МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Национальный исследовательский ядерный университет
«МИФИ»

Материалы
IV Международной научно-практической конференции

«Цифровая экономика в контексте национальной безопасности»

14 декабря 2021 г., Москва

Москва 2022

УДК 330.47:[007+004.9](06)
ББК 65.012
М43

Материалы IV Международной научно-практической конференции «Цифровая экономика в контексте национальной безопасности», 14 декабря 2021 г., Москва. М.: НИЯУ МИФИ, 2022. - 145 с.

В сборнике рассматриваются научные исследования и имеющиеся практики касаемо тем цифрового общества, цифровой безопасности, цифровых технологий, активно внедряемых в современном мире и используемых в образовании и карьере, цифровых финансов, регулирования правовых аспектов, образовательной реформы и защиты информационных потоков.

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

Материалы издаются в авторской редакции
Получены до 14.12.2021

ISBN 978-5-7262-2848-8

Подписано в печать 09.02.2022. Формат 60x84 1/16.
Печ. л. 9.
Национальный исследовательский ядерный университет «МИФИ»
115409, Москва, Каширское ш., 31

Содержание

УДК 005.934:004:330.4

Вопросы обеспечения экономической безопасности в условиях цифровизации экономики

Ф.А. Хамидова
к.э.н., доцент кафедры международных финансов-кредита ТФИ,
Ташкент, Узбекистан
E-mail: faridaxon.xamidova@mail.ru

Аннотация*: в статье изучен вопрос развития потребности в обеспечении экономической безопасности, также пути обеспечения экономической безопасности в Узбекистане изучены в разрезе направлений экономической безопасности на основе статистических и общедоступных данных по республике.*

Ключевые слова: *экономическая безопасность, продовольственная безопасность, энергетическая безопасность, финансовая безопасность, кадровая безопасность, инновационная безопасность, инвестиционная безопасность, внешнеэкономическая безопасность.*

Issues of ensuring economic security in the conditions of digitization of the economy

Abstract: *the article studies the issue of the development of the need to ensure economic security and the ways of ensuring economic security in Uzbekistan are studied in the context of areas of economic security on the basis of statistical and publicly available data on the republic.*

Keywords: *economic security, threats, national security, food security, energy security, financial security, personnel security, innovative security, investment security, foreign economic security.*

В современных условиях, где рост значения цифровых технологий в экономике ускоряет процессы углубления рыночных отношений, процессов глобализации и интеграции. Цифровая экономика — это новая современная форма хозяйствования, в которой основным фактором производства и управления выступает совокупность больших данных в цифровой форме и процесс их обработки. Практическое применение полученных результатов, в свою очередь позволяет добиться гораздо большей эффективности по сравнению с традиционными формами хозяйствования.

В условиях все более углубления рыночных отношений и цифровизации экономики, обеспечение экономической безопасности приобретает все более объективное значение.

Сущность экономической безопасности можно определить, как такое состояние экономики и институтов власти, при котором обеспечивается гарантированная защита национальных интересов, социально направленное развитие страны, достаточный экономический и оборонный потенциал даже при неблагоприятных условиях развития внутренних и внешних процессов. Экономическая безопасность представляет собой такое состояние экономики, которое позволяет удовлетворить всю совокупность экономических потребностей общества, обеспечивает его независимость, стабильное и устойчивое развитие, прогресс, достойное положение в мировой экономике, надежную защищенность от внутренних и внешних угроз, не позволяющую скатываться за критический предел. Экономическая безопасность также определяется как совокупность условий и факторов, обеспечивающих независимость национальной экономики, ее стабильность и устойчивость, способность к обновлению и совершенствованию.

Для изучения современного состояния экономической безопасности в Узбекистане, прежде всего, необходимо разделить экономическую безопасность на группы, на основе которых можно изучать и делать выводы, опираясь на конкретные факты.

Рисунок 1 – Направления экономической безопасности (источник: Разработано авторами на основании анализа зарубежной литературы)

Следуя данному направлению проанализируем текущую ситуацию в Узбекистане в разрезе приведенных выше направлений экономической безопасности.

1. Продовольственная безопасность

Продовольственная безопасность означает достижение достаточного снабжения населения страны основными продуктами питания, снижение зависимости от импортных продуктов с использованием внутренних возможностей.

По данным ООН, в настоящее время в мире голодают 815 миллионов человек, а к 2050 году это число достигнет 2 млрд. 12,9% из них проживают в развивающихся странах. Сорок пять процентов смертей среди детей в возрасте до пяти лет вызваны недоеданием. Сегодня по этой причине ежегодно умирает 3,1 ребенка [1].

Следует отметить, что, когда речь заходит о продовольственной безопасности, первое, что приходит на ум – сельское хозяйство. Аграрный сектор является основным поставщиком основных продуктов для всего населения земли, которые являются источником жизни для всех без исключения.

После обретения Узбекистаном независимости для обеспечения пищевой безопасности осуществлены меры в двух направлениях:

1. Расширение площадей личных подсобных хозяйств сельского населения и выделение новых земель под огороды.
2. Пересмотр структуры сельскохозяйственных культур.

В 2019 году доля сельского, лесного и рыбного хозяйства в ВВП страны составила 28,1%. Доля населения, занятого в сельском, лесном и рыбном хозяйстве составила 26%.

В целом за 2017–2019 годы валовая продукция сельского хозяйства увеличилась в 1,5 раза, а на душу населения – в 1,4 раза (в ценах 2019 года). При этом производство сельхозпродукции увеличилось в 1,3 раза, животноводства – в 1,7 раза [2]. На сегодняшний день проведен ряд реформ по обеспечению продовольственной безопасности населения страны, в результате которых ни одна сельскохозяйственная продукция не стала дефицитной на местных рынках.

«Стратегию развития сельского хозяйства Республики Узбекистан на 2020–2030 годы» можно назвать правовой основой будущей работы по обеспечению продовольственной безопасности. Этот документ определяет порядок, в котором вопросы продовольственной безопасности населения Узбекистана будут рассматриваться в ближайшие годы.

2. Энергетическая безопасность

В то же время энергетический сектор достиг уровня, который играет более решающую роль в развитии экономики, чем другие ее составляющие. Следовательно, определение вклада энергетического фактора в экономическую безопасность имеет решающее значение для анализа экономической безопасности. Обеспечение энергетической безопасности

становится одной из основных задач по созданию условий для нормального функционирования всех секторов экономики.

На сегодняшний день на базе АО «Узбекэнерго» образовано три акционерных общества: «Иссиқлик электр станциялари», «Узбекистон миллий электр тармоклари» и «Худудий электр тармоклари». Цель подобной реорганизации – переход на современные методы выработки, транспортировки, распределения и продажи электроэнергии.

По оценкам экспертов, сегодня у каждого домохозяйства есть возможность сэкономить в среднем 400 кВтч электроэнергии в год. Если каждая семья сэкономит 400 кВтч электроэнергии, то количество сэкономленной электроэнергии в стране составит 1,8 миллиарда. кВтч. Сэкономленной таким образом электроэнергии, например, хватит для снабжения электроэнергией Джизакской или Сырдарьинской областей в течение всего года.

На сегодняшний день в сфере электроэнергетики производственная мощность республики превысила 14,1 тысяч МВт.

Основная часть или 85,8% данных производственных мощностей приходится на долю теплоэлектростанций. К 2030 году общая электрическая нагрузка в часы максимального потребления увеличилась с 11 000 МВт в осенне-зимний период 2018–2019 гг. до 20 000 МВт. Таким образом, к 2030 году страна должна будет увеличить свою энергоемкость почти в 1,8 раза [3].

3. Финансовая безопасность

Финансовая безопасность служит гарантией независимой финансово-экономической политики страны. Финансовая безопасность находит свое отражение в предотвращении значительного оттока капитала за границу, предотвращении конфликтов по поводу распределения ресурсов национальной бюджетной системы между разными уровнями власти, ослаблении влияния глобальных кризисов, обеспечении стабильности финансово-экономических параметров. Финансовая безопасность также предусматривает профилактику финансовой преступности.

По мнению некоторых авторов, финансовая безопасность страны – это:

- защита финансовых интересов субъектов финансовых отношений на всех уровнях;
- обеспечение национальной экономики и ее секторов ликвидными активами для удовлетворения спроса на финансовые ресурсы и выполнения соответствующих обязательств;
- состояние стабильности и устойчивости финансовой системы к негативным влияниям;

– совокупность финансовых возможностей для эффективной организации национальной экономической системы и обеспечения устойчивого экономического роста.

Снижение уровня инфляции, достижение стабильности банковской системы, вывод финансового рынка, в частности, рынка капитала, на наиболее развитый рыночный уровень, развитие пенсионного обеспечения, страхования, борьба с экономической преступностью и ряд других финансовых направлений является основой обеспечения финансовой безопасности. В последние годы в Узбекистане был проведен ряд реформ в этих областях, государство регулярно рассматривает вопросы финансовой безопасности. В частности, необходимо признать и подчеркнуть вопросы либерализации валютного рынка в последние годы, радикальные изменения в банковской системе, полную реорганизацию рынка капитала, переход к системе инфляционного таргетирования.

4. Кадровая безопасность

Кадровая безопасность – это обеспечение экономической безопасности предприятия за счет снижения рисков и угроз, связанных с некачественной работой сотрудников, их интеллектуальным потенциалом и трудовыми отношениями в целом, при этом кадровая безопасность обеспечивается за счет привлечения высококвалифицированных и надежных сотрудников. Сегодня интерес к государственной службе растет как никогда, и важно серьезно рассматривать вопросы кадровой безопасности. Особенно в контексте пандемии коронавируса, которая обострилась в 2020 году, кадровая безопасность стала важным вопросом.

Действительно, в период пандемии желание работать в государственном секторе значительно возросло среди населения, занятого в частном секторе. Прежде всего, это выражается в том, что в период изоляции госслужащие получали полную поддержку со стороны своих организаций, а частный сектор, наоборот, выжил, сократив множество рабочих мест.

Кризис в экономике и на рынке труда, вызванный пандемией COVID-19, может привести к росту мировой безработицы почти на 25 миллионов чело век. Сокращение занятости также означает огромную потерю доходов для сотрудников. По оценке Международной организации труда, к концу 2020 года потери составят от 860 млрд. долларов до 3,4 трлн. долларов США. Это приводит к снижению потребления товаров и услуг, что, в свою очередь, отрицательно сказывается на экономических перспективах предприятий и целых стран [5].

Ежегодно рынок труда Узбекистана пополняют 600–700 тысяч человек, а количество создаваемых рабочих мест достигает 500 тысяч. В результате количество безработных ежегодно увеличивается на 200 000

человек. По данным Министерства занятости и трудовых отношений Республики Узбекистан, общая численность рабочей силы в стране (мужчины в возрасте 16–59 лет и женщины в возрасте 15–54 лет) составляет 19 миллионов человек. Из них 5,1 миллиона работают неформально и около двух миллионов – за границей [6].

В целях обеспечения безопасности сотрудников в Республике Узбекистан, прежде всего, для работы в государственном секторе, для повышения престижа государственной гражданской службы на всех уровнях, особенно среди молодежи, для устранения предпосылок коррупции, волокиты и бюрократии 3 октября 2019 года принят Указ Президента Республики Узбекистан «О мерах по кардинальному совершенствованию кадровой политики и системы государственной гражданской службы в Республике Узбекистан». Данным документом было создано Агентство развития государственной службы, и безопасность государственных служащих была полностью определена как его непосредственная функция.

5. Инновационная безопасность

До сего времени анализ сущности инноваций показывает, что при переходе на инновационный путь развития серьезные изменения произойдут не только в экономике и ее составляющих, но и в развитии личности, мировоззрения, в психологии, политике, социально-экономической, научно-технической, образовательной и культурной сферах. Для решения этих многогранных проблем, возникающих в процессе формирования инновационной экономики, ее безопасного развития возникает объективная необходимость в новом направлении в системе экономической безопасности – инновационной безопасности.

Инновационная безопасность – это совокупность условий и инновационных факторов, обеспечивающих независимость национальной экономики, ее инновационное развитие, способность постоянно вводить новшества и развиваться, добиваться стабильности и международной конкурентоспособности [7].

Инновационная безопасность является элементом инновационной экономики (развития) страны и оценивается на международном уровне с помощью Глобального инновационного индекса (GII).

После пятилетнего перерыва в рейтинге GII- 2020 Узбекистан получил рейтинг по 65 показателям и занял 93-е место из 131 страны (Швейцария 1-е, Швеция 2-е, США 3-е, Россия 47-е, Казахстан 77-е, Кыргызстан 94-е и Таджикистан – 109-е место).

Возвращение Узбекистана в рейтинг GII на 29 позиций выше по сравнению с пятилетней давностью, является первым результатом позитивных изменений в реформах, в частности, в политике прозрачности

и открытости, а также в инновациях. В рейтинге GII 2020, включающем 80 показателей, Узбекистан занимает 81-е место в мире по количеству инновационных ресурсов, то есть 95-е место в субиндексеинституциональных затрат, 77-е место по человеческому капиталу и исследованиям, 72-е место по инфраструктуре и 90-е место по. эффективности знаний и технологий.

В рейтинге GII-2020 страна входит в ТОП-10 стран по следующим субпоказателям: легкость открытия бизнеса – 8 место, выпускники научных и инженерных специальностей – 7 место и валовое накопление капитала – 8 место. При этом наша страна заняла 12–45 места по еще 8 важным показателям.

Кроме того, Узбекистан по-прежнему имеет низкий рейтинг GII по следующим показателям: качество законодательства – 127 место, верховенство закона – 124 место, экспорт ИКТ-услуг – 129 место, валовые затраты на исследования и разработки, финансируемые из-за рубежа – 96 место [8].

6. Инвестиционная безопасность

Инвестиционная безопасность – это способность органов государственной власти напрямую влиять на инвестиционные процессы, происходящие в стране в рамках существующей правовой базы, которая определяет конкурентоспособность и устойчивый рост национальной экономической системы.

В последние годы, как и во всех сферах, инвестиционная деятельность Узбекистана претерпела значительные позитивные изменения и реформы.

В частности, подписание Президентом Республики Узбекистан Закона «Об инвестициях и инвестиционной деятельности» от 25 декабря 2019 года стало самой важной реформой среди проводимых преобразований. Именно на основании этого закона регулируется инвестиционная деятельность в Узбекистане, защищаются права иностранных инвесторов.

В 2019 году объем инвестиционного развития за счет всех источников финансирования достиг 220,7 трлн. сумов, что в 2 раза превышает утвержденный годовой прогноз. Объем инвестиций в основной капитал составил 189,9 трлн. сумов, обеспечены темпы роста в 1,3 раза выше, чем за аналогичный период 2018 года.

Значительный рост инвестиционной активности обусловлен притоком капитала иностранных инвестиций и кредитов на сумму 13,3 млрд. долларов США, в том числе:

- прямые иностранные инвестиции – 9,3 млрд долларов (в том числе инвестиции в основной капитал – 6,6 млрд долларов США);

– средства международных финансовых институтов – 4,0 миллиарда долларов. (в том числе инвестиции в основной капитал – 3,2 млрд. долларов США) [9].

Несмотря на значительное улучшение позиций Республики.

7. Внешнеэкономическая безопасность

Внешнеэкономическая безопасность – это состояние экономической системы, которое воплощает жизненно важные экономические интересы страны, защищает внутреннюю экономическую деятельность от внешних угроз, создает условия для оптимальной интеграции экономики между народное разделение труда и обеспечивает баланс экономических интересов во внешнеэкономической деятельности. Иными словами, внешнеэкономическая безопасность – это комплекс мер различного уровня (макро- и микроэкономического, политического, социального, личного и др.), направленных на защиту внутренней экономики, а также рациональное осуществление внешнеэкономической интеграции.

В условиях нестабильности мировой экономики главным интересом внешнеэкономической безопасности является сохранение и укрепление позиций страны в мировой экономической системе. Внешнеэкономическая безопасность страны обычно оценивается показателями внешнеэкономической деятельности. По итогам января-июня 2020 года внешнеторговый оборот (ВТО) страны составил 15 855,8 млн. долларов США и снизился на 528,0 млн долларов США или на 18,2% по срав нению с соответствующим периодом 2019 года.

Экспорт ВТО снизился на 6 285,4 млн. долларов США (на 22,6%), а объем импорта составил 9 570,4 млн. долл. США (снижение на 15,0%). За отчетный период отмечен пассивный внешнеторговый баланс – 3 285,0 млн. долларов США.

Несмотря на принимаемые в нашей стране меры по поддержке внешней торговли и дальнейшему укреплению сотрудничества со странами СНГ в этой сфере, в январе-июне 2020 года доля стран СНГ во внешнеторговом обороте составила 34,4% и снизилась на 3,8% по сравнению с 2018 годом. ВТО других зарубежных стран в январе-июне 2020 года увеличился на 3,8% по сравнению с аналогичным периодом 2018 года, и их доля в общем объеме ВТО составила 65,6% [8].

Углубленный анализ данных, представленных в разделе о тенденциях экономической безопасности выше, не проводился. Однако мы считаем, что предоставленной информации достаточно, чтобы понять, какие меры принимаются для обеспечения экономической безопасности в Узбекистане.

Следует отметить, что вопросы экономической безопасности и ее обеспечения в Узбекистане, ограничивая ее уровень до уровня

оптимальных показателей, до сих пор не обоснованы никаким законодательным актом. Итак, если мы хотим, чтобы Узбекистан достиг высоких результатов во всех рейтингах мирового сообщества, государство должно разработать нормативно-правовые акты об экономической безопасности нашей страны и внедрить их на практике в нашей стране.

Также предлагается разработать «Стратегию обеспечения и повышения уровня экономической безопасности страны», которая включает следующие аспекты, непосредственно влияющие на достижение и поддержание наиболее эффективного уровня экономической безопасности:

- укрепление экономического суверенитета Республики Узбекистан;
- повышение устойчивости экономики под воздействием внешних и внутренних проблем и угроз;
- обеспечение экономического роста;
- доведение научно-технического потенциала экономического развития до мирового уровня и повышение его конкурентоспособности;
- повышение уровня и качества жизни населения.

Предлагается, чтобы государственная политика в области обеспечения экономической безопасности состояла из следующих основных направлений:

- развитие государственного управления, экономического прогнозирования и стратегического планирования;
- обеспечение стабильного роста реального сектора экономики;
- создание экономических условий для развития и внедрения современных технологий, стимулирования инновационного развития, а также совершенствование нормативно-правовой базы в этой сфере;
- устойчивое развитие национальной финансовой системы;
- региональное развитие Узбекистана, укрепление единства его экономического пространства;
- повышение эффективности внешнеэкономического сотрудничества и реализация конкурентных преимуществ экспортно-ориентированных секторов экономики;
- обеспечение безопасности экономической деятельности;
- развитие человеческого потенциала.

Словом, только в результате обеспечения экономической безопасности и его эффективного мониторинга мы сможем увидеть Узбекистан на вершине международных рейтингов в мировом сообществе.

В заключении подчеркивается, что обеспечение экономической безопасности в процессе формирования цифровой экономики является

одной из неотложных задач на сегодняшний день. Ведь путем обеспечения экономической безопасности можно добиться повышения конкурентоспособности национальной экономики, достижения устойчивого экономического роста и, в конечном счете, обеспечения национальной безопасности страны.

Список использованных источников:

1. Международная экономическая безопасность. Отчет Генерального секретаря ООН. 1987 год. 4-5 страницы. [Электронный ресурс]. URL:https://digitallibrary.un.org/record/ 63732/files
2. Михайленко А. Механизм обеспечения экономической безопасности России// Мировая экономика и международные отношения. - 1996, № 7. - С. 119-127.
3. Министерство энергетики: Цели, задачи, планы и достижения. [Электронный ресурс] URL: http:// minenergy.uz/uz/lists/view/10
4. Слюнина, В.А. Социально-экономическая безопасность региона в условиях инновационного развития [Электронный ресурс] / В.А. Слюнина // Экономика и менеджмент инновационных технологий. 2012. – № 5. – URL: http://ekonomika.snauka.ru/2012/05/763
5. Рынок труда в Узбекистане: как COVID-19 открыл новые возможности. [Электронный ресурс] https:// uz.sputniknews.ru/ economy/20200926/15060208/Rynok-truda-v-zbekistane-kak-C0VlD-19-otkryl-novye-vozmozhnosti.html
6. Отчет Международной Организации Труда. [Электронный ресурс] https://www.ilo.org/moscow/ news/ WCMS_739003/lang-ru/index.htm
7. Сакович В.А. Инновационная безопасность: основные понятия, сущность. - Наука и техника. Т. 15, № 2 (2016).
8. Статистика Министерства инвестиций и внешней торговли Республики Узбекистан. [Электронный ресурс] https://mift.uz/ru/ investment-statistics
9. Данные Государственного комитета по статистике Республики Узбекистан. Внешнеэкономическая деятельность, 2020 год.

УДК 004.056.53:005.52

Исследование сетевой атаки на объект информационной системы

К.В. Куклев
студент 2 курса магистратуры НИЯУ МИФИ, Москва
E-mail: kuklevkv@gmail.com
В. Давыденко
старший преподаватель кафедры «Финансовый мониторинг»
НИЯУ МИФИ, Москва
E-mail: VIDavydenko@mephi.ru
В.А. Рычков
старший преподаватель кафедры «Финансовый мониторинг»
НИЯУ МИФИ, Москва
E-mail: VArychkov@mephi.ru

Аннотация: *в данной статье рассмотрены сетевые атаки: SMURF, DNS с усилием, TCP Reset. Экспертами относятся данные атаки к наиболее опасным атаки, поскольку эти атаки имеют эффект усилия и наиболее губительными для информационной системы.*

Ключевые слова: *атака, угроза, DoS-атака, эффект усиления, система, запрос, широковещательная рассылка, протокол, ICMP ECHO пакет, DDoS-атака, DNS-атака с усилием.*

Investigation of a network attack on an information system object

Abstract: *this article discusses network attacks: SMURF, DNS with effort, TCP Reset. Experts consider these attacks to be the most dangerous attacks, since these attacks have the effect of effort and are the most disastrous for the information system.*

Keywords: *attack, threat, Dos attack, amplification effect, system, request, broadcast, protocol, ICMP ECHO packet, DDoS attack, DNS attack with effort.*

Введение

Наибольшей процент компаний сегодня используют гигантские возможности, которые дает интернет. Однако надо заметить, что вместе с возможностями всемирная сеть приносит большое количество угроз информационной безопасности. Реализация данных угроз может привести к высокому материальному и репутационному ущербу для бизнеса.

Технические характеристики и уровень уязвимости критически важных данных в сетях делают защиту этих данных не простой задачей. Новые вторжения в системы промышленных процессов, работающие в инфраструктуре, вызвали необходимость в разработке более совершенных стратегий, предназначенных для обнаружения этих типов угроз без нарушения работы инфраструктуры.

Гибридная архитектура

Наибольшее количество инфраструктур основано на гибридных инфраструктурах, объединяющих все классические ИТ-сети и промышленные ОТ-сети, управляющие компонентами, взаимодействующими с физическими объектами.

Изоляция от интернета

Этот раздел требует большего внимания, так как растущая тенденция совместимости между типами инфраструктуры также увеличивает количество доступных векторов атак. Системы управления такими инфраструктурами обычно изолированы от Интернета и связаны внутри внутренней сети.

SCADA

Есть еще эти системы управления SCADA, они видны и даже доступны через интернет. В большом количестве этих систем отсутствуют такие системы, как управление критической инфраструктурой. Системы SCADA могут в качестве прохода злоумышленников для получения закрытой информации и для планирования более изощренных атак.

1. Сетевая атака «SMURF»

Атака SMURF считается экспертами наиболее опасным типом DoS-атаки. В стандартном сценарии хост A отправляет запрос ICMP-эхо (ping) на хост B, вызывая автоматический ответ. Время, необходимое для получения ответа, используется в качестве меры виртуального расстояния между двумя хостами.

В широковещательной IP-сети запрос на пинг отправляется каждому хосту, запрашивая ответ от каждого из получателей. При атаках Smurfs злоумышленники используют эту функцию для увеличения трафика своих атак.

Процесс этой атаки таков, что запрос отправляется либо на сетевой адрес, либо на широковещательный (широковещательный) адрес, но в любом случае устройство должно переходить с уровня 3 на уровень 2, по мере необходимости. согласно RFC 1812 «Требования к IP-маршрутизаторам версии 4» (Требования к IP-маршрутизаторам версии 4). В стандартной сети класса C (24-битное распределение адресов) сетевой адрес будет равен 0, а широковещательный адрес будет равен 255. Эта широковещательная рассылка обычно является диагностической, позволяя

вам идентифицировать работающие системы без необходимости пинговать каждый адрес в диапазоне.

Атака SMURF использует функции прямой передачи и требует как минимум трех участников: атакующего, усиливающую сеть и жертву. Злоумышленник отправляет поддельный пакет ICMP ECHO на широковещательный адрес. Адрес, с которого пришел этот пакет, заменяется адресом жертвы, чтобы создать впечатление, что целевая система инициировала запрос. Затем следуют следующие действия — поскольку пакет ECHO отправляется на широковещательный адрес, все системы сети подкрепления возвращают свои ответы жертве. Если вы отправите один ICMP-пакет в сеть из 100 систем, злоумышленник будет инициировать бафф DoS-атаки сотни раз.

Разновидностью атаки SMURF является атака Fraggle. Атака по сути такая же, как атака Smurf, но вместо отправки эхо-запроса ICMP на адрес прямой широковещательной рассылки она отправляет пакеты UDP. Для атаки Fraggle это тот же процесс смягчения последствий.

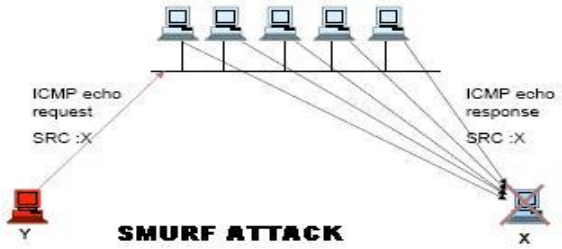

Рисунок 1 – Сетевая атака «SMURF»

Коэффициент усилий зависит от состава сети, поэтому злоумышленник ищет большую сеть, способную полностью подавить работу системы-жертвы. В этой статье рассмотрим следующий пример. Предположим, злоумышленник отправляет 14 КБ непрерывного трафика ICMP на широковещательный адрес укрепляющей сети из 100 узлов. Сеть злоумышленника подключена к сети Интернет по двухканальному ISDN-соединению, усиливающая сеть подключена к линии ТК со скоростью передачи 45 Мбит/с, а сеть жертвы подключена к линии T1 (1,544 Мбит/с). с) подключен. Расчет показывает, что злоумышленник может генерировать 14 Мбит/с трафика в целевой сети, у которой будет мало шансов продолжить нормальную работу, так как вся полоса пропускания линии T1 будет полностью занята. Один из вариантов атаки — фраггл (осколочная граната). Эта атака основана на smurf, но использует UDP-пакеты вместо

ICMP. Злоумышленник отправляет поддельные пакеты UDP на широковещательный адрес сети усилителя, обычно порт 7 (эхо).
Каждая система в сети, которой разрешено отвечать на эхо-пакеты, будет возвращать пакеты системе-жертве, что приводит к созданию большого объема трафика. все равно будет захвачен ненужным трафиком.

2. DNS-атака с усилием

Force Attack наиболее распространенная DDoS-атака, использующая рекурсивные серверы имен.

Атака методом перебор - это метод взлома, который использует метод проб и ошибок для взлома паролей, учетных данных для входа и ключей шифрования. Это простая, но надежная тактика для получения несанкционированного доступа к отдельным учетным записям и системам, и сетям организаций. Хакер пробует несколько имен пользователей и паролей, часто используя компьютер для тестирования широкого спектра комбинаций, пока не найдет правильную информацию для входа.

Атака DNS аналогична атаке smurf, за исключением того, что в этом случае злоумышленник отправляет небольшие запросы преобразователю DNS, как будто вынуждая его отправлять ответы на поддельный адрес. В пример можно привести серию атак, которые проводились в феврале 2007 года, было проведено много атак на корневые DNS сервера, от работы данных серверов на прямую зависит функционирование всех сетей.

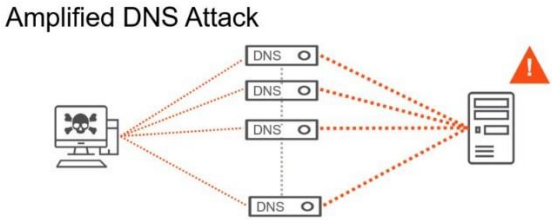

Рисунок 2 – DNS-атака с усилием

3. TCP Reset

Атака сброса TCP, также известная как "поддельные сбросы TCP", "поддельные пакеты сброса TCP" или "атаки сброса TCP", представляет собой способ взлома и прекращения подключения к Интернету путем отправки поддельного пакета сброса TCP. Этот метод взлома может быть использован брандмауэром или злоумышленником для прерывания интернет соединений.

Сброс TCP выполняется путем манипулирования пакетами RST в TCP-соединении. Пакет RST — это заголовок, который сигнализирует о необходимости повторного подключения. Обычно это используется, когда обнаружена ошибка или если вы хотите остановить передачу данных. Злоумышленник может разорвать данное соединение и передавать свои пакеты для совершения атаки.

Вы можете избежать этого типа — вам нужно отслеживать каждый передаваемый пакет и следить за тем, чтобы последовательность чисел поступала в правильном порядке. За это отвечают системы глубокого анализа трафика.

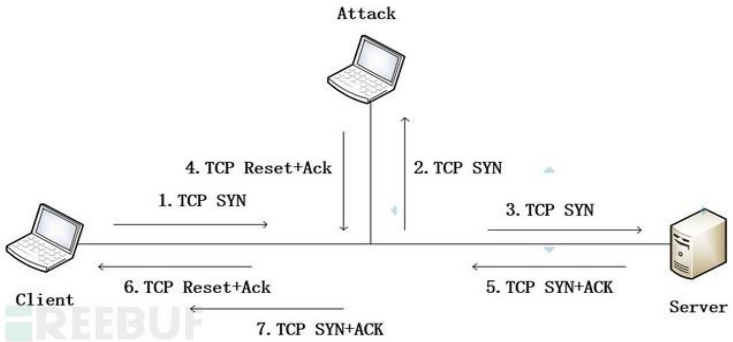

Рисунок 3 – Атака сброса TCP

Заключение

В данной статье были рассмотрены наиболее опасные атаки для информационной системы и способы их реализации. Было проведено сравнение атак по силе их воздействия на информационную систему. В рамках данной статьи было выявлено, что сетевая атака Smurf одна из наиболее опаснейших атак для информационной системы, потому что один сетевой пакет данной атаки может нанести в сотни раз больше ущерба чем остальные. Приведенные выше атаки очень опасны для информационной системы, они могут привести к необычайно серьезным последствиям для дальнейшего ведения бизнеса.

Список используемых источников:

1. Новиков, Ю.В. Аппаратура локальных сетей: функции, выбор, разработка / Ю.В. Новиков, Д.Г. Карпенко. - М.: Эком, 2013. - 288 с.
2. Фостер, Дж.С. Защита от взлома: сокеты, эксплойты, shell-код: выявление уязвимостей операционных систем и прикладных программ к атакам хакеров / Дж.С. Фостер. - М.: ДМК, 2013. - 784 с.

3. Чирилло, Д. Обнаружение хакерских атак / Д. Чирилло. - М.: СПб: Питер, 2017. - 864 с.
4. Рисунок 1: https://yandex.ru/images/search?from=tabbar&text=%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%B0%D1%8F%20%D0%B0%D1%82%D0%B0%D0%BA%D0%B0%20%C2%ABSMURF&pos=3&img_url=https%3A%2F%2Fkey.technospot.net%2Fblogs%2Fimg%2Fsmurf-attack.jpg&rpt=simage
5. Рисунок 2: https://yandex.ru/images/search?from=tabbar&text=DNS%20%D0%B0%D1%82%D0%B0%D0%BA%D0%B0%20%D1%81%20%D1%83%D1%81%D0%B8%D0%BB%D0%B8%D0%B5%D0%BC&pos=0&img_url=https%3A%2F%2Fwww.dns.com%2Fuploads%2FUEditorImages%2F201901%2F14%2F3df7179123a3794813c2ffdff14b993b.jpg&rpt=simage
6. Рисунок 3: https://yandex.ru/images/search?from=tabbar&text=TCP%20Reset&pos=3&img_url=http%3A%2F%2Fimage.3001.net%2Fimages%2F20170531%2F14961644728644.jpg!small&rpt=simage
7. http://ru.wikipedia.org/wiki/
8. https://xakep.ru/2002/06/18/15561/
9. http://inforsec.ru/technical-security/network-security/77-dns-attack
10. https://ipwithease.com/tcp-rst-flag/

УДК 004.056.3:005.52

Методы аудита информационной безопасности

В.Г. Гредычян
студент 4 курса бакалавриата НИЯУ МИФИ, Москва
E-mail: vikagredychian@gmail.com

Аннотация: *в данной статье рассматривается понятие аудита информационной безопасности и его актуальность, рассмотрена схема по проведению программы аудита. В конце представлены основные методологии аудита информационной безопасности.*
Ключевые слова: *информационная безопасность, аудит информационной безопасности, риски, угрозы, методология аудита информационной безопасности.*

Modern information technologies for information security in logistics

Abstract: *this article describes notions of information security audit and its relevance, the article reviews scheme for the audit programme. In addition, the article reviews the main methodologies for information security audit.*
Keywords: *information security, information security audit, risks, threats, information security audit methodology.*

В вопросе о том, чтобы построить систему, которая бы обеспечивала информационную безопасность особую важность представляют процессы по обеспечению контроля и проверки состояния информационной безопасности, то есть аудит информационной безопасность (ИБ). Под аудитом подразумевается систематический, независимый и документированный процесс установления объективного свидетельства (данных, которые подтверждают наличие или истинность чего-либо) и его объективного оценивания для получения степени соответствия критериям аудита (ГОСТ Р ИСО 19011-2021 "Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента", 01.07.2021).

Таким образом, аудит информационной безопасности представляет собой процесс, в котором обеспечивается получение оценок (качественных или количественных) о состоянии системы на текущий момент. Различие данного понятия от информационной безопасности в том, что последнее – это состояние защищённости информации или данных, а аудит ИБ – это процесс.

Можно отметить в последнее время стремительное развитие информационных технологий и систем, что в то же время сопровождается ростом угроз информационной безопасности. По этой причине особую важность имеет аудит информационной безопасности, задачами которыми являются разработка документации по обеспечению безопасности на предприятии; обоснование необходимости в проведении изменений в системе информационной безопасности; участие в обучении персонала по обеспечению безопасности информационной системы.

К целям аудита информационной безопасности относятся оценка безопасности информационной системы на текущий момент и её соответствия стандартам и нормативно-правовым документам, которые есть на текущий момент; оценка рисков, их прогнозирование и анализ; разработка рекомендаций для внедрения новых механизмов безопасности в систему для повышения её эффективности или совершенствования имеющихся.

Аудит информационной безопасности может подразделяться на два типа: внутренний (аудит первой стороны), который выполняется сотрудниками предприятия; внешний, в котором учувствуют сторонние специалисты, которые заинтересованы в деятельности организации. Внешний аудит может называться аудитом второй стороны, в котором принимают участие потребители или какие-то другие лица от их имени; и его называют аудитом третьей стороны, который проводится независимыми аудиторскими компаниями, например, государственными органами.

Благодаря аудиту информационной безопасности организация может противостоять рискам ИБ или минимизировать ущерб от их наступления. Под рисками согласно ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения» подразумевается следствие влияние неопределённости на достижение поставленных целей (ГОСТ Р 51897-2011/Руководство ИСО 73:2009 "Менеджмент риска. Термины и определения", 1.12.2012). Риск может быть результатом какой-либо ошибки или бездействия, но в конечном итоге это проводит к потере репутации компании, финансовым расходам, к переходу клиентов организации к их конкурентам. По этой причине данной проблеме нужно уделять особое внимание.

Для начала рассмотрим управление программой аудита информационной безопасности (Рис. 1).

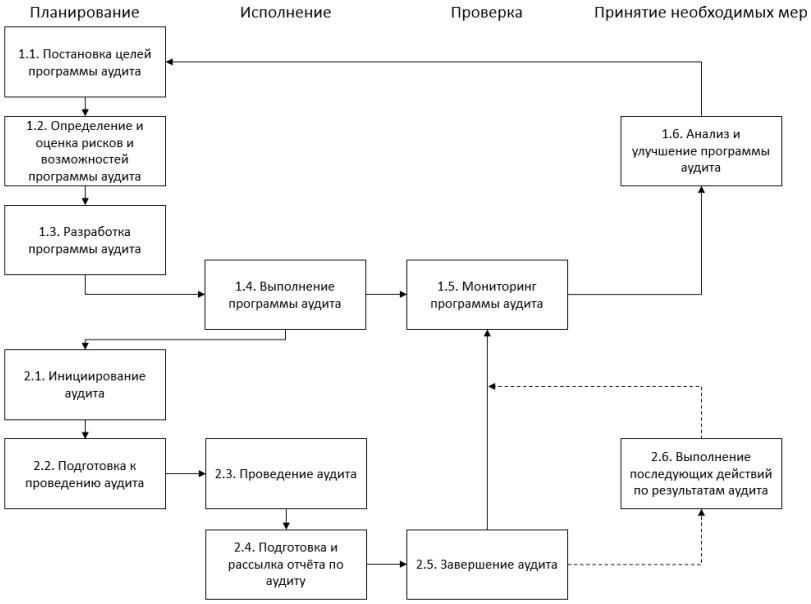

Рисунок 1 – Схема действия для совершения управления программой аудита

Как видно из схемы, для начала заказчику необходимо поставить цель аудита, чтобы было понятно, в каком направлении следует двигаться в дальнейшем. Данная цель не должна противоречить стратегии развития заказчика аудита.

Далее определяются риски и возможности, связанные с программой аудита, и проводится их оценка.

Далее проводится разработка программы аудита, в ходе которой определяются роли; ответственность, которая будет возложена на тех, кто осуществляет управление программой аудита, и определяется компетентность, которой они должны обладать; определяется объём программы аудита, ресурсы.

Во время того как осуществляется программа аудита, определяются его цели, критерии и области, которые должны быть согласованы с целями программы аудита; выбирается метод аудита, отбираются члены аудиторской группы.

Далее проводится мониторинг программы аудита за счёт оценки основных показателей.

Наконец, анализируется программа аудита для того, чтобы определить, были ли достигнуты основные цели. В ходе анализа получается результат, по которому совершенствуется программа.

Во время работ (1.1 – 1.6) осуществлялось управление программой аудита. Проведение аудита осуществляется в шагах 2.1. – 2.6.

При инициировании аудита определяются возможности проведения аудита, чтобы быть уверенным в достижении целей аудита.

Далее идёт подготовка к проведению аудита, в ходе которой анализируется документированная информация, проводится планирование аудита; между членами аудиторской группы распределяются обязанности; подготавливается документированная информация членами аудиторской группы.

В ходе проведения аудита для сопровождающих и наблюдателей распределяются обязанности, проводится вступительное заседание, собирается и проверяется информация, и готовятся заключения по аудиту и заключительное заседание.

Далее составляется отчёт о заключениях по аудиту, который в последствии анализируется, утверждается и рассылается заинтересованным сторонам.

Когда все планы по аудиту выполнены, то аудит считается завершённым. В последствии могут выполняться корректирующие мероприятия для улучшения аудита.

Организация должна регулярно осуществлять мониторинг аудита и его совершенствование, поскольку помимо противодействия растущим угрозам у неё будет возможность повышать конкурентоспособность, и она более привлекательной для новых клиентов и партнёров.

Далее будут рассмотрены методы аудита информационной безопасности, к которым относятся аудит на основе анализа рисков, аудит на основе анализа стандартов информационной безопасности, аудит на основе комбинирования метода анализа рисков и метода по использованию стандартов ИБ, а также аудит на основе экспериментального исследования системы или же её прототипов.

Для начала рассмотрим аудит на основе анализа рисков, в котором осуществляется анализ рисков с использованием определённых методов. Под анализом рисков подразумевается систематическое использование информации для определения источников риска и количественной оценки риска (ГОСТ Р ИСО/МЭК 27001-2006 "Информационная техноогия. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования", 1.02.2008). В данной случае определяются требования для системы и сверяется фактическое состояние с требуемым. При таком подходе нужно, чтобы квалифицированные специалисты проводили анализ, это довольно трудоёмкая задача. Следует учитывать и то, что данный метод зависит от выбранного метода анализа рисков и его применимость к определённой системе, которая исследуется.

Анализ рисков ИБ осуществляется путём их идентификации, когда определяются последствия от нанесённого ущерба, определяются угрозы, их источники, может потребоваться классифицирование угроз, после проверяются имеющиеся средства защиты и те, которые могут использоваться в дальнейшем. В ходе анализа рисков необходимо проведение идентификации уязвимостей системы, последствий при нарушении её информационной безопасности. Существуют различные методы для проведения анализа риска, они подразделяются на качественные, количественные и комбинированные.

В аудите на основе анализа стандартов информационной безопасности осуществляется установления наборов требований в соответствии с рассматриваемым стандартом, которые относятся к исследуемой системе. Можно считать данный метод наиболее практичным. Это объясняется тем, что в стандартах представлены базовые наборы требований безопасности для самых различных систем. Обычно организациями проводится данная методология аудита для того, чтобы в конечном итоге получить сертификат, который даёт подтверждение об уровне безопасности. Это позволяет компаниям повышать конкуренцию на рынке, находить новых более крупных клиентов или же новых партнёров.

В случае комбинирования методы анализа рисков и методов с использованием стандартом ИБ можно добиться лучшего эффекта, поскольку в стандартах можно встретить базовые наборы требований для различных систем, а после можно за счёт анализа рисков получить дополнительные требования, это позволит обеспечить учет особенности системы, которая исследуется. Принимается во внимание и тот момент, что в методе анализа рисков аудитор не имеет изначально никаких требований, а в случае комбинации есть уже какой-то базовый набор, поэтому последний способ считается более простым по сравнению с первым. Стоит учитывать и то, что метод с анализированием стандартов не учитывает специфики отдельной системы, что имеется в комбинированном методе. По этой причине такой подход может дать наибольший эффект.

Отдельно выделяется метод аудита, в котором используются экспериментальные исследования системы или её прототипов, где создаются разнообразные сетевые атаки против системы, в результате чего обнаруживаются «слабые стороны» системы, её уязвимости, проверяется её эффективность. Данный подход подразделяется на несколько направлений, в которых оценивается устойчивость технических средств и способ защиты (технический метод), оценивается устойчивость имеющихся организационных мер и поведение сотрудников в случае атаки на системы (организационный метод), а также применяется комплексный аудит с применением двух вышеперечисленных технологий.

Для возможности проведения аудита информационной безопасности нужна команда, которая в свою очередь будет специализироваться на информационной безопасности. Благодаря аудиту можно получить полную и единую информацию о состоянии системы, выявить её проблемы, повысив тем самым эффективность деятельности организации, а также получить экономический эффект от проделанной работы.

Таким образом, на сегодняшний момент за счёт стремительного развития информационных технологий и систем существуют необходимость в аудите информационной безопасности, для проведения которого есть различные методы, которые были рассмотрены в данной статье. Организация самостоятельно выбирает подходящий для неё метод, достоинства и недостатки которых были рассмотрены выше. Нет единого подхода по аудиту информационной безопасности, но самым оптимальным и эффективным вариантом является комбинация нескольких методов. Стоит акцентировать внимание и на регулярности проведения аудита. В таком случае у организации уже будет имеющая информация о прошлой деятельности в области аудита, что даёт возможность своевременно разрабатывать все необходимые рекомендации.

Список использованных источников:

1. «ГОСТ Р ИСО 19011-2021 "Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента"» 1.07.2021. [В Интернете]. Available: https://docs.cntd.ru/document/1200179216.
2. «ГОСТ Р 51897-2011/Руководство ИСО 73:2009 "Менеджмент риска. Термины и определения"» 1.12.2012. [В Интернете]. Available: https://docs.cntd.ru/document/1200088035.
3. «ГОСТ Р ИСО/МЭК 27001-2006 "Информационная техноогия. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"» 1.02.2008. [В Интернете]. Available: https://docs.cntd.ru/document/1200058325?marker=7D20K3.
4. «ГОСТ Р ИСО/МЭК 27007-2014 "Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности"» 01.06.2015. [В Интернете]. Available: https://docs.cntd.ru/document/1200112881.
5. Ф. И. Ченушкина С. В., «Аудит информационной безопасности на предприятии: определение составляющие, виды» 2018. [В Интернете]. Available: https://elibrary.ru/item.asp?id=35368347.

УДК 005.591.4

Некоторые аспекты процедуры реорганизации предприятий

Е.Г. Казакова
аспирант 2-го курса кафедры «Финансовый мониторинг»
ИФТЭБ НИЯУ МИФИ, Москва
E-mail: EGKazakova@mephi.ru
Е.Р. Мысева
аспирант 2-го курса кафедры «Финансовый мониторинг»
ИФТЭБ НИЯУ МИФИ, Москва
E-mail: ERMyseva@mephi.ru
М.В. Филиппова
ассистент кафедры «Финансовый мониторинг»
ИФТЭБ НИЯУ МИФИ, Москва
E-mail: MVFilippova@mephi.ru

Аннотация: *в статье рассматривается процедура реорганизации предприятия в форме слияния, присоединения, разделения, выделения, преобразования. Раскрываются некоторые особенности проведения процедуры в зависимости от выбранной формы реорганизации.*
Ключевые слова: *реорганизация, слияние, присоединение, разделение, выделение, преобразование.*

Some aspects of the reorganization procedure of enterprises

Abstract: *the article discusses the procedure of reorganization of the enterprise in various forms. Some features of the procedure depending on the chosen form of reorganization are revealed.*
Keywords: *reorganization, merger, takeover, split-up, spin-off, transformation.*

Процедура реорганизации может являться эффективным инструментом по выводу предприятия из кризисного состояния, к которому прибегают управленцы. Реорганизация применяется для различных целей от увеличения доли присутствия компании на рынке до оптимизации налогообложения. Также была распространена реорганизация с целью уклонения от уплаты налогов, так как ранее не предполагался переход ответственности по налогам к новообразованному предприятию. В бюджет так и не поступала уплата по долгам и старое предприятие

ликвидировалось. Но эта ситуация была скорректирована внесенными изменениями в налоговый кодекс, которые предусмотрели возможность перехода таких обязательств к новой компании [3, 13].

Еще одной возможной целью реорганизации может быть «дебюрократизация», которая представляет собой снижение расходов на управленческих аппарат, когда несколько компаний объединяются под единым руководством, например, в случае со слиянием, присоединением. Также могут сокращаться расходы и на другие сферы, такие как маркетинг, бухгалтерский учет и другие [4, 6].

Согласно статье 57 Гражданского кодекса Российской Федерации (далее – ГК РФ) реорганизация производится в форме слияния, присоединения, разделения, выделения, преобразования. Реорганизация юридического лица может проведена не только в одной форме, но и в нескольких. Реорганизация может быть осуществлена по решению учредителей (участников) юридического лица или органа юридического лица, уполномоченного на это. Возможна реорганизация и нескольких юридических лиц, в том числе и различных организационно-правовых форм. Также реорганизация в форме разделения или выделения возможна по решению суда. Такой механизм, например, предусматривается Федеральным законом «О защите конкуренции» от 26.07.2006 N 135-ФЗ в целях предотвращения монополистической деятельности (ст. 38) [8].

Реорганизация считается совершенной с момента государственной регистрации образованных юридических лиц, кроме присоединения. В случае реорганизации в форме присоединения ситуация юридическое лицо считается реорганизованным с момента внесения в единый государственный реестр юридических лиц информации о прекращении деятельности присоединенного юридического лица. При этом, во всех случаях реорганизации, регистрация юридического лица допускается только в случае истечения срока на обжалование такого решения по правилам статьи 60 ГК РФ.

Создание нового юридического лица посредством реорганизации не является чем-то необычным. Так согласно данным Федеральной налоговой службы России за 2020 год, из 3157496 зарегистрированных юридических лиц 78977 образовано путем реорганизации, а 18063 находятся в процессе реорганизации. В 2021 году ситуация схожая: из 3282810 юридических лиц 75527 образовано путем реорганизации, а 11674 находятся в процессе реорганизации [7].

На Рис. 1 показано, из каких этапов состоит процедура реорганизации.

Процедура реорганизации требует привлечение специалистов в соответствующей области, так как регулируется большим количеством нормативно-правовых актов. Некоторые из них представлены на рис. 2.

Рисунок 1 – Этапы процедуры реорганизации

Рисунок 2 – Некоторые нормативно-правые акты, регулирующие процедуру реорганизации

Современные тенденции рынка все чаще диктуют свои условия собственникам бизнеса, именно поэтому в случае кризисных ситуаций на предприятиях, руководителям приходится обращаться к процедурам реорганизации предприятия. Обращение к реорганизации способствуют

оптимизации финансовых активов предприятия, а также дальнейшему обеспечению устойчивости бизнеса.

При проведении процедуры реорганизации, как отмечалось ранее, очень важна правопреемственность, т. е. переход обязательств от реорганизуемого юридического лица (лиц) к новому лицу или лицам. По этой причине законодатель предусмотрел положения, согласно которому, в случае отсутствия в передаточном акте указания на правопреемственность, в регистрации нового юридического лица заявителям будет отказано (ГК РФ, ст. 59) [3, 14].

Далее будет рассмотрена реорганизация предприятия путем выделения.

Согласно законодательству, например, выделением общества признается создание одного или нескольких обществ с передачей ему (им) части прав и обязанностей реорганизуемого общества без прекращения последнего (п. 1 ст. 55 Федерального закона от 8 февраля 1998 г. № 14-ФЗ «Об обществах с ограниченной ответственностью»). При выделении из состава юридического лица одного или нескольких юридических лиц к каждому из них переходят права и обязанности, реорганизованного в соответствии с разделительным балансом (п. 4 ст. 58 ГК РФ).

Процесс реорганизации в форме выделения совершается в несколько этапов, которые показаны на Рис. 3.

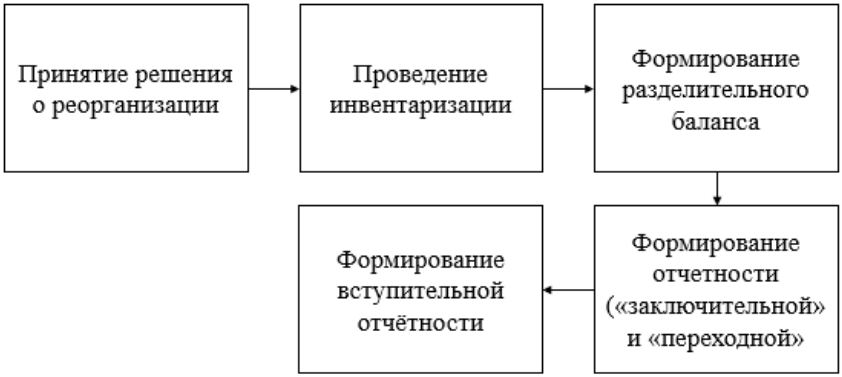

Рисунок 3 – Этапы реорганизации путем выделения

Принятие решения о реорганизации происходит посредством собрания участников в полном составе. Целью собрания является не только принятие решения о непосредственно реорганизации, но и решение ряда вытекающих вопросов, например, в какие сроки будет производиться инвентаризация имущества и обязательств, какие способы оценки имущества и обязательств необходимо использовать, в каком порядке

будет происходить формирование уставного капитала, каким образом будет распределяться прибыль и другие.

На этапе проведения инвентаризации формируется отчетность, в том числе отчетность, относящаяся к тому месяцу, когда заканчивается инвентаризация.

Этап формирования разделительного баланса важен для понимания финансового положения предприятия, основанием для создания разделительного баланса служит бухгалтерская отчетность, которая составляется за последние отчетные даты непосредственно перед передачей имущества.

Этап формирования «заключительной» и «переходной» отчетности связан со следующим. Внесение записи в ЕГРЮЛ является моментом государственной регистрации. На момент внесения предприятия в ЕГРЮЛ организация должна предоставить два вида отчетности – «заключительную», в ней описывают имущество и обязательства предприятия перед передачей другому владельцу, и «переходную».

Вновь созданная организация также должна сформировать бухгалтерскую отчетность – этот тип отчетности называется «вступительной». В основе этого типа отчетности находится разделительный баланс.

Далее рассмотрим реорганизацию путем слияния. В действующем законодательстве под слиянием понимают создание нового общества с дальнейшей передачей созданному юридическому лицу прав и обязанностей (всех) обществ, которые подвергаются реорганизации, и полное прекращение обязанностей и прав последних. Стоит отметить и то, что общества, которые участвуют в слиянии, полностью прекращают свою деятельность, и, следовательно, существование. Весьма часто слияние называют «альтернативной ликвидацией», которая позволяет уйти из бизнеса нерентабельным компаниям с наименьшими потерями.

Каждое юридическое лицо может подвергаться реорганизации в форме слияния, но в отдельных случаях слияние организаций реализовывается с предварительного согласия антимонопольного органа [8].

Не стоит забывать, что процесс слияния двух компаний или предприятий является процессом весьма трудоемким.

Принято выделять 7 основных этапов, по которым проходит реорганизация путем слияния (рис. 4):

Рисунок 4 – Реорганизация путем слияния

Первым этапом является этап выбора участников, которые будут реорганизованы путем слияния. После нахождения обществ, которые готовы присоединиться к реорганизации предприятия, проходят собрания, на которых каждое общество решает следующие вопросы: в какой форме будет проходить реорганизация, какие положения будет содержать договор о слиянии, устав общества, передаточный акт.

Согласно законодательству, в договоре о слиянии должно быть оговорено следующее:

- порядок и условия слияния (удовлетворяющие все стороны договора);
- доля уставного капитала и порядок обмена этой долей для создаваемого общества;
- порядок и сроки назначения нового собрания акционеров или участников общества.

Информация о реорганизации предприятия должна быть доведена до сведения регистрирующих органов посредством уведомления.

Этап подготовки к процессу реорганизации носит в большей степени «бумажный» характер. Ведь именно сейчас необходимо собрать определенный перечень документов, который необходим для правильного проведения реорганизации путем слияния. На Рис. 5 показано, какие документы необходимы для реорганизации путем слияния.

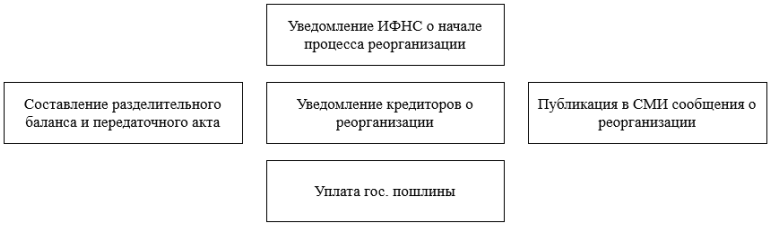

Рисунок 5 – Документы для реорганизации путем слияния

Не последнюю роль в процессе реорганизации играет ИФНС. ИФНС вносит запись в ЕГРЮЛ о создании нового юридического лица и о прекращении деятельности юридических лиц, которые были преобразованы, и направляет копии решений. ИФНС выдает заявителю документы, свидетельствующие об изменении в ЕГРЮЛ, а также передает регистрационное дело регистрирующему органу. Процесс регистрации путем слияния завершается с момента регистрации нового юридического лица.

Реорганизация предприятия путем преобразования – это замена организационно-правовой формы существующего юридического лица. Согласно законодательству, имеющиеся общества могут реорганизовываться в любой другой вид хозяйственного общества.

Процедура преобразования юридических лиц содержит в себе несколько этапов, продемонстрированных на Рис. 6.

Рисунок 6 – Этапы реорганизации юридического лица путем преобразования

Подготовка к процессу реорганизации путем преобразования несколько отлична от формы слияния. Отличия главным образом состоят в различии пакета документов, необходимых для данной процедуры.

Документы необходимые для реорганизации в форме преобразования показаны на Рис. 7.

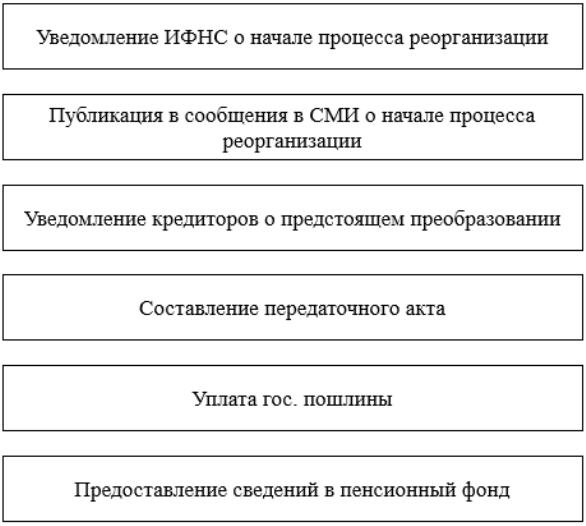

Рисунок 7 – Документы, необходимые для проведения процедуры преобразования

В случае реорганизации путем преобразования, ИФНС также совершает ряд действий, таких как внесение записи в ЕГРЮЛ о создании нового юридического лица и прекращении деятельности старых, выдает соответствующие документы, передает регистрационное дело регистрационному органу.

Реорганизация путем разделения – это ликвидация юридического лица и передача его прав и обязанностей новому юридическому лицу. При такой форме реорганизации происходит деление юридического лица на два и более новых юридических лиц с переходом прав и обязанностей первоначального юридического лица к последним.

Этапы реорганизации юридического лица путем разделения:

1. Принимается решение о реорганизации путем разделения. Совместным собранием учредителей общества выносится решение о реорганизации, которое включает в себя решение по поводу формы реорганизации, устава новых предприятий, разделительного баланса.

2. Для проведения процедуры реорганизации необходимо уведомить государственные регистрирующие органы о начале процедуры.

3. Создание нового (новых) юридических лиц.

4. Подготовка к процессу реорганизации в форме разделения:

- уведомление ИФНС о начинании процесса реорганизации;
- проведение инвентаризации;
- публикация в СМИ сообщения о реорганизации;
- уведомление кредиторов о будущей реорганизации;
- составление разделительного баланса;
- уплата госпошлины.

5. Подача документов в ИФНС.

6. Завершение процесса реорганизации путем разделения.

Документы, необходимые для реорганизации путем разделения представлены на Рис. 8.

Заявление в установленной форме
Протокол общего собрания участников реорганизуемого общества
Передаточный акт
Доказательства уведомления кредиторов реорганизуемого общества
Устав нового общества
Протокол общего собрания участников нового общества
Документ об оплате гос. пошлины
Документ, подтверждающий присвоение выпуску или выпускам акций государственного регистрационного номера или идентификационного номера (только для акционерных обществ)

Рисунок 8 – Документы, необходимые для проведения реорганизации путем разделения

Пятым видом реорганизации предприятий является присоединение. Данный вид реорганизации используется в том случае, когда признается прекращение деятельности одного или нескольких обществ с неотъемлемой передачей всех прав и обязанностей другому юридическому лицу.

Стоит отметить тот факт, что прибегать к реорганизации путем присоединения могут только те организации, у которых одинаковая организационно-правовая форма. Решение о начале реорганизации путем присоединения принимается на общем собрании всех участников каждого из обществ.

Порядок реорганизации путем присоединения показан на Рис. 9

Рисунок 9 – Этапы реорганизации путем присоединения

Важно отменить еще и необходимость соблюдения трудового законодательства в ходе процедуры реорганизации, хотя, в отличие от процедуры ликвидации, изменение собственника не является основанием для увольнения работника, согласно ст. 75 Трудового кодекса РФ (за исключением руководителя, заместителей, главного бухгалтера) [2]. В случае сокращения работника из-за реорганизации ему положены такие же выплаты, как и в случае сокращения при ликвидации [5, 83].

Также в Российской Федерации с 2014 года допускается реорганизация с сочетанием различных форм, а также реорганизация, в которой принимают участие несколько юридический лиц различной организационно правовой формы. Данные изменения для правовой среды России являются новыми, так как предыдущие нормативно-правовые акты, в том числе и в СССР, не предусматривали такой возможности в ходе одной реорганизации [6, 134].

Таким образом, реорганизация предприятия или предприятий является сложной процедурой и носит многоэтапный характер. В ходе реорганизации происходит изменение юридического лица, которое требует

большого внимания к документам необходимым для проведения реорганизации.

Список использованных источников:

1. «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 N 51-ФЗ [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102033239 (дата обращения: 17.11.2021).
2. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102074279 (дата обращения: 17.11.2021).
3. Воробьева Л. С. Реорганизация предприятий в Российской Федерации // Налоги и финансы. 2013. № 4. С. 13–17.
4. Масликов В. А. Проблемы управления реорганизацией предприятий в современных условиях // Материалы Афанасьевских чтений. 2018. № 2 (23). С. 5–10.
5. Никитин Е. Н. Материальные гарантии, компенсирующие неблагоприятные последствия реорганизации или ликвидации предприятия // Вестник Московского университета МВД России. 2021. № 4. С. 80–85.
6. Нуждин Т.А. Комбинированная реорганизация юридических лиц // Право. Журнал Высшей школы экономики. 2018. № 1. С. 133–157.
7. Статистика по государственной регистрации | ФНС России | 77 город Москва [Электронный ресурс]. URL: https://www.nalog.gov.ru/rn77/related_activities/statistics_and_analytics/regstats/ (дата обращения: 26.10.2021).
8. Федеральный закон "О защите конкуренции" от 26.07.2006 N 135-ФЗ [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102108256 (дата обращения: 15.11.2021).

УДК 004.056:338.2

Особенности экономической безопасности в условиях цифровизации

Х.С. Хаджаев
ио.доцент кафедры экономики ТФИ, Ташкент, Узбекистан
E-mail: khabibulla_1965@mail.ru

Аннотация: *в данной статье рассмотрены особенности экономической безопасности в условиях цифровой экономики. Обоснована актуальность обеспечения экономической безопасности с учетом цифровизации экономик стран мира, в том числе и Узбекистана. Анализированы процессы, происходящие в мировой экономике в области безопасности, а также сделано заключение автора по данной проблемы.*
Ключевые слова: *национальная безопасность, цифровая экономика, информационные технологии, развитие, кибербезопасность*.

Features of economic security in the context of digitalization

Abstract: *this article examines the features of economic security in the digital economy. The urgency of ensuring economic security, taking into account the digitalization of the economies of the countries of the world, including Uzbekistan, has been substantiated. The processes occurring in the world economy in the field of security are analyzed, and the author's conclusion on this problem is made.*
Keywords: *national security, digital economy, information technology, development, cybersecurity.*

Современный этап развития во всех странах мира, в том числе и в Узбекистане связан с проблемами обеспечения экономической безопасности, так как от экономической безопасности зависит стабильность в стране. Учитывая это обстоятельство вопросы, связанные с экономической безопасностью, считаются актуальной проблемой и для стран мировой экономики, и для Узбекистана. Поэтому для решения этой проблемы уделяется особое внимание. Как утверждает Лещенко Ю. Г «Национальная безопасность является одним из основополагающих интересов современного государства, объектом постоянного исследования и мониторинга» [1]. В современных условиях во всем мире получило развитие цифровая экономика, которая предусматривает применение

цифровых технологий и постоянно снижает эффективность традиционных мер государственного управления. Это происходит под воздействием процессов глобализации и формирования транснациональных сетей распределения ресурсов и готовой продукции, мобилизация капитала и рабочей силы. Все эти процессы приводят ограничению регулирующих полномочий правительств и в конечном счете угрожают экономической безопасности стран. Развитие информационно-коммуникативных технологий с учетом требований современности обусловливает переход к цифровой трансформации. По экспертным оценкам, которое указано в Концепциях Национальной стратегии устойчивого развития Республики Беларусь на период до 2035 года. «потенциальный экономический эффект от цифровизации достигнет 19-34% общего прироста ВВП к 2025 году» [2]. Каждая страна может обеспечить увеличения своих возможностей с учетом развитие цифровой экономики, которая является одним из приоритетов экономического развития. Исходя из этого использования имеющихся возможностей по применению цифровых технологий в экономическом развитии каждой страны остается актуальным вопросом и в сегодня. При определении масштабов развития экономики и общества в течение длительного периода процесс использования цифровых технологий будет иметь важное значение и в конечном счете приводит к тому, что в жизни людей будет происходит кардинальные изменения. Каждый процесс имеет свои положительные и отрицательные стороны. Так и цифровая экономика имеет свои отрицательные стороны такие как нарушение безопасности конфиденциальности личных данных населения, засорения информационного пространства.

Каждая деятельность, так и деятельность в области применения цифровых технологий в экономике связан с определенными рисками, которые могут быть угрозой при реализации национальных интересов и при обеспечении национальной безопасности.

Так как важен обеспечения национальной экономической безопасности, можем анализировать существующие понятия «национальной экономической безопасности». Под национальной экономической безопасностью понимаются «не только защищенность национальных интересов, но и готовность, способность институтов власти создавать механизмы реализации и защиты национальных интересов развития отечественной экономики, поддержания социально-политической стабильности общества» [3].

Своих произведениях Лев М.Ю и Лещенко Ю.Г отмечали, что «Вызовы, связанные с цифровыми технологиями, обусловливают необходимость выработки комплекса мер, направленных на обеспечение экономической безопасности» [4].

В условиях цифровой экономики каждая страна приводит свою государственную политику в области обеспечения экономической безопасности. При этом использует такие механизмы регулирования, как способы воздействия посредством правовых, экономических и организационных мер.

В условиях цифровой экономики основные угрозы приносят ущерб национальным интересам стран, в результате нарушается состояние защищенности системы за счет рисков в области технологии.

Экспертами Всемирного экономического форума определены следующие технологические риски:

- неблагоприятные последствия технического прогресса для физических и юридических лиц, также для экосистем;
- разрушение критической информационной инфраструктуры;
- цифровое неравенство;
- цифровая концентрация мощностей;
- неэффективность мер кибербезопасности;
- несоблюдение технологии управления.

Таблица 1 – Технологические риски, определенные экспертами ВЭФ

Технологические риски					
Неблагоприятные последствия технического прогресса для отдельных лиц, предприятий, экосистем;	Разрушение критической информационной инфраструктуры	Цифровое неравенство	Цифровая концентрация мощностей	Неэффективность мер кибербезопасности в результате быстрого развития форм и механизмов киберпреступлений	Несоблюдение технологии управления

Среди технологических рисков, определенных экспертами ВЭФ риски, связанные с разрушением критической информационной инфраструктуры предполагает ухудшение или отключение критической цифровой инфраструктуры в результате системной зависимости от технологий. Что касается цифрового неравенства, то оно предполагает неравный доступ к критически важным цифровым сетям и технологиям на различных уровнях из-за того, у всех разные инвестиционные возможности, у некоторых отсутствуют необходимые навыки, недостаточна покупательная способность, различны правительственные ограничения. Под цифровой концентрацией мощностей понимается сосредоточение критически важных цифровых знаний у одного или нескольких субъектов

национальной экономики, который может привести к дискреционным механизмам ценообразования и неравному доступу к товарам и услугам. В результате быстрого развития форм и механизмов киберпреступлений страны могут потерять определенную часть своих экономических финансовых ресурсов, может усилятся напряженность в области геополитики, возникать социальная нестабильность из-за неэффективности мер кибербезопасности. Несоблюдение технологии управления предусматривает отсутствие институтов или правил использования критически важных цифровых сетей и технологий, использование различными государствами или группами государств несовместимой цифровой инфраструктуры, протоколов, стандартов [5]. Цифровая безопасность показывает на сколько население той или иной стран умеет оценивать риски онлайн-мошенничества при работе в условиях цифровой экономики, каковы у них знания в области обеспечения безопасности своих персональных данных, а также о негативных последствиях цифровых устройств на окружающую среду, физическое и психическое здоровье каждого из нас.

Так как происходит процессы перехода к цифровой экономике, вместе с тем обостряются угрозы информационной безопасности. Из-за этого все государства начали обратят внимания на обеспечения кибербезопасности.

Как и другие страны, так и Россия начала обратить внимание на информационную безопасность, которая впервые вошёл в обновлённую стратегию национальной безопасности России. Стратегия национальной безопасности России - базовый документ стратегического планирования, определяющий национальные интересы и стратегические национальные приоритеты России. А также в этом документе отражены цели и задачи государственной политики в области обеспечения национальной безопасности и устойчивого развития России на долгосрочную перспективу. Как отмечено, в исследованиях Т. Костылевой, выделение информационной безопасности в качестве нового приоритета национальной безопасности вызвано более активным, чем прежде, проявлением этих угроз, а соблюдение информационной безопасности должно обеспечить суверенитет страны в информационном пространстве и быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства. [6].

С угрозами кибербезопасности сталкивается и Узбекистан. По данным Агентства информации и массовых коммуникаций в 2020 году в мире было зафиксировано 1 120 масштабных кибератак, были взломаны 20 млрд. записей. А в Узбекистане в адресном пространстве Uznet было зафиксировано свыше 27 млн. угроз вредоносной и подозрительной

активности, а мониторинг кибербезопасности зафиксировал 342 инцидента. Несмотря на то, что это незначительно на фоне мировых показателей, но необходимо учитывать, что в последние годы процессы цифровизации в Узбекистане в сфере государственного управления и экономики стремительно ускоряются, а доля цифровой экономики в ВВП страны составляет 2,2 процента. [7]. Как отмечаются в исследованиях в области цифровой экономики средний оптимальный показатель должен составлять 7-8%. Как показывают мировая статистика этот показатель в Великобритании составляет 12,4%, Южной Кореи – 8%, Китае – 6,9%, Индии – 5,6%, в то же время в России – 2,8%, Казахстане – 3,9%. Предусмотрено увеличение долю цифровой экономики в ВВП Узбекистана в 2 раза к 2023 году, а долю электронных государственных услуг — довести до 60% к 2022 году. [8]. Разработан проект Концепции развития системы «Электронное правительство» Республики Узбекистан. В соответствии с этим проектом к 2025 году планируется довести долю услуг ИКТ в ВВП до 5,0%, а к 2030 году – до 10%. Результаты анализа показывают, что в настоящее время в Узбекистане реализуется более 260 проектов, направленных на последовательное внедрение элементов цифровой экономики и «электронного правительства. Осуществлен запуск системы мгновенных платежей для хозяйствующих субъектов и предпринимателей в режиме 24/7.

В течение 2020-2022 годов в сферу информационных технологий и коммуникаций предусмотрено привлечение инвестиций на сумму в 498,1 млн. долларов, а также реализация 1 627 проектов по цифровой трансформации регионов и отраслей. За эти годы рассмотрено повышение уровня охвата интернетом населенных пунктов. Планировано доведения количество портов широкополосного доступа до 2,5 миллиона единиц, проложить 20 тысяч км оптоволоконных кабелей. Увеличить охват населения мобильным интернетом до 95% посредством развития сетей сотовой связи. В настоящее время для достижения цели противодействия угрозам информационной безопасности и защиты национального киберпространства на законодательном уровне прорабатывается вопрос принятия Национальной стратегии по данному вопросу и завершения разработка закона «О кибербезопасности».

Страны предъявляют различные требования к цифровым технологиям из-за того, что существует неравномерное развития экономики разных стран в мире. Те страны, которые начинают переходит к цифровым технологиям надеются развить свою цифровую инфраструктуру и стремятся ускорить цифровую трансформацию, чтобы повысить свою национальную конкурентоспособность. Те страны, которые последуют за странами, которые добились успеха по развитию цифровых технологий

стремятся быть более эффективными, экологической точки зрения более удачными и умными с помощью цифровых технологий. Для большинства стран — экономических лидеров, включая США, Великобританию, Германию, Японию и других одной из приоритетных направлений было становление цифровой экономики. По оценкам экспертов Мирового Экономического Форума (WEF) внедрение цифровых технологий имеет способность по повышению производительности труда в компаниях на 40% [9].

Цифровая трансформация помогает стимулировать экономическое развитие и производительность, о чем свидетельствует опыт многих стран и отраслей активно принимавшие участия в процессе цифровой экономики. Во всем мире сильно изменяются состояния жизни людей с быстрым развитием 5G и искусственного интеллекта. В этой сфере скорость развития прямым образом зависит от инвестиций в инфраструктуру информационно-коммуникационных технологий и программного обеспечения. Учитывая это, все страны своих национальных стратегиях приоритетными направлениями развития определили 5G и искусственный интеллект. Между странами идет соревнования высоких технологий с участием США, Китая, Южной Кореи, Японии и европейских стран. В этом процессе каждая страна с целью получения первыми стратегические преимущества и повышения конкурентоспособности в ключевых отраслях продвигает свои стратегии и политику в области 5G и искусственного интеллекта.

Если обратим внимание на эти процессы, то США первыми предложили реализовать систематическую национальную стратегию 5G и в настоящее время проводят исследования и разработки в области 5G, коммерческого применения и обеспечения национальной безопасности, а Китай предложил активно проводить исследования и разработки в области 5G, разрабатывать стандарты и содействовать развитию отрасли в дополнение к созданию ведущей глобальной сети мобильной связи к 2025 году, Европейские страны запустили стратегии 5G и стратегию индустрии 4.0 и имеют стремления стать первыми в области кибербезопасности 5G. Что касается Японии, то она направили свои силы на исследования и разработки стандартов 5G. Кроме этого она выпустила Стратегию технологий искусственного интеллекта для разработки дорожной карты развития индустрии искусственного интеллекта. Если Южная Корея запустила коммерческие услуги 5G в рамках крупных мероприятий, то появление сети 5G в крупных российских городах предусмотрено к 2024 году.

В заключении следует отметить, то что особенности экономической безопасности в условиях цифровой экономики и обеспечения его в странах

мира и в том числе и Узбекистана дает возможность предотвращения определенных проблем, возникающих при применении цифровых технологий, которые связаны с кибербезопасностью.

Список использованных источников:

1. Лещенко Ю. Г. Национальные интересы в контексте обеспечения экономической безопасности государства в условиях глобальной интеграции: эволюционно-теоретический аспект // Вопросы инновационной экономики. – 2020. – № 4. – с. 2375-2390. (Дата обращения: 9.12.2021)
2. Концепция Национальной стратегии устойчивого развития Республики Беларусь на период до 2035 года. [Электронный ресурс]. URL: http://www.economy.gov.by/uploads/files/ObsugdaemNPA/Kontseptsija-na-sajt.pdf (Дата обращения: 9.12.2021).
3. Сенчагов В.К. и др. Экономическая безопасность: Производство - Финансы - Банки. / под редакцией В.К. Сенчагова / А. И. Архипов, А. Р. Белоусов, Р. А. Белоусов [и др.]. - Москва: ЗАО Финстатинформ, 1998. – 621.Закон Республики Узбекистан «Об электронной коммерции» (новая редакция). [Текст] №ЗРУ-385 от 22 мая 2015 г. (Дата обращения 9.12.2021)
4. Лев М.Ю. Лещенко Ю.Г. Цифровая экономика: на пути к стратегии будущего в контексте обеспечения экономической безопасности // Вопросы инновационной экономики. – 2020. – № 1. – с. 25-44. – 9.12.2021)
5. The Global Risks Report 2021. [Электронный ресурс]. URL: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf/ (Дата обращения 9.12.2021)
6. Костылева Т. Информационная безопасность в обновлённой Стратегии национальной безопасности России выделена как приоритетное направление. https://d-russia.ru/ 05.07.2021 (Дата обращения 9.12.2021)
7. Абатуров В, Кибербезопасность – проблема общая. ЦЭИР. Журнал «Экономическое обозрение» №7 (259) 2021 https://review.uz/post (Дата обращения 9.12.2021)
8. Кутбитдинов Ю Узбекистан о цифровизации https://review.uz/post/uzbekistan-otsifroviyvaetsya, ЦЭИР Экономическое обозрение №10 (238) 2019 (Дата обращения 9.12.2021)
9. WEF (2018a). Digital Transformation Initiative. Unlocking $100 Trillion for Business and Society from Digital Transformation. Executive summary. P. 12. http://reports.weforum.org/digital-transformation/wp-content/ blogs.dir /94/ mp/files/ pages/files/dti-executive-summary-20180510.pdf (Дата обращения: 7.02.2020).

УДК 005.584.1:004.658

Отслеживание взаимодействий со смарт-контрактами в блокчейне Ethereum

А.С. Гридин
студент 6-го курса НИЯУ МИФИ, Москва
E-mail: alexqrid@gmail.com
В. Давыденко
старший преподаватель кафедры «Финансовый мониторинг»
ИФТЭБ НИЯУ МИФИ, Москва
E-mail: VIDavydenko@mephi.ru
В.А. Рычков
старший преподаватель кафедры «Финансовый мониторинг»
ИФТЭБ НИЯУ МИФИ, Москва
E-mail: VARychkov@mephi.ru

Tracking interactions with smart contracts on the Ethereum blockchain

Аннотация: *смарт-контракты являются относительно новой, но очень быстро развивающейся, и популярной технологией. Данная область мало изучена, но ежедневно появляется десяток финансовых продуктов на основе смарт-контрактов в блокчейне различных криптовалют. Возможность анализа активности контрактов и взаимодействия с ними предоставляются небольшим количеством сервисов и в достаточно ограниченной степени. На сегодняшний день не существует универсального решения для анализа активности контрактов, для каждого отдельного контракта необходим индивидуальный подход. В данной статье рассматривается методика отслеживания вызовов функций смарт-контрактов в транзакциях блокчейна Эфириум и распознавания названий таких функций.*

Ключевые слова: *блокчейн, эфириум, смарт-контракты, солидити.*

Tracking interactions with smart contracts on the Ethereum blockchain

Abstract: *smart contracts are relatively new, but tremendously fast emerging technology. The domain lacks of researches, but everyday tens of new financial products based on smart contracts appears on the blockchain of various cryptocurrencies. A little number of providers give a limited ability for analyzing contract's activity. There is no universal solution for analyzing the activity of contracts, and the individual approach is needed for each contract. This article*

discusses a technique of tracking calls to smart contracts on Ethereum blockchain transactions and recognizing the name of the contracts function that have been called during the interaction.

Keywords*: blockchain, ethereum, smart-contracts, solidity.*

Введение

Отслеживание транзакций в сети определенной криптовалюты не представляет собой сложный и трудоёмкий процесс. На сегодняшний день существуют более десяти сервисов, с помощью которых можно найти любую транзакцию в сети любой криптовалют. Такие сервисы называются «обозревателями блоков». Эти сервисы отличаются по полноте предоставляемой информации. Например, одни могут предоставлять полную информацию о транзакции, включая взаимодействие со смарт – контрактами [1][2], а другие [3] могут показать лишь информацию о количестве криптовалюты, отправленной в данной транзакции, что не является достаточным для анализа транзакции и представляет проблему как для аналитиков, так и для пользователей сервиса. Полная информация о транзакции должна включать в себя не только информацию о переводах криптовалюты, но и информацию о том, к каким смарт-контрактам происходило обращение в этой транзакции и какие функции смарт-контрактов были вызваны.

В данной статье рассматривается методика отслеживания вызовов функций смарт-контрактов в рамках той или иной транзакции и алгоритм распознавания названия этих функций.

Получение данных из блокчейна Эфириум.

Сеть криптовалюты Эфириум представляет собой P2P-сеть (точка-точка) [4]. Для того чтобы стать одним из участников сети и получать информацию о состоянии сети, блоках, транзакциях и об аккаунтах, достаточно запустить программу-клиент данной криптовалюты. На сегодняшний день, для Эфириум существует более шести программ-клиентов, написанных на различных языках программирования [5]. Общее в реализации этих клиентов то, что все они удовлетворяют спецификации Эфириум [6], которая описывает функционирование блокчейна и сети Эфириум, другими словами, алгоритм работы программ-клиентов один и тот же, поэтому сетевое взаимодействие различных узлов между собой не нарушает общую работу и состояние сети.

Для получения каких-либо данных из блокчейна Эфириум, необходимо отправить запрос к API узла сети. Это может быть узел сети, который можно запустить самому на компьютере, удовлетворяющим определенным требованиям [6], либо получить доступ к другим, уже запущенным кем-то, узлам сети. Все примеры API запросов к узлу сети, приведенные в данной

статье, выполнены с использованием клиента, написанного на языке программирования Go [7], потому что данный клиент обладает наиболее широким набором методов API, отдаёт данные в читаемом формате JSON [8] и официально поддерживается сообществом Ethereum Foundation.

В статье [9] описывается алгоритм для отслеживания событий определенных смарт-контрактов и приведены примеры для отслеживания эмиссии и изъятия из обращения популярнейшего токена в сети Эфириум – Tether USD. Хотя отслеживание событий и является основным источником данных об активности смарт-контрактов, но будет ли вызвано событие и произведена запись в лог транзакции, в конечном итоге, решает разработчик. Если разработчик решит не добавлять данный функционал в код контракта, то отследить активность такого контракта, т.е., обращение к данному контракту со стороны других аккаунтов и манипуляции, осуществляемые данным контрактом, значительно сложнее. Вообще говоря, не имея в распоряжение доступа к API узла, это не представляется возможным, потому что обозреватели блоков, как правило, не показывают таких деталей, потому что это создаёт дополнительную нагрузку на их инфраструктуру и может замедлять скорость синхронизации их узлов с другими участниками сети. Однако данная информация является критичной как с точки зрения безопасности взаимодействия с контрактом, так и с точки зрения получения полной информации о транзакции заинтересованными лицами.

Информацию о транзакции в блокчейне Эфириум можно получить с помощью вызова метода «*eth_getTransactionByHash*» у API узла сети [10] с указанием идентификатора транзакции. На рисунке 1 представлена информация, полученная от узла сети, для транзакции с идентификатором *0x7d52cf58fe78403e8816dae6e900baff92b35760b4ed81cecd2590eafcde3dad*.

Рисунок 1 – Информация о транзакции из блокчейна Эфириум

В полях *from*, *to* указаны адреса отправителя транзакции и получателя соответственно, а поле *value* указано количество криптовалюты, отправленной от отправителя к получателю. Произведение значений полей *gas* и *gasprice даёт* значение комиссии, оплаченной отправителем для того, чтобы данная транзакция попала в блокчейн. Любопытным является то, что в транзакции на рисунке 1 поле *value* содержит нулевое значение. На первый взгляд, получив такую информацию о транзакции, может показаться, что она не имеет никакого смысла, потому что никакого перевода криптовалюты не было осуществлено, а комиссия была списана с аккаунта отправителя. Чаще всего такое бывает, если в качестве получателя указан адрес смарт-контракта, как в данной транзакции.

В поле *input* транзакции закодированы данные, передаваемые смарт-контракту, а именно, функция контракта и значения аргументов, которые она принимает на вход. Если посмотреть информацию об этой транзакции на сайте обозревателя блоков Etherscan [11], то можно увидеть, что в данной транзакции у контракта, адрес которого указан в поле *to*, вызвана функция *cast(address[] _targets, bytes[] _datas, address _origin)*. Данная функция принимает на вход 3 аргумента: массив адресов, массив байт и адрес. Для понимания манипуляций, производимых контрактом при вызове данной функции, необходимо иметь исходный код контракта. Но проблема заключается в том, что одни контракты, могут вызывать функции других контрактов и тогда, для отслеживания всей цепочки вызовов, необходимо получить исходные коды всех контрактов, чьи функции вызываются.

Для отслеживания всей цепочки вызовов в API узла сети есть метод «*debug_traceTransaction*». Если вызвать данной метод и указать ему идентификатор транзакция, то можно получить всю цепочку вызовов функций контрактов.

Рисунок 2 – Информация о транзакции с сайта Blockchair.com

Например, в транзакции, рассмотренной выше, было осуществлено 174 вызова функций различных контрактов, как показано на рисунке 2 [12]. Blockchair является единственным обозревателем блоков Эфириум, который показывает всю цепочку вызовов функций смарт-контрактов.

Алгоритм распознавания названий вызываемых функций смарт-контрактов.

Иметь цепочку вызовов функций контрактов недостаточно для получения полного понимание о вызываемых функциях. Для этого необходимо уметь прочитать закодированный вызов функции, в котором, в том числе и закодировано название вызываемой функции. Правила кодирования этих данных описаны в документации языка программирования Solidity [13].

Как следует из документации [14] название вызываемой функции кодируется следующим образом: берётся сигнатура функции, от неё вычисляется значение хеш-функции Keccak-256 [15] и от результата берутся первые 4 байта (8 символов). Эти первые 4 байта называются селектором функции. Сигнатура функции представляет собой название функции и типы данных аргументов, которые она принимает на вход. Пример вычисления значения хеш-функции представлен на рисунке 3. Если сравнить первые 8 символов хеша на рисунке 3 и первые 8 символов, не считая 0x, поля *input*, указанного на рисунке 1, то можно заметить, что они одинаковы.

Рисунок 3 – Вычисление значения хеш-функции от сигнатуры функции смарт-контракта

Так как хеш-функция является односторонним преобразованием, т.е. из её результата нельзя получить исходное значение, то для распознавания функций контрактов, вызываемых в транзакциях, необходимо иметь базу

сигнатур функций, интересующих нас контрактов, иными словами, снова возникает необходимость наличия исходного кода смарт-контракта. Однако данное ограничение можно обойти, воспользовавшись открытой базой сигнатур функций контрактов, и разработать универсальное решение, подходящее не под определенные контракты, а для миллионов различных контрактов.

Такая база сигнатур находится в открытом доступе и в неё может добавлять сигнатуры любой желающий [16]. Таким образом, для распознавания названий функций контрактов, вызванных в определенной транзакции, необходимо выполнить следующие шаги:

– Получить цепочку вызовов с использованием API метода «*debug_traceTransaction*» узла сети Эфириум.
– Рекурсивно пройтись по всей цепочке вызовов и сопоставить первые 8 символов (без учёта 0x) поля *input* с имеющейся базой сигнатур функций. Для последнего можно воспользоваться открытой базу сигнатур [16].

В рамках данного исследования предложенный алгоритм был внедрён в исходный код узла сети Эфириум и, несмотря на большое количество обрабатываемой информации, добавление в метод «debug_traceTransaction» ещё одного этапа обработки данных, практически не сказалось на скорости его выполнения, потому что была продумана эффективная организация данных по сигнатурам в виде хранилища ключ-значения. Результат работы модифицированного API метода «debug_traceTransaction», который отдаёт названия вызванных функций контракта, можно видеть на рисунке 4.

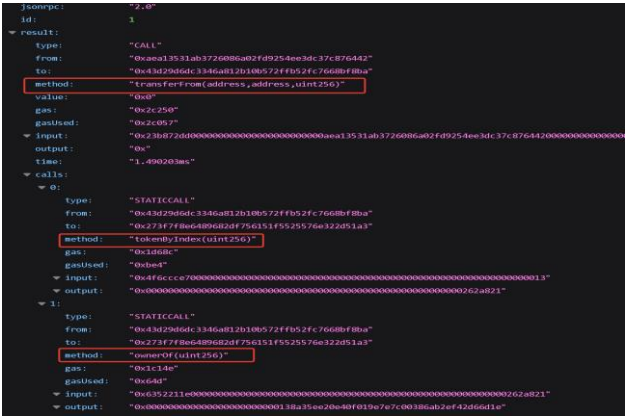

Рисунок 4 – Результат вызова модифицированного API метода «debug_traceTransaction» узла сети Эфириум

Заключение

В ходе работы была рассмотрена методика отслеживания вызовов функций контрактов, а также разработан и реализован алгоритм распознавания названий вызванных функций. Реализация алгоритма была написана на языке программирования Go и внедрена в исходный код узла сети Эфириум, написанного на языке Go. Разработанный алгоритм можно использовать не только для криптовалюты Эфириум, но и для других криптовалют, реализующих работу смарт-контрактов с использованием виртуальной машины Эфириум.

На сегодняшний день многие пользователи криптовалют взаимодействуют со смарт-контрактами с использованием сторонних сервисов, в которых они не могут отследить какие функции контракта вызываются при взаимодействии с ним. С помощью алгоритма, описанного в данной статье, можно без большого труда получить необходимую информацию. Это важно, потому что сторонние сервисы не всегда могут действовать в интересах пользователей, к тому же, учитывая, что популярность мошеннических схем с использованием криптовалют только растёт, пользователям необходимо иметь полное представление о совершаемых транзакциях.

Для разработчиков смарт-контрактов, данное решение позволит сэкономить много времени при отладке работы смарт-контрактов в тестовых сетях, потому что пропадёт необходимость поиска имени вызванной функции по хешу сигнатуры.

Данная разработка особо актуальна в связи с развитием инфраструктуры, так называемых, децентрализованных финансов, которые представляют собой работающие на смарт-контрактах различные продукты (биржи обмена, кредитные и страховые продукты, деривативы и стейблкоины), потому что сложность смарт-контрактов таких продуктов схожа с корпоративными приложениями состоящих из нескольких тысяч строк кода.

Список использованных источников:

1. Blockchair. Universal blockchain explorer and search engine [Электронный ресурс]. – URL: https://blockchair.com (дата обращения 15.12.2021)
2. Etherscan. Ethereum (ETH) Blockchain Explorer. [Электронный ресурс]. – URL: https://etherscan.io (дата обращения 15.12.2021)
3. Blockchain. Blockchain Explorer - Search the Blockchain | BTC | ETH | BCH. [Электронный ресурс]. – URL: https://blockchain.com (дата обращения 15.12.2021)
4. R. Schollmeier. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications // Proceedings First

International Conference on Peer-to-Peer Computing, p. 101(2001). DOI: 10.1109/P2P.2001.990434.
5. Ethereum Foundation Blog. Nodes and clients [Электронный ресурс]. – URL: https://ethereum.org/en/developers/docs/nodes-and-clients (дата обращения 15.12.2021)
6. Ethereum Foundation. Ethereum yellow paper [Электронный ресурс]. – URL: https://ethereum.github.io/yellowpaper/paper.pdf (дата обращения 15.12.2021)
7. Github. Official Go implementation of the Ethereum protocol [Электронный ресурс]. – URL: https://github.com/ethereum/go-ethereum/blob/master/go.mod#L3 (дата обращения 15.12.2021)
8. JSON. JavaScript Object Notation [Электронный ресурс]. – URL: https://www.json.org/json-ru.html (дата обращения 15.12.2021)
9. Гридин, А. С. Отслеживание транзакций токенов в блокчейн сети Ethereum на примере эмиссии токена USD Tether / А. С. Гридин // Материалы Второго Международного научно-практического форума по экономической безопасности «VII ВСКЭБ».
10. Ethereum Wiki. Json-rpc requests [Электронный ресурс]. – URL: https://eth.wiki/json-rpc/API (дата обращения 15.12.2021)
11. Etherscan. Ethereum transaction hash details [Электронный ресурс]. – URL: https://etherscan.io/tx/0x7d52cf58fe78403e8816dae6e900baff92b35760b4ed81cecd2590eafcde3dad (дата обращения 15.12.2021)
12. Blockchair. Ethereum / Transaction / 0x7d52cf58fe78403e8816dae6e900baff92b35760b4ed81cecd2590eafcde3dad – Blockchair. [Электронный ресурс]. – URL: https://blockchair.com/ethereum/transaction/0x7d52cf58fe78403e8816dae6e900baff92b35760b4ed81cecd2590eafcde3dad (дата обращения 15.12.2021)
13. Solidity. Solidity programming language [Электронный ресурс]. – URL: https://soliditylang.org (дата обращения 15.12.2021)
14. Solidity. Function selector and argument encoding [Электронный ресурс]. – URL: https://docs.soliditylang.org/en/develop/abi-spec.html#function-selector-and-argument-encoding (дата обращения 15.12.2021)
15. Guido Bertoni, Joan Daemen, Michael Peeters, Gilles Van Assche. Keccak specifications (2009).
16. 4byte.directory. Ethereum Signature Database [Электронный ресурс]. – URL: https://www.4byte.directory (дата обращения: 15.12.2021)

УДК 004.658:004:330.4

Проблемы адаптации блокчейна в контексте цифровой экономики

В.М. Селезнёв
старший преподаватель Финансового Университета, Москва
кандидат технических наук
E-mail: VMSeleznyov@fa.ru

Аннотация: *с момента появления 12 лет назад блокчейн до сих пор не получил широкого распространения за пределами криптовалюты. В этой статье автор анализирует состояние внедрения в 2021 году ряда приложений блокчейна, которые ранее считались успешными в прессе и научной литературе, и выдвигает гипотезу о том, что успех блокчейна достижим только в тех областях, где цифровизация невысока.*
Ключевые слова: *внедрение блокчейна, криптовалюта, цифровая экономика.*

Problems of adaptation in the digital economy

Abstract: *since introduction 12 years ago blockchain still has not find wide adoption beyond cryptocurrency. In this article author analyses state of adoption in 2021 of a number of blockchain applications previously regarded as successful in press and scientific literature and states a hypotheses that blockchain success is achievable only in fields where digitization is low.*
Keywords: *blockchain adoption, cryptocurrency, digital economy.*

Технологии блокчейн уже более 12 лет, но по-видимому следует констатировать, что несмотря на значительные инвестиции, интерес к ней определялся и определяется преимущественно в контексте рынка криптовалюты (Рис 1). Основной всплеск интереса к блокчейну, как независимой от криптовалют технологии, начался в 2016 году, и связан с выходом ряда прогнозов, где блокчейн рассматривался как основа цифрового будущего. Среди этих публикаций, особо отметить стоит книгу «отца» цифровой экономики Дона Тэпскотта «Технология блокчейн: то, что движет финансовой революцией сегодня» [1] в которой он выделил такие важнейшие технологические свойства блокчейна как: распределенность, равноправность, неизменность информации, скорость, анонимность и бесплатность. Согласно его выводам, обладающая такими свойствами система, неизбежно станет основной технологией новой цифровой

экономики. Ряд исследователей пошли ещё дальше, предположив, что блокчейн является основополагающей технологией, которая ляжет в основу «нового интернета» [2]. А благодаря тому факту, что внедрение новых технологий ускоряется, новое блокчейн будущее наступит очень скоро, нужно только увеличить финансирования блокчейн компаний и немного подождать. Хотя, ряд исследователей, в частности автор, указывали на то что блокчейн не является основополагающей технологией, очевидно, не обладает приписываемыми свойствами [3, 4], и, поэтому вряд ли будет массово внедрен в ближайшее время с позитивным экономическим эффектом, вопросом задержки внедрения блокчейна (в широком смысле, включая все разновидности распределенных реестров) наука заинтересовалась лишь в последний год, за который WoS и Scopus зарегистрировали около 400 статей посвященных теме задержки внедрения блокчейн.

Действительно, согласно теории «диффузии инноваций» инвестиции в блокчейн, составившие к 2021 году 4.9 миллиардов евро [5], должны были привести к уровню проникновения технологии «раннее большинство» т. е. не менее 34.5% потребителей, при том что текущее проникновение технологии, включая криптовалюту, даже в самой «криптоволютной» стране – Украине, составляет только 12% [6], что меньше уровня «ранние последователи». Для сравнения инвестиции в квантовые технологии составили к 2021 году 3 миллиарда [7], при том что квантовая связь активно используется, а квантовые компьютеры активно решают актуальные задачи, которые невозможно решить обычной вычислительной техникой. При этом, особо стоит отметить что, в классическом виде, блокчейн ещё и чудовищно неэффективен, даже при столь малом уровне адаптации, только биткоин в 2021 году потреблял 115 Tw/h электричества, что сравнимо с потреблением страны Испании [8].

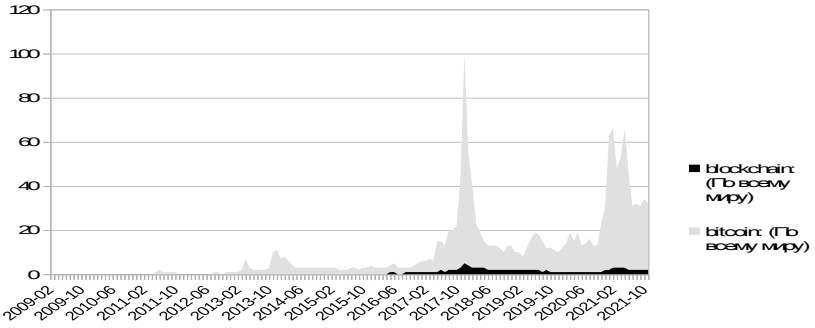

Рисунок 1 – Основной интерес с блокчейну существует только в контексте криптовалюты. (График Google trends)

В анализе факторов влияющих на принятие решений о внедрении блокчейна авторами научных статей были использованы многочисленные социологические опросы, построенные и использованием различных теорий и фреймворков внедрения инноваций, среди который кроме теории диффузии инноваций, были использованы унифицированная теория принятия и использования технологии, фреймворк технология-организация-окружение (TOE framework), теория внедрения интер-организационных систем (IOS adoption theory) и собственные эмпирические построения авторов [9,10]. Среди влияющих на адаптацию технологии факторов были отмечены как комплексные – «готовность экосистемы» [10], так и индивидуальные – сложность, доверие, приватность, безопасность, давление рынка, давление регуляторов, готовые бизнес кейсы, поддержка топ менеджмента, размер организации [11, 12], и даже «крутость» и любопытство [13]. Не отрицая большую важность этих исследований, актуальность и обоснованность, следует отметить, что они дают большей частью «мгновенную» картину, «на данный момент». В частности примеры «успеха» внедрения технологии. Поэтому, интерес вызывает что происходит с успешными внедрениями через год, два, три. Краткий результат состояния данных успешных внедрений в конце 2021 года, приведен в Таблице 1. В качестве основы взята таблица из работы [12], отражающая успех внедрения блокчейна в различных компаниях в 2019-20 годах. Для лучшего понимания, таблица разделена на типы проектов по отраслям и отдельно выделены «инфраструктурные проекты», поскольку успешные продажи инфраструктурных продуктов, в прямую, очевидно, не связаны с успехами внедрения технологии в прикладных областях экономики.

Таблица 1 – Инфраструктурные проекты

Компания	Продукт	Состояние в 2021	Комментарии
R3	Corda-blockchain platform for finance. Блокчейн платформа для финансовых приложений.	Бизнес внедрения продукта развивается. Существуют программы развития, обучения, сертификации. С 2019 в процессе тестирования. Применяется в системе аккредитивов Contour.	Строго говоря, не «блокчейн», поскольку единый распределенный лог транзакций отсутствует. Согласно описанию «это протокол передачи сообщений между участниками системы, созданный под влиянием биткоина».
IBM	Watson IoT Platform (ранее известная как cloud blockchain	Платформа развивается, и даже нашла прикладные применения (например в системе контроля грузов Maersk). Однако, в целом, IBM перенесла приоритеты	Классический частный распределенный реестр.

	platform, ADEPT)	стратегического развития с блокчейна на искусственный интеллект. [14]	
Microsoft	The Confidential Consortium Framework (до 2019 The Coco Framework)	Не нашел применения до настоящего времени. Кроме того Microsoft's Azure Blockchain as a Service был закрыт в сентябре 2021. [15]	Строго говоря не является блокчейном. Представляет собой фреймворк создания распределенных регистров путем кобинирования доверенной облачной среды исполнения, продвинутой публичной криптографии и набора консенсусных механизмов, для создания различных сценариев потенциального применения в бизнесе.
Oracle	Oracle Blockchain Platform (до 2020 OABCS)	Активно развивается и предлагается. (Последняя версия Ноябрь 21 года). Интеграторами предлагаются продукты на его основе для поддержки цепочки поставок.	Насколько является «блокчейном» – спорный вопрос. Permissionless и хранит транзакции в полноценной базе данных.

Проекты в области финансов

Contour Pte. Ltd.	Contour (до 2020 называлась Voltron. Обработка аккредитивов (Letter of Credit).	Платформа торгового финансирования. Продукт основан на R3 Corda. Участвуют в тестировании около 50 банков среди которых ABN Amro, Standard Chartered, ING, MUFG и отечественный Альфа-банк. Достигнуты определенные успехи внедрения Contour, ранее обрабатываемых вручную, стала занимать менее 24 часов вместо 5-10 дней.
Facebook	Libra Coin	Продукт по крайней мере отложен, если не закрыт. [16]
Wells Fargo	Internal stablecoin. Внутренняя криптовалюта.	Банк регулярно объявлял о применении блокчейна в разных банковских приложения, включая торговлю ценными бумагами, страхование и т. д. В основном, судя по всему, для создания маркетингового шума в прессе. Внутренняя криптовалюта в настоящее время очевидно никак не используется.
J.P Morgan	JPM coin. Стабильная криптовалюта.	В настоящее время просто долларовый депозит. Записи о котором «дублируются в блокчейне» (вероятно по маркетинговым причинам).

Проекты в области связи:

Verizon	Blockchain virtual SIM. Виртуальная SIM карта, eSIM.	Компания подала патентную заявку на данное решение. О реализации пока ничего не слышно.

LG	Uplus Payment service. Мобильные платежи на блокчейне.	U+ довольно успешный пакет телекоммуникационных сервисов и тарифов, в том числе с поддержкой мобильных платежей. Несмотря на то что в 2018 году заявлялись намерения использовать блокчейн некоторым образом, в настоящее время мобильные платежи осуществляются через традиционные каналы.

Поддержка цепочки поставок / Логистика

Maersk	TradeLens. Управление логистикой морских перевозок	Тестировалась в партнерстве с IBM с 2014 года. В 2021 запущена в ограниченную эксплуатацию. Работу с системой поддерживают около 300 партнеров. Решение отслеживает движение грузов с помощью датчиков, и полностью цифровизует сопроводительные документы, в том числе таможенные.
Global Shipping Business Network (GSBN)	Cargo Release. Управление логистикой морских перевозок	Начало опытной эксплуатации в сентябре 2021.Решение аналогичное TradeLens но созданное консорциумом перевозчиков и портовых опреаторов (COSCO, Hapag-Lloyd, Hutchison ports, OOCL, PSA, QGGJ, SIPG) на решениях Oracle.
Walmart	Food supply chain. Система контроля цепочки поставок отдельных категорий продуктов.	Компания многократно запускала различные проекты на «блокчейне», в том числе подавала патентные заявки на собственную «валюту». Системы отслеживания цепочки поставок на базе Hyperledger Fabric были запущены для поставок манго и для поставок бекона. Основная проблема в том, что у поставщиков, в настоящий момент, отсутствуют стимулы для занесения информации в блокчейн Walmart.
Консорциум авто производителей (BMW, Ford, Renault)	MOBI. Блокчейн консорциум.	Собственно говоря не разрабатывает блокчейн-продукты. Консорциум издал ряд предложений по стандартизации различного рода информации о автомомобиле, запасных частях, отслеживания поездок, которая может использоваться в различных распределенных реестрах. В частности стандарты Vehicle Identity (идентификации автомобиля), Trusted Trip Credential (информация о поездках), Electric Vehicle Grid Integration (о сети заправок электромобилей), Connected Mobility Data Marketplace (рынок обмена авто-информацией). Так же предложен свой стандарт на смарт-контракты. Информации о реализации этих стандартов пока не поступало.

Проекты здравоохранения

Healthbank	Healthcare management (Управление здоровьем)	Компания существует, но продукт с 2017 года находится в состоянии «скоро выйдет».

Gem	Healthcare management (Управление здоровьем)	Собрав деньги с инвесторов, компания так и не запустила продукт в области здравоохранения. В настоящее время торгует криптовалютой.
CoverUS	Маркетплейс здравоохранения	Продукт не вышел. Компания существует как сеть дисконтных карт на рецептурные лекарства.

Товарные биржи

Grainchain	Торговля зерном для мелких фермеров [17]	«В разработке» с 2013 года. В интервью Форбс, основатель биржи отмечает что основная проблема мелких фермеров, не в доверии и честных платежах, а в логистике и доступе к элеваторам. И эти проблемы продуктом не могут быть решены.
BanQu	Система торговли фермерскими продуктами и товарами для поддержки фермерства.	У системы есть успешные нишевые внедрения. Так, в 2021 году системы удалось достаточно широко запустится в Замбии, благодаря поддержке InBev и COVID ограничениям.

Энергетика

Grid+	P2P торговля электричеством, управление торговлей электричеством	В настоящее время под этим брендом продается аппаратный криптокошелек.
Wepower	P2P торговля электричеством, управление торговлей электричеством	Компания активно создает инфоповоды. Собственная криптовалюта торгуется $0.004167
EWF	P2P торговля электричеством, управление торговлей электричеством	Вероятно самый успешный проект в области «криптоэнергетики». Имеет около 100 партнеров. Но решение «проходит тестирование» с 2017 года.

Web 3.0

Storj	Децентрализованное, шифрованное облачное хранилище.	Собственно говоря, не вполне понятно где в решении «блокчейн», кроме того что в качестве оплаты принимается криптовалюта
Blockstack	Децентрализованный DNS для блокчейн приложений	К DNS, в принципе, отношения не имеет. Просто крипто-схема с красивыми бессмысленными словами в описании.

Цифровая демократия

Kaspersky	Блокчейн система голосования	Результаты применения оспаривались в судебных инстанциях. Т.е. доверия к системе не возникло только исходя из имманентных свойств блокчейна.

Решения для идентификации

SelfKey	Blockchain based self-sovereign identity system. Система управления персональными данными и идентификации на блокчейне.	Хотя «кошелек» для хранения персональных данных выпущен, основной бизнес компании - криптовалюта.
Zamna	Система идентификации. В 2021 объединена с системой информации о здоровье.	В текущем виде – идентификации + информации о здоровье, система предлагается для верификации туристов в аэропортах, для реализации карантинных ограничений. В настоящее время компания занимается «построением инфраструктуры».
Civic	Identity Verification. Система индетификации.	В настоящее время система нацелена на применение в области DeFi, т. е. не рассматривается за пределами криптовалютного рынка.

Разумеется, в таблице 1 не исчерпывается список проектов, считавшихся на момент выхода (иногда и считающиеся сейчас) «успешными». За пределами рассмотрения в данной статье остались Amazon Managed Blockchain, Telegram TON, национальная «криптовалюта» Венесуэлы Petro и многое другое.

Рассматривая многочисленные провалы и значительно меньшее количество относительно успешных внедрений, даже кратко рассмотрев Таблицу 1, можно сделать хоть и предварительный, но вполне однозначный вывод – успешное внедрение блокчейн (широком смысле) происходит только в тех областях, где до этого уровень цифровизации бил низкий, или отсутствовал вообще. Так, в морских перевозках, до настоящего времени контейнеры не отслеживались с помощью электронных средств, а сопровождающие документы были бумажные. Аккредитивы до недавнего времени, хоть и были в электронном (сканированном) виде, обрабатывались все равно вручную. Поэтому возникает вопрос – можно считать данные успешные кейсы примерами достоинств конкретной технологии блокчейн, или это пример успешной цифровизации? Второй, менее однозначный вывод, текущая пандемийная ситуации, стимулирует внедрение блокчейн. Но, опять-таки, во видимому в рамках общей стимуляции цифровых технологий во время пандемии [18], не конкретно технологических достоинств блокчейна.

Список использованных источников:

1. Тапскотт, А., Тапскотт, Д. Технология блокчейн: то, что движет финансовой революцией сегодня. – М.: ЭКСМО, 2017.

2. Iansiti, M., Karim, R. L. The Truth About Blockchain / Iansiti M., Karim R. L. // Harvard Business Review. – 2017. – Issue January-February. – URL: https://hbr.org/2017/01/the-truth-about-blockchain
3. Николаев, В.А., Селезнёв, В.М. Блокчейн и цифровое будущее. Обещания новой технологии против реальности / Николаев В.А., Селезнёв В.М. // АУДИТ. – №2. – 2019
4. Krylov, G.O., Seleznev, V. M. Current state and development trends of blockchain technology in the financial sector – DOI 10.26794/2587-5671-2019-23-6-26-35 / Krylov G.O., Seleznev V. M. // Finance: Theory and Practice. – 23(6). – 2019
5. Blockchain Market with COVID-19 Impact Analysis, by Component (Platforms and Services), Provider (Application, Middleware, and Infrastructure), Type (Private, Public, and Hybrid), Organization Size, Application Area, and Region - Global Forecast to 2026 [441 Pages Report] // Markets and Markets [сайт]. – 2021. – URL: https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html
6. Cryptocurrency across the world. Global crypto adoption // Triple A: [сайт]. – 2021. – URL: https://triple-a.io/crypto-ownership/
7. Leprince-Ringuet, D. Quantum computing is at an early stage. But investors are already getting excited / Leprince-Ringuet D. // Zdnet: [сайт]. – Sep15, 2021. – URL: https://www.zdnet.com/article/quantum-computing-is-at-an-early-stage-but-investors-are-already-getting-excited/
8. Bitcoin network power demand // University of Cambridge: [сайт]. – 2021. – URL: https://ccaf.io/cbeci/index
9. Semenova V. Technology adoption theories in examining the uptake of blockchain technology in the framework of functionalist and interpretive paradigms – DOI 10.14267/VEZTUD.2020.11.03 / Semenova V. // Budapest management review – 11. – 2020
10. Lustenberger, M. Ecosystem Readiness: Blockchain Adoption is Driven Externally – DOI 10.3389/fbloc.2021.720454 / Lustenberger M., Malešević S., Spychiger F. // Frontiers in Blockchain. – 16 Aug. – 2021
11. Clohessy, T. Antecedents of blockchain adoption: An integrative framework – DOI 10.1002/jsc.2360 / Clohessy T., Treiblmaier H., Acton T., Rogers N. // Strategic Change. – 2020. – 29. – 501-515.
12. Sanka, A.I. A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research – DOI 10.1016/j.comcom.2020.12.028 / Sanka A.I., Irfan M., Huang I., Cheung R.C.C. // Computer Communications. – 169. – 2021. – 179-201
13. Koens, T. Blockchain adoption drivers: The rationality of irrational choices – DOI 10.1002/cpe.5843 / Koens T., Aubel V.P., Poll E. // Concurrency and

Computation. – Volume 33, Issue 8 (Special Issue: 2018 ICCBB2018. KEIA2018. LSDVE2018. TACTS). – 25 April. – 2021
14. Allison I. IBM Blockchain Is a Shell of Its Former Self After Revenue Misses, Job Cuts: Sources / Allison I. // CoinDesk: [сайт]. – 14 Sep. – 2021. – URL: https://www.coindesk.com/business/2021/02/01/ibm-blockchain-is-a-shell-of-its-former-self-after-revenue-misses-job-cuts-sources/
15. Litan A. Microsoft ends Azure Blockchain Service; Where is Enterprise Blockchain heading? / Litan A. // Gartner blogs [сайт]. – 25 May. – 2021. – URL: https://blogs.gartner.com/avivah-litan/2021/05/24/microsoft-ends-azure-blockchain-service-where-is-enterprise-blockchain-heading/
16. Gerarg D. Libra Shrugged: How Facebook Tried to Take Over the Money. – UK. CreateSpace Independent Publishing Platform. – 2020
17. Anzalone R. GrainChain Goes Global On Symbiont's Blockchain. Small Farmers Are Signing Up. // Forbes [сайт]. – 27 Mar. – 2020. – URL: https://www.forbes.com/sites/robertanzalone/2020/03/27/grainchain-goes-global-on-symbionts-blockchain-small-farmers-are-signing-up/
18. Amankwah-Amoah J. COVID-19 and digitalization: The great acceleration – DOI 0.1016/j.jbusres.2021.08.011 / Amankwah-Amoaha J., Khan Z., Woo G., Knigh G. // Journal of Business Research. – Volume 136. – 202. – pp. 602-611

УДК 005.334:330.131.7

Проекты развития как инструмент нанесения ущерба национальной финансовой безопасности зарубежной страны

Д.Н. Осадчев
студент 2 курса аспирантуры Дипломатической академии
Министерства иностранных дел РФ
E-mail: daniil.osadchev@gmail.com
Научный руководитель: В.М. Грибанич
доктор экономических наук, профессор
E-mail: gribanich@rambler.ru

Аннотация: *в статье рассматриваются программы, направленные на оказание содействия международному развитию, которые могут быть прикрытием для продвижения национальных интересов страны. Автор разбирает примеры оказания помощи через межправительственные организации и в рамках двусторонних отношений. Выдвигает гипотезу того, что национальные системы ПОД/ФТ/ФРОМУ могут повысить общее качество оказания помощи в развитии.*

Ключевые слова: *содействие международному развитию; национальные системы противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения; национальная безопасность.*

Development projects as a tool for damaging national financial security of a foreign country

Abstract: *the article touches upon programs designed to boost international cooperation for development that can potentially occur as a pursue for national interests. The author analyses examples of aid via intergovernmental organisations and bilateral relations as well as suggest a hypothesis on a potential of national systems of combat against money laundering and terrorism financing being capable of improving the overall quality of international cooperation for development.*

Keywords: *international cooperation for development, national systems of combat against money laundering, financing terrorism, financing the distribution of mass destruction weapons, national security.*

В статье прежде всего речь пойдет о проектах развития в рамках, так называемого, «Содействия международному развитию» (далее – СМР). Использование термина СМР требует аккуратного подхода к его детерминации, так как его определение варьируется от страны или организации. Автором предложено рассматривать в статье термин СМР, как оказание помощи одним субъектом по отношению к другому, направленной на устойчивое социально-экономическое развитие субъекта-получателя помощи, урегулирование кризисных ситуаций, возникающих вследствие стихийных бедствий, техногенных катастроф и других чрезвычайных ситуаций, внутренних и (или) международных конфликтов путем технической, финансовой, гуманитарной и иной помощи. А также как один из механизмов решения глобальных и региональных проблем, противодействия новым вызовам и угрозам. Данный подход основывается на интерпретации СМР Российской Федерацией. За рубежом терминология СМР отличается амбивалентностью и как было ранее отмечено в разных государствах имеет различный смысл.

Первоначально политика содействия международному развитию проводилась более развитыми странами в отношении менее развитых. Основной целью такой политики являлась минимизация влияния последствий экономического отставания стран на развитие глобального сообщества и поддержание равномерного развития во всем мире. Под благой идеей развития общества со временем стали замечать наличие национальных интервенций в страны, которые получатели помощь по линии СМР. Такая помощь стала постепенно перерастать в неотъемлемый инструмент проведения внешней политики страны, оказывающей помощь, – страны-доноры помощи. Инструмент показал себя настолько хорошо, что со временем помощь по линии СМР начали предоставлять не только развитые экономики, но и развивающиеся. Тогда примерно и произошла переоценка и идейное изменение понимания оказания помощи в развитии.

Страны, увидевшие потенциал инструмента СМР раньше других, создали национальные институты, учитывающие национальные интересы страны-донора помощи. Национальные институты занимались согласованием интересов бизнеса, компаний оборонно-промышленного комплекса, неправительственных организаций, осуществляющих деятельность на территории страны, получающей помощь.

Развитие направления не ограничилось созданием двусторонних отношений между странами-донорами и странами-реципиентами помощи. Сфера СМР охватила такие организации, как «G20» («большая двадцатка»), «G7» («большая семерка» / «большая восьмерка»), «BRICS» («БРИКС») и т.п. В 1948 году создана «Организация экономического сотрудничества и развития» («ОЭСР», «OECD»), нацеленная на

координацию проектов экономической реконструкции Европы в послевоенное время.

Стоит отметить, что последние 10 лет соотношение оказанной помощи в двустороннем порядке по отношению к многостороннему способу составляет примерно 70:30. При определении направления оказания помощи можно выделить три общие цели, которые страны-доноры преследуют: 1) политические; 2) экономические; 3) гуманитарные.

Политические цели проявляются в усилении лояльности действующей власти страны, получающей помощь, или же наоборот в изменении правящего режима посредством поддержки оппозиционно настроенных групп. Вместе с тем встречаются политические мотивы, направленные на поддержание стабильности и безопасности страны-реципиента.

К экономическим мотивам можно отнести желание страны-донора выстроить торговые связи через страну-реципиента, получив тем самым дополнительный канал сбыта товара, конкурентное преимущество.

Гуманитарные цели направлены на улучшение качества жизни в стране, получающей помощь, поддержку близких в культурно-религиозном плане этно-конфессиональных групп.

СМР претерпевает изменения не только в интерпретации термина, но и в способах, критериях и формах оказания помощи. Начиная от помощи вооруженным силам стран-реципиентов, включая поставки военной техники и иной военной продукции до прямой поддержки бюджета, финансирования бюджетов организаций, целевых программ и фондов, проектного финансирования, предоставления экспертов, предоставления стипендий и других затрат на обучение студентов, облегчения бремени задолженности стран-реципиенты и пр.

Рассмотрим более подробно способы оказания помощи на примере конкретных проектов и организаций, занимающихся СМР.

Успешным примером оказания помощи через межправительственную организацию является программа «Продовольствие в обмен на работу». Программа нацелена на уязвимых и часто испытывающих нехватку продовольствия людей, живущих в неустойчивых, бедных ресурсами и сложных природных условиях, в районах, которые предрасположены к климатическим бедствиям и подвержены частым потрясениям.

«Продовольствие в обмен на работу» является инициативой Всемирной продовольственной программы Организации Объединенных Наций (ВПП ООН), направленная на предоставление неотложных потребностей в продовольствии при помощи денежных выплат, ваучеров и продовольственных пайков и в то же время программа нацелена на поощрение создания или восстановления активов, которые позволяют улучшить долгосрочную продовольственную безопасность и

устойчивость. С 2013 года программы в более чем 50 странах помогают 10–15 миллионам человек каждый год восстанавливать сотни тысяч гектаров деградировавших земель для их продуктивного использования, выполнять посадки тысяч гектаров леса, строить десятки колодцев, прудов и подъездных дорог и обучаться методам получения средств к существованию и ведения сельского хозяйства.

В качестве негативного примера стоит упомянуть недавние последствия оказания СМР США в качестве страны-донора при предоставлении помощи Афганистану. Ежегодно на протяжение почти двух десятилетий США тратили миллиарды долларов на военные операции, нацеленные на укрепления стабильности и мира в регионе, однако программа США не предусматривали каких-либо серьезных экономических вливаний в инфраструктуру. Прикрываясь идей поимки террористов, угрожавших национальной безопасности Америки, использовала только силовые инструменты. США удалось лишь частично реализовать свои цели. В 2013 году ненадолго вернув около 70 процентов территорий страны официальным властям. По разным источникам за все время в один момент на территории Афганистана находилось от 15 до 100 тысяч американских военных, большая часть из них была выведена, к началу 2021 года осталось 2500 солдат, в августе 2021 года был эвакуирован последний американский военнослужащий. Предстоит более детальный анализ проведенной политики по линии СМР США по отношению к Афганистану, но уже сегодня можно сделать вывод, что оказанная помощь негативно сказалась на благополучии региона.

Помощь может оказываться как напрямую, посредством открытия специальных счетов страной-реципиентом в стране-доноре помощи, так и опосредовано через бизнес, неправительственные организации и компании, созданные под реализацию конкретных проектов в стране, получающей помощь.

Разберем пример оказания помощи через многостороннюю организацию посредством специально открытой организации в стране-реципиента. Страна-донор помощи совершает перевод средств в форме целевого финансирования в межправительственную организацию, та в свою очередь переводить средства в неправительственную организацию (далее – НПО) для реализации гуманитарного проекта по оказанию помощи потерпевшим от техногенной катастрофы, которая в итоге и доведёт средства до пострадавших от катастрофы. С позиции страны-донора, канал доведения помощи является межправительственная организация, а для многосторонней организации этим каналом уже будет служить НПО. В такой цепочке существуют два риска. Первый связан с контролем доведения средств до конечного получателя в полном объеме, второй

касается качества помощи, предоставляемой НПО, пострадавшим от катастрофы. Если за первый риск ответственность несет межправительственная организация, то прозрачность исполнения своих обязательств НПО могут вызвать сомнения.

Национальные системы противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (далее – ПОД/ФТ/ФРОМУ) и механизмы, используемые системой, могут быть именно тем инструментом, который поможет повысить качество оказываемой помощи и прозрачность направляемых потоков средств на цели СМР.

Изучение вопроса спецификации ассигнования средств, направленных на цели СМР, занимает особое место у ученных всего мира. К примеру, одним из направлений изучения является анализ корреляции внешнеполитических и внешнеэкономических интересов стран доноров помощи через географическое распределение потоков помощи с применением эконометрических методов.

Автор выдвигает гипотезу того, что система ПОД/ФТ/ФРОМУ готова к внедрению в уже существующие институты СМР, а вместе с тем и создание собственных направлений СМР по оказанию помощи в странах-реципиентах по улучшению качества контроля за получаемой помощью и выявлению признаков интервенции со стороны страны-донора.

Так возможна интеграция имеющихся практик контроля за потоками средств в такие международные институты как Новый банк развития (НБР), ранее известный как Новый банк развития БРИКС («BRICS»), созданный государствами-участниками БРИКС (Бразилия, Россия, Индия, Китай и ЮАР). Цель Банка является финансирование инфраструктурных проектов и проектов устойчивого развития в государствах БРИКС и развивающихся странах. Через интеграцию существующих механизмов и при помощи экспертов из системы ПОД/ФТ/ФРОМУ Банк смог бы получить дополнительные инструменты контроля и мониторинга за качеством направления помощи. Страны, подключившиеся к работе по данному направлению, смогли бы поделиться своим опытом, который в дальнейшем можно было бы использовать непосредственно в странах-реципиентах.

Говоря про создание собственных направлений СМР через системы ПОД/ФТ/ФРОМУ, стоит отметить, что уже сегодня наработана серьезная практика такой работы. Так АНО «Международный Учебно-методический Центр Финансового Мониторинга» (далее – МУМЦФМ) занимается содействием профессиональному развитию специалистов по финансовому мониторингу через обучающие мероприятия для сотрудников надзорных

органов, осуществляющих деятельность в сфере ПОД/ФТ/ФРОМУ, тем самым повышает экспертный потенциал национальных антиотмывочных систем. Создаёт кадровый потенциал для национальных систем ПОД/ФТ/ФРОМУ посредством проведения Международной олимпиады по финансовой безопасности популяризация финансовую безопасность как норму жизни у молодежи нового типа мышления.

В рамках деятельности Совета руководителей подразделений финансовой разведки государств — участников Содружества Независимых Государств (далее – СРПФР) СРПФР совместно с МУМЦФМ, как базовой организации СРПФР, проводит аналитические исследования в рамках реализации проекта «Прозрачный блокчейн». Предоставляет доступ к системе «Прозрачный блокчейн», который позволяет странам выявлять новые методологии проведения финансовых преступлений в сфере криптовалюты.

Евразийской группой по противодействию легализации преступных доходов и финансированию терроризма (далее – ЕАГ) в рамках Рабочей группы по техническому содействию выявляются типологии оказания помощи и определяются направления для дальнейшего развития СМР в рамках антиотмывочных системы государств-участников ЕАГ.

Подводя итог стоит отметить, что оказание помощи тем, кто в ней нуждается путем создания достойных условий жизни, преодоление разрыва между разными странами в экономических, технологических, культурных сферах является неотъемлемой составляющей нашего развития, общей целью человеческой цивилизации.

СМР требует особого внимания со стороны национальных систем ПОД/ФТ/ФРОМУ, способных, объединив свои усилия, улучшить качество оказываемой помощи, тем самым повысить общий уровень развития мирового сообщества.

Список использованных источников:

1. Федеральный закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" от 07.08.2001 N 115-ФЗ.
2. Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента" от 20.07.2012 N 121-ФЗ.
3. Братко А. Г., Короткий Ю. Ф., Ливадный П. В. Финансовый мониторинг. Учебное пособие для бакалавриата и магистратуры. – М.: Юстицинформ, 2018. – 696.

4. Официальный сайт Организации экономического сотрудничества и развития (ОЭСР), 2021. – Режим доступа: https://oecdru.org, свободный.
5. Официальный сайт Базы данных российских экспертов для международного развития, 2021. – Режим доступа: https://expertsfordevelopment.ru, свободный
6. Официальный сайт Министерства финансов Российской Федерации, 2021. – Режим доступа: https://minfin.gov.ru/ru/perfomance/international/development/, свободный.
7. Официальный сайт Правительства Российской Федерации, 2021. – Режим доступа: http://government.ru/rugovclassifier/897, свободный.
8. Официальный сайт Министерства иностранных дел Российской Федерации, 2021. – Режим доступа: https://www.mid.ru/foreign_policy/official_documents/asset_publisher/CptICkB6BZ29/content/id/64542, свободный.
9. Официальный сайт Научно-исследовательского финансового института Минфина России, 2021. – Режим доступа: https://www.nifi.ru/images/FILES/Journal/Archive/2019/1/statii/fm_2019_1_08.pdf, свободный.
10. Официальный сайт «Wiley Online Library», «Will ‘Emerging Donors’ Change the Face of International Co-operation» 2021. – Режим доступа: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-7679.2006.00330.x, свободный.
11. Официальный сайт «Global Financial Integrity», «Financial Crime in Latin America and the Caribbean» 2021. – Режим доступа: http://www.gfintegrity.org/reports, свободный.
12. Официальный сайт International Monetary Fund, «Financial sector assessment program financial system stability assessment» 2021. – Режим доступа: http://www.imf.org/external/pubs/ft/scr/2016/cr16167.pdf, свободный.
13. Официальный сайт Oxford Bibliographies, 2021. – Режим доступа: https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0040.xml, свободный.
14. Официальный сайт Организации Объединенных Наций, 2021. – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/decade2_devstrategy.shtml, свободный.
15. Официальный сайт Организации Объединенных Наций, 2021. – Режим доступа: https://www.un.org/en/development/desa/policy/mdg_gap/mdg_gap2012/mdg8report2012_ruw.pdf, свободный.

УДК 37.014:004

Роль обучения параллельным вычислениям в базе данных в подготовке специалистов ИТ-профиля

М. Серік
д.п.н., профессор ЕНУ им.Л.Н.Гумилева, Нур-Султан
С.К. Жумагулова
докторант 2 года обучения ЕНУ им.Л.Н. Гумилева, Нур-Султан
E-mail: saulesha_81@mail.ru
Д.А. Казимова
к.п.н., доцент Карагандинского университета им.Е.А.Букетова
Караганда

Аннотация: *в статье исследуются ключевые вопросы обучения реализации параллельных вычислений в базе данных в образовательном процессе. В результате активного развития параллельных вычислений возникает необходимость формирования у обучающихся навыков параллельного программирования. Разработка и внедрение в образовательный процесс методики обучения реализации параллельных вычислений в базе данных даст возможность обучающимся получить умения и навыки параллельной обработки масштабной информации базы данных за короткий интервал времени.*

Ключевые слова: *базы данных, параллельные вычисления, образовательный процесс, информационные технологии, методология*.

The role of parallel computing training in the database in the training of IT specialists

Abstract: *the article examines the key issues of teaching the implementation of parallel computing in a database in the educational process. As a result of the active development of parallel computing, there is a need for purposeful formation of appropriate skills among students. The development and introduction into the educational process of the methodology of teaching the implementation of parallel computing in a database will enable students to acquire the skills and abilities of parallel processing of large-scale database information in a short period of time.*

Keywords: *databases, parallel computing, educational process, information technology, methodology*.

Множество программных проектов от самого разного рода предприятий сегодня активно применяют системы управления базами данных (СУБД). Сегодня огромное разнообразие СУБД может удовлетворить различные потребности в сфере обработки данных. Как свидетельствуют данные организации по сбору и представлению информации о СУБД различных парадигм DB-Engines и каждый месяц публикующей результаты исследований популярности СУБД, хотя в настоящее время растут потребность в NoSQL- и NewSQL-баз данных, пальмой первенства по использованию как и прежде удерживают реляционные базы данных (БД) [1].

Реляционные БД с успехом решают свои основные задачи, такие как:

- хранение новых записей;
- считывание данных;
- поиск информации;
- защита информации от несанкционированного применения.

Но одновременно с этим в результате роста объема данных большинство реляционных БД сталкиваются с проблемой низкой скорости считывания данных. Глобальным решением даннной проблемы стало использование в базе данных параллельных вычислений.

Основой параллельных вычислений является ахитектура современных мультизадачных процессоров, в которых ядро способно реализовывать ряд операций (потоков вычислений) паралелльно. В результате стоит сложная задача распределения и координации данных потоков для оптимизации осуществления задач, которые возложены на БД.

Среди важнейших задач БД являются:

- обеспечение одновременного доступа множества пользователей;
- обеспечение ранжирования доступа к данным согласно правилам и обеспечение безопасности для самой БД и для ее пользователей;
- обеспечение масштабируемости (возможность доставки новых серверов либо карт памяти без необходимости при этом переписывать архитектуру либо изменять функции доступа к БД);
- распределение протоколов обмена данными и разделения задач между отдельными процессорами и потоками вычислений.

Благодаря СУБД можно эффективно хранить данные, а также использовать данные внутри организации в режиме совместного доступа. Среду СУБД состаляют разработчики, системные администраторы и непосредственно пользователи. Она также содержи такие компоненты, как оборудование, данные, программное обеспечение, процедуры. К одним и тем же данным БД имеют оперативный доступ двое и больше пользователей без каких-либо дополнительных усилий. Система позволяет осуществить поиск необходимых данных в масштабной БД всего за

несколько мгновений. Применение СУБД целесообразно в целях организации разного рода типов данных, к примеру записи о персонале, инвентаре и пр.[2]

В целом, параллельные вычисления представляют собой реаизацию больших масштабных вычислений, а также обработку в параллельном режиме большого объема данных за весьма короткий временной интервал.

Использование параллельных вычислительных систем представлет собой стратегическое направление развития аппаратного обеспечения, что возникло в результате ограничения максимально возможного быстродействия обычных последовательных машин, а также почти регулярным наличием вычислительных задач, для решения которых недостаточно возможностей имеющихся средств аппаратного обеспечения.

Однако важно отметить отсутствие распространенности применения параллелизма. Причиной такой сложившейся ситуации можно назвать достоаточно недешевую стоимость высокопроизводительных систем.

Основную роль в научно-методических исследованиях играют параллельные вычисления в базах данных. В связи этим возникает необходимость во внедрении в образовательный процесс высшего учебного заведения для подготовки будущих специалистов ИТ-профиля. К тому же сегодня параллельные вычисления становятся обязательной частью содержания дисциплин программирования и информатики.

Технология параллельного программирования способна в занчительной мере изменить алгоритмическую деятельность специалиста ИТ-профиля.

Помимо способов создания программы, программирование с помощью параллельной технологии способно также менять мыслительную деятельность человека путем формирования параллельного стиля мышления. Кроме того, сформированный параллельный стиль мышления позволяет человеку получить навыки параллельной обработки данных и написания программ с параллельным алгоритмом.

Учитывая вышесказанное, имеет смысл выделять программирование БД как отдельное направление подготовки. Они крайне востребованы, круг их задач специфичен, уникален и требует определенного набора компетенций и знаний, имеющих отличия от прочих областей прикладного программирования. Данная область активно развивается и необходима специализация в ней для того, чтобы успевать за темпом технологических изменений и новыми решениями.

К обучающимся образовательных программ ИТ-профиля в числе других предъявляются следующие требования, представленные на рисунке 1.

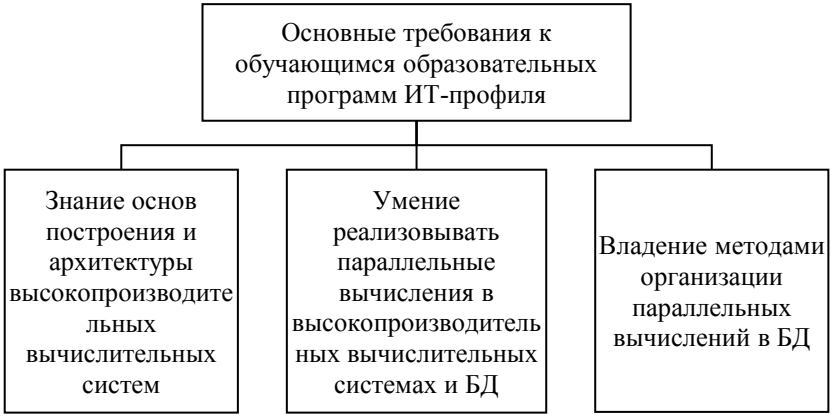

Рисунок 1 – Основные требования к обучающимся образовательных программ ИТ-профиля

Таким образом, неотъемлемыми условиями формирования предметной компетенции обучающихся ИТ-профиля и приоритетными квалификационными характеристиками современного ИТ-разработчика служат знание актуальных тенденций развития высокопроизводительных систем для достижения параллелизма, а также способность писать программы параллельной обработки данных в БД.

Но к моменту изучения обучающимися параллельного программирования в БД они испытывают сложность в понимании данного направления, так как данный вид программирования в корне отличается от привычных методов структурного программирования.

Авторские труды К.Ю. Богачева, С.А. Лупина и др. освещают вопросы методики преподавания параллельных вычислений в вузах. В них отмечено, что изучение обучающимися параллельного программирования является сложной дидактической педагогической проблемой, причиной этого можно назвать его непосредственное влияние на формирование их мировоззрения и мыслительной деятельности. Лишь при условии наличия сформулированного стиля мышления человек может научиться выполнять параллельную обработку данных и создавать программное обеспечение для суперкомпьютерных систем.

Параллельный стиль мышления являет собой способ алгоритмической мыслительной деятельности, позволяющий строить параллельный алгоритм [3].

Освоение новой технологии параллельных вычислений в системе подготовки будущих специалистов ИТ-профиля способствует возникновению вопросов относительно специфики методики преподавания параллельных вычислений в БД.

Таким образом, сегодня можно вести речь о недостаточном уровне педагогического и методического изучения этой проблемы в общем, и для вузов в частности.

Сложность организации взаимодействия параллельных процессов в базе данных, а также сопутствующие ей информационные процессы свидетельствуют о целесообразности выбора информационного подхода к обучению в качестве основы для разработки методической обучающей системы будущих специалистов ИТ-профиля параллельным вычислениям в базе данных [4].

Ниже приведены противоречия, подтверждающие актуальность данного исследования:

- противоречия между требованиями информационного общества к формированию параллельного стиля мышления будущих специалистов ИТ-профиля, и недостаточным уровнем практической и теоретической базой исследований в указанной сфере;
- противоречия между целесообразностью внедрения в вузах в подготовку будущих специалистов ИТ-профиля курсов параллельного программирования в базе данных и тем фактом, что для подобной подготовки отсутствует конкретная методическая система;
- противоречия между возможностью формирования параллельного стиля мышления студентов в ходе изучения параллельных вычислений и тем фактом, что сегодня отсутствуют методы и способы достижения требуемого уровня формирования параллельного стиля мышления обучающихся [5].

Все изложенные противоречия характеризуют проблему исследования, суть которой заключается в определении методической системы обучения обучающихся параллельному программированию в базе данных, способствующей формированию параллельного стиля мышления в процессе предметной подготовки в вузе.

Можно заключить, что обучающиеся вузов приобретут параллельный стиль мышления, а также смогут успешно усвоить материал в области вычислительных технологий при условии присутствия в методической системе обучения параллельным вычислениям в базе данных понятия параллельных вычислений, определения этапов его формирования, осуществления анализа программно-технического обеспечения реализации параллельных вычислений в базе данных, а также наличия разработанных

методик обучения реализации параллельных вычислений в базе данных в вузах.

Список использованных источников:

1. Богачев К.Ю. Основы параллельного программирования. - М.: БИНОМ. Лаборатория знаний, 2003.-127с.
2. Лупин С.А., Посыпкин М.А. Технологии параллельного программирования. Серия: Высшее образование. - М.: Форум, Инфра-М, 2008. - 208 с.
3. Миллер Р., Боксер Л. Последовательные и параллельные алгоритмы: Общий подход. - М.: БИНОМ. Лаборатория знаний, 2006. - 406 с.
4. Немнюгин С.А., Стесик О.Л. Параллельное программирование для многопроцессорных вычислительных систем - СПб.: БХВ-Петербург, 2002. - 400 с.
5. Носов М.Т., Ерахтин В.М. Параллельные вычисления. Основы параллельного программирования. М.: Форум, Инфра-М, 2011. - 277 с.

УДК 007.52:004:330.4

Роль роботизации в цифровой экономике

А.Р. Азизова
студентка 4 курса НИЯУ МИФИ, Москва
E-mail: amina.rust01@gmail.com

Аннотация: *данная статья описывает важное направление в развитии цифровой экономике – роботизацию. А также ее важность в эпоху цифровой трансформации.*
Ключевые слова: *роботизация бизнес-процессов, цифровая экономика, автоматизация, оптимизация, цифровая трансформация, цифровые технологии.*

The role of robotics in the digital economy

Abstract: *this article describes an important area in the development of the digital economy – robotics. Moreover, it is about its importance in the era of the digital transformation.*
Keywords: *RPA, digital economy, automation, optimization, digital transformation, digital technology.*

Первоначально экономика зародилась еще до нашей эры. Тогда она была представлена в виде бартера или натурального обмена, то есть обмене одного товара на другой без использования денежных средств. По мере развития экономических отношений потребовались изменения и улучшения. После чего были изобретены товарные деньги, которые представляли из себя товар, который мог быть использован в хозяйстве. Это были, например, скот или зерно. На следующем этапе развития в торговле стали использовать драгоценные металлы и монеты. И уже после этого появились первые денежные купюры.

Этапом начала цифровой экономики считается появление денежных купюр с указанием цифрового номинала. Следующие изменения цифровая экономика начала претерпевать с момента появления различных цифровых технологий, компьютеров, интернета, мобильных устройств.

Понятие «цифровой экономики» было введено в 1995 года Д.Тапскоттом. Цифровая экономика – совокупность экономических отношений, основанных на использовании электронных технологий.

Для полного рассмотрения данной темы необходимо оценить важность роботизации в цифровой экономике.

При рассмотрение вышеперечисленного необходимо решить главные вопросы этой темы, а именно:

– Оценить выгоды для цифровой экономики от технологий RPA,
– Выявить преимущества и недостатки роботизированных технологий в эпоху цифровой трансформации.

В процессе исследования применяются следующие методы:

1. Сбор и анализ данных,
2. Сравнение статистических показателей.

Цифровые технологии также по-другому называются сквозными. К ним мы относим: квантовые технологии, большие данные, технологии беспроводной связи, робототехнику, нейротехнологии и искусственный интеллект.

Данные направления стали главными катализаторами цифровой трансформации. В результате чего, все больше инвестиций идут на данные направления. Согласно расчетам ИСИЭЗ НУ ВШЭ была определена следующая динамика затрат.

Рисунок 1 – Динамика затрат на новые и традиционные ИКТ в мире

В настоящее время цифровизация проникла во все сферы экономики: промышленную, сельскохозяйственную, медицину, бизнес, образование.

Выделяются следующие показатели в ходе реализации цифровой трансформации:

1. Увеличение доступных услуг в электронном виде,
2. Увеличение доли рынка,

3. Рост выручки и сокращение затрат,
4. Повышение удовлетворенности клиентов.

Преимущества реализации цифровой трансформации:

1. Позволяет принимать более взвешенные и оперативные решения. При этом данные решения опираются на быстро изменяющиеся требования клиентов.
2. Повышение производительности с помощью автоматизации наиболее важных процессов. Помимо этого, цифровая трансформация позволяет работать в удаленном режиме.
3. Вовлеченность клиентов. Цифровая трансформация позволяет поддерживать активные отношения с потребителями.
4. Обеспечение информационной безопасности. Обычно при работе с цифровыми системами прибегают к специалистам по кибербезопасности.
5. Укрепление партнерских отношений. Цифровая трансформация также позволяет поддерживать гибкие отношения с партнерами.
6. Развитие услуг по требованию достигается с помощью использования гибких ИТ-технологий.

Рассмотрим подробнее проблемы и перспективы цифровой трансформации. Очевидно, что уровень цифровизации страны влияет на ее конкурентоспособность. Поэтому цифровая трансформация является приоритетным направлением в России на сегодняшний день. Так в 2016 году президентом был подписан указ в рамках «Стратегии научно-технического развития РФ». Данный указ предусматривает создание правовых, технический, финансовых и организационных условий, способствующих развитию цифровой экономики в России. А уже в июле 2017 году была утверждена программа «Цифровая экономика РФ». Данная программа определяет комплект целей и задачей, а также стратегию планирования научно-технического развития РФ на 2017-2030 года.

Одним из направлений цифровой экономики является робототехника. Робототехника – это наука, занимающаяся созданием автоматизированных технологий (роботов). Робот – это запрограммированное устройство, выполняющее механические и рутинные процессы без участия человека.

В начале роботизация процессов на предприятии охватывала преимущественно производственные процессы, но сейчас данные технологии все больше проникают в сферы финансов и управления, а также в сферу работы складов.

На данных момент роботизация бизнес-процессов является популярным и перспективным направлением.

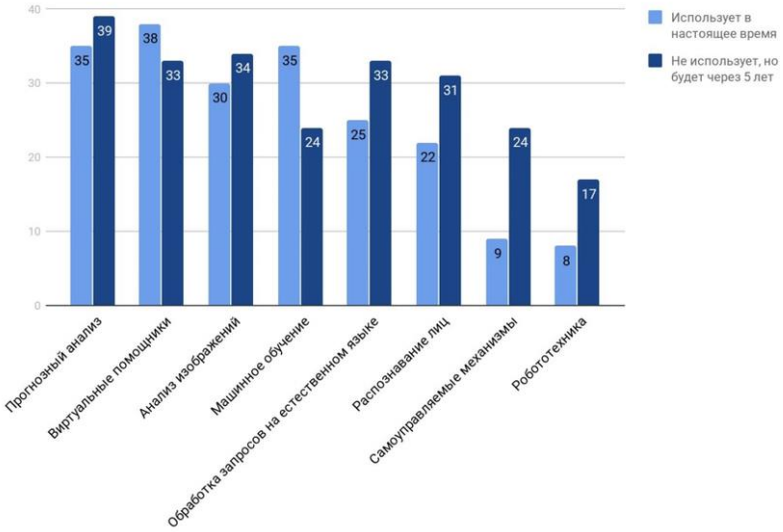

Рисунок 2 – Процент использования сквозных технологий в настоящее время и перспективы использования на будущее

Мы можем заметить, что робототехника охватывает самый низкий процент использования на сегодняшний день. Причиной этому может служить боязнь изменений и недостаточная осведомленность о преимуществах данных технологий со стороны организаций.

Главным отличие применения робототехники на предприятии от других направлений развития цифровой экономики является то, что данных технологии накладываются на уже существующую структуру, не изменяя ее работу. То есть технологии RPA является виртуальным сотрудником, выполняющим нужные действия в системе вместо человека. Данное преимущество, позволяет легко оценить экономическую эффективность и быстро получить отдачу.

Лидирующие отрасли применения роботизированных технологий: финансовая сфера, энергетика, промышленность, логистика.

Теперь рассмотрим немного статистических данных в данной сфере.

Экономия затрат на поддержание функционирования деятельности предприятия при использовании роботов на предприятии может широко варьироваться от 15 до 90%.

Главным индикатором рынка робототехники является плотность роботизации, то есть количество роботов на 10 000 занятых работников. По данным 2021 года, в России в 2020 году на 10 000 работников приходилось лишь 5 роботов.

Согласно данным Фонда развития интернет-инициатив, в 2020 году число компаний, которые используют цифровую трансформацию в своих организациях возросло с 25% до 48%. А также выросло и применение цифровых технологий в организациях на 38%.

Если сравнить популярность роботизации бизнес-процессов в России и на мировом рынке. То на начало 2021 года 42% организаций уже внедрили данные технологии на свое предприятие, а на мировом рынке этот показатель составляет 53%. Таким образом, мы можем сделать вывод, что Россия не отстает от тенденций мирового рынка и догоняет его.

Рассмотрим основные преимущества использования роботизации для цифровой экономики.

1. Повышение скорости выполнения задач и принятия решений.
2. Те предприятия, которые имеют высокий уровень цифровизации, явно имеют высокое конкурентное преимущество.
3. Внедрение технологий RPA на предприятии позволяет повысить качество производимого товара или оказываемой услуги, снизить количество ошибок, исключить влияние человеческого фактора, а также повысить производительность.
4. Высокий спрос к технологиям RPA обеспечивается за счет их высокой гибкости. Данные решений делаются очень быстро и легко поддаются изменениям, что крайне необходимо в текущей неустойчивой экономической ситуации. Если говорить о средней длительности внедрения данных технологий на предприятии, то обычно это занимает 4-6 недель.

Рассмотрим немного подробнее поэтапное внедрения технологий RPA:

На первой стадии, как и в любом проекте выполняется сбор и анализ требований. После этого внедряются поэтапные изменения, затем выявляется результат проделанной работы, анализируется и оценивается. И уже в заключении, происходит автоматизация бизнес-процессов на уровне всего предприятия.

5. Более того, в настоящее время роботам вводятся элементы искусственного интеллекта, что позволяет роботизированной технике работать более эффективно.

Цифровая трансформация различных предприятий помимо наличия широкого спектра преимуществ, также имеет и свои недостатки.

1. Одним из них является сокращение рабочих мест и доходов, то есть безработица. Но это мнение можно считать ошибочным, потому что

внедрение роботизированных технологий на предприятие, повлечет за собой создание новых рабочих мест. Это будут различные ИТ-специальности, отслеживающие деятельность роботов.

2. Помимо этого, процесс автоматизации бизнес-процессов посредством их роботизации требует достаточных временных и денежных ресурсов. Но несмотря на это, отдачу инвестиций можно получить в достаточно короткий срок.

Что же мешает развитию роботизации в России? Прежде всего, это наличие большого количества дешевой рабочей силы, а также недостаток квалифицированных кадров по обучению работе с роботизированной техникой. Но стоит отметить, что это не снижает интерес к данным технологиям со стороны организаций.

Цифровая трансформация также затрагивает трансформацию роботов, выполняющих рутинные и механические процессы к созданию интеллектуального робота, которому будут внедрены аналитические инструменты.

Рисунок 3 – Цифровая трансформация роботов

Рассмотрим этапы перехода от обычного робота до интеллектуального.

На первом этапе робот выполняет рутинные операции на предприятии без вмешательства человека. Сюда мы может отнести копирование данных, форматирование и проведение элементарных математических подсчетов. Данные роботы помогают избежать найма дополнительного персонала для выполнения данных операций или дополнительной загрузки уже существующего персонала.

На следующем этапе работа робототехники осуществляется с помощью человека. К таким операциям мы уже можем отнести сверка данных, изменение, поиск данных в нескольких системах одновременно, а также

копирование и перенос данных из одной системы в другую. В данной ситуации человек помогает системе инициировать работу.

На третьем этапе робот способен динамически маршрутизировать коммуникации с клиентами.

И на заключительном этапе используются технологии искусственного интеллекта. С помощью него роботы смогут работать с большим массивом данных и предлагать решения, учитывая все множество существующих факторов.

Какое будущее можно ожидать с использованием роботизированных технологий? Во-первых, очевидно, что большинство рабочих мест будет сокращено. Но несмотря на это, будут популярны различные аналитические профессии, а также профессии, связанные с разработкой и поддержанием технологий RPA. Из этого можно сделать вывод, что люди больше не будут конкурировать из-за заработной платы, так как главными конкурентными преимуществами станут креативность и знания.

В заключении еще раз отметим, что роботизированные технологии являются важной частью цифровой экономики. Подтверждением этому могут служить рассмотренные выше выгоды для бизнеса от роботизации бизнес-процессов на предприятии.

Список использованных источников:

1. Карпов, В.К. (2017). Роботизация и ее место в цифровой экономике.
2. Бондаренко, В.М. (2008). Мировоззренческий подход к формированию, развитию и реализации «цифровой экономики». Современные информационные технологии и ИТ-образование.
3. Джон Будро, Р. Д. (2019). Реинжиниринг бизнеса: Как грамотно внедрить автоматизацию и искусственный интеллект. Москва: альпина паблишер.
4. Бьёрн, А. (2003). Бизнес-процессы. Инструменты совершенствования. Москва: РИА «Стандарты и качество».
5. Каргина, Л.А. (2020). Цифровая экономика. Москва: Прометей.
6. Фонд Развития Интернет-Инициатив (ФРИИ): https://www.iidf.ru/.
7. Институт статистических исследований и экономики знаний (ИСИЭЗ):https://issek.hse.ru/.

УДК 004.45:005.934:336.77

Применение отдельных методов деревьев решений для выявления неблагонадежных кредитных организаций - субъектов бюджетного процесса

Н.Л. Меньшиков
аспирант 3 курса аспирантуры НИЯУ МИФИ, Москва
E-mail: nick.menshikov@yandex.ru
В.Ю. Радыгин
к.т.н., доцент кафедры «Финансовый мониторинг»
НИЯУ МИФИ, Москва
E-mail: vyradygin@mephi.ru
Н.С. Приказчикова
Главный специалист-эксперт Управления развития информационных технологий Федеральной службы по финансовому мониторингу
В.В. Иванов
д.ф-м.н., профессор кафедры прикладной математики №31 института лазерных и плазменных технологий
НИЯУ МИФИ, Москва

Аннотация: *предложения по применению методов машинного обучения в целях идентификации девиантной деятельности кредитных организаций, вовлеченных в противоправную деятельность по легализации преступных денежных средств и финансированию терроризма.*

Ключевые слова: *управление рисками; использование методов машинного обучения; выявление рисков в кредитно-финансовой сфере; машинное обучение; дерево решений; кредитные организации – участники бюджетного процесса;*

System analysis and credit institutions deviant activities identification in Rosfinmonitoring objectives

Abstract: *proposals are given on the use of machine learning methods in order to identify deviant activities of credit institutions involved in illegal activities related to money laundering and terrorist financing.*

Keywords: *management of risks; machine learning methods application; identification of risks in the credit and financial sector; machine learning; decision tree.*

Введение

Актуальность данной работы обуславливается необходимостью разработки новых методик и алгоритмов обнаружения потенциально проблемных кредитных организаций, использующих финансовую систему России для легализации полученных преступным путем денежных средств.

Внедрение информационных технологий в информационное обеспечение деятельности аналитических подразделений, позволяет формировать основания для первичного анализа имеющейся информации.

Поскольку в части минимизации финансовых рисков, при исполнении государственных контрактов необходимо проверять и исследовать информацию, содержащуюся непосредственно в самих операциях, то главной задачей выступает поиск нарушений норм права, основанный на расчете взаимосвязанных показателей с целью выявления несоответствий.

Управление рисками, возникающими в ходе исполнения государственных контрактов, является одной из важнейших задач минимизации финансовых потерь. При этом характер риска определяет и способ возможного управления им.

Оценку рисков необходимо начинать с выбора тех принципов, которые могут обеспечить системный и непрерывный анализ риск-носителя. Первостепенными являются вопросы выбора методов анализа и показателей характеризующих риск. Показатели, применяемые для оценки риска должны не только адекватно отражать размер риска, но и подвергать оценке факторы на него влияющие.

Модели машинного обучения могут упростить процедуры принятия решений в части минимизации рисков, например:

- принятие решений о инициации проверочных мероприятий в отношении организаций на основе скоринга;
- установление риск-лимитов в отношении заемщиков или контрагентов;
- оптимизация условий предоставления бюджетного финансирования;
- портфельное моделирование в целях построения прогноза денежных потоков;
- оценка дефолтности пула активов на основе индивидуального анализа входящих в его состав кредитов;
- риск - оценка контрагентов на предмет вероятности невыполнения обязательств по контрактам;
- интеграция используемых методологий, моделей и экспертных систем в процедурах управления рисками.

Работа нацелена на оценку участников бюджетного процесса, далее рассматриваются кредитные организации, вовлечённые в этот процесс.

Учитывая, что машинное обучение основано на выявлении эмпирических закономерностей в данных, его алгоритмы противопоставляют модели, разработанные с его применением тем экспертным системам, которые создаются на основе накопленных знаний и суждений. Учитывая то, что различные модели имеют разное целевое назначение, то спор об эффективности каких-то конкретных моделей не возникает, поскольку одна модель может дополнять другую, а итоговый результат применения модели скорее всего будет разный.

Учитывая вышеизложенные требования, может возникнуть риск встретить следующие проблемы при формировании выборки.

Во-первых, сведения могут быть нерелевантны для обучения модели в рамках решения поставленных задач.

Во-вторых, на этапе классификации наблюдений может возникнуть неоднозначность при даже в отношении такого признака как факт дефолта. Зачастую банки в целях прибегают к реструктуризации проблемных кредитов во избежание моментального дефолта заемщика с целью его отсрочки на период, когда банк с позиции своих финансовых показателей будет готов абсорбировать стресс капитала и финансового результата при отражении потерь. Данное наблюдение не будет классифицировано как дефолт и отражено в отчетности кредитной организации. Данный факт может свидетельствовать о том, что правила фиксации фактов дефолтов должны быть расширены относительно применяемых на текущий момент времени для формирования отчетности. Следует уточнить, что вынужденные реструктуризации в приведенном выше примере стоит учитывать, как факты дефолта. Вместе с тем, не факт, что накопленная статистика может быть релевантна для обучения модели в соответствии с поставленными задачами.

В-третьих, рассматриваемая задача систематизации и интерпретации накопленных данных может представляться сложно реализуемой при отсутствии соответствующего опыта и инструментов обработки, но в случае использования необработанных данных результат может оказаться довольно неожиданным, и не соотносящимся как с ожиданиями разработчиков. Затем, в целях обкатки используемой модели, она должна пройти процедуру валидации на тестовой выборке. Важно чтобы тестовая выборка была отличной от обучающей, иначе в ходе реализации этого этапа все перечисленные выше трудности могут возникнуть. Зачастую, валидация проводится в регулятивных целях в тех случаях, когда применение модели и ссылающиеся на нее внутренние документы должны быть согласованы Банком России. Вместе с тем, процедуры разработки и

валидации должны быть достаточно автоматизированы, что бы модель можно было дообучить с учетом актуальной статистики.

Обозначенные проблемы, связанные с формированием выборок и разработкой моделей, не являются свидетельством того, что эти проблемы будут недоступны небольшим кредитным организациям. Обучающая выборка не обязательно формируется на основе статистики кредитного учреждения, вероятно, но и открытые сведения о финансовых результатах иных кредитных организаций также могут быть использованы.

Так, в качестве методов машинного обучения были использованы наиболее распространенные методы деревьев решений.

Модели деревьев решений служат для создания систем классификации на основе набора решающих правил. Если данные возможно разделить на классы, то можно применить существующие данные для создания правил классификации как старых, так и новых наблюдений с довольно высокой точностью. Например, построить дерево для классификации кредитных рисков.

Этот процесс содержит в своих правилах лишь те атрибуты, которые действительно важны для принятия решения, а атрибуты не вносящие значения в точность дерева игнорируются. Это дает возможность сократить данные до необходимых полей, перед тренировкой других методов обучения, например, нейросеть.

Модель дерева решений может быть переведена в набор правил IF-THEN, которая в некоторых случаях предоставляет информацию в более понятной форме.

Алгоритмы построения дерева

Для проведения классификационного анализа, а также в целях сегментации, доступны некоторые алгоритмы, просматривающие все поля из списка данных для поиска того поля, которое даст лучшую классификацию или наилучший прогноз путем разделения данных на подгруппы. Этот процесс используется рекурсивно и подгруппы разделяются на все меньшие, меньшие блоки, пока деревья не будут завершены. Поля назначения, а также поля входа, применяемые при построении дерева, могут быть как непрерывными, так и категорийными, исходя из используемого алгоритма. Если поле назначения непрерывно, генерируется дерево регрессии; если же поле назначения категорийное, генерируется дерево классификации.

Узел дерева классификации и регрессии C&R генерирует деревья решений, которые могут классифицировать и предсказывать наблюдения. Метод применяет рекурсивное разделение для разделения обучающих записей на сегменты - узел дерева считается чистым, если 100% записей в дереве находится в определенной категории поля назначения.

Поля назначения, а также входные поля, могут быть в числовом диапазоне, так и категориальными, а все расщепления - бинарны.

Узел CHAID генерирует деревья решений с помощью статистики статистику х-квадрат чтобы определить оптимальные расщепления. В отличие от узлов дерева C&R и QUEST, CHAID может создавать не только бинарные деревья, т.е. некоторые расщепления могут иметь более двух ветвей в некоторых случаях. Поля входа и поля назначения могут быть количественными (числовой диапазон) или категориальными. Исчерпывающий CHAID - это модификация метода CHAID, в которой проводится более подробная работа по изучению всех возможных расщеплений для каждого предиктора, но для вычисления требуется больше времени.

Ниже приведено несколько общих методов использования анализа на основе деревьев:

Сегментация: Идентификация тех, кого можно отнести к определенной группе.

Стратификация: Назначение наблюдений в одной из категорий, например, в группу высокого, среднего или низкого риска.

Предсказание: Создание правил и использование их в предсказаниях будущих событий. Прогнозирование также может означать попытку связывать предсказываемые атрибуты со значениями определенных непрерывных переменных.

Сокращение данных и экранирование переменных: Выбор полезных подмножеств предикторов из перечня переменных, которые могут использоваться при создании формальных параметрических моделей.

Идентификация взаимодействия: Идентификация связей, принадлежащих к определенной группе, а также указание их в формальной параметрической модели.

Изменение категорий, дискретизация непрерывных переменных: Процесс перекодирования категорий предикторов групп и непрерывных переменных с минимальными потерями информации.

Аналитики Росфинмониторинга в своей работе сталкиваются с большими объемами данных, что с одной стороны является преимуществом, а с другой – недостатком в части отсутствия у сотрудников понимая, как обрабатывать имеющиеся в их распоряжении данные.

В связи с чем была поставлена задача разработки алгоритма обработки массива данных и одновременно генерации правил классификации объектов исследования с целью установления их финансовой устойчивости и возможного риска отзыва лицензии.

Проанализировав разные модели классификации объектов анализа, было принято решение о рациональности использования моделей CHAID и дерева C&R, так как их общая точность (согласно результатам обработки данных в SPSSModeler) составила 69,6 и 68,7 соответственно.

Этапы обработки данных, доступных для использования аналитикам Федеральной службы по финансовому мониторингу

1. В Единой информационной системе финансового мониторинга содержится более 150 показателей финансовой деятельности кредитных организаций. Рассмотрим выборку данных за период 7 лет с 2013 по 2020 годы. Выборка состоит из 923 субъектов.

В ходе анализа показателей были обнаружены мало заполненные показатели, произведено их удаление, после чего выборка сократилась до 92 единиц.

2. С оставшимися показателями проведен корреляционный анализ, в результате выявлена сильная взаимная корреляция между отдельными показателями.

3. Так как показателей много и отдельные из них сильно коррелированы является целесообразным снизить признаковое пространство с использованием факторного анализа при этом главные компоненты станут ортогональными.

4. Реализуем факторный анализ после автоматической подгонки данных в IBM SPSS Modeler, которая включает шаги.

а) Исключили номинальные поля со слишком большим количеством уникальных значений
б) Исключили категориальные поля со слишком большим количеством значением в одной категории
в) Заменили пропущенные значения средним значением
г) Все количественные поля приведены к одной общей шкале (где среднее значение = 0, стандартное отклонение = 1).

5. С использованием функционала IBM SPSS Modeler из общей совокупности исходных данных методом главных компонент факторного анализа были выделены 17 главных компоненты (общая дисперсия = 80 %).

6. В ходе интерпретации главных компонент (факторов) были сделаны следующие выводы:

1 внутренний фактор – включает в себя всевозможные внутренние и внешние операции банка (расходные и приходные) внутри страны и зарубежом, в том числе подозрительные операции с точки зрения места их совершения и клиентуры, а также операции, информация о которых возможно не представлена в Росфинмониторинг (общий интегральный показатель).

3 внутренний фактор – содержит показатели, которые характеризуют операции банка как сомнительные, а также указывают на обслуживание банками лиц, признанных ЦБ России и Росфинмониторингом фиктивными.

Причем установлено следующее, чем больше значение 3 фактора, тем больше риск отзыва лицензии у кредитной организации.

7. Визуализируем кредитные организации на декартовой плоскости, образованной парами главных компонент (Рис. 1-3).

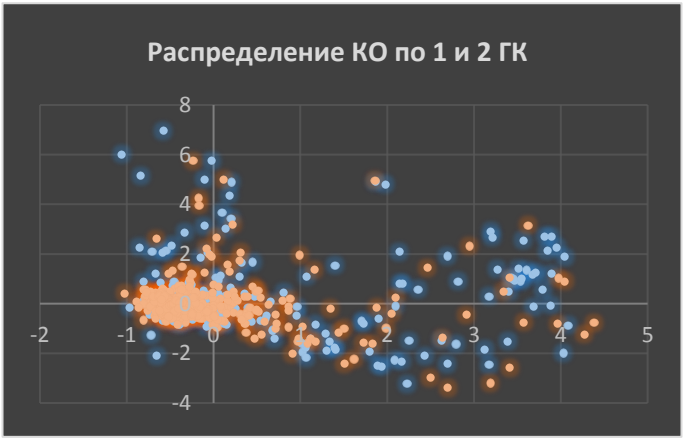

Рисунок 1 – Распределение благонадежных и не благонадежных кредитных организаций по 1й и 2й главной компоненте

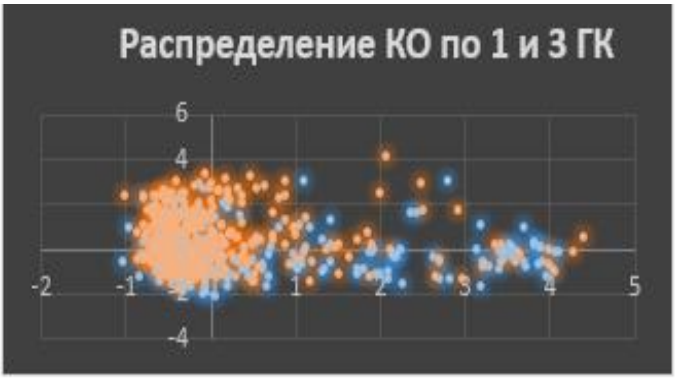

Рисунок 2 – Распределение благонадежных и не благонадежных кредитных организаций по 1й и 3й главной компоненте

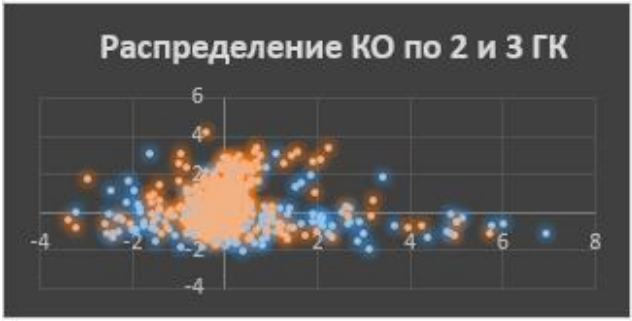

Рисунок 3 – Распределение благонадежных и не благонадежных кредитных организаций по 2й и 3й главной компоненте

Визуальный анализ объектов исследования не позволяет выделить отдельные классы для кредитных организаций.

В связи с чем принято решение использовать методы классификации, заложенные в функционале IBM SPSS Modeler.

Сейчас широко распространены методы деревьев решений для классификации. Метод решений деревьев применяется при решении задач классификации и предполагает разделение исходной информации на группы до тех пор, пока не получатся однородные (или почти однородные) множества. Сочетание правил, дающих такое разбиение, позволит потом делать прогноз (то есть определить вероятный номер класса) для новой информации.

Метод деревьев решений применяется для решения задач классификации в самых различных областях и является одним из наиболее эффективных видов решений.

Итак, дерево решений – это модель, представляющая собой совокупность правил для принятия решений.

Графически она представляется в виде древовидной структуры, в которой моменты принятия решений совпадают с так называемыми узлами. Процесс ветвления происходит в узлах, то есть разделяет на так называемые ветви в зависимости от сделанного выбора. Конечный терминальный узел называется лист. Каждый лист является конечным результатом последовательного решения.

Данные, которые подлежат классификации, содержатся в так называемом «корне» дерева. В соответствии с решением, принятым в узлах, процесс в конечном счете остановится в одном из листьев, в котором переменной отклика для искомого номера присваивается то или иное значение.

Метод деревьев решений является реализацией принципа так называемого «рекурсивного разделения». Эту стратегию также называют «Разделяй и властвуй». В узлах начиная от корневого выбирается признак, значение которого используются для разделения всей информации на 2 класса. Процесс выполняется до того момента, пока критерий остановки не сработает. Такая ситуация возможна в следующих случаях:

- Все (или почти все) данные данного узла принадлежат одному и тому же классу;
- Не осталось признаков, по которым можно построить новое разбиение;
- Дерево превысило заранее заданный «лимит роста» (если таковой был заранее установлен).

Процесс деления обычно останавливается, когда каждая группа хотя бы на 80% элементов будет сформирована из элементов одного и того же класса – так называемый критерий оптимальности.

7. На вход были передана исследуемая выборка со значениями 17 факторов. (Рис.4)

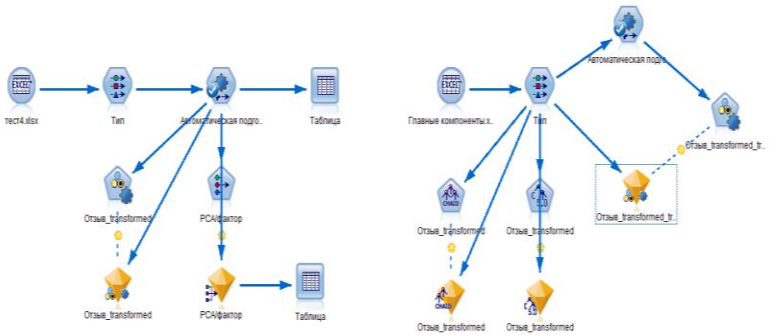

Рисунок 4 – Визуализация исследуемой выборки

8. Наибольшая общая точность была достигнута в модели деревьев решений CHAID. Для сравнения также исследованы результаты классификации по модели Дерево C&R. (Рис. 5)

Модель	Время построения (минут)	Макс выигрыш	Макс достигнутый выигрыш в (%)	Рост(Верхние 30%)	Общая точность (%)	Число использованных полей	Площадь под кривой
CHAID 1	< 1	1089,052	68	1,314	66,197	5	0,695
Логистическая...	< 1	1 085,0	72	1,331	65,547	17	0,692
Нейронная се...	< 1	1 050,0	68	1,324	64,464	17	0,689
Дерево C&R 1	< 1	935,0	80	1,362	62,839	17	0,679
C5 1	< 1	894,058	51	1,198	61,972	1	0,620
Quest 1	< 1	883,174	52	1,189	61,755	6	0,616
Список решен...	< 1	834,442	41	1,278	60,672	4	0,631

Рисунок 5 – Распределение результатов классификации по модели Дерево C&R

1) Сформированы правила отбора кредитных организаций, вовлеченных в противоправную деятельность по ОД/ФТ.

2) Построено дерево решений по алгоритму CHAID. (Рис.6)

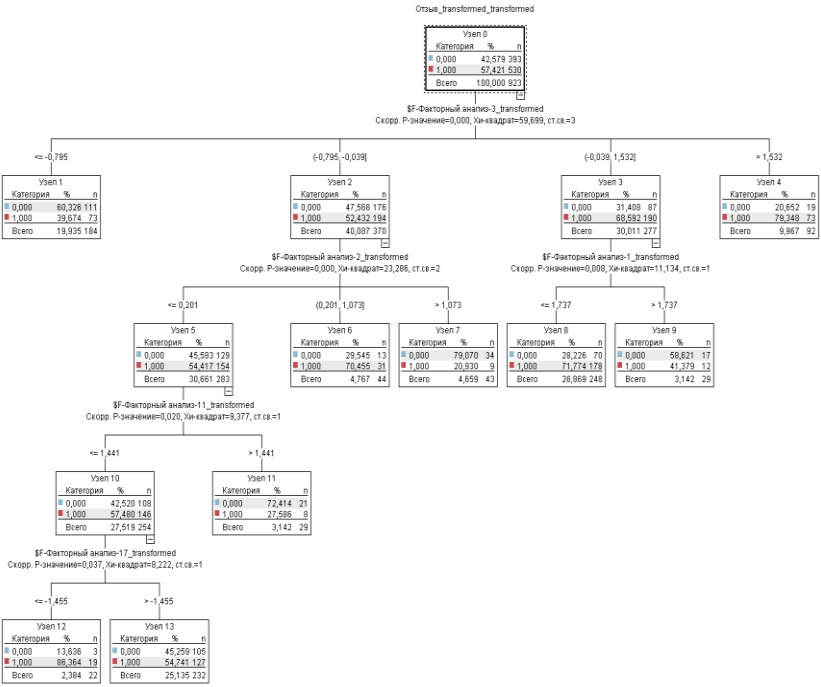

Рисунок 6 – Дерево решений по алгоритму CHAID

10. Результаты применения Дерево C&R (Рис.7)

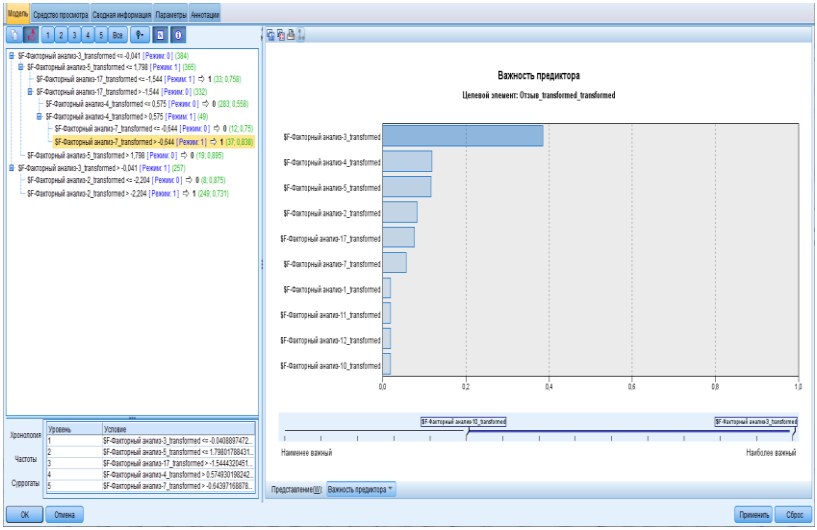

Рисунок 7 – Визуализация распределения ликвидированных банков по 3й главной компоненте

В ходе проведения анализа с использованием функционала IBM SPSS Modeler идентифицированы правила классификации кредитных организаций на предмет вовлеченности в противоправную деятельность, в частности ОД/ФТ, а также произведено ранжирование главных компонент по степени влияния главной компоненты на целевой элемент.

Сформированы правила отбора кредитных организаций, вовлеченных в противоправную деятельность по ОД/ФТ.

Вместе с тем, приведены распределения ликвидированных банков (Рис. 8), и банков с высокой степенью благонадежности (Рис. 9).

Также, было установлено, что распределение банков по 3й главной компоненте подчиняется закону отличному от нормального закона. Одновременно, распределение благонадежных банков по 3й главной компоненте соответствует нормальному закону распределения.

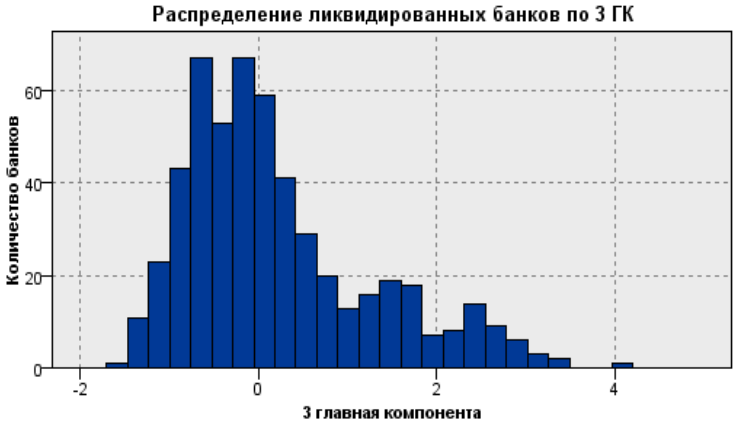

Рисунок 8 – Распределение ликвидированных банков

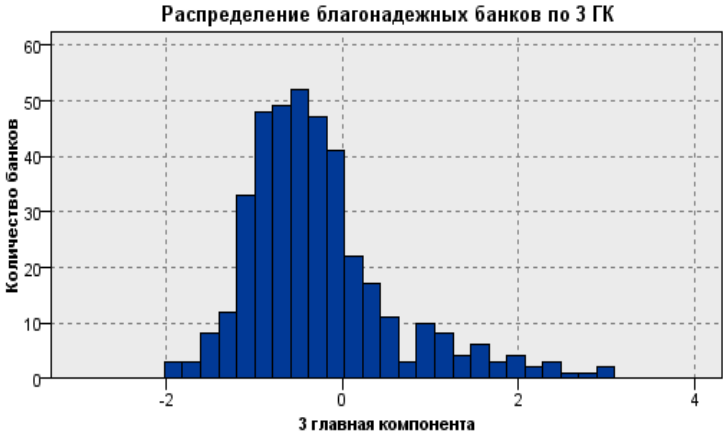

Рисунок 9 – Распределение благонадежных банков

2) Построено дерево решений по алгоритму C&R.

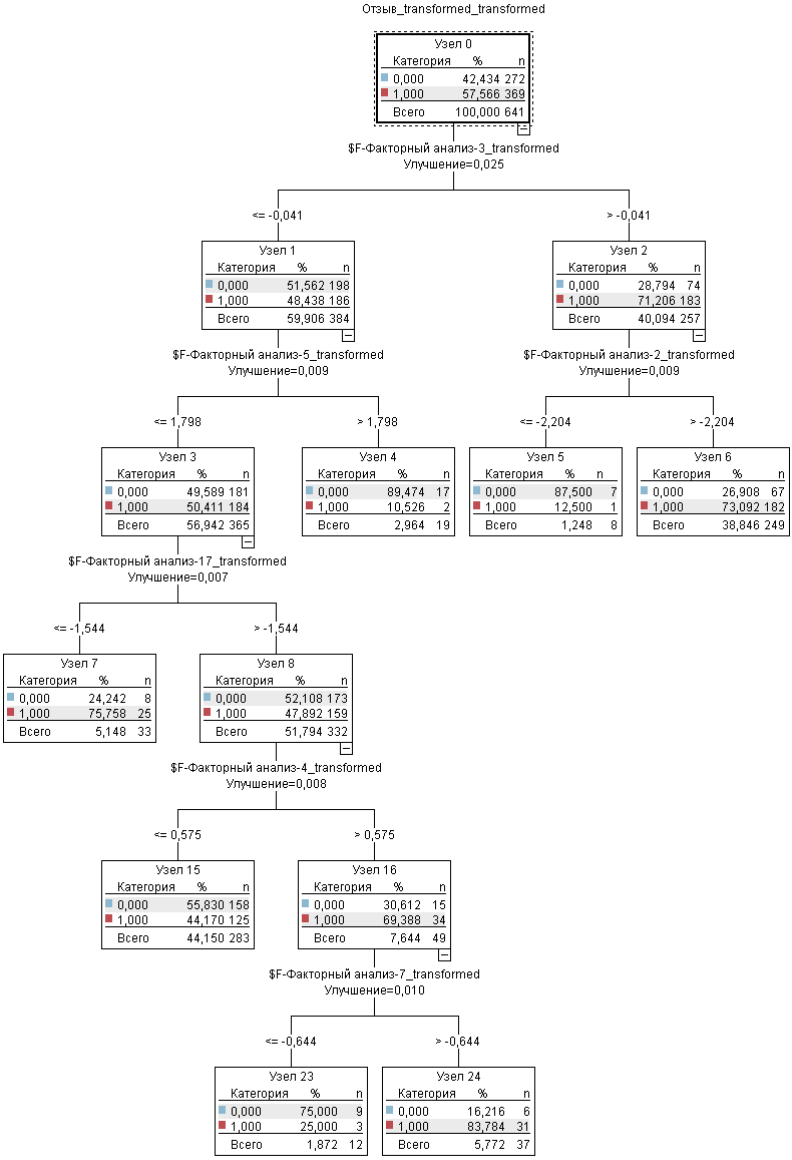

Рисунок 10 – Дерево решений по алгоритму C&R

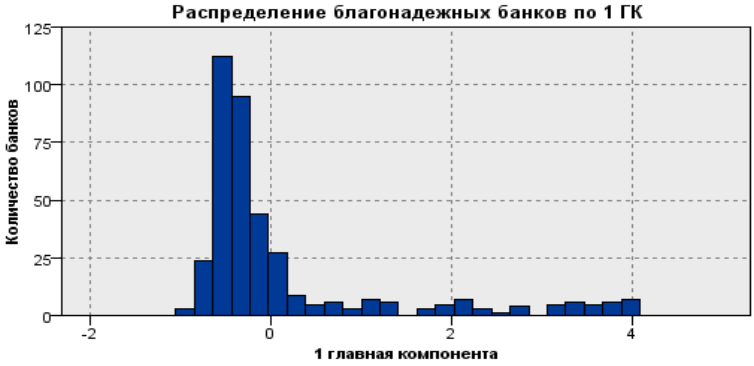

Рисунок 11 – Распределение благонадежных банков по 1й главной компоненте

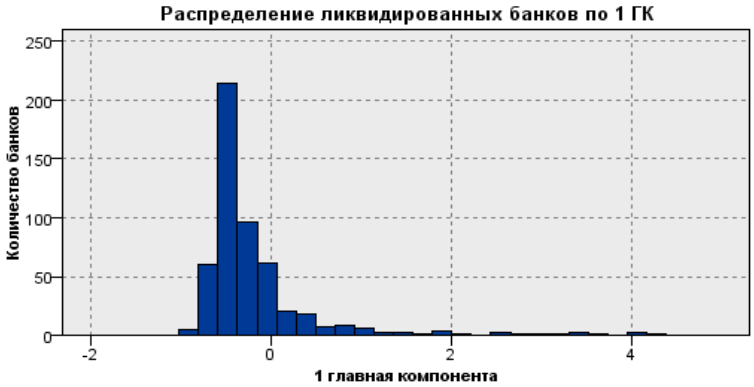

Рисунок 12 – Распределение ликвидированных банков по 1й главной компоненте

Так, изложенная выше работа проведена с целью разработки и апробации новых методик и алгоритмов обнаружения потенциально проблемных кредитных организаций, использующих финансовую систему России для легализации денежных средств, полученных преступным путем. В ходе исследования были применены различные методы машинного обучения в целях выявления более подходящего для реализации задач, стоящих перед аналитиками.

Список использованных источников:

1. Елисеев О.Е. Управление рисками в контрактации [Электронный ресурс] // Информационно-экономические аспекты стандартизации и технического регулирования: Научный интернет-журнал. 2012. – № 3(7).
2. 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.
3. 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.

УДК 004.4:004.056

Современные методологии разработки безопасного программного обеспечения

А.А. Тулеубаева
студент 4 курса бакалавриата НИЯУ МИФИ, Москва
E-mail: aigerim.tuleubayeva@yandex.ru
А.Б. Камолов
студент 4 курса бакалавриата НИЯУ МИФИ, Москва
E-mail: kamolov.amir2000@yandex.ru
В.А. Рычков
старший преподаватель кафедры финансового мониторинга № 75
НИЯУ МИФИ, Москва
E-mail: VARychkov@mephi.ru

Аннотация: *В статье рассмотрены современные методологии разработки программного обеспечения, созданные с целью обеспечить ПО необходимым уровнем безопасности. Описаны основные моменты в методологиях DevOps и DevSecOps. Приведены примеры самых часто используемых в настоящее время инструментов для разработки безопасного программного обеспечения.*
Ключевые слова: *DevOps, DevSecOps, CI/CD.*

Managing the organization's business processes in an organization as a part of digital transformation

Abstract: *The article discusses modern software development methodologies. The main points of the DevOps and DevSecOps methodology are described. Examples of the most commonly used tools for secure software are given.*
Keywords: *DevOps, DevSecOps, CI/CD.*

Постоянное развитие информационных систем и, как следствие, появление все большего количества новых уязвимостей программного обеспечения обуславливает создание и развитие особых методологий, направленных на обеспечение качества разрабатываемого программного обеспечения, а также снижение рисков за счет использования эффективных практик и наличия методов контроля и оптимизации. Появление новых методологий определило задачи их эффективного применения и обеспечения безопасности разрабатываемого ПО.

Уязвимости программного обеспечения имеют разного рода природу и всевозможные варианты их использования в самых неблагоприятных, как и для владельца, так и для пользователя программного обеспечения, целях. Особенно это демонстрируется в последние годы, когда даже крупные корпорации и лидеры IT-сферы успешно подвергаются различным атакам злоумышленников. Является очевидным, что минимизация количества этих уязвимостей – одна из главных и актуальных задач сегодняшнего дня для мирового сообщества разработчиков программного обеспечения и специалистов в области информационной безопасности.

Безопасное программное обеспечение — программное обеспечение, разработанное с использованием совокупности мер, направленных на предотвращение появления и устранение уязвимостей программы.

Постоянное совершенствование методологий разработки программного обеспечения стало результатом необходимости обеспечить программный продукт высокой устойчивостью и максимально удовлетворить потребности конечного пользователя для получения конкурентного преимущества в сфере разработки ПО. В ходе эволюции отрасли были созданы и нашли свое широкое применение на практике параллельно с классическими методологиями, как «Водопад» и «Спираль», гибкие методологии Agile и DevOps. Их популярность обусловлена возникновением инструментов с возможностью адаптации к постоянно изменяющимся потребностям пользователей, а также ускорения процесса разработки программного обеспечения. К примеру, это касается платформ Continuous Integration и Continuous Delivery (CI/CD) и технологии контейнеризации.

Development and Operations (DevOps) — это комплекс практик, принципов и инструментов, которые автоматизируют и интегрируют процессы между командами разработчиков и другими участниками проекта создания программного обеспечения, как администраторы, тестировщики и т.д. Методология является гибким подходом для исключения как временных, так и организационных препятствий для обеспечения более быстрого процесса разработки надежного ПО, путем расширения прав и возможностей команды, организации меж командного общения и совместной работы, а также применения автоматизации технологий там, где это является возможным. С применением данной методологии, в отличие от классических моделей, процесс разработки больше не стоит отдельно от операций развертывания и поддержки кода.

Рисунок 1 – Основополагающие процессы DevOps

В рамках DevOps разработка и оптимизация программного обеспечения происходят эффективнее и быстрее, что помогает сокращать время на выпуск версий программного обеспечения и делать релизы чаще. В результате компании могут повысить уровень обслуживания клиентов и более эффективно конкурировать на рынке.

Важной особенностью DevOps является автоматизация процессов как непрерывная доставка (CD), которая предоставляет возможность разработчикам поставлять изменения в ПО чаще и в относительно короткие сроки, а также непрерывная интеграция (CI), ориентированная на интеграцию модулей и частей программного обеспечения. Конвейер CI / CD — это набор практик, который подразумевает под собой внесение небольших изменений с фиксацией. Задача CI заключается в обеспечении последовательности и автоматизации способов компиляции и компоновки, тестирования и упаковки программного обеспечения. Непрерывная поставка (CD) начинается после успешного завершения процесса непрерывной интеграции (CI).

Методология содержит шесть основополагающих принципов:

Клиентоориентированность;

Сквозная ответственность всех членов команды за обеспечение производительности ПО;

Непрерывное улучшение;

Автоматизация — это ключевой момент DevOps;

Командная работа;

Мониторинг — еще одна крайне необходимая часть методологии, которая обязывает тщательно контролировать и тестировать программное обеспечение.

DevOps – связующий элемент между разработчиками, старающимися добавлять функции в программу, администраторами, осуществляющими контроль стабильности ПО, а также тестировщиками, производящими проверки функционала. Таким образом, в условиях налаженной организации процессов DevOps происходит улучшение коммуникации и повышение качества программного обеспечения.

Основные этапы жизненного цикла DevOps:

1. Этап планирования. Менеджеры проектов в сотрудничестве с командой занимаются определением и описанием функций и возможностей создаваемого ПО. На данном этапе происходит планирование и мониторинг выполнения задач, управление гибкой разработкой инструментами популярных гибких методологий вроде Scrum и Kanban. Используются инструменты управления проектами как Jira, Confluence, Trello, Asana, Azure DevOps, Clarizen и т.д.;

Этап разработки. Включает в себя все моменты написания кода – программирование, тестирование, интеграция кода. Для параллельной работы над кодом используются системы управления версиями как Mercurial, Git, SVN, Subversion, и системы, вносящие огромное количество преимуществ в совместную работу команды разработки ПО как GitHub, GitLab и Bitbucket;

Этап сборки. Исходный код программы преобразуется в форму, которая может быть запущена в компьютерной системе. На этом этапе задействованы в основном разработчики и системные администраторы. Используются инструменты CI как Jenkins, TravisCI, а также инструменты автоматизированной сборки как Maven, Gradle, Apache Ant, Apache Buildr, MSBuild и т. д.;

Этап тестирования. На этом этапе программное обеспечение проверяется отделом обеспечения качества с использованием инструментов автоматизированного тестирования, примерами которых являются JUnit, Bugzilla, Jmeter, Selenium, и т.д. Автоматизация тестирования может повысить качество программного обеспечения и снизить риски;

Этап развертывания. На данном этапе происходят процессы установки и запуска версий ПО в производственной среде и условиях. DevOps команды используют методики развертывания, помогающие обнаружить и оперативно устранить проблемы до того, как они окажут влияние на взаимодействие с клиентами. Автоматизация сокращает количество ручных операций, что дает возможность производить большее количество

релизов, а также снизить количество ошибок. Не существует уникального инструмента для автоматизированного развертывания, который будет работать для любого программного обеспечения и любой среды. Однако, широкое применение на практике для данного этапа жизненного цикла получили инструменты как Ansible, Docker, Kubertenes, Virtualbox, AWS CodeDeploy и LXD;

Этап эксплуатации. Данный этап адаптирует и поддерживает инфраструктуру, в которой функционирует программное обеспечение. Данный этап, в основном, лежит на плечах системных администраторов, которые используют комбинации групп инструментов как: инструменты управления конфигурацией Ansible, Puppet, Chef и SaltStack; инструменты безопасности Fortify Static Code Analyzer, Sonarqube и Veracode; инструменты и системы управления базами данных;

Этап мониторинга. Это практика, в которой команды управления и мониторинга производят контроль ПО и инфраструктуры 24/7. Здесь происходит постоянный контроль производительности ПО и записывается информация об использовании программы. Наиболее популярными используемыми инструментами являются инструменты наблюдения и контроля состояния вычислительных узлов и служб как Zabbix, Ganglia и Nagios, инструменты управления серверами и сетью как Zenoss, инструменты анализа логов как Splunk, а также другие инструменты мониторинга как New Relic, AppDynamics и т.д. На этом этапе выявляются и исправляются системные ошибки, проблемы с сетью и ошибки несоответствующего поведения программного обеспечения;

Непрерывная обратная связь. Это подразумевает под собой процесс регулярного сбора обратной связи, а также инструменты для получения информации из обратной связи. В DevOps каждый из команды имеет доступ к комментариям пользователей ПО. Популярные инструменты для организации обратной связи - Jira Service Management, Slack и GetFeedback.

DevOps помогает повысить производительность и надежность программного обеспечения. Этапы жизненного цикла выполняются непрерывно, пока ПО не достигнет необходимого качества.

В качестве преимуществ методологии DevOps можно выделить такие пункты как то, что методология относительно проста и имеет возможность гибкой организации задач, а также то, что за счет постоянного мониторинга и отладки, уменьшается уязвимость программного обеспечения и повышается его надежность, устойчивость и восстанавливаемость. За счет внедрения DevOps можно увеличить скорость и объемы разработки, а также методология способствует инновациям.

Но методология, естественно, и не лишена недостатков. Например, можно выделить невозможность использования DevOps в условиях работы

со сложными и объектно-ориентированными моделями. Также стоит заметить, что для обеспечения успешного взаимодействия и эффективности DevOps, необходим высокоэффективный менеджмент и изменение не просто процессов и инструментов, а в целом – всей культуры, что является не таким простым и легким делом. Без соблюдения основных принципов DevOps невозможен.

В рамках классических методологий, в основном, вопрос обеспечения безопасности ПО выносился в конец, после разработки, а специалисты в области обеспечения безопасности представляли собой отдельную команду, особо не участвующую в других этапах жизненного цикла. Вместе с широким применением Agile и DevOps, позволяющим ускорять процесс разработки и увеличивать скорость релизов, проявилась проблема неэффективности данного подхода. DevSecOps — development, security, operations стал закономерным логическим расширением методологии разработки DevOps с акцентом на обеспечение безопасности ПО. Цель DevSecOps в интеграции задач безопасности в каждую стадию жизненного цикла разработки ПО.

Методология DevSecOps подразумевает внедрение процессов идентификации и устранения угроз безопасности в процесс DevOps. Суть DevSecOps заключается в автоматизации проверки безопасности разрабатываемого программного продукта и выполнении на протяжении всего жизненного цикла ПО, что способствует разработке безопасного программного обеспечения с минимально возможным количеством уязвимостей. Автоматизация в DevSecOps играет огромную и важнейшую роль, давая возможность командам постоянно следить за ПО и оперативно обеспечивать безопасность, к примеру, средствами автоматического анализа кода, расследования угроз и мониторинга соответствий.

Устраняя пропасть между командами разработки, обеспечения безопасности и операционной, повышается возможность создания безопасного программного обеспечения, с минимально возможными рисками и максимально возможной устойчивостью к атакам.

Внедрение DevSecOps имеет свои тонкости и особенности. Стоит рассмотреть несколько основных моментов.

1. Члены команды должны быть положительно настроены и устойчивы к изменениям условий работы при внедрении методологии. Для персонала, который не работал в рамках DevOps, сложнее освоиться к сотрудничеству и взаимодействию с другими подразделениями. Для более эффективного внедрения DevSecOps необходимо учитывать потребности и приоритеты руководства и членов групп разработки, безопасности и эксплуатации. Если ранее команды работали автономно, то кооперация потребует тщательного планирования и менеджмента;

DevSecOps требует обеспечения безопасности разрабатываемого ПО с самого начала ЖЦ. Следовательно, является необходимым повышение навыков и знаний всех членов команд о методах безопасной разработки и тестировании;

Для повышения качества программного обеспечения необходимо определить приоритеты в требованиях безопасности, а также осуществлять проверку политик безопасности и оценку автоматизированных тестов экспертами в области обеспечения безопасности;

Некоторые из уже используемых инструментов в DevOps могут оставаться полезными после перехода и в DevSecOps, если они способствуют автоматизации работы, повышают эффективность разработки и/или упрощают совместную деятельность. Примерами таких инструментами могут быть статический анализ SAST, динамический анализ DAST и контроль Open Source. В идеале, если команды совместно решают вопрос используемых средств, подходов и инструментов.

В случае статического тестирования безопасности приложений (SAST) для выполнения статического анализа кода используются предопределенные сигнатуры безопасности. Вследствие этого, SAST не может точно определить неизвестные угрозы и выдает ложноотрицательные результаты, что повышает риски. Средства SAST сложно применить в средах с использованием нескольких языков программирования, так как для каждого языка необходимы отдельные конфигурации. Для эффективного поиска и исправления уязвимостей при проведении статического анализа кода разработчики должны быть высококвалифицированными экспертами.

Средства динамического анализа кода (DAST) производят анализ функционала программы по уже готовым наборам тестов и сканируют ПО для обнаружения возможных уязвимостей безопасности. DAST имеет минимальное количество ложных срабатываний и часто используется в веб-приложениях. Один из недостатков инструментов DAST является не предоставление точной информации о причинах уязвимости и, тем самым, появляется возможность проявления ложноположительного результата.

Эти ложные срабатывания тратят время команд безопасности и разработчиков на ручную проверку, что замедляет и удлиняет циклы релиза модулей и частей ПО.

DevSecOps нуждается немного в другом подходе для обеспечения максимального уровня безопасности ПО. Интерактивное тестирование безопасности приложений (IAST) использует эту другую модель. Контрольно-измерительные приборы безопасности встраиваются в программное обеспечение, позволяя автоматизировать процесс идентификации уязвимостей и проверки исправлений. IAST обеспечивает

непрерывное управление уязвимостями в режиме реального времени и рассматривает не только программный код, но и отслеживает время исполнения и сведения о потоке данных, информацию о конфигурации, HTTP-запросы и ответы, библиотеки с открытым исходным кодом, платформы и другие компоненты с открытым исходным кодом и серверные соединения.

Количество ложных срабатываний в IAST минимизируются, а найденные уязвимости классифицируются на основе наиболее распространенных и подверженных наибольшему риску, что позволяет разработчикам и команде безопасности эффективнее решать выявленные проблемы.

Отличие между DevOps и DevSecOps в том, что DevOps — это интеграция процессов разработки и доставки приложений, а в DevSecOps все эти процессы объединяются с безопасностью. DevOps фокусируется на технологиях и методах, которые налаживают взаимодействия команд, в то время как DevSecOps сосредоточена на методах, которые могут добавить функции безопасности в DevOps.

Задачи разработки считаются завершенными при условии выполнения всех функциональных требований и успешном прохождении всех этапов проверки на наличие уязвимостей. Выбор методологии зависит от множества факторов и характеристик проекта, ожиданий и требований к программному обеспечению. Однако, в любом случае, необходимо обеспечить высокий уровень безопасности программного обеспечения.

Для разработки программного обеспечения с минимально возможным количеством уязвимостей необходимо автоматизировать процессы там, где это может быть сделано, повышать уровень знаний и навыков всех членов команды, участвующих в процессе создания программного продукта, а также использовать комбинации различных инструментов и подходов для обеспечения качества ПО.

Список использованных источников:

1. DevOps: устранение разногласий между разработчиками и операторами [Электронный ресурс] / авт. Atlassian. - 6 12 2021 г.. - https://www.atlassian.com/ru/devops.
2. DEVSECOPS [Электронный ресурс] / авт. security Contrast. - 9 12 2021 г.. - https://www.contrastsecurity.com/knowledge-hub/glossary/devsecops.
3. DevSecOps [Электронный ресурс] / IBM Cloud Education / IBM - https://www.ibm.com/ru-ru/cloud/learn/devsecops.
4. Makosi, R. DevOps Concepts / R. Makosi // Вестник Хакасского государственного университета им. Н.Ф. Катанова. – 2017. – No 20. – P. 32-34..

5. Ганжур, М. А. Анализ методологий devops и devsecops / М. А. Ганжур, Н. В. Дьяченко, А. С. Отакулов // Молодой исследователь Дона. – 2021. – № 5(32). – С. 8-10..
6. Головашов, С. Программные решения для обеспечения цикла непрерывной разработки / С. Головашов // Системный администратор. – 2021. – № 1-2(218-219). – С. 66-68..
7. ГОСТ Р 56939-2016. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования - www.consultant.ru.
8. Инструменты DevOps [Электронный ресурс] / авт. Atlassian. - 9 12 2021 г.. - https://www.atlassian.com/ru/devops/devops-tools.
9. Что такое DevOps? [Электронный ресурс] / авт. Microsoft. - 8 12 2021 г.. - https://docs.microsoft.com/ru-ru/devops/what-is-devops.

УДК 005.934:004:330.4

Теневая экономика и экономическая безопастность в условиях цифровизации

Б.И. Исроилов
д.э.н., профессор ТГЭУ
E-mail: b.isroilov@tsue.uz
isbokhodir@gmail.com

Аннотация: *в тезисе рассмотрена сущность теневой экономики и изучено мировая, а также отечественной тенденции ее развития. Развития теневая экономика не только подрывает основы экономики и ее стабильное развитие в целом, влияет на состояния экономическую безопасность страны. По результатам исследования даны предложения по сокращению ее размеров.*

Ключевые слова: *теневая экономика, объём теневой экономики, причина ее возникновения, экономическая безопасность.*

Shadow economy and economic security in the context of digitalization

Abstract: *the article examines the essence of the shadow economy and studies the study of the world, as well as the domestic practice of its development. Since the shadow economy not only undermines the foundations of the economy and its stable development in general, the authors examined its impact on the country's economic security. As a result, proposals were given for his crushing.*

Keywords: *shadow economy, the volume of the shadow economy, the reason for its occurrence, economic security.*

В условиях глобализации и цфровизвции мирового экономического хозяйство экономическая безопасность приобрела новое значение в мировой экономике. Экономическая безопасность неразрывно связана с такими показателями, как экономический рост, стабильность социально-экономической системы, государственные доходы, налоговая база, государственный долг, инфляция, безработица и объему теневой экономику.

Экономическая безопасность в настоящее время затрагивает не только государство в целом, но и каждого человека в отдельности. Нестабильность и кризисная ситуация в экономике имеют негативные последствия для каждой семьи. Но только ли экономика в XXI веке имеет влияние на экономическую безопасность государства? Чтобы ответить на этот вопрос,

необходимо проанализировать экономическую безопасность в системе национальной безопасности Узбекистана, последствия политических решений, деятельность учреждений, влияние экономической безопасности регионов, знать, как устроена государственная система обеспечения экономической безопасности. Необходимо расставить приоритеты в реальном секторе экономики и инновационной сфере, изучить инструменты защиты интеллектуальной собственности с целью обеспечения стабильности экономического положения Узбекистана, для достижения экономического роста в стране, роста национального благосостояния и соответственно благосостояния каждой отдельной семьи.

На современную финансовую систему страны и финансовую безопасность страны оказывают негативное влияние «теневая экономика», коррупция, «бегство капитала за рубеж» и использование оффшоров для нелегальной минимизации налогов. С теневой экономикой связан ряд негативных последствий для государства и общества. Теневая экономика оказывает отрицательное воздействие на состояние государственных финансов, прежде всего на формирование доходов бюджетов всех уровней. Это, в свою очередь, затрудняет финансирование расходов, связанных с осуществлением функций государства, таких как управление, оборона, развитие фундаментальной науки и других. Фактически, теневая экономика прямо подрывает финансовые основы государственного суверенитета.

Оценивая структуру и масштабы этих негативных явлений, необходимо находить новые формы борьбы с этими угрозами экономической безопасности страны. Например, для обеспечения экономической безопасности на рынке услуг необходимо привлечение инвестиций, устранение недобросовестной конкуренции.

Действительно, экономический рост не может быть устойчивым без динамичного развития экономик других стран. Пока экономика не будет развиваться, не будет адекватного ответа на внешние и внутренние угрозы, т.е. способность экономики выжить в сложных ситуациях останется абстрактной. Поэтому вопрос об определении уровня экономической безопасности, степени нормального экономического развития, уровня, на котором оно становится опасным, является предметом жарких споров и дискуссий среди ученых в этой области.

Состояние экономической безопасности оценивается системой объективных критериев и показателей, определяющих предельные размеры функционирования экономической системы. Система показателей для оценки уровня экономической безопасности и определения их нормативных значений важна в государственной экономической политике. Поэтому в развитых странах мира, показатели уровня экономической

безопасности страны и их пороговые значения утверждаются на правительственном уровне.

На экономическую безопасность государства в свою очередьи влияет объем теневой экономики. Рост теневой экономики приведет к сокращению государственных доходов за счет уменьшения налоговой базы, в свою очередь это, приводит к снижению качества социально-экономических условий в целом.

Теневая экономика – это определенная экономическая деятельность, которая осуществляется на территории государства с целью уклонения от уплаты налогов и официально не учитывается. Поэтому ее развитие имеет негативное воздействие на социально-экономическое положение [1].

Изучение причин возникновения и проблемы теневой экономики привлекли внимание исследователей еще в 30 - х годах XX века. Потому что доля теневой экономики в производстве товаров и оказываемых услугах в этом периоде, несколько возросла. Первоначально в 1939 году американский криминалист Э.Х.Сатерленд в своей работе "Являются ли преступления людей в белых воротничках преступлениями?" оценивал вопросы развития неформальной экономики наряду с самим крупным бизнесом [2].

В 1977 г. вышла статья П. Гутмана [3] «Подпольная экономика» - первая работа, в которой была отмечена важность борьбы с неучтенной экономической деятельностью. В СССР научной литературе термин «теневая экономика» возник в связи с анализом «теневой» хозяйственной деятельности в 1960-е гг. с введением УК СССР 1961 г.

Позднее американский исследователь Г.Бекера [4], российские ученые М.Николаева, Ю.Шевяков [5] тоже обратили внимание в своих исследованиях на развитие, элементы и другие аспекты неформальной экономики в обществе.

Рост объема и определение механизмов противостоят проблемам развития теневая экономика беспокоила общества и в 1983 году в г. Белефелде была проведена первая международная конференция по вопросам теневой экономике, на которой было представлено более 40 докладов.

В 1991 г. в Женеве прошла конференция, посвященная теневой экономике. По ее материалам было опубликовано специальное руководство по статистике теневой экономики в странах с рыночной системой хозяйствования. Это быль фундаментом начало этапа учет объема теневого экономика в целом.

Теневая экономика существует в любом обществе, и ее размеры, помимо всего прочего, зависят от расходов государства на содержание контролирующих органов. Поэтому на языке классических экономических

учебников оптимальный размер теневой экономики представлен точкой 0, идеализированным условием является отсутствие коррупции (рис№1).

Рисунок 1 – Связь теневой экономики и расходы на содержание государственных органов

Среди ученых стран СНГ так же много споров вызывает вопрос о масштабе теневой экономики. Учеными проанализированы, дополнены и разработаны многочисленные методы и методология измерения масштабов теневой экономики [6-10].

Теневая экономика является сложным явлением характерным для всех стран мира. По данным Всемирного банка среднемировой уровень теневой экономики составляет 17,2 % ВВП, однако этот показатель отличается в разных странах. Например, самый низкий показатель выявлен в Швейцарии: он равен 8,6 %, в Китае – 10,2 %, в России – 39,0 %, а самый высокий уровень теневой экономики отмечается в Боливии – 66,4%. Объем мировая теневая экономика оценивается около 13 трлн долл. США. Мировая теневая экономика в последние десятилетия растет быстрее, чем официальная. Согласно экспертным оценкам, в США теневая экономика за год создает товаров и услуг на 700 млрд долл. В Норвегии 37,5% населения связано с нелегальной экономикой в роли продавцов либо покупателей [11].

Согласно исследованию профессора австрийского университета Кеплера Ф.Шнейдера, размер теневой деятельности составляет в странах Европы в среднем 18% ВВП [12].

Столь продолжающейся объем теневой экономики представляется весьма опасным с точки зрения экономической политики в условиях глобализации. Это приведет к деградации национальных налоговых

систем. Также, экономическая политика, основанная на неверных показателях экономической статистики, отрицательно влияет на стабильность развития экономики. И как результате разработки международных институтов по координации экономической политики, которая является способствующим фактором функционирования современного всемирного хозяйства, также могут оказаться неэффективными.

К стимулирующим факторам развития размер теневой экономики является:

- рост потребностей вместе с ростом доходов у всех слоев населения;
- опережающая динамика доходов в сравнении с ростом производительности труда, относительно низкие темпы роста производства потребительских товаров и услуг;
- сдерживание экономической инициативы, уход активных предпринимателей в "теневой" бизнес;
- накопление относительно больших средств в руках дельцов "теневой" экономики и сращивание ее с уголовной преступностью;
- естественное стремление населения максимально поднять свои доходы, используя в этих целях любые способы, что в условиях ограничения легальных возможностей толкает людей в сферу "теневого" бизнеса;
- монополизм в экономике, диктат производителя, полная бесправность конечного потребителя - населения.

По мнению некторых ученых теневая экономика в постсоветских странах выступает в роли важного инструмента поддержки экономического и социального равновесия. Они считают что, в условиях переходного периода с помощью теневого сектора создаются условия для выживания бизнеса и населения. Например, В.Ю.Буров считает что, при всех минусах теневая деятельность дает преимущества: малому бизнесу – увеличение прибыли; активному населению–возможность трудиться и получать доходы; потребителям – приобретать товары и услуги по более низким ценам [13].

По нашему мнению несмотря на перечесленных позитивных стороны любое проявление теневой экономики является опасным для полноценного развития экономики стран. Эти явления приведут к замедлению экономическое развитие в целом. В частности:

- сокращается налоговая база, растет налоговый пресс на легальный сектор экономики;
- снижается конкурентоспособность легальной экономики и подталкивает других экономических структур к уходу в тень;

– усиливается ресурсное обеспечение коррупции, что ведет к росту ее масштабов.
– неконтролируемые крупные финансовые ресурсы позволяют влиять на государственную политику, СМИ и избирательные компании различного уровня. Это также способствует развитию коррупции;
– национальный доход перераспределяется в пользу элитной группы, что обусловлено коррупцией и контролем криминальных групп над теневой экономикой. Это ведет к имущественному расслоению в обществе;
– происходит утечка капиталов за границу;
– расширяется неконтролируемая торговля низкокачественными товарами и товарами, опасными для потребителя.

Небходимо отметить что, несмотря на осуществляемой экономических реформ в Узбекистане объем теневой экономика до сих пор остаются высоким. Результаты исследования МВФ в Узбекистане показали что, доля теневой экономики долгое время держится на уровне от 30 до 50 % ВВП. Наибольшее значение доли теневой экономики от ВВП наблюдалось в 2019 году и составило 52 %, наименьшее значение в 2002 году – 31 % [11].

Проблемы и причины развития теневой экономики изучаются как отечественными, так и зарубежными учеными и практиками. Например, в исследованиях развития теневой экономики в предпринимательской деятельности Узбекистана были выявлены следующие причины:

– *множественные налоги, сборы и отчисления, а также их размер.*

– *высокие косвенные налоги* – акцизы, налог на добавленную стоимость, таможенные пошлины.

– *высокие налоги на бизнес* – налоги на прибыль, имущество дивиденды.

– *проблемы с банками* – осуществление расчетов, платежей, качество обслуживания;

– *трудности, связанные с бухгалтерской и другой отчетностью* - перед различными органами.

Поэтому государство в последнее время уделяет особие внимание на сокращение теневой экономики путем применени экономических рычагов. Так с 1 января 2021 года в стране снижено регулятивное и административное бремя, происходит автоматизацияи процедур и упрощение порядка соблюдения требований налогового законодательства [14].

Как показывает мировой опыт, обеспечение надлежащего уровня финансовой безопасности на всех уровнях - это гарантия независимости государства и предупреждения наступления негативных последствий открытости национальной экономики, условие стабильности и

эффективной жизнедеятельности общества, достижения достаточного взаимодействия с международными финансовыми и экономическими институтами.

Сегодня как никогда большое значение приобретают прозрачность и легальность операций в национальных финансовых системах. По этой причине крайне важно создать действенные механизмы противодействия теневой экономике и коррупции, чтобы не только защитить работоспособность финансовой системы страны, но и обеспечить должное использование государственных средств в целях борьбы с последствиями кризиса связанных с последствиями COVID-19.

По результатам анализа и исследований считаем необходимым:

- ввести порядок зачёт часть налогов на доход физических лиц осуществляющих расчетов в безналичном путем;
- с целью обеспечения быстрого обмена информацией и обеспечения эффективного надзора за инспекциями внедрить систему «e-Inspector»;
- расширить использование сторонних данных и больших данных (Big Data) для выявления незарегистрированных налогоплательщиков и транзакций;
- для повышения эффективности налогового контроля создать бесконтактные центры по обмену информацией между налоговыми органом, гражданами и бизнесом;
- расширить возможности центров обработки данных в налоговых и таможенных органах в получении информации о транзакциях.

Список использованных источников:

1. Капитонова Н.В., Капитонова А.А. Теневая экономика в условиях пандемии COVID-19 в России // Теневая экономика. – 2020. – № 4. – с. 193-204. – doi: 10.18334/tek.4.4.111865.
2. Сатерленд Э.Х. Являются ли преступления людей в белых воротничках преступлениями? Социология преступности. Современные буржуазные теории: Сборник статей.
3. П.Гутман. Подпольная экономика/.П.Гутман.М.:Экономика,1977.С.42. Экономическая библиотека.
4. Беккер Г. Преступление и наказания: экономический подход. / Истоки. Вып.4. - М.: ГУ- ВШЭ, 2000. – 28-29 с.
5. Николаева М.И., Шевяков Ю.А. Теневая экономика: методы анализа и оценка. - М. : ЦЭМИ, 1987. – 53 с.
6. Тумунбаярова Ж.Б., Анциферова М.Д. Неформальная занятость: причины и факторы, определяющие ее уровень // Теневая экономика. – 2018. – № 4. – с. 139-149. – doi: 10.18334/tek.2.4.40935.

7. Исроилов Б.И., Ибрагимов Б.Б., Ахмедов З. Влияния теневой экономики на экономическую безопасность страны // Теневая экономика. – 2021. – Том 5. – № 4.– doi: 10.18334/tek.5.4.113690.
8. Алимов Г.А., Исроилов Б.И. Теневая экономика, коррупция, взяточничество: уголовно-правовая оценка. / Монография. - Т.: Тафаккур, 2020. – 200 с.
9. Исроилов Б.И. Усиление ответственности юридических лиц за коррупционные правонарушения//Известия Иссык-Кульского форума бухгалтеров и аудиторов стран ЦА. – 2018. – № 2(21). – с. 405-407.Б.И. Исроилов - Иқтисодий хавфсизликни таъминлашнинг долзарб масалалари. // Мамлакат иқтисодий хавфсизлигини таъминлашнинг устувор йўналишлари.Тўплам. 5-6с.
10. The World Bank.Оценка объема теневой экономики Узбекистана. 2020.
11. Schneider F. Restricting or Abolishing Cash: An Effective Instrument for Fighting the Shadow Economy, Crime and Terrorism?. Econ.jku.at. [Электронный ресурс]. URL: http://www.econ.jku.at/papers/2017/wp1709.pdf.
12. Буров В.Ю. Совершенствование системы государственного регулирования малого предпринимательства в условиях доминирования теневой экономической деятельности // Теневая экономика. – 2019. – № 1. – с. 9-16. – doi: 10.18334/tek.3.1.39948.
13. Указ Президента Республики Узбекистан от 30 октября 2020 года УП№ 6098 «Об организационных мерах по сокращению теневой экономики и повышению эффективности деятельности налоговых органов». «Собрание законодательства Республики Узбекистан», 2 ноября 2020 г., N 43, ст. 475

УДК 005.86:004:334.7

Управление бизнес-процессами в организации в рамках цифровой трансформации

В.А. Чекунова
студент 4 курса бакалавриата НИЯУ МИФИ, Москва
E-mail: v.a.chekunova@gmail.com
В.А. Рычков
старший преподаватель кафедры «Финансовый мониторинг»
ИФТЭБ НИЯУ МИФИ, Москва
E-mail: VARychkov@mephi.ru
В. Давыденко
старший преподаватель кафедры «Финансовый мониторинг»
ИФТЭБ НИЯУ МИФИ, Москва
E-mail: VIDavydenko@mephi.ru

Аннотация: *данная статья посвящена анализу современных тенденций цифровой трансформации организаций в рамках цифровой экономики, в частности в сфере управления бизнес-процессами с применением цифровых технологий и программных решений. Рассмотрены риски, возникающие в рамках внедрения и использования специализированных информационных технологий.*
Ключевые слова: *бизнес-процессы, управление бизнес-процессами, цифровая экономика, цифровизация, риски.*

Managing the organization's business processes in an organization as a part of digital transformation

Abstract: *this article analyses current trends in the digital transformation of organizations, in particular in the area of digital business process management. The risks arising from the introduction and use of specialized information technologies are considered.*
Keywords: *business processes, BPM, digital economy, digitalization, risks*.

На данный момент в России и мире актуален вопрос цифровизации и цифровой трансформации. Все страны стремятся развивать цифровую экономику в рамках своего государства. Данное направление активно развивается при поддержке правительств, которые также осуществляют мониторинг и контроль исполнения поставленных задач. При этом перед

организациями как крупного, так и среднего и малого бизнеса стоит ряд однотипных задач, в ходе исполнения которых рекомендовано использование специализированных информационных технологий и программных решений. В рамках комплексной цифровой трансформации российской экономики была поставлена задача преобразования инфраструктуры организаций и предприятий с помощью внедрения и применения цифровых технологий.

Целью данной работы является выявление факторов риска на основании анализа последних тенденций в сфере цифровой экономики и цифровизации в целом, в частности цифровой трансформации в рамках управления бизнес-процессами в организациях.

В соответствии с поставленной целью определены задачи:

1. Обзор предметной области;
2. Анализ актуальности вопроса управления бизнес-процессами организаций в рамках цифровой трансформации;
3. Классификация рисков цифровой трансформации бизнес-процессов организаций.

В процессе исследования использованы следующие методы:

1. Сбор и анализ статистических данных;
2. Сравнительный анализ данных.

Прежде чем переходить к вопросу управления бизнес-процессами в организациях в рамках цифровой трансформации, необходимо разобраться в терминах «бизнес-процесс», «цифровая экономика» и «цифровизация бизнес-процессов».

В учебных пособиях, различных статьях и материалах термин «бизнес-процесс» определяется по-разному. Ниже, в таблице 1, приведены примеры раскрытия данного понятия.

Таблица 1 – Определение понятия «бизнес-процесс»

Автор	Определение понятия «бизнес-процесс»
М. Хаммер, Дж. Чампи (Ч. Д. Хаммер, 1997)	«совокупность различных видов деятельности, в рамках которой «на входе» используются один и более видов ресурсов, и в результате «на выходе» создается продукт, представляющий ценность для потребителя»
М. Рыбаков (Рыбаков М. Ю. , 2016)	Четко зафиксированный в письменном виде алгоритм выполнения многократно повторяющейся деятельности.
Эксперты Гарвардского университета	Совокупность всех действий, предпринимаемых предприятием с использованием как человеческих ресурсов, так и технологий и информации, в целях реализации своей деятельности.

В рамках данной стать термин «бизнес-процесс» мы будем определять как логически завершенную цепочку повторяющихся и взаимосвязанных между собой операций, направленных на достижение поставленных перед организацией целей.

Что же касается понятия «Цифровая экономика», то здесь также нельзя дать конкретного определения. Всемирный банк определяет цифровую экономику как взаимосвязанную систему социальных, экономических и культурных отношений, при этом в основе использования данных отношений лежит использование цифровых информационно-коммуникационных технологий. Согласно материалам (Deloitte) компании Deloitte под цифровой экономикой подразумевается форма экономической активности, которая возникает благодаря большому количеству примеров взаимодействия людей, предприятий, устройств, данных и процессов в сети. В рамках же Национальной программы «Цифровая экономика Российской Федерации» (РФ) к цифровой экономике «следует относить такой тип экономических систем, в котором преобладающая часть национального продукта обеспечивается видами деятельности, так или иначе связанными с производством, обработкой, хранением и распространением информации».

Аналогичная ситуация с термином «цифровизация бизнес-процессов». Цифровизация бизнес-процессов подразумевает перевод текущих бизнес-процессов организации в цифровую форму с использованием цифровых технологий для повышения производительности и конкурентоспособности. По данным (Минцифры, 2020), представленным в методических рекомендациях по цифровой трансформации государственных корпораций и компаний с государственным участием, цифровизация бизнес-процессов представляет из себя оптимизацию бизнес-процессов компании за счет применения цифровых технологий.

На данный момент цифровизация деятельности повсеместно стала одним из ключевых тенденций в ходе развития как мировой, так и отечественной экономики. Данная тема является частью стратегической повестки многих организаций. Направления активно развивается, поддерживается и регулируется со стороны государства. Например, в 2018 году в России была принята программа «Национальная экономика Российской Федерации» (РФ) , согласно которой процесс цифровизации реализуется во многих государственных учреждениях последние несколько лет.

Кроме того, стоит отметить огромное влияние пандемии Covid-19 на функционирование организаций по всему миру. Ряд ограничительных мер, предпринятых в рамках предотвращения распространения коронавирусной инфекции, способствовали ускорению темпов цифровой трансформации.

Многие компании были вынуждены пересмотреть бизнес-модели, в соответствии с которыми осуществляли свою деятельность, а также осуществить перевод многих процессов в цифровой формат за короткий срок. На сегодняшний момент цифровая трансформация фактически крайне необходима для устойчивого развития, эффективности бизнеса, а также высокой конкурентоспособности. На рисунке 1 представлена диаграмма, отображающая статус цифровой трансформации по отраслям российской экономики на 2020 год.

Рисунок 1 – Статус цифровой трансформации по отраслям российской экономики на 2020 год
(Источник: отчет KMDA (KMDA, 2020) «Цифровая трансформация в России»)

В 2021 году большинство компаниям пришлось в ускоренном темпе внедрять использование информационных технологий в рамках цифровой трансформации. К таким решениям относятся следующие программные продукты (описания приведены наиболее крупным системам):

1. *Системы управления бизнес-процессами* (Business Process Management System, BPMS). В зависимости от компании производителя, подобные системы позволяют моделировать, описывать, внедрять бизнес-процессы, обеспечивают прозрачность исполнения, предоставляют функции мониторинга и контроля за выполнением с помощью количественных и качественных показателей как отдельных бизнес-процессов, так и определенных цепочек. Отдельно отметим одну из важных функций – непрерывный анализ текущей ситуации внутри

организации, а также возможность внесения изменений в рамках повышения качества исполнения бизнес-процессов на основе полученных после этапа анализа данных;

2. *Системы планирования материальных ресурсов* (Manufacturing Resource Planning, MRP);

3. *Системы планирования производственных мощностей* (Capacity Requirements Planning, CRP);

4. *Системы объемно-календарного планирования* (MPS);

5. *Системы планирования финансовых ресурсов* (FRP);

6. *Системы планирования ресурсов предприятия* (Enterprise Resource Planning, ERP). Использование систем подобного класса позволяет управлять движением ресурсов, планировать производство, оптимизировать для повышения качества управления себестоимостью продукции и пр.

Использование подобных систем позволяет повысить экономическую эффективность реализации деятельности организаций, значительно снизить ряд операционных затрат на производство товаров и услуг, снизить временные и финансовые затраты на реализацию бизнес-процессов.

Однако, несмотря на преимущества, которые появляются в ходе использования информационных технологий в рамках цифровой трансформации деятельности организаций, стоит отметить и рост ряда рисков.

Под рисками в деятельности организаций подразумевается потенциальная возможность наступления событий, которые вызывают определенный ущерб. Ущерб может быть разным в зависимости от сложившейся ситуации: материальный, финансовый, потеря времени, трудовой и др.

В рамках подготовки данной статьи была собрана экспертная группа, с помощью которой были выявлены ряд рисков, которые могут возникнуть в организации в рамках цифровой трансформации в сфере управления бизнес-процессами. Результат представлен в таблице 2.

Таблица 2 – Риски внедрения информационных технологий в рамках цифровой трансформации деятельности организаций

№	Название риска	Описание
1.	Кадровый риск	В результате оцифровки бизнес-процессов и дальнейшего анализа в целях выявления неэффективных процессов и их оптимизации, модернизации или реинжиниринга для повышения эффективности деятельности организации может возникнуть ситуация, при которой часть сотрудников будет не востребована. Это приведет к сокращению численности персонала.

2.	Ошибки при процессе оцифровки	Локальный риск, который может существенно повлиять на дальнейшую деятельность организации. Если выявить ошибку позже, а не на стации оцифровки, то придётся нести временные и финансовые убытки для устранения и дальнейшей корректировки.
3.	Вопрос информационной безопасности и защиты информации	Для предотвращения вероятности утечки внутренней информации необходимо использовать сертифицированные программные решения и нанимать специалистов по информационной безопасности.
4.	Сбой программного продукта	Даже кратковременный сбор в работе программного решения может существенно повлиять на сроки выполнения задач, что в свою очередь может привести к репутационным рискам для организаций, работающих в коммерческой сфере.
5.	Санкционные меры	В сложившейся внешнеэкономической и политической ситуации стоит быть готовыми к введению ряда новых ограничений, что может также коснуться и программных решений, на которых базируется деятельность многих организаций.

Подводя итоги, отметим стремительный рост цифровой трансформации. Активное стимулирование со стороны правительства, влияние пандемии Covid-19, стремительное развитие технологий – все это указывает на необходимый характер адаптации организаций под актуальную ситуацию на рынке. В рамках цифровой трансформации происходит переосмысление и преобразование бизнес-моделей, согласно которым реализуется деятельность, а также бизнес-процессов. Для этого рекомендовано использовать специализированные информационные системы, однако не стоит забывать о наличии вероятности возникновения рисков, связанных с данными программными решениями, и быть готовыми оперативно реагировать и ликвидировать их возникновение. Эти шаги способствуют организациям оставаться конкурентоспособными несмотря на влияние ряда внешних и внутренних факторов, а также поддерживать экономическую эффективность на должном уровне.

Список использованных источников:

1. What is digital economy? [В Интернете] / авт. Deloitte. - 1 12 2021 г.. - https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html.Бизнес-процессы: как их описать, отладить и внедрить. Практикум. [Книга] / авт. Рыбаков М. Ю. . - [б.м.] : Издательство Михаила Рыбакова, 2016. - стр. 392.
2. Методические рекомендации [В Интернете] / авт. Минцифры. - 6 11 2020 г.. - 5 12 2021 г.. - https://digital.gov.ru/uploaded/files/metodicheskie-rekomendatsii-po-tsifrovoj-transformatsii-gk.pdf.

3. Полезные материалы. Суть цифровой экономики [В Интернете] / авт. РФ Правительство // О национальной программе. - 1 12 2021 г.. - https://digital.ac.gov.ru/poleznaya-informaciya/4213/.
4. Реинжиниринг корпорации: Манифест револючии в бизнесе. Пер. с англ. / авт. Ч. Д. Хаммер Дж. Чампин. - 1997 г..
5. Цифровая трансформация в России - 2020 / авт. KMDA. - Москва : [б.н.], 2020 г.

УДК 005.86:005.334:336.7

Управление риском отмывания преступных доходов через банковский сектор экономики

Д.А. Усачева
студент 2 курса магистратуры ФГАОУ ВО «Севастопольский государственный университет», Севастополь
E-mail: dianka.usacheva.98@mail.ru
Ю.Ю. Шеина
студент 2 курса магистратуры ФГАОУ ВО «Севастопольский государственный университет», Севастополь
E-mail: Julua_Sheina1999@mail.ru
Научный руководитель: Н.В. Алесина
к.э.н., доцент кафедры «Финансы и кредит» ФГАОУ ВО «Севастопольский
государственный университет», Севастополь
E-mail: alesina_nv@mail.ru

Аннотация: *Легализация преступных доходов и финансирование терроризма невозможны без участия кредитных организаций, в силу чего проблема оценки рисков использования банковского сектора в этих целях является весьма актуальной. В статье представлены итоги анализа сомнительных операций банковского сектора, рассмотрена программа управления рисками в кредитных организациях.*

Ключевые слова: *банковский сектор, отмывание денежных средств, управление риском, сомнительные операции, Банк России, Росфинмониторинг. экономические преступления.*

Managing the risk of laundering criminal proceeds through the banking sector of the economy

Abstract: *Legalization of criminal proceeds and financing of terrorism are impossible without the participation of credit institutions, so the problem of assessing the risks of using the banking sector for this purpose is very urgent. The article presents the results of the analysis of dubious operations of the banking sector, considers the risk management program in credit institutions.*

Keywords: *banking sector, money laundering, risk management, questionable transactions, Bank of Russia, Rosfinmonitoring. economic crimes.*

В сфере противодействия легализации доходов, полученных преступным путем, основным риском кредитной организации является риск отмывания денежных средств.

Через банковский сектор производится подавляющее большинство операций с денежными средствами в наличной и безналичной формах. В связи с этим недобросовестные клиенты могут воспользоваться благоприятными условиями рассредоточения сомнительных активов и маскировки преступных доходов, тем самым реализовывая схемы легализации (отмывания) денежных средств.

По данным ООН за год легализуется порядка 2-5% от мирового ВВП, что составляет 1,6-4 триллиона долларов.

По оценкам, представленным в Российском обзоре экономических преступлений, совершенных за 2020 год, в РФ зафиксировано 950 преступных деяний в сфере легализации (отмывания) доходов. На основании полученных данных были выявлены следующие тенденции (Таблица 1) [1].

Таблица 1 – Динамика экономических преступлений, совершенных в России и преступлениях в области легализации доходов в России за 2016-2020 гг., ед.

Выявленные преступления	2016	2017	2018	2019	2020
Экономической направленности	108754	105087	109463	104927	105480
в том числе в области легализации доходов, полученных преступным путем	818	711	993	946	950
Всего преступлений	2160063	2058476	1991532	2024337	2044221

Из данных таблицы видно, что динамика выявленных экономических преступлений и преступлений в области отмывания преступных доходов волнообразна. Так, в 2017 году, в сравнении с 2016 годом, число выявленных экономических преступлений уменьшилось на 3 667 ед. или на 3,37%, в 2018 году был заметен рост таких преступлений на 4 376 ед. или на 4,16%, в 2019 году - снижение до 104 927 ед., а в 2020 г. снова рост до 105 480 ед. Подобно динамике выявленных экономических преступлений меняется и число выявленных преступлений в области легализации доходов, полученных преступным путем, что наглядно отображено на графике (Рисунок 1).

Рисунок 1 – Динамика экономических преступлений в области легализации преступных доходов в России за 2016-2020 гг.

Легализация преступных доходов — это серьезное экономическое преступление. Преступники с помощью использования финансовых операций и обычной хозяйственной деятельности стремятся скрыть истинное происхождение и назначение использования принадлежащих им денежных средств, которые обычно связаны с коррупцией, уклонением от уплаты налогов, наркобизнесом, деятельностью террористических организаций и другими видами организованной преступности. Во избежание сокрытия преступных доходов с использованием кредитных организаций Центральный Банк РФ осуществляет мероприятия, направленные на борьбу с сомнительными операциями в финансовой системе во взаимодействии с Росфинмониторингом, правоохранительными органами, Федеральной налоговой службой и другими контрольно-надзорными органами.

Общий перечень сомнительных операций определен в ст. 6 ФЗ №115[2]. Положения настоящего закона постоянно обновляются и дорабатывается в целях обеспечения возможности выявления вновь возникающих преступных схем. Последняя редакция была принята 28.10.2021 года.

В результате целенаправленной борьбы объемы сомнительных операций в последние годы имели устойчивую отрицательную динамику. Согласно данным Банка России, в российском банковском секторе в 2020 году они сократились на 26%.

По сравнению с 2019 годом вывод денежных средств за рубеж по сомнительным основаниям уменьшился на 20 %. (Рисунок 2) [3].

Рисунок 2 – Количество сомнительных операций в банковском секторе РФ в 2014-2020 гг., млрд. руб.

В соответствии с данными о числе сомнительных операций, осуществляемых через банковский сектор РФ за анализируемый период, наблюдается отрицательная динамика с 2014 года по 2020 год. Такие изменения связаны с усилением контроля за банковскими операциями в связи с установками Финмониторинга. Кроме того, на сокращение сомнительных операций в значительной степени влияет цифровизация банковской сферы, которая позволяет эффективнее отслеживать и быстрее пресекать данные злоупотребления. Благодаря действующему антиофшорному законодательству и возможностью взаимного обмена информацией о движении денежных средств по счетам заграницей между налоговыми органами разных стран, сокрытие преступниками своих доходов также осложняется. ФНС Российской Федерации автоматически получает выявленные данные о сомнительных транзакциях на иностранных счетах налогоплательщиков от иностранных налоговых служб в соответствии с Положениями Конвенции о взаимной административной помощи по налоговым делам и Страсбургской конвенции. Благодаря чему известная предпринимателям типология отмывания денежных средств становится неэффективна, и, соответственно, используется значительно реже.

На графике прослеживается сокращение объемов вывода денежных средств за рубеж: в 2014 году сумма выведенных за пределы страны денег составляла 816 млрд. руб., в 2015 г. она уменьшилась до 501 млрд. руб., т.е. на 61 %. В 2016 году анализируемый показатель продолжил тенденцию к сокращению (сумма выведенных средств составила 183 млрд. руб.). В 2020 году было выведено за рубеж только 53 миллиарда рублей. Кроме того, удельный вес преступлений, связанных с обналичиванием денежных средств в составе сомнительных операций так же сократился.

В 2020 году Банку России совместно с кредитными организациями удалось минимизировать риски вывода денежных средств по таким каналам как:

– сомнительные операции, связанные с международными транспортными перевозками;
– сомнительные операции с ценными бумагами;
– сомнительные сделки по оказанию рекламных услуг.

Кроме того, сократился объем вывода денежных средств по неоднократным переуступкам долга между недобросовестными участниками при осуществлении внешнеэкономической деятельности, а также нерезидентами по поставкам товаров [3].

Проведя анализ экономических преступлений в области отмывания преступных доходов, а также анализ сомнительных операций, следует понимать, что легализовать преступные доходы без участия банковской системы государства невозможно. Финансовые организации являются частью подавляющего большинства схем отмывания денежных средств, используемых преступниками. Именно поэтому осуществление контроля над исполнением кредитными организациями требований законодательства (Федерального закона № 115-ФЗ) является важнейшим аспектом системы противодействия легализации преступных доходов и финансирования терроризма в целом [2].

Ключевыми аспектами деятельности кредитных организаций в сфере минимизации рисков отмывания доходов являются:

– своевременное выявление существующих рисков;
– объективная оценка риска;
– эффективное управление риском, направленное на его устранение или снижение до допустимого уровня; [4, с. 42].

Управление риском отмывания доходов, полученных преступным путем, представляет собой совокупность мер, принимаемых кредитными организациями с целью выявления, оценки и минимизации риска путем применения инструментов, предусмотренных законодательством РФ [5].

При осуществлении мер, направленных на минимизацию рисков ОД/ФТ, кредитная организация вправе:

– запросить у клиента дополнительную информацию для подтверждения законности операции;
– отказать клиенту в проведении операции, если имеются сведения, что она проводится в целях ОД/ФТ;
– отказать клиенту в открытии банковского счета (вклада);
– расторгнуть договор банковского счета с клиентом.

Субъекты первичного финансового мониторинга, в том числе кредитные организации, обязаны разрабатывать правила внутреннего контроля (ПВК), в которых отображены основные программы управления риском отмывания (легализации) денежных средств. Требования к составлению ПВК содержатся в Положении Банка России №375-П, однако данный перечень не является исключительным [5].

В рамках осуществления ПВК кредитная организация:
– устанавливает собственную программу по идентификации клиента и его представителя, бенефециарного владельца и выгодоприобретателя;
– устанавливает порядок проведения идентификации и случаи упрощенной идентификации клиента;
– разрабатывает меры по выявлению государственных должностных лиц, в т.ч. иностранных;
– определяют способы взаимодействия с клиентом;
– устанавливают требования к форме и содержанию анкеты в целях идентификации клиента;
– проводит оценку уровня риска сомнительных сделок, а также причин возникновения такого риска, и т.д. [6, с. 63].

В целях осуществления внутреннего контроля кредитные учреждения должны разработать программу управления рисками отмывания денег и финансирования терроризма, в соответствии с которой они обязаны принимать меры по отнесению клиентов к определенным классам на основе критериев риска для операций, осуществляемых клиентом в незаконных целях, а также определять риск вовлечения банка и его сотрудников в использование банковских продуктов для отмывания денег [7].

Программа управления рисками отмывания денег и финансирования терроризма содержит в себе:
– методы выявления и оценки таких рисков в деятельности клиентов и рисков использования услуг банка в схемах отмывания денег;
– порядок назначения и анализа уровня выявленных рисков;
– функции для мониторинга транзакций клиентов и т.д.

Программа идентификации операций клиентов, подлежащих обязательному контролю, и операций, которые могут быть заподозрены в

совершении в целях отмывания денег и финансирования терроризма, должна включать:

- признаки, свидетельствующие о сомнительности операций;
- особенности идентификации операций, подлежащих обязательному контролю, и операций с признаками подозрительности;
- процедура углубленной проверки документов и информации о клиенте с целью доказательства или опровержения возникающих сомнений в наличии признаков подозрения в его деятельности;
- порядок, основания и условия принятия решения об отнесении операций к определенному классу рисков;
- порядок документирования информации об операциях, а также предоставления такой информации в Росфинмониторинг и т.д.

Кредитные организации также обязаны разрабатывать программы применения защитных мер в отношении своих клиентов, мер по замораживанию (блокированию) средств или иного имущества клиентов и т.д.

Все вышеперечисленные меры направлены на сокращение рисков вовлечения кредитных организаций и их клиентов в схемы отмывания денег и финансирования терроризма.

Несмотря на это, на практике встречаются ситуации, когда вопреки принятым мерам, банковские учреждения в ходе деятельности допускали рисковые случаи, связанные с отмыванием доходов. Результатом таких случаев могут послужить прямые или косвенные финансовые потери для представителей данного сектора. Кроме того, существуют и обратные ситуации, когда физические лица - клиенты банка при осуществлении предпринимательской деятельности (например, самозанятые лица) сталкивались с проблемой приостановления операций по счетам из-за стабильных периодических поступлений на них денежных средств из разных источников. Эта проблема нашла свое решение и в данном случае предпринимателям разрешили открывать отдельный счет для ведения предпринимательской деятельности и личный счет.

Таким образом, эффективность управления риском отмывания преступных доходов с использованием банковского сектора направлена на предотвращение вовлечения кредитных организаций в преступные схемы в качестве инструмента отмывания денежных средств и финансирования терроризма, и на осуществление должного контроля над исполнением банковскими учреждениями требованиям законодательства в сфере ОД/ФТ.

Список использованных источников:

1. Официальный сайт МВД России. [Электронный ресурс]. – Режим доступа: https://мвд.рф/ / (Дата обращения 18.11.2021)
2. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее - Федеральный закон № 115-ФЗ). [Электронный ресурс]. – Режим доступа: http://www. consultant.ru. (Дата обращения 17.11.2021).
3. Официальный сайт Банка России [Электронный ресурс]. – Режим доступа: https:// https://cbr.ru/ (Дата обращения 15.11.2021).
4. Ионина Т.Р. Актуальные риски легализации преступных доходов в банковском секторе и программы их минимизации/ Т.Р. Ионина. - Текст: непосредственный // Вестник экспертного совета - №3. – С. 42-47.
5. Положение Банка России от 02.03.2012 № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». [Электронный ресурс]. – Режим доступа: http://www.consultant.ru (Дата обращения 17.11.2021).
6. Маскутова А.А. Контроль за проведением сомнительных операций клиентами кредитных организаций и оценка риска вовлечения кредитных организаций в отмывание незаконно полученных доходов / А.А. Маскутова. - Текст: непосредственный // Проблемы экономики и юридической практики - №4. – С. 62-66.
7. Официальный сайт Федеральной службы по финансовому мониторингу [Электронный ресурс]. – Режим доступа: http://www.fedsfm.ru (Дата обращения 17.11.2021).

УДК 004:364-7:005.521

Цифровизация отраслей социальной сферы: перспективы и риски

Н.А. Оразбаева
студент 2 курса магистратуры КарУ имени академика
Е.А. Букетова,
Караганда
E-mail: orazbaeva.nursulu@bk.ru
Научный руководитель: С.Ш. Мамбетова
к.э.н., доцент кафедры менеджмента КарУ имени академика
Е.А. Букетова, Караганда
E-mail: sagynysh.2012@mail.ru

Аннотация: *благодаря использованию цифровых технологий социальный сектор становится мобильным, подверженным изменениям, и, соответственно, повышается качество социальных услуг. В статье рассматриваются предпосылки и условия широкого использования цифровых технологий в социальной сфере, а также риски использование цифровизации в социальной сфере.*
Ключевые слова: *цифровизация социальной сферы, информатизация, цифровое неравенство, социальные риски, социализация информации.*

Digitalization of social sectors: prospects and risks

Abstract: *thanks to the use of digital technologies, the social sector becomes mobile, subject to change, and, accordingly, the quality of social services increases. The article discusses the prerequisites and conditions for the widespread use of digital technologies in the social sphere, as well as the risks of using digitalization in the social sphere.*
Keywords: *digitalization of the social sphere, informatization, digital inequality, social risks, socialization of information.*

В наше время протекает период в обществе, в котором совершаются значительные перемены в различных конфигурациях предоставления общественных услуг, сопряженные с "числовой трансформацией" государственного управления, а также ключевых разделов социальной сферы. Принимая во внимание массовые характерные черты информатизации социальной сферы, и общества в полной мере, необходимо выделить, то что все без исключения больше выявляются

только лишь технические нюансы данного процесса, его воздействие на формирование производственных взаимоотношений и новейших технологий. В наименьшем уровне предусматриваются социальные элементы информатизации. Несмотря на те нюансы культуры считаются более значимыми с целью сообщества с точки зрения их результатов, их возможно пренебрегать. Предпосылками цифровизации общественной области считаются применение информативных технологий с целью увеличения качества существования, а также условий с целью расширения человеческого капитала.

В своем понимании цифровая трансформация раскрывает сущность свою как в создании соответствующей инфраструктуры, так и активность участников рынка, и надлежащее использование цифровых ресурсов. Государство, которое преуспевает в области цифровизации и нацелено на передовые технологии будущего открывает путь к улучшению качества, скорости и эффективности всех процессов.

Социальная сфера включает в себя предоставление ряда базовых услуг в области здравоохранения, образования, культуры и спорта. В связи с этим, развитие и трансформация именно социальной сферы станет отражением происходящих в обществе тенденций.

Главной целью цифровизации социально-трудовой области считается облегчение управленческих операций, предоставление наибольшей прозрачности, а также доступности общественной поддержки и помощи людям, но кроме того оптимизация действий принятия решений с помощью формирования концепции умственного рассмотрения и моделирования будущего на базе больших данных.

На сегодняшний день цифровая трансформация охватила достаточно многие сферы жизнедеятельности, такие как производство и бизнес, а также каждого отдельного жителя земного шара. Согласно имеющихся условиям, цифровизацию стоит рассматривать не только как неизбежность всего общества, но и как процесс, становящийся обновленной основой взаимодействия и существования людей в будущем.

Предоставление стремительного введения числовых технологий в социальной сфере на территории страны — это одна из целей государственного развития. Вследствие применения цифровых технологий, социальная сфера приобретает статус мобильной, берет на себя перемены также, равно как результат, свойство социальных услуг улучшается. Однако, в то же время цифровые технологические процессы никак не считаются общественно промежуточными — с одной стороны, они раскрывают новейшие возможности, способности также постановления с целью сообщества, но с иной стороны, они кроме того считаются основой общественных устремлений.

Трансформация нынешнего сообщества к модификации цифрового формирования — проявление не только лишь всемирное и по этой причине потребуется детального корректировки государственных общественно-политических стратегий, однако также сравнительно недостаточно исследовано с точки зрения сопряженных с ним социально-политических рисков. Для нашего государства многофункциональность инноваций, а также научно-технических действий в комбинации с их значительным риском формирует несколько вопросов и опасностей, которые приводят к созреванию посылов с целью предстоящих инцидентов и потрясений во всем мире. По этой причине, на сегодняшний день обговорить не только лишь достоинства числового формирования, а также задать вопрос об его общественных также общественно-политических вопросах и кроме того об создании новейшего, техносоциального целевого сообщества.

Так в настоящее время, проводится применение массово цифровых технологий в социальной сфере лишь только в небольшом количестве стран, это объясняется тем, что необходимо соблюдать ряд условий.

Во-первых, готовность социальной сферы к трансформации и применению цифровых технологий является важной частью стратегии развития. Во-вторых, довольно продвинутая и развитая технологическая сфера в стране, позволит быстрее адаптироваться и ускорить процесс перевода социальной сферы на цифровой лад. В-третьих, вовлеченность самого населения в активное использование цифровых технологий позволит указать на необходимость его внедрения в социальную сферу, опираясь на потребности общества.

На территории Республики Казахстан цифровизация социальной сферы — это амбициозная цель, которая отражает развитие страны и населения в целом. Отрасли социальной сферы становятся мобильными и менее чувствительны к различным переменам благодаря применению цифровых технологий, которое предопределяет рост качества оказываемых услуг. Наличие цифровых технологий и их явное применение предполагает свои перспективы, возможности, в то же время выступает источником социальных рисков.

Риски цифровизации социальной сферы:

- утечка информации;
- недостоверность информации;
- утрата старых профессий, что повлечет за собой потерю рабочих мест;
- нарушение личной жизни, увеличение краж персональных данных;
- хакерство, угроза безопасности;
- рост уровня сложности и потеря контроля.

Цифровая трансформация предполагает уход от бумажной волокиты. Большинство внутренних процессов должно функционировать с применением передовых технологий. Внедрение в социальные отрасли технологий направлено на автоматизацию социальной помощи многим слоям населения, но в то же время возникает проблема в оказании помощи более пожилым слоям.

Под результатами цифровизации как уже существующие, так и будущие (прогнозируемые) понимают [1, 63]:

- возрастание степени сосредоточения информации на социальную сферу;
- образование предпосылок роста уровня населения в культурном плане в результате развития цифровой сферы;
- неравенство населения в следствии цифровизации — риск поляризации знаний в обществе;
- увеличение роста новых профессий, риск утраты целого ряда профессий.

Предоставленные выше отрицательные стороны цифровизации перекрывают ее положительные, такие как:

- повышенный уровень прозрачности;
- рост объема легкодоступной информации;
- скорость в предоставлении и обменом информацией;
- свобода слова, возможность самореализации;
- отсутствие расстояния во время коммуникации с людьми и организациями;
- доступ и более эффективное использование государственных услуг;
- доступ к профессиональным знаниям, появление новых рабочих мест.

Происходящие изменения и их неизбежность, напротив нацелены на создание системы общих ценностей для проведения трансформаций, которые преобразуют четвертую промышленную революцию в новые возможности для всех членов общества.

С целью постановления данной проблемы Министерство вместе со специалистами также резидентами предпринимательство-общества создал новейшие комбинация к цифровизации здравоохранения.

Подобным способом, система самочувствия базируется в заинтересованностях больного также разделяется на 4 сферы:

- предотвращение болезней и соперничество с ними;
- раннее обнаружение болезней;
- врачебная поддержка;
- терапия и восстановление затяжных болезней [2].

Принимая во внимание не так давно произошедшие массовые негативные действия, в том числе всемирную пандемию, карантинные лимитирования, а также финансовые потрясения, здравоохранение считается один с основных ценностей для каждого государства.

Инновационные информативные технологические процессы увеличили информированность людей об льготе в общественное предоставление, однако данное только лишь основание цифровых изменений, имеется также прочие двигающие мощи перемен.

Таким образом, благодаря применению цифровых технологий в следующих отраслях: транспорт, торговля, образование, здравоохранение, социальная защита и государственный сектор значительно изменяется весь уклад жизни общества. В следствии, государство, которое имеет технологически развитую социальную сферу повышает свою конкурентоспособность на мировом рынке.

Список использованных источников:

1. Романова Н.В. Цифровизация услуг в социальной сфере: проблемы и перспективы / Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика, 2020. С. 58-65.
2. Цифровизация здравоохранения. URL: https://m.egov.kz/cms/ru/healthcare?mobile=yes, 2021.

УДК 004:336

Цифровой рубль: концепция суверенных валют

А.М. Сизов
аспирант Департамента Информационной Безопасности
Финансового Университета при правительстве РФ
E-mail: gipno2009@yandex.ru
Научный руководитель: Г.О. Крылов
д.ф.-м.н, к.т.н., к.ю.н, профессор, ЗРВШ профессор кафедры
информационной безопасности Финансового университета
профессор кафедры №75 НИЯУ МИФИ
E-mail: GKrilov@fa.ru

Аннотация: *в настоящее время можно наблюдать активный процесс цифровизации и компьютеризации всех процессов и систем общества. Цифровизация не обошла стороной и валюты и денежные отношения общества, и сейчас человечество стоит на пороге третьего вида валют – цифровых суверенных валют. В данной статье пойдет речь о специфике новой валюты Центробанка России – Цифрового Рубля, будут проанализированы документы, характеризующие и специфицирующие новую валюту, а также поставлены вопросы, которые необходимо решить в ходе разработки и тестирования новой валюты. Цифровой Рубль и суверенные валюты – важный и сложный новый шаг, который позволит ускорить транзакции, уменьшить их стоимость, интегрироваться с другими платформами и др.*

Ключевые слова: *цифровой рубль, распределенный реестр, блокчейн, информационная безопасность, информационные угрозы, суверенная валюта.*

Digital ruble: the concept of sovereign currencies

Abstract: *at present, one can observe an active process of digitalization and computerization of all processes and systems of society. Digitalization has not bypassed the currencies and monetary relations of society, and now humanity is on the verge of a third type of currency - digital sovereign currencies. This article will discuss the specifics of the new currency of the Central Bank of Russia - the Digital Ruble, will analyze the documents that characterize and specify the new currency, and also raise questions that need to be addressed during the development and testing of a new currency. The Digital Ruble and sovereign*

currencies are an important and complex new step that will speed up transactions, reduce their cost, integrate with other platforms, etc.

Keywords: *digital ruble, distributed ledger, blockchain, information security, information threats, sovereign currency.*

Сейчас в мире можно наблюдать активное изменение процессов общества, их цифровизацию и автоматизацию. Практически любая сфера жизни общества неизбежно переводится в компьютерный формат, где она проходит этапы автоматизации и адаптации к использованию в новых современных реалиях. Наблюдать данный процесс можно с активного развития компьютеров и компьютерных систем, а именно с 2000-2005-х годов.

Помимо активного развития компьютерных систем, также развиваются и остальные системы, включая финансовые, речь о которых и пойдет в данной статье. За последнее десятилетие можно было наблюдать за изменением концепции платежей, когда бумажную валюту практически полностью сменила технология электронных быстрых платежей. По прогнозам экспертов, к концу 2021 года доля безналичных операций в объеме платежей превысит 74%, а доля в числе транзакций станет выше 65%[1]. Причина такого разброса очевидна: в эпоху цифровизации намного быстрее и удобнее расплачиваться системой быстрых платежей, так как для этого требуется только «нажатие нескольких кнопок» и электронный девайс (смартфон), который сейчас используется практически повсеместно.

Однако, на заре стоит «третья форма денег» — это цифровая суверенная валюта. После относительного успеха и большом использовании новых валют, основанных на технологии Блокчейн (криптовалют) различные государства задумались о введении собственных валют, частично или полностью основанных на аналогичной технологии.

Суверенная валюта – это такая валюта, эмитентом и абсолютным владельцем которой является исключительно Центральный Банк (далее – ЦБ) какого-либо государства. Соответственно, суверенная валюта, выпускающийся ЦБ Российской Федерации – это и цифровой рубль (далее – ЦР). Другой важной характеристикой суверенных валют является их цифровая составляющая, то есть то, что они базируются и работают при помощи компьютерных технологий, и в основном при помощи технологии распределенных реестров.

Первоначально, в документе «Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы», утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203, и программы «Цифровая экономика Российской Федерации», утвержденной

распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. указана необходимость введения ЦР в повсеместное использование к 2030 году, а также введение в начале 2022 валюты в тестовом режиме. Также, концепция Цифрового Рубля была описана в докладе для общественных консультаций Центробанка в октябре 2020 года, а затем конкретизирована в документе «Концепция цифрового рубля» в апреле 2021 года [3].

Многие государства обсуждают или реализовывают переход на суверенные цифровые валюты из-за следующих преимуществ:

1. Уменьшение стоимости транзакций, а также увеличение скорости их проведения;
2. Повышение доступности безналичных платежей за счет офлайн режима оплаты валютой;
3. Гарантируемая Центробанком защищенность средств;
4. Возможность интеграции с другими платформами;
5. Другие преимущества.

Модель Цифрового рубля была представлена в докладе Центробанка России «Концепция цифрового рубля».

Модель D представляет собой двухуровневую розничную модель.

Первый уровень – Банк России.

Оператор платформы (Банк России):

- создает, сопровождает и развивает платформу цифрового рубля;
- подключает финансовые организации и Федеральное казначейство к платформе цифрового рубля;
- определяет правила осуществления операций на платформе цифрового рубля;
- создает и распространяет стандарты для работы с платформой цифрового рубля;
- определяет политику обеспечения информационной безопасности и киберустойчивости платформы цифрового рубля.

Эмитент (Банк России):

- проводит эмиссию цифровых рублей, обладает собственным эмиссионным онлайн-кошельком;
- обеспечивает зачисление и списание цифровых рублей для финансовых организаций и Федерального казначейства;
- осуществляет открытие кошельков финансовым организациям и Федеральному казначейству на платформе цифрового рубля.

Второй уровень – финансовые организации и Федеральное казначейство.

Финансовая организация:

– осуществляет открытие и пополнение кошельков клиентам на платформе цифрового рубля;
– осуществляет процедуры, предусмотренные законодательством в сфере ПОД / ФТ / ФРОМУ, валютным законодательством;
– проводит проверки электронной подписи клиента, антифрод-проверки, проверку лимитов и реквизитов по операциям;
– осуществляет переводы и платежи по поручению клиентов на платформе цифрового рубля.

Федеральное казначейство:

– является специальным участником платформы цифрового рубля;
– осуществляет операции с кошелька Федерального казначейства в счет обеспечения деятельности бюджетных организаций.

Важной спецификой ЦР является возможность офлайн переводов, что является основательным преимуществом ЦР перед системой быстрых платежей. Центробанк описывает процесс офлайн-переводов следующим образом:

«Возможность офлайн-переводов предполагается обеспечить для C2C, C2B-, B2C-операций. Для совершения офлайн-операций, помимо онлайн-кошелька, клиенту будет открыт второй кошелек в цифровых рублях непосредственно на мобильном устройстве. Пополнение офлайн-кошелька будет осуществляться клиентом путем перевода цифровых рублей с его онлайн-кошелька при наличии доступа к сети Интернет. Планируется, что офлайн-перевод может выполняться с использованием технологии беспроводной передачи данных малого радиуса действия (например, Bluetooth, NFC).»

Стоит отметить основные различия между суверенными валютами и криптовалютами – валютами, которые работают на основе технологии Блокчейн. Цифровой рубль будет работать на основе гибридной технологии, используя преимущества как децентрализованных, так и централизованных систем. Из децентрализованных систем в ЦР войдут принципы распределенного реестра – данные о транзакциях будут храниться распределенно. Также, очень полезны будут принципы смарт-контрактов, при помощи которых можно будет создавать специальные алгоритмы, которые будут фиксировать и с точностью, с помощью компьютерного интеллекта, фиксировать статус выполнения сделки и ее оплату. Наконец, может быть использована технология «окрашенных монет» - когда, например, ЦР может быть использован только на какие-то конкретные цели – например, специальные государственные контракты или закупки.

Особенности распределенных реестров, а в частности технологии блокчейн, которые не будут использоваться – это полная

децентрализованность систем (по аналогии с биткоином), а также полная анонимность транзакций – очевидно, эти свойства не соотносятся со спецификой суверенных валют, так как государству необходим полный контроль и мониторинг системы цифровой валюты. Центробанку необходим полный контроль и централизация системы для возможности полного мониторинга всех транзакций для возможности, например, пресечения незаконных транзакций.

Одним из направлений, которое можно рассмотреть в концепции новых Цифровых Валют – это возможность внедрения механизмов анализа транзакций и своевременного предупреждения операторов (людей) о потенциально незаконных транзакциях. Например, при рисковых транзакциях система может передать оповещение оператору, при которым оператором вместе с алгоритмами будут рассмотрены и проанализированы другие операции учредителя транзакции, посредством которых оператор может сделать объективный вывод о законности данных транзакции. Данные возможности могут быть использованы из-за преимуществ полностью централизованной валюты и, соответственно, из-за централизованности информации о транзакции. Данное предложение является одной из потенциальных возможностей продуктивного и полезного использования новой технологической структуры валюты Цифрового Рубля.

Одним из важнейших вопросов при внедрении системы является статус цифрового рубля в системе, а именно связь «горизонтали» и «вертикали». ЦР должен работать по аналогии со стейблкоинами, то есть поддерживаться какой-либо фиатной валютой, в данном случае рублем. Это идет в разрез с концепцией криптовалют, которые являются идейным источником суверенных валют, так как их эмиссия работает по другим принципам (принципам майнинга), и они не поддерживаются какой-либо валютой, что делает их специфику неприменимой к суверенным валютам.

Остаются также другие вопросы технического характера, применимые к суверенным цифровым валютам: где будут размещены реестры цифрового рубля и соответствующих систем? Как будет проходить мониторинг транзакций цифрового рубля? Кто и как получит доступ к системам цифрового рубля, для, например, контроля противодействию ПОД/ФТ/ФРОМУ? Данные вопросы требуют дальнейшего анализа и подробного рассмотрения, ведь без спецификации данных вопросов невозможно корректное и безопасное функционирование валюты.

Заключение

В ходе работы был проведен анализ технологической составляющей цифрового рубля, были проведены сравнения данной концепции с существующими валютами, как реальными, так и цифровыми.

Цифровой рубль определенно является очень важным и перспективным шагом в новую экономику РФ. Однако, для корректного введения и использования технологии необходимо детально рассмотреть и решить вопросы как технического, так и экономического и социального характера.

Список использованных источников:

1. Больше половины всех банковских операций перешло в онлайн https://rg.ru/2021/08/17/bolshe-poloviny-vseh-bankovskih-operacij-pereshlo-v-onlajn.html (дата обращения: 13.10.2021)
2. Цифровой рубль. Доклад для общественных консультаций [Электронный ресурс] https://www.cbr.ru/analytics/d_ok/dig_ruble/ (дата обращения: 13.10.2021)
3. Концепция цифрового рубля. [Электронный ресурс] http://www.cbr.ru/content/document/file/120075/concept_08042021.pdf (дата обращения: 13.10.2021)
4. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system //Decentralized Business Review. – 2008. – С. 21260.
5. Estonia – the Digital Republic Secured by Blockchain. [Электронный ресурс] https://www.pwc.com/gx/en/services/legal/tech/case-studies/the-digital-republic-secured-by-blockchain.html (дата обращения: 13.10.2021)
6. Последнее китайское предупреждение биткоину. Компартия окончательно запретила криптовалюты [Электронный ресурс] https://www.bbc.com/russian/news-58681243 (дата обращения: 13.10.2021)
7. Крылов, Г. О. Проблемы безопасности оборота цифровых финансовых активов в криптоэкономике: монография / Г. О. Крылов, В. М. Селезнев. — Москва : Прометей, 2020. — 348 с.
8. Варнавский А. В., Бурякова А. О., Себеченко Е. В. Блокчейн на службе государства. – 2020.
9. Свон, М. Блокчейн. Схема новой экономики / Свон, М. – Москва: Олимп-Бизнес, 2017. – 240 с
10. Запорожан А. Я. ЦИФРОВОЙ РУБЛЬ ЦБ РФ //Управленческое консультирование. – 2021. – №. 6 (150). – С. 32-39.
11. Синельникова-Мурылева Е. В. Цифровой рубль: риски и выгоды //Экономическое развитие России. – 2021. – Т. 28. – №. 5. – С. 36-39.
12. Пшеничников В. В. Перспективы эмиссии цифрового рубля и его функционирования в платежном обороте страны //Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. – 2020. – Т. 13. – №. 6.

УДК 004:005.521

Что можно ожидать от цифровизации

А.Н. Норкина
к.э.н., доцент кафедры финансового мониторинга
НИЯУ МИФИ, Москва
E-mail:ANNorkina@mephi.ru
С.С. Носова
д.э.н., профессор кафедры финансового мониторинга
НИЯУ МИФИ, Москва
E-mail: SSNosova@mephi.ru

Аннотация: *рассматривается суть цифровизации как результат масштабного использования цифровых технологий в режиме современных интеграционных процессов в международном пространстве с целью усиления экономического потенциала страны. Раскрыты тенденции цифровизации, которые бросают нам вызов, прививают чувство прогресса, заставляют чувствовать светлое будущее. Исходя из этого обоснована степень влияния генерации цифровых технологий в трансформирующий фактор экономического прогресса.*
Ключевые слова: *пандемия COVID-19, цифровизация, цифровая экономика, цифровой бизнес.*

What can be expected from digitalization

Abstract: *the essence of digitalization is considered as a result of the large-scale use of digital technologies in the mode of modern integration processes in the international space in order to enhance the economic potential of the country. The tendencies of digitalization that challenge us, instill a sense of progress, make us feel a bright future are revealed. Based on this, the degree of influence of the generation of digital technologies on the transforming factor of economic progress has been substantiated.*
Keywords: *COVID-19 pandemic, digitalization, digital economy, digital business.*

Введение

В современную эпоху цифровизация стала важнейшей необходимостью во всех сферах экономики, что и является основой для ее долгосрочного успеха. Анализируя использование цифровых технологий как "ядра" взаимодействия науки, бизнеса и правительства, можно

утверждать о неизбежности повышения качества жизни человека и процветания общества в целом. В России определены пути последовательной реализации скоординированной стратегии на основе использования цифровых технологий во всех сферах экономической и общественной деятельности. Внедрение "цифрового духа" в социально-экономическую жизнь, особенно в области разработки технологий искусственного интеллекта, ускоряет достижения глобальных преимуществ и снижения рисков в современном экономическом развитии в ответ на пандемию COVID-19.

1 Теоретический анализ

Цифровые технологии экспоненциально увеличивают состояние информационного пространства, а значит и масштаба трансформации экономической деятельности. [8] В этой связи меняется структура экономической системы, а вместе с ней и ее динамические свойства, так как ключевым элементом процесса цифровой трансформации является переход от аналоговых или физических технологий к цифровым системам данных. В этой связи развитие цифровизации следует рассматривать как новое явление в современной экономической жизни, так как она "проявляется в появлении совершенно новых технологий, таких как большие данные, облачные технологии, искусственный интеллект". [1] Цифровые технологии меняют всю экономическую жизнь: покупки клиентов (например, Amazon), занятость (Uber), инвестиции (Betterment и Wealthfront), создание стоимости. Именно, в этой связи использование цифровых технологий заставляет компании пересмотреть текущую стратегию и научиться справляться с проблемами, вызванными увеличением цифровизации. Сегодня Убер. Airbnb. Амазонка, Яблоко, PayPal являются лидерами отрасли. Ожидается, что цифровые платформы будут иметь потенциал для множества целей для промышленных предприятий, например, при интеграции в концепцию Индустрии 4.0. Цифровые платформы становятся все более и более устоявшимися в нынешнюю цифровую эпоху, и с ней приходит много новых бизнес-идей и моделей. В этом аспекте цифровые технологии, должны стать движущей силой экономического прогресса. [7] Целесообразно подчеркнуть, что "основа для успешного внедрения ИИ в контексте цифровой трансформации предлагает конкретные рекомендации в области интеллекта, интеграции, гибкости и лидерства бизнес-компаний. [2,110] Доминирующая логика исследований в области управления по-прежнему основывается на предположениях, полученных из неоклассической экономики, где агрегированные данные анализируются на основе использования эконометрических подходов и, соответственно, предположения о рациональном поведении производителя и потребителя.

Как утверждают эксперты, это также является неотъемлемой частью менеджмента в условиях цифровизации. Но подчеркивается, что цифровизация экономики может повлиять на "внедрение принципиально новых бизнес-возможностей и бизнес-моделей." [3, 537] Итак, в основе различных трансформационных процессов стоит переход от индустриально-рыночной к информационно-сетевой системе управления, определяющей исторический смысл современного этапа развития общества. [6] Иначе говоря, цифровизация приведет к росту производства, ведь она позволяет снизить операционные затраты и дает возможность компаниям уменьшить свою зависимость от такого фактора, как разница в уровнях оплаты труда в разных странах. [5] В этих условиях появляются новые требования к управлению трансформационными процессами. Информация все больше становится объектом мошеннических действий. [10]

2 Результаты

2.1. Цифровизация рабочих мест: постановка вопроса

Ключевой вопрос в исследованиях и дебатах о цифровизации - это проблема поляризации рабочих мест и заработной платы. В странах со стареющим населением темпы вхождения в рабочую силу замедляются по сравнению с выходом. Кроме того, фирмы сообщают о несоответствии навыков для имеющихся рабочих мест. Эти изменения повышают стимул к автоматизации рабочих мест, но также облегчают адаптацию, поскольку на рынке труда будет меньше участников, ищущих рабочие места. В то же время сопоставление навыков и имеющихся рабочих мест может по-прежнему оставаться проблемой и представляет собой задачу сделать период адаптации менее трудным с точки зрения рисков для социального обеспечения. Отсюда успехом к благосостоянию в этот период перемен является гибкий рынок труда с равными возможностями. Более общая гибкость помогла бы сгладить структурные изменения и снизить риск роста структурной безработицы в переходный период. Только экономика совместного использования может обеспечить некоторую необходимую гибкость – если она будет процветать. Это позволит людям переключаться между фрилансом - образованием - регулярным трудоустройством.[4] Для того чтобы экономика совместного использования функционировала хорошо, необходимо адаптировать системы социальной защиты и системы социального обеспечения. Системы в Швеции и многих других странах рассчитаны на полную занятость в одном учреждении или фирме. Люди, работающие внештатно в качестве самозанятых или в небольших компаниях, с трудом вписываются в эту рамку. Эта тема широко обсуждается в докладах и правительственных комиссиях западных стран.

2.2. Проблема самозанятых в условиях цифровизации

Проблема самозанятых не в том, что эти люди идут на более высокий риск по целому ряду жизненноважных вопросов, таких как предпочтение большей свободы или стремление к росту вознаграждения. Проблема скорее в том, что асимметрия между самозанятостью и занятостью особенно велика в развитых странах, особенно это наглядно в Швеции. Например, самозанятые платят в систему социального обеспечения, чтобы претендовать на ее услуги, но они не могут в той же степени пользоваться этими льготами, поскольку вся структура построена вокруг статуса работника со всеми сопутствующими правами и льготами (отпуск по уходу за ребенком, оплачиваемый отпуск, дополнительные пенсионные права, гарантия занятости). Согласно одному из расчетов, работники получают 88 процентов денег обратно в течение жизни от взносов на социальное обеспечение, выплачиваемых их работодателями. Соответствующий показатель для самозанятых составляет около 49 процентов. Из-за характера деловых обязательств в небольших фирмах самозанятые не могут брать больничные или отпуск по уходу за ребенком. Самозанятые теоретически могут находиться в отпуске по уходу за ребенком в будние дни, но тогда они получают более низкие пособия. Чтобы получить полное пособие, родители должны использовать семь дней отпуска в неделю, включая выходные. Неопределенность может быть наибольшей при переходе от наемного работника к самозанятому, когда риск банкротства фирмы может быть высоким. В целом, системы льгот, ориентированы на то, чтобы лучше быть наемным работником, чем самозанятым. Позиция, занятая экспертами, заключается в том, что в условиях цифровизации в будущем так же будет работа, как и в прошлом.

2.3. Стратегия кибербезопасности

Цифровые взаимодействия между предприятиями и потребителями создают сегодняшнее сетевое общество через мощные информационные системы и подключенные устройства. В этом свете продолжает укореняться исследование, которое фокусируется на интеграции (цифровых) ресурсов поставщиками услуг и клиентами услуг для совместного создания ценности в системах обслуживания. Быстрый прогресс в области информационных технологий позволяет разрабатывать новые информационные системы, которые позволяют создавать совершенно новые конфигурации сервисных систем и технологий. Все это способствует росту цифровизации и в тоже время этот рост сопровождается киберугрозами и киберрисками в виде вредоносных программ, эскалации организованной киберпреступности, утечки личной информации и данных. В этой связи страны должны подготовиться к борьбе с финансовыми махинациями[10]. С целью процветания

цифровизации в России необходима эффективная стратегия кибербезопасности, соответствующая международным стандартам и служащая для сохранения информационных активов организаций, достижения состояния защищенности личности, государства и общества, как от внутренних, так и внешних информационных угроз. Главный ее принцип заключается в поддержке последовательного подхода к таким аспектам кибербезопасности, как правовые, технологические и организационные Перспективой национальной стратегии кибербезопасности является выявление ключевых направлений, адресованных организациям (администрации или предприятию) с целью разработки благоприятной рекомендательной базы для реализации ее стратегии, обеспечивающей приемлемый уровень информационной безопасности. Основной целью стратегии является разработка платформы, основанной на успешном опыте стратегий кибербезопасности и разворота международных стандартов и референтов. Для того, чтобы страны могли процветать в цифровой экономике, разрабатывается стратегия на национальном уровне, чтобы обеспечить необходимую основу и инфраструктуру для обеспечения безопасности киберпространства. Странам необходимо сбалансировать потребности цифровых экономик и обеспечить надежность и безопасность киберпространства.

Заключение

1. Если России удастся создать цифровую бизнес-среду, то она выйдет на мировой уровень глобальной цифровизации.
2. Чтобы уменьшить асимметрию между наемным работником и фрилансером с точки зрения риска, необходимо упростить для фрилансеров использование и получение выгод от социального обеспечения. Основная идея состоит в том, чтобы люди получали более высокие доходы после уплаты налогов, одновременно снижая риск роста неравенства.
3. В условиях цифровизации информация может быть использована в мошеннических целях. Кибератаки являются самой высокой угрозой информационной безопасности. Чтобы остановить или, по крайней мере, уменьшить кибератаки, необходимо рассматривать кибербезопасность как важнейший элемент экономического прогресса.

Данная работа поддерживается программой повышения конкурентоспособности НИЯУ МИФИ

Список использованных источников:

1. Belk, R. (2014). You are what you can access: Sharing and Sharing consumption on the Internet. J. Bus. Res. (67 (8)): 1595-1600

2. Davenport T.H., Ronanki R. (2018) Artificial Intelligence for the Real Word // Harvard business rev. - Boston, (96 (1/2): 108-116.
3. Gomber, P., Koch, Ya. & Siring, M. (2017). Digital finance and Fintech: current research and future research directions. Economy Bus 87, 537-580 doi.
4. Hall J. W., Kruger A. B. **(**June 2017**)** Job Market Analysis for Uber Driver Partners in the USA Industrial and Labor Relations Survey 71 (10) doi
5. PwC (apr, 2018) named the leaders in digitalization. (itweek.ru)
6. Rogers, D. (2017). Digital transformation. ISBN: 978-5-9909347-7-1 (chitai-gorod.ru)
7. The new digital economy. How it will transform business (White paper). 2011. Oxford, Oxford Economics.
8. Nosova, S., Norkina, A., Makar, S., Fadeicheva, G. (2021) Digital transformation as a new paradigm of economic policy // Procedia Computer Science, Vol. 190 pp. 657-665 doi
9. Nosova, S., Norkina, A.. (2021) Digital technologies as a new component of the business process // Procedia Computer Science, Vol. 190 pp. 651-656 doi
10. Носова С.С., Норкина А.Н., Морозов Н.В. (2021) Типологии финансовых махинаций. Москва: КНОРУС: 476