

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Национальный исследовательский ядерный университет
«МИФИ»

**Материалы
III Международной
студенческой научной конференции**

**«Инновационные механизмы
управления цифровой и региональной
экономикой»**

17-18 июня 2021 г., Москва

Москва 2021

УДК 338.2:001.895
ББК 65.050.2
М43

Материалы III Международной студенческой научной конференции «Инновационные механизмы управления цифровой и региональной экономикой», 17-18 июня 2021 г., Москва. М.: НИЯУ МИФИ, 2021. - 108 с.

В сборнике рассматриваются научные исследования и имеющиеся практики в области экономических реформ XXI века, включая проблемы развития институтов планирования и управления, а также технологий, методик и приемов обеспечения цифровых трансформаций.

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

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

Материалы издаются в авторской редакции
Получены до 17.06.2021

ISBN 978-5-7262-2803-7

© НИЯУ МИФИ, 2021
© Авторы статей, 2021

Подписано в печать 20.07.2021. Формат 60х84 1/16.
Печ. л. 6,75.
*Национальный исследовательский ядерный университет
«МИФИ»
115409, Москва, Каширское ш., 31*

Содержание

<i>Анализ особенностей деятельности и рисков субъектов малого предпринимательства в строительной отрасли</i> Д.Ю. Елкина, Е.К. Курдина	4
<i>Анализ ценообразования в сфере закупок услуг по проведению внешнего аудита</i> В.М. Сушков, П.Ю. Леонов	11
<i>Борьба с киберпреступностью: регулирование вопросов информационной безопасности в рамках экономической безопасности страны</i> Е.Д. Игошина, Ю.М. Мехонцева, А.К. Завалишина	20
<i>Зонт безопасности или сглаживание амплитуды циклических колебаний посредством цифровизации как основа экономической безопасности РФ</i> А.К. Вязникова, Н.В. Кузнецова, П.Ю. Леонов	31
<i>Использование аналитических процедур для выявления манипулирования отчетностью в части сведений об основных средствах</i> В.М. Сушков, Н.С. Белогина	38
<i>Использование современных аналитических технологий при проведении практических занятий по дисциплине «Экономическая безопасность» на примере комплекса Лампир</i> М.Н. Синадский, О.Ю. Синадская	51
<i>Маркетинг страховых услуг</i> Е.Р. Мысева, Е.Г. Казакова	67
<i>Проблемы правового регулирования использования персонального электротранспорта</i> Е.Ю. Хромова	73
<i>Реинжиниринг бизнес-процессов предприятия, как инструмент выживания в конкурентной среде</i> А.Н. Норкина, Е.Р. Мысева	80
<i>Теоретические основы маркетингового исследования рынка. Этапы реализации анализа рынка</i> Е.Р. Мысева, Д.А.Глебова	85
<i>Черный рынок персональных данных</i> Е.О. Алексеев, А.С. Вяткина, А.И. Минеева, А.К. Завалишина	92
<i>Экономические преступления в период пандемии COVID-19</i> А.И. Натарова, О.С. Котелянец	100

Анализ особенностей деятельности и рисков субъектов малого предпринимательства в строительной отрасли

Д.Ю. Елкина
студентка 5 курса специалитета НИЯУ МИФИ, Москва
Email: dasha217991@gmail.com
Е.К. Курдина
студентка 5 курса специалитета НИЯУ МИФИ, Москва
Email: kurdinakatya97@mail.ru

Аннотация: В данной статье рассматриваются отраслевые особенности деятельности субъектов малого предпринимательства в строительной отрасли. Приводятся основные статистические данные по кредитам, предоставленным субъектам малого предпринимательства. Раскрываются основные проблемы и риски, касающиеся исследуемой отрасли. Анализируются программы государственной поддержки и эффективность их применения.

Ключевые слова: субъекты малого предпринимательства, риски, строительная отрасль, программа государственной поддержки

Analysis of the peculiarities of the activities of small businesses in the construction industry

Abstract: This article examines the sectoral features of the activities of small businesses in the construction industry. Provides basic statistical data on loans granted to small businesses. The main problems and risks related to the studied industry are revealed. The programs of state support and the effectiveness of their application are analyzed.

Keywords: small businesses, risks, construction industry, state support program.

На сегодняшний день развитие института малого и среднего предпринимательства (далее – МСП) является одним из приоритетных направлений экономики в целях обеспечения устойчивого роста ее реального сектора. Несмотря на небольшой вклад субъектов МСП в ВВП России по сравнению с зарубежными странами (не более 22%), данный сектор обладает достаточным потенциалом, частично разрешает социально-экономические проблемы общества. Однако из-за имеющихся особенностей остается на стадии «зарождения». Одной из особенностей

является его структурная однородность. Наибольшую долю составляет торговая деятельность – около 55%, остальная часть представлена неторговыми видами деятельности, из которых около 25% относится к промышленному (обрабатывающему) производству и строительству [2]. Особое внимание стоит обратить на строительную отрасль, которая, несмотря на существенный вклад в структуру МСП становится наиболее уязвимой. По результатам исследований, проводимых Сбербанком, на протяжении последних трех лет строительная отрасль имеет отрицательный темп прироста по числу активных компаний – в среднем на 5% ежегодно. Под активными компаниями в данном контексте понимаются зарегистрированные юридические лица, имеющие обороты по счетам [6]. Вследствие пандемии COVID-19, ситуация на рынке ухудшилась из-за остановки ряда строительных проектов и отсутствием заказов. Так, при сохранении данной тенденции возможно изменение структуры сектора МСП, которое может повлечь за собой нехватку хозяйствующих субъектов, занимающихся предоставлением строительных услуг для крупных предприятий и частных лиц.

Субъекты МСП строительной отрасли делятся на три группы: узкопрофильные, многопрофильные и комбинированные. Многие годы в российской практике наиболее устойчивыми являлись узкопрофильные организации, многопрофильные и комбинированные напротив имели более низкие экономические показатели и часто не выдерживали конкуренцию. Однако в связи с нестабильной экономической ситуацией, в частности на рынке строительства, наиболее прибыльными стали компании комбинированного типа, которые помимо строительных услуг, осуществляют деятельность в смежных отраслях, таких как транспортировка и хранение, торговля строительными материалами и т.д.

Основной причиной данной тенденции является особенность строительного сектора, которая заключается в ее цикличности и высокой волатильности. Данная отрасль зависит от большого количества факторов, например, доходы населения (неплатежеспособность заказчиков), нестабильность градостроительного законодательства на государственном и региональном уровнях, конкуренция на рынке, высокий процент по кредитам, высокая налоговая нагрузка, недостаток заказов, высокая стоимость материалов и т.д.

Кроме этого, строительный бизнес считается довольно «закредитованным», а также входящим в топ отраслей по просроченным платежам. Если обратиться к статистике по объему кредитов субъектов МСП, то можно заметить, что в среднем в период с 01.01.2019 по 28.01.2021 почти 6% от общего числа кредитов, предоставленных субъектам МСП, относится именно на жилищное строительство и имеет положительную

динамику [1,7]. Наибольшее количество кредитов было получено в ноябре-декабре 2020 года в целях восстановления деятельности после пандемических шоков (Рис.1).

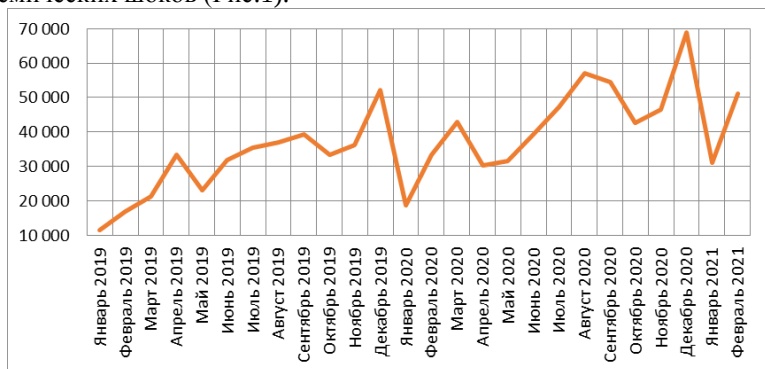


Рисунок 1 - Объем кредитов субъектам МСП, млн руб.

Получение большего количества кредитов неразрывно связано с увеличением просроченных платежей, в частности в период пандемии в связи с резким падением доходов компаний. Так, за аналогичный период они составили 13% от всей просроченной задолженности по кредитам, что в количественном выражении составило рекордный максимум за последние годы [7]. При этом объемы просроченной задолженности продолжают расти, в связи с невхождением отрасли в список наиболее пострадавших видов деятельности, то есть «кредитные каникулы» на нее не распространяются (рис.2).

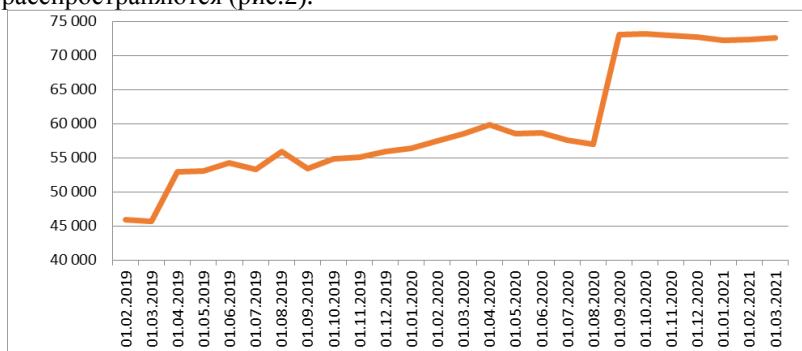


Рисунок 2 – Динамика просроченных платежей, млн руб.

Как следствие, основным финансовым риском в строительной отрасли является риск ликвидности. Этот бизнес, как отмечалось ранее, сильно

зависит от дополнительных источников финансирования. Многие субъекты малого предпринимательства не могут с высокой долей вероятности спрогнозировать свою платежеспособность в будущем, но и не смогут осуществлять свою деятельность без дополнительных ресурсов. У подобных компаний небольшое число клиентов, а маркетинговые затраты для привлечения новой аудитории достаточно велики. Таким образом, долговая нагрузка возрастает большими темпами, а возможность выплачивать задолженность практически отсутствует. По результатам опроса более 16% небольших застройщиков не смогут реализовать свои проекты. Основной причиной этого решения, как отмечалось ранее, является высокая долговая нагрузка [10].



Рисунок 3 – Результаты опроса субъектов МСП, %

Кроме этого, анализируемой отрасли присущи и высокие барьеры для входа на рынок. Для субъектов малого предпринимательства в современных условиях это очень актуально, так как у них нет соответствующих связей, полного понимания ведения такого рода бизнеса и т.д.

На основе анализа российской практики можно выделить следующие проблемы, возникающие в ходе осуществления деятельности субъектами МСП соответствующей отрасли [3]:

1) Качество проектов на выходе: субъектам малого предпринимательства зачастую не хватает ресурсов на покупку качественных материалов, квалифицированную команду проектировщиков и строителей, что впоследствии сказывается на качестве постройки. Также стоит отметить, что на анализируемом рынке до сих пор актуальна проблема нехватки специалистов.

2)Корректировки проектов: некачественные чертежи, неправильно определенный размер, неожиданный скачек в стоимости материалов – все это сказывается на затратах.

3)Документооборот: одна из основных проблем строительной отрасли. Бумажная волокита и бюрократия из-за большого количества разрешений, согласований и т.п. К сожалению, не всем небольшим компаниям удастся получить необходимую документацию, так как зачастую им приходится конкурировать с крупными компаниями.

4)Экологический риск: не у всех небольших компаний есть возможность утилизировать строительные отходы, что наносит вред окружающей среде. Неправильная утилизация отходов также преследуется законом.

Также проблемой является огромная стоимость проектов, в частности в связи с введением эскроу-счетов, которые в какой-то мере помогли отрасли «избавиться» от недобросовестных компаний, но и свели к минимуму получение необходимого финансирования для малого предпринимательства, несмотря на приоритетность данного направления для государства. В стандартных требованиях банка заложены критерии, которые практически исключают возможность удовлетворить подобную заявку малому бизнесу из-за неуверенности в их платежеспособности и устойчивости; значимую роль играет и отсутствие репутации.

Несмотря на наличие возможностей получения кредитов, большинству субъектов МСП было отказано около 40% застройщикам, при этом 35% застройщиков получили кредит не в полном размере и только 25% получили одобрение. По данным РИА Новости [2] причины отказа банка в предоставлении финансирования распределились следующим образом (рис.4).

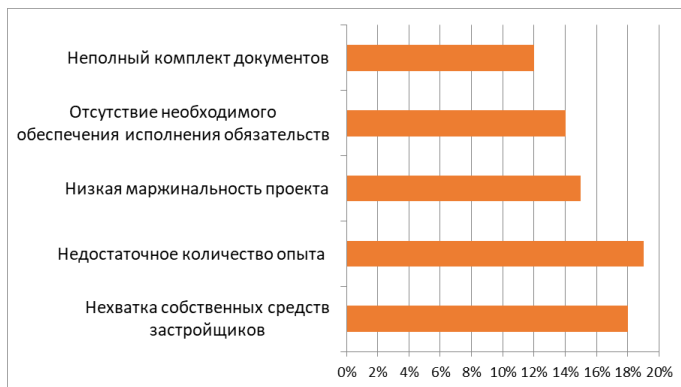


Рисунок 4 – Результаты опроса субъектов МСП, %

Как следствие, большинство респондентов столкнулись с проблемой отсутствия опыта, нехваткой собственных средств, а также низкой маржинальностью проектов, особенно в менее развитых регионах России.

Для решения данной проблемы в рамках поддержки субъектов МСП была разработана программа субсидирования низкомаржинальных проектов. Согласно программе проектного финансирования, в стандартных требованиях банков были заложены новые критерии, которые дают возможность удовлетворить заявку на получение финансирования субъекту МСП [9]:

1. Показатель LLCR должен находиться от 1,05 до 1,15 (рассчитывается кредитором).

2. Планируемая стоимость проекта не должна превышать 500 млн руб.

3. Реализация жилищного проекта возможна в регионе с низкими доходами на душу населения на 15 и более процентов от среднедушевых доходов населения по стране согласно утвержденному списку. В данный перечень входит 49 регионов России, например, республика Адыгея, город Севастополь, Забайкальский край, Калининградская область и т.д.

4. Получение кредитов после 17.01.2021 года.

Кроме указанных программой требований, банки имеют право проводить дополнительные проверки клиентов, в частности оценить опыт застройщиков, репутацию, кредитную историю, проанализировать основные экономические показатели компаний, но эти требования гораздо ниже, чем для крупных предприятий.

Таким образом, хочется еще раз отметить, что субъекты малого предпринимательства в строительной отрасли имеют огромное количество препятствий для ведения своей деятельности. Со сложностями можно столкнуться практически на каждом этапе (получение финансирования, разрешений на строительство и согласований и т.д.), а также возможна нехватка денег на рекламу, недобросовестные поставщики и подрядчики, волатильность спроса и многое другое. К сожалению, из-за таких барьеров с рынка уходят многие субъекты МСП, в частности те, которые могут принести в отрасль большое количество новаторских идей и проектов, тем самым способствовать технологическому развитию строительного сектора. Остается открытым вопрос с высоким уровнем «закредитованности» субъектов МСП. Несмотря на предложенную программу субсидированного кредитования, многие эксперты отмечают ее неэффективность уже на первом этапе реализации. Прежде всего, это связано с низкой стоимостью проекта, существует необходимость увеличения стоимости хотя бы до 620 млн руб., так как большинство проектов не попадает под программу финансирования несмотря на низкие показатели рентабельности. При этом положительной остается динамика

ухода с рынка строительства, в результате чего остаются не полностью реализованные проекты, площадь проблемных застроек достигает 12 млн кв. м [5]. Как следствие, строительная отрасль субъектов МСП нуждается в программах поддержки со стороны государства, в которых будут учитываться отраслевые особенности, направленные на минимизацию барьеров рынка и снижение высокой долговой нагрузки.

Список использованных источников:

1. Банки выдали рекордную за 5 лет сумму кредитов предпринимателям. URL: <https://www.vedomosti.ru/finance/articles/2020/02/26/823922-banki-rekordnuyu> (дата обращения: 18.04.2021).
2. Единый реестр субъектов малого и среднего предпринимательства // ФНС РФ URL: <https://ofd.nalog.ru/> (дата обращения: 18.04.2021).
3. Купечков, А. М. Проблемы субъектов малого и среднего предпринимательства в строительной сфере / А. М. Купечков, О. В. Лустина. — Текст: непосредственный // Молодой ученый. — 2016. — № 17 (121). — С. 430-433. — URL: <https://moluch.ru/archive/121/33363/> (дата обращения: 18.04.2021).
4. Малое и среднее предпринимательство в России и регионах в 2019–2020 гг. // Российская Экономика в 2019 году. URL: https://www.researchgate.net/publication/340901999_Maloe_i_srednee_predprinimatelstvo_v_Rossii_i_regionah_v_2019-2020_gg (дата обращения: 18.04.2021).
5. Малым застройщикам поднимают потолок // Коммерсантъ URL: <https://www.kommersant.ru/doc/4710838> (дата обращения: 18.04.2021).
6. Развитие малого и среднего бизнеса в России // СберДанные URL: https://www.sberbank.com/common/img/uploaded/files/pdf/analytics/s_m_business_d5.ev.pdf (дата обращения: 18.04.2021).
7. Сведения о размещенных и привлеченных средствах // Банк России URL: https://cbr.ru/statistics/bank_sector/sors/ (дата обращения: 18.04.2021).
8. Статистика // СПАРК интерфакс URL: <https://www.spark-interfax.ru/statistics> (дата обращения: 18.04.2021).
9. Субсидирование низкомаржинальных объектов строительства // наш.дом.рф URL: <https://xn--80az8a.xn--d1aqf.xn-p1ai/%D0%BC%D0%> (дата обращения: 18.04.2021).
10. Эксперты рассказали о главных проблемах малых застройщиков в России // РИА Новости URL: <https://realty.ria.ru/20210301/zastroyschiki-1599436316.html> (дата обращения: 18.04.2021).

Анализ ценообразования в сфере закупок услуг по проведению внешнего аудита

В.М. Сушков
студент 4 курса специалитета НИЯУ МИФИ, Москва
Email: vmsushkov@mail.ru

П.Ю. Леонов
к.э.н., доцент кафедры финансового мониторинга НИЯУ МИФИ,
аттестованный аудитор, Москва
Email: p.u.leonov@gmail.com

Аннотация: В статье рассматриваются особенности проведения закупок аудиторских услуг в Российской Федерации. Описывается процесс формирования себестоимости аудиторской проверки. Сопоставляется уровень цен на закупки аудиторских проверок с минимально допустимым. Предлагаются меры по минимизации возможности нарушения рыночных принципов при закупках аудита.

Ключевые слова: аудиторские услуги, контрактная система, начальная (максимальная) цена, недобросовестная конкуренция, антидемпинговые меры.

Analysis of pricing in the field of procurement of external audit services

Abstract: The article discusses the features of the procurement of audit services in the Russian Federation. The process of formation of the cost of the audit is described. The level of prices for procurement of audits is compared with the minimum acceptable. Measures are proposed to minimize the possibility of violation of market principles in audit procurement.

Keywords: audit services, contract system, initial (maximum) price, unfair competition, anti-dumping measures.

Одним из способов приобретения услуг по проведению внешнего негосударственного аудита является создание открытого конкурса на их закупку. Как показывает практика, сфера закупок в Российской Федерации подвержена высокому риску несоблюдения законодательства, в частности необоснованного занижения цен на контракты. Низкие цены на аудиторские услуги не только нарушают принцип свободной рыночной конкуренции, но и ставят под удар престиж аудиторской профессии.

К учреждениям, заказывающим аудиторские услуги на контрактной основе, в частности, относятся государственные компании и корпорации, публично-правовые компании, а также организации, имеющие в своем уставном капитале не менее 25% государственных средств. [1, ч. 3 ст. 5]

Законодательную базу, регулирующую закупки аудиторских услуг, составляют следующие нормативные акты:

1. Федеральный закон №44-ФЗ «О контрактной системе по закупке товаров, работ, услуг для обеспечения муниципальных и государственных нужд»

Данный закон раскрывает основные понятия и устанавливает принципы закупочной деятельности, обязательные для применения всеми сторонами закупок. [2]

2. Федеральный закон №307-ФЗ «Об аудиторской деятельности»

Данный закон определяет особенности сферы аудита в РФ. В частности, статья 5 раскрывает порядок проведения закупок обязательного аудита. [1]

3. Методические рекомендации по организации и проведению открытых конкурсов на право заключения договора на проведение аудита бухгалтерской (финансовой) отчетности организаций, указанных в части 4 статьи 5 Федерального закона «Об аудиторской деятельности»

Данный документ детализирует порядок проведения конкурса, оценки заявок, определения начальной (максимальной) цены, заключения договора, требования к участникам закупок и пр. [3]

Важно отметить, что закон 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» в отношении закупок аудиторских услуг не применяется.

Особенностями проведения закупок услуг по проведению обязательного аудита являются:

1. Исключительное проведение аудита аудиторскими компаниями;
2. Проведение открытого конкурса не реже одного раза в пять лет;
3. Проведение открытого конкурса в электронной форме;
4. Необязательность обеспечения заявок на участие в конкурсе или обеспечение исполнения контракта;
5. Осуществление закупок только у субъектов малого и среднего предпринимательства компаниями, чья выручка за отчетный период составляет менее 1 млрд рублей;
6. Возможность осуществления закупок как в рамках контрактной системы, так и по правилам проведения коммерческих торгов;
7. Оценивание участников закупок на основании как стоимостных, так и нестоимостных критериев.

Так, вес цены контракта должен составлять не менее 30%, а максимальный вес нестоимостных критериев (квалификация аудиторской

фирмы, ее деловая репутация) не более 70%. [4] Таким образом, при выборе исполнителя у заказчика присутствует возможность в большей степени опираться не на стоимость планируемых к получению аудиторских услуг, а на их качество. В то же время, закон не запрещает устанавливать стопроцентную значимость в отношении стоимостных критериев.

При определении справедливого уровня договорной цены необходимо грамотно рассчитать себестоимость предстоящей аудиторской проверки. Для стабильного обеспечения своих клиентов услугами высокого качества каждая фирма должна регулярно совершать весьма значительные расходы. При этом аудиторская деятельность, как и любой другой вид бизнеса, существует в жестких рамках: доходы должны превышать расходы.

Основными компонентами, формирующими себестоимость, являются:

1. Расходы на оплату труда

Качественный аудит требует привлечения квалифицированных и опытных специалистов. При этом за светлые головы аудиторские фирмы конкурируют не только друг с другом, но и с финансовыми подразделениями иных экономических субъектов. Следовательно, необходимо достойно оплачивать их труд.

2. Информационное обеспечение профессиональной деятельности

Информационно-аналитическая база аудиторской фирмы должна включать постоянно пополняемый справочно-информационный фонд литературы, включая профессиональные периодические издания по всем направлениям деятельности, а также доступ к справочно-правовым системам.

3. Методологическое обеспечение профессиональной деятельности

Методологическая поддержка – важный фактор непрерывного совершенствования качества услуг. В эту статью расходов включаются затраты на содержание специалистов, занимающихся разработкой и совершенствованием методик оказания аудиторских услуг.

4. Расходы на техническое обеспечение специалистов

Проведение аудита невозможно без компьютерной техники с современным программным обеспечением. Лицензионные программные продукты позволяют повышать качество и скорость работы сотрудников, а также снизить число привлекаемых к работе специалистов.

5. Расходы на обучение и повышение квалификации персонала

Для того, чтобы соответствовать потребностям современного бизнеса, аудиторам требуется непрерывно повышать квалификацию. Это требует посещения семинаров, тренингов, прохождения стажировок, профессиональных курсов, международной сертификации и т.п., расходы на которые, как правило, покрываются работодателем.

6. Расходы содержание офиса

Аудиторская фирма должна иметь офис с хорошей транспортной доступностью, а также содержать его путем оснащения высокотехнологичным оборудованием, офисной техникой, средствами связи и Интернетом.

7. Командировочные расходы

Сегодня даже небольшие аудиторские фирмы работают с клиентами, офисы которых располагаются за пределами региона регистрации компании. В связи с этим затраты на оформление выездных документов, страховки, транспорт, проживание сотрудников составляют достаточно большие суммы.

8. Расходы на инфраструктуру, обеспечивающую основную деятельность

В любой компании помимо основного подразделения функционируют вспомогательные: бухгалтерия, охрана, секретариат, хозяйственная служба и др. Служебный персонал непосредственно не участвует в оказании аудиторских услуг, однако расходы на его содержание ложатся на плечи заказчика.

9. Расходы на уплату налогов, сборов и обязательных платежей

Аудиторы, так же как и их клиенты, должны быть законопослушными налогоплательщиками. Уплата НДС, налога на прибыль и страховых взносов с заработной платы является неотъемлемой статьей расходов любой аудиторской компании. [5]

Поскольку аудиторские организации имеют возможность рассчитывать индивидуальную себестоимость отдельного заказа, то, как правило, ими используется позаказный метод учета затрат и калькулирования себестоимости. Это значит, что все прямые затраты учитываются по установленным экономическим субъектом статьям калькуляции по каждому заказу. В их состав в первую очередь включаются расходы на заработную плату специалистов и социальные отчисления. Остальные виды затрат в большинстве случаев являются косвенными (накладными), учитываются по местам их возникновения и включаются в себестоимость отдельных заказов в соответствии с установленной базой (ставкой) распределения.

Каждому заказу присваивается идентификационный номер, который проставляется в первичных документах, связанных с заказом. Это позволяет соотнести произведенные прямые затраты с объектом учета затрат и включить их в себестоимость заказа. Косвенные затраты могут распределяться как по окончании выполнения заказа, так и предварительно. Затраты на заказ, не законченный на конец месяца, отражают в составе незавершенного производства. Также возможно

разукрупнение заказов, при котором каждый этап накапливает собственную себестоимость и затем сдается заказчику.

Особенностью аудиторской деятельности является достаточно большой интервал времени между продажей услуг и получением денежных средств. В ряде случаев договор на проведение проверки может заключаться за несколько лет до ее фактического проведения.

Существуют альтернативные варианты отражения стоимости проверки в договоре. В первом случае возможно указание стоимости часа работы специалистов и их количество, входящее в рабочую группу. Окончательная стоимость проверки рассчитывается после ее завершения. Данный способ требует высокой степени доверия между аудиторской компанией и аудируемым лицом – клиент должен быть уверен в том, что каждый оплаченный им час используется по назначению. [6] Более распространенным вариантом является фиксация в договоре полной стоимости аудиторской проверки. В этом случае аудиторская фирма должна достаточно точно оценить себестоимость предстоящей проверки, что зачастую является крайне сложным процессом, поскольку стоимость аудита зависит от множества факторов, среди которых:

- различие в ведении бухгалтерского учета;
- разнообразие организационно-правовых форм, а также видов деятельности;
- различие систем налогообложения;
- различие квалификации главных бухгалтеров;
- невозможность точно учесть затраты времени аудитора на проведение проверки;
- зависимость заработной платы аудитора от стоимости проверки.

В связи с этим в аудиторских фирмах, как правило, не бывает стандартных тарифов на услуги. Аудит конкретной организации требует индивидуальных затрат, что отражается на договорной стоимости проверки. Кроме того, стабильно высокое качество оказываемых услуг напрямую сказывается на их стоимости. В связи с этим низкая контрактная цена закупок аудиторских проверок должна настораживать потребителя. Ее могут предлагать либо крайне прогрессивные компании, обнаружившие неизвестные конкурентам возможности снижения издержек, либо компании, снижающие себестоимость за счет ухудшения качества услуг.

Соотношение цены и качества в аудиторской деятельности можно представить в качестве графика, изображенного на рис.1.

Так, себестоимость аудиторской проверки C монотонно возрастает при повышении ее качества K . При этом рост начинается не с нуля, так как даже «черный» аудит требует затрат на составление аудиторского заключения. В начале рост плавный, однако при высоком качестве аудита

К становится достаточно резким, поскольку даже малое увеличение К требует значительного увеличения затрачиваемых при проверке ресурсов.

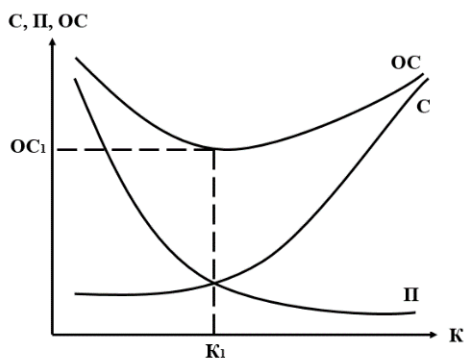


Рисунок 1 – Функции зависимости себестоимости, репутационных потерь и обобщенной себестоимости от качества аудиторских услуг

Потери аудиторской организации П из-за судебных исков пользователей аудита, снижения престижа и т.п. резко уменьшаются в диапазоне малых значений К и затем монотонно спадают, но не до нуля: даже при близком к идеальному качеству проверки возможны потери аудиторской организации вследствие ошибочного решения суда, последующего нарушения конфиденциальности проверки сотрудниками аудиторской фирмы и пр. Сумма этих двух кривых, назовем ее обобщенной себестоимостью проверки ОС, имеет минимум при средних значениях К. Именно эта результирующая кривая должна быть в центре внимания руководства аудиторских фирм. Именно обобщенная себестоимость аудита, а не просто его себестоимость, является отправной точкой при формировании цены аудита. [7]

В качестве варианта расчета порогового значения цены закупки на проведение аудита бухгалтерской (финансовой) может использоваться следующая формула:

$$ПЗ_{АП} = \frac{((3П + СВ) * ССЧ * 12 + АП + ВСРО + СПС + ПК) * НДС * (1 + НП)}{КолП}$$

где ПЗ_{АП} – пороговое значение цены аудиторской проверки, руб.;

3П – среднемесячная заработная плата аудитора, руб.;

ССЧ – среднесписочная численность организации, чел.;

СВ – страховые взносы, руб.;

АП – арендная плата, руб.;

ВСПО – взносы в саморегулируемые организации, руб.;
СПС – оплата справочно-правовой системы, руб.;
ПК – повышение квалификации (обучение), руб.;
НДС – налог на добавленную стоимость, начисляемый сверху;
НП – норма прибыли;
КолП – количество проектов в год, шт.

Важно отметить, что данный расчет содержит только базовые затраты аудиторской фирмы и, следовательно, отражает минимально допустимый уровень стоимости аудиторской проверки. Каждой отдельной организации следует корректировать формулу в зависимости от особенностей как собственной деятельности, так и деятельности заказчика проверки.

На данный момент при установлении цены контракта определяется только начальная (максимальная) цена. Она рассчитывается на основании данных о рыночных ценах услуг, планируемых к закупке (цен на проведение аудиторской проверки). При установлении начальной (максимальной) цены договора следует запросить информацию по ценовым предложениям аналогичных услуг не менее чем у 5 организаций, которые могут исполнить данную закупку в связи со специализацией своей деятельности. [3] В данную категорию подпадают аудиторские и консалтинговые фирмы, а также индивидуальные аудиторы.

Проанализируем уровень цен на закупки аудиторских услуги в России по контрактам, завершенным в 2020 году. Для этого из Единой информационной системы в сфере закупок (zakupki.gov.ru) случайным образом было выбрано 50 компаний из 10 различных регионов РФ и рассчитано пороговое значение стоимости аудиторской проверки по формуле, представленной выше.

Необходимые для расчета данные были получены из открытых источников:

- Среднемесячная заработная плата аудитора – как средняя заработная плата бухгалтера (включая аудитора) с сайта Федеральной государственной службы статистики;
- Среднесписочная численность организации – как среднее значение численности персонала из выборки организаций с сайта Руспрофайл (4 человека);
- Арендная плата – как минимальная стоимость 1 кв. метра офисного помещения с сайтов-агрегаторов недвижимости Циан, Здание.Инфо, Авито, умноженная на среднесписочную численность персонала и норму площади на одно рабочее место;
- Взносы в саморегулируемые организации – как среднее значение годовых взносов в СПО ААС с официального сайта саморегулируемой организации (от 60 до 80 тыс. руб.);

- Оплата справочной системы – как приблизительная стоимость СПС Консультант для бухгалтеров и аудиторов с официального сайта сервиса (540 тыс. руб.);

- Повышение квалификации (обучение) – как средняя экспертная оценка с форумов сети Интернет (от 150 до 180 тыс. руб.);

- Норма прибыли – как показатель рентабельности оказанных услуг (отношение чистой прибыли к выручке) для компаний, занимающихся финансовой и страховой деятельностью, с сайта ФНС (34,7%).

Показатель «количество проектов в год» носит наиболее относительный характер, поскольку зависит от уровня сложности проверок, осуществляемых аудиторской организацией. В связи с этим, учитывая, что среднесписочная численность организации составляет 4 человека, рассмотрим три варианта:

1. Наиболее вероятный – 15 проверок в год;
2. Менее вероятный – 30 проверок в год;
3. Крайне маловероятный – 60 проверок в год.

Результаты расчетов представлены в табл.1.

Таблица 1 – Сопоставление цен закупок аудиторских проверок с минимальным порогом

Субъект РФ	КолП = 15		КолП = 30		КолП = 60	
	Выше порога	Ниже порога	Выше порога	Ниже порога	Выше порога	Ниже порога
Москва	40%	60%	60%	40%	100%	0%
Красноярский край	0%	100%	80%	20%	100%	0%
Владимирская область	40%	60%	40%	60%	100%	0%
Хабаровский край	20%	80%	60%	40%	100%	0%
Свердловская область	20%	80%	40%	60%	80%	20%
Волгоградская область	20%	80%	60%	40%	100%	0%
Новосибирская область	60%	40%	100%	0%	100%	0%
Республика Башкортостан	20%	80%	80%	20%	100%	0%
Приморский край	60%	40%	80%	20%	100%	0%
Архангельская область	20%	80%	40%	60%	80%	20%
Итого по выборке	30%	70%	64%	36%	96%	4%

Как можно видеть, в выборке из 50 случайных компаний при стандартном количестве проектов в год стоимость более половины контрактов в 2020 году было заключено на сумму, не превышающую

минимальную стоимость проверки. При увеличении количества проектов число контрактов с обоснованной стоимостью увеличивается, однако не достигает 100% даже при практически недостижимом числе проверок – 60 в год (более одной проверки в неделю).

В качестве причин низких цен на закупки аудиторских услуг можно выделить:

1. Недобросовестность заказчиков, которые пытаются сэкономить за счет приобретения услуг низкого качества;
2. Недобросовестность исполнителей, которые снижают цены за счет ухудшения качества предоставляемых услуг;
3. Затруднительный доступ к сведениям о стоимости уже проведенных аудиторских проверок, поскольку многие участники рынка считают данную информацию конфиденциальной;
4. Несовершенство российского законодательства в области организации закупок, которое позволяет осуществлять необоснованную ценовую политику на законных основаниях.

Таким образом, проблема заниженных цен на закупки по проведению внешнего негосударственного аудита сохраняется актуальной. Одним из возможных способов ее решения может стать практическое применение формулы расчета порогового значения цены закупки на проведение аудита отчетности непосредственно во время заполнения данных на сайте размещения информации о закупке. Эффективность процесса может быть повышена с помощью его автоматизации – ввода параметров деятельности аудиторской организации и вывода на их основе порогового значения цены договора. Таким образом, будет устранена возможность устанавливать цены, в несколько раз меньше необходимой для качественного проведения всех аудиторских процедур по проверке бухгалтерской (финансовой) отчетности организации.

Список использованных источников:

1. Федеральный закон от 30.12.2008 N 307-ФЗ «Об аудиторской деятельности» (ред. от 09.03.2021) // Официальный интернет-портал правовой информации [Электронный источник] – Режим доступа: <http://publication.pravo.gov.ru/Document/View/0001202007310082>.
2. Федеральный закон от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (ред. от 30.04.2021) // Официальный интернет-портал правовой информации [Электронный источник] – Режим доступа: <http://publication.pravo.gov.ru/Document/View/0001201304080023>.

3. Методические рекомендации по организации и проведению открытых конкурсов на право заключения договора на проведение аудита бухгалтерской (финансовой) отчетности организаций, указанных в части 4 статьи 5 Федерального закона «Об аудиторской деятельности» // Официальный сайт Минфина России [Электронный источник] – Режим доступа: https://minfin.gov.ru/ru/document/?id_4=22989.
4. Постановление Правительства РФ от 28 ноября 2013 г. N 1085 «Об утверждении Правил оценки заявок, окончательных предложений участников закупки товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // Официальный интернет-портал правовой информации [Электронный источник] – Режим доступа: <http://publication.pravo.gov.ru/Document/View/0001201312020017>.
5. Пятенко С.В. Организация работы аудитора и консультанта: Учебно-практическое пособие / М.: ИД ФБК-ПРЕСС, 2001. – 376 с.
6. Васильева М.В., Журавлева Н.А. Особенности формирования себестоимости аудиторских услуг в современных российских условиях // Управленческий учет. – 2006. – № 4. – с. 104 - 108.
7. Голосов О.В., Гутцайт Е.М. Аудит: концепция, проблемы, стандарты, контроль, эффективность, кризис / М.: Издательство «Бухгалтерский учет», 2005. – 512 с.

УДК 004.056.5:005.934:330.46

© Е.Д. Игошина, Ю.М. Мехонцева, А.К. Завалишина, 2021

**Борьба с киберпреступностью: регулирование вопросов
информационной безопасности в рамках экономической безопасности
страны**

Е.Д. Игошина

студентка 4 курса специалитета ИРИТ-РТФ, УрФУ, Екатеринбург

Email: igoshina_katy26@mail.ru

Ю.М. Мехонцева

студентка 4 курса специалитета ИРИТ-РТФ, УрФУ, Екатеринбург

Email: lulu9751@gmail.com

А.К. Завалишина

ассистент кафедры финансового менеджмента

НИЯУ МИФИ, Москва

Email: akzavalishina@gmail.com

Аннотация: *В цифровом обществе информационные угрозы в рамках экономической безопасности страны приобретают особую важность. В данной статье рассмотрены проблемы реализации политики экономической безопасности РФ в информационной сфере, а также степень ее эффективности для предотвращения совершения киберпреступлений и нанесения ущерба экономике страны.*

Ключевые слова: *киберпреступность, экономическая безопасность, информационная безопасность, информационные технологии.*

Fighting cybercrime: regulating information security issues within the framework of the country's economic security

Abstract: *In a digital society, information threats within the framework of the country's economic security are of particular importance. This article discusses the problems of implementing the economic security policy of the Russian Federation in the information sphere, as well as the degree of its effectiveness in preventing the commission of cybercrimes and causing damage to the country's economy.*

Keywords: *cybercrime, economic security, information security, information technology.*

Современная экономика под влиянием технологических достижений активно трансформируется в цифровую экономику нового поколения. Цифровая трансформация – это глобальный мировой тренд [2, с. 81], который неизбежно влечет за собой новые виды угроз и стремительную адаптацию преступных схем к изменяющимся условиям. Повсеместная автоматизация труда и активное развитие информационно-коммуникационных технологий породили новую область криминальной активности – киберпреступность. Согласно источнику [3], основу киберпреступности составляет ограниченный круг деяний, направленных против конфиденциальности, целостности и доступности компьютерных данных или систем. В условиях цифровизации экономическая безопасность страны тесно взаимосвязана с политикой информационной безопасности. Отсутствие своевременной защиты и быстрого реагирования на инциденты информационной безопасности может повлечь за собой неблагоприятные для экономики последствия на различных уровнях. Поэтому вопрос эффективности регулирования информационной составляющей экономической безопасности как никогда актуален.

В данной статье будут рассмотрены проблемы политики экономической безопасности в информационной сфере, влияние киберпреступности на общее состояние экономики Российской Федерации, а также проведен

анализ эффективности принятой политики экономической безопасности для предотвращения совершения киберпреступлений и нанесения ущерба экономике страны.

В своем исследовании Дрындак А. А. определила «информационные войны и киберпреступность» как одну из современных угроз экономической безопасности [1, с. 93–94]. Развитие информационных технологий в совокупности с ускоренным процессом глобализации позволило данной угрозе не только увеличить темпы и простоту реализации, но и расширить область возможного наносимого вреда. В информационном обществе человек, владеющий технологиями и знаниями, становится невероятно влиятельным.

На сегодняшний день киберпреступность представлена множеством видов неправомерных деяний. От простого мошенничества в сети и распространения вирусных программ информационная преступность эволюционировала до полномасштабных кибертеррактов, атак хакеров на защищенные государственные сети и продуманных финансовых преступлений. Многогранность киберпреступности в ее проявлениях подробно освещена в исследовании [1].

Киберпреступления остаются одной из самых сложных категорий преступлений. Осипенко А. Л. отметил ряд особенностей, характеризующих данный вид преступлений, такие как повышенная латентность; интеллектуальный и трансграничный характер деятельности; возможность совершения преступного деяния одновременно в нескольких местах в автоматизированном режиме; дистанционный способ совершения преступления; многоэпизодичность в совокупности с множественностью потерпевших, их неосведомленность о том, что они подверглись преступному деянию, а также невозможность предотвращения и пресечения указанных преступлений традиционными средствами [10, с. 109–110].

Киберпреступность в экономике нацелена на получение финансовой выгоды. Наиболее распространенный пример данного явления – нанесение экономического ущерба в виде воровства средств и конфиденциальной информации. Преступные действия могут быть направлены не только на простых граждан, но также на организации, государственные институты, личную информацию и персональную кибербезопасность [3]. В отличие от физической попытки ограбления действия киберпреступников, как правило, незаметны, а масштабность атаки и отсроченное наступление последствий также дает злоумышленникам некоторое преимущество. Правоохранительные органы зачастую затрудняются установить место совершения преступления, найти доказательства причастности или обнаружить виновных в преступном деянии. Однако проблема не всегда

заключается в неувлечимости злоумышленников. Так, Долбилов А. В. [17, с. 3] отмечает, что ввиду особой специфики киберпреступлений наличие у сотрудников правоохранительных органов специальных знаний в сфере информационных технологий приобретает особую значимость. Таким образом, отсутствие необходимой квалификации персонала с юридическим образованием является одной из ключевых проблемных моментов в области расследования киберпреступлений.

По мнению авторов статьи [3], «киберпреступность постепенно трансформируется в большой, широко разветвленный бизнес с доходами, сопоставимыми с доходами от наркоторговли». В данном исследовании были освещены виды киберпреступлений, получившие большую распространенность за прошедший 2020 год, такие как кибермошенничество, информационные блокады, компьютерный шпионаж и другие посягательства, которые представляют повышенную опасность для общества. Всемирная сеть также широко используется для пропаганды различных экстремистских идей и движений [3, с.4].

По данным МВД РФ за 2020 отчетный год число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети «Интернет» – на 91,3%, при помощи средств мобильной связи – на 88,3% [5]. Сбербанк ранее сообщил, что за 2019 год потери российской экономики от деятельности хакеров составили около 2,5 трлн рублей. По предварительной оценке, в 2020 году этот показатель вырос до 3,5–3,6 трлн рублей [6]. Для сравнения федеральные расходы на борьбу с пандемией в России тот же период составили около 2,86 трлн рублей.

Positive Technologies сообщили, что за 2020 только 14% атак были направлены против частных лиц, в то время как наибольший урон получил коммерческий сектор. Больше всего злоумышленников интересовали государственные и медицинские учреждения, а также промышленные компании [8]. На диаграмме, представленной Positive Technologies в своем исследовании (рис.1), отражены типы данных, которые подверглись наиболее частым атакам киберпреступников. Высокую ценность для киберпреступников представляют персональные данные физических лиц, данные, составляющие коммерческую тайну, и учетные записи пользователей. Во многом этому поспособствовало внедрение электронного документооборота в работу компаний.

Данные результаты были подтверждены в отчете Cisco по кибербезопасности для малого и среднего бизнеса [9]. Наиболее значимой угрозой 2020 года с нанесением максимального ущерба стали программы-вымогатели («вирусы-шифровальщики»), способные остановить работу систем предприятия более чем на 24 часа. Жертвами атак становились

представители как мелкого, так и крупного бизнеса. Существенный урон экономическому благополучию компании способны нанести кражи учетных данных и программы-шпионы. Также, среди лидирующих угроз представлены атаки DDoS, которые занимают третье место по силе негативных последствий для крупных компаний, в то время как для малого бизнеса важной проблемой по-прежнему остается фишинг.



© Positive Technologies

Рисунок 1 - Типы украденных данных (в атаках на организации) [8]

Стабильное экономическое развитие предприятия в современных условиях невозможно без должного подхода к обеспечению сетевой безопасности. Сложное устройство внутренней сети компании, ее масштабность, квалифицированность и подготовленность сотрудников, а также наличие базовых мер защиты собственного информационного пространства – это ключевые аспекты предприятия, способные стать уязвимостями для кибератак при поверхностном подходе к их качеству. Результаты деятельности компаний влияют на экономическое положение регионов и страны в целом. В связи с этим, качество обеспечения информационной безопасности в масштабе предприятий в совокупности напрямую влияет на общий уровень экономической безопасности. Таким образом, сотрудничество между государством и частным сектором становится одним из основополагающих принципов противодействия киберпреступности для государства.

Однако фундамент противодействия киберпреступлениям в экономике – это в первую очередь нормативная составляющая экономической безопасности страны. По мнению Степаченовой О. С. [18] само понятие

«нормативно-правовая база экономической безопасности» в России не сформировано в полной мере и, как правило, не рассматривается отдельно от национальной. Неоднозначный подход к определениям может стать причиной возникновения новых угроз. Безусловно, база в области национальной экономической безопасности удовлетворяет критериям национальной безопасности РФ. Однако, вместе с тем, единой нормативно-правовой системы, регламентирующей вопросы экономической безопасности не существует [18, с. 167–170]. Поэтому более специфические угрозы, такие как кибератаки и прочие преступные действия, использующие информационные технологии, не регулируются как самостоятельная подобласть среди экономических угроз.

В Стратегии экономической безопасности РФ до 2030 года среди вызовов и угроз экономической безопасности РФ фигурируют рост криминализации экономики, подверженность финансовой системы глобальным рискам, а также уязвимость информационной инфраструктуры финансово-банковской системы [11]. Возможный ущерб от реализации данных угроз может быть колоссальным. Политика предотвращения экономического ущерба от действий киберпреступников в Российской Федерации представлена отдельными документами, направленными в первую очередь на своевременное обнаружение преступной активности в информационном пространстве и быстрое устранение последствий этой активности (которые, в большинстве случаев, все-таки имеются).

Так, например, Указом Президента РФ от 12.12.2014 года №К 1274 была принята Концепция, которая представила государственную Систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (СОПКА). По данным системы ГосСОПКА, в 2020 году было выявлено более 120 тыс. воздействий на информационную инфраструктуру РФ. Кроме того, Концепция предполагает создание системы защиты от киберугроз органов государственной власти и финансовых учреждений. Также, в 2015 году Центральный банк РФ положил начало Центру борьбы с киберугрозами финансового характера, задачами которого является сбор сведений о кибератаках на банки и их клиентов, о потенциальных киберугрозах и последующая передача данных финансовым учреждениям [12, с. 257–258].

Взаимосвязь информационной безопасности и экономического благополучия страны очевидна, однако отсутствие фиксированного регулирования противодействия киберпреступности в рамках экономической безопасности позволяет рассматривать данный аспект лишь в рамках общей информационной безопасности. В частности, Стратегия экономической безопасности делает лишь небольшой акцент на уязвимости банковской сферы к действиям киберпреступников, в то время

как угроза в данной сфере более чем серьезна. Это относится не только к мошенничеству с кредитными картами и прочими попытками взлома, но и к более скрытным процедурам, таким как отмывание преступных доходов. Средства, обращающиеся в теневом секторе, требуют предварительной обработки, прежде чем будут внедрены в легальный денежный оборот. Криминализация экономики – одна из основных угроз экономической безопасности страны, которая стимулируется техническими достижениями и повсеместной доступностью к информации, что значительно упрощает реализацию киберпреступлений. Замкнутый круг совершения преступления и необходимости «очистить» полученный доход негативно сказывается на состоянии экономики. Более подробный анализ действий преступников, направленных на финансовые учреждения с целью скрыть факт проведения операций в рамках легализации преступных средств, а также мер противодействия, которые принимают банки для пресечения этой деятельности, представлен в статье Игошиной Е. Д [14].

В 2020 году финансовые учреждения стали третьими по частоте кибератак, в то время как лидерство досталось государственным структурам и сфере промышленности. Несмотря на многочисленные принятые государством меры, в марте 2021 года сервис Ростелеком-Solar сообщил о двухкратном росте числа атак на объекты критической информационной инфраструктуры через инфраструктуру подрядчика в 2020 году. В частности, атаки были совершены на банки, атомные предприятия, объекты здравоохранения, электроснабжения, военные объекты и госструктуры. Центр мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар» выявил и отразил свыше 1,9 млн атак, что на 73% превышает показатель 2019 года. Кроме того, в Ростелеком-Solar отметили, что с изменением специфики атак угроза кибербезопасности перешла на государственный уровень [13]. Количество сложных целенаправленных атак с каждым годом растет. Это ставит под вопрос как безопасность страны в целом, так и ее экономическое благополучие в частности.

Экономические риски промышленного сектора в связи с проблемами информационной безопасности также могут значительно обостриться. Реализация киберугроз в промышленной отрасли влечет за собой глобальные последствия. Так, например, Positive Technologies в своем исследовании [8] сообщили о некоторых международных инцидентах в промышленном секторе: «В ходе атаки на инфраструктуру водоснабжения и канализации в Израиле хакеры планировали изменить концентрацию хлора в подаваемой в жилые дома воде, что привело бы к массовому отравлению, а инцидент с отключением электроэнергии из-за кибератаки в Индии сказался на работе фондовой биржи, больниц и транспортной

системы нескольких городов». Случаи также были зафиксированы в Китае, Италии и Румынии. В Российской Федерации подобные инциденты открыто не афишируются во избежание возможных репутационных проблем, однако количество атак на промышленные компании в 2020 году увеличилось практически на 91%, что негативно сказывается не только на работе отдельных компаний, но и на показателях отраслей.

Чем можно объяснить подобный рост преступности? Во многом на это повлияло повсеместное внедрение дистанционного режима работ и автоматизация производств и процессов. Авторы статьи [7] связывают подобный рост киберпреступности в Российской Федерации с несколькими возможными причинами:

1. Трудности в определении местоположения злоумышленников.
2. Несовершенство правоохранительной деятельности компетентных органов.
3. Несовершенство российского законодательства.
4. Высокий уровень латентности киберпреступлений.
5. Отсутствие системы взаимодействия с правоохранительными органами зарубежных стран [7, с. 212].

Злоумышленники используют множество способов скрыть адрес отправителя и информацию о маршрутизации сообщений. Это может быть обусловлено как широтой применения информационных технологий, так и несовершенством введенных мер регулирования деятельности по противодействию киберпреступности. К снижению эффективности выявления совершенных преступлений и пресечения негативных последствий также могут привести трудности трактовки законодательных актов. Кроме того, сотрудники предприятий в силу различных обстоятельств (например, во избежание репутационных рисков компании) сознательно умалчивают об инцидентах компьютерной безопасности, что в дальнейшем может повлиять не только на статистику выявленных преступлений, но и на своевременную разработку или обновление стратегии противостояния подобным деяниям. Впоследствии, это может негативно повлиять на принятие и осуществление политики информационной и экономической безопасности.

Информационное пространство не имеет четких границ, что позволяет киберпреступности иметь характер глобальной международной проблемы. Важно не только поддерживать внутреннее взаимодействие государства с частным сектором, но также принимать во внимание опыт других стран по вопросам кибербезопасности. Чем большим объемом знаний об актуальных угрозах обладает государство, тем более качественными будут меры по предупреждению возможных угроз.

В России на настоящий момент 28 глава УК РФ [19] регламентирует ответственность за преступления в сфере компьютерной информации. Выделяется несколько составов киберпреступлений: неправомерным доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ), нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ), неправомерное воздействие на критическую информационную инфраструктуру РФ (ст.274 прим. 1 УК РФ). Авторы статьи [16] считают данный перечень недостаточно адаптированным к новым видам преступлений в сфере информационных технологий. И проблема сложности прогнозирования возможных угроз является весомым препятствием в разработке мер, направленных на предотвращение кибератак. Однако решение этой проблемы во многом зависит от качественного сотрудничества с другими странами и применением их положительного опыта в вопросах кибербезопасности [16, с. 44–45]. Так, Козлова О. Е. и другие [16] предлагают на начальном этапе разрешить вопрос об отказе России подписать Конвенцию Совета Европы о преступности в сфере компьютерной информации, зафиксировать все основные IT определения для упрощения международной работы по примеру США, рассмотреть возможность создания новых подразделений и ведомств для противостояния киберпреступности.

Международное сотрудничество в борьбе с кибертерроризмом осуществляется в рамках ООН, Совета Европы, Международной организации экспертов, Интерпола, Европола [15, с. 38], а также множества специализированных организаций, таких как IMPACT, ICSPA, МСЭ [12, с. 257]. Подобные организации призваны облегчить взаимодействие стран и сосредоточить ресурсы на решении общих проблем. Однако законодательство Российской Федерации не обеспечивает прямого сотрудничества с правоохранительными органами иностранных государств на необходимом уровне. Поэтому Чепрасова и Шмарион в своей статье предлагают разработать и законодательно закрепить в соответствующих документах механизм взаимодействия ОВД с вышеупомянутыми иностранными органами [12, с. 259].

Киберпреступность – современная угроза, способная нанести серьезный материальный, финансовый и экономический ущерб. В ходе исследования мы выяснили, что меры, принимаемые Россией для противодействия быстрому росту киберпреступности не являются достаточными в полной мере. Безусловно, положение России в 2020 году нельзя определить как критическое. Однако быстрый рост теневой занятости и увеличение киберпреступности более чем на 90% в течение одного года говорит о нарастающем напряжении в информационной сфере

и о трудностях в реализации политики экономической безопасности. Разрешить данную проблему ресурсами одной страны не представляется возможным, поэтому международное сотрудничество, исследование иностранного опыта и внесение правок в нормативные акты страны может поспособствовать улучшению текущей ситуации. Киберпреступность быстро эволюционирует и адаптируется под изменяющиеся условия. Где государство видит проблему, там злоумышленники открывают новые возможности. Не имея достаточной гибкости законодательства и быстроты реагирования на новые киберугрозы, государство не сможет обеспечить необходимый уровень информационной и экономической защиты, достаточный для поддержания стабильного состояния экономики.

Список использованных источников:

1. Дрындак А.А. Трансформация угроз экономической безопасности в условиях глобальных экономических вызовов / А. А. Дрындак // Вестник студенческого научного общества ГОУ ВПО "Донецкий национальный университет". – 2019. – Т. 3. – № 11. – С. 92–97.
2. Бушуев А.Л. Киберпреступность и преступления в сфере информационных технологий как угроза экономической безопасности стран - членов ЕАЭС / А. Л. Бушуев // Актуальные проблемы развития ЕАЭС в условиях современных глобальных изменений: Материалы Всероссийской научно-практической конференции, Иркутск, 12 декабря 2019 года / Под научной редакцией И.В. Цвигун, А.В. Шалака. – Иркутск: Байкальский государственный университет, 2021. – С. 81–86.
3. Киберпреступность как угроза экономической безопасности / Д. Б. Басирова [и др.] // Аллея науки. – 2020. – Т. 1. – № 3(42). – С. 333–337.
4. Семакина Т.В. Киберпреступность и экономическая безопасность организации / Т. В. Семакина // Сборники конференций НИЦ Социосфера. – 2020. – № 24. – С. 158–160.
5. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2020 года / Официальный сайт МВД Российской Федерации [Электронный ресурс] // Режим доступа: <https://xn--b1aew.xn--p1ai/reports/item/22678184/> (Дата обращения: 06.06.2021 г.).
6. Россия могла потерять до 3,6 трлн рублей из-за киберпреступлений в 2020 году – «Сбербанк» / Новости компаний – Finam.ru [Электронный ресурс] // Режим доступа: <https://www.finam.ru/analysis/newsitem/rossiya-mogla-poteryat-do-3-6-trln-rubleiy-iz-za-kiberprestupleniiy-v-2020-godu-sberbank-20201228-163126/> (Дата обращения: 04.06.2021 г.).
7. Позднякова Т. С. Развитие киберпреступности как угроза экономической безопасности Российской Федерации / Т. С. Позднякова,

- С.А. Гребенкина // Актуальные вопросы развития инновационной экономики: Сборник статей Всероссийской научно-практической конференции, Великий Новгород, 09 октября 2019 года / Под редакцией В.А. Трифонова, Я.В. Паттури. – Великий Новгород: Новгородский государственный университет имени Ярослава Мудрого, 2019. – С. 209–214. – DOI 10.34680/Innovation.2019.40.
8. Актуальные киберугрозы: итоги 2020 года / Портал Positive Technologies [Электронный ресурс] // Режим доступа: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/> (Дата обращения: 08.06.2021)
 9. Большие возможности обеспечения безопасности в мире малого бизнеса/Серия отчетов Cisco по кибербезопасности за 2020 год - Малый и средний бизнес [Электронный ресурс]/Режим доступа: https://www.cisco.com/c/dam/global/ru_ru/products/security/pdf/2020_cisco_smb-cybersecurity-report_10myths_ru.pdf (Дата обращения: 05.06.2021)
 10. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы / А.Л. Осипенко. – Омск: Изд-во Омск. акад. МВД России, 2009. – 479 с.
 11. Указ Президента Российской Федерации от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» / Доступ из справ.-правовой системы Гарант [Электронный ресурс] // Режим доступа: <https://www.garant.ru/products/ipo/prime/doc/71572608/> (Дата обращения: 04.06.2021 г.).
 12. Чепрасова Ю.В. Основные направления противодействия киберпреступности / Ю. В. Чепрасова, П. В. Шмарин // Вестник Воронежского института МВД России. – 2020. – № 3. – С. 256-262.
 13. ИБ-центр ФСБ: доля кибератак на органы власти в 2020 году выросла вдвое / Новостной портал Seldon News [Электронный ресурс] // Режим доступа: <https://news.myseldon.com/ru/news/index/249890201> (Дата обращения: 08.06.2021 г.).
 14. Игошина Е.Д. Оценка эффективности алгоритмов обнаружения подозрительных банковских транзакций // Международная научно-практическая конференция для преподавателей, аспирантов и студентов. – Язык в сфере профессиональной коммуникации. – 2020. – С. 522–527.
 15. Атнашев В.Р. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом / В. Р. Атнашев, С.Н. Яхеева // Евразийская интеграция: экономика, право, политика. – 2019. - №3. – С.37-42.
 16. Козлова О.Е. Перспективы применения положительного опыта зарубежных стран в борьбе с киберпреступностью в Российской

- Федерации / О. Е. Козлова, А. В. Самойлова, Э. В. Твердохлебова // Актуальные научные исследования в современном мире. – 2020. – № 8-5(64). – С. 42-47.
17. Долбилов А.В. Противодействие киберпреступности как угрозе экономической безопасности государства / А. В. Долбилов // Форум. Серия: Гуманитарные и экономические науки. – 2021. – № 2(22). – С. 236-239.
18. Степченкова О.С. Нормативно-правовая база экономической безопасности Российской Федерации [Электронный ресурс] / Современная экономика: проблемы и решения. - Региональная экономика. – Т.11. – 2016. – С.164-177.
19. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 07.02.2019) / Доступ из справ.-правовой системы Консультант [Электронный ресурс] // Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/ (Дата обращения: 10.06.2021 г.)

УДК 005.934:004:330.46

© А.К. Вязникова, Н.В. Кузнецова, П.Ю. Леонов, 2021

Зонт безопасности или сглаживание амплитуды циклических колебаний посредством цифровизации как основа экономической безопасности РФ

А.К. Вязникова
студентка 4 курса специалитета НИЯУ МИФИ, Москва
Email: s.vznkv@gmail.com

Н.В. Кузнецова
студентка 4 курса специалитета НИЯУ МИФИ, Москва
Email: nadyakuznetsova555@mail.ru

П.Ю. Леонов
к.э.н., доцент кафедры финансового мониторинга
НИЯУ МИФИ, Москва
Email: p.u.leonov@gmail.com

Аннотация: В статье анализируется влияние цифровизации на состояние экономических циклов. Рассматривается потенциальная модель сглаживания амплитуды циклических колебаний. Дается описание существенных факторов цифровизации. Проводится сравнение результатов воздействия цифровизации на уровень экономической безопасности в зависимости от характера экономических кризисов.

Ключевые слова: *цифровизация, амплитуда циклических колебаний, финансовый сектор, экономическая безопасность, экономический кризис.*

Safety umbrella or smoothing the amplitude of cyclical fluctuations through digitalization as the basis of the economic security of the Russian Federation

Abstract: The article analyzes the impact of digitalization on the state of economic cycles. A potential model for smoothing the amplitude of cyclic oscillations is considered. A description of the essential factors of digitalization is given. The results of the impact of digitalization on the level of economic security are compared depending on the nature of economic crises.

Keywords: digitalization, amplitude of cyclical fluctuations, financial sector, economic security, economic crisis.

С чем в современном обществе ассоциируется слово «цифровизация»? Является ли данное понятие чётко определённым показателем, характеризующим степень защищённости и развитости экономической системы страны, или же оно напоминает, скорее, идеальную, недостижимую модель, к которой общество стремится из года в год? На сегодняшний день вопрос понимания смысла, который вложен в термин «цифровизация», актуален, поскольку, в зависимости от степени осознания данного понятия, можно выделить перечень факторов цифровизации, что, в свою очередь, позволит оценить вероятность влияния внедрения технологий на состояние экономической безопасности государства в целом.

Если рассматривать цифровизацию в контексте экономических циклов, то прежде всего следует отметить вариативность (многогранность) её проявления, поскольку единого шаблона, описывающего результат влияния цифровизации на экономику государства, нет: частота наступления экономических кризисов или подъёмов зависит, в том числе, от многочисленных факторов, не включающих в себя цифровизацию. Так, например, одними из решающих показателей, способных нарушить или укрепить устойчивость экономической системы государства, а значит, повлиять на цикличность экономики в целом, являются: политическая нестабильность государства, его особенности экономической политики, миграция и иммиграция населения, а также увеличение или уменьшение степени личного потребления, сказывающегося не только на объёмах производства, но и на уровне занятости населения. [1, с. 39]

В связи с этим объективно определить роль цифровизации, ориентируясь на анализ только определённого экономического кризиса, и создать уникальную для всех стран модель, показывающую чётко

выявленный тренд роста или спада экономики, не представляется возможным, однако характеристика факторов, способных оказать воздействие на модификацию экономического цикла, а также предложение возможных результатов, в той или иной степени отражающих эффект цифровизации, позволят расширить понимание как самого термина цифровизации, так и его роли в экономической безопасности государства.

Стоит отметить, что деятельность таких финансовых органов, как Министерство финансов Российской Федерации, Банк России, Федеральное казначейство, Федеральная налоговая служба, уже направлена, в том числе, на сглаживание амплитуды циклических колебаний. Так, например, согласно ст. 35 Федерального закона от 10.07.2002 N 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», среди основных методов денежно-кредитной политики Банка России выделяют установление ориентиров роста денежной массы, процентные ставки по операциям Банка России и др. [2] При этом в годовом отчёте Банка России за 2020 год можно подробнее ознакомиться с характеристикой данных инструментов, а также с целью их применения, направленной на укрепление ценовой стабильности, а именно на поддержание годовой инфляции вблизи четырёх процентов на постоянной основе.

Таким образом, основываясь на инструментах, с помощью которых финансовые органы регулируют общую экономическую ситуацию в стране, уже можно выделить ряд факторов, оказывающих непосредственное воздействие на цикличность экономики. При этом цифровизация не теряет свою актуальность, поскольку способна повлиять на состояние экономической безопасности в неменьшей степени, чем перечисленные инструменты сглаживания. Возможно, поэтому в 2020 году цифровизация стала одним из стратегических приоритетов деятельности Центрального Банка. [3]

Чтобы наглядно проиллюстрировать эффект цифровизации, рассмотрим один из возможных вариантов изменения экономического цикла в результате усиления влияния внедрения технологий в финансовый сектор (рис. 1).

На рис.1 прежде всего следует обратить внимание на ярко выраженную чёрную линию, находящуюся на уровне 0, - так называемый стержень экономики, подразумевающий под собой стабильность, устойчивость общей экономической ситуации в стране.

Тригонометрическая функция, также представленная на графике, характеризует экономический цикл. При этом можно заметить две её вариации: первая - отражает изначальное положение экономики, наличие подъёма и кризиса без участия цифровизации, вторая - иллюстрирует

состояние экономического цикла после внедрения цифровых технологий в финансовый сектор.

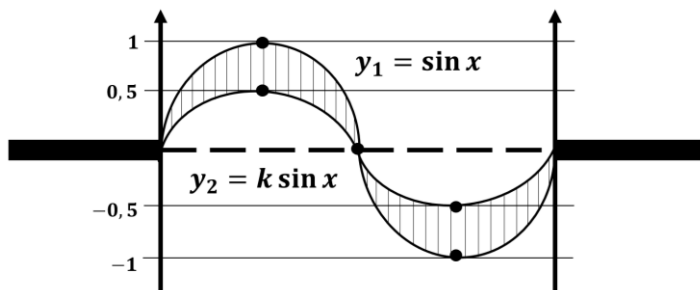


Рисунок 1 - Потенциальная модель сглаживания амплитуды циклических колебаний

Таким образом, если изначальное положение функции описывается (а точнее, симулируется) уравнением $y = \sin x$, то её изменённое состояние характеризуется уравнением $y = k \sin x$, где k - фактор цифровизации. Поскольку функция находится в отрезке $[-1; 1]$ и k не может быть равен нулю (ввиду «неидеальности» модели, объяснение чему будет рассмотрено в данной статье позже), то коэффициент k , «размещённый» на оси ординат, принимает дробные значения, что, в свою очередь, способствует сглаживанию циклических колебаний.

Возникает вопрос: какие именно факторы могут позволить функции «приблизиться» к вышеописанному стержню? Прежде всего, необходимо акцентировать внимание на том, что данная модель, в которой наблюдается сглаживание с помощью вводимых инструментов, представляет собой лишь один из вариантов графиков, поскольку та же цифровизация, представленная с другой стороны (например, внедрение цифровых технологий в финансовый сектор в определённый период, когда уровень развития экономики сильно отличается от её состояния в другом периоде), может повлиять на функцию совершенно противоположным образом, а соответственно, мы будем наблюдать уже не сглаживание амплитудных колебаний, а, например, увеличение частоты наступления экономических кризисов и подъёмов (а соответственно, коэффициент k будет занимать другое положение в функции). В связи с этим, важно подчеркнуть, что предлагаемая модель рассматривает лишь один из возможных результатов реакции состояния экономики на «соприкосновение» с цифровизацией.

Что касается потенциальных факторов (коэффициент k), то при их определении необходимо учитывать общественную среду, в которой эти факторы могут возникнуть. В связи с этим, прежде чем выделять ряд

инструментов цифровизации, следует рассмотреть некоторые статистические данные, в той или иной степени характеризующие общую обстановку в стране. Так, например, согласно представленным Росстатом данным, оценивающим ВВП за 2020 год, спрос на финансовые услуги возрос, что, в свою очередь, обусловило увеличение добавленной стоимости в финансовой сфере на 7,9%. [5] Таким образом, на основе вышерассмотренных данных, можно выдвинуть предположение о том, что финансовая сфера становится более востребованной, а значит, требует дополнительных усилий со стороны, в том числе, государства на поддержание и дальнейшее развитие инфраструктуры, обеспечивающей защиту финансовой сферы от неблагоприятных воздействий. При этом цифровизация может послужить поддержкой в развитии и укреплении бизнес-среды, поскольку информационная сфера также расширяет свои масштабы: согласно исследованию, проведённому McKinsey, использование социальных сетей распространено среди 3 млрд человек, а около 360 млн человек участвуют в трансграничной электронной торговле. [6] Таким образом, подтверждается актуальность внедрения цифровых технологий в жизнь людей - возрастает потребность в использовании цифровых платформ не только для экономических целей, но и для бытовых нужд.

Если выделять факторы цифровизации, способные сгладить амплитуду колебаний экономических циклов, то одну из существенных ролей будет играть рост количества участников передачи информации по потокам цифровой торговли, ведущий к появлению возможности быстрой смены контрагентов, что способно непосредственно повлиять на синхронизацию циклических колебаний.

Кроме того, увеличение скорости предоставления аналитических данных способствует ускорению процесса принятия решений в области передачи информации, что, в свою очередь, может привести, с одной стороны, к сокращению операционных расходов, а с другой стороны, к росту объёмов передаваемой продукции.

Необходимо отметить, что тригонометрическая функция в нашей модели никогда не достигнет вышеописанного стержня, однако будет бесконечно стремиться к нему, постепенно сглаживая амплитуду циклических колебаний.

Почему, на наш взгляд, невозможно достичь полного равновесия и, тем самым, минимизировать риск возникновения экономических кризисов и подъёмов полностью, сделав его настолько несущественным, что он бы не смог оказать значительное влияние на экономику в целом? Однако, при всей невозможности достичь так называемой цели, почему необходимо всё же стремиться к ней? Другими словами, почему наличие циклических

колебаний - не только неизбежно, но и полезно для экономической политики государства, а полезность, при этом, не опровергает предложенную нами теорию о важности стремления к сглаживанию данных циклических колебаний?

Чтобы ответить на данные вопросы, необходимо вспомнить самые крупные экономические кризисы Российской Федерации и, проанализировав их влияние на общую экономическую ситуацию в стране, постараться выявить закономерность в их воздействии на жизнь людей.

Так, если ключевой проблемой экономического кризиса, наступившего в первой половине 1990-х годов, являлась инфляция, подорвавшая мотивацию людей в сфере долгосрочного инвестирования в производство, а также обесценившая оборотный капитал, то особенностью кризиса 2014-го года можно считать наличие одновременного воздействия огромного количества создающих серьёзные проблемы факторов, ранее влияющих, в основном, по-отдельности. Среди подобных «вызовов» можно назвать следующие: инфляция, принявшая рекордное на тот момент, значение; отток капитала, составивший более 100 млрд долларов; падение цен на нефть, характеризующееся показателями, более низкими по сравнению с заложенными ценами в бюджете на 2014 - 2015 гг.; санкции, введённые против Российской Федерации, ограничивающие её возможности и, тем самым, наносящие вред экономике. [4]

Таким образом, в зависимости от особенностей общей экономической ситуации в стране, а также от уровня готовности государства предпринимать действия по устранению негативных последствий, и будет установлена степень влияния факторов, а значит, единой закономерности в определении эффекта от цифровизации - нет, поскольку на экономический цикл одновременно влияет множество факторов помимо цифровых технологий. Кроме того, взаимодействие каждого фактора цифровизации с каким-либо другим фактором, участвующим в формировании состояния экономики, а значит, влияющим на амплитуду циклических колебаний, тоже будет иметь свои особенности, т.е. результат взаимодействия одной группы инструментов будет отличаться от результата взаимодействия другой группы.

Другой характерной чертой кризисов является их неизбежность, поскольку они представляют собой, в том числе, закономерный этап развития государства, позволяющий обнаружить серьёзные упущения и недостатки в экономической политике и предпринять определённые действия не только для устранения неэффективных звеньев в общей структуре и укрепления слабых сторон, но и для предотвращения возможных дальнейших обстоятельств, тормозящих планируемое развитие

и, тем самым, негативно сказывающихся на экономической безопасности страны.

Что же касается необходимости стремиться к минимизации риска наступления экономического кризиса, а значит, к сглаживанию амплитуды циклических колебаний (несмотря на недостижимость полного выравнивания функции, иллюстрирующей данные колебания), то здесь стоит отметить зависимость уровня экономической безопасности страны от состояния экономических циклов. Так, например, в п. 12 Стратегии экономической безопасности РФ усиление структурных дисбалансов в финансовой системе признано угрозой экономической безопасности. [7] Таким образом, целенаправленное устранение подобных вызовов, способных негативно отразиться на состоянии экономического цикла, должно служить одним из основных приоритетов государства. При этом цифровизация, оказывающая влияние на состояние финансового сектора, способна также увеличить (уменьшить) уровень и экономической безопасности страны в целом.

Подводя итог, подчеркнём наличие возможности разностороннего влияния внедрения цифровых технологий в экономику, когда каждый вариант событий заслуживает свою собственную, отдельную модель, отражающую индивидуальные особенности конкретного периода, определённого цикла. Мы рассмотрели один из таких вариантов, а именно: сглаживание амплитуды циклических колебаний, подразумевающее под собой не только укрепление стабильности и устойчивости экономики страны, но и создание более крепкого фундамента для развития будущих поколений.

Список использованных источников:

1. Саталкина Н. И. Макроэкономика для бакалавров: учебное пособие/ Н. И. Саталкина, Г. И. Терехова, Ю. О. Терехова. – Тамбов: Изд-во ФГБОУ ВПО «ТГТУ», 2014. – 108 с.
2. Федеральный закон от 10.07.2002 № 86-ФЗ (ред. от 20.04.2021) «О Центральном банке Российской Федерации (Банке России)» // Правовая справочно-информационная система «КонсультантПлюс»
3. «Годовой отчёт Банка России за 2020 год». [В Интернете]. Режим доступа: http://www.cbr.ru/about_br/publ/god/. (дата обращения: 12.06.2021)
4. Ильясова Э.Н., Умерова З.Н. Экономический цикл и его влияние на современную экономику российской федерации // Сборник научных трудов. В 2-х томах. Под общей редакцией З.О. Адамановой. – РИНЦ. – 2019. – С. 660 - 664.

5. «Росстат представляет первую оценку ВВП за 2020 год». [В Интернете]. Режим доступа: <https://rosstat.gov.ru/folder/313/document/113015>. (дата обращения: 12.06.2021)
6. The new dynamics of financial globalization. McKinsey Global Institute, 2017. 24 p.
7. Указ Президента РФ от 13.05.2017 N 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // Правовая справочно-информационная система «КонсультантПлюс»

УДК 005.52:005.934:657.633.8

© В.М. Сушков, Н.С. Белогина, 2021

**Использование аналитических процедур для выявления
манипулирования отчетностью в части сведений об основных
средствах**

В.М. Сушков
студент 4 курса специалитета НИЯУ МИФИ, Москва
Email: vmsushkov@mail.ru
Н.С. Белогина
к.э.н, доцент кафедры «Бухгалтерский учет и аудит»
НИЯУ МИФИ, Москва
Email: nsbelog@gmail.com

Аннотация: В статье анализируются методы манипулирования бухгалтерской (финансовой) отчетностью в части раскрытия информации об основных средствах организации. Предлагаются аналитические процедуры выявления искажений сведений об основных средствах на основе методов финансового и статистического анализа. Делаются выводы об эффективности их применения в российской практике.

Ключевые слова: манипулирование отчетностью, мошенничество с основными средствами, аналитические процедуры, методики выявления искажений отчетности, дерево мошенничества, закон Бенфорда, модель Бениша.

Using analytical procedures to detect accounting misstatements in terms of
information about fixed assets

Abstract: The article analyzes the methods of financial statements manipulation in terms of disclosing information about the fixed assets of an organization. Analytical procedures for detecting distortion of information about fixed assets based on the methods of financial and statistical analysis are proposed. Conclusions are made about the effectiveness of their application in Russian practice.

Keywords: financial statements manipulation, fraud with fixed assets, analytical procedures, fraud tree, methods of detecting distortions in financial statements, Benford's law, Beneish model.

Основные средства являются ключевыми активами для большинства хозяйствующих субъектов, поскольку образуют производственно-техническую базу и определяют производственный потенциал. Как правило, это активы высокой стоимости, которые используются многократно и в течение длительного периода времени сохраняют свои свойства.

В соответствии с п. 4 ФСБУ 6/2020 «Основные средства», под основными средствами признаются активы, одновременно обладающие следующими признаками:

1. Способность приносить экономические выгоды в будущем (характеристика актива);
2. Использование в ходе обычной деятельности, для предоставления за плату во временное пользование, для управленческих нужд и пр. (характеристика актива);
3. Использование в течение периода, превышающего 12 месяцев, или обычного операционного цикла, превышающего 12 месяцев (характеристика внеоборотного актива);
4. Материально-вещественная форма. [1]

Для обеспечения бесперебойного процесса производства продукции, выполнения работ или оказания услуг экономические субъекты могут иметь основные средства в собственности или привлекать во временное пользование.

Контроль за состоянием и учетом основных средств является неотъемлемой частью системы внутреннего контроля организации, предметом внешнего аудита, а также проверок со стороны налоговых органов (в части формирования налоговой базы по налогу на прибыль и имущественного налога). Повышенное внимание к данному объекту учета объясняется его уязвимостью как к непреднамеренному, так и к умышленному искажению в учете и бухгалтерской отчетности.

Мошенничество с бухгалтерской (финансовой) отчетностью предполагает умышленное не отражение или изменение фактов

хозяйственной жизни в бухгалтерском учете и отчетности, осуществляемое с целью получения неправомερных или незаконных преимуществ и способное ввести в заблуждение пользователей отчетности. [2, 3] Ассоциация специалистов по расследованию мошенничества (ACFE) разработала и опубликовала в Глобальном исследовании мошенничества за 2020 год модель отнесения видов мошенничества по категориям, известную как «дерево мошенничества». [2] Одной из категорий данной модели является мошенничество с бухгалтерской (финансовой) отчетностью, основные направления которого приведены на рис. 1.



Рисунок 1 – Направления мошенничества с бухгалтерской (финансовой) отчетностью

Основные средства организации подвержены риску мошенничества с использованием всех пяти представленных схем. В табл.1 приведены примеры таких мошеннических действий, сгруппированные по способам.

Таблица 1 – Примеры мошенничества с основными средствами

Мошенническая схема	Мошеннические действия
А) Временные разницы	1. Неравномерное начисление амортизации с целью сглаживания прибыли 2. Начисление амортизации текущего года в последующем периоде с целью завышения активов и прибыли 3. Начисление амортизации последующего периода в отчетном году с целью занижения налоговой базы по налогу на прибыль 4. Оприходование основных средств, приобретенных в начале следующего отчетного периода, в конце текущего периода с целью завышения активов 5. Оприходование излишков основных средств, выявленных по результатам инвентаризации,

	проведенной в начале следующего отчетного периода, в конце текущего периода с целью завышения активов 6. Отражение доходов, связанных с выбытием основных средств в начале следующего отчетного периода, в конце текущего периода с целью повышения инвестиционной привлекательности, улучшения финансового положения, получения бонусов управленческим персоналом
В) Приписки и сокрытие выручки	1. Неотражение выручки от реализации основного средства с целью занижения налоговой базы по налогу на прибыль 2. Завышение выручки от реализации основного средства с целью повышения инвестиционной привлекательности, улучшения финансового положения, получения бонусов управленческим персоналом
С) Приписки и сокрытие обязательств/расходов	1. Завышение амортизации путем выбора нерационального метода, метода, не соответствующего учетной политике или ПБУ 6/01 (ФСБУ 6/2020), фальсификации документов аналитического учета с целью занижения налоговой базы по налогу на прибыль, ухудшения финансового положения 2. Занижение амортизации путем выбора нерационального метода, метода, не соответствующего учетной политике или ПБУ 6/01 (ФСБУ 6/2020), фальсификации документов аналитического учета с целью завышения активов 3. Преждевременное списание основных средств с целью незаконного присвоения, уменьшения налоговой базы по налогу на имущество и налогу на прибыль 4. Начисление амортизации по истечении срока полезного использования с целью занижения налоговой базы по налогу на прибыль
Д) Неправильная оценка активов	1. Занижение первоначальной стоимости основных средств с целью занижения налоговой базы по налогу на имущество 2. Завышение первоначальной стоимости основных средств с целью завышения активов и занижения налоговой базы по налогу на прибыль 3. Амортизация объектов природопользования с целью занижения налоговой базы по налогу на прибыль

	4. Скрытие под видом ремонтных работ затрат на модернизацию или новое строительство с целью снижения налоговой базы по налогу на имущество и налогу прибыль в текущем периоде 5. Переоценка основных средств до стоимости, выше справедливой, с целью завышения активов 6. Переоценка основных средств до стоимости, ниже справедливой, с целью занижения налоговой базы по налогу на имущество 7. Занижение срока полезного использования основных средств с целью ускоренного списания и незаконного присвоения 8. Завышение срока полезного использования основных средств с целью замедленного списания и завышения активов 9. Завышение ликвидационной стоимости основных средств с целью завышения активов 10. Завышение оценочных обязательств на демонтаж и восстановление окружающей среды после ликвидации основных средств с целью занижения налоговой базы по налогу на прибыль 11. Невыполнение требования о проверке основных средств на обесценение с целью завышения активов
Е) Раскрытие неверной информации	1. Отражение в отчетности объекта основных средств, который фактически отсутствует по причине: ▪ Незаконного присвоения ▪ Реализации без списания ▪ Не отражения выявленных недостатков при проведении инвентаризации 2. Отражение в отчетности объекта основных средств, подлежащего списанию или перегруппировке по причине: ▪ Физического или морального износа ▪ Невозможности приносить экономические выгоды ▪ Не использования в производстве, либо для управленческих нужд, либо для сдачи в аренду ▪ Предположения к продаже ▪ Предназначения к использованию в течение срока менее 12 месяцев ▪ Искусственной пересортицы основных средств

	3. Отражение в отчетности основных средств, полученных в аренду или на ответственное хранение, с целью завышения активов 4. Не отражение в отчетности объекта основных средств, который фактически используется, с целью избежания уплаты налога на имущество 5. Не отражение в отчетности материальных ценностей, полученных при ликвидации основных средств, излишков основных средств, выявленных по результатам инвентаризации, по причине незаконного присвоения 6. Не отражение в отчетности основных средств, сданных в аренду, с целью избежания уплаты налога на имущество
--	---

Исходя из данных табл.1, основные средства наиболее уязвимы к мошенничеству с неправильной оценкой. Это объясняется широким спектром операций, требующих оценки основных средств – формирование первоначальной стоимости, ее уменьшение или увеличение в результате переоценки или проведения модернизации, определение остаточной стоимости при ежемесячном начислении амортизации, выбытии и пр. Более того, список данных операций расширился с введением в действие ФСБУ 6/2020 «Основные средства», который обязателен к применению, начиная с отчетности за 2022 год. Поскольку разработка стандарта велась на основе МСФО (IAS) 16 «Основные средства», в его содержании появился ряд положений, требующих от руководителя и бухгалтера организации вынесения профессионального суждения. Так, при принятии к учету основных средств теперь необходимо определять ликвидационную стоимость, создавать оценочные обязательства на демонтаж и восстановление окружающей среды после их ликвидации, а также регулярно проверять основные средства на обесценение. Поскольку оценка данных операций производится субъективно, нежели чем на основе документов или инструкций, это накладывает на сотрудников организации большую ответственность и, как следствие, может отразиться на достоверности финансовой отчетности.

Мотивами совершения рассмотренных мошеннических действий в первую очередь выступают желание завысить стоимость внеоборотных активов, в частности, для улучшения финансового положения при получении заемных средств; незаконное присвоение основных средств или создание условий для их присвоения; занижение налоговой базы по налогу на прибыль и налогу на имущество организаций. Виновными лицами могут выступать бухгалтеры, сотрудники производственных подразделений,

экспедиторы, юристы, менеджеры, директора и т.д. вплоть до собственников.

Одними из методов обнаружения мошенничества с основными средствами являются аналитические процедуры. Аналитические процедуры – это оценка финансовой информации посредством анализа вероятных взаимосвязей между финансовыми и нефинансовыми данными, которая способствует выявлению отклонений и соотношений, которые противоречат прочей имеющейся информации или существенно расходятся с ожидаемыми показателями. [4] Рассмотрим виды аналитических процедур, направленных на выявление мошеннических действий в отношении основных средств организации.

В первую очередь, эффективно использовать методы финансового анализа показателей состояния, движения и эффективности использования основных средств. Наиболее распространенные из них представлены в табл. 2. [5, 6]

Таблица 2 – Показатели состояния, движения и эффективности использования основных средств

Показатель	Расчет	Значение
Показатели состояния и движения основных средств		
Коэффициент ввода (обновления) основных средств	$K_{\text{ввода}} = \frac{\text{Приход ОС}}{\text{Стоимость ОС}_{\text{к.г.}}}$	Доля новых основных средств во всех основных средствах, имеющих на конец отчетного периода
Коэффициент выбытия основных средств	$K_{\text{выб}} = \frac{\text{Расход ОС}}{\text{Стоимость ОС}_{\text{н.г.}}}$	Доля выбывших основных средств во всех основных средствах, имеющих на начало отчетного периода
Коэффициент прироста основных средств	$K_{\text{пр}} = \frac{\text{Приход ОС} - \text{Расход ОС}}{\text{Стоимость ОС}_{\text{н.г.}}}$	Оценка относительного увеличения или уменьшения основных средств
Коэффициент износа основных средств	$K_{\text{изн}} = \frac{\text{Амортизация}_{\text{накопл}}}{\text{Стоимость ОС}_{\text{к.г.}}}$	Оценка износа основных средств в отношении начисленной амортизации

Коэффициент годности основных средств	$K_{\text{годн}} = 1 - K_{\text{изн}} = \frac{\text{Остаточная стоимость}}{\text{Стоимость ОС}_{\text{к.г.}}}$	Оценка физического состояния основных средств в отношении остаточной стоимости
Средняя норма амортизации (норма восстановления) основных средств	$\text{Ср. н.}_{\text{ам}} = \frac{\text{Амортизация}_{\text{год}}}{\text{Стоимость ОС}_{\text{год}}}$	Оценка уровня начисляемого износа основных средств
Временные характеристики состояния основных средств		
Период (срок) полного обновления основных средств	$T_{\text{обн}} = \frac{\text{Стоимость ОС}_{\text{к.г.}}}{\text{Приход ОС}}$	Период времени, через который полностью обновятся основные средства, имеющиеся на конец отчетного периода
Период полного выбытия основных средств	$T_{\text{выб}} = \frac{\text{Стоимость ОС}_{\text{н.г.}}}{\text{Расход ОС}}$	Период времени, через который полностью выйдут основные средства, имеющиеся на начало отчетного периода
Средний нормативный срок службы основных средств	$T_{\text{спи}_{\text{норм}}} = \frac{\overline{\text{Стоимость ОС}_{\text{год}}}}{\text{Амортизация}_{\text{год}}}$	Период времени, при котором основные средства могут использоваться до полного износа
Средний фактический срок службы основных средств	$T_{\text{спи}_{\text{факт}}} = \frac{\text{Амортизация}_{\text{накоп}}}{\text{Амортизация}_{\text{год}}}$	Период времени, при котором основные средства фактически используются до полного износа
Остаточный срок службы основных средств	$T_{\text{ост}} = \frac{\overline{\text{СПИ}}}{K_{\text{годн}}}$	Период времени, по истечении которого имеющиеся основные средства будут полностью изношены

Показатели эффективности использования основных средств		
Фондоотдача (оборачиваемость) основных средств	$FO = \frac{\text{Выручка}}{\text{Стоимость ОС}_{\text{год}}}$	Выручка, полученная с каждого рубля, вложенного в основные средства
Фондоотдача активной части основных средств	$FO_a = \frac{\text{Выручка}}{\text{Ст. акт. части ОС}_{\text{год}}}$	Выручка, полученная с каждого рубля, вложенного в основные средства, непосредственно используемые в производственном процессе
Фондоемкость основных средств	$FE = \frac{1}{FO} = \frac{\text{Стоимость ОС}_{\text{год}}}{\text{Выручка}}$	Стоимость основных средств, приходящаяся на каждый рубль проданной продукции (работ, услуг)
Фондовооруженность	$FV = \frac{\text{Стоимость ОС}_{\text{год}}}{\text{Численность рабочих}}$	Стоимость основных средств, которой располагает один работник
Фондорентабельность	$R_{OC} = \frac{\text{Чистая прибыль}}{\text{Стоимость ОС}_{\text{год}}}$	Прибыль, полученная с каждого рубля, вложенного в основные средства

При анализе показателей состояния, движения и эффективности использования основных средств следует обращать внимание на значительные отклонения и колебания показателей организации в сравнении со среднеотраслевыми, показателями партнеров и конкурентов, а также на нелогичные зависимости между показателями. Например, наличие низкой фондоотдачи и фондорентабельности при высоких коэффициентах ввода (обновления) и прироста основных средств, низкая фондоемкость при высоких коэффициентах выбытия и износа основных средств, превышение коэффициента выбытия над средней нормой амортизации или периода полного выбытия над нормативным сроком службы основных средств.

При этом анализ финансовых показателей рекомендуется проводить не в единый момент времени, а в динамике и структуре. Для этого задействуются методы горизонтального и вертикального экономического анализа. Горизонтальный анализ (анализ тренда) базируется на анализе

показателей за различные периоды времени. С помощью вертикального анализа (анализа структуры) изучается соотношение выбранного показателя с другими однородными показателями в рамках одного отчетного периода. [6] Использование данных методов позволяет выявлять необычные тенденции изменения показателей и их нелогичную структуру, что может являться признаком манипулирования отчетностью.

Кроме того, возможно использование факторного метода экономического анализа, который позволяет измерить степень влияния факторов на результативный показатель. [6] Простейшей факторной моделью в рамках анализа основных средств будет являться зависимость фондоотдачи от выручки и среднегодовой стоимости основных средств. В нормальных экономических условиях влияние обоих факторов должно быть сбалансированным. Нелогичной структурой будет являться высокий вклад в фондоотдачу среднегодовой стоимости основных средств по сравнению с выручкой.

Помимо этого, в отношении основных средств информативным является построение следующих факторных моделей:

1. Влияние на фондоотдачу всех основных средств эффективности использования активной части основных средств и их структуры;
2. Влияние на фондоотдачу производительности труда и фондовооруженности;
3. Влияние на фондорентабельность рентабельности продукции (конкурентоспособности продукции) и фондоотдачи;
4. Оценка эффективности использования основных средств по относительному высвобождению/вовлечению основных средств (по среднегодовой стоимости основных средств);
5. Факторный анализ прироста выручки для определения экстенсивного или интенсивного пути использования основных средств;
6. Оценка эффективности использования основных средств по относительной экономии/перерасходу амортизационных расходов.

Дополнять анализ финансовых показателей состояния и эффективности использования основных средств могут следующие процедуры:

1. Сопоставление цен покупки и продажи основных средств со среднеотраслевыми;
2. Сопоставление налоговой нагрузки юридического лица по налогу на имущество со среднеотраслевыми;
3. Отслеживание денежного содержания выручки от реализации основных средств.

Помимо методов финансового анализа в мировой практике для выявления преднамеренного искажения информации широко применяется метод статистического анализа, часто называемый в литературе «Закон

Бенфорда» (закон первой цифры, закон аномальных чисел). Его суть заключается в сопоставлении эмпирического распределения частот возникновения первой цифры в искусственно созданном числовом массиве данных с теоретическим, измеренном Фрэнком Бэнфордом в 1938 году. Вероятность цифры быть первой измеряется по формуле:

$$P(d) = \log_b(d + 1) - \log_b(d) = \log_b\left(1 + \frac{1}{d}\right),$$

где b – система счисления ($b > 2$);

d – цифры в данной системе счисления ($d \in \{1, \dots, b - 1\}$).

Так, для десятичной системы счисления вероятности появления первой цифры представлены на рис. 2.

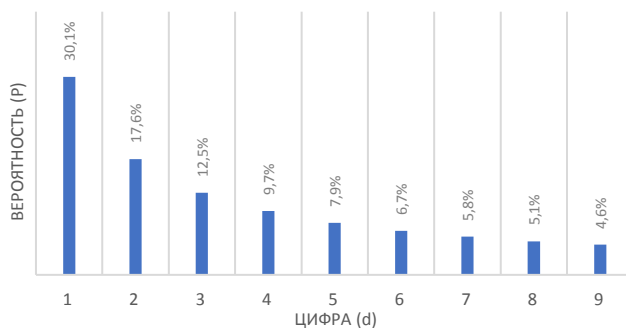


Рисунок 2 – Вероятности появления первой цифры в десятичной системе исчисления

Существенные отклонения распределения частот появления первых цифр в реальном массиве данных от распределения Бенфорда, таким образом, позволяют сделать предположение о наличии ошибок или искажений в нем. На проверяемый массив данных, тем не менее, накладывается ряд существенных ограничений – он должен быть числовым, достаточно большого объема и не ограничен минимальными или максимальными значениями. [7]

Закон Бенфорда в последние десятилетия получил широкое распространение и стал применяться во внешнем и внутреннем аудите, внутренних расследованиях, налоговых проверках, страховой, оценочной деятельности, прогнозировании банкротства, обнаружения DOS-атак и т.д. При этом разработано множество вариаций классического метода, таких как анализ частот первой и второй цифр, дублей, первой пары цифр, первой тройки цифр, округлений и пр.

В целях обнаружения искажений по операциям и событиям с основными средствами в качестве массивов данных могут выступать суммы бухгалтерских проводок, выставленных счетов, начисленной

амортизации, затрат на текущий ремонт и модернизацию, суммы в налоговых декларациях. Причем для эффективного применения тестов на основе закона Бенфорда значения в выборках должны состоять из нескольких порядков, что может быть проблематично для малых компаний с неинтенсивной операционной и инвестиционной деятельностью. [8]

Наконец, известной в международной практике аналитической процедурой выявления искажений в бухгалтерской (финансовой) отчетности является система показателей, разработанная Мессодом Бенишем в 1999 году («карта нормативных отклонений финансовых индикаторов»). Это комплексная методика, созданная для обнаружения риска манипуляций с отчетностью зарубежных компаний, которая в первую очередь ориентирована на фондовый рынок. В части проверки основных средств в данной модели рассчитывается коэффициент амортизации (DPI, depreciation index) по следующей формуле:

$$DPI = \frac{D_{t-1}/(D_{t-1}+PPE_{t-1})}{D_t/(D_t+PPE_t)},$$

где D – сумма амортизации (depreciation);

PPE – стоимость основных средств (property, plant and equipment);

t – номер года.

Исходя из анализа финансовой отчетности более 1500 компаний из базы Standart & Poor's Compustat, профессор Бениш определил, что среднее значение коэффициента DPI для добросовестных компаний составляет 1,001. [7] Значение показателя выше единицы, а также динамика его изменения в сторону увеличения свидетельствует о том, что эффективная норма амортизации основных средств замедляется и компания увеличивает срок начисления амортизации с целью занижения расходов. Для российских компаний, интересы которой в большинстве случаев заключаются в занижении налоговой базы по налогу на прибыль, данный коэффициент рационально проверять на занижение, то есть на увеличение сумм начисленной амортизации с целью завышения расходов, а также занижения стоимости основных средств (создание условий для преждевременного списания).

Подводя итог, следует отметить, что ни одна из рассмотренных аналитических процедур не способна выявить конкретные объекты основных средств, с которыми производятся недобросовестные действия. Более того, обнаружение подозрительных признаков в деятельности компании не является абсолютным свидетельством совершения мошеннических действий, а лишь основанием для проведения более детального анализа, в том числе с использованием иных методов – инвентаризации, осмотра, опроса, инспектирования документов, встречной проверки и пр. Аналитические методы выступают объективными инструментами выявления «красных флажков» значительного искажения

бухгалтерской (финансовой) отчетности в части основных средств, наиболее распространенными способами которого в российской практике являются вуалирование незаконного присвоения, завышение или занижение оценочных показателей, расходов и обязательств, а также необоснованная капитализация расходов.

Список использованных источников:

1. Федеральный стандарт бухгалтерского учета ФСБУ 6/2020 «Основные средства» (введен в действие на территории Российской Федерации Приказом Минфина России от 17.09.2020 № 204н) // Официальный интернет-портал правовой информации [Электронный источник] – Режим доступа: <http://www.pravo.gov.ru>.
2. 2020 ACFE Report to the Nations // Association of Certified Fraud Examiners [Электронный источник] – Режим доступа: <https://www.acfe.com/report-to-the-nations/2020/>.
3. Международный стандарт аудита 240 «Обязанности аудитора в отношении недобросовестных действий при проведении аудита финансовой отчетности» (введен в действие на территории Российской Федерации Приказом Минфина России от 09.01.2019 N 2н) // Официальный сайт Минфина России [Электронный источник] – Режим доступа: <http://www.minfin.ru/>.
4. Международный стандарт аудита 520 «Аналитические процедуры» (введен в действие на территории Российской Федерации Приказом Минфина России от 09.01.2019 N 2н) // Официальный сайт Минфина России [Электронный источник] – Режим доступа: <http://www.minfin.ru/>.
5. Когденко В.Г., Крашенинникова М.С. Особенности анализа основных средств и финансовых вложений на основе новых форм отчетности (пояснения к бухгалтерскому балансу и отчету о прибылях и убытках) // Экономический анализ: теория и практика. – М.: ООО «Издательский дом «Финансы и кредит». – 2012. – № 25 (280). – с. 8 - 20.
6. Когденко В.Г. Экономический анализ / М.: Юнити, 2012. – 392 с.
7. Суйц В.П., Хорин А.Н., Жакипбеков Д.С. Диагностика недостоверности отчетности организации: статистические методы в оценке достоверности бухгалтерской отчетности // Аудит и финансовый анализ. – М.: ООО Издательство «ДСМ Пресс». – 2015. – № 1. – с. 179 - 188.
8. Вараксина А.С. Методы выявления искажений информации об основных средствах в бухгалтерской отчетности // Сборник статей II международной научно-практической конференции – М.: Научно-издательский центр «Актуальность.РФ». – 2018. – с. 259 - 260.

**Использование современных аналитических технологий при
проведении практических занятий по дисциплине «Экономическая
безопасность» на примере комплекса Лампир**

М.Н. Синадский
студент 2 курса специалитета УНЦ «Информационная безопасность»
ИРИТ-РтФ УрФУ, Екатеринбург
Email: mishasinad@yandex.ru
О.Ю. Синадская
старший преподаватель УНЦ «Информационная безопасность»
ИРИТ-РтФ УрФУ, Екатеринбург
Email: o.iu.sinadskaia@urfu.ru

Аннотация: с целью проведения практико-ориентированных занятий по изучению информационно-аналитических систем безопасности предложен модуль генератора массивов биллинговой информации о взаимодействии пользователей, учитывающий поведенческую модель абонентов на основе шаблонов перемещений.

Ключевые слова: информационно-аналитические системы безопасности, генератор, биллинговая информация.

Investigation of fraud in cellular networks using modern analytical technologies
on the example of the Lampir complex

Abstract: in order to conduct practice-oriented classes on the study of information and analytical security systems, a module for generating arrays of billing information about user interaction is proposed, which takes into account the behavioral model of subscribers based on movement patterns.

Keywords: information and analytical security systems, generator, billing information.

В соответствии с образовательной программой специалитета 10.05.04 «Информационно-аналитические системы безопасности», разработанной на основе требований Федерального государственного образовательного стандарта высшего образования, выпускник с квалификацией «специалист по защите информации» со специализацией «Информационная безопасность финансовых и экономических структур» должен быть подготовлен к профессиональной деятельности в сфере применения

автоматизированных информационно-аналитических систем, обеспечивающих обработку и анализ специальной информации (финансовой и экономической), а также функционирующих в составе этих систем прикладных средств современных информационных технологий.

Достижение результатов освоения образовательной программы осуществляется посредством освоения группы взаимосвязанных между собой компетенций, которые формируются в рамках дисциплин и позволяют выпускнику реализовать определенный вид профессиональной деятельности и соответствующие ему профессиональные задачи. В частности, способность решать задачи выявления, классификации и последующего предметного анализа информационных объектов с признаками подготовки и/или совершения преступлений в финансовой и экономической сферах деятельности (ОПК-2.3), а также способность разрабатывать и применять автоматизированные технологии обработки больших информационных потоков (массивов) финансовой и/или экономической информации в режиме реального времени (ОПК-2.4) [1].

В рамках обеспечения информационной безопасности с целью выявления и расследования, в том числе, фактов мошенничества с использованием средств связи применяются информационно-аналитические системы безопасности (далее — ИАСБ). При проведении на потоках по направлению «Информационная безопасность» практических занятий по расследованию компьютерных инцидентов, в ходе которых изучаются ИАСБ, должны использоваться массивы биллинговой информации. При этом использование настоящих данных невозможно, в том числе в силу ограничений, накладываемых ФЗ «О связи» [2].

Для совершенствования методики обучения и создания условий для проведения практико-ориентированных занятий по изучению аналитических методик в рамках компьютерного полигона Учебно-научного центра «Информационная безопасность» ИРИТ-РтФ УрФУ развернут «Генератор массивов биллинговой информации» [3]. Одна из задач проекта — разработка модулей программного комплекса генератора массивов биллинговой информации, соответствующих реальным массивам по формату данных, статистической и поведенческой модели абонентов.

В рамках проекта реализована генерация массивов биллинговой информации о взаимодействии пользователей в сетях операторов сотовой связи, которая заключается в создании псевдослучайных действий абонентов на основании статистико-событийной модели [4]. Генерация осуществляется с учетом статистических распределений, сгенерированной совокупности имен, фамилий и отчеств с их частотным распределением, случайных неповторяющихся данных IMSI, IMEI, MSISDN, LAC, CELLID, а также шаблонов перемещений.

Для придания итоговому массиву биллинговой информации наибольшей реалистичности поведенческих характеристик абонентов разработан генератор шаблонов перемещений. В модуле реализован алгоритм поведения вымышленных абонентов, основанный на задании их осмысленных перемещений в рамках населенного пункта по заданной территории между базовыми станциями операторов сетей сотовой связи.

Карта населённого пункта (города) разделена на отдельные квадраты. Для каждой клетки квадрата задаются уникальные параметры LAC (Location Area Code – код локальной зоны) и CellID (уникальный номер, предназначенный для идентификации базовых станций) обслуживающих её базовых станций, которые могут модифицироваться посредством применения списков базовых станций.

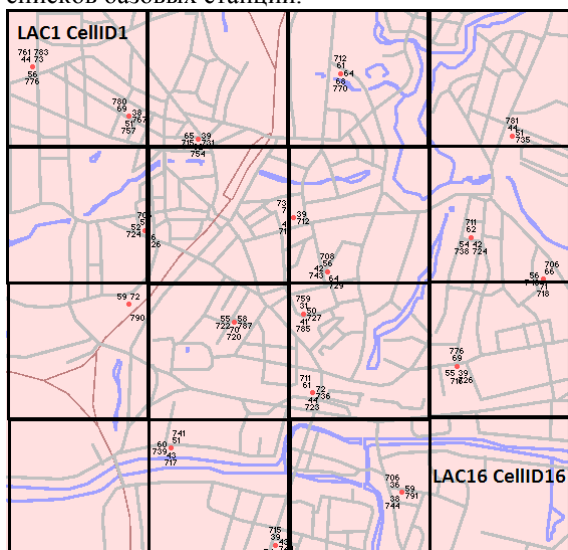


Рисунок 1 - Схема разделения территории на области действия базовых станций

Передвижение абонентов в рамках населенного пункта описывается шаблонами перемещений. Шаблон перемещений представляет собой упорядоченный по времени список LAC и CellID, по которому отслеживается передвижение абонента в течение заданного времени. Так как каждой базовой станции ставятся в соответствие ее прямоугольные координаты, то шаблон перемещений является набором геометок позиций полей карты. Количество меток определяется частотой обновления геопозиции. Геометка показывает, в каком из участков местности находился абонент в период между обновлениями геопозиции. Коррекция перечня LAC, CellID и их прямоугольных координат на географической

карте позволяет формировать биллинг для произвольного населенного пункта.

При генерации биллинга каждому абоненту присваивается один из заранее сгенерированных шаблонов перемещений, что позволяет учитывать различные поведенческие характеристики абонентов. Входными данными для модуля являются: размер квадрата карты, в который вписан город; необходимое количество шаблонов перемещений; частота считывания обновления геопозиции; временные промежутки, в которые абоненты совершают перемещение от объектов «дом» до объектов «работа» и обратно. В зависимости от полученных на вход параметров, определяющих характеристики населенного пункта и поведенческие свойства абонентов, модуль формирует массив шаблонов перемещений, который в дальнейшем используется для учета движения абонентов между базовыми станциями.

Модуль генератора шаблонов перемещений является совокупностью блоков: генерации объектов на карте; инициализации начального состояния; выбора пункта назначения; перемещения между объектами. В начале работы модуля происходит инициализация и считывание входных параметров. Далее осуществляется создание объектов на карте: «домов» (на половине ячеек карты), «работ» (на четверти ячеек карты) и «магазинов» (на четверти ячеек карты). Карта представляет собой упорядоченный список номеров квадратов (ячеек карты), нумерация ведется построчно от 0 и до максимального значения, задаваемого размером города. Следующим шагом создается структура данных абонента: позиции дома, работы, временные метки. Имитация перемещения абонента происходит по временным меткам. При наступлении временного события происходит назначение цели («работа» или «дом») перемещения абонента, вспомогательная функция рассматривает движение абонента по двум осям, и каждый временной промежуток перемещает его на одну геометку ближе к цели. Перемещение между объектами происходит по кратчайшему пути, но если абонент движется от объекта «работа» к объекту «дом», и на пути следования в пределах меры близости оказывается объект «магазин» (при этом признак посещения объекта «магазин» не был определен положительно), то абонент обязательно изменяет траекторию, посещая объект «магазин», а потом продолжает движение к цели – объекту «дом».

Результатом работы является модуль генератора шаблонов перемещений, учитывающий поведенческие характеристики абонентов и характеристики местности – размер поля карты и количество объектов, размещенных на ней. В формируемом массиве шаблонов перемещений для

произвольного количества абонентов задается индивидуальное осмысленное движение по полю карты.

В рамках расследования компьютерного инцидента поставлена задача: по суточному массиву биллинговой информации необходимо определить, каким абонентам совершались звонки с определённого номера. Для анализа взяты массивы данных сгенерированные в работах [4, 5].

Данную задачу можно решить с помощью ИАСБ Lampyre [6], на рис. 2 изображен титульный экран ИАСБ.

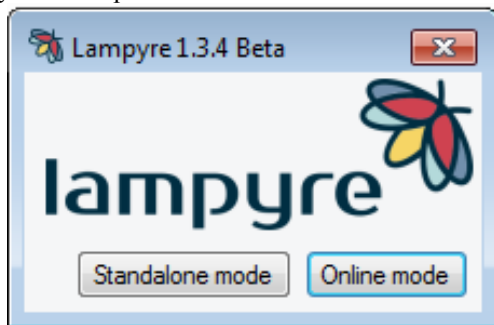


Рисунок 2 - Экран выбора режима работы ИАСБ Lampyre

В начале работы создается новое «расследование» (рис.3), в которое осуществляется загрузка файла, содержащего массив биллинговых данных (рис.4).

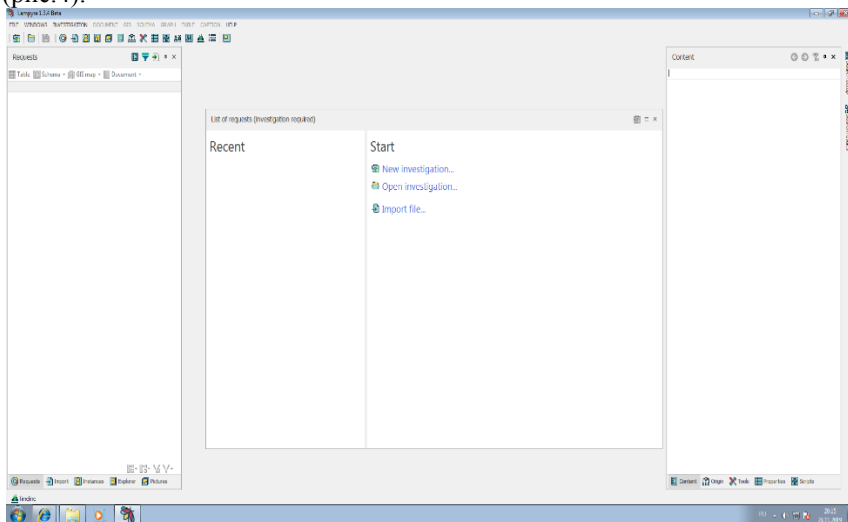


Рисунок 3 - Начальный экран ИАСБ Lampyre

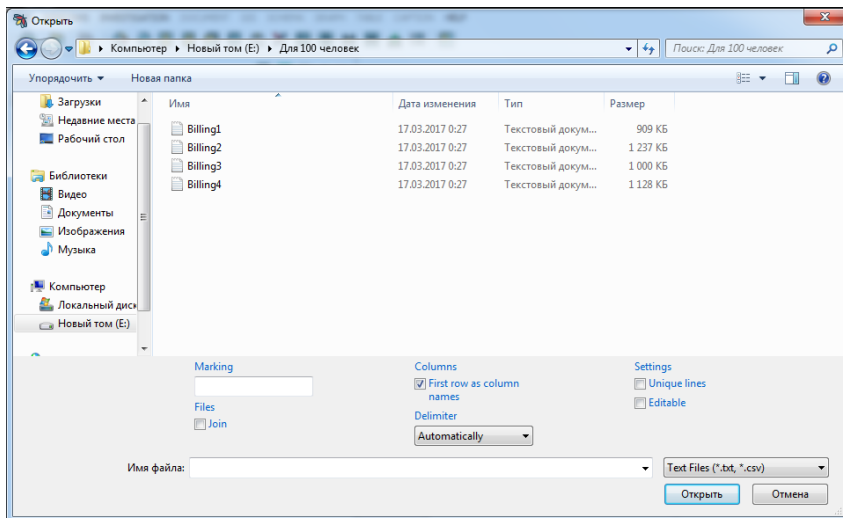


Рисунок 4 - Экран выбора анализируемого документа

В рабочей площади экрана появляется окно с массивом биллинговой информации (рис. 5).

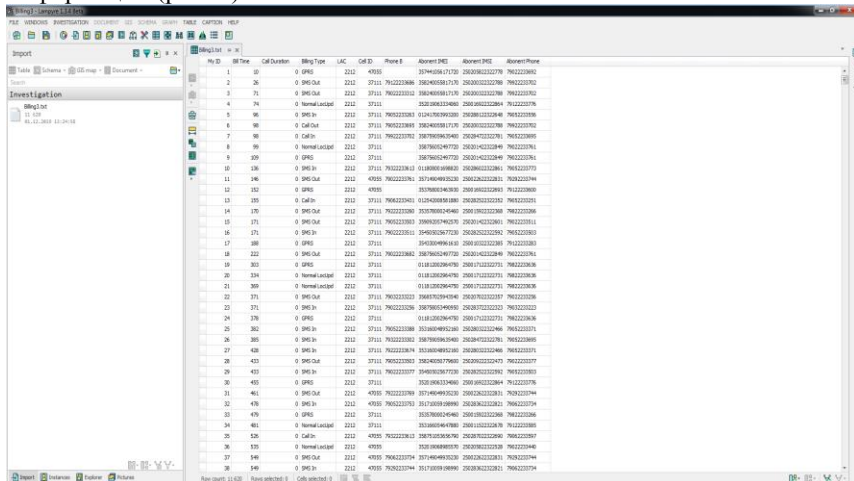


Рисунок 5 - Массив биллинговых данных в интерфейсе ИАСБ Lamprute

Биллинговые системы — автоматизированные системы расчетов, вычисляющие стоимость услуг связи для каждого клиента и хранящие информацию о тарифах и прочих стоимостных характеристиках, которые

используются телекоммуникационными операторами для выставления счетов абонентам и взаиморасчетов с другими поставщиками услуг. Выполняемые биллинговой системой операции называются биллингом, а хранимая информация — биллинговой информацией [7].

Структура массивов биллинговой информации включает в себя следующую метainформацию:

- телефонный номер абонента-источника соединения,
- телефонный номер, принимающий соединение,
- дата и время начала звонка,
- длительность звонка,
- тип соединения: звонок, SMS, USSD и т.д.

Массив биллинговой информации представляет собой упорядоченную по временной метке совокупность записей. Каждая запись (строка) является структурой данных, в которую входят 12 полей, которые могут быть как заполненными, так и пустыми. Формат рассматриваемых массивов данных имеет следующие столбцы, имеющие существенное значение для анализа:

EventId — уникальный идентификатор записи;

BillTime — время звонка с точностью до секунды;

CallDuration — длительность звонка в секундах;

BillingType — тип соединения;

LAC — Local Area Code или код локальной зоны — набора базовых станций. Состоит из 2 байт, от 0001h до FFEh. Внутри себя содержит описание одной или нескольких сот;

CellID — идентификатор соты, обслуживаемой базовой станцией. Состоит из 2 байт и может принимать любые значения в этом диапазоне. В рамках одной страны и для одного оператора связи LAC и CellID однозначно идентифицируют соту;

AbonentIMEI — IMEI абонента — серийный номер устройства;

AbonentIMSI — IMSI абонента — глобальный ID самого абонента во всех мобильных сетях;

AbonentPhone — MSISDN номер телефона — номер телефона абонента, инициировавшего соединение (MSISDN — Mobile Subscriber Integrated Services Digital Number — номер мобильного абонента цифровой сети, не содержится на SIM-карте, а сопоставлен с IMSI SIM-карты, и предназначается для передачи номера телефона назначенному абоненту и для получения звонков на телефон);

PhoneB — номер телефона, принимающего соединение.

Инструмент Content позволяет получить краткую статистику по всем данным, находящимся в массиве (рис 6).

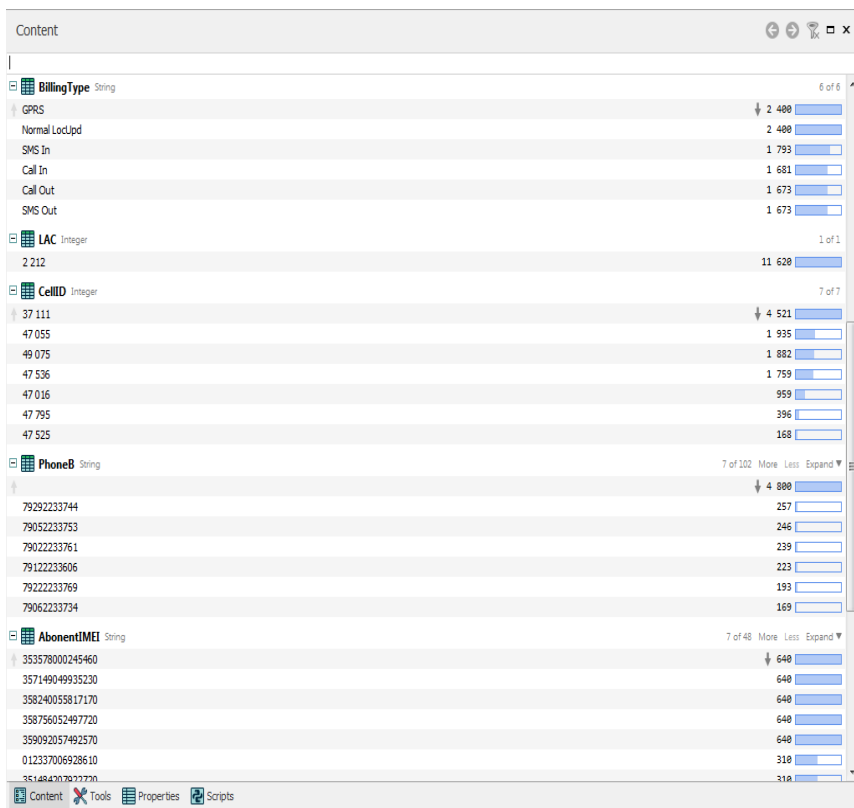


Рисунок 6 - Краткая статистика данных биллинга

Поле Billing Type показывает, что наибольшее количество событий в биллинге — это события Normal LocUpd, что вызвано регистрацией абонентских терминалов на базовой станции; все события в биллинге связаны с единственной базовой станцией 2212 (поле LAC), так как биллинг взят по данной станции, наибольшее количество взаимодействий происходит в соте 37111 (поле CellID), было зарегистрировано 4521 операций, в целом равномерно распределены входящие и исходящие звонки и SMS-сообщения.

Инструмент add mapping позволяет создавать типовые связи по двум полям массива (рис. 7). Есть возможность создания множества таких связей. Для распознавания связей между абонентами выбирается связь phone – phone.

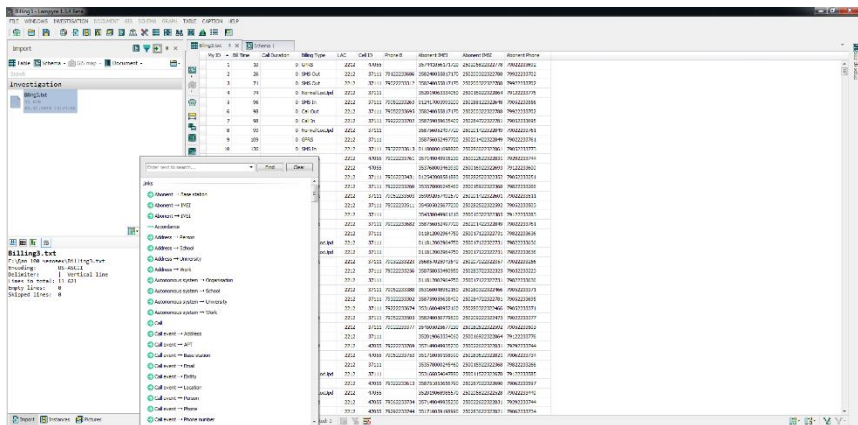


Рисунок 7 - Вызов функции add mapping

Далее откроется окно Mapping configuration, где указываются поля анализируемых данных (рис. 8). В этом случае необходимо выбрать поля AbonentPhone и PhoneB.

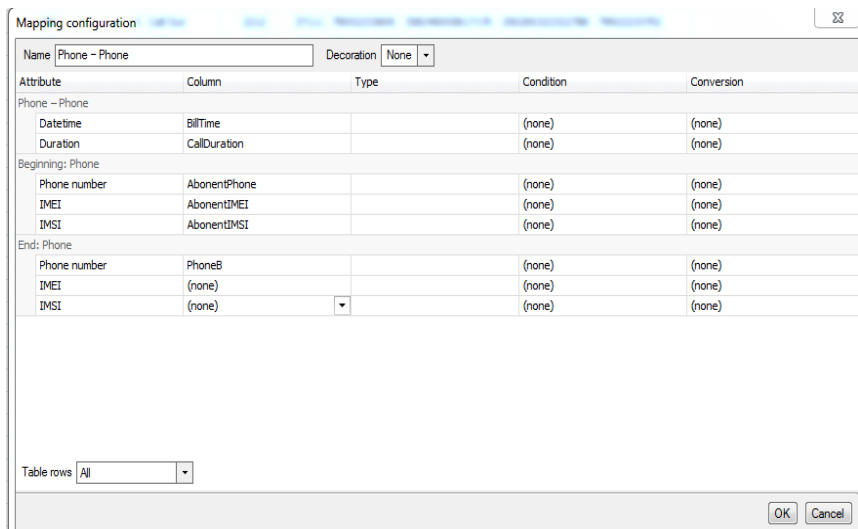


Рисунок 8 - Экран функции Mapping configuration

Для визуализации и анализа выбранных связей с помощью функции создания схем выбирается подготовленная на предыдущем этапе связь (рис. 9).

GRAPH TABLE CAPTION HELP								
Schema		Complete		Phone – Phone				
Select columns		Structure						
Phone	Call Duration	Billing Type	LAC	Cell ID	Phone B	Abor		
1	10	0 GPRS	2212	47055		3574		
2	26	0 SMS Out	2212	37111	79122233686	3582		
3	71	0 SMS Out	2212	37111	79022233312	3582		
4	74	0 Normal LocUpd	2212	37111		3520		
5	96	0 SMS In	2212	37111	79052233263	0124		
6	98	0 Call Out	2212	37111	79052233695	3582		
7	98	0 Call In	2212	37111	79922233702	3587		
8	99	0 Normal LocUpd	2212	37111		3587		

Рисунок 9 - Процесс открытия созданной схемы Phone – Phone

Далее, на вкладке Schema проецируется граф выбранных данных (рис. 10).

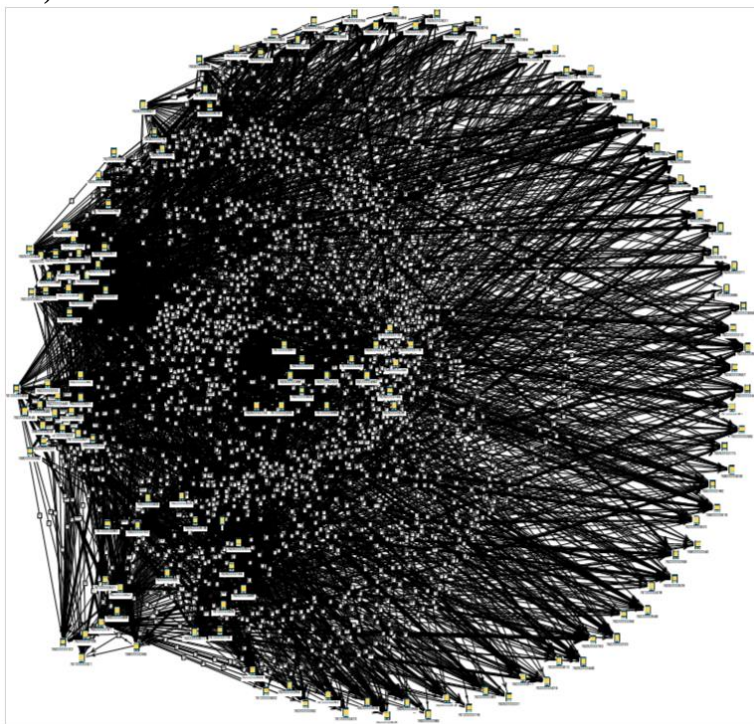


Рисунок 10 - Визуализация графа на вкладке Schema

Анализировать такой граф практически невозможно – он представляет собой «месиво» всевозможных пересечений. Для разбора необходимо осуществить выборку данных по некоторым полям исходного массива. В поле данных AbonentPhone выбирается определенный номер (в данном случае 79022233256), а в поле Billing Type – тип взаимодействия Call Out (рис.11). Далее повторяется запрос для меньшего числа записей.

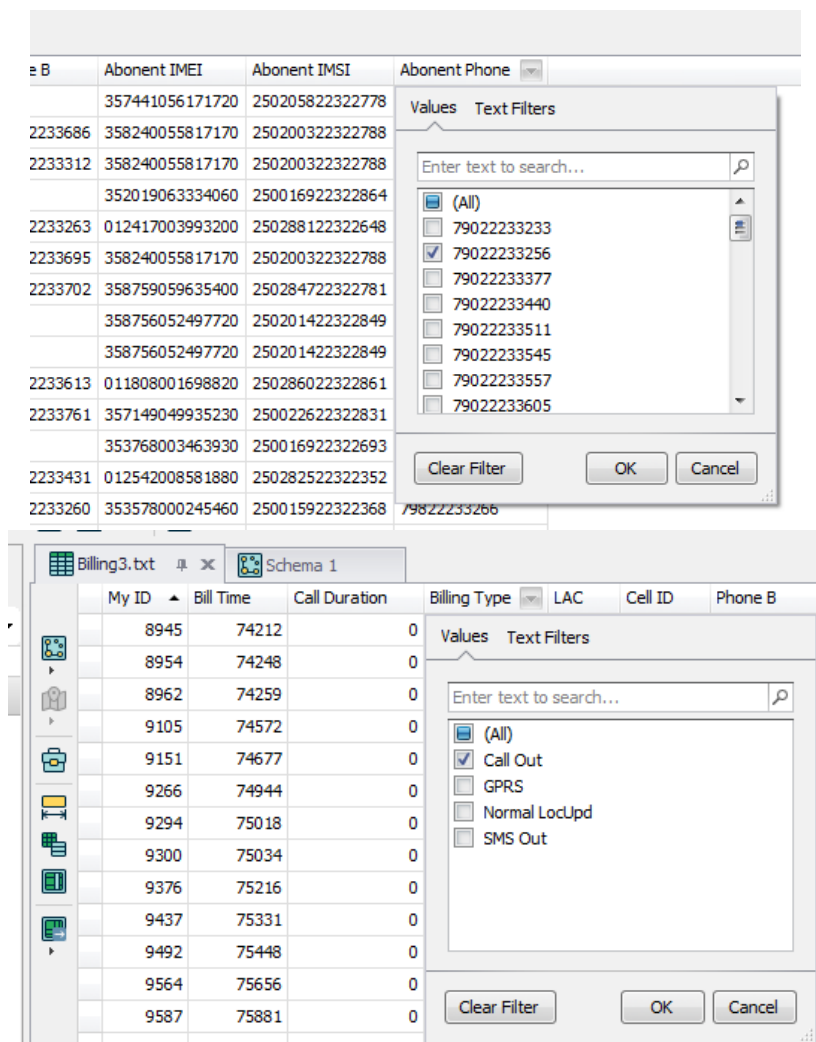


Рисунок 11 - Выбор абонента и типа соединения

Представление графов связей может быть реализовано различными раскладками [8]: древовидная, круговая, ортогональная, с учетом сил взаимодействия, доминирующая, «Forced Lin-Log».

При древовидной раскладке каждая структура содержит элемент, не имеющий вышестоящего (рис. 12). Этот элемент может считаться первым (или стартовым) узлом.

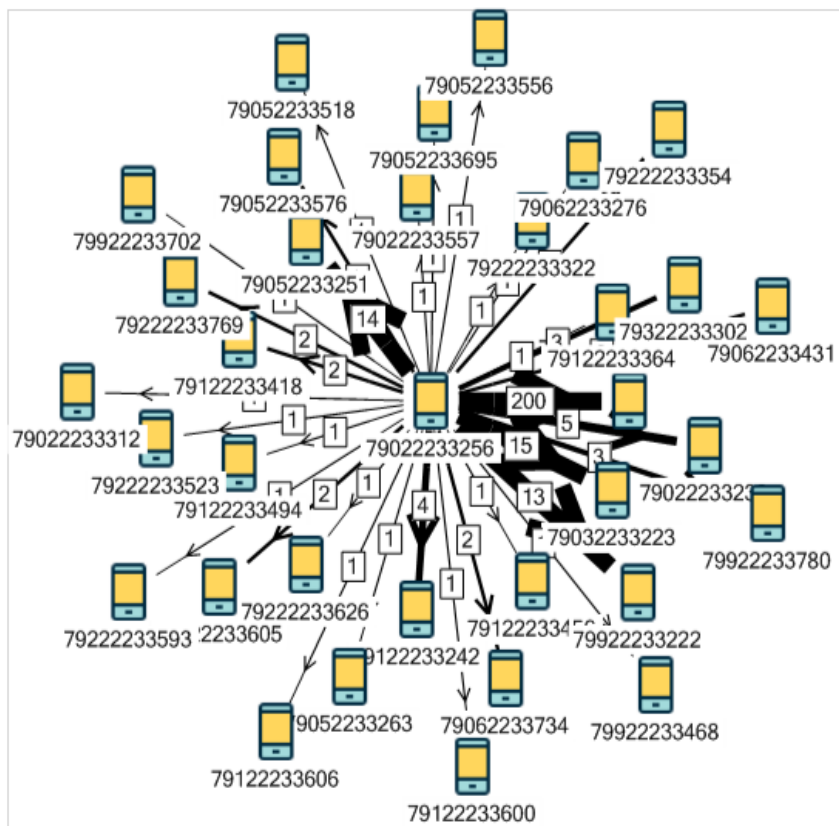


Рисунок 12 - Новый древовидный граф, описывающий звонки выбранного абонента

Круговой граф — это граф пересечений множества хорд окружности (рис. 13). То есть, это неориентированный граф, вершины которого можно отождествить с хордами окружности, и эти вершины смежны тогда и только тогда, когда соответствующие хорды пересекаются. В некоторых случаях можно использовать несколько кругов.

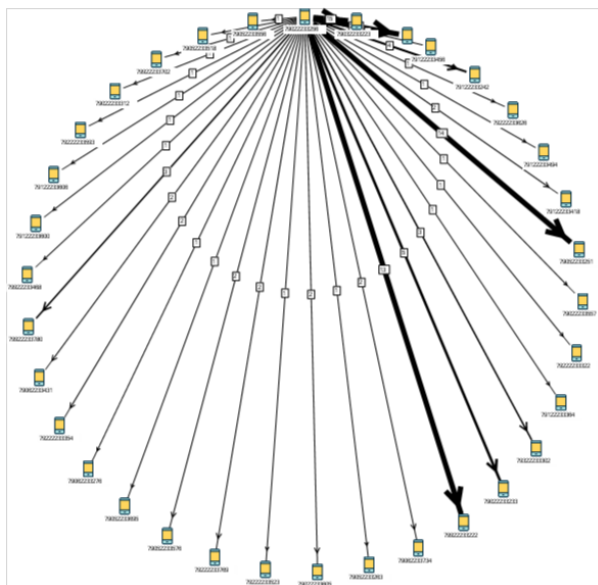


Рисунок 13 - Новый граф в форме круга

Методы ортогональной компоновки, которые позволяют краям графика проходить горизонтально или вертикально, параллельно осям координат компоновки (рис. 14).

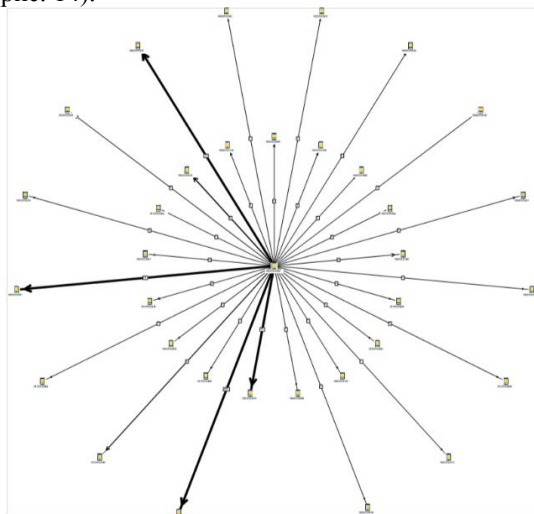


Рисунок 14 - Новый граф в ортогональной форме

Раскладка по силам взаимодействия объединяет силы притяжения между смежными вершинами с силами отталкивания между всеми парами вершин, строится схема, в которой длины ребер малы, а вершины хорошо разделены (рис. 15).

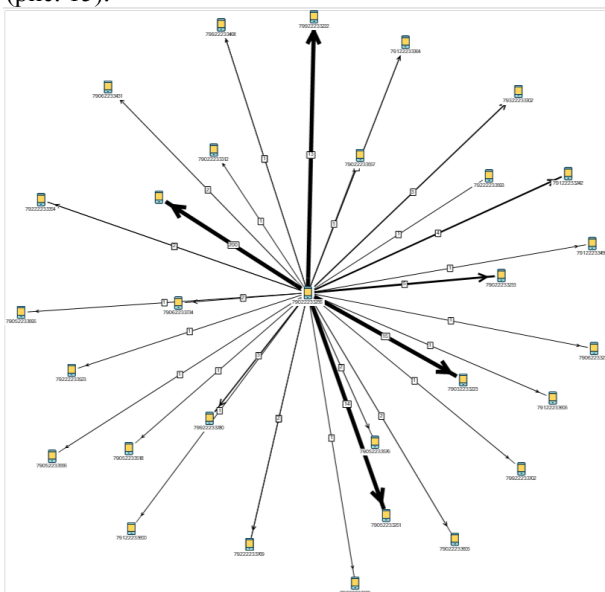


Рисунок 15 - Новый граф, расположенный по силам взаимодействия

Раскладка «доминирование» размещает вершины таким образом, что основная вершина располагается вверху (рис. 16). Таким образом, макет визуализирует отношение вершин графа.

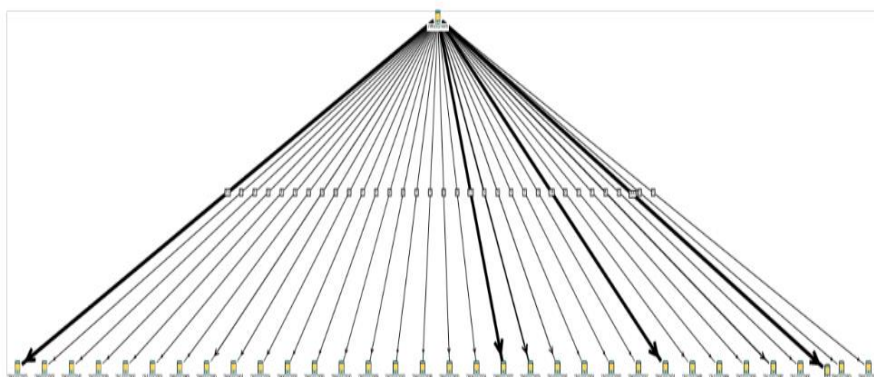


Рисунок 16 - Новый граф, расположенный в доминирующей форме

Раскладка Forced Lin-Log также учитывает силы притяжения между смежными вершинами, при этом выделяет кластеры взаимодействия (рис. 17).

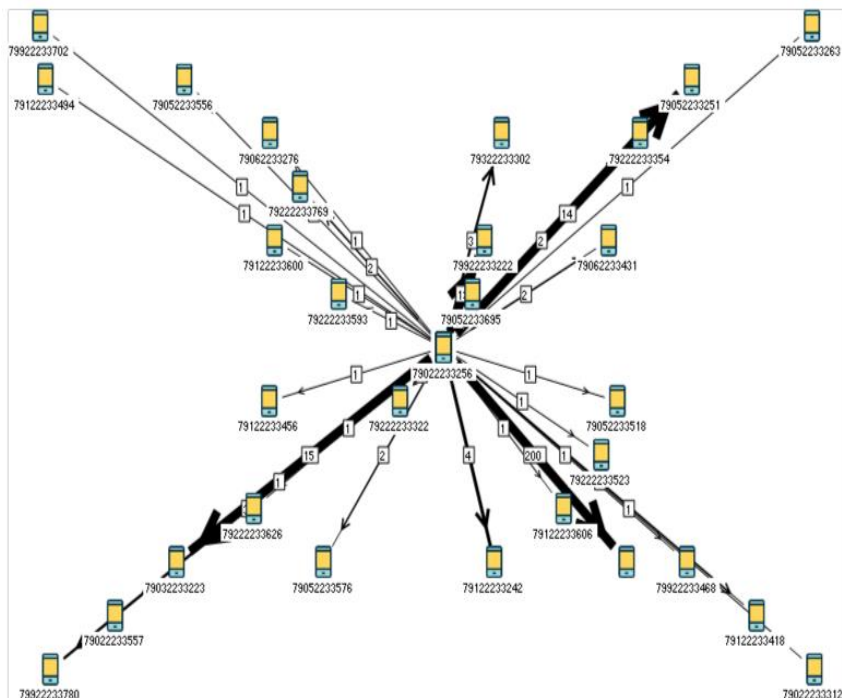


Рисунок 17 - Новый граф, расположенный в форме Forced Lin-Log

Таким образом, при проведении на потоках по направлению «Информационная безопасность» практических занятий по расследованию компьютерных инцидентов, можно использовать ИАСБ Lampruge. Данное средство позволяет имитировать различные связи между абонентами, возникающие в типовых преступных ситуациях: мошенничество, коррупция и другие преступления экономического характера. Другим достоинством использования предложенного комплекса программных средств является возможность создания и отработки типовых аналитических методик при расследовании указанных преступлений.

Список использованных источников:

1. Приказ Минобрнауки России от 26.11.2020 № 1460 "Об утверждении федерального государственного образовательного стандарта высшего

- образования - специалитет по специальности 10.05.04 Информационно-аналитические системы безопасности" (Зарегистрировано в Минюсте России 22.12.2020 N 61702) // URL: https://base.garant.ru/400105120/53f89421bbdaf741eb2d1ecc4ddb4c33/#block_1000 (дата обращения: 10.06.2021).
2. Федеральный закон № 126-ФЗ от 7 июля 2003 г. «О связи» // КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 10.06.2021).
 3. Igor Semenishchev, Alexey Sinadskiy, Mikhail Sinadskiy, Nikolay Sinadskiy, Pavel Sushkov. Method for Forming the Dynamic Components of Conditionally Real Data Arrays Based on Color Petri Net Algorithms for Organizing a Computer Training Platform for Investigating Information Security Incidents // Proceedings – 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2020. Institute of Electrical and Electronics Engineers Inc., 2020. p. 582-585.
 4. Семенищев И.А., Синадский А.Н., Синадский Н.И., Сушков П.В. Синтез массивов биллинговой информации на основе статистико-событийной модели взаимодействия абонентов сетей сотовой связи. — Вестник УрФО. Безопасность в информационной сфере. — 2018. № 1 (28). — С. 47–56.
 5. Синадский А.Н., Семенищев И.А., Синадский Н.И. Создание учебных массивов условно-реальных данных о взаимодействии пользователей сетей сотовой связи // Сборник трудов XVII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства»: в 2 томах. — Челябинск: ЧелГУ, 2018. — С. 217-223.
 6. Data analysis & OSINT tool for everyone. — URL: <https://lampyre.io> (дата обращения: 10.06.2021).
 7. Семенищев И.А., Синадский А.Н., Синадский Н.И. Алгоритм формирования массива биллинговой информации на основе статистической модели поведения абонентов сотовой связи // Сборник материалов XV Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых «Безопасность информационного пространства». — Курган: Курганский ГУ, 2016. — С. 199-203.
 8. Смирнова О.С., Шишков В.В. Графовый подход при составлении характеристики социального объекта / International Journal of Open Information Technologies ISSN: 2307-8162 vol. 5, no.6, 2017. — URL: <https://cyberleninka.ru/article/n/grafovyy-podhod-pri-sostavlenii-harakteristiki-sotsialnogo-obekta/viewer> (дата обращения: 10.06.2021).

Маркетинг страховых услуг

Е.Р. Мысева

заместитель начальника отдела правового и методического обеспечения
учебного процесса ИФТЭБ НИЯУ МИФИ, Москва

Email: ERMyseva@mephi.ru

Е. Г. Казакова

аспирант 1-го курса кафедры №75 «Финансовый мониторинг»,
ИФТЭБ НИЯУ МИФИ

Email: EGKazakova@mephi.ru

Аннотация: В данной статье рассматривается специфика маркетинга страховых услуг, основные задачи, которыми занимается служба маркетинга, и важность страхового маркетинга в современном обществе.

Ключевые слова: маркетинг, страховой маркетинг, маркетинг страховых услуг, маркетинговые исследования рынка, конкурентоспособность организации, анализ рынка.

Insurance services marketing

Abstract: in this paper we examine the specifics of insurance services marketing, main tasks of marketing service and the importance of insurance marketing in modern society.

Keywords: marketing, insurance marketing, insurance services marketing, market research, organization competitiveness, market analysis.

Страховой маркетинг — это система приемов, обеспечивающая достижение требуемой доходности страховой компании через наилучшее удовлетворение потребностей потребителя. В частности, сюда входят способы и методы убедить множество людей купить страховку. [1]

Основная задача маркетинга страховых услуг — это выполнение желаний потребителя в страховой защите. Что касается маркетинга страхования — значительное улучшение финансовых ресурсов компаний и потребителей, таким образом затрагивается ещё и сфера финансов.

Благодаря исследованию рынков происходит доскональное и глубокое изучение потенциальных потребителей, что в свою очередь ведет к созданию потребительских групп. Именно данные группы, привлекаемые

в страховую компанию, как клиенты, приносят организации наибольшую прибыль.

Специфика страховой услуги заключается в том, что она является одновременно и потребительской, и финансовой, поэтому и страховой маркетинг обладает своими отличительными чертами. Страхование является потребительским товаром из-за того, что его приобретают для непосредственного пользования и покупателями могут быть и юридические, и физические лица. Главной целью страхования является компенсация ущерба при наступлении страховых случаев.

В настоящее время в России постоянно повышается количество различных происшествий из-за возрастающего износа и нарушений условий эксплуатации разных технических объектов, нехватки требуемых мероприятий по их предупреждению и предотвращению, недостатком эффективных схем борьбы с негативными последствиями природных и техногенных катастроф. Выполняя защиту от последствий чрезвычайных ситуаций, страхование выступает в роли гарантии постоянности производства, как рыночный механизм возмещения урона. Так же страховыми компаниями создаются резервы различных предупредительных мероприятий, из которых впоследствии оплачиваются мероприятия по предотвращению страховых случаев и снижению степени риска. Помимо этого, страховая компания, заключая договор с клиентом, приобретает средства, которые могут быть вложены в развитие для получения дохода.

Вложения страховщика должны отвечать требованиям прибыльности, возвратности, диверсификации и ликвидности. В основном, как объект инвестирования компании предпочитают такие, которые могут дать уверенный доход без особого риска (например, депозиты крупных банков, государственные ценные бумаги и т. д.). Получается, что экономика государства получает постоянного инвестора со стабильным притоком долгосрочных вложений.

Страховая компания в ущерб развитию или накоплению средств тратит на выплату страховых платежей часть своего дохода. Из-за того, что в процессе страхования совершается перераспределение финансовых ресурсов, то оно является так же и финансовой услугой. Страхование небезуспешно конкурирует с прочими финансовыми услугами (например, банков и пенсионных фондов), но пока что это относится только к развитым странам.

Так как нет компенсации ущерба от страхового случая, пока он не произошёл, то потребителю может выплачиваться страховой бонус как дополнительный доход. Учитывая это, страховые компании объясняют

клиентам их потребность в страховании, проводя большую агитационную работу.

Достигается это при соблюдении ряда условий.

1. Продукт должен учитывать все нужды потребителя и обязательно быть корректным с юридической точки зрения. Продавец будет бессилён, если продукт не нужен клиенту или, если он не заинтересован в страховании.

2. Положительный имидж компании крайне необходим, если компания хочет привлекать клиентов. На потребителя и на принятие им решения о пользовании услугами компании негативно влияет недостаток информации о компании. И, наоборот, потребителем благоприятно воспринимается информация о размере уставного капитала, стабильном состоянии компании и прочее. Помимо этого, в страховой маркетинг входит разработка и внедрение страховых продуктов, изучение конкурентов, исследование нужд возможных потребностей, а также систем продажи продукции, созданием и функционированием необходимой посреднической сети и инфраструктуры.

3. Страховой компании необходимо обладать отработанной системой продаж, в основе которой находятся высококвалифицированные продавцы, которыми могут являться как штатный персонал компании, так и сторонние специалисты.

Изучение спроса на страховом рынке в первую очередь требует, чтобы в структуре страховой компании была организован отдел маркетинга, который может исследовать состав потенциальных страхователей и их потребности в страховых услугах. [2]

Если смотреть с экономической точки зрения, то в условиях малого уровня доходов затраты на страхование стоят далеко не на первом месте, т. е. спрос зависит от платёжеспособности. И, напротив, при благоприятном состоянии дел в стране доля расходов на страхование может увеличиваться.

Выделяют два вида страхового спроса: индивидуальный и корпоративный. Индивидуальный спрос — это спрос со стороны физических лиц, а корпоративный — это спрос различных предприятий и юридических лиц. В разных ситуациях одно и то же лицо может быть, как физическим, так и юридическим, так что разделение — это очень размытое. В России большая часть страхований приходится на корпоративный спрос от юридических лиц, а в странах Европы и Америки, наоборот, приходится на физические лица.

С юридической же точки зрения заключение страховых договоров может быть ограничено только право- и дееспособностью лиц. В страховании изучение потребительского спроса осуществляется с помощью, например, тестирования, опросов, исследования статистики

прибылей и убытков возможных потребителей, сбор и анализ полученной информации. Так как страховые потребности клиентов не являются наиболее важными, то задачей страхового маркетинга является не только удовлетворение, но и формирования спроса. Для того, чтобы в числе остальных доходы направлялись ещё и на страхование, следует необходимость соблюдения некоторых условий, таких как платёжеспособность, уровень экономического мышления, информированность возможного потребителя о страховании.

Существует два способа исследования конкурентной среды на рынке страховых услуг:

- 1) Используя сторонние источники информации, проанализировать текущее положение дел на рынке;
- 2) Или же обратиться к своим источникам.

Второй способ даёт возможность увидеть цельную картину именно тех направлений, которые необходимы, однако такой способ гораздо дороже. Поэтому использования обоих способов является лучшим вариантом изучения рынка.

Страховщики — это юридические лица, которые в установленном законом порядке право на осуществление страховой деятельности, и именно они могут определять предложение страховых услуг. На структуру и объём этого предложения в данный момент времени в немалой степени влияют различные факторы, например, уровень издержек или конкуренции. [3]

В страховом маркетинге, равно как и в прочих областях, существует два основных вида конкуренции: неценовая (более выгодные условия) и ценовой (более низкие цены).

Основные факторы неценовой конкуренции это:

- количество компаний на рынке (прямая зависимость);
- среднее значение ставок комиссионных вознаграждений и расходов (обратная зависимость);
- степень риска (обратная зависимость);
- доходность инвестиций страховых компаний
- положение дел на рынке и его структура;
- Прибыльность/убыточность страховых операций;
- налогообложение страховых организаций;
- Ценовая конкуренция (т. е. снижение стоимости услуг страхования) может реализовываться за счет нормы прибыли и расходов страховщика.

В случае, если страховщик является крупной компанией с уверенной позицией на рынке, то средством снижения тарифов может служить нетто-ставка. В противном же случае, если компания достаточно небольшая, то

снижение нетто-ставки с целью, например, захвата рынка может стать причиной невыполнения своих обязательств и, как следствие, банкротства.

Спрос на услуги страхования тем выше, чем качественней сервис у данной страховой компании, поэтому обслуживание потребителей — это одна из важнейших частей удовлетворения интересов страхования. Но улучшение качества сервисного обслуживания, что закономерно, вызывает повышения уровня затрат, соответственно, страховой компании следует найти наиболее оптимальное для себя отношение экономических факторов страхового обслуживания к, собственно, самому уровню сервиса.

Главной задачей отдела страхового маркетинга компании является выявление различных закономерностей между спросом на услуги страхования и экономическими факторами обслуживания клиентов, где отсутствие жалоб на качество обслуживания со стороны клиентов и есть основной показатель качества сервисного обслуживания.

Остальные же задачи отдела маркетинга страховой компании выглядят следующим образом:

- исследование рынка страховщика;
- исследование вероятных потребителей;
- анализ мотивации возможного потребителя во время подписания договора страхования;
- изучение рекламной деятельности;
- изучение предоставляемого вида страховых услуг;
- исследование различных способов продвижения страховых услуг от страховой компании к вероятному потребителю и установление наиболее эффективных;
- анализ конкуренции, определение её уровня и форм.

Исследование рынка страховщика необходимо для определения возможной емкости рынка на разные услуги страхования по нескольким похожим видам страхования. Конечными результатами исследования является определение страховщиком наиболее выгодных регионов для предоставления различных видов страхования. Следуя из вышенаписанного, становится очевидным тот факт, что полученные результаты исследования рынка будут напрямую связаны с платежеспособностью населения, а также его спросом на различные виды страхования. В случае игнорирования данных вопросов страховой компанией, это может привести к потере рынка, что повлечет немедленное банкротство.

На сегодняшний день опыт развитых стран представляет большое количество методов исследования причин выбора потенциальных клиентов и их реакции на различные продукты страховой компании. Зарубежные страховые компании активно применяют в своей

маркетинговой практике совокупность разнообразных анкет, тестирований и опросов, которые помогают изучить мотивы будущих потребителей с разными социальными статусами. Грамотное и своевременное применение полученных данных при исследовании причин выбора клиентами того или иного продукта, может позволить страховщику правильно реагировать на различные ситуации, которые могут сложиться на рынке страховых услуг.

Изучение предоставляемого вида страховых услуг предоставляет организации сведения о пожеланиях клиента, исходя из условий договора. Также следует отметить тот факт, что именно страховщик отвечает за реализацию рекламы, на кого ее стоит ориентировать, каким способом следует представлять страховые продукты потенциальным клиентам. Опыт страховых компаний развитых стран рекомендует следовать такому правилу: страховой договор необходимо предоставить там, где он нужнее всего возможному клиенту и где он с большей вероятностью подпишет его.

Для полноценного изучения конкуренции следует определить основных конкурентов на рынке, выявить их сильные и слабые стороны, провести анализ всей деятельности, конкурирующей организаций, а именно: изучить продукцию на рынке, стоимость товаров и услуг, проанализировать положение организации на рынке и т. д.

Существует два основных вида конкуренции в сфере страховых услуг. Это конкуренция неценовая и ценовая.

Неценовая конкуренция в первую очередь повышает уровень сервисных услуг страховых компаний, которые они оказывают своим потребителям (бесплатные юридические консультации, приоритетные права при покупке и тому подобное). Реклама, особенно в настоящее время, когда её роль увеличилась во много раз, всегда была основным приёмом неценовой конкуренции. При помощи как раз рекламы страховщики стараются создать положительный имидж компании в сознании потребителей.

Отличие же ценовой конкуренции заключается в том, что она основана на тарифной ставке. Самым популярным методом выделиться на рынке и привлечь наибольшее количество потребителей является понижение тарифной ставки. Ценовая конкуренция — это орудие в первую очередь небольших страховых компаний, так как они не могут тягаться с крупными компаниями рынка страховых услуг в сфере неценовой конкуренции из-за отсутствия возможностей. [4]

Исходя из вышенаписанного можно сделать вывод, что страховой маркетинг не станет эффективным и прибыльным до тех пор, пока не будет опираться на глубокий анализ потенциальных и уже имеющих клиентов. Иными словами, маркетинг в страховании по большей части — это анализ доходности рынков и последующий их захват и удержание.

Список использованных источников:

1. Маркетинг: общий курс. Учеб. Пособие, 5-е издание. *Калюжной Н.Я., Якобсон А.Я.* ISBN:978-5-370-01493-2 476 Москва: *Омега-Л*, 2010
2. Шамаева А. Психологические аспекты в страховом маркетинге: практическое пособие / А. Шамаева. – Москва: Лаборатория книги, 2010. – 53 с.
3. Проблемы финансов, кредита и бухгалтерского учета в условиях реформирования экономики. Материалы студенческой международной научно-практической конференции. Под редакцией проф. В. А. Федорова, проф. Е. А. Карловской. 2015 Издательство: Тихоокеанский государственный университет (Хабаровск)
4. Особенности конкуренции в страховом предпринимательстве Шишликов А.А. Вестник Московской академия предпринимательства (Москва) ISSN: 2073-9621, 2011
5. Принципы и задачи маркетинга в страховой деятельности. Велиметров Р.Ш. Транспортное дело России Учредители: ООО "Редакция газеты "Морские вести России" (Москва) ISSN: 2072-8689, 2009
6. Практикум по страховому маркетингу / О. В. Козьменко, В. С. Лысенко. – Издательство Сумы: Университетская книга, 2014. – 224 с.

УДК 340:629.3

© Е.Ю. Хромова, 2021

Проблемы правового регулирования использования персонального электротранспорта

Е.Ю. Хромова

к.ю.н., доцент Москва

Email: predstavitelskaya@mail.ru

Аннотация: *Статья посвящена проблемам законодательного урегулирования особенностей использования электротехнических индивидуальных средств передвижения: электровелосипедов, электросамокатов, сегвеев, гироскутеров, моноколес, а также предлагаемым способам решения актуальных в данной сфере вопросов.*

Ключевые слова: *электровелосипед, электросамокат, сегвей, гироскутер, моноколесо, средство индивидуальной мобильности, электротранспорт.*

Problems of legal regulation of the use of personal electric transport

Abstract: The article is devoted to the problems of legislative regulation of the peculiarities of the use of electrotechnical individual vehicles.

Keywords: electric bike, electric scooter, segway, hoverboard, unicycle, personal mobility, electric vehicles.

Использование персональных самобалансирующих электротранспортных средств в крупнейших отечественных городах постоянно растет, и вопросы регулирования использования этих средств передвижения становится весьма актуальным. Рассматривая положения о необходимости правового регулирования использования электросамокатов, гироскутеров, моноколес, сегвеев и иных самобалансирующих средств индивидуальной мобильности (здесь и далее - СИМ) становится очевидным, что безопасность пешеходов наравне с лицами, управляющими вышеуказанной моторной техникой на электрической тяге перейдет в категорию законодательно допустимой только после внесения изменений в Правила дорожного движения и Кодекс Российской Федерации об административных правонарушениях, законы об административных правонарушениях субъектов и муниципальных образований РФ.

На современном этапе развития мировой законодательной практики не наблюдается единства в подходах к регулированию использования физическими лицами средств индивидуальной мобильности. Средство передвижения - портативный электротранспорт - во многих странах технически незаконен [с. 28, 15]. Так, они полностью запрещены как на дорогах, так и на тротуарах в Джакарте, Сингапуре и Шанхае [8]. Во Франции существует частичное ограничение на использование СИМ - там недопустима езда по тротуару, за исключением специально отведенных мест [с.15,13]. Пользователям при управлении СИМ запрещается надевать наушники, а максимальная скорость не может превышать 25 км/ч [7].

В российском законодательстве специальные понятия и нормы, устанавливающие требования к лицам, использующим сегвеи, гироскутеры, моноколеса, электрические самокаты, отсутствуют.

Однако, уже получил широкое развитие новый термин - кикшеринг, который представляет собой услугу по предоставлению самокатов в краткосрочную аренду. Данное средство передвижения является экологичным и удобным, но его использование возможно лишь в теплое время года для преодоления коротких расстояний.

Исходя из вышеописанного, ярко обозначается необходимость подробного рассмотрения нескольких самостоятельных вопросов.

Во-первых, подлежит правовому урегулированию возможность использования средств индивидуальной мобильности на электротяге

(портативного электротранспорта) на дорогах общего пользования, тротуарах и пешеходных дорожках [6].

Во-вторых, необходимо законодательно, на различных уровнях правотворческого процесса, установить особенности эксплуатации вышеуказанных электромоторных устройств на городских улицах, тротуарах, в парках, скверах и иных публичных местах с одновременной высокой плотностью пешеходов. Требуется внесение соответствующих изменений в федеральные нормативные акты, в том числе и в Правила дорожного движения РФ.

Перевозка электромоторного средства индивидуальной мобильности [с.34, 12] выступает третьим вопросом, требующим незамедлительного нормативного реагирования. Способы перевозки в общественном транспорте до сих пор остаются архаичными и небезопасными в силу большого веса указанных транспортных средств и их габаритов [11]. Вес СИМ влечет опасность для жизни и здоровья его владельца (арендатора), поскольку перемещение с электровелосипедом, сегвеем или электросамокатом в общественном городском транспорте, в том числе рельсовом наземном и подземном, предполагает подъем электрического транспортного средства на определенный уровень высоты с целью перемещения его с тротуара (дороги) в салон единицы общественного транспорта. Такое перемещение сопряжено с применением физической мускульной силы человека - владельца данного СИМ, наличием у него навыков и умений перемещения таких грузов в пространстве, отсутствием хронических заболеваний, которые бы не позволили ему перемещать данный электротранспорт, а также хорошее самочувствие владельца или арендатора СИМ на момент подъема и перемещения в общественный транспорт, внутри него (размещение в салоне наземного городского транспорта), перемещение в подземном городском транспорте, в том числе подземных пешеходных переходах, ступенях, подвижных частях эскалаторов, а также при выходе из него.

В четвертых, существует острая необходимость в правовых нормах, определяющих порядок и правила хранения электротранспорта в жилых помещениях: в комнатах и квартирах собственников средств индивидуальной мобильности, жилых домах частного сектора (городских и сельских поселений, дачных товариществ и др.), местах общего пользования в многоэтажных жилых домах: на межквартирных лестничных площадках, в общих коридорах, в лифтовых холлах, чердаках, тамбурах, подвальных помещениях, лоджиях, балконах и т.д. Данное положение вызвано неоднократными случаями возгорания электросамокатов, электровелосипедов и электромопедов в жилых домах

с серьезными последствиями для вышеназванных помещений и их владельцев.

Наконец, в настоящее время на законодательном уровне не закреплена и не раскрыта классификация электротранспортных средств индивидуальной мобильности, не определены категории участников движения, к которым можно приравнять вышеуказанный транспорт.

Таким образом, рассматривая понятие электротранспорта как средства индивидуальной мобильности, следует подробнее разобраться с понятиями, уже содержащимися в действующем федеральном законодательстве и соотнести с ним технические характеристики рассматриваемых СИМ для определения категорий участников движения на электротранспорте.

В соответствии с Правилами дорожного движения механическое транспортное средство представляет собой транспортное средство, приводимое в движение двигателем. Законодатель распространяет данное понятие и на любые самоходные машины.

По действующему федеральному законодательству, лица, использующие СИМ, являются пешеходами [с.6, 16]. Так, в Правилах дорожного движения (здесь и далее - ПДД) пешеходом является лицо, находящееся вне транспортного средства на дороге либо на пешеходной или велопешеходной дорожке и не производящее на них работу. К пешеходам приравниваются лица, ведущие велосипед, мопед, мотоцикл, а также использующие для передвижения роликовые коньки, самокаты и иные аналогичные средства [п.1,4]. Возникает вопрос, также требующий правового регулирования: термин «ведущий» транспортное средство в новой, действующей реальности предполагает, что владелец или арендатор велосипеда или самоката, перемещаясь рядом с ним, везет его по территории пешеходной зоны или указанное лицо использует его как средство для ускоренного передвижения, находясь на нем, приводя его в движение с помощью собственной физической мускульной силы и управляя рулевым узлом? В первом случае представляется уместным использование понятия «пешеход» для лица, идущего рядом с механическим агрегатом. В ключе понимания термина «пешеход» как лица, использующего по назначению транспортное средство индивидуальной мобильности для ускорения своего перемещения может быть отнесено лишь к владельцам агрегатов и приспособлений, не имеющих мотора. К лицам, управляющим транспортными средствами индивидуальной мобильности на электротяге понятие «пешеход» применимо быть не может, поскольку в крупных отечественных мегаполисах известны случаи наезда водителями электросамокатов и электровелосипедов на пешеходов, которые при таких столкновениях

получали тяжкий вред здоровью. К настоящему времени ответственность для водителей гироскутеров, электросамокатов и сегвеев не предусмотрена, поскольку они приравниваются к пешеходам. Данное положение недопустимо, поскольку некоторые электросамокаты способны развивать скорость до 85-100 км/ч. В такой ситуации право физических лиц-пешеходов на свободное передвижение нарушается путем поставления в опасность самого передвижения участников движения по специально отведенным для пешего перемещения местам - паркам, скверам, общественным пространствам, тротуарам.

Мопед - это двухколесное механическое транспортное средство, максимальная конструктивная скорость которого не превышает 50 км/ч, имеющее электродвигатель номинальной максимальной мощностью в режиме длительной нагрузки более 0,25 кВт и менее 4 кВт⁴. По тексту данного определения очевидно, что мопед имеет один, в свете рассматриваемой статьи электрический, двигатель. Однако, на электросамокатах, которые по настоящее время передвигаются по пешеходным зонам, возможно наличие и двух электромоторов, в сумме дающих 1600-5400 Вт., если одного двигателя недостаточно. Указанная высокая мощность ощущается сразу на старте, что является небезопасным как для пешеходов, так и для водителей электротранспорта.

Следует отметить, что вес электросамоката составляет 35-45 кг, сегвея - 30-35 кг, электровелосипеда - до 120 кг, а максимальная скорость - 100 км/ч, 30 км/ч и 90 км/ч соответственно. Таким образом, скоростной электровелосипед с мотором мощностью более 250 Вт и до 4000 Вт по действующему российскому законодательству соответствует мопеду [10], требует регистрации в ГИБДД и наличия водительских прав категории «М» или выше [14]. При отсутствии водительского удостоверения на право управления транспортным средством и регистрации такого транспортного средства допускается езда только на электровелосипедах с двигателем на 250 Вт, приравниваемых к безмоторным велосипедам. Принимая во внимание массу самокатов, составляющих 5-12 кг, снабженных рулевым механизмом и приводимых в движение мускульной силой человека, становится очевидной недопустимость эксплуатации вышеописанных электротранспортных средств индивидуальной мобильности на территориях пешеходных зон. Электросамокат и электровелосипед при чрезвычайно высоких указанных мощностях, весе и развиваемых скоростях необходимо законодательно приравнивать к мопедам, обязать владельцев и арендаторов указанных транспортных средств регистрировать их в ГИБДД [п.3,5] и получать водительские права, поскольку отнесение сложных технических механизмов не допустимо к разряду портативных.

На основании изложенного автором настоящей статьи предлагается приравнять транспорт на электротяге как средство индивидуальной мобильности к определениям «пешеход», «велосипед» и «мопед» в зависимости от конструктивной скорости движения, веса транспортного средства и его мощности.

Конечной целью выделения вышеуказанных категорий является развитие инфраструктуры для электрических транспортных средств индивидуальной мобильности: строительство отдельных безопасных зон для движения, разделение пешеходных потоков и путей для электротранспорта с движением на таких средствах только по специально выделенным полосам, запрет предоставления в аренду электромеханических транспортных средств индивидуальной мобильности в не оборудованных для целей безопасного использования парках, а также предусмотреть возможность страхования гражданской ответственности. Безусловно, необходимым является создание правовой базы, определяющей преимущество в движении пешеходов перед лицами, использующими персональный транспорт на электротяге, в том числе особый режим эксплуатации электротранспортных средств индивидуальной мобильности [ст.264, 2]. Необходима классификация данных устройств, определяющая их как механические транспортные средства, признаваемые источником повышенной опасности, что позволит на законодательном уровне гарантировать пешеходам получение дополнительной правовой защиты.

Список использованных источников:

1. Конституция Российской Федерации: принята всенар. голосованием 12 дек. 1993 г. [с учетом поправок, внесенных Законами Рос. Федерации о поправках к Конституции Рос. Федерации от 30 дек. 2008 г. № 6-ФКЗ, от 30 дек. 2008 г. № 7-ФКЗ, от 5 февр. 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ] // Собрание законодательства Российской Федерации. - 2014. - № 31. - Ст. 4398.
2. Уголовный кодекс Российской Федерации: Федер. закон от 13 июня 1996 г. № 63-ФЗ; принят Гос. Думой 24 мая 1996 г.: одобрен Советом Федерации 5 июня 1996 г.: [в ред. от 2 авг. 2019 г.] // Официальный интернет-портал правовой информации: гос. система правовой информации.
3. Кодекс Российской Федерации об административных правонарушениях: Федер. закон от 30 дек. 2001 г. № 195-ФЗ; принят Гос. Думой 20 дек. 2001 г.: одобрен Советом Федерации 26 дек. 2001 г.: [ред. от 2 авг. 2019 г.] // Собрание законодательства Российской Федерации. - 2002. - № 1, ч. 1. - Ст. 1.

4. Правила Дорожного Движения Российской Федерации: Постановление Правительства РФ от 23.10.1993 № 1090 (ред. от 31.12.2020) «О Правилах дорожного движения» (вместе с «Основными положениями по допуску транспортных средств к эксплуатации и обязанности должностных лиц по обеспечению безопасности дорожного движения») (с изм. и доп., вступ. в силу с 01.03.2021).
5. Постановление Правительства РФ от 21.12.2019 № 1764 «О государственной регистрации транспортных средств в регистрационных подразделениях Государственной инспекции безопасности дорожного движения Министерства внутренних дел Российской Федерации» (вместе с «Правилами государственной регистрации транспортных средств в регистрационных подразделениях Государственной инспекции безопасности дорожного движения Министерства внутренних дел Российской Федерации»).
6. Бадагуев Б.Т. Безопасность дорожного движения: Приказы, инструкции, журналы, положения / Б.Т. Бадагуев - М.: Альфа-Пресс, 2017.
7. Бадагуев Б.Т. Эксплуатация транспортных средств (организация и безопасность движения) / Б.Т. Бадагуев. - М.: Альфа-Пресс, 2018.
8. Бершадский В.Ф. Основы управления механическими транспортными средствами и безопасность движения: Учебник / В.Ф. Бершадский, Н.И. Дудко, В.И. Дудко... - Мн.: Амалфея, 2018.
9. Блинкин М.Я. Безопасность дорожного движения: история вопроса, международный опыт, базовые институты / М.Я. Блинкин. — М.: ИД ВШЭ, 2018.
10. Волков В.С. Основы расчета систем автомобилей, обеспечивающих безопасность движения: Учебное пособие/В.С. Волков - СПб.: Лань, 2015.
11. Горев А.Э. Организация автомобильных перевозок и безопасность движения: Учебное пособие для студ. высш. проф. образования / А.Э. Горев, Е.М. Олещенко. — М.: ИЦ Академия, 2018.
12. Коноплянко В.И. Организация и безопасность дорожного движения. / В.И. Коноплянко. — М.: Высшая школа, 2017.
13. Ксенофонтов И.В. Основы управления мотоциклом и безопасность движения: Учебник / И.В. Ксенофонтов. — М.: Academia, 2018.
14. Майборода, О.В. Основы управления автомобилем и безопасность движения. Учебник водителя транспортных средств категорий С, D, E / О.В. Майборода. — М.: Академия, 2019.
15. Пятницкий Л.Н. Безопасность дорожного движения глазами физика / Л.Н. Пятницкий. — М.: КД Либроком, 2019.
16. Что должны знать дети о правилах дорожного движения. Дорожная безопасность. Памятка (комплект из 200 буклетов). - М.: Учитель, 2017.

Реинжиниринг бизнес-процессов предприятия, как инструмент выживания в конкурентной среде

А.Н. Норкина

к.э.н., доцент кафедры финансового мониторинга ИФТЭБ НИЯУ МИФИ, Москва

Email: ANNorkina@mephi.ru

Е.Р. Мысева

заместитель начальника отдела правового и методического обеспечения учебного процесса ИФТЭБ НИЯУ МИФИ, Москва

Email: ERMyseva@mephi.ru

Аннотация: В данной работе был проведен анализ актуальных методов и понятия реинжиниринга бизнес-процессов, проанализирована важность применения реинжиниринга бизнес-процессов для повышения конкурентоспособности предприятия в современных условиях, а также детализирована суть реинжиниринга бизнес-процессов на основе последних научных работ в этой области.

Ключевые слова: реинжиниринг, реинжиниринг бизнес-процессов, бизнес-процесс, управление, инновации.

Enterprise business processes reengineering as a survival tool in competitive enviroment

Abstract: In this paper we held analysis of latest concepts and methods in the field of business process reengineering (BPR), the importance of BPR for increasing the competitiveness of an enterprise. Additionally, the essence of BPR is detailed based on current studies in this field.

Keywords: reengineering, BPR, business process, management, innovation.

При возникновении кризисных явлений в экономике предприятиям необходимо использование радикальных инструментов менеджмента. Предприятие, которое стремится выжить на рынке или же улучшить свою конкурентоспособность и положение, должно постоянно совершенствовать свои технологии производства. Существует множество методов, с помощью которых компания может делать свою работу более результативной. Реинжиниринг бизнес-процессов по праву можно отнести к одному из наиболее эффективных и действенных подходов повышения

уровня результативности деятельности организации, а также улучшения качества самой работы.

Реинжиниринг бизнес-процессов это не просто изменение порядка работы предприятия, это глобальное, фундаментальное и доскональное переосмысление рабочих процессов в организации, которые повлекут за собой улучшения показателей компании по всем направлениям и напрямую затронут наиболее важные показатели деятельности компании, а именно клиентоориентированность, качество товара, сервис, цены и другое.

Данные показатели полностью отражают основные цели реинжиниринга:

1. Обслуживание клиентов на высоком уровне (качество, сервис)
2. Повышение эффективности работы на всем предприятии (темпы, стоимость)

В конечном счете реинжиниринг направлен на улучшение данных показателей предприятия, которые в свою очередь обеспечивают повышение конкурентоспособности предприятия в условиях быстрых изменений на рынках сбыта и в потребностях покупателей (клиентов). [1]

Реинжиниринг можно выделить в группу одних из важных и основным приемов, существующих в инновационном менеджменте, именно реинжиниринг напрямую связан с инновационными процессами. Стоит отметить, что он направлен не только на улучшение качества работы конкретной организации или на производство какой-то новой продукции, но и на реализацию и продвижение предлагаемых товаров и услуг. Перед внедрением реинжиниринга бизнес-процессов на предприятии или же в какую-то компанию надо четко понимать, что конечной целью реинжиниринга являются нововведения в организации, которые в свою очередь укрепят позиции на рынке и позволят выдержать высокую конкуренцию. Другими словами, реинжиниринг можно с уверенностью называть инновацией.

Исходя из вышенаписанного можно сделать вывод, что реинжиниринг – это своего рода услуги, которые становятся необходимы любому предприятию для внутренней перестройки своей трудовой деятельности. Американский ученый М.Хаммер долгое время занимался вопросами реинжиниринга и дал ему следующее определение, которое состоит из четырех слов: «фундаментальный», «радикальный», «резкий» («скачкообразный») и «процесс». [2]

Обычно выделяется три типа предприятий, которым необходимо и целесообразно провести реинжиниринг:

1. Предприятия (компании), которые находятся в состоянии глубокого кризиса. Это связано с тем, что цены на товары и услуги,

оказываемые предприятием, значительно выше, чем у основных конкурентов, но при этом качество и сервис значительно хуже. У компаний такого типа нет выбора, т. е. им необходимо срочно провести реинжиниринг или же решиться на другие шаги по улучшению своего состояния на рынке. Если же руководство компании не решится на какие-то крайние меры по выходу из кризисного положения, то этой компании (предприятию) грозит неминуемое разорение.

2. Предприятия (компании) чье положение на рынке является удовлетворительным. Часто у такого типа компаний дела идут неплохо, но их дальнейшая деятельность находится под угрозой. Это связано с тем, что на рынке появляются новые конкуренты, изменяются требования к продукции у покупателей (клиентов), меняется экономическое окружение и т. п.

3. Предприятия (компании), у которых нет никаких проблем в настоящем и не предвидятся проблемы в ближайшем будущем. Данный тип компаний – это компании, занимающие лидирующие места на рынке. Реинжиниринг необходим и для того, чтобы опережать конкурентов по всем направлениям деятельности и создавать уникальные конкурентные преимущества.

Бизнес-процесс – это цепь логически связанных, повторяющихся действий, в результате которых используются ресурсы предприятия для переработки объекта (физически или виртуально) с целью достижения определенных измеримых результатов или продукции для удовлетворения внутренних или внешних потребителей.

Во время структуризации компании или же предприятия, вся деятельность данной компании рассматривается, как набор бизнес-процессов. Бизнес-процессы принято делить на четыре большие группы:

- Основные бизнес-процессы – генерируют доходы компании;
- Обеспечивающие бизнес-процессы – поддерживают инфраструктуру компании,
- Бизнес-процессы управления – управляют компанией,
- Бизнес-процессы развития – развивают компанию.

Классификация такого типа удобна в использовании менеджерами компании, т. к. помогает визуализировать деятельность компании, что в свою очередь способствует эффективному управлению данной компании.

Группа «Основные бизнес-процессы» приносит предприятию прибыль и является центром прибыли.

Группа «Обеспечивающие бизнес-процессы» поддерживают основные бизнес-процессы и процессы развития, создают инфраструктуру предприятия.

Группа «Бизнес-процессы управления» является управленческой группой, которая обеспечивает управление другими группами.

Группа «Бизнес-процессы развития» основной целью данной группы является обеспечить компании выживаемость на рынке товаров (услуг) в связи с ожесточенной конкуренцией и обеспечить прирост прибыли в долгосрочной перспективе развития компании. Данную группу часто называют центром-инвестиций.

Следует отметить, что во многих случаях бизнес-процессы развития часто являются бизнес-проектами, которые в свою очередь состоят хоть и из разовых, но уникальных и повторяющихся мероприятий, направленных на проведение автоматизации, реструктуризации, реализации новых товаров на рынок, модернизации ассортиментной политики предприятия и иных проектов, которые являются неотъемлемой частью стратегического развития любого предприятия.

Если основываться на работах М.Хаммера и Дж.Чампи, то они утверждают, что реинжиниринг бизнес-процессов является переосмыслением и реконструкцией бизнес-процессов, направленных на достижение максимальных улучшений в современных условиях критериях производительности, таких как качество, скорость, услуги, стоимость.

Во время реализации проекта реинжиниринга следует отметить наиболее значимую из проблем – проблему конфликта в различных проявлениях, а именно: внутриорганизационный конфликт, конфликт целей и задач, конфликт разрабатываемой структуры и так далее. Успех и положительный результат проекта во многом зависит от подхода к реинжинирингу, выбранного компанией, и способов разрешения проблемы конфликта. Далее представлены основные подходы проведения реинжиниринга. Несмотря на огромное количество подходов, которые используются на практике, принято выделять три основные:

- «Zero-approach» основывается на разработке бизнес-модели организации с нуля или же с чистого листа. В основе подхода лежит представление построения идеального образа организации, который основывается на практических и теоретических представлениях, а также субъективных ожиданий ответственных лиц, проводящих реинжиниринг.

- «Подход на основе решений» основывается на построении бизнес-модели на основе моделирования системы принимаемых управленческих решений с постоянным совершенствованием, отладкой и построением других бизнес-процессов, которые основываются на оптимальной системе принятия решений;

- «Детальный анализ». Главная идея данного подхода заключается в том, что в нем полностью отражается сегодняшнее положение организации и будущее построение модели бизнес-процессов. В данном подходе

проводится глубокий анализ ключевых проблем и достижений организации, создается детальное описание деятельности организации, что в дальнейшем позволяет осуществлять построение процессов, основываясь на прежнем опыте компании. [3][4]

Суть реинжиниринга бизнес-процессов заключается в тотальной (или, как отмечено некоторыми авторами «радикальной» [5][6]) перестройке всей структуры организации именно за счет данных изменений организация может значительно изменить и повысить результативность своей деятельности. Система управления реорганизуется, оптимизируются процессы взаимодействия между подразделениями предприятия, что влечет за собой отсечение непродуктивных процедур и сосредоточение деятельности на процессах, которые приносят предприятию максимально возможный уровень развития.

Современная конкурентная среда диктует предприятиям все новые и новые требования, в условиях ожесточенной конкурентной борьбы и быстро изменяющихся условий рынка предприятия вынуждены уделять все больше внимания повышению результативности работы на каждом этапе деятельности каждого подразделения предприятия. Помимо оттачивания деятельности на всех этапах жизненного цикла продукта существует острая необходимость наличия эффективной системы взаимодействия подразделений компании и аппарата управления, которая не только способна эффективно решать текущие задачи предприятия, но и имеет возможности изменения процедур взаимодействия в угоду быстро меняющимся внешним факторам без снижения результативности.

Список использованных источников:

1. Коньшев В. А. Применение инновационных технологий в реструктуризации предприятий. Вестник оренбургского государственного университета. ISSN: 1814-6457 eISSN: 1814-6465
2. Ситников А.А., Ситников С.Г. Анализ использования оперативного менеджмента в финансовом менеджменте. Электронный научный журнал. Учредители: Общество с ограниченной ответственностью "АР-Консалт" (Люберцы) eISSN: 2414-5041
3. Набоков М. В., Чистов Д. А. Подходы и методологии реинжиниринга бизнес-процессов телекоммуникационного предприятия. Известия волгоградского государственного технического университета Учредители: Волгоградский государственный технический университет (Волгоград) ISSN: 1990-5297
4. Репин В. В., Елиферов В.Г. Процессный подход к управлению. Моделирование бизнес-процессов / Владимир Репин, Виталий Елиферов. – М.: Манн, Иванов и Фербер, 2013. – 544 с

5. HL Bhaskar. Business process reengineering framework and methodology: a critical study. International Journal of Services. 2018 - inderscienceonline.com
6. VW Elapatha, SN Jehan. An Analysis of the implementation of business process re-engineering in public services. Journal of Open Innovation: Technology. 2020.

УДК 339.138:005.52

© Е.Р. Мысева, Д.А. Глебова, 2021

Теоретические основы маркетингового исследования рынка. Этапы реализации анализа рынка

Е.Р. Мысева

заместитель начальника отдела правового и методического обеспечения
учебного процесса ИФТЭБ НИЯУ МИФИ, Москва

Email: ERMyseva@mephi.ru

Д.А. Глебова

студент 2-го курса бакалавриата РАНХиГС, г. Москва

Email: glebova534999@gmail.com

Аннотация: В данной статье рассматривается важность проведения маркетинговых исследований, как маркетинговые исследования влияют на развитие конкурентоспособности организации и развитие компании в целом.

Ключевые слова: маркетинг, маркетинговые исследования рынка, конкурентоспособность организации, анализ рынка, оценка.

Theoretical bases of market research. Market analysis stages

Abstract: in this paper we discuss the importance of market research, how market research affects organization competitiveness development and organization development in general.

Keywords: marketing, market research, organization competitiveness, market analysis, market evaluation

С середины двадцатых годов прошлого века в мире началось активное исследование рынков, многие источники связывают это с популяризацией рекламы в США на радиопрограммах. Именно тогда многие компании начали активно рекламировать свои товары и услуги по радио, а также стали обращать внимание и анализировать значимость демографии при

выборе спонсируемых ими радиопрограмм. Со временем все большее количество рекламодателей было заинтересовано в изучении влияния внешних факторов рынка на деятельность их организаций. Исследовались не только демографические показатели, но и политические, экономические, технологические и пр.

В современном мире исследование рынка – важнейший этап работы менеджера по маркетингу. Ведь именно от грамотного анализа рынка зависит процветание компании – нахождение свободных рыночных ниш, выбор максимально прибыльного целевого рынка, прогнозирование поведения всех игроков рынка. Именно исследование рынка дает четкие ответы на поставленные вопросы – что ждут потребители, что им необходимо, какие предпочтения у потребителей, в чем они нуждаются.

Под маркетинговым исследованием рынка подразумевается процесс систематического сбора, обработки и объективного анализа информации об основных аспектах бизнес-среды. Детальное маркетинговое исследование рынка необходимо проводить на первоначальном этапе становления бизнеса с целью поиска новых возможностей для компании и формировании наиболее эффективной маркетинговой стратегии.

По окончании исследования можно определить наиболее результативные способы ведения конкурентной борьбы, продумать пути выхода на новые рынки, появляется возможность осуществления сегментации – выбор целевых рынков и рыночных ниш для определенной организации.

В маркетинговые исследования рынка входит всестороннее изучение факторов, которые составляют бизнес-среду, а именно:

- Изучение состояния рынка. Здесь рассматриваются основные тенденции, реакции покупателей на новые товары, изменения предпочтений потребителей, емкость рынка.

- Анализ нормы прибыли в конкретной отрасли;
- Изучение доли разнообразных организаций на рынке, возможности и перспективы развития;

- Анализ целевых сегментов, спецификации поведения и требования к новым продуктам;

- Детальное изучение конкурентов, анализ сильных и слабых сторон организации.

К основной цели маркетингового исследования рынка можно отнести стратегическое планирование компании, выбор стратегии и тактики для улучшения своих позиций на рынке, повышению конкурентоспособности, выявлению перспектив развития в разных сегментах рынка. При этом возникает необходимость снижения уровня неопределенности рыночной

ситуации для того, чтобы минимизировать бизнес-риски и возможные потери.

После определения целей маркетингового исследования рынка ставятся и решаются следующие задачи:

1. Составление последовательного плана исследования рынка;
2. Определение сроков и бюджета анализа рынка;
3. Выбор методов исследования;
4. Проведение необходимых исследований рынка;
5. Проведение анализа полученной информации по рынку;
6. Подготовка обобщающего обзора рынка;
7. Составление презентации по исследованию рынка.

План маркетингового исследования рынка должен включать в себя этапы исследования основных структурных компонентов рынка.

■ Первый этап исследования включает в себя изучение состояния рынка. Рынок – весьма динамичная структура, требующая постоянного наблюдения. Важнейшим и ключевым показателем, на который грамотные маркетологи обращают свое пристальное внимание – это емкость рынка. Ведь именно данный показатель сообщает какое количество товаров и услуг потребители могут приобрести в тот или иной период времени (неделя, месяц, год). Для расчета данного показателя следует использовать следующую формулу:

$$V = A \times N$$

Где: V – размер рынка, A – численность целевой аудитории (тысяч человек), N – норма потребления продукции за период. [1]

Именно на основе данного показателя можно вычислить максимальный уровень продаж, который может достичь организация в определенном регионе.

Вторым не менее важным показателем является уровень спроса. Следует иметь четкое представление о том, как меняются предпочтения потребителей за определенные периоды времени.

Необходимо принимать во внимание динамику рынка, а именно развивается или, наоборот, сокращается. В случае активного развития рынка стоит определить возможный потенциал и возможности роста, что же касается этапа стагнации, то здесь необходимо четко понимать, как долго будет продолжаться это состояние.

■ Второй этап включает в себя выявление целевых сегментов.

В анализе, в первую очередь, проводится сегментация рынка, затем выделяются ключевые сегменты потребителей, которые могут принести компании прибыль. Под сегментами подразумевают однородную группу

потребителей, обладающую схожими потребностями и покупательскими привычками по отношению к товару или услуге компании. [3] Для сегментации аудитории могут быть использованы различные критерии, такие как возраст, пол, профессия, социальный статус, уровень дохода, интересы и пр. Целевым сегментом рынка принято называть один из сегментов, который выбирается в качестве ключевого и наиболее важного во время осуществления стратегии дифференцированного маркетинга.

Для полного понимания картины, а именно на какие сегменты стоит ориентироваться первоначально, следует провести дополнительный анализ, а именно:

1. Установить емкость каждого из сегментов;
2. Определить доступность разных групп потребителей;
3. Изучить географический аспект;
4. Спланировать приблизительные временные и финансовые затраты для старта деятельности.

Таким образом, грамотно проведенный отбор целевых сегментов позволит компании избавиться от лишних затрат и направить ресурсы на привлечение «прибыльных» клиентов.

▪ Третий этап направлен на исследование деятельности конкурентов на рынке. Конкуренты – это организации или компании, производящие аналогичный товар или товары-заменители, а также осуществляющие свою деятельность на том же самом рынке, что и другие производители. [2]

Анализ деятельности конкурентов необходим, прежде всего, для разработки эффективной стратегии противодействия с целью захвата или защиты той или иной рыночной доли. В первую очередь следует найти информацию о самих организациях и их предполагаемых возможностях. На что следует обратить внимание:

- Используемые технологии;
- Квалификация персонала (как часто проходят тренинги, курсы повышения квалификации и т. д.);
- Уровень доходности и прибыльности;
- Изучить возможное наличие патентов или уникальных технологий, которыми обладают конкуренты;
- Возможность получения инвестиций;
- Доступ к редким и ценным ресурсам.

Следующим шагом будет изучение товаров и услуг соперников. Рассматривать нужно глазами покупателя для наиболее объективной оценки. Для этого можно оценить характеристики продукта по шкале и отобразить это в виде «паутинной» диаграммы как на рис. 1.



Рисунок 1 - Оценка товара конкурентов

И, наконец, последний шаг – систематизирование полученных данных и объективное сравнение всех игроков рынка.

- Четвертый этап маркетингового исследования рынка – ценовой анализ, т. е. изучение ценового позиционирования конкурентов, а также среднерыночных цен на товары. Цены обеспечивают компании запланированную прибыль, именно через цены реализуются конечные коммерческие цели компании, определяется уровень эффективности всего сбытового и производственного процессов.

Важно понимать структуру самой цены, из чего она строится. Цена представляет из себя себестоимость плюс затраты на продвижение и рекламную кампанию плюс наценка, следует также подсчитать прибыль от каждой осуществленной продажи. В данном случае стоит учитывать не просто стандартные цены, а также наличие акций, бонусных программ, специальных предложений, условий рассрочки и т.д..

Чтобы увидеть полную картину, складывающуюся на рынке, необходимо разделить всех игроков рынка на ценовые сегменты – эконом, премиум и пр. Исходя из анализа ценового позиционирования конкурентов, можно грамотно выстроить ценовую политику своей

компании и определить, как именно позиционировать свой товар – дорогой, но качественный, или экономичный и доступный.

Стоит обратить внимание на то, как изменяются среднерыночные цены – в сторону увеличения или уменьшения и какие причины могут этому поспособствовать.

▪ Пятый важный этап в маркетинговом анализе рынка – исследование основных каналов дистрибуции, т. е. участников рынка, вовлеченных в процесс производства и распространения товара или услуги. [4]

На данном шаге необходимо выделить основные элементы: оптовые и розничные сети, склады, отдельные магазины, транспортные компании. Рассматриваются как отдельные предприятия, так и логистическая система в целом – как продукция движется от производителя к конечным потребителям, сколько времени и средств затрачивается на процесс, через каких посредников проходит товар и т. д.

При исследовании необходимо выяснить следующее:

1. Определить какие предприятия функционируют в данном регионе (фирменные сети магазинов, супермаркеты, киоски);

2. Процент точек (мест), где можно купить товары определенного производителя в конкретном регионе;

3. Изучить территориальное расположение, уровень и размер продаж главных магазинов региона;

4. Уровень плотности (густоты) дистрибуции, то есть отношение количества магазинов к плотности населения в определенном регионе;

5. Контингент, то есть необходимо провести анализ потенциальных покупателей (средняя сумма чека, какие товары наиболее востребованы той или иной категорией потребителей, место жительства и т. д.).

▪ Шестой этап – оценка эффективности рекламной кампании. Здесь важно понять, каким образом конкуренты привлекают потенциальных клиентов и удерживают реальных, какие инструменты при этом используют. Существует несколько инструментов комплекса маркетинговых коммуникаций, которые представлены в табл.1.

Таблица 1 – Основные элементы комплекса маркетинговых коммуникаций

Название элемента	Обоснование элемента
Реклама	Распространение не персонализированной информации в газетах, журналах, интернете, ТВ, радио, на плакатах, баннерах и т. д.
Стимулирование сбыта	Проводятся специальные мероприятия, направленные на то, чтобы потенциальный покупатель приобрел товар или услугу. Наиболее популярные методы: бесплатные образцы товаров, купоны на скидку, всевозможные акции, разнообразные конкурсы и другое.

PR/пропаганда	Создается исключительно позитивный имидж компании, а также ее продукции, чаще всего за счет интервью, обзоров, публикаций и иных материалов в СМИ.
Личные продажи	Личный контакт продавца с покупателем при представлении продукции.

Для комплексного исследования необходимо также понимать, как работать с конкретным типом людей, чем руководствуются люди при покупке, на что обращают внимание при покупке в первую очередь и т. д.

Изучение потребностей людей проводится в нескольких направлениях:

- Ожидания относительно стандартов обслуживания, качества и цен продукции;

- Мотивация, изучение потребностей и целей покупки.

- Ключевые критерии (что покупатель хочет получить, в первую очередь, от товара или услуги);

- Процесс принятия решения покупки (чем руководствуется – эмоциями или логикой, с кем советуется);

- Причины недовольства и претензий клиента касательно продукта или сервиса.

Понимание реальных и потенциальных клиентов – необходимое условие для создания доверительных отношений, которые потом могут перерасти в лояльность к продукции и привести к узнаваемости компании.

В основе современной концепции маркетинга лежат человеческие нужды, выражающиеся в потребностях, которые меняются с течением времени и весьма специфичны для различных людей и культур. Рынок, с его меняющейся конъюнктурой и нестабильным человеческим спросом, требует грамотного маркетингового исследования. Ф

Важно понимать, что результаты исследования помогут определить наиболее эффективную стратегию завоевания новых клиентов, а также эффективные способы ведения конкурентной борьбы.

Маркетинговый анализ рынка является важнейшим инструментом при планировании бизнеса и дальнейшего развития компании. Как было выявлено, анализ рынка весьма трудоемкий процесс, состоящий из: постановки целей исследования, выявлении задач, составления плана действий, выбора методов сбора и обработки полученной информации и составления итогового отчета. На основе полученных данных о рынке строится дальнейшая стратегия компании.

Список использованных источников:

1. Романов М. В., Муратова С. А. Экономические аспекты применения методов биотехнологии при производстве посадочного материала

садовых культур наука и образование Учредители: Мичуринский государственный аграрный университет (Мичуринск)

2. Резник Г.А. Введение в маркетинг: Учебное пособие / Г.А. Резник. - 3-е изд., перераб. и доп. - Москва: НИЦ ИНФРА-М, 2014. - 202с.
3. Маркетинг. Реклама. PR. Сборник студенческих работ / ред. И. А. Куянцев. – Москва: Студенческая наука, 2012. – 1983с.
4. Электронный ресурс <https://directsalez.ru/>
5. Рыжикова Т.Н. Аналитический маркетинг: что должен знать маркетинговый аналитик: учебное пособие. — Москва: ИНФРА-М, 2021. — 288с.
6. Торговое дело: коммерция, маркетинг, менеджмент. Теория и практика: монография / под науч. ред. д.э.н., проф. Д. И. Валигурского. - Москва: Издательско-торговая корпорация «Дашков и К°», 2020. - 306с.

УДК 340:342.72/.73

© Е.О. Алексеев, А.С. Вяткина, А.И. Минеева, А.К. Завалишина, 2021

Черный рынок персональных данных

Е.О. Алексеев

студент 4 курса специалитета УрФУ ИРИТ-РТФ, Екатеринбург

Email: llen9@mail.ru

А.С. Вяткина

студент 4 курса специалитета УрФУ ИРИТ-РТФ, Екатеринбург

Email: arinka02799@gmail.com

А.И. Минеева

студент 4 курса специалитета УрФУ ИРИТ-РТФ, Екатеринбург

Email: anna_mineyeva@mail.ru

А.К. Завалишина

ассистент кафедры финансового менеджмента НИЯУ МИФИ, Москва

Email: akzavalishina@gmail.com

Аннотация: с каждым годом в сеть утекает всё больший объём персональных данных. Актуальность темы заключается в том, что из-за недостаточных мер защиты утечки случаются всё чаще и чаще. Данные попадают в даркнет, где их может приобрести любой желающий. В данной статье исследуется сущность чёрного рынка персональных данных, а также предлагается рассуждение на тему: можно ли с ним бороться?

Ключевые слова: *чёрный рынок, даркнет, персональные данные, криптовалюта, базы данных.*

Personal data black market

Abstract: every year more and more personal data is leaking into the network. The relevance of the topic lies in the fact that due to insufficient protection measures leaks occur more and more often. The data goes to the darknet, where anyone can purchase it. This article examines the essence of the black market for personal data, and also offers a reasoning on the topic: can we fight it?

Keywords: black market, darknet, personal data, cryptocurrency, databases.

Вступление

Сеть интернет поработила человечество: поиск информации, просмотр фильмов и прослушивание музыки. Везде нужно указывать персональные данные: ФИО, телефон, почту. Важно, что люди так часто их оставляют, что почти невозможно говорить о полной защите конфиденциальности.

«Приватность мы уже проехали, упустили — мы все в цифровом мире. Ящик Пандоры уже открыт», — так охарактеризовал современный мир Сергей Солонин, глава платёжного сервиса Qiwi [3].

Можно прийти к выводам: если персональные данные крадут, значит на них есть спрос. Либо они сразу попадут в руки мошенников, либо попадут на чёрный рынок, где в дальнейшем будут проданы. Чёрный рынок — это подпольный рынок или серия сделок, которые имеют некоторый аспект незаконности или характеризуются некоторой формой неподдерживаемого поведения с институциональным набором правил, но нам нужна лишь небольшая сфера этого рынка — чёрный рынок персональных данных.

История появления чёрного рынка данных

Неизвестно, когда появился чёрный рынок, потому что большинство покупателей и продавцов молчали о своей связи с ним. При этом точно можно сказать, что чёрные рынки впервые появились в Китае. В то время на них еще не продавали запрещенные товары, единственное, что отличало их от обычных рынков — более низкие цены. В 1315 году, после великого года, чёрный рынок появился в Европе, на них люди уже торговали запрещенным товаром, зерном.

Логично было бы предположить, что если сейчас персональные данные продаются на чёрных рынках, то их продажа появились вместе с ними, но это не так. Потребность в них появилась намного раньше, до нашей эры, ведь в Священной Римской империи точно были информаторы.

Как устроен чёрный рынок данных?

Чёрный рынок устроен также как и любой другой. Одни люди предлагают товар, другие готовы платить за него деньги. Отличает его то, что сделки осуществляются через специальные форумы в даркнете.

Сделка может проходить с гарантом и без. Гарант — никто иной как посредник в финансовых вопросах между лицами предоставляющими определенные услуги/товары и заказчиками в интернет-сделках, который обеспечивает полное выполнение всех условий сделки обеими сторонами при этом не преследуя интересы ни одной из них. Обычно гарант берет за свои услуги 4-6% от суммы сделки.

В отличие от большинства товаров, продажа персональных данных сейчас активно развивается в мессенджерах.

«Массмаркет, назовем его B2C, отчасти мигрировал в мессенджеры. Есть еще B2B — тут сделок меньше, товар более уникальный, продажи происходят как на доверии продавцу, так и с участием гаранта», — слова CEO Hacken Дмитрия Будорина [3].

Что продают?

На чёрном рынке персональных данных есть всё — адреса электронных почт, пароли и сведения о передвижении любого человека. Российский же рынок состоит из продажи баз данных и услуг по «пробиву» конкретных лиц. «Пробив» — это противоправная услуга, с помощью которой злоумышленники получают из закрытых баз данных информацию о конкретном человеке или организации [5].

Большим спросом у мошенников пользуются базы данных. «Если это просто список электронных почт, ценность у такой базы сомнительная. Если это список электронных почт с паролями, то ценность у неё выше. Чем разнообразнее информация, тем она ценнее», — говорят независимые эксперты [3].

Также в даркнете на продажу выставлены программы, предназначенные для взлома определённых систем. Дополнительно предлагается услуга по «пробиву» человека. Данные позволяют получить практически любые сведения об объекте поиска: от информации о его перемещениях до детализации звонков. Всё это преступники используют для совершения сложных преступлений, а службы безопасности организаций — для внутренних проверок. Это стоит в разы дороже других услуг, которые представлены на рынке, поэтому требуется меньшим спросом.

На чёрном рынке можно также встретить продажу официальных аккаунтов бирж криптовалюты, хотя это нечастое явление.

Кто продаёт?

Со слов специалистов персональные данные попадают в даркнет либо от инсайдеров, либо в результате взломов баз данных. Главная причина утечки персональных данных — сотрудники компаний, обладающие

доступом к ним, которые перепродают их для получения личной выгоды. Этими сотрудниками могут быть как работники банков и операторы связи, так и сами правоохранители. Важно помнить, что продавцы не всегда есть взломщики — частое явление, когда большие базы складываются из нескольких баз поменьше, которые уже были в сети. Например, мошенник, который продал базу из 773 млн уникальных адресов электронной почты и более 21 млн паролей, не взламывал никакие ресурсы. Он лишь собрал вместе данные, которые он нашёл в сети интернет [3].

Конкретно взлом осуществляется хакерскими группами, которые продают информацию, полученную на чёрном рынке. Их методы: взлом открытых серверов с базами данных с помощью известных им уязвимостей и копирование баз данных, которые оказались в сети из-за халатности администраторов.

Данные конкретного лица, вплоть до его точного нахождения, часто сливают в сеть сами сотрудники спецслужб, отмечают эксперты.

Кто покупает?

Основными покупателями персональных данных являются предприниматели и злоумышленники. Для тех и других мотивацией являются первоначальные исследования и получение новой полезной информации. Эти данные необходимы для планирования курса действий. Почему компании прибегают к таким действиям? Так, они могут устраивать рассылки спама или разведывать сведения о конкурентных компаниях. Мошенники же пользуются личной информацией для фишинга или мошенничества в виде звонков.

«Пробив» конкретного лица чаще всего используют представители спецслужб. Более того, эксперты отвечают, что в России и бывших союзных республиках такая услуга распространена шире [3].

Какая валюта рынка?

Почти все сделки на даркнет-маркетплейсах, продающих персональные данные, осуществляются в биткоинах. Это подтвердило исследование Rand Corporation [3].

Основные способы оплаты: биткоин и Perfect Money. Опытные покупатели используют Zcash и Monero, потому что они обладают повышенной анонимностью. Их минус – нестабильность курса.

Криптовалюты используются при проведении операций между продавцами и покупателями, а также когда продаётся эксклюзив. Дальнейшая перепродажа криптовалюты происходит через электронные кошельки, либо банковские карты, зарегистрированные на номинальных владельцев [3]. В секторе «пробива» всё работает точно также. Однако в нём можно найти даже наличные деньги, потому что некоторые инсайдеры продают данные друзьям, которые уже являются посредниками.

Цены на персональные данные

Сколько стоят персональные данные россиян? Цены на услуги варьируются в зависимости от сложности задачи от 700 рублей до десятков тысяч. Стоимость данных разных операторов отличается. К примеру, пробить данные паспорта абонента оператора «Билайн» стоит 800 рублей, а «Теле-2» — 5000 рублей.

Ниже представлена табл.1 с ценами на данные в российском сегменте чёрного рынка [4]. Данные представлены исключительно с целью ознакомления.

Таблица 1 – Цены на услуги российского сегмента на чёрном рынке данных

Услуга	Цены, руб.
«Пробив» номера через «Роспаспорт»	1300
Узнать владельца автомобиля	1300
СНИЛС, ИНН и ЕГРН	1500
Детализация звонков	От 1500
Узнать о передвижениях по России на транспорте	2000
Местоположение человека по звонку	От 2500
Все пересечения границ	3000
Подпись и печать юрлиц	3500
«Пробив» через систему «Поток» на дорогах Москвы, Петербурга и Краснодара	От 6000 в месяц
Данные о федеральном розыске и запрете на въезд в страну	4000-7000
Проверка списка пассажиров в любом транспорте	От 7000
Наблюдение с системы камер «Безопасный город» по Москве и Мособласти за последние пять дней	10 000
Взлом почт	От 8000 до 45 000

Данные о человеке по номеру телефона могут можно пробить через ботов мессенджера «Telegram» по ежемесячной подписке или разовому переводу.

Чем опасен чёрный рынок данных?

Формирование и развитие «черного рынка» персональных данных создают ряд проблем для государства, граждан, предприятий и организаций.

Во-первых, персональные данные, которые попадают в даркнет, приобретаются незаконным путем и преступными методами. А это причиняет вред как юридическим, так и физическим лицам.

Во-вторых, во многих случаях персональные данные используются в злонамеренных целях. Кража персональных данных может иметь ряд

негативных последствий для их владельцев. Ниже представлены данные опроса людей, чьи персональные данные были украдены [1].



Диаграмма 1 – Данные опроса людей

Кража личных данных наносит большой ущерб бизнесу. Факты показывают, что это постоянный риск для компаний и к подобным ситуациям всегда нужно быть готовым. Для компаний, столкнувшихся с утечкой данных, самая большая финансовая потеря — это потеря репутации. После таких инцидентов компании должны предпринять необходимые шаги для восстановления доверия клиентов и снижения долгосрочных негативных финансовых последствий.

Большинство утечек данных являются результатом кибератак. Для расследования и выявления таких инцидентов требуется много времени. Компании признают, что чем больше времени требуется для обнаружения и предотвращения утечек данных, тем дороже это обходится. Объем таких расходов растет с каждым годом [9]. Для выявления и предотвращения таких угроз необходимо использовать личный опыт и увеличивать инвестиции в технологии. В строго регулируемых областях, таких как здравоохранение и финансовые услуги, утечка данных обходится дороже, поскольку уровень и вероятность потери репутации и клиентов в результате таких инцидентов в этих областях выше. Если персональные данные попадут в руки иностранной разведки через рынок незаконной торговли, то могут возникнуть серьезные проблемы для национальной безопасности. Так, с помощью технологий больших данных можно анализировать большое количество персональных данных, из которых можно извлечь различную полезную информацию, представляющую

интерес для иностранных спецслужб. Эта информация может отражать отношение, взгляды и подходы граждан к любому вопросу в любой стране, а также их материальное, моральное, психологическое состояние и состояние здоровья. Кроме того, эта информация может быть использована спецслужбами для совершения любых провокаций против страны.

Другой целью получения персональных данных через даркнет является использование их для вымогательства посредством шантажа и запугивания. В таких ситуациях чиновники, которых шантажируют злоумышленники, обладающие их персональными данными, вынуждены подчиняться их требованиям.

Что дальше

С каждым годом чёрный рынок данных только расширяется, не только из-за цифровизации общества, но и благодаря переходу части обывателей данного рынка в мессенджеры.

«Очень скоро люди, которые потеряли работу, пойдут заниматься мелким хакерством. Те форумы, которые продавали слитые базы данных, уже стали известными широкому кругу людей. Более предприимчивые стали организовывать каналы сбыта через мессенджеры, чтобы зарабатывать не на самих взломах, а на перепродаже информации», — мнение Дмитрия Будорина [3].

Как защитить свои персональные данные?

От утечек персональных данных никто не застрахован. Однако, существует ряд мер, которые позволят сократить эту вероятность настолько, на сколько это возможно. Обезопасить персональные данные поможет «цифровая гигиена».

Цифровая гигиена – это набор правил безопасного поведения в цифровом пространстве. Именно соблюдение определённых правил поможет избежать утечки личных данных.

Специалисты рекомендуют выполнять следующее [8]:

- установка антивируса;
- составление сложных паролей из букв, символов и цифр;
- периодическая смена паролей;
- игнорирование подозрительных файлов и ссылок из электронных писем, SMS и в соцсетях;
- избегание подозрительных сайтов;
- отсутствие одинаковых паролей на разных интернет-страницах;
- регистрирование аккаунта на специальную сим-карту, номер которой будет никому неизвестен
- разные почты — рабочая и для личных целей;
- удаление писем, содержащих конфиденциальную информацию (пароли, данные паспорта, номера телефонов);

- использование двухфакторной идентификации;
- периодическая проверка почты на взлом.

Заключение

Нужно остановить рост черного рынка данных, а затем его искоренить. Но скорее всего это невозможно сделать в нынешних реалиях. Где есть спрос, там и предложение, а спрос на персональные данные всегда будет. Будут вестись расследования, появляться новые дела на обывателей черных рынков, но незаконная деятельность уже перебралась в мировую паутину и теряет некую физическую составляющую, так что задача поимки нарушителей закона будет усложняться с каждым годом. Искоренить продажу персональных данных на данном этапе не представляется возможным.

Список использованных источников:

1. Cook G. «How Much Is My Identity Worth on the Black Market?» [Электронный ресурс] // Режим доступа: <https://www.findreviews.com> (дата обращения: 10.06.2021)
2. Статья «Как работают чёрные рынки» [Электронный ресурс] // Режим доступа: <https://nesrakonk.ru/mechanics-black-market/>
3. Статья «Как устроен черный рынок данных: кто продает, кто покупает и можно ли защитить себя» [Электронный ресурс] // Режим доступа: <https://forklog.com/kak-ustroen-chernyj-rynok-dannyh-kto-prodaet-kto-pokupaet-i-mozhno-li-zashhitit-sebya/>
4. Статья «“Пробив” по всем структурам: как сливают данные россиян и сколько это стоит» [Электронный ресурс] // Режим доступа: <https://tjournal.ru/analysis/249234-probiv-po-vsem-strukturam-kak-slivayut-dannye-rossiyan-i-skolko-eto-stoit>
5. Статья «Пробив - что это такое или ваши персональные данные уже давно не ваши» [Электронный ресурс] // Режим доступа: <https://koreanst.livejournal.com/95591.html>
6. Статья «Теневая глобализация» [Электронный ресурс] // Режим доступа: <https://mgimo.ru/upload/iblock/e25/e253e4ce34a3205df166a949d70956a6.pdf>
7. Статья «Тотальная слежка: как устроен рынок торговли пользовательскими данными» [Электронный ресурс] // Режим доступа: <https://www.rbc.ru/magazine/2018/04/5aafdfc99a7947654297214d>
8. Статья «Утечка персональных данных: как обезопасить себя в интернете» [Электронный ресурс] // Режим доступа: <https://tvk6.ru/publications/news/40306/>
9. Nuncic M. «The Black Market for Data» [Электронный ресурс] // Режим доступа: <https://www.ontrack.com/en-us> (дата обращения: 10.06.2021)

Экономические преступления в период пандемии COVID-19

А.И. Натарева

студентка 3 курса специалитета НИЯУ МИФИ, Москва

Email: natarovaanglina@mail.ru

О.С. Котелянец

ассистент кафедры финансового мониторинга НИЯЦ МИФИ, Москва

Email: OSKotelyanets@mephi.ru

Аннотация: Статья посвящена увеличившемуся количеству экономических преступлений в период пандемии COVID-19. Подробно рассматривается зарубежный опыт мошеннических действий и меры их противодействия. Отдельное внимание уделено такому виду преступления, как мошенничество в сети Интернет за рубежом и, в частности, в Российской Федерации.

Ключевые слова: мошенничество, экономические преступления, безопасность, киберпреступность, пандемия, коррупция, зарубежный опыт, меры противодействия.

Economic crimes in the period of the pandemic COVID-19

Abstract: The article is devoted to the increased periodic number of economic crimes in the COVID-19 pandemic. The foreign experience of fraudulent activities and their countermeasures have been studied in detail. Special attention is paid to this type of crime as online fraud, in particular, in the Russian Federation.

Keywords: fraud, economic crimes, security, cybercrime, pandemic, corruption, foreign experience, countermeasures.

Коррупция является глобальной проблемой мирового сообщества и угрозой современной цивилизации, поскольку препятствует нормальному функционированию и социально-экономическому развитию общества. Коррупция как социальное явление в том или ином объеме проявляется в любой стране, обостряя все возрастающие противоречия в отношениях между гражданским обществом и государством, особенно в условиях развития рыночных отношений. В этой статье мы взглянули на проблему коррупции в разрезе пандемии COVID – 19.

Ситуация с COVID-19 затронула жизнь практически каждого человека на Земле: с каждым днем увеличивается число зараженных и погибших по всему миру. На сегодняшний день о болезни многое неизвестно, поэтому предсказать конец глобального кризиса никто не может. Пандемия оказывает большое влияние на экономическую сферу, в которой все больше распространяется мошенничество, киберпреступность, нецелевое и неправомерное использование правительственных ресурсов или международной финансовой помощи. Все больше компаний теряют прибыль, клиентов, поставщиков или же вовсе становятся банкротами из-за невозможности погашения обязательств. Для предотвращения роста заболевших и для эффективности рабочего процесса, директора стараются перевести своих сотрудников на дистанционный формат работы, предоставляя необходимую технику для качественного выполнения обязанностей.

Многие сотрудники по борьбе с экономическими преступлениями работают удаленно, однако эффективность их работы значительно отличается от обычных компаний с ограниченным доступом к защищенным системам и файлам, что снижает их способность собирать, обрабатывать, анализировать и оценивать информацию о делах ПОД / ФТ.

Отмывание денег остается ключевым фактором транснациональной организованной преступности, связанной с COVID-19. К часто упоминаемым преступлениям относятся:

- Покупка подлинного медицинского оборудования и лекарств, полученных обманным путем;
- Перенаправление, перехват и неправомерное использование благотворительных пожертвований.

В ответ на возникающие риски ключевые регулирующие органы на основных рынках выпустили заявления, призывающие финансовые учреждения оказывать помощь потребителям и предприятиям в это время экономической неопределенности путем ослабления некоторых аспектов их требований в области ПОД/ФТ, таких как привлечение клиентов и их тщательная проверка. В то же время финансовым учреждениям напоминают, что они должны оставаться строгими в своем контроле ПОД/ФТ и соблюдении требований, в то время как большинство надзорных органов откладывают свои проверки на месте и сообщают, что надзор может быть ослаблен в разгар вспышки болезни.

Растущие угрозы и преступления совершенные в период пандемии

Изучение зарубежного опыта формирования антикоррупционного правосознания является одним из важнейших направлений получения информации о том, какими средствами, методами, в каких формах возможно создать обстановку нетерпимости к коррупции и снизить

уровень коррупционной преступности государства. Изучение и учет практики зарубежных стран позволяют избежать ошибок, противоречий в антикоррупционной деятельности и выбрать правильные подходы в стратегии борьбы с коррупцией.

Значение зарубежного опыта противодействия коррупции на государственной службе, включающего разнообразные по своему содержанию меры для решения задачи формирования антикоррупционного правосознания государственных служащих, обусловлено тем, что правосознание – это особый правовой феномен, который развивается под влиянием комплекса разносторонних факторов, включающих особенности исторического развития страны, специфику функционирования институтов государства, целенаправленную деятельность по формированию антикоррупционного мировоззрения и сознания, социальную обстановку. Процесс его формирования предполагает воздействие на личность и общество в целом с разных сторон, затрагивающих устранение правовых, социальных, экономических, духовно-нравственных и других причин и условий коррупции.

Как показывает зарубежный опыт, формирование антикоррупционного правосознания в основном происходит в двух направлениях: формирование антикоррупционной правовой идеологии; формирование антикоррупционной правовой психологии. В период пандемии число предикатных преступлений резко возросло, и как следствие, возросло число попыток отмыть доходы, полученные преступным путём, используя различные коррупционные схемы.

Коррупция, злоупотребление служебным положением для получения личной выгоды, — это больше, чем потраченные деньги: она нарушает общественный договор и подрывает способность государства обеспечивать экономический рост на благо всех граждан. Коррупция была проблемой и до кризиса, но пандемия COVID-19 повысила значимость более сильного управления по трем причинам.

Во-первых, во всем мире государство стало играть бóльшую роль в экономике в целях борьбы с пандемией и предоставления экономической помощи людям и компаниям. Эта возросшая роль критически важна, но также она расширяет возможности для коррупции. Чтобы деньги и меры помогали людям, которые в них больше всего нуждаются, государствам необходима своевременная и прозрачная отчетность, ретроспективные ревизии и процедуры подотчетности, а также тесное сотрудничество с гражданским обществом и частным сектором.

Во-вторых, по мере ухудшения ситуации в области государственных финансов, странам необходимо предотвращать уклонение от уплаты

налогов и растрату и потерю средств вследствие коррупции в сфере государственных расходов.

В-третьих, кризисы проверяют веру людей в правительство и институты, а значение этического поведения возрастает, когда медицинские услуги пользуются таким большим спросом. Доказательства коррупции могут подорвать способность страны эффективно реагировать на кризис, углубляя экономические последствия и грозя потерей политической и социальной сплоченности.

За время действия ограничений и изоляции граждан, экономические преступления в интернете за первое полугодие 2020 года выросли на 76% по сравнению с предыдущим первым полугодием 2019. По данным Генпрокуратуры, с апреля по июнь, как раз в период общей самоизоляции, зафиксировано 82,5 тыс. случаев мошенничества с использованием современных средств связи и информации.

Заместитель председателя Совета Безопасности РФ Дмитрий Медведев, на совещании, посвященном криминогенной обстановке, обратил внимание на столь проблемный аспект в сфере экономических преступлений и призвал выработать дополнительные меры для их предотвращения «Речь идет о проведении целого ряда межведомственных мероприятий, в том числе, связанных с предотвращением бюджетных хищений, защитой людей от цифровой преступности и миграционного криминала, вовлечением молодежи в экстремистскую и террористическую деятельность».

Ежедневно мошенники стараются воспользоваться ситуацией с COVID-19 для получения доступа к нелегальным доходам или для своих особых целей. По данным информационных источников, основные виды (преступных) операций можно разделить на следующие виды:

1. Мошенничество

1.1. Подделка медицинских товаров первой необходимости, такие как одноразовые перчатки, медицинские маски и лекарственные препараты.

В самый разгар пандемии цены на данную категорию товаров поднялись почти в 9-10 раз и стали самым главным средством обмана потребителей. Из-за закрытия большого числа магазинов, в том числе и аптек, заказать такие товары можно было только через интернет. Мошенники создают свой собственный сайт магазина похожего на реальный, покупатель оплачивает свои товары путем ввода данных кредитной карты после чего ждет своей доставки, которая по итогу остается у мошенников. Мошенники, создав сайт-двойник, могут похитить личные данные карты покупателя, а в будущем воспользоваться ими для снятия всех средств с этой карты. Согласно Уголовному Кодексу (УК РФ) ст. 238.1. обращение фальсифицированных, недоброкачественных и

незарегистрированных медицинских изделий могут наказываться принудительными работами, лишением права занимать определенные должности или заниматься определенной деятельностью на определенный срок, а также штраф в особо крупном размере.

1.2. Выдача себя за сотрудников медицинских предприятий или государственных служащих.

Преступники связываются чаще всего с физическими лицами и утверждают, что их родные смертельно больны или же попали в автомобильную аварию. Дальнейшее развитие ситуации заключается в вымогании денежных средств путем получения личных данных, в особенности информации о банковских или наличных средствах.

2. Киберпреступность

2.1. Фишинговые атаки через электронную почту или социальные сети

С увеличением пользователей социальных сетей, появился новый вид мошенничества-фишинг, целью которого является получение доступа от пользователей к их конфиденциальным данным, в особенности логинам и паролям. Преступники отправляют запрос пользователю ПО или мобильных устройств для скачивания вредоносной ссылки, выдавая себя за медицинскую организацию.

2.2. Мошенничество с использованием корпоративной электронной почты

В связи с переводом большого количества сотрудников на удаленный формат работы, киберпреступники ищут новые пути обмана с целью получения конфиденциальных данных о клиентах и транзакциях. Эта информация затем используется в целевых фишинговых письмах, в которых преступники представляют как скомпрометированный бизнес и запрашивать оплату за законные товары или услуги, но вместо этого направляют этот платеж на свои незаконные счета.

Пример мошенничества в период пандемии на территории РФ

В то время, как врачи борются за жизнь людей, мошенники не сидят на месте и пытаются заработать с столь опасной болезни, охватившей весь мир.

В век цифровых технологий существует масса возможностей заработка в интернете, один из которых в период самоизоляции просочился практически к каждому пользователю социальных сетей «Как заработать на коронавирусе». Программа данного вебинара состоит из 3-х частей:

- Как получить доход на мировых катастрофах;
- Как зарабатывать на кризисах, трагедиях и глобальных эпидемиях;
- Что делать, когда эпидемия закончится.

Вводный вебинар, как правило, бесплатный, однако последующие части можно посмотреть только за дополнительную оплату. При вводе данных

Вашей банковской карты, а именно: номер карты, имя и фамилия, срок действия и CVC код, преступники получают денежные средства, но при этом не предоставляют доступ к продолжению «обучающего» курса и блокируют Ваш аккаунт.

Другой пример мошенничества в период пандемии COVID-19 такой: Исполнительный директор Всемирной организации здравоохранения (ВОЗ) Майкл Райан заявил, что на текущий период времени в мире не существует действующих лекарств от коронавируса 2019-nCoV, которое со 100% вероятностью сможет победить такой вирус. Некоторые лекарственные препараты пытаются обогатиться за счет пандемии, таким стал «Арбидол», компоненты которого активно борются с гриппом, ОРВИ и короновирусом, однако клинических испытаний не было проведено, которые хоть как-то могли бы подтвердить эффективность данного препарата. Так, Американское управление по контролю качества лекарств и продуктов и вовсе отказалось его регистрировать. Громкими обещаниями заинтересовалась и Федеральная антимонопольная служба РФ (ФАС). Комиссия ФАС признала нарушением рекламу «Арбидола» о лечении коронавируса, согласно Кодексу об административных правонарушениях (КоАП ст. 14.3) и наложила штраф в размере от 200 тыс. до 500 тыс. руб.

Закключение. На протяжении всей человеческой истории людей преследовали различные заболевания и некоторые из них перерастали в целый эпидемии: бубонная чума, испанский грипп и сегодня-глобальная пандемия COVID-19, постигшая практически каждую семью. Человечество увидело насколько уязвимыми являются системы безопасности многих банков в период пандемии, как легко люди поддаются панике и могут запросто отдать свои личные данные в руки мошенникам, насколько незащищены внутренние сети и системы компании, включая самые крупные. Пандемия продемонстрировала те проблемы, над которыми всему человечеству стоит работать и что нужно изменить. Уже сейчас необходимо больше применять современные средства идентификации клиента, которые очень сложно обойти преступникам. Компаниям необходимо увеличить затраты на повышение внутренней безопасности, в частности, на повышение защищенности сетей и серверов. У граждан нужно повышать культуру пользования банковскими картами, более подробно и тщательно информировать пожилых людей о тех рисках, которые грозят им, в случае разглашения данных карты.

Борьба с коррупцией является общемировой проблемой, которая угрожает стабильности как отдельных стран, так и глобально всему человечеству. Очевидно, что одной из важнейших задач государственной антикоррупционной политики является задача по коренному перелому общественного сознания, формированию в обществе атмосферы жёсткого

неприятия коррупции. Решение этой задачи обеспечивается, прежде всего, путём формирования антикоррупционного мировоззрения и сознания. При этом, как свидетельствует зарубежный опыт, основным фактором, непосредственно влияющим на формирование антикоррупционного мировоззрения и сознания, является образование и воспитание. Также необходимо перенимать опыт борьбы с коррупцией у стран, которые истребили эту проблему у себя в стране. К таким странам относится Малайзия и Сингапур.

Список использованных источников:

1. Money-laundering and COVID-19: profit and loss (14.04.2020, Vienna) [Electronic resource] // United Nations Office on Drugs and Crime: [website]. URL: https://www.unodc.org/documents/Advocacy-Section/UNODC_-_MONEY_LAUNDERING_AND_COVID19_-_Profit_and_Loss_v1.1_-_14-04-2020_-_CMLS-COVID19-GPML1_-_UNCLASSIFIED_-_BRANDED.pdf (дата обращения: 20.11.2020).
2. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации - 17 июня 1996 г. - № 25 - раздел IX.
3. Аналитическая записка Глобальной инициативы против транснациональной организованной преступности – Текст: электронный // Министерство внутренних дел: официальный сайт. – URL: https://мвд.рф/upload/site1/folder_page/019/882/802/Globalnaya_initsiativa_a_Prestupnost_i_Infektsiya1.pdf (дата обращения: 20.11.2020).
4. Отмывание денег: изменения в банковском регулировании – Текст: электронный // Ассоциация сертифицированных специалистов в сфере отмывания денежных средств: официальный сайт – URL: <https://www.moneylaundering.com/news/covid-19-lockdowns-impact-on-money-laundering-is-limited-temporary/> (дата обращения: 19.11.2020).
5. Зарубежный опыт противодействия коррупции и возможности его применения в странах ЕАЭС: сайт. – URL: <https://revolution.allbest.ru/> (дата обращения: 19.11.2020).
6. Новостной интернет-портал Рамблер: официальный сайт. – URL: <https://news.rambler.ru/world/43629651-voz-lekarstv-ot-novogo-koronavirusa-ne-suschestvuet/?updated> (дата обращения: 20.11.2020).
7. Интернет-портал РБК: официальный сайт. – URL: <https://www.rbc.ru/society/10/03/2020/5e67a0089a7947824ea6e37e> (дата обращения 19.11.2020).
8. Интернет-портал РБК: официальный сайт. – URL: <https://www.rbc.ru/society/31/08/2020/5f48ea169a79477e21e25d9d> (дата обращения 19.11.2020).

