принимать решения касательно того, какая информация является нужной из собранных данных и наличие в ней пользы для бизнеса при использовании на том или ином рабочем месте.

Особое место в цифровой бизнес-модели имеет учетно-контрольная среда компании, которая формируется из двух подсистем – учетная и контрольная подсистемы. Учетная подсистема включает финансовый учет, управленческий учет и налоговый учет. Каждый вид учета имеет свои основные параметры, но при этом они тесно взаимосвязаны. Взаимосвязь проявляется через реализацию общего направления – содействовать выработке управленческих решений, повышающих эффективность и результативность деятельности, и возможность их практического применения.

Контрольная подсистема характеризуется совокупностью трех составляющих: контрольная среда, учетная подсистема и контрольные процедуры, предназначенные для предупреждения, обнаружения и исправления имеющихся ошибок информации, для недопущения ее искажения. На практике, контрольную подсистему разделяют на внутреннюю и внешнюю составляющие – внутренний и внешний аудит. Внутренний аудит в зависимости от объема проводимых операций и масштабов деятельности компании может иметь самостоятельные направления: финансовый аудит, управленческий аудит, налоговый аудит.

Учетная и контрольная подсистемы являются составляющими общей системы бизнес-среды компании и в совокупности формируют учетно-контрольную систему организации, представляющую собой способ организации учетно-контрольных процессов.

Учетно-контрольная система основывается на бухгалтерской информации. Для контроля в системе используются оперативные данные, техническая и статистическая информация. В связи с этим, учетно-контрольную систему можно рассматривать как процесс сбора, обработки, анализа и оценки всех видов информации, используемых на микро и макроуровнях, а далее для принятия управленческих решений.



Рисунок 1 – Структурные элементы традиционной учетно-контрольной системы в условиях системно-ориентированного подхода
Источник: [2, с. 90]

Представленный рисунок демонстрирует тесную взаимосвязь учета и контроля, которые как составляющие учетно-контрольной системы являются необходимыми в производственном и управленческом процессе.

Организация учетно-контрольной системы компании осуществляется и координируется бухгалтером, где реализуется выполнение основной задачи: на основе учетной информации обобщить, интегрировать учетные и внутренние контрольные операции в единый процесс и направить на обеспечение его непрерывности. Конечный результат процесса – это разработка рекомендаций для принятия управленческих решений.

Учетная и контрольная подсистемы в условиях цифровой трансформации выходят на новый уровень, где цифровой капитал рассматривается, как принципиально новый источник прибыли и фактор конкурентоспособности бизнеса. Дальнейшее развитие учетно-контрольной среды компании неразрывно связано с применением информационных технологий, для устранения недостатков существующей аналитической, контрольной и учетной систем. Информация, формируемая данными системами, должна быть краткой, понятной и релевантной для принятия управленческих решений и особо полезной в создании новой цифровой бизнес-среды компании.

С каждым годом, цифровая трансформация учетной и контрольной подсистем компании будет возрастать, что объясняется необходимостью решения новых задач с применением ИТ-новаций, способствующих повышению эффективности и результативности учетных и контрольных процессов, которые в свою очередь, отразятся на качестве информационного обеспечения отдельных подразделений и пользователей, объединенных единой цифровой платформой. Следует отметить, происходит не просто преобразование данных в бумажных носителях в цифровые, а происходят процессы поиска, обработки, обобщения отчетности, сопоставимости, контроля ошибок, осуществление процессов и их результатов с помощью ИТ-инструментария.

Цифровая трансформация учетно-контрольной среды компании в соответствии с требованиями цифровой экономики должна включать следующие компоненты – информационный, организационный, программный и методический. Представленные компоненты становятся основными информационными системами и интегрируются вокруг так называемой веб-системы и между собой. Такая система обеспечивает поддержку и автоматизацию процессов управления всех составляющих деятельности компании. Качественное развитие цифровых сервисов в учетно-контрольной среде организации минимизирует человеческий фактор в принятии решений и расширяет возможности в своевременном получении качественной информации о происходящих в компании

процессах. Цифровизация, как инструмент позволяет создавать, реализовывать и пользоваться преимуществами учетной и контрольной подсистем организации, через усиливающиеся ИТ-технологии. Отлаженная централизованная ИТ-система позволяет обеспечить хозяйствующему субъекту продуктивную деятельность высокого уровня, тем самым улучшая его позиционирование на рынке.

Особое место в цифровой трансформации бизнес-среды компании занимает цифровизация системы бухгалтерского учета, что позволяет внедрять в бизнес-процессы компании новые концепции обработки и передачи информации, а именно:

- облачные технологии или облачные вычисления, позволяющие существенно увеличить эффективность всех видов бизнеса. Их мобильность позволяет оптимально быстро синхронизировать работу сотрудников или нескольких удаленных офисов в единой базе данных;

- бухгалтерский учет финансово-хозяйственной деятельности в режиме реального времени;

- искусственный интеллект в системе учета и контроля товарно-материальных запасов (автономный дрон для инвентаризации товарных запасов);

- технология «BigData» используется для хранения, структурирования, управления, анализа информации, ее обработки, создания аналитических отчетов;

- расширенный язык финансовой, управленческой, налоговой отчетности различных сфер бизнеса XBRL (eXtensible Business Reporting Language), обеспечивающий переход от простого электронного варианта бухгалтерской (финансовой) и нефинансовой отчетности (в виде PDF-отчетов) в интерактивный цифровой формат бизнес-отчетности;

- электронный обмен данными EDI (Electronic data interchange) обеспечивает обмен информацией и документами, осуществляемый на бумажных носителях, электронным документооборотом между компьютерными сетями;

- блокчейн-технология, позволяющая записывать, хранить активы, обязательства, транзакции и предоставляет методы учета движения денежных средств и сверки счетов.

В совокупности потенциал новых технологий обработки и передачи информации, используемых компаниями в цифровой бизнес-среде способны привести к кардинальным трансформационным изменениям в учетно-контрольной системе компании, повысить эффективность учетных и контрольных процедур и обеспечит более современные форматы эффективного управления.

Цифровая трансформация учетно-контрольной среды компании должна решить основную задачу – перейти не просто на цифровизацию учетных и контрольных процедур (перевод учетных и контрольных процессов в электронный формат), а создание «умного» учета и контроля финансово-хозяйственной деятельности компании, с использованием эффективных инструментов контроля и управления организацией по технологии «СМАРТ-учета». Реализацию цифровой трансформации необходимо проводить в три этапа:

1. Подготовительный этап предполагает корректировку структуры организации, информационных потоков между подразделениями, регламентов учетных и контрольных процедур.

2. Этап внедрения предусматривает рационализацию взаимодействий в учетной и контрольной среде компании с детализацией регламентов и стандартов учета.

3. Этап применения характеризуется сочетанием профессиональных аспектов учета и ИТ-инфраструктуры.

Таким образом, учетно-контрольная среда компании в условиях цифровизации переходит на новый уровень, создавая условия для использования эффективных инструментов ИТ-новаций в системе внутреннего контроля, аналитики и прогнозирования, в создании новой, отвечающей современным запросам бизнес-модели компании. Следует отметить, что по нетипичным операциям собственное суждение бухгалтера будет сохраняться, но при этом запросы будут смещаться в сторону специалистов, умеющих работать в формате «digital».

Список использованных источников:

1. Исследование ООН «Электронное правительство,2020» <https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20-%20Russian.pdf>
2. Гудков А.А. Понятие и характеристика учетно-контрольной системы предприятия//Сборник научных статей по бухгалтерскому учету, экономическому анализу и аудиту, посвященных юбилею заслуженного профессора ННГУ им. Н.И. Лобачевского, доктора экономических наук Е.А. Мизиковского. 2018. С.89-93
3. Карпова, Т. П. Направления развития бухгалтерского учета в цифровой экономике // Известия СПбГЭУ. 2018. № 3. С.52-57
4. Маслова Е. Блокчейн – это навсегда, готовьтесь. URL: <https://secretmag.ru/cases/interview/elena-masolova-tokenstars-blokchein-eto-navsegda-gotovytes.htm>.

Формирование встроенной модели управления рисками на предприятии

Е.В. Усман

к.э.н., доцент кафедры финансового менеджмента

НИЯУ МИФИ, Москва,

E-mail: elenusman@rambler.ru

Аннотация: В условиях высоких рисков на действующих предприятиях должна быть разработана адекватная система реагирования на риски. Поиск оптимальной, соответствующей специфике деятельности системы управления рисками - одна из сложнейших задач, стоящих на текущий момент перед предприятием. В статье рассмотрены подходы к формированию встроенной модели управления рисками на предприятии.

Ключевые слова: риск-аппетит, система ключевых индикаторов риска, встроенная модель управления рисками.

Formation of a built-in risk management model at the enterprise

Abstract: In conditions of high risks, an adequate risk response system should be developed at existing enterprises. The search for an optimal risk management system that corresponds to the specifics of the activity is one of the most difficult tasks currently facing the enterprise. The article discusses approaches to the formation of a built-in risk management model at the enterprise.

Keywords: risk appetite, system of key risk indicators, built-in risk management model.

Согласно ГОСТ Р 51897-2011, риск определяют как следствие влияния неопределенности на достижение поставленных целей [1, стр.4]. В современных условиях количество факторов неопределенности существенно увеличилось. Основное влияние на деятельность предприятия оказывают внешние риски, не подлежащие контролю со стороны предприятия. Руководство предприятий вынуждено приспосабливаться к высоким уровням неопределенностей факторов внешней среды, разрабатывать стратегию и тактику управления рисками. Формирование встроенной модели управления рисками на предприятии позволит снизить влияние катастрофических рисков, оптимально распределить ресурсы в рамках системы «риск-доходность».

Встроенная модель управления рисками предполагает автоматическое реагирование компании на изменение уровня внешних рисков. Цель формирования встроенной модели – достижение устойчивости к риску компании в условиях нестабильности факторов внешней среды. Компанию можно считать устойчивой к риску, если она эффективно функционирует при всех вариантах развития событий, а риск-последствия могут быть предотвращены предусмотренными в планах компании мероприятиями (лимитирование рисков, страхование, резервирование, диверсификация и т.д.).

С целью проверки организации на устойчивость к риску особую актуальность приобретают методы оценки риска, основанные на стресс-тестировании деятельности предприятия и его отдельных подразделений. Стресс-тестирование может быть применено на всех этапах управления рисками и исследовать влияние исключительных, но вероятных событий. Итоги стресс-тестирования позволят предприятию количественно оценить величину предполагаемых убытков и сформулировать рекомендации по управлению в условиях максимальных рисков.

Оптимальная схема управления рисками на предприятии должна предусматривать гибкий механизм реагирования на изменения факторов внешней среды. Все функции управления (прогнозирование, планирование, организация, мотивация, контроль) должны иметь встроенную функцию реагирования на риски.

Таблица 1 – Применение методов оценки риска в процессе управления организацией

Функция управления	Элемент процесса риск-менеджмента	Методы
Прогнозирование	Идентификация риска, обмен информацией	Контрольные листы, предварительный анализ опасностей, структурированное интервью, метод Дельфи, структурированный анализ сценариев методом "что, если?" (SWIFT)
Планирование	Оценка риска, обмен информацией	Анализ сценариев, анализ воздействия на бизнес, анализ дерева решений, моделирование методом Монте-Карло
	Сравнительная оценка риска, обмен информацией	HAZOP, Байесовский анализ, анализ видов и последствий отказов (FMEA)

Организация	Мониторинг риска, обмен информацией	НАССР, LOPA, анализ "галстук-бабочка"
Контроль	Оценка риска, сравнительная оценка риска, обмен информацией	Анализ причин и последствий, FMEA

В процессе планирования мероприятий по управлению рисками следует осуществить оценку приемлемого для предприятия риска с учетом позиции и ожиданий стейкхолдеров. Приемлемый риск – элемент стратегического планирования, определяемый на этапе постановки стратегических целей и задач. Приемлемый риск должен быть основан на уверенности менеджмента в том, что принятие риска в таком объеме позволит компании увеличивать стоимость. Формирование стратегических ориентиров определяет целевые установки компании, выявляет показатели эффективности, к которым компания стремится в долгосрочной перспективе. Однако не следует путать ключевые показатели эффективности и ключевые индикаторы риска. Ключевые индикаторы эффективности оценивают фактически достигнутый результат, в то время как ключевые индикаторы риска должны не только отражать предпочтительные для компании риски, но и оценивать реальные последствия для компании опасных событий.

Определим основные этапы по формированию риск-ориентиров компании:

Этап 1. Оценка емкости к риску компании, то есть выявление максимального риска, который компания в состоянии принять. Фактически данный этап определяет зону катастрофических рисков, при достижении которой предприятие рискует потерять собственный капитал и стать банкротом.

Этап 2. Определения риск-аппетита компании, то есть объема риска, который компания в действительности сможет принять для достижения своих целей. Риск-аппетит – показатель комплексного воздействия всех рисков на организацию. Основными требованиями к формированию риск-аппетита компании являются: комплексность, контролируемость, соответствие стратегическим ориентирам компании, учет количественных и качественных показателей, прогностический подход, интегрированность в общую систему управления.

На этапе определения риск-аппетита необходимо выполнить следующие шаги:

Шаг 1. Определение модели расчета риск-аппетита. Наиболее актуальной моделью определения риск-аппетита в существующих условиях является модель, основанная на стресс-тестировании

организации. Модель подразумевает установление комбинации факторов, приводящих к худшему состоянию для организации.

Шаг 2. Формирование системы показателей, характеризующих текущее состояние и динамику показателей риск-аппетита с учетом отраслевой принадлежности.

Шаг 3. Декомпозиция системы показателей и определение системы ключевых индикаторов риска для каждого риска, необходимых и достаточных для принятия решения менеджерами компании.

Шаг 4. Определение значимости ключевых индикаторов риска, то есть веса каждого ключевого индикатора с системе индикаторов.

Шаг 5. Формирование стратегии риск-аппетита и доведение стратегических ориентиров до сотрудников предприятия.

Следует помнить, что риск-аппетит является стратегическим ориентиром, однако в условиях высоких рисков для компании рекомендуется корректировать данный показатель не реже одного раза в год.

Этап 3. Определение толерантности к риску, то есть объема риска, который компания может принять в существующих условиях с учетом ожиданий заинтересованных лиц (акционеры, кредиторы, поставщики, менеджеры предприятия, сотрудники и т.д.). Под толерантностью к риску следует понимать возможные отклонения ключевых индикаторов риска, приемлемые для организации в существующих условиях.

Этап 4. Формирование категорий риска по функциональным подразделениям организации и определение системы ключевых индикаторов риска для каждого функционального подразделения с определением лимитов риска. Под лимитом риска будем понимать пороговые значения ключевых индикаторов риска, превышение которых не допустимо в рамках действующей модели управления рисками.

Рекомендуем, в рамках каждого подразделения, установить три уровня ключевых индикаторов:

1. Уровни ключевых индикаторов, находящихся в зоне допустимых рисков и не требующие корректирующих мер.

2. Уровни ключевых индикаторов, находящихся в зоне критических значений и требующие корректирующих мер.

3. Уровни ключевых индикаторов, находящихся в зоне катастрофических рисков и требующих применения комплекса мер с целью недопущения катастрофических последствий.

В условиях высоких рисков особую актуальность приобретает качественная система ключевых индикаторов риска, количественно характеризующих источники риска[2,стр.4]. Определим требования к формированию системы ключевых индикаторов риска:

1.Простота для оценки, интерпретации и мониторинга.

2.Актуальность для текущей ситуации, поэтому ключевые индикаторы должны постоянно пересматриваться. На основании анализа текущей ситуации могут быть добавлены новые индикаторы, пересмотрены текущие, исключены неактуальные.

3. Учет отраслевой специфики и особенностей функционирования предприятия. Следует помнить, что не существует универсальной системы ключевых индикаторов и их границ, поскольку сам набор индикаторов и их численное значение, будут существенно отличаться в разрезе различных отраслей промышленности.

4.Оптимальность, поскольку система ключевых индикаторов риска должны быть минимальна и достаточна для выявления факта реализации риска.

5.Исключение дублирующих индикаторов, то есть ключевые индикаторы не должны быть частными случаями других индикаторов.

6.Учет существенности риска, оцениваемого индикатором. Определение уровня значимости может быть проведено на основе коэффициента значимости.

7.Экономичность индикатора, определяемая как соотношение затрат на получение данных по индикатору и уровня риска.

8.Количественная измеримость, дающая возможность оценки факта реализации риска или роста вероятности реализации риска [3,стр.12]. С этой точки зрения, предпочтительными являются количественные индикаторы.. Качественные индикаторы могут быть применены в ситуации, когда невозможно осуществить оценку стоимостных потерь для предприятия в случае реализации риск-события. Количественная измеримость также позволяет осуществлять сравнительную оценку риска, осуществлять сопоставление с отраслевыми индикаторами, определять динамику риск-факторов.

Оценка эффективности мероприятий по управлению рисками должна строится на принципах:

1.Мероприятия по управлению рисками эффективны, если увеличивают ценность фирмы.

2.Стоимость мероприятий по управлению рисками не должны превышать возможных убытков в случае реализации рисков.

3.При оценке эффективности мероприятий по управлению рисками должен учитываться фактор времени.

Автором рекомендуется осуществлять оценку эффективности встроенной модели управления рисками на основе показателя чистого дисконтированного дохода, рассчитанного по схеме «действующего

предприятия». Фактическим показателем эффекта будет выступать значение приростного чистого дисконтированного дохода.

Формула приростного чистого дисконтированного дохода:

$$NPV_{\text{инт}} = NPV_{\text{рм}} - NPV_{\text{баз}},$$

где

$NPV_{\text{инт}}$ – приростный чистый дисконтированный доход, характеризующий рост ценности фирмы в результате внедрения встроенной модели управления рисками;

$NPV_{\text{рм}}$ - дисконтированный доход с учетом внедрения встроенной модели управления рисками;

$NPV_{\text{баз}}$ - дисконтированный доход без учета внедрения встроенной модели управления рисками.

При значении показателя приростного NPV больше нуля, встроенная модель управления рисками эффективна и ее следует принять, поскольку в долгосрочной перспективе она обеспечит прирост ценности фирмы. При значении показателя меньше нуля – модель не окупится и следует отказаться от внедрения. Частная ситуация, при которой значение приростного чистого дисконтированного дохода будет равна нулю, означает необходимость внесения дополнительных корректировок в существующую систему с возможным сокращением расходов на ее содержание.

В условиях высоких рисков факторов внешней среды, организации должны постоянно осуществлять мониторинг риска, принимая решения с учетом актуального риск-аппетита. Управление рисками должно обязательно строиться на принципе «участия»: каждый сотрудник предприятия должен быть осведомлен о риск-аппетите компании, ключевых индикаторах риска, лимитах риска. Встроенная модель управления рисками позволит повысить управляемость рисками, снизить чувствительность к рискам организации, предотвратить влияние катастрофических рисков и снизить вероятность банкротства.

Список использованных источников:

1. ГОСТ Р 51897-2011/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения
2. Р 50.1.090-2014 Менеджмент риска. Ключевые индикаторы риска
3. <https://new.nfa.ru/upload/iblock/516/Rukovodstvo-po-upravleniyu-riskami.pdf>

Франчайзинг как инструмент стратегического управления и развития в сфере фаст-фуда на примере Макдоналдс

М.В. Черненко

студентка 4-го курса НИЯУ МИФИ

E-mail: otep.sh@gmail.com

Т.Н. Бочкарева

к.т.н., доцент кафедры финансового менеджмента

НИЯУ МИФИ, Москва

E-mail: tnbochkareva@mephi.ru

Аннотация: В статье говорится о характеристиках и влиянии стратегических ресурсов на деятельность организации, а также о возможных угрозах экономической безопасности РФ в отрасли общественного питания.

Ключевые слова: общественное питание, корпорации, менеджмент организации, противодействие угрозам экономической безопасности.

Selection of strategic resources to ensure the economic security of the company

Abstract: The article talks about the characteristics and influence of strategic resources on the activities of the organization, as well as about possible threats to the economic security of the Russian Federation in the public catering industry.

Keywords: public catering, corporations, organization management, countering threats to economic security.

Общественное питание – это отрасль экономики, отвечающая за производство и сбыт готовой пищевой продукции и организующая услуги по ее потреблению. На сегодняшний день данная индустрия состоит из большого количества компаний и предприятий различного уровня и качества обслуживания, из которых можно выделить [3]:

- Рестораны – это предприятия, которые специализируются на предоставлении широкого и сложного ассортимента блюд;
- Бары – это заведения, продающие в основном алкогольную продукцию и закуски к ним;

– Столовые – это предприятия, которые ориентированы на достаточно узкий сегмент потребителей;

– Кафе – это организации, предоставляющие своим посетителям широкий выбор десертной продукции, а также специализирующиеся на продаже чая и кофе;

– Предприятия быстрого обслуживания – это вид субъектов общепита, который предлагает небольшой ассортимент готовой продукции из полуфабрикатов и ориентируется на высокую скорость обслуживания.

Данная отрасль экономики удовлетворяет широкий спектр потребностей потребителей, за счет чего получает все большую популярность среди потенциальных предпринимателей и инвесторов. Можно выделить такие преимущества отрасли как:

1. Увеличение свободного времени населения;
2. Удовлетворение социально-культурных потребностей населения;
3. Комплексное снижение затрат на ведение домашнего хозяйства;
4. Рациональное использование финансовых ресурсов населения;
5. Повышение доходов малоимущих слоев населения;
6. Предоставление новых рабочих мест.

Стоит акцентировать внимание на том, что общественное питание – специфичная многофакторная отрасль, так как сочетает в себе три основные функции:

1. Производственная функция: позволяет отнести общепит к сфере материального производства, так как в процессе производства на предприятиях общественного питания создается новый продукт, а сотрудники производят новую стоимость, т. е. национальный доход. Однако стоит учесть, что данная функция содержит в себе нюансы, которые отличают отрасль от «классической» производственной:

– Объем производимой продукции зависит от спроса на нее, контингента потребителя и типа конечного предприятия и как правило не хранится на складах (ввиду коротких сроков годности готовой продукции);

– Процесс производства хаотичен, так как не несет серийного характера и зависит от спроса на конкретный период времени;

– Сама отрасль динамичная, и ориентирована на конкретную аудиторию;

– Почти все готовые товары имеют аналоги у различных конкурирующих предприятий, следовательно, большинство продукции – это субституты.

2. Функция реализации: заключается в продаже потребителю продуктов общественного питания в качестве товаров, которые имеют дополнительную стоимость и новые потребительские

свойства. Поэтому выполнение этой функции позволяет сравнить организации общепита с предприятиями торговли.

3. Функция организации услуг по обслуживанию и потреблению пищи: делает отрасль уникальной и специфической, так как не встречается более ни в одной другой отрасли народного хозяйства. Сущность данной функции заключается в предоставлении организации потребления на месте производства и реализации пищи. Следовательно, Отрасль общественного питания относится не только к производственной и торговой сфере, но и к сфере услуг.

Общественное питание – динамичная отрасль, которая охватывает интересы практически всего населения, следовательно, стоит рассмотреть современные тенденции в ее развитии:

- Востребованность сегмента быстрого питания. Эта тенденция характеризуется демократизацией рынка, следовательно, позиции фаст-фуда в отрасли усиливаются.
- Сетивизация общественного питания. В период локдауна во время пандемии COVID-19 несетевые заведения закрывались гораздо чаще, что привело к освобождению и дальнейшему захвату корпорациями новых рыночных долей.

Стоит заметить, что на текущий момент в России самой эффективной моделью ведения бизнеса оказался франчайзинг – около 48% всех сетевых ресторанов открыты именно по франшизе (McDonald's, KFC, Subway, ГрильХаус, Соfix и т. д.).

В структуре рынка преобладают (рисунок 1) [1]:

1. Заведения FastFood (47%), что обусловлено высокой скоростью обслуживания, доступными ценами, сильными маркетинговыми стратегиями (огромные финансовые вложения в рекламу, акции, программы лояльности).
2. Кафе (18%).
3. Рестораны (14%)
4. Бары (11%)
5. StreetFood или уличные киоски (7%)

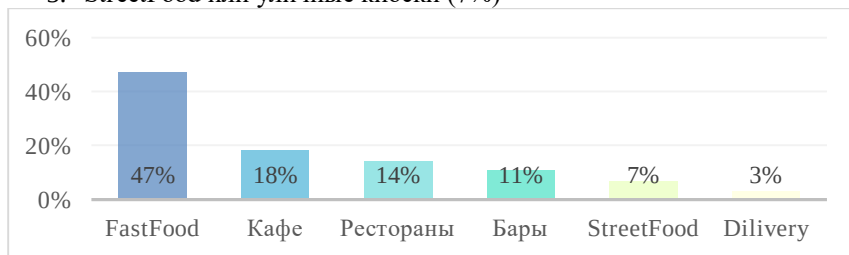


Рисунок 1 – Структура рынка общественного питания

В данный момент наиболее перспективным и инвестиционно-привлекательным элементом отрасли общественного питания является сегмент фаст-фуда. В связи с ускорением темпов жизни общества, появлению технического и информационного прогресса, стремлению к многозадачности рынок фаст-фуда (по данным Росстата) занял 55% от доли отрасли.

Характерной чертой сегмента можно считать неоднородность и разносторонний охват целевой аудитории, так как предприятия фаст-фуда способны удовлетворить очень сложный набор потребностей и не акцентируют внимание на уровне дохода, возрасте, социальном статусе или интересах - данный сегмент рынка доступен всем. Именно по этой причине ежегодно растет спрос на услуги предприятий быстрого обслуживания, что приводит к ежегодному увеличению сектора на 25%.

Основными источниками роста компаний в сегменте фаст-фуда являются:

1. Открытие новых точек производства и реализации готовых товаров из полуфабрикатов. Например, McDonald's начал активно осваивать Дальний Восток, создав дочернее предприятие ООО «ДВРП» и перенаправив в регион квалифицированные кадры – менеджеров и инструкторов по обучению.
2. Расширение меню. Ежегодно вводится новая линейка продукции, рассчитанная на увеличение товарооборота и среднего чека за счет «лимитированности» продукции.
3. Внедрение инновационных технологий, которые уменьшают время обслуживания, что приводит к увеличению товарооборота компании и привлечению новых посетителей.
4. Использование западных концепций, таких как «монопродукт» и минимализм.
5. Использование франчайзинга.

Франчайзинг – это договорные отношения между франчайзером и франчайзи, при которых компания, дающая франшизу, обязана поддерживать интерес к бизнесу, инвестируя первоначальные капитальные вложения, передавая свои технологические разработки и раскрывая все нюансы ведения бизнеса в конкретной сфере. При этом франчайзи вносит дополнительные капиталовложения за счет собственных ресурсов, усилия по развитию бизнеса и опыт работы из различных рынков, работая при этом под торговой маркой франчайзера. Рассмотрим реализацию этой формы организации бизнеса на примере одной из самых успешных транснациональной компании McDonald's.

Компания осуществляет свою деятельность более чем в 100 странах мира, при этом выбирая как основную форму ведения бизнеса именно франчайзинг: более 90% ресторанов в США управляются франчайзи.

Для того, чтобы стать владельцем ресторана, потенциальному партнеру необходимо заплатить от 45 000 долларов компании, при этом окончательная сумма инвестиций определяется главным офисом в зависимости от региона. Так же франчайзи вынужден платить McDonalds роялти в виде 4% от процентов от продаж. Несмотря на крупную сумму инвестиций и ежемесячных отчислений получатель франшизы получает такие преимущества как:

1. Возможность избежать ошибок при открытии бизнеса с нуля: отсутствие необходимости в составлении бизнес-плана и проведении детального исследования рынка;
2. Готовая и отлаженная концепция бизнеса: отсутствие потребности в создании и дальнейшем масштабировании жизнеспособного продукта;
3. Возможность от экономии масштаба при взаимоотношениях с контрагентами: проявляется в желании потенциальных поставщиков и подрядчиков работать с крупной и значимой на рынке компаний;
4. Ведение бизнеса под известным брендом: заключается в уже имеющихся доверии и лояльности потребителей к уже разрекламированному имени компании;
5. Снижение расходов на рекламу и продвижение продукции: компания сама разрабатывает маркетинговую стратегию и финансирует создание и распространение рекламных продуктов;
6. Снижение расходов на анализ рынка, продумывания стратегии выхода на рынок: отсутствие необходимости самостоятельно проводить анализ сегмента, строить прогноз продаж и формировать бюджет, так как данные функции корпорация берет на себя и предоставляет поддержку и ресурсы франчайзи.

Стоит учитывать, что в России концепция франчайзинга только начинает развиваться, поэтому McDonald's использует «гибридную» форму организации бизнеса, постепенно открывая предприятия под управлением франчайзи, которые являются крупными предприятиями, из-за чего корпорация получает такие преимущества как:

1. Расширение сбытовой сети при минимальных затратах и небольшом риске;
2. Осуществление и усиление контроля над раздробленными рынками;
3. Быстрое распространение торговой марки;

4. Покрытие расходов на обучение и поддержку франчайзи происходит за счет денежных поступлений за пользование торговой маркой.

Несмотря на значительное количество преимуществ франчайзинга McDonald's, существует ряд недостатков и рисков, которые мешают развитию бизнеса в данной форме. Во-первых, это паушальный взнос (затраты на покупку франшизы), так как данные инвестиции способны значительно сократить объем капитала, что приведет к неспособности франчайзи платить роялти и покрывать расходы на аренду, закупку оборудования и трат на декор. Во-вторых, франчайзер несет репутационные риски, связанные с некомпетентностью или ненадежностью юридического или физического лица, получившего франшизу: независимо от изначальной организации и эффективности бизнеса существует вероятность в предоставлении некачественного обслуживания, обнародования коммерческой тайны или иных факторов, которые подорвут доверие к компании. В-третьих, существует риск расторжения договора в силу несоблюдения франчайзи своих обязательств, что приведет к закрытию или временной приостановки деятельности предприятия и последующим финансовым потерям. Наконец, риск несоблюдения концепции предприятия, так как франчайзи хоть и имеют самостоятельность, но она ограничена правилами и нормами McDonald's, нарушение которых может повлиять как на репутацию компании, так и на ее финансовое состояние.

Для наиболее полного изучения франчайзинга как инструмента стратегического управления необходимо воспользоваться PEST- и SWOT-анализами, которые помогут выявить сильные и слабые стороны компании, а также потенциальные возможности и угрозы.

Таблица 1 – PEST-анализ

Политические	Экономические
1. Внешняя политика государства; 2. Коррупционные риски; 3. Регулирование франчайзинга через нормативно-правовые акты.	1. Уровень инфляции; 2. Валютный курс; 3. Уровень конкуренции в сегменте фаст-фуда; 4. Выгода открытия новых предприятий под управлением франчайзи.
Социокультурные	Технологические
1. Тренды и тенденции в обществе; 2. Наличие квалифицированных кадров;	1. Динамика появления ноу-хао в отрасли; 2. Совершенствование технологий, улучшающих обслуживание

3. Культурные особенности в регионе.	3. Степень цифровизации отрасли.

Стоит акцентировать внимание на том, что факторы, описанные в таблице 1, непосредственно влияют на репутацию компании, ее прибыль и ведение бизнеса в целом, так же стоит учитывать, что PEST-анализ показывает факторы макросреды, которые не в полной мере описывают риски и возможности компании на рынке. Выявить сильные и слабые стороны компании, работающей по франшизе, возможно через проведение SWOT-анализа.

Таблица 2 – SWOT-анализ

SWOT-анализ	Возможности	Угрозы
	1. Расширение зоны влияния и захват новых рынков; 2. Наличие четких территориальных границ	1. Высокий уровень конкуренции; 2. Недостатки франчайзинговой системы; 3. Риски, связанные с франчайзингом
Сильные стороны	Сильные стороны и возможности	Сильные стороны и угрозы
1. Готовая концепция ведения бизнеса; 2. Увеличение скорости распространения бренда; 3. Сильный маркетинг, в который вкладывается только франчайзер	1. Рост прибыли за счет открытия новых точек сбыта продукции; 2. Развитие и приобретение жестких стандартов обслуживания	1. Угроза перенасыщения рынка; 2. Отсутствие полной самостоятельности в принятии решений
Слабые стороны	Слабые стороны и возможности	Слабые стороны и угрозы
1. Законодательная база; 2. Большие затраты на покупку торговой марки; 3. Репутационные риски	1. Отсутствие необходимости или невозможность развития в определенном регионе; 2. Нереализованный предпринимательский потенциал франчайзи	1. Потеря потребителей из-за недобросовестности франчайзи; 2. Падение выручки из-за факторов внешней и внутренней среды.

Таким образом организационно-управленческая деятельность в форме франчайзинга имеет ряд преимуществ, которые помогают компаниям успешно конкурировать на рынке, эффективно вести бизнес и избегать больших убытков в кризисные периоды.

Список использованных источников:

1. Федеральная служба государственной статистики. Социально-экономическое положение России — 2020 г. https://gks.ru/bgd/regl/b20_01/Main.htm
2. Акимова, Р. А. Анализ состояния и тенденции развития рынка общественного питания в России / Р. А. Акимова. — Текст : непосредственный // Молодой ученый. — 2021. — № 10 (352). — С. 51-53.
3. Батраева Э. А. Экономика предприятия общественного питания: учебник и практикум для СПО / Э. А. Батраева. - 2-е изд., перераб. и доп. - М.: Издательство Юрайт, 2018. - 390 с.

Цифровая трансформация в деятельности региональных интеграционных объединений (на примере африканского региона)

Е.В. Дробот

к.э.н., доцент, ответственный редактор

ООО «Первое экономическое издательство», Москва

E-mail: elenadrbot@mail.ru

Аннотация: В статье анализируется влияние цифровизации на процессы региональной интеграции в Африке. Определены главные проблемы цифровой трансформации стран Африки. Обоснована необходимость принятия универсальных рамочных стандартов управления цифровыми данными и кибербезопасности в Африке.

Ключевые слова: Африканская континентальная зона свободной торговли, интеграция, кибербезопасность, цифровая трансформация, цифровизация

Digital transformation in regional integration (the African region case)

Abstract: The impact of digitalization on regional integration in Africa is discussed. The main problems of digital transformation in African countries are identified. The necessity of adopting universal frameworks for digital data management and cybersecurity in Africa is substantiated.

Keywords: African Continental Free Trade Area, integration, cybersecurity, digital transformation, digitalization

Африканская континентальная зона свободной торговли (African Continental Free Trade Area, далее – AfCFTA) начала функционировать 1 января 2021 г. В состав AfCFTA вошли 54 из 55 стран – членов Африканского союза (АС) [8, с. 465–482; 10, с. 351–378]. Ожидаемые преимущества создания единого африканского рынка в рамках AfCFTA эксперты связывают, во-первых, со снижением тарифных и нетарифных барьеров во внутриафриканской торговле, в результате чего прогнозируется увеличение регионального экспорта на 29% в период с 2020 по 2035 год [33, с. 9], а во-вторых, со снижением производственных издержек и экономии за счет эффекта масштаба для местных производителей и экспортеров.

Тем не менее для обеспечения полной реализации потенциала AfCFTA необходимо обеспечить цифровую трансформацию в африканском регионе.

Эффективная политики в сфере цифровизации стран африканского континента должна быть направлена на обеспечение свободного потока данных и информации между странами AfCFTA для облегчения сотрудничества и обмена знаниями, а также на снижение издержек торговой интеграции и устранение существующих структурных барьеров для внутрирегиональной торговли в Африке [9, с. 869–896; 11, с. 355–376; 17, с. 3109–3120; 23, с. 69–70; 32, с. 63–66].

Следует отметить, что если проблемы цифровизации стран и континентов достаточно широко рассматриваются в современных научных исследованиях [6, с. 911–928; 7, с. 443–454; 12, с. 689–714; 13, с. 443–454; 14, с. 455–480; 18, с. 47–60], то особенности влияния цифровой трансформации на страны африканского региона изучены недостаточно. По поисковому запросу «цифровизация» на 17 ноября 2021 г. на портале ELIBRARY.RU можно обнаружить 148143 публикации, из них всего 4 посвящены цифровизации в Африке [2, с. 38–47; 3, с. 429–439; 4, с. 38–45; 5]. По поисковому запросу «цифровая трансформация» на 17 ноября 2021 г. на портале ELIBRARY.RU размещено 150412 публикаций, из них всего 5 затрагивают особенности цифровой трансформации в Африке [1, с. 557–560; 15, с. 277–280; 16, с. 78–90; 19, с. 92–108; 20, с. 160–161].

Именно поэтому интерес представляет исследование влияние цифровой трансформации экономики на процессы региональной интеграции, в частности на африканском континенте.

Как цифровизация может помочь развитию интеграционных процессов в Африке?

Функционирование AfCFTA на базовом уровне регулируется пятью инструментами. Это форум для онлайн-переговоров, цифровая платежная система, система мониторинга и устранения нетарифных барьеров, Африканская торговая обсерватория (African Trade Observatory, АТО) и правила происхождения товаров. И для обеспечения успешной работы всех вышеназванных инструментов требуется эффективное цифровое подключение [30].

Развитие цифрового сектора африканского континента имеет решающее значение для экономической интеграции и может помочь устранить некоторые давние структурные торговые барьеры, обеспечивая при этом справедливое распределение выгод от участия стран в AfCFTA.

Рассмотрим примеры того, как цифровая трансформация может помочь преодолеть эти барьеры.

1. Цифровизация обеспечивает оптимизацию торговых операций и бизнес-процессов за счет снижения затрат. Использование цифровых технологий помогает снизить транзакционные издержки, такие как затраты на поиск всех видов экономических ресурсов и факторов производства и координацию логистики, которые связаны с традиционными каналами доставки, а также преодолеть языковые барьеры. Более широкое внедрение цифровых технологий в таможенное регулирование также может повысить эффективность внешнеэкономических операций за счет ускорения всех видов таможенных процедур и операций, включая транзит, экспорт и импорт. Кроме того, как показывает опыт осуществления предпринимательской деятельности в условиях пандемии COVID-19, благодаря доступу к цифровым платформам многие виды бизнеса не только смогли успешно адаптироваться к новым экономическим реалиям, но и повысить свою устойчивость к потрясениям.

2. Цифровизация обеспечивает улучшение условий участия в глобальных производственно-сбытовых цепочках за счет упрощения обмена информацией. Цифровые платформы оказались особенно полезными для потенциальных покупателей и продавцов во многих регионах, устраняя лишние барьеры в цепочке создания стоимости. Цифровой обмен информацией о правилах и стандартах ведения бизнеса между участниками рынка и предоставление более точной информации о предпочтениях потребителей расширяет торговые возможности. Увеличение доступности информации о рынке с помощью анализа больших объемов данных может облегчить африканским поставщикам расширение их участия в глобальных производственно-сбытовых цепочках.

3. Цифровизация расширяет доступ на новые рынки, особенно для малых предприятий, которые составляют подавляющее большинство фирм в большинстве стран Африки. Например, в Нигерии, 95% всех фирм относятся к категории микро- и малых предприятий [24]. Эти предприятия, как правило, обладают меньшими возможностями с точки зрения вариантов финансирования и наличия цифровых навыков для адаптации своих бизнес-операций к условиям конкуренции на региональных и глобальных рынках. Например, в Нигерии только 18% микро- и малых предприятий знают об AfCFTA и новых возможностях, тогда как осведомленность средних предприятий составляет 67% [24].

4. Цифровые технологии могут предоставить новые возможности для особо уязвимых групп населения, например, для занятых в неформальном секторе и для живущих в сельских районах, устраняя барьеры для расширения бизнеса и одновременно способствуя более эффективному

развитию рынка услуг для обеспечения быстро растущих потребностей населения континента.

5. Цифровизация может способствовать доступу к финтех-кредитованию, краудфандингу и другим способам финансирования и оплаты. Это особенно актуально для небольших предприятий-экспортеров в Африке, поскольку в результате цифровой трансформации улучшаются их возможности по расширению и обслуживанию клиентской базы.

6. Используя платформы электронной торговли, африканские предприниматели получают возможность привлекать новых местных и зарубежных деловых партнеров и клиентов.

Однако, несмотря на огромный потенциал и важность цифровизации для региональной интеграции, уровень цифрового развития в Африке остается пока достаточно невысоким.

Что мешает цифровой трансформации в Африке?

Остановимся на важнейших проблемах в сфере цифровой трансформации в Африке, от способности решать которые будет зависеть успех AfCFTA.

Во-первых, уровень внедрения цифровых технологий и их использования в Африке по-прежнему очень низок. Доступ к Интернету в Африке ограничен: только 47% населения континента имеют доступ к Интернету по сравнению со средним показателем в 63% по всему миру [27]. Качество цифровой инфраструктуры также остается невысоким: 59% от общего числа всех доступных в Африке мобильных технологий составляют достаточно медленные системы мобильной связи второго поколения 2G, а на системы 4G приходится всего 6% рынка сотовой телефонии [25]. Поэтому неудивительно, что большинство африканских стран не готовы к использованию лучших достижений глобальной цифровой революции.

Пандемия COVID-19 и вызванные ее проблемы уже показали важность улучшения цифровой связи между странами AfCFTA. Так, переговоры по фазе II AfCFTA, которые из-за пандемии велись онлайн, были замедлены из-за проблем с подключением и опасений по поводу безопасности [21]. Учитывая, что правительства по-прежнему испытывают трудности с цифровым соединением друг с другом, малые и микропредприятия и домашние хозяйства в Африке, несомненно, сталкиваются с более серьезными проблемами.

Во-вторых, еще одна проблема цифровой трансформации в Африке связана с отсутствием национальных и региональных рамочных стандартов управления данными.

В условиях развития региональной экономической интеграции стран Африки в формате AfCFTA происходит рост трансграничной экономической деятельности на континенте, что приводит к расширению обмена данными. В результате требуется согласование действий стран AfCFTA в сфере регулирования использования данных и цифровых систем, в частности онлайн-платежей. Кроме того, странам AfCFTA следует уделить внимание координации своих действий по таким вопросам, как налогообложение цифровых платформ и промышленная политика, направленная на поддержку предпринимателей, ведущих бизнес онлайн.

Поскольку доверие является необходимым условием для обеспечения непрерывного трансграничного цифрового взаимодействия, необходима четкая структура управления данными на национальном и региональном уровнях. Такие законы необходимы для того, чтобы развеять опасения, связанные с защитой конституционных прав граждан, включая права на неприкосновенность частной жизни, защиту данных и свободу слова.

И в Африке первые шаги в этом направлении уже были сделаны. Так, в 2014 г. на региональном уровне Африканский союз инициировал принятие Конвенции о кибербезопасности и защите персональных данных [22]. Однако только 14 стран Африки подписали Конвенцию, из них восемь – ратифицировали.

Также в 2020 г. Африканский союз разработал Стратегию цифровой трансформации для Африки на 2020–2030 гг. [26]. Цель стратегии состоит в том, чтобы служить дорожной картой в освоении цифровых технологий для содействия созданию полностью интегрированного и инклюзивного цифрового общества к 2030 г., ставя главной задачей улучшение благосостояния населения Африки. Поскольку стратегия является относительно новой, оценивать ее эффективность пока преждевременно.

Однако, несмотря на наличие Конвенции о кибербезопасности и защите персональных данных и Стратегии цифровой трансформации Африки на 2020–2030 гг., в Африке отсутствует надежная и скоординированная система рамочных стандартов управления данными, которая помогла бы обеспечить бесперебойность и совместимость данных.

По данным Конференции Организации Объединенных Наций по торговле и развитию (далее – ЮНКТАД), значительное число африканских стран пока не приняли законодательство для защиты цифровых сделок и операций и использования персональных данных [31]. По данным на апрель 2020 г., только в 25 странах Африки действует

законодательство в сфере защиты онлайн-покупателей, в 27 – о защите персональных данных, в 33 – о защите цифровых сделок и в 39 странах приняты законы о киберпреступности (рис. 1).

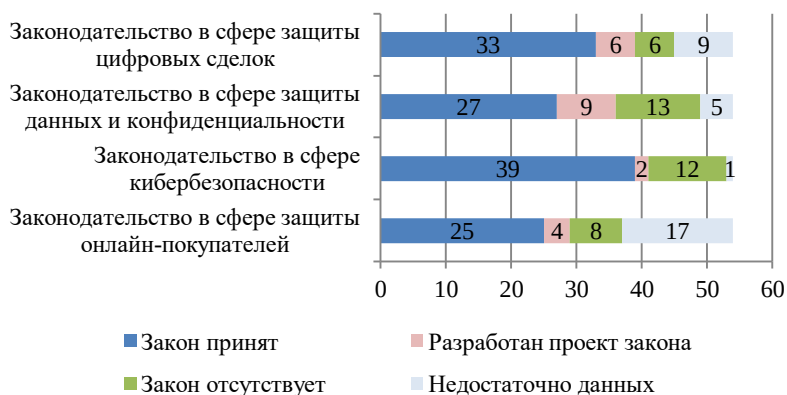


Рисунок 1 – Число африканских стран, принявших законодательство в сфере цифровой безопасности [31]

В результате того, что странам Африки свойственен различный уровень «цифровой зрелости», принятые или разрабатываемые законы по защите цифровых данных не согласованы. В большинстве стран Африки также отсутствует правоприменительная практика в сфере кибербезопасности, не хватает финансовых и человеческих ресурсов, а также надежных институтов для поддержки развития цифровой среды.

Для повышения конкурентоспособности африканской цифровой экономики и максимального использования потенциала Африканской континентальной зоны свободной торговли правительствам африканских стран необходимо скоординировать свои национальные стратегии и унифицировать законодательство в области кибербезопасности, конфиденциальности, защиты персональных данных и трансграничных сделок, а также разработать универсальные рамочные стандарты управления цифровыми данными.

Помимо обеспечения безопасности данных, в целях развития цифровой экономики в Африке чрезвычайно важно расширять доступ к цифровым технологиям, к сети Интернет по доступным ценам, в том числе путем увеличения государственных расходов на развитие информационно-коммуникационной инфраструктуры и создания более благоприятных нормативных условий для инвестиций частного сектора [28]. В качестве одного из средств достижения этой цели выступает Программа развития

инфраструктуры в Африке с объемом финансирования более 11 млн долл. США, принятая Африканским банком развития [29].

Развитие дальнейшего сотрудничества в области информационных технологий, кибербезопасности, международного роуминга приведет к расширению внутриафриканской торговли и производственной интеграции в рамках Африканской континентальной зоны свободной торговли.

В результате можно будет говорить о перспективах единого panaфриканского цифрового рынка к 2030 г. и реализации Стратегии цифровой трансформации для Африки на 2020–2030 гг., которой предусмотрено создание «интегрированного и инклюзивного цифрового общества и экономики в Африке для улучшения качества жизни граждан Африки, укрепления экономики, обеспечения ее диверсификации и развития» [26].

Список использованных источников:

1. Агоштинью, А. К. Цифровая трансформация и страны Африки / А. К. Агоштинью, В. В. Бритвина // СНК-2020 : материалы Юбилейной LXX открытой международной студенческой научной конференции Московского Политеха, Москва, 21–24 апреля 2020 года. – Москва : федеральное государственное бюджетное образовательное учреждение высшего образования «Московский политехнический университет», 2020. – С. 557–560.
2. Аджимет, Г. Х. Деятельность мировых ритейлеров в условиях цифровизации / Г. Х. Аджимет // Ученые записки Крымского инженерно-педагогического университета. – 2021. – № 2(72). – С. 38–47. – DOI 10.34771/UZCEPU.2021.72.2.009.
3. Алхассан, Т. Ф. Финансирование инновационного развития экономики стран Африки: роль цифровизации и финансовых инноваций / Т. Ф. Алхассан, А. Д. Куадио, Д. Э. Гомадо // Вестник Российского университета дружбы народов. Серия: Экономика. – 2020. – Т. 28. – № 3. – С. 429–439. – DOI 10.22363/2313-2329-2020-28-3-429-439.
4. Гаврилов, А. В. Проблемы цифровизации сельского хозяйства развивающихся стран / А. В. Гаврилов // Наука без границ. – 2021. – № 7(59). – С. 38–45.
5. Гаврилова, Н. Г. Цифровизация сельского хозяйства: перспективное направление решения продовольственной проблемы африканских стран / Н. Г. Гаврилова, Р. Р. Мухаметзянов // International Agricultural Journal. – 2021. – Т. 64. – № 5. – DOI 10.24412/2588-0209-2021-10367.

6. Городнова, Н. В. Развитие цифровой экономики: теория и практика / Н. В. Городнова // Вопросы инновационной экономики. – 2021. – Том 11. – № 3. – С. 911–928. – doi: 10.18334/vinec.11.3.112227.
7. Грачев, С. А. Моделирование влияния цифровизации на развитие социально-экономических систем / С. А. Грачев // Вопросы инновационной экономики. – 2021. – Том 11. – № 2. – С. 443–454. – doi: 10.18334/vinec.11.2.112224.
8. Дробот, Е. В. Африканская континентальная зона свободной торговли как новый этап экономической интеграции на африканском континенте / Е. В. Дробот // Экономические отношения. – 2021. – Том 11. – № 3. – С. 465–482. – doi: 10.18334/eo.11.3.112133.
9. Дробот, Е. В. Конкурентоспособность стран Африканской континентальной зоны свободной торговли в условиях пандемии COVID-19 / Е. В. Дробот // Вопросы инновационной экономики. – 2021. – Том 11. – № 2. – С. 869–896. – doi: 10.18334/vinec.11.2.112132.
10. Дробот, Е. В. Трансформация отраслевой структуры инновационного бизнеса в Африке и вызовы пандемии коронавируса / Е. В. Дробот, И. Н. Макаров, А. Л. Сапунцов // Вопросы инновационной экономики. – 2021. – № 1. – С. 351–378. – doi: 10.18334/vinec.11.1.111858.
11. Дробот Е. В. Африканская континентальная зона свободной торговли в зеркале международной экономической интеграции: Quo Vadis? / Е. В. Дробот, А. Л. Сапунцов // Экономические отношения. – 2021. – Том 11. – № 2. – С. 355–376. – doi: 10.18334/eo.11.2.112139.
12. Дудин, М. Н. Тенденции, возможности и угрозы цифровизации национальной экономики в современных условиях / М. Н. Дудин, С. В. Шкодинский // Экономика, предпринимательство и право. – 2021. – Том 11. – № 3. – С. 689–714. – doi: 10.18334/epp.11.3.111785.
13. Завьялов Д. В. Цифровые платформы как инструмент и условие конкурентоспособности страны на мировом рынке товаров и услуг / Д. В. Завьялов, Н. Б. Завьялова, Е. В. Киселева // Экономические отношения. – 2019. – № 2. – С. 443–454. – doi: 10.18334/eo.9.2.40608.
14. Костин, К. Б. Современные технологии цифровой экономики как драйвер роста мирового рынка товаров и услуг / К. Б. Костин, А. А. Березовская // Экономические отношения. – 2019. – № 2. – С. 455–480.
15. Кузьмин, Д. В. Цифровые трансформации в странах Субсахарской Африки / Д. В. Кузьмин // Экономика и предпринимательство. – 2020. – № 9(122). – С. 277–280. – DOI 10.34925/EIP.2020.122.9.057.
16. Новикова, З. С. Цифровая трансформация экономики как вектор развития Африки / З. С. Новикова // Экономика Африки в эпоху

- глобальной технологической революции. – Москва : Институт Африки РАН, 2019. – С. 78–90.
17. Павлов, В. В. Расширение участия стран Африки в международной промышленной кооперации / В. В. Павлов, А.Л. Сапунцов // Экономика, предпринимательство и право. – 2020. – Том 10. – № 12. – С. 3109–3120. – doi: 10.18334/epp.10.12.111506.
 18. Печаткин В. В. Уровень цифровизации видов экономической деятельности как фактор их конкурентоспособности в условиях пандемии / В. В. Печаткин, Л. М. Вильданова // Вопросы инновационной экономики. – 2021. – Том 11. – № 1. – С. 47–60. – doi: 10.18334/vinec.11.1.111893.
 19. Руденко, Л. Н. Перспективы цифровой трансформации экономики арабских стран / Л. Н. Руденко // Российский внешнеэкономический вестник. – 2019. – № 5. – С. 92–108.
 20. Юзеф, Х. А. М. Цифровая трансформация на Ближнем Востоке и в Северной Африке / Х. А. М. Юзеф // Проблемы и перспективы развития научно-технологического пространства : Материалы III Международной научной интернет-конференции. В 2-х частях, Вологда, 24–28 июня 2019 года. – Вологда : Вологодский научный центр Российской академии наук, 2019. – С. 160–161.
 21. Adedeji Adeniran, Sone Osakwe. Why Digitalization and Digital Governance Are Key to Regional Integration in Africa. Center for Global Development. May 11, 2021. – URL: <https://www.cgdev.org/blog/why-digitalization-and-digital-governance-are-key-regional-integration-africa> (date of access: 17.11.2021).
 22. African Union Convention on Cyber Security and Personal Data Protection. African Union, June 27, 2014. – URL: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> (date of access: 17.11.2021).
 23. Benedict Okey. Facilitating the transformational AfCFTA: Tools for eliminating bottlenecks / In FORESIGHT AFRICA 2021 / Okey Benedict. – BROOKINGS, 2021. – P. 69–70.
 24. Continental Integration & the Nigerian Economy. The Effect of the African Continental Free Trade Area on Medium Small and Micro-scale Enterprises in Nigeria. NACCIMA, September 2020. – URL: <https://naccima.com/media-center/research-reports/307-report-impact-of-the-african-continental-free-trade-area-afcfta-on-nigerian-micro-small-and-medium-enterprises.html> (date of access: 17.11.2021).
 25. Digital Economy Report 2019. – UNCTAD/UN, Geneva, 2019. – 172 p. – URL: <https://unctad.org/webflyer/digital-economy-report-2019> (date of access: 17.11.2021).

26. The Digital Transformation Strategy for Africa (2020–2030). African Union, May 18, 2020. – URL: <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030> (date of access: 17.11.2021).
27. Internet World Stats. Usage and Population Statistics. – URL: <https://www.internetworldstats.com/stats.htm> (date of access: 17.11.2021).
28. Overview: Priorities to make digitalisation work for all in Africa. OECD library 2021. – URL: <https://www.oecd-ilibrary.org/sites/7b66a37e-en/index.html?itemId=/content/component/7b66a37e-en> (date of access: 17.11.2021).
29. Programme for Infrastructure Development in Africa (PIDA). African Development Bank Group, 2021. – URL: <https://www.afdb.org/en/topics-and-sectors/initiatives-partnerships/programme-for-infrastructure-development-in-africa-pida> (date of access: 17.11.2021).
30. Schelenz, L. Digitalization in Africa: Interdisciplinary Perspectives on Technology, Development, and Justice / L. Schelenz, K. Kerstin Schopp // International Journal of Digital Society (IJDS). – 2018. – № 4. – DOI: 10.20533/ijds.2040.2570.2018.0175.
31. UNCTAD E-Commerce Legislation Index – April 2020. UNCTAD, 2020. – URL: <https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide> (date of access: 17.11.2021).
32. Wamkel Mene. Making the AfCFTA Vision our reality / In FORESIGHT AFRICA 2021 / Mene Wamkel. – BROOKINGS, 2021. – P. 63–66.
33. World Bank. The African Continental Free Trade Area: Economic and Distributional Effects. – Washington, DC: World Bank, 2020. – 138 p. – doi: 10.1596/978-1-4648-1559-1.

Цифровой рубль как новая форма российской национальной валюты

В.А. Кузнецова

слушатель 5 курса МосУ МВД России им. В.Я. Кикотя, Москва

E-mail: lera12071999@mail.ru

Научный руководитель: Т.Н. Агапова

профессор кафедры экономической безопасности, финансов и
экономического анализа МосУ МВД России им. В.Я. Кикотя, Москва

E-mail: tnagapova@gmail.com

Аннотация: Цель написания статьи – исследовать сущность цифрового рубля как новой формы российской валюты. При написании были использованы методы анализа и сравнения преимуществ и недостатков появления новой формы рубля, а также рисков, которые могут возникнуть при внедрении новой цифровой валюты в российскую экономику. Автор высказывает поддержку выпуска цифрового рубля.

Ключевые слова: цифровой рубль, российская национальная валюта, Центральный Банк РФ.

Digital Ruble as a New Form of Russian National Currency

Abstract: The purpose of this article is to explore the essence of the digital ruble as a new form of Russian currency. When writing, methods were used to analyze and compare the advantages and disadvantages of the appearance of a new form of the ruble, as well as the risks that may arise when introducing a new digital currency into the Russian economy. The author expresses support for the issue of the digital ruble.

Keywords: digital ruble, Russian national currency, Central Bank of the Russian Federation.

В современной России, как и в других странах мира уже давно существует две основные формы платежных средств: наличные и безналичные деньги. Однако цифровые технологии не стоят на месте и начинают становиться неотъемлемой частью нашей жизни. Таким образом, сейчас в условиях цифровизации мировой экономики и стремительного развития финансовых технологий общество требует появления кардинально новых способов платежей. Такой запрос становится причиной

появления новых форм национальных валют в различных государствах мира, не обходит эта тенденция стороной и Российскую Федерацию.

К одной из таких новых форм можно отнести цифровой рубль, возможность выпуска которого активно изучается Центральным Банком Российской Федерации в настоящий момент. Цифровой рубль – это цифровая форма денег, которая будет выпускаться Центральным Банком РФ в ближайшем будущем наряду с безналичными и наличными денежными средствами, в качестве новой российской национальной валюты. Стоит отметить, что цифровой рубль создаётся не с целью замены, а в качестве дополнения к уже имеющимся и привычным нам формам наличных и безналичных денег. Обсуждать возможность появления цифровых денег в России, так называемого «цифрового рубля», начали еще в конце 2020 года. Тогда был выпущен консультационный доклад «Цифровой рубль», в котором были представлены различные формы реализации данного проекта и обсуждалась необходимость его внедрения. Сейчас прототип платформы цифрового рубля находится на стадии разработки, а изменение законодательной базы РФ и тестирование проекта начнется уже в начале 2022 года. И к 2030 году новая форма российской национальной валюты должна войти в обращение в Российской Федерации и стать привычной нам, как уже существующие наличные и безналичные денежные средства.

Причинами, по которым Центральный Банк РФ считает необходимым появление цифрового рубля, служат:

- ускорение процесса совершения различных денежных операций, сделать их удобнее и безопаснее, чем с использованием наличных и безналичных денег;
- обеспечение доступности к цифровым деньгам всех экономических субъектов, что станет причиной уменьшения стоимости различных платёжных услуг и повышения конкуренции среди финансовых организаций;
- уменьшение наличной денежной массы в России;
- поддержание развития цифровых экономических отношений в Российской Федерации;
- обеспечение конкурентоспособности экономики России на мировой арене.

Эту новую форму российской национальной валюты Центральный Банк РФ будет эмитировать в виде цифрового кода, который должен будет храниться на электронных кошельках Центрального банка РФ.

Алгоритм эмиссии цифровых денег в России имеет простую схему. Она представлена ниже.



Рисунок 1 – Алгоритм эмиссии цифрового рубля в России

Согласно данным Концепции цифрового рубля появление новой цифровой валюты имеет как положительные, так и отрицательные аспекты, а также немало рисков, поэтому пока непонятно успешным ли будет проект введения новой цифровой валюты в России. По данным этой же Концепции 75 % респондентов общественной консультации в рамках доклада «Цифровой рубль» считают необходимым внедрение российской цифровой валюты уже сегодня и отмечают множество преимуществ этого проекта над наличными и безналичными платёжными средствами, потому что цифровые деньги сочетают в себе свойства присущие как наличным, так и безналичным денежным средствам. К таким преимуществам можно отнести:

- возможность осуществления платёжных и иных операций как в онлайн режиме, так и без доступа к сети Интернет (офлайн-режим);
- снижение стоимости платёжных операций или переводов денежных средств за счёт установления Банком России пороговых комиссий, что делает цифровой рубль более выгодным для россиян, чем использование банковских карт для совершения подобных операций только с большей переплатой, появляющаяся из-за процентов, выставленных обслуживающими клиента коммерческими банками;

- повышенный уровень доступности к цифровым платежам, возникающий за счёт возможности его использования без доступа к сети Интернет, то есть в офлайн-режиме, что будет являться явным плюсом для жителей отдаленных и малонаселенных районов нашей огромнейшей по площади территории страны;

- повышение уровня конкуренции на финансовом рынке, что может стать причиной появления инновационных высокотехнологичных продуктов и сервисов, предлагаемых обслуживающими коммерческими организациями и повышения качества обслуживания клиентов;

- повышение уровня финансовой безопасности за счёт гарантированной защиты денежных средств клиента, которые будут храниться на специальных электронных кошельках Центрального Банка РФ, посредством наличия уникального кода цифрового рубля, который позволит отслеживать движение денежных средств клиента. То есть в случае банкротства финансовой организации, денежные средства все равно остаются доступны клиенту через любую другую финансовую организацию, клиентом которой они являются, так как они хранятся на электронном кошельке, а не на счёте в банке.

Несмотря на явные имеющиеся преимущества цифрового рубля над другими формами расчётов для граждан и предпринимательства, 16 % респондентов не поддержали проект внедрения цифровой валюты в нашей стране, так как не увидели сильно значимых преимуществ цифрового рубля и высокой необходимости в такой форме российской валюты. А согласно мнению оставшихся 9 % респондентов необходимость появления цифрового рубля будет актуальна только на последующих этапах. Новая форма российской национальной валюты, цифровой рубль, по мнению респондентов, также должна удовлетворять их требования в высоком уровне безопасности и защищённости от различного рода мошеннических действий, удобстве и простоте использования даже финансово неграмотными клиентами и возможности использования цифровых денег в любое время, в любом месте, без доступа к сети Интернет. Повышения уровня финансовой грамотности в рамках этого проекта можно достигнуть за счёт проведения информационной кампании, которая будет направлена на более полное раскрытие информации о цифровом рубле в целом и о способах его использования.

Теперь считаю необходимым раскрыть преимущества внедрения цифрового рубля не только для граждан и финансового рынка, но и для государства. Во-первых, к ним стоит отнести контроль за расходованием средств бюджета, который достигается за счёт гарантированного обеспечения доставки целевого финансирования в виде выплат гражданам или предпринимателям. Во-вторых, значительное повышение

эффективности осуществления контроля за движением бюджетных средств, при минимальных затратах и операционных рисках. В-третьих, упрощение производства и повышение эффективности трансграничных платежей за счёт объединения новой формы российской национальной валюты с аналогичными цифровыми валютами других государств мира.

Однако, несмотря на наличие большого количества преимуществ внедрения цифрового рубля в качестве новой формы денежных средств, существует немало рисков реализации данного проекта. Во-первых, это группа технических рисков. Самый главный из них, по моему мнению, это сложность обеспечения использования платформы цифрового рубля без доступа к сети Интернет, то есть в офлайн-режиме. Для снижения этого риска Центральный Банк РФ в ближайшем будущем начнёт проводить различные исследования, направленные на изучение возможности обеспечить офлайн-режим. Следующим серьёзным техническим риском является обеспечение конфиденциальности, то есть информационной безопасности, индивидуальных данных клиентов, которые планируют использовать цифровой рубль как одну из форм российской национальной валюты. И ещё одним, не менее существенным техническим риском будет являться сложность массового аппаратного обеспечения всех будущих пользователей цифрового рубля. Центральным Банком РФ в качестве меры снижения этого риска предлагается широкое развитие IT-инфраструктуры и активное привлечение российских производителей, которые будут готовы к разработке достаточного количества аппаратного обеспечения в России. Во-вторых, риском, который не будет относиться к техническим, является риск оттока ликвидности. Снизить этот риск Центральный Банк РФ предлагает за счёт растягивания процесса внедрения цифрового рубля и обеспечения кредитных организаций возможностью использовать лимитные механизмы при операциях с этой новой формой денег, что позволит обеспечить, во-первых, абсолютный контроль за этим процессом, во-вторых, снизит вероятность быстрого оттока денежной массы из банковского сектора, и, в-третьих, даст возможность коммерческим организациям адаптироваться и скорректировать свою структуру баланса.

Главным и самым существенным минусом появления новой формы российской национальной валюты, цифрового рубля, будет слабый уровень киберустойчивости. К сожалению, существующий в настоящее время механизм киберустойчивости банковского сектора не достиг необходимого уровня, чтобы защитить пользователей цифрового рубля от различного рода киберпреступлений, таких как взлом личного профиля пользователя и хищение его денежных средств, сбои системы при её использовании в офлайн-режиме и другие.

Основными схемами операций по движению цифрового рубля будет:

- Эмиссия цифрового рубля;
- Открытие специального электронного кошелька пользователем цифровой валюты и его пополнение;
- Осуществление переводов российской цифровой валюты между клиентами финансовых организаций (физическими лицами);
- Использование цифрового рубля как средства платежа, то есть в качестве оплаты купленных товаров.

Итак, подводя итог изучению заявленной в статье темы: «Цифровой рубль как новая форма российской национальной валюты», можно сделать следующие выводы.

Поддерживая появление цифрового рубля в нашей стране, следует отметить, что в век стремительного развития цифровых технологий, необходимо не отставать от других развитых государств, уже активно внедряющих цифровые деньги в свою экономику, либо планирующих сделать это в ближайшем будущем. Изучение этого вопроса является интересным и актуальным, так как проблема появления цифровых денег в мировой практике в силу своей новизны пока еще недостаточно проработана с научной точки зрения. В развитии находятся исследования сущности, факторов и последствий на каждом, выделенном в статье, аспекте:

- сущность цифрового рубля;
- причины необходимости его появления;
- алгоритм выпуска Центральным банком РФ новой цифровой валюты;
- преимущества и недостатки её появления;
- риски, с которыми может столкнуться государство при его внедрении;
- возможные операции, которые можно будет осуществлять, используя новую цифровую валюту.

Список использованных источников:

1. Банк России. Концепция цифрового рубля – Москва, 2021 г. –Режим доступа:http://www.cbr.ru/content/document/file/120075/concept_08042021.pdf (дата обращения:18.11.2021).
2. Чернышова Е. Цифровой рубль: зачем он запускается и как будет работать, 2021 г. – Режим доступа: <https://trends-rbc-ru.turbopages.org/trends.rbc.ru/s/trends/industry/60e4014c9a7947816217cac1> (дата обращения:18.11.2021).
3. Болдова К. Цифровой рубль: зачем он нужен России, 2021 г. – Режим доступа: <https://journal.open-broker.ru/research/zachem-nuzhen-cifrovoy-rubl/> (дата обращения:18.11.2021).

Цифровой рубль: риски и обеспечение безопасного функционирования

Н.К. Норец

к.э.н., доцент кафедры финансов и кредита Институт экономики и управления «КФУ им. В.И. Вернадского», Симферополь

E-mail: naduhai@inbox.ru

Аннотация: Цифровизация всех секторов экономики обусловила возникновение и новых видов финансовых взаимодействий, новых финансовых продуктов и услуг. Автором дается попытка рассмотреть риски и угрозы внедрения цифрового рубля, выпускаемого Центральным банком Российской Федерации.

Ключевые слова: цифровой рубль, Центральный банк, национальная валюта, бумажные деньги, безопасность, цифровая экономика.

Digital rouble: risks and providing its safe functioning

Abstract: Digitalizing all sectors of economics promoted the springing up new types of financial cooperation, new financial products and services. The author makes an attempt to analyze the risks and threats of embedding digital rouble, being emitted by the Central Bank of the Russian Federation.

Keywords: digital rouble, Central Bank, national currency, paper currency, safety, digital economics.

Перспективы внедрения в оборот цифровых валют будоражат умы ученых-экономистов многие годы. Переход к цифровым реалиям, ускоренным санкционными и ковидными мероприятиями, способствовали внедрению цифровых, электронных, игровых/сетевых валют во всем мире. Российская Федерация, двигаясь в ногу с современными тенденциями, приняла к рассмотрению разработанную Центральным банком концепцию цифрового рубля [7]. Попытки оценить и «разгадать» загадку цифрового рубля наблюдаются в трудах отечественных экономистов: И.В. Кисарова [2], В.Э. Кроливецкой [3], И.Е. Шакера [8], Е.А. Ягуповой [9] и многих других, вопросами безопасного функционирования цифровых валют посвящены работы Д.Д. Буркальцевой [1], И.В. Курьяновой [4], Н.К. Норец [5, 6].

В.Э. Кроливецкая в своем докладе в 2020 году предположила, что

«цифровой рубль обнаруживает большое сходство с электронными деньгами» [3, С. 463]. Нам все же кажется, что имеется ряд отличий, причем значимых, что выделяет цифровой рубль от электронного рубля. Одной из таких особенностей является то, что функционирование цифрового рубля возможно не только в сети Интернет и посредством неё, а также как и наличного, офлайн, путем прямых переводов электронных средств с чипа, находящегося на карте банкноты. Эта его особенность так же несет в себе некоторые риски: поскольку в случае его утери, кражи или размагничивания чипа вернуть средства представляется невозможным. Цифровой рубль, также, как и «реальный» рубль, в отличие от безналичного, будет иметь уникальный цифровой код (серию и номер, например), что делает его подобным бумажному рублю и отследить движение каждого рубля становится более реальным, чем отслеживание онлайн-движения средств. Этот же принцип затрудняет подделку и фальсификацию этого вида валюты, в отличие от реальных (бумажных) денег.

Формирование цифрового рубля позволит контролировать нежелательные транзакции участников финансовых операций. Особенностью цифрового (в отличие от бумажного) рубля является наличие «следа», «цифровой памяти» о предыдущих владельцах и операциях, в которых он участвовал. Такая «память» позволит регулятору отслеживать незаконные и сомнительные операции, что позволит пресекать «отмывание» денег, участие в операциях по приобретению оружия, наркотиков, торговле людьми и их органами.

Возникает так же ряд вопросов с пассивным использованием банками остатков на счетах (иногда граждане получают дополнительные бонусы за наличие таких остатков), т.к. хранение цифровых рублей будет персонифицировано и таким образом, будет заморожено в некотором смысле.

Разработка и внедрение в оборот цифрового рубля, скорее всего, сформирует цифровое обязательство Центрального банка РФ в части использования цифрового рубля в качестве средства платежа и способа хранения стоимости. Цифровой рубль ЦБ РФ при его всеобщем использовании сформирует следующий шаг в развитии безналичных видов денег в формировании расчетов с прочими кредитными организациями. Таким образом, выделится новый вид денег – «цифровые деньги», который дополнит денежную массу, т.к. он не заменит электронные, а будет самостоятельной цифровой валютой. Таким образом возникают вопросы его денежно-кредитного регулирования, оценки ликвидности, дисконтной политики, механизмов формирования ставок и т.д.

Резкое и всеобщее внедрение цифрового рубля, скорее всего, приведет

к очищению экономики, что, безусловно, положительно, однако, небольшие денежно-кредитные учреждения вряд ли смогут противостоять новым условиям, что может вызвать «дефляционный шок».

Предполагается, что цифровой рубль станет новым более удобным, дополнительным средством расчета как среди физических и юридических лиц, так и выйдет на международные рынки. Если говорить о внутреннем движении цифрового рубля – то он предоставит дополнительные возможности для граждан в труднодоступных, малонаселенных регионах, где доступ к цифровой инфраструктуре ограничен.

Современные деньги при реализации этого сценария будут выполнять роль обслуживания товарного и финансового рынков, а также частичного регулирования финансового сектора с целью повышения стабильности финансовой и экономической систем [8, С. 14].

Нынешние российские деньги необходимы в качестве «буферного заграждения» для цифрового рубля, используемого в широком обиходе, для обычных сделок с товарами и услугами на рынке страны и в меньшей мере – за рубежом, в странах-партнерах, с которыми есть договоренность о взаимной поддержке валют [цит. по: 2, С. 203].

Предполагается, что наличные рубли останутся в обороте при осуществлении сделок, однако возможно, что их курс (спрос) может быть ниже, чем у цифрового рубля – что обусловлено законами спроса и предложения, а также возможностью совершать прочие сделки используя наличность. В 2014 году, при переходе экономики Крыма в экономику России, когда в республике фактически функционировали обе валюты одновременно (украинская гривна и российский рубль) преимущественно розничная торговля принимала к оплате российский рубль, курс рубля возрос и от гривны пытались поскорее избавиться. В настоящее время в Симферополе при оплате проезда в общественном транспорте безналично – цена ниже, чем при оплате наличными. Разумным видится сохранение наряду с эмиссией цифрового рубля эмиссия бумажного рубля с использованием его безналичной формы, переход должен быть постепенным, по мере развития инфраструктуры использования цифрового рубля. Считаем, что сравнение цифрового рубля Центрального банка РФ с криптовалютой неуместно, поскольку в случае с цифровым рублем имеет место фиксированный эмитент, который обеспечивает эмитируемую валюту, определен объем выпуска, имеет персональный номер (табл. 1).

Таблица 1 – Сравнение видов национальной валюты в России*

Основные элементы	Наличные рубли	Электронные рубли	Цифровые рубли
Эмитент	Центральный Банк РФ	Финансовые институты	Центральный Банк РФ

Форма	Защищенная бумага	Цифровая запись в банковской базе	Чип-карта
Персонализация	На предъявителя	Персонализированы	Персонализированные или на предъявителя
Ариал функционирования	Преимущественно страна происхождения	Преимущественно страна происхождения	Неограниченно
Объём эмиссии	Решение эмитента	Решение по национальной валюте	Решение эмитента
Форма хранения	Банковская ячейка	Магнитная карта или счет	Цифровой номер
Способ обращения	Двустороннее обращение	Двустороннее обращение	Двустороннее обращение
Эквивалентность	Устанавливается эмитентом	Эквивалент наличной валюты	Не эквивалентно наличной валюте
Кредитное обеспечение	Правительство	Правительство	Правительство
Безопасность	средняя	высокая	Более высокая
Стоимость обслуживания процесса обращения	высокая	высокая	низкая
Инструменты реализации обращения	Денежно-кредитная система государства	Интернет, сеть банкоматов	Программное обеспечение
Средство сбережения	Без начисления процентов	С возможностью начисления процентов	Без начисления процентов

* при введении цифрового рубля в обращение

Необходимости сокращать количество пользователей и владельцев цифрового рубля ЦБ РФ нет, поскольку он, скорее всего, будет обеспечен ценными бумагами, таким образом коммерческие банки смогут принимать цифровые рубли в оборот как резервные, обеспечивая их возврат ценными бумагами в ЦБ. Регулирование денежной массы и эмиссии цифровых рублей возьмет на себя сам ЦБ РФ, что станет гарантом обеспеченности платежей и большему внедрению этого вида денег в финансовые процессы как внутри страны, так и за ее рубежом. Таким образом общая ликвидность государства будет зависеть от цифрового рубля, следовательно, будет стремиться к максимуму.

Основными угрозами функционирования цифрового рубля видятся следующие:

- Риски функционирования или разрушение сформировавшейся двухуровневой банковской системы;
- Отток депозитов и риск потери ликвидности коммерческих банков;
- Уход с рынков малых банковских структур и возникновение острой конкуренции коммерческих банков и Центрального банка;
- Возможное увеличение процентных ставок на пользование капиталом;
- Наличие геополитических рисков, ограничивающих возможность внешнего воздействия отечественных банковских организаций;
- Слабое развитие цифровой инфраструктуры в отдельных регионах;
- Низкий уровень финансовой грамотности населения;
- Контроль со стороны государства всех финансовых операций населения;
- Увеличение количества киберпреступности, связанной с цифровыми технологиями.

В декабре текущего года, после многочисленных обсуждений и консультаций, Центральным Банком РФ будет представлена концепция развития цифрового рубля Российской Федерации. Уже сейчас известно, что планируется 4 модели развития, и постепенное внедрение планируется до 2030 года. И общество и бизнес понимают необходимость введения такой формы расчетов, несмотря на возникающие вопросы и недоразумения, Россия, наравне с другими государствами, внедряет цифровые технологии во все сферы жизни.

Список использованных источников:

1. Буркальцева Д.Д., Блажевич О.Г., Жарова А.Р., Бунчук Н.А., Ниязбекова Ш.У., Бекирова С.Э. Финансовая безопасность государства // Крымский федеральный университет имени В.И. Вернадского. Симферополь, 2020.
2. Кисаров И.В. О переходе к цифровому рублю / И.В. Кисаров // Вестник тверского государственного университета. Серия: экономика и управление. – 2021. – № 1 (53). – С. 198-208.
3. Кроливецкая В.Э. Цифровой рубль как новация в денежном обращении России // VI международная научно-практическая конференция "Новеллы права, экономики и управления 2020", Гатчина, 25-26 ноября 2020 года. – С. 461-466.
4. Курьянова И.В., Абибуллаев М.С. Потенциальные риски использования виртуальных валют в современной платежной системе // Экономика строительства и природопользования. 2018. – № 2 (67). – С. 87-97.
5. Норец Н.К. Цифровая безопасность банковской сферы / Н. К. Норец // международная научно-практическая онлайн конференция «Развитие

- Российской экономики и ее финансовая безопасность в условиях современных вызовов и угроз», г. Ростов, 22-23 октября 2020 г. – С. 183-186.
6. Норец Н.К. Цифровое мошенничество в финансовой и банковской сферах / Н.К. Норец // V Международная научно-практическая конференция «Финансово-экономическая безопасность Российской Федерации и ее регионов», г. Симферополь, 29-30 сентября 2020 г. – С. 49-50.
 7. Цифровой рубль: концепция Центрального Банка Российской Федерации. – https://www.cbr.ru/analytics/d_ok/dig_ruble/
 8. Шакер И.Е. Цифровая валюта Центрального банка: трансформация финансовой экосистемы и эволюция видов денег / И. Е. Шакер // Финансы, деньги, инвестиции. – № 3/2018. – (67). – С. 8-17.
 9. Ягупова Е.А. Цифровой рубль в банковской системе России // Финансовые рынки и инвестиционные процессы. сборник трудов по материалам VIII научно-практической конференции с международным участием. – 2021. – С. 168-170.

Due diligence как фактор управления рисками в сделках слияний и поглощений

М.Д. Парфенова

к.э.н., доцент кафедры финансового менеджмента

НИЯУ МИФИ, Москва

E-mail: mdparfenova@mephi.ru

Аннотация: В статье представлены ключевые аспекты проверки и экспертизы потенциальной сделки слияния и поглощения для целей подтверждения и соответствия цены сделки с реальным положением юридического субъекта, являющегося объектом сделки. Дью дилиженс способствует принятию обоснованных решений путем повышения качества информации, доступной лицам, принимающим решения.

Ключевые слова: слияния и поглощения, управление рисками, оценка и анализ, комплексная проверка, юридическая экспертиза.

Due diligence as a risk management factor in M&A transactions

Abstract: The article presents the key aspects of verification and examination of a potential merger and acquisition transaction in order to confirm and compare the transaction price with the actual position of the legal entity that is the subject of the transaction. Due diligence contributes to informed decision-making by improving the quality of information available to decision makers.

Keywords: mergers and acquisitions, risk management, assessment and analysis, due diligence, legal expertise.

Одним из сложных периодов новейшей истории всего мира, в том числе и России, обусловлен возникшей пандемией коронавируса, в результате которой был проверен на прочность и устойчивость бизнес, его гибкость, способность к трансформации и адаптации к текущим реалиям. В этой связи сделки слияний и поглощений (далее М&А) становятся способом проведения таких трансформаций, и особую важность приобретают взвешенные, продуманные инвестиции. Статистика рынка М&А за первое полугодие 2021 года [3] показывает восстановление положительного темпа как в количестве, так и в стоимости сделок (рост на 38% и 16% соответственно) после незначительного их снижения в 2020 году (снижение на 15% и 5% соответственно) [4]. Такая динамика связана с тем,

что совокупность последствий коронавируса на экономику привели к частичному снижению уровня доверия и интереса к бизнесу со стороны потенциальных инвесторов. В условиях экономической неопределенности возникает сложность в определении инвестиционной стоимости активов. Эти обстоятельства обусловили необходимость и значимость предынвестиционного анализа, позволяющего выявить дальнейшие возможности роста бизнеса и экономики. Такой комплексный анализ способствует принятию более обоснованных инвестиционных решений.

Сам по себе процесс *M&A* включает в себя множество этапов и может занимать несколько месяцев и даже лет. Ниже представлены ключевые этапы *M&A*:

1. Определение стратегии приобретения (*M&A strategy*).
2. Определение целей приобретения (*Target screening*).
3. Проведение комплексной проверки и оценки (*Due diligence*).
4. Заключение договора купли-продажи (*Transaction execution*).
5. Процесс интеграции приобретения (*Integration*).

Структурирование сделки происходит в рамках первых двух этапов, когда формируется корпоративная стратегия и оценивается возможность реализации корпоративного видения; определяются потенциальные пути приобретения; определяются стратегии по достижению органического и неорганического роста; определяются цели и расставляются приоритеты.

На следующем этапе проводится *Due diligence* приобретаемых активов/компаний, включающий в себя как минимум юридическую, финансовую и налоговую проверки. Данный этап имеет особое значение в подготовке к реализации сделок *M&A*, поскольку его результаты позволяют выявить возможные риски и угрозы, и впоследствии принять инвестору наиболее взвешенные решения относительно предполагаемой сделки по приобретению. В заключительных этапах принимается решение о том, каким образом будет оформлена сделка купли-продажи, через покупку акций или через покупку активов; затем производится процесс закрытия сделки и последующей интеграцией, слиянием компаний.

Рассмотрим подробнее вопросы комплексной проверки сделок *M&A*. С точки зрения инвестора-покупателя, *Due diligence* позволяет ему удостовериться в своих ожиданиях в отношении сделки и минимизировать потенциальные риски (рис.1). С точки зрения продавца, *Due diligence* может обеспечить с одной стороны доверие покупателя, с другой, тщательная финансовая проверка может фактически показать, что справедливая стоимость компании больше первоначально рассчитанной.

Целостный, комплексный подход сводит к минимуму риски, пробелы и передачу функций и обеспечивает получение прибыли. На первоначальной стадии сделок *M&A* риски высокие (*Approach risk*), ресурсы сосредоточены

на совершении транзакции, а не на интеграции и связанных с ней издержках. Риск передачи (*Handoff risk*) существенно ниже, поскольку сделка совершена, основные транзакционные издержки позади, а издержки на интеграцию еще не сформированы. Риск исполнения (*Execution risk*) становится ниже на заключительном этапе, так как тут возникают только затраты, связанные с интеграцией бизнеса.

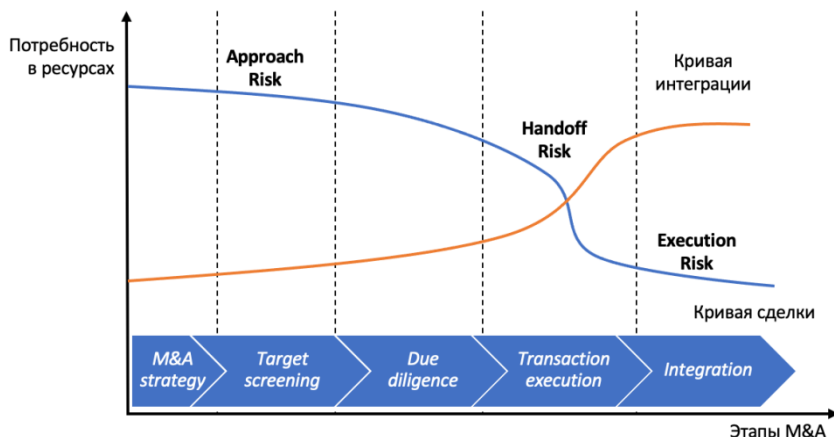


Рисунок 1 — Изменение уровня риска на разных этапах M&A

Типичные вопросы, которые затрагиваются в ходе *Due diligence* можно представить следующим образом:

- своевременное получение синергетического эффекта от сделки M&A;
- неопределенность в отношении заявлений целевого руководства о росте;
- стабильность клиентской базы;
- ускорение закрытия сделки;
- структурирование налогового и бухгалтерского учета;
- структура внутреннего контроля;
- влияние нормативных вопросов на отрасль целевой компании;
- выявление и количественная оценка налоговых рисков и оптимизация связанных с ними льгот;
- вознаграждения сотрудникам, системы информационных технологий и методы управления рисками;
- инспекция цепочки поставок и производственной площадки;
- финансирование и риски, связанные с обязательствами.

Представленные критерии являются как финансовыми, так и нефинансовыми факторами стоимости компании [1]. Таким образом, факторы стоимости определяют цену и структуру сделки, а также определяют характер и объем *Due diligence*. Отсюда следует процесс *Due diligence*, который включает в себя следующие его основные виды: финансовый, операционный, коммерческий, налоговый, кадровый, юридический, стратегический.

1. Операционный *Due diligence*. Заключается в проверке различных объектов, принадлежащих продавцу, и определении того, отражаются ли все операционные расходы в финансовых показателях или нет. Операционный *Due diligence* также дает представление о том, какие эксплуатационные расходы понесет вероятнее всего покупатель при заключении сделки *M&A*.
2. Коммерческий *Due diligence*. Поскольку клиенты являются жизненной силой любого бизнеса, виды *Due diligence* неизменно включают в себя пристальный взгляд на клиентскую базу целевой компании и охватывает анализ следующих нефинансовых факторов стоимости бизнеса [2]:
 - вклад клиентов в выручку компании, выявление «самых крупных клиентов»;
 - текущая кредитная политика компании;
 - оценка удовлетворенности клиентов;
 - список с объяснением причины потери крупных клиентов за последние несколько лет.
3. Налоговый *Due diligence* в отношении налоговых обязательств включает в себя пересмотр всех налогов, которые компания обязана уплатить, и обеспечение их надлежащего расчета без намерения занижения налогов. Ключевые проблемы в области слияний и поглощений:
 - обязательства и условные обязательства;
 - соблюдение налогового законодательства;
 - аудиты и налоговые проверки;
 - налоговые риски;
 - действительность налоговых атрибутов (например, чистые операционные убытки, кредиты на НИОКР);
 - предыдущие ограничения налоговых атрибутов из-за смены владельца.
4. Кадровый *Due diligence*. Заключается в экспертизе человеческого капитала компании: численность персонала, текучесть кадров, средний уровень оплаты труда, производительность труда, показатели обучения и развития персонала [2].

5. Юридический *Due diligence*. Юридическая экспертиза чрезвычайно важна и обычно включает в себя изучение и обзор следующих элементов: устав, протоколы заседаний, собраний акционеров, контракты, лицензионные или франчайзинговые соглашения, кредитные соглашения, договора банковского финансирования и кредитных линий, стороной которых является компания.
6. Стратегический *Due diligence*. Экспертиза в отношении оценки того, насколько хорошо целевая компания вписывается в общий стратегический бизнес-план покупателя. Например, частная инвестиционная фирма, рассматривающая новое приобретение, спросит, насколько хорошо предлагаемая цель дополнит существующий портфель компаний фирмы. Крупная корпорация, рассматривающая возможность сделки по слияниям и поглощениям, оценивает, насколько легко (или насколько сложно) можно успешно объединить целевую компанию в общую корпоративную организацию покупателя.
7. Финансовый *Due diligence*. Финансовая проверка является одной из наиболее важных в M&A и проводится для окончательного принятия решений о сделках, ведения переговоров и, в конечном счете, планирования и исполнения сделки M&A.

В рамках данного исследования, сфокусируемся подробнее на основных направлениях финансовой проверки, направленных на получение представления о бизнесе, операциях, финансовой бухгалтерской отчетности. Проверке подлежат основные финансовые факторы стоимости компании, например, качество доходов и прибыли, инвестированный и оборотный капитал, уровень долговой нагрузки, длительность операционного и финансового циклов [1].

Качество прибыли влияет на прибыль до вычета процентов, износа и амортизации (*EBITDA*) и на прибыль до вычета процентов и налога (*EBIT*), которые обычно напрямую влияют на свободный денежный поток целевой компании и, следовательно, на стоимость сделки. Цели качественного анализа прибыли:

- понять операционные показатели движения денежных средств, включая суммы, доступные для обслуживания долга;
- определить элементы, которые необходимо учитывать при нормализации показателя *EBITDA* компании и на основе полученного результата оценить коэффициент покрытия процентов прибылью и плечо финансового рычага;
- определить на основе исторических показателей прибыли ожидаемый темп его роста в будущем, что необходимо для моделирования будущего денежного потока и оценки стоимости бизнеса.

Другие факторы, которые влияют на качество прибыли, но могут не применяться при нормализации показателя EBITDA, включают помимо финансовых, нефинансовые факторы стоимости компании [1]:

- структура затрат;
- соотношение постоянных затрат к переменным;
- влияние операций в иностранной валюте;
- клиентская составляющая, условия, скидки;
- бонусы и другие единовременные выплаты и пр.

Следующий ключевой компонент, влияющий на свободный денежный поток это оборотный капитал. Тщательный анализ оборотного капитала, особенно в капиталоемких отраслях, может существенно повлиять на результаты финансовой экспертизы. В рамках оценки показателей, определяющих оборотный капитал, рассматриваются не только их абсолютные величины (оборотные активы, кредиторская задолженность), но и относительные. Ключевыми являются такие показатели, как период оборота дебиторской и кредиторской задолженности, соотношение дебиторской и кредиторской задолженности, тип кредитной политики, закупочные цены [1]. При моделировании стоимости целевой компании требуется анализ исторических данных оборотного капитала, оценка влияния сезонности, длительности предоставляемой клиентам отсрочки и получаемой от поставщиков. Ключевым моментом является оценка возможности дальнейшего использования бесплатных источников финансирования (кредиторской задолженности).

Другие области *Due diligence* включают в себя информационные технологии, выпуск ценных бумаг, интеллектуальную собственность, экологическую проверку, исследования и разработки (НИОКР). Проведение *Due diligence* имеет решающее значение для любого успешного приобретения.

Осуществление такой комплексной проверки позволит усовершенствовать модель оценки и структуры сделки M&A, достичь улучшения синергии, разработать дополнительные рычаги воздействия на переговорах, выявить и минимизировать риски.

Список использованных источников:

1. Парфенова М.Д. Разработка методики анализа факторов формирования стоимости промышленной компании: автореф. дис. канд. экон. наук: 08.00.05 / М.Д. Парфенова; НИЯУ МИФИ. – Москва, 2016. – 22 с.
2. Парфенова М.Д. Сбалансированная система финансовых и нефинансовых показателей как инструмент управления стоимостью компании/ М.Д. Парфенова // Финансовая аналитика: проблемы и решения. – 2013. - №33(171). С. 40-49.

3. Рынок слияний и поглощений. Итоги M&A 2020 года [Электронный ресурс] // Информационное агентство АК&М – Режим доступа: <http://mergers.akm.ru/stats/34>, свободный (дата обращения 18.11.2021).
4. Рынок слияний и поглощений. 1 полугодие 2021 года [Электронный ресурс] // Информационное агентство АК&М – Режим доступа: <http://mergers.akm.ru/stats/36>, свободный (дата обращения 18.11.2021).

ESG-трансформация

А.А. Николаев

студент 4 курса НИЯУ МИФИ, Москва

Е.Р. Гордеева

студент 4 курса НИЯУ МИФИ, Москва

E-mail: realtonn@gmail.com

В.Г. Когденко

заведующая кафедрой финансового менеджмента

НИЯУ МИФИ, Москва

E-mail: vgkogdenko@mephi.ru

Аннотация: Мировая экономика активно движется в направлении устойчивого развития с учетом реализации принципов ответственного отношения к окружающей среде (E), высокого уровня социальной ответственности (S) и качества корпоративного управления (G). Глобальные инвесторы активно сокращают объем инвестиций в компании, которые игнорируют устойчивые стратегии. Все больше промышленных, инфраструктурных и социальных проектов, реализуемых бизнесом и государством, оцениваются с точки зрения факторов ESG.

Ключевые слова: экологии, социальная ответственность, корпоративное управление, инвестор, бизнес, инвестиционный продукт.

ESG-transformation

Abstract: The global economy is actively moving towards sustainable development, taking into account the implementation of the principles of responsible attitude to the environment (E), a high level of social responsibility (S) and the quality of corporate governance (G). Global investors are actively reducing the volume of investments in companies that ignore sustainable strategies. More and more industrial, infrastructure and social projects implemented by business and the state are evaluated from the perspective of ESG factors.

Keywords: environment, social, corporate governance, investor, business, investment products.

1. Введение

Вопросы устойчивого развития и борьбы с климатическими изменениями все чаще становятся предметом пристального внимания органов регулирования финансовых рынков и органов исполнительной власти в разных странах. Оценка рисков и возможностей, связанных с изменениями климата, отношением к окружающей среде, взаимоотношениями с обществом в целом и локальными сообществами, соблюдением прав человека и другими вопросами устойчивого развития, становится актуальной глобальной тенденцией и будет определять направления экономической и финансовой повестки в ближайшем будущем. Под “устойчивым развитием” понимается развитие, отвечающее потребностям настоящего времени без ущерба для способности будущих поколений удовлетворять свои собственные потребности. Повестка дня в области устойчивого развития до 2030 года, принятая резолюцией Генеральной Ассамблеи Организации Объединенных Наций 25 сентября 2015 года, и Парижское соглашение от 12 декабря 2015 года, принятое 21-й сессией Конференции Сторон Рамочной конвенции Организации Объединенных Наций об изменении климата и подписанное от имени Российской Федерации в г. Нью-Йорке 22 апреля 2016 года (далее — Парижское соглашение по климату), создали юридическую и идеологическую основу для нового глобального перераспределения потоков капитала в пользу рынков, обеспечивающих продвижение целей устойчивого развития. Повышению эффективности такого перераспределения потоков капитала способствуют разработанные заинтересованными международными организациями рекомендации, методологические руководства и стандарты для участников финансовых рынков, направленные на повышение прозрачности компаний и доступности информации нефинансового характера, связанной с их деятельностью. [6]

2. Новый мировой стандарт ESG-раскрытий.

На сегодняшний день в мире создано достаточно стандартов отчетности, не являющейся “традиционной” финансовой. Однако, CFA Institute - глобальная ассоциация профессиональных инвесторов - проводит сегодня консультации в преддверии написания ещё одного добровольного стандарта.

Стандарт предназначен для оценки инвестиционных продуктов, обладающих характеристиками “ESG” - то есть имеющих отношение к социальной ответственности, экологии или корпоративному управлению.

Целью создания стандарта является обеспечение инвесторов информацией, на основе которой они смогут лучше понимать

характеристики предлагаемых им инвестиционных продуктов и сравнивать их между собой.

3. Методологический центр по финансовым инструментам устойчивого развития.

ВЭБ.РФ – национальный институт развития, главная задача которого – обеспечение роста российской экономики и улучшение качества жизни людей. В диалоге с министерствами, ведомствами, Банком России, экспертным и бизнес-сообществом ВЭБ.РФ ведёт разработку национальной системы зелёного финансирования. Она должна помочь российским компаниям заимствовать средства для реализации зелёных проектов на более выгодных условиях.

Распоряжением Правительства Российской Федерации №3024-р от 18 ноября 2020 года ВЭБ.РФ был определён в качестве методологического центра по финансовым инструментам устойчивого развития. Основой разработанной ВЭБ.РФ в этом статусе системы зеленого финансирования являются таксономия зеленых проектов и стандарт зеленого финансирования (критерии проектов устойчивого развития и требования к системе верификации), утвержденные Постановлением Правительства Российской Федерации №1587 от 21 сентября 2021 года. При разработке таксономии и стандарта учтены национальные приоритеты и ведущие международные практики (ICMA, CBI, IDFC, Европейский Союз) и национальные приоритеты. [4]

4. Рынок ESG-инструментов.

На текущий момент российский рынок составляет всего 2 млрд долларов, тогда как международный перевалил отметку в 1 трлн долларов. По целевому использованию лидером является чистый транспорт (76%), а также расширение социально-экономических возможностей населения (15%). В то время как в структуре зарубежных размещений 2020 года целевое использование крайне разнообразно: 15% пришлось на возобновляемые источники энергии, 12% – на зеленые здания, по 10% – на доступ к базовой инфраструктуре и чистый транспорт, 9% – на расходы на борьбу с COVID-19 и прочее.

Таблица 1 – Российские объемы устойчивого финансирования
пока незаметны в мировом объеме

Зеленые облигации, млрд долл.		Социальные облигации, млрд долл.	
США	61,4	Франция	49,6
Германия	41,3	США	10,3
Франция	37,0	Япония	8,3
Китай	15,7	Корея	7,7
Нидерланды	15,0	Нидерланды	4,5
...		...	
Россия	2,4	Россия	0,4

На сегодняшний день рынок эмитентов облигаций определяется несколькими компаниями, однако мы видим высокий интерес со стороны крупных корпораций, у которых уже есть ESG-рейтинги. [3]

5. Компании, занимающие лидирующие позиции в ESG-рейтинге Raex.

ESG — это ряд критериев, которыми можно оценить, как деятельность конкретной компании влияет на общество и окружающую среду.

В 2000 году вступил в силу Глобальный договор ООН — самая масштабная инициатива, объединившая, по данным за 2017 год, более девяти тысяч компаний из 166 стран мира. Его целью было сформулировать принципы социально-корпоративной ответственности, которых бы придерживались все прогрессивные компании мира.

На 2021 год только 62 российские организации являются участниками этого договора. Среди них:

– Компания: «Энел Россия» (российская энергетическая компания. Обеспечивает электро- и теплоснабжение посредством ГРЭС и ветропарков).

ESG-деятельность: В «Энел Россия» команда по устойчивому развитию существует с апреля 2015 года, она была трансформирована из группы по корпоративной социальной ответственности.

В 2020 году мажоритарный акционер компании Группа Enel заявила, что планирует вложить €70 млрд в усиление своего присутствия на рынке

возобновляемой энергетики во всем мире до 2030 года. В мае 2021 года «Энел Россия» ввела в эксплуатацию Азовскую ВЭС — свой первый коммерческий проект, производящий «зеленую» энергию.



Рисунок 1 – Азовская ВЭС

– Компания: «Росатом» (российская государственная компания, работающая с атомными технологиями в различных отраслях).

ESG-деятельность: «Росатом» присоединился к Глобальному договору ООН в 2020 году. В качестве приоритетных целей устойчивого развития компания заявляет:

- а) недорогую и чистую энергию;
- б) достойную работу и экономический рост;
- в) индустриализацию, инновации и инфраструктуру;
- г) ответственное потребление и производство;
- д) борьбу с изменениями климата;
- е) партнерство в интересах устойчивого развития.

За счет того, что атомная энергетика является низкоуглеродной, она способствует снижению «парникового эффекта». Компания работает с направлениями, затрагивающими ядерную медицину, ядерную науку, ветроэнергетику и технологии послыонного наращивания и синтеза продуктов (к примеру, 3D-печать).

– Компания: «Северсталь» (металлургическая компания, ведущая сталелитейную и горнодобывающую деятельность).

ESG-деятельность: «Северсталь» — участник Глобального договора ООН с 2018 года.

Цели по природоохранной деятельности на 2018-2025 годы:

- снизить массу сброса загрязняющих веществ в водные объекты на 12%;

- сократить массу размещаемых отходов на 20%;
- достигнуть снижения выбросов в атмосферу загрязняющих веществ на 13%.

Также «Северсталь» рассчитывает снизить удельные выбросы парниковых газов на 3% до 2023 года и на 10% до 2030-го.

– Компания: «Газпром» (один из лидеров России по разведке и разработке месторождений нефти и газа, нефтепереработке, а также производству и сбыту нефтепродуктов).

ESG-деятельность: «Газпром нефть» входит в Глобальный договор ООН с 2020 года. За 2020 год компании удалось достичь следующих показателей в области ESG:

- а) снижение количества выбросов парниковых газов на 12%;
- б) 44 водоочистительные установки;
- в) на 22% сократилось количество образуемых отходов за 2017-2020 годы.

За 2020 год «Газпром» инвестировал более 49 млрд руб. в охрану окружающей среды. Для добычи ископаемых в Печорском море была разработана отдельная программа, благодаря которой в море не сбрасывают отходы производства, а также предусматривается контроль за фауной и флорой районов деятельности компании и восполнение биоресурсов (таких, как редкие виды рыб).

– Компания: МКБ (российский коммерческий банк)

ESG-деятельность: Рабочая группа по устойчивому развитию в МКБ была создана в 2019 году. Компания избрала для себя шесть целей устойчивого развития, которые интегрирует в свою глобальную стратегию. Среди них:

- а) хорошее здоровье и благополучие;
- б) качественное образование;
- в) достойная работа и экономический рост;
- г) индустриализация, инновации и инфраструктура;
- д) ответственное потребление и производство;
- е) партнерство в интересах устойчивого развития.

В 2019 году в МКБ был запущен проект цифровизации бизнеса, цель которого — снижение влияния деятельности банка на окружающую среду.

Компания рассчитывает до 2023 года сделать 95% розничных сервисов доступными онлайн, 75% кредитных сделок заключать в электронном формате, а также на 15% ежегодно снижать количество нецифровых сервисов.

Банк разработал стратегию в области устойчивого развития на 2021-2023 годы, в рамках которой планирует перевести три крупнейших офиса под стандарты «зеленых» и внедрить практику раздельного сбора мусора в

отделениях Москвы, МО и Санкт-Петербурга, а также отказаться от использования одноразовой пластиковой посуды во всех офисах и сократить потребление воды на 36%, а потребление электричества — на 30% в собственных зданиях компании.

Также МКБ рассчитывает начать утилизировать 100% макулатуры в трех регионах присутствия, а объем закупаемой бумаги сократить на 30% (относительно показателей 2019 года).

МКБ собирается выделить не менее 100 млрд руб. на реализацию проектов устойчивого развития.

– Компания: «Норникель» (горно-металлургическая компания, крупнейший в мире производитель никеля).

ESG-деятельность: «Норникель» присоединился к Глобальному договору ООН в 2016 году. Компания избрала для себя шесть целей устойчивого развития, которые интегрирует в свою глобальную стратегию. Среди них:

- а) хорошее здоровье и благополучие;
- б) достойная работа и экономический рост;
- в) индустриализация, инновации и инфраструктура;
- г) устойчивые города и населенные пункты;
- д) ответственное потребление и производство;
- е) борьба с изменением климата.

По каждой из целей компания ведет отчетность. Так, в социальном аспекте ESG за 2020 год «Норникель» предоставила 72,8 тысячам своих сотрудников ДМС, \$219 млн было выделено на развитие энергетической инфраструктуры.

На 3% удалось снизить выбросы парниковых газов, 86% воды используется повторно, а доля возобновляемой энергии от потребления составила 46%.

Компания разработала «Серную программу», за счет которой планирует сократить выбросы диоксида серы в Норильске и Красноярском крае на 90% к 2025 году. На нее в общей сложности выделяют \$4,3 млрд.

В долгосрочных целях «Норникеля» — нулевая смертность на производстве и ежегодное снижение коэффициента травматизма с потерей рабочего времени на 15%. С 2013 года частота несчастных случаев сократилась на 54%, а показатели коэффициента травматизма уменьшились на 57%.

– Компания: «Сбер» (крупнейший в России универсальный банк).

ESG-деятельность: Направления действий «Сбера» в рамках экологической политики:

- а) сокращение объема отходов и потребляемых ресурсов;
- б) повышение энергоэффективности;

- в) финансирование проектов в области возобновляемой энергетики;
- г) разработка стратегии в области ответственного финансирования.

Цифровизация всех сфер банка позволяет ежегодно сокращать бумажный документооборот на 30% — в 2020 году количество бумаги, которая передается на хранение в архив и выдается клиентам, сократилось на 3,7 тыс. тонн. В компании работают над сокращением потребления воды и электричества — за пять лет удалось уменьшить количество потребляемой электроэнергии на 20%. К сентябрю 2021 года уже 27 офисов банка полностью перешли на возобновляемые источники энергии, а экономия энергоресурсов за 9 месяцев 2021 года составила 175 млн руб.

«Сбер» финансирует проекты в области возобновляемой энергетики. Так, банк инвестировал в Самарскую солнечную электростанцию, ВЭС в Ростовской области и предоставил кредит «Энел Россия» на строительство Кольской ВЭС. [2]

6. Заключение.

Крупнейшие инвестиционные институты и банки быстро осознали, что зеленая повестка станет на долгие годы основным драйвером не только бюджетных вливаний, но и экономики в целом. В результате этого высокий ESG-рейтинг стал своеобразным пропуском для реального бизнеса к главному источнику дешевых финансовых ресурсов на рынке. А это, в свою очередь, привело к тому, что соблюдение принципов ESG стало одним из важных обычаев деловой практики для самого широкого круга предпринимателей.

Список использованных источников:

1. Резолюция, принятая Генеральной Ассамблеей 25 сентября 2015 года: [Электронный ресурс]. URL: https://unctad.org/system/files/official-document/ares70d1_ru.pdf (Дата обращения: 01.11.2021).
2. Компания RB.RU: [Электронный ресурс]. URL: <https://rb.ru/list/esg-specialisti/>. (Дата обращения: 01.11.2021).
3. Рейтинговое агентство «Эксперт РА»: [Электронный ресурс]. URL: https://raexpert.ru/researches/sus_dev/esg2021/#part2. (Дата обращения: 01.11.2021).
4. Государственная корпорация развития «ВЭБ.РФ»: [Электронный ресурс]. URL: <https://veb.ru/ustojchivoe-razvitie/zeljonoe-finansirovanie/>. (Дата обращения: 01.11.2021).
5. «Новый мировой порядок ESG-раскрытий»: [Электронный ресурс]. URL: https://gaap.ru/articles/Novyy_mirovoy_standart_ESG_raskrytiy/. (Дата обращения: 01.11.2021).

6. Рекомендации по раскрытию публичными акционерными обществами нефинансовой информации, связанной с деятельностью таких обществ. Публичным акционерным обществам от 12.07.2021 № ИН-06-28/49: [Электронный ресурс].
URL: https://cbr.ru/StaticHtml/File/117620/20210712_in-06-28_49.pdf. (Дата обращения: 01.11.2021).