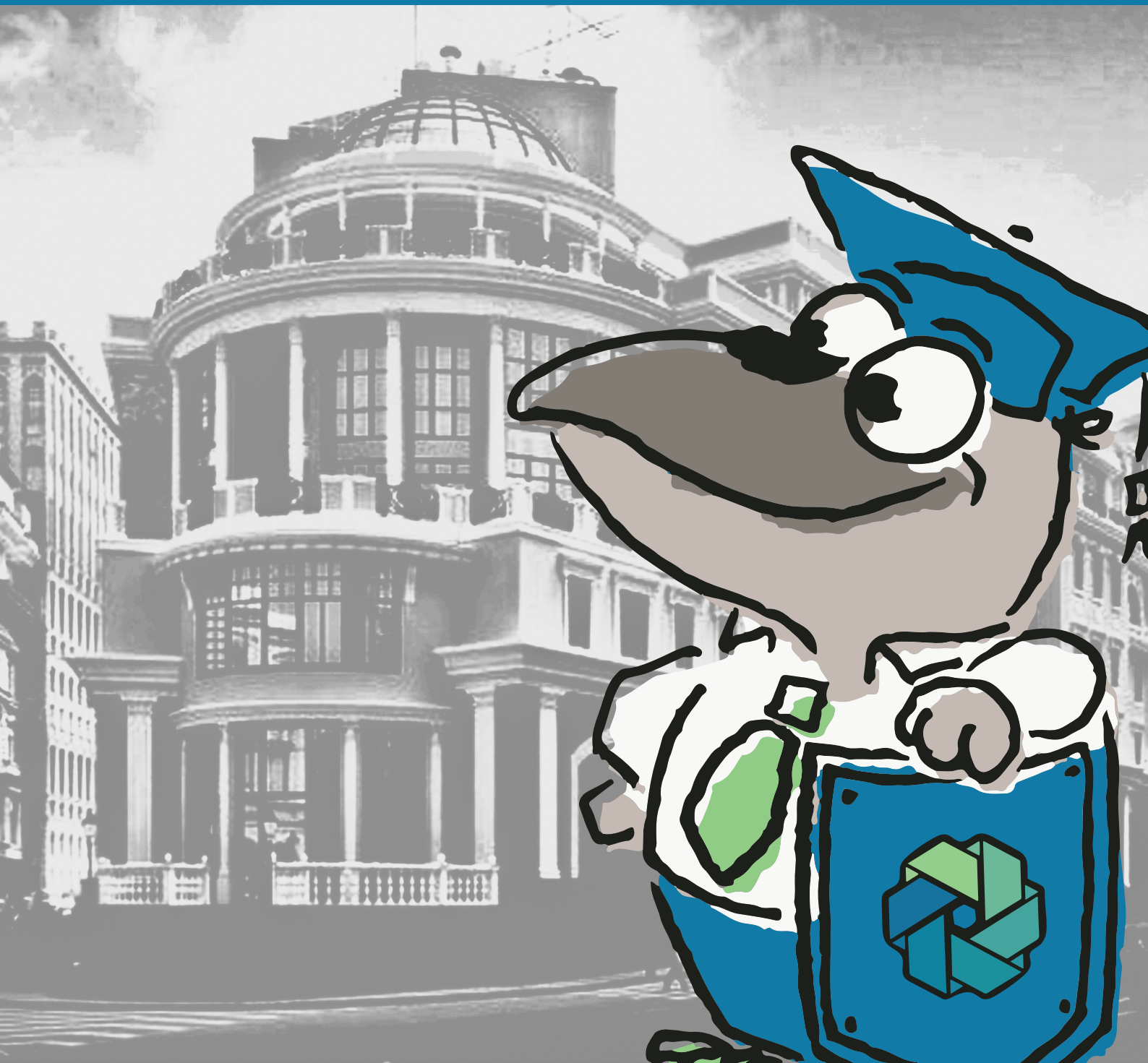
“БЕЗОПАСНОСТЬ РОССИЙСКОГО БИЗНЕСА В СОВРЕМЕННЫХ УСЛОВИЯХ”

МАТЕРИАЛЫ ТРЕТЬЕЙ И ЧЕТВЕРТОЙ СТУДЕНЧЕСКИХ НАУЧНО-ПРАКТИЧЕСКИХ КОНФЕРЕНЦИЙ



ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

ИНСТИТУТ ПРОБЛЕМ БЕЗОПАСНОСТИ НИУ ВШЭ

БЕЗОПАСНОСТЬ РОССИЙСКОГО БИЗНЕСА в СОВРЕМЕННЫХ УСЛОВИЯХ

Ежегодная студенческая научно-практическая конференция

СБОРНИК МАТЕРИАЛОВ,
представленных на конференции в 2018 и 2019 гг.

МОСКВА, 2020

УДК: 338.2; 004.056; 331.45; 658.027.45

Тезисы докладов Ежегодной студенческой научно-практической конференции «Безопасность российского бизнеса в современных условиях» Института проблем безопасности НИУ ВШЭ / Сост. и отв. ред. Макаров А.В. – М:, 2020. – 175 с.

В данном издании публикуются тезисы докладов Ежегодной студенческой научно-практической конференции «Безопасность российского бизнеса в современных условиях» Института проблем безопасности НИУ ВШЭ за 2018 и 2019 гг. Представленные работы посвящены широкому спектру тем в рамках пленарного заседания и секций конференций: «Интересы личности, общества и государства в динамике преодоления рисков и угроз безопасности», «Обеспечение экономической и финансовой безопасности бизнеса. Деловая (конкурентная) разведка», «Обеспечение безопасности материальных ресурсов бизнеса и защита персонала» и «Организационное поведение в бизнесе и управление сложными системами безопасности».

СОДЕРЖАНИЕ

ВСТУПИТЕЛЬНОЕ СЛОВО

ШУЛЬЦ ВЛАДИМИР ЛЕОПОЛЬДОВИЧ
Доктор философских наук, профессор,
член-корреспондент РАН.

Изучение современного состояния функции управления безопасностью в структуре бизнес-менеджмента является одной из важнейших проблем развития экономики. Эта отрасль безопасности стала частью осмысления современного экономического пространства, характерного для зарубежного и российского общества.

Отрадно, что в Высшей школе экономики эти проблемы приобретают как учебный, так и научный смыслы. Существование вот уже ряда лет дисциплины «Безопасность предпринимательской деятельности» позволяет сделать ряд выводов.

Во-первых, можно констатировать большую востребованность этой дисциплины у студентов всех факультетов ВШЭ. Следовательно, подход к созданию междисциплинарной дисциплины, где соединяются различные концептуально-понятийные поля, взаимодополняющие друг друга, был оправдан как учебно-методически, так и научно-практически.

Во-вторых, важно отметить все возрастающую научную активность студентов в их попытках самостоятельно проанализировать проблемы обеспечения безопасности предпринимательской деятельности, что выражается в возрастающем уровне докладов как на научных конференциях, так и в ходе изучения дисциплины и подготовке зачетных и экзаменационных работ.

Изучение нашей дисциплины студентами разных факультетов, их общение по общим и частным проблемам обеспечения безопасности предпринимательской деятельности вызывает все возрастающий мультипликативный эффект, удвоение или утроение компетенций. В этом можно убедиться, ознакомившись с материалами первых двух студенческих научных конференций.

И последнее. Институтом проблем безопасности ВШЭ был подготовлен и выпущен учебник «Безопасность предпринимательской деятельности» - первым в своем роде системным пособием. Издаваемый сборник материалов является дополнением и в какой-то мере развитием тех вопросов и проблем, которые в учебнике обозначены. Таким образом можно утверждать, что новая дисциплина развивается уже совместными усилиями студентов и преподавателей.

БАГНЮК ДМИТРИЙ ВЯЧЕСЛАВОВИЧ
выпускник факультета бизнеса и менеджмента
НИУ ВШЭ, г. Москва
E-mail: dv.bagnyuk@mail.ru

РАЗРАБОТКА МЕТОДОВ И МЕТОДИК УПРАВЛЕНИЯ ПРОЦЕССОМ ВЫЯВЛЕНИЯ ПРИЗНАКОВ КОРРУПЦИОННОГО ПОВЕДЕНИЯ УЧАСТНИКОВ ЗАКУПОК С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИХ СИСТЕМ?

BAGNYUK DMITRY VYACHESLAVOVICH
Bachelor Alumni, faculty of business and management
National Research University «Higher School of Economics», Moscow

THE DEVELOPMENT OF METHODS AND TECHNIQUES FOR MANAGING THE PROCESS OF IDENTIFYING SIGNS OF CORRUPT BEHAVIOR OF PROCUREMENT PARTICIPANTS USING INFORMATION AND ANALYTICAL SYSTEMS

Аннотация: В статье рассматривается коррупционное поведение участников государственных закупок в России и предлагаются меры для выявления коррупционного поведения. На примере анализа конкретных закупок авторы разрабатывают конкретную методику выявления незаконных способов проведения тендерного аукциона и приходят к выводу, что для качественной оценки незавершенной закупки на предмет недобросовестной конкуренции можно опираться на 4 основных критерия (частота победы одного и того же поставщика, наличие связей между участниками, средний процент понижения от начальной максимальной цены контракта и проверка тендерной документации), а для оценки уже состоявшей закупки – 3 критерия (начальная максимальная цена контракта, срок подписания итогового и оценка дополнительных условий закупки по контракту).

Abstract: The article discusses the corrupt behavior of participants in public procurement in Russia and suggests measures to identify corrupt behavior. Using an example of an analysis of specific purchases, the authors develop a specific methodology for identifying illegal methods of conducting a tender and conclude that, for a qualitative assessment of unfinished procurement, unfair competition can be based on 4 main criteria (frequency of victory of the same supplier, presence of connections between participants, the average percentage of decrease from the initial maximum price of the contract and verification of tender documentation), and 3 criteria to evaluate an already completed purchase (initial maximum price of the contract, the signing date of the final and the assessment of additional terms of purchase under the contract).

Ключевые слова: Государственные закупки; коррупция; противодействие коррупции; безопасность бизнеса; конкуренция; мониторинг коррупции.

Keywords: State procurements; corruption; combating corruption; business security; competition; corruption monitoring.

Введение

Ни для кого не секрет, что коррупция является одним из главных тормозов развития российской экономики. Одной из причин, из-за которой сложно минимизировать коррупционные действия в стране, является само определение коррупции.

Есть две трактовки: узкая и широкая. В узком понимании под коррупцией предполагают подкуп-продажность представителей власти. Однако сторонники широкой трактовки концентрируют внимание на корыстном поведении должностного лица, тем самым можно охватить довольно широкий круг коррупционных деяний.

По данным международной неправительственной организации Transparency International, которая опубликовала ежегодный рейтинг стран по уровню восприятия коррупции за 2017 год, Россия находится на 135 месте среди 180 возможных [1]. По словам Михаила Гришанкова, депутата Государственной думы 3 – 5 созывов (1999 – 2011 гг.), сфера госзакупок является наиболее коррумпированной в России. Государство несет существенные потери в данной сфере. Сегодня большое количество госзакупок осуществляется с заранее известным «победителем». Из-за отсутствия конкуренции и непрозрачности системы госзакупок очень сильно страдает бизнес и другие сферы в экономике.

Стоит отметить, что госзакупки в РФ регламентируются ФЗ № 44. Данный закон был принят в 2013 году, однако многие его положения вступали в юридическую силу только через годы, этот процесс продолжается и сегодня. Цель данного акта – улучшить эффективность финансирования, в связи с чем были утверждены разные виды закупок в зависимости от категорий поставщиков и выдвигаемых к объекту торгов требований [2].

Особенности сферы государственных и муниципальных закупок

В зависимости от способа информирования и участия заказчиков различают открытые и закрытые госзакупки.

По ФЗ №44 установлены такие способы закупок:

- конкурентные – предусматривают наличие нескольких поставщиков продукции или исполнителей услуг;
- приобретение необходимых для нужд государственных и муниципальных органов товаров или услуг у единственного поставщика или подрядчика.
- В свою очередь конкурентные способы разделяются на:
- конкурсы (открытый, с ограниченным участием, двухэтапный, закрытый с ограниченным участием, закрытый двухэтапный);
- аукционы (электронный аукцион, закрытый аукцион);
- запрос котировок;
- запрос предложений.

При размещении государственных и муниципальных заказов в большинстве случаев подразумевается наличие конкурентной среды, где объективно определяется наилучшее предложение из поступивших. Но, как показывает практика, в некоторых случаях ответственные сотрудники заказчиков пользуются своими полномочиями для обеспечения победы конкретного участника заказа, пообещавшего наибольшие «комиссионные» со сделки (в СМИ также часто используется «откат»).

Коррупционные риски могут возникнуть в любой стадии государственных и муниципальных закупок. Храмкин А. А. в книге «Противодействие коррупции в госзакупках» определяет следующие основные этапы процесса закупок: формирование заказа, размещение заказа и исполнение контрактов [3]. Останавливаясь поподробней на каждом из них, автор определяет, благодаря какими путями образуется возможность проявления коррупционного поведения участников закупок.

На стадии формирования заказа коррупционные риски возникают при:

- определении приоритетов заявок государственных заказчиков на закупку;
- исследовании приоритетов рынка;
- выборе способа размещения заказа;
- формировании плана-графика закупок.
- На этапе размещения заказа коррупционные риски возникают:
- в ходе разработки документации;
- при размещении извещения о закупке;
- в период подготовки заявок участниками;
- на процедуре вскрытия конвертов с заявками;
- при рассмотрении заявок;
- в процессе оценки и сопоставлении заявок;
- при заключении контракта.

На этапе исполнения контракта коррупционные риски возникают:

- при администрировании контракта;
- при приемке объекта закупок;
- в гарантийный период.

Некоторые из этих признаков будут обсуждаться в кейсах. Стоит отметить, что данные факторы являются основными, но не единственными. Существуют другие различные признаки, которые специфичны для конкретной отрасли, региона или ведомства.

Объем взяток и нецелевых расходов в сфере госзакупок в России примерно составляет 1 трлн руб. в год, а это почти 20% от ежегодного объема закупок для государственных нужд [4].

На закупках по завышенным ценам государство в 2016 году потеряло около 180 миллиардов рублей (2,68 процента от всего объема заказов). Об этом говорится в ежегодном Национальном рейтинге прозрачности закупок.

Самая большая доля закупок по максимальной цене, говорится в исследовании, на федеральном уровне – 35,8 процента. У региональных и муниципальных закупок этот показатель составляет около 29,7 процента [5].

В 2011 году прокуроры выявили и пресекли более 33 тыс. нарушений законодательства на рынке госзакупок. В результате к административной и дисциплинарной ответственности привлечены 9,3 тыс. человек [1].

В начале апреля Минфин сделал заявление: только 4% госзакупок в России проводится на конкурентной основе. Остальные 96 – это закупки у единственного поставщика или с применением «иных способов» (см. Рисунок 1).

Об этом сообщает ТАСС со ссылкой на годовой отчёт министерства финансов. Это значит, что доля конкурсов с реальной конкуренцией за выполнение заказов государственных структур составляет всего 3,6 процента [6].

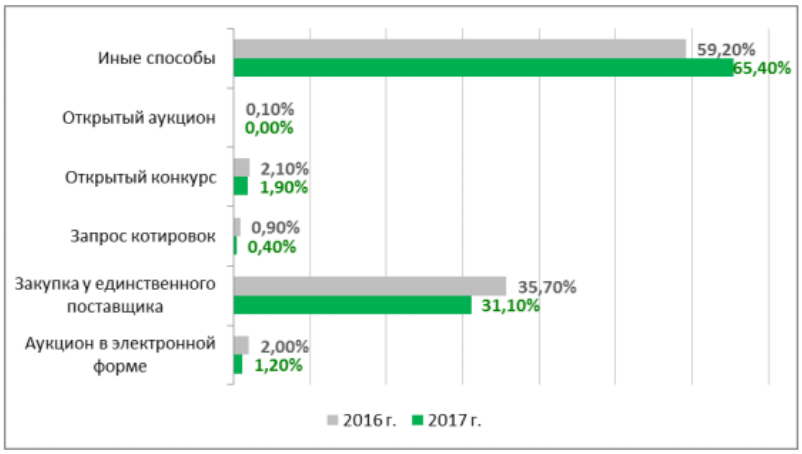


Рисунок 1. Закупки в разрезе способов их осуществления

Технология выявления признаков коррупционного поведения

Всего предложено два типа технологии. В первом случаем мы рассматриваем технологию, которая используется для анализа закупок, которые объявлены, но еще не проведены. Другая технология представляет анализ уже проведенных закупок.

Начнем с технологии до проведения закупок. У нас есть 4 критерия, после прохождения которых закупки попадают в зону риска. После этого организатор, имея список подозрительных закупок и используя конечный критерий, сможет подтвердить или отклонить гипотезу о наличии коррупции. При подтверждении гипотезы у организаторов будут неопровержимые доказательства для подачи аргументированной жалобы в ФАС.

Перейдем к самим критериям. Самый главный и первый признак наличия коррупция – это выявление связей между участниками закупок. Связи могут быть между заказчиком и участником закупки, между двумя участниками закупок и так далее. При нахождении какой-либо из этих связей мы переходим к следующему критерию.

Вторым критерием является средний процент понижения от начальной максимальной цены контракта. Обычно, стоимость госзаказа в результате честных конкурентных торгов снижается на 20-30% – такой позиции, в частности, придерживаются эксперты ФАС РФ. В итоге получаем два возможных сценария развития коррупциогенных событий:

- когда снижение НМЦК минимально (0,5%–1%);
- когда снижение НМЦК слишком большое (от 40-50% и выше).

В случае с большим понижением может наблюдаться демпинг, но данная ситуация не говорит о наличии коррупционной составляющей. Закупки с понижением менее 20% могут вызывать подозрения в отсутствии конкуренции. Если мы видим такие закупки, то переходим к следующему критерию.

Третьим критерием является частота побед одного и того же исполнителя. Если частота побед в той связи, которую мы обнаружили, повторяется часто, то это может свидетельствовать о недобросовестном поведении и наличии коррупционной составляющей и в таком случае мы двигаемся в нашем анализе дальше.

Четвертым критерием является закупка у единственного поставщика. Включение данного критерия в наш анализ может исказить его и в итоге мы получим недостоверную информацию, поскольку в подобных закупках присутствует естественная монополия. Для примера возьмем ПАО «ОАК». Он является материнской компанией почти всех авиастроительных корпораций в России. Одной из дочерних компаний является ПАО «ИЛ». Между этими двумя компаниями постоянно проводятся закупки у единственного поставщика на разработку новых самолетов. Если рассматривать эту ситуацию с точки зрения нашей технологии, то обе компании можно назвать коррумпированными, но, так как здесь присутствует определенная монополия, такой вывод делать нельзя. Таким образом, мы не включаем в наш анализ закупки у единственного поставщика, поскольку это является отдельной темой для обсуждения и исследования.

Если определенная закупка прошла по всем критериям, то она переходит в зону риска и в список подозрительных закупок, что позволяет использовать следующий критерий – проверка документации. Этот критерий говорит о возможных барьерах, которые можно проследить в документации закупки. Основные моменты, на которые нужно обращать внимание:

- Срок исполнения контракта по 44 ФЗ, индикатором этой коррупционной схемы являются подозрительно малые сроки исполнения контракта;
- Срок оплаты контракта. Можно говорить о недобросовестности закупки, если срок оплаты превышает 30 или 15 дней, в зависимости от требований к исполнителю;
- Гарантийные обязательства исполнителя. Если в контракте указаны заведомо малые сроки гарантийных обязательств, это наталкивает на мысль, что к исполнителю не предъявляются достаточно строгие требования и качество исполнения работ не играет роли;
- По техническим заданиям проведенных закупок достаточно точно можно оценить нацеленность заказчика на недобросовестную и коррумпированную сделку с подставным лицом.

После того, как исследуемая закупка прошла по первым четырем критериям и попала в зону риска, а далее прошла по критериям документации и были обнаружены барьеры для добросовестных поставщиков, организаторы, члены закупочные комиссии, аналитики, участники закупок могут обращаться в ФАС с аргументированной жалобой.

Теперь же представим технологию, которая поможет выявить признаки коррупции по уже проведенным закупкам. Всего есть три основных критерия, которые помогут это сделать.

Первый – это заниженная или завышенная начальная максимальная цена контракта. Таким образом, начальная цена контракта может:

- превышать среднюю рыночную стоимость продукции закупки. Если НМЦК была определена некорректно умышленно, то заказчик планирует заработать на этом деньги («распилить»);
- быть ниже средней рыночной стоимости продукции закупки. Если заказчик в документации указал НМЦК ниже среднерыночной стоимости продукции, то возможно некачественное выполнение условий контракта. Если это было сделано умышленно, то, вероятнее всего, часть работ просто не будет выполнена, а такая низкая цена была назначена для того, чтобы отсечь других исполнителей от участия в закупке.

Получаем, что, как заниженная, так и завышенная цена НМЦК служит поводом для подачи жалобы в ФАС РФ, так как это говорит либо о коррупционной составляющей, либо о некомпетентности заказчика.

Перейдем ко второму критерию. После подписания контракта с исполнителем может выясниться, что заказчику необходимо дополнительно закупить определенные позиции из контракта у данного поставщика, что естественно увеличит цену. Если данный показатель превышает 10%, то исследуемая закупка носит недобросовестный характер, что опять таки является поводом для подачи жалобы.

Третий критерий – это подписание контракта и акта выполненных работ т. е. сколько прошло времени после подписания контракта до приема результатов выполненной работы. Краткий фактический срок выполнения работ подрядчиком явно указывает на недобросовестность проведенной закупки. Скорее всего такая закупка уже была выполнена и только потом по ней проводится закупка.

После того, как закупка не удовлетворила хотя бы одному из этих критериев, можно обращаться в ФАС с аргументированной жалобой.

Таким образом, была представлена технология до проведения закупки и после. Данную технологию можно автоматизировать для выявления подозрительных закупок, что очень сильно упростит работу организаторам на торговых площадках.

Анализ закупки № 0348100073418000079
Предмет закупки: Оказание дератизационных, дезинсекционных и дезинфекционных услуг
Заказчик: ФГБУ «НИИ ЦПК ИМЕНИ Ю.А.ГАГАРИНА» (ИНН 5050077618)
Цена контракта: 500 000,00 руб.
Обеспечение заявки: 5 000,00 руб. (1 %)
Обеспечение контракта: 150 000,00 руб.

В данной закупке мы применим технологию до проведения закупок. В первую очередь обратимся к критерию выявления связей между участниками закупок. Было найдено 199 связей (цепочек) между заказчиком и поставщиком. Рассмотрим один из примеров (см. Рисунок 2).

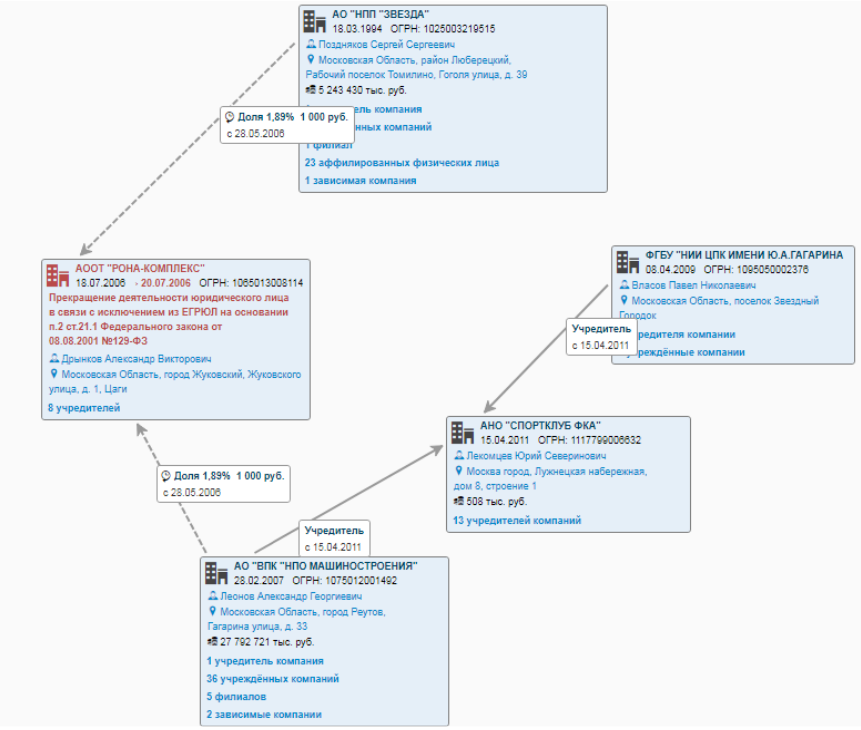


Рисунок 2. Поиск связей между поставщиком и заказчиком

Несложно разглядеть некоторую аффилированность, поэтому переходим ко второму критерию. Заказчик завершил 2743 закупок в сумме на 8,5 млрд. рублей. Средний процент снижения цены – 12,1 %, что несколько ниже нормального, по мнению экспертов ФАС, показателя в 20-30%. Однако можно увидеть, что средний доступ к торгам составляет 94%, и это можно считать хорошим показателем (см. Рисунок 3).

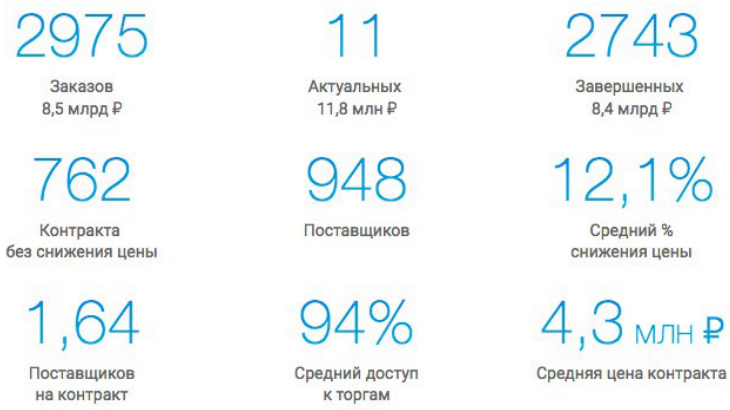


Рисунок 3. Данные о заказчике

Посмотрев на последние завершенные заказы компании (см. Рисунок 4), мы можем увидеть, что в каждом из них принимало небольшое количество поставщиков (1-3), а цена была понижена (0 – 25,49%). Процент понижения цены в отдельно взятой сделке высок.

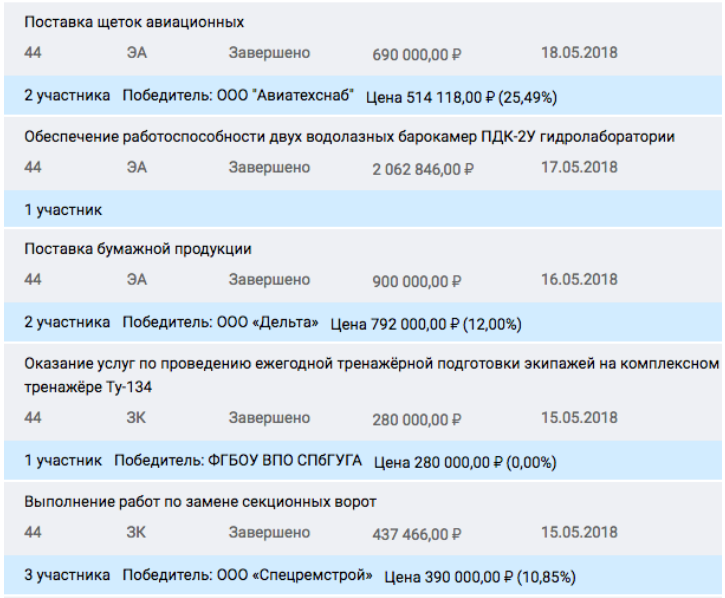


Рисунок 4. Последние завершенные заказы ФГБУ «НИИ ЦПК ИМЕНИ Ю.А.ГАГАРИНА»

Средний процент понижения довольно низок, так что есть смысл перейти к третьему критерию. Можно увидеть, что у данного заказчика есть поставщики с большим количеством участия в аукционах и долей побед в 80-93% (см. Рисунок 5). Тем не менее, некоторые из этих компаний можно считать естественными монополиями в своих сферах из-за специфичности их деятельности. Об этом свидетельствует диапазон 0-1,6 % снижения цены. Несомненно, на это необходимо обратить внимание.

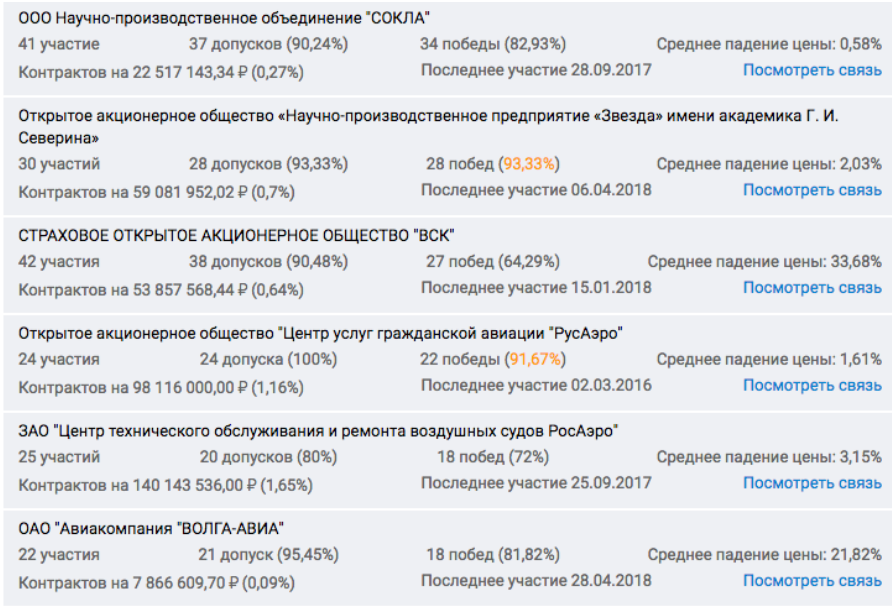


Рисунок 5. Поставщики с большой долей побед в аукционах

Присутствуют поставщики с огромным процентом побед и крохотным снижением цены, так что двигаемся дальше. В аукционах данного заказчика принимали участие и компании, которые были единственным поставщиком практически во всех заявках заказчика, например, ОАО «Научно-производственное предприятие «Звезда» имени академика Г. И. Северина». 30 раз компания участвовала в аукционах, 28 раз из них она одерживала победу, в том числе 27 раз – была единственным поставщиком, со средним падением цены в 2,03% (см. Рисунок 6).

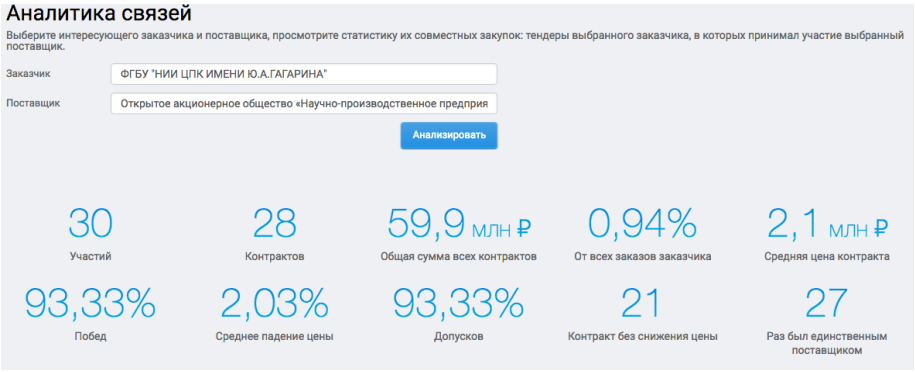


Рисунок 6. Связи заказчика с поставщиком ОАО «Научно-производственное предприятие «Звезда» имени академика Г. И. Северина»

В 1 случае из 28 побед в закупке принимала участие еще 1 компания. Цены не указаны, поскольку победа была одержана без снижения цены контракта (см. Рисунок 7).

Участник	Цена	Дата и время подачи	Решение комиссии
Общество с ограниченной ответственностью Научно-производственное объединение "СОКЛА"	-	06.11.2014 в 13:23	Соответствует
Открытое акционерное общество «Научно-производственное предприятие «Звезда» имени академика Г. И. Северина»	-	11.11.2014 в 09:11	Соответствует

Рисунок 7. Информация о контракте

Большое количество закупок у единственного поставщика искажает анализ в рамках нашей технологии, поэтому его надо приостановить. У организаторов закупок есть весомые причины подавать жалобу, а у поставщиков – не участвовать в этой закупке.

Анализ закупки №: 0848300048418000420

Предмет закупки: Оказание услуг по ликвидации стихийных свалок, сбору и вывозу мусора с территории сельского поселения Молоковское Ленинского муниципального района.

Заказчик: МБУ «ДОРСЕРВИС» (ИНН 5003115016)

Цена контракта: 3 000 492,29 руб.

Обеспечение заявки: 30 004,92 руб. (1%)

Обеспечение контракта: 900 147,69 руб. (3%)

В данной закупке мы применим технологию до проведения закупок. В первую очередь обратимся к критерию выявления связей между участниками закупок. Было найдено 3 связи (цепочек) между заказчиком и поставщиком. Рассмотрим один из примеров (см. Рисунок 8).

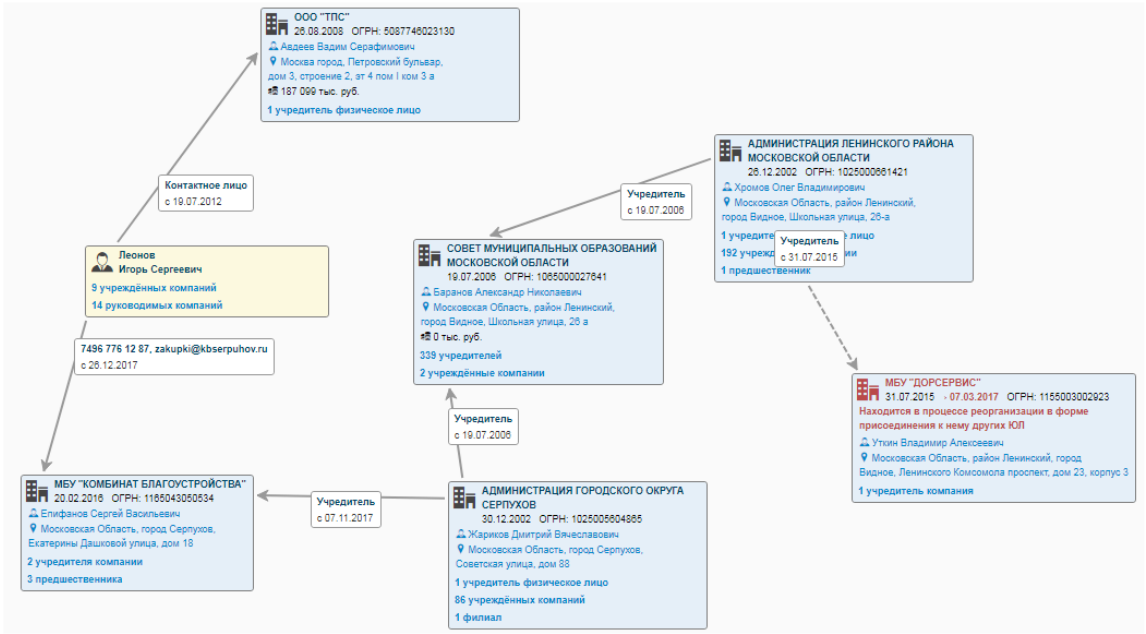


Рисунок 8. Схема аффилированных лиц

Определенных связей совсем немного, но, тем не менее, они присутствуют, поэтому обратимся ко второму критерию. Заказчик завершил 430 закупки в сумме на 1,2 миллиарда рублей (см. Рисунок 9). Несмотря на высокий доступ к торгам (98,2%), во всех закупках принимали участие всего 173 поставщика, средний процент снижения цены небольшой – 16,7%, показатель количества поставщиков на 1 контракт тоже можно считать удовлетворительным (2,67).

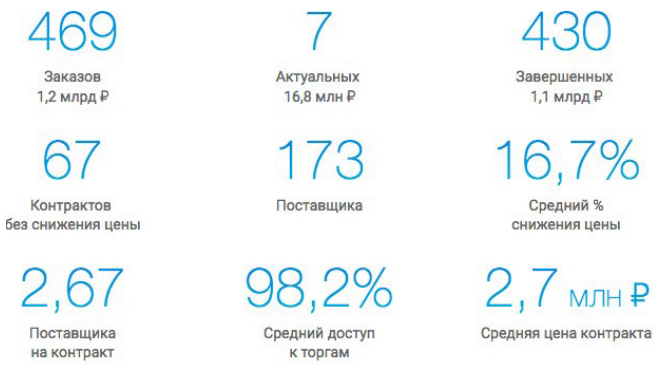


Рисунок 9. Анализ заказчика

Средний процент понижения выглядит довольно неудовлетворительным, поэтому мы двигаемся дальше. Мы видим, что в аукционах данного заказчика некоторые компании принимали участие 9-40 раз. Среднее падение цены всегда ниже нормального (от 0 до 16,7%), и процент побед этих фирм неоднозначный (от 39,29% до 100%). При этом данные организации не являются монополиями в своих сферах, так что, скорее всего, между заказчиком и этими исполнителями возможна коррупционная связь (см. Рисунок 10).

ООО ПК «Экодор»			
40 участий	40 допусков (100%)	29 побед (72,5%)	Среднее падение цены: 15,46%
Контрактов на 148 744 496,59 ₽ (13,04%)		Последнее участие 03.05.2018	Посмотреть связь
ООО "ЦЕНТР МАТЕРИАЛЬНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ"			
14 участий	14 допусков (100%)	13 побед (92,86%)	Среднее падение цены: 1,26%
Контрактов на 14 832 715,36 ₽ (1,3%)		Последнее участие 07.06.2017	Посмотреть связь
ООО 'СВЕТСТРОЙ'			
14 участий	14 допусков (100%)	12 побед (85,71%)	Среднее падение цены: 3,07%
Контрактов на 50 746 886,27 ₽ (4,45%)		Последнее участие 07.11.2017	Посмотреть связь
ООО "ТЕХСТРОЙ"			
28 участий	28 допусков (100%)	11 побед (39,29%)	Среднее падение цены: 9,6%
Контрактов на 80 049 233,77 ₽ (7,02%)		Последнее участие 10.05.2018	Посмотреть связь
МУНИЦИПАЛЬНОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ ГОРОДСКОГО ПОСЕЛЕНИЯ ВИДНОЕ ЛЕНИНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА МОСКОВСКОЙ ОБЛАСТИ "ВИДНОВСКИЙ ТРОЛЛЕЙБУСНЫЙ ПАРК"			
11 участий	11 допусков (100%)	9 побед (81,82%)	Среднее падение цены: 8,38%
Контрактов на 2 460 078,23 ₽ (0,22%)		Последнее участие 24.01.2018	Посмотреть связь
ООО "СК Аделэнд-XXI"			
13 участий	13 допусков (100%)	9 побед (69,23%)	Среднее падение цены: 14,35%
Контрактов на 29 390 097,34 ₽ (2,58%)		Последнее участие 03.05.2018	Посмотреть связь
ООО «Технологический Процессинг и Сервис»			
9 участий	9 допусков (100%)	9 побед (100%)	Среднее падение цены: 10,75%
Контрактов на 39 185 192,64 ₽ (3,44%)		Последнее участие 03.04.2018	Посмотреть связь

Рисунок 10. Поставщики с наибольшим числом побед в аукционах

Рассмотрим закупки с участием ООО «Технологический Процессинг и Сервис» (см. Рисунок 11). 100% побед, при этом всего 1 раз был единственным поставщиком, минимальный показатель среднего падения цены (10,75%).

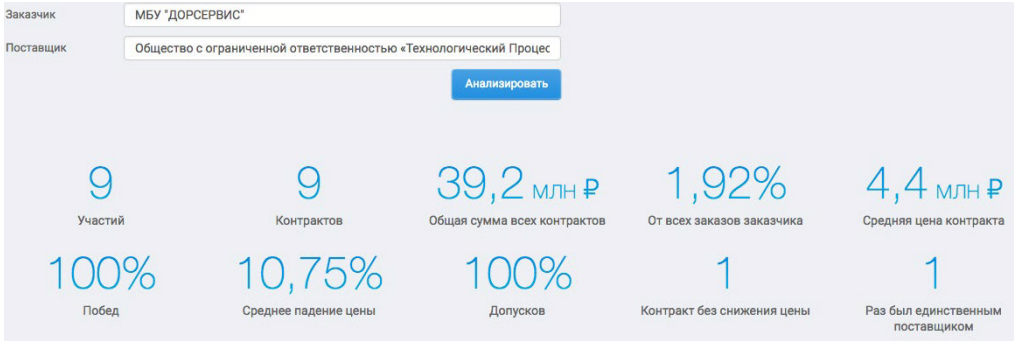


Рисунок 11. Связи заказчика с поставщиком ООО «Технологический Процессинг и Сервис»

В целом можно утверждать, что частота побед одних и тех же исполнителей выше среднего. Закупки у единственного поставщика заказчик устраивает не очень часто, поэтому этот критерий мы пропускаем. В целом, есть немало аргументов, чтобы перевести данную закупку в зону риска, поэтому будем проверять документацию.

Дата проведения аукциона – 18 июня 2018 года, сроки на исполнение контракта – с момента заключения контракта до 31.12.2018. Оплата производится Заказчиком в срок, не превышающий 30 (тридцати) дней со дня подписания Заказчиком Акта сдачи-приемки услуг. В гарантийных сроках нет необходимости. Начальная максимальная цена контракта определена в соответствии с «Методическими рекомендациями по применению методов определения начальной (максимальной) цены контракта», утвержденной приказом Министерства экономического развития РФ от 02.10.2013г. N 567 с применением метода сопоставимых рыночных цен (анализа рынка). Нарушения стиля в документации отсутствуют.

Техническое задание составлено достаточно подробно, но при этом всё ТЗ занимает примерно 3 страницы, к каждой позиции не приведены единицы измерения и их необходимое количество. Также было обнаружено отсутствие в документации Формы-2, что говорит о низких барьерах входа на аукцион и как следствие - высокой конкуренции.

Вывод: несмотря на хорошую документацию к аукциону, есть некоторая причина полагать, что заказчик данной закупки коррумпирован, а именно, наблюдается многократное сотрудничество с одними и теми же поставщиками, аффилированность с ними, низкий процент снижения максимальной цены, высокая доля побед некоторых поставщиков и малое количество поставщиков на один контракт.

Анализ закупки № 0373200014218000519

Предмет закупки: Поставка оборудования для сбора и хранения отходов при выполнении работ по благоустройству дворовых территорий.

Заказчик: ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ «ЖИЛИЩНИК РАЙОНА ДОРОГОМИЛОВО

Цена контракта: 4 225 000, 00 руб.

Обеспечение заявки: 84 500, 00 руб.

Обеспечение контракта: 1 267 500, 00 руб.

Здесь также будет применена технология до проведения закупок. Начнем с критерия аффилированности. Внимание привлекла компания ООО «О-РСИ», имеющая 47,62% побед. У данной компании есть только один заказчик и это ГБУ «ЖИЛИЩНИК РАЙОНА ДОРОГОМИЛОВО». (см. Рисунок 12). В своих самых первых контрактах компания понижала цену на 8-47 % от первоначальной, в последних же контрактах понижение цены составляет 1-1,5%. Это может говорить о возможной договоренности поставщика с данным заказчиком.

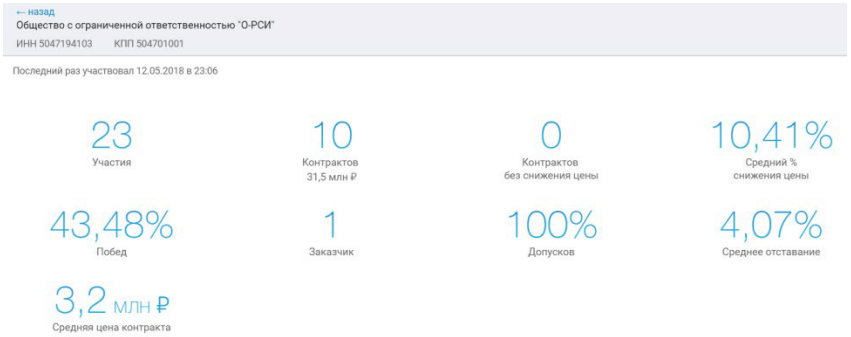


Рисунок 12. Характеристика компании ООО «О-РСИ»

В закупках, где победила ООО «О-РСИ» также постоянными участниками являлись ООО «ИБ ЗЕЛЕНЫЙ ДВОР», ООО «МАСТЕРОК», «СТРОЙИНВЕСТСЕРВИС». В 4 из 6 закупок с 2 участниками вторым претендентом являлась компания «ООО «МАСТЕРОК», в каждой из этих закупок побеждал ООО «О-РСИ», отклонения в цене у обеих компаний составляли 0,5-1,5%. Однако связей между этими компаниями обнаружено не было.

Ситуация с первым критерием выглядит довольно очевидно, поэтому можно смело двигаться ко второму. Заказчик завершил 337 закупок в сумме на 5,4 млрд. рублей. Средний процент снижения цены – 15,5 %, что достаточно близко к нормальному, по мнению экспертов ФАС, показателю в 20-30%. Средний доступ к торгам составляет 99,5%, и это можно считать отличным показателем (см. Рисунок 13).

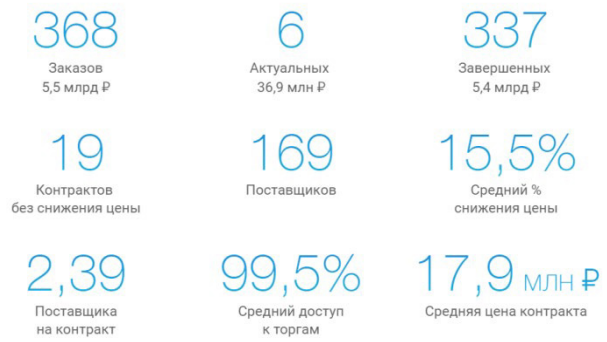


Рисунок 13. Данные о заказчике

Посмотрев на последние завершенные заказы компании (см. Рисунок 14), мы можем увидеть, что в каждом из них принимало небольшое количество поставщиков (1-3), а цена была понижена (0 – 25,49%). Процент понижения цены в отдельно взятой сделке высок.

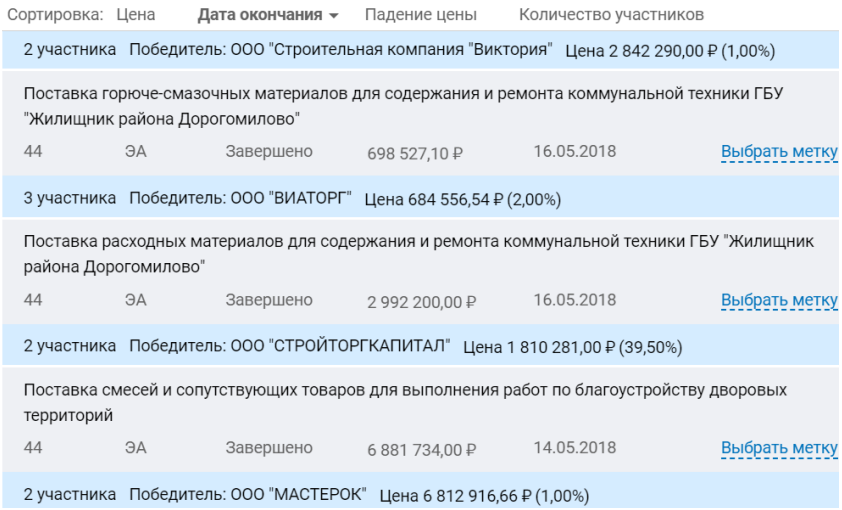
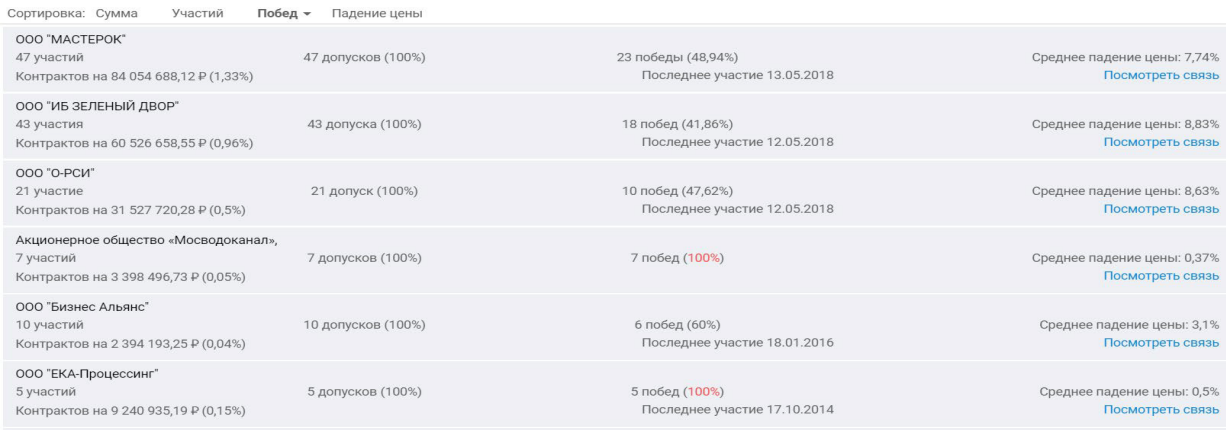


Рисунок 14. Последние завершенные заказы ГБУ «ЖИЛИЩНИК РАЙОНА ДОРОГОМИЛОВО»

В целом, процент снижения ниже приемлемого, поэтому двигаемся дальше. Можно увидеть (см. Рисунок 15), что у данного заказчика есть поставщики с большим количеством участия в аукционах, но их доля побед составляет 40-60%, что не является критичным показателем. Есть и несколько заказчиков с долей побед 100%, однако некоторые из этих компаний можно считать естественными монополиями в своих сферах из-за специфичности их деятельности. Об этом свидетельствует диапазон 0-0,5 % снижения цены.



Сортировка: Сумма | Участий | **Побед** | Падение цены

ООО "МАСТЕРОК" 47 участий Контрактов на 84 054 688,12 ₽ (1,33%)	47 допусков (100%)	23 победы (48,94%) Последнее участие 13.05.2018	Среднее падение цены: 7,74% Посмотреть связь
ООО "ИБ ЗЕЛЕНЫЙ ДВОР" 43 участия Контрактов на 60 526 658,55 ₽ (0,96%)	43 допуска (100%)	18 побед (41,86%) Последнее участие 12.05.2018	Среднее падение цены: 8,83% Посмотреть связь
ООО "О-РСИ" 21 участие Контрактов на 31 527 720,28 ₽ (0,5%)	21 допуск (100%)	10 побед (47,62%) Последнее участие 12.05.2018	Среднее падение цены: 8,63% Посмотреть связь
Акционерное общество «Мосводоканал», 7 участий Контрактов на 3 398 496,73 ₽ (0,05%)	7 допусков (100%)	7 побед (100%)	Среднее падение цены: 0,37% Посмотреть связь
ООО "Бизнес Альянс" 10 участий Контрактов на 2 394 193,25 ₽ (0,04%)	10 допусков (100%)	6 побед (60%) Последнее участие 18.01.2016	Среднее падение цены: 3,1% Посмотреть связь
ООО "ЕКА-Процессинг" 5 участий Контрактов на 9 240 935,19 ₽ (0,15%)	5 допусков (100%)	5 побед (100%) Последнее участие 17.10.2014	Среднее падение цены: 0,5% Посмотреть связь

Рисунок 15. Поставщики с наибольшим количеством побед

Идем далее к четвертому критерию. В аукционах данного заказчика практически нет закупок, в которых принимал участие только один поставщик, а если и были, то только у естественных монополий, таких как Мосводоканал. В целом мы можем с натяжкой добавить эту закупку в зону риска и все-таки проверить документацию.

Явных нарушений, связанных с анализом документов закупки, обнаружено не было. Исполнитель оказывает услуги в течение 10 календарных дней от даты заключения настоящего Контракта, что является коротким сроком. Расчеты за оказанные услуги производятся в срок не более 15 (пятнадцати) банковских дней с момента подписания акта приемки-передачи товара заказчиком. Гарантия на поставляемый товар должна быть не менее двенадцати месяцев с момента поставки, что является обыкновенным сроком для данного типа продукции. Предмет закупки сформулирован достаточно чётко, хотя обнаружен расхождение по количеству с предметов закупки по ТЗ и по НМЦК. В ТЗ указана закупка 3 предметов: шкаф для ТБО – 5 шт., Шкаф для приема и хранения ТБО контейнерный герметичный, с педальным приводом крышек люка – 51 шт., Шкаф для хранения противогололедных материалов – 14 шт. В НМЦ указан расчет стоимости для 56 шкафов для приема и хранения ТБО контейнерный герметичный (51 шт.+ 5 шт.). Непонятно, зачем в техническом задании прописаны требования для обоих шкафов, если в итоге расчет приводится для шкафов второго типа.

Также в самом ТЗ совершенно не прописаны требования для предмета «Шкаф для хранения противогололедных материалов», не указан его объем и примерные характеристики. Однако его расчет стоимости приведен в НМЦ. Такие расхождения скорее всего могут указывать на недостаточную проработанность и возможную спешку при оформлении ТЗ. Также было обнаружено отсутствие в документации Формы-2. Не достаточная детализация и отсутствие Формы-2 говорит о низких барьерах входа на аукцион и как следствие - высокой конкуренции.

Все вышеперечисленные факторы скорее говорят о достаточной конкурентности данной закупки. Таким образом, на основании анализа можно выделить одно важное нарушение – отсутствие четкого описания объекта закупки в техническом задании и отсутствие документации Формы-2. Из-за чего возможны конфликты и даже судебные разбирательства с поставщиком.

IV. Заключение

В данной работе была предложена методика для выявления признаков коррупционного поведения участников закупок с применением информационно-аналитических систем, разработаны меры, помогающие внешнему лицу оценить добросовестность закупки, то есть оценить риски при принятии управленческого решения. На реальных примерах была представлена реализация

предложенного механизма, выделены 4 ключевых фактора, свидетельствующие о коррупционной составляющей в текущей закупке и 3 ключевых фактора, свидетельствующие о коррупционной составляющей в уже исполненной (завершенной) закупке.

Статья будет полезна сотрудникам службы безопасности предприятия, тендерных и юридических отделов компании, поскольку помогает провести качественный и комплексный анализ потенциальных контрагентов, то есть минимизировать риск принятия неверного управленческого решения о начале сотрудничества, сократить или свести на «нет» экономический ущерб фирме от принятия неверного решения, оценить риски работы с конкретным участником аукционных закупок.

Список литературы

1. Храмкин, А. А. Противодействие коррупции в госзакупках. 2 изд. СПб.: Российская академия государственной службы при Президенте РФ, Институт подготовки кадров для системы государственных и муниципальных закупок (Институт госзакупок РАГС), 2012.
2. Коррупция: где она живет и процветает // ВЦИОМ - Режим доступа: http://wciom.ru/index.php?id=459&uid=113417
3. Минфин: только 4% госзакупок в России проводится на конкурентной основе // 5 канал - Режим доступа: https://www.5-tv.ru/news/194348/
4. Разновидности тендерных закупок // О-тендере - Режим доступа: http://otendere.com/zakupki/informaciya-zakupki/raznovidnosti-tendernyx-zakupok.html
5. Россия в Индексе восприятия коррупции – 2017: посадки не помогли // Трансперенси Интернешнл - Режим доступа: https://transparency.org.ru/research/indeks-vospriyatiya-korruptsii/rossiya-v-indekse-vospriyatiya-korruptsii-2017-posadki-ne-pomogli.html
6. Ущерб от госзакупок по завышенным ценам оценили в 180 миллиардов рублей в год // Meduza - Режим доступа: https://meduza.io/news/2016/12/07/uscherb-ot-goszakupok-po-zavyshennym-tsenam-otsenili-v-180-milliardov-rubley-v-god

КОСТРОМИН ЕВГЕНИЙ ВЛАДИМИРОВИЧ
студент факультета права
НИУ ВШЭ, г. Москва
E-mail: evkostromin96@gmail.com

ЗАГАДОЧНЫЙ БИТКОИН: БЛАГО ИЛИ ВСЕМИРНАЯ УГРОЗА?

KOSTROMIN EVGENY VLADIMIROVICH
student, faculty of law
National Research University «Higher School of Economics», Moscow

THE MYSTERIOUS BITCOIN: GOOD OR GLOBAL THREAT?

Аннотация: В настоящей статье анализируются некоторые преимущества (легкость совершения операций, свобода от регулирования и т.д.) и недостатки биткоина. Под сомнение ставится наличие полной анонимности пользователей биткоина. Среди прочих недостатков особо выделяются: (1) высокая волатильность курса, (2) уязвимость для хакерских атак и мошенничества. Делается вывод о нецелесообразности интеграции биткойна в современную экономику России.

Abstract: In this article there's an analysis of the advantages (the ease of committing operations, freedom of regulation, etc.) and disadvantages of the bitcoin. Being put into question is the lack of full anonymity of the users of the bitcoin. Among other disadvantages particularly stands out the following ones: (1) high volatility of the course, (2) vulnerability to hacker attacks and fraud. The conclusion made about the inexpediency of integration of the bitcoin in Russian economy.

Ключевые слова: биткоин, криптовалюты, цифровая экономика, цифровое право, риски, анонимность, волатильность, преимущества, правовая природа биткоина

Keywords: bitcoin, crypto-currencies, digital economy, digital law, risks, anonymity, volatility, advantages, bitcoin's legal nature

Идея о том, что биткойну присуща
какая-то особая ценность — просто шутка
Уоррен Баффет [1]

В настоящее время тематика, связанная с технологией блокчейн и криптовалютами, невероятно актуальна и популярна в мировом масштабе: ведутся дискуссии о целесообразности легализации биткоина; разрабатывается множество Интернет-проектов с использованием альткойнов; ведутся споры о правовой природе биткоина (это разновидность электронных (цифровых) денег, фиатные деньги, материальная вещь (товар), ценная бумага или современный правовой феномен, требующий отдельной нормативно-правовой регламентации?)[2].

На мой взгляд, всё вышесказанное — хаос и хайп. Но что в итоге? в итоге, в нашей стране криптовалюта не легализована, отсутствует чёткое определение криптовалюты (в проекте ФЗ о криптовалютах Минфина, дано понятие криптовалюты как «цифрового финансового актива», которым, при этом, нельзя расплачиваться на территории РФ [3]).

Тем не менее, представители государственной власти, чиновники различного уровня систематически лестно отзываются о криптовалютах (Президент [4], Премьер-министр [5]). Кроме того, Центробанк уже несколько месяцев пытается создать крипторубль [6]. Отмечу: ЦБ РФ, делая различные заявления относительно криптовалюты, всё чаще называет биткойн «цифровым товаром» [7], тогда как Минфин относит криптовалюту к «иному имуществу» [8], ссылаясь на ГК РФ.

Возникает закономерный вопрос: что есть биткойн? Придуманный кучкой мошенников «пузырь», обречённый лопнуть уже в очень скором времени или неиссякаемое «электронное золото», благо XXI века, которое необходимо развивать и оберегать (стоимость биткойна на 29 ноября 2017 г. была баснословно велика: $11441 тысяч [9]; достигнув в 20-х числах февраля 2018 г. отметки в $12000 тысяч, уже вчера 26.02.2018 курс биткойна упал ниже $10000 тысяч [10])?

Со своей стороны, крайне осторожно и большим недоверием отношусь к миру криптовалют, поэтому в данной работе считаю целесообразным поставить и проанализировать проблему рисков при явных преимуществах биткойна.

Так, каковы же основные преимущества исследуемого феномена.

Поскольку биткойн не требует регистрации и/или идентификации, то первая его ценность — анонимность (пользователю не надо передавать какие-либо персональные данные в процессе идентификации или сведения об объекте покупки третьим лицам); второе преимущество — децентрализованный характер (тут всё понятно: никакого контроля (в т.ч. со стороны государства) над биткоин-транзакциями нет и быть не может); математические расчёты составляют основу существования биткойна и в этом его основная ценность (соглашусь, математика не есть ценность физического мира или авторитет какого-либо государственного органа (вспоминаем фиатные денежные ресурсы, которые не защищены от инфляции, в то время как биткоин защищён по вышеназванной причине); при использовании биткоина не нужно платить никаких обязательных комиссий за перевод криптовалюты (т.е. транзакционные издержки весьма малы, например, можно сравнить отправку биткойна с отправкой почты с возможностью установления минимальной суммы, причитающуюся тому майнеру, создавшему успешно функционирующий блок для данной транзакции); по своей сути биткойн — феномен, функционирующий в глобальных масштабах, что в свою очередь обеспечивает весьма простую процедуру осуществления платежей по всему миру, по сути, в любое место; кроме того, платежи в рамках системы биткойн — окончательны и неоспоримы [11; 490–492].

Если безоговорочно верить сторонникам криптовалюты биткойн, то получается, что криптовалюты выступают действенным средством обретения свободы в банковско-экономическом плане, ведь лишь при участии финансовых посредников (банков) субъект может вступить в экономические отношения, а криптовалюты — не результат эмиссионной деятельности банков, т.к. создаются майнером (по сути, любым желающим компьютерным пользователем).

Но так ли всё безоблачно на самом деле? Неужели при использовании биткойна нет никаких рисков и угроз для плательщика?

Во-первых, ни одна криптовалюта (в т.ч. биткойн) не обеспечивает высокий уровень анонимности участника сделки.

Безусловно, нельзя отрицать, что мир криптовалют крайне закрыт, даже замкнут по сравнению с привычными нам валютами. Однако, считаю, что этот факт не означает, что пользователи криптовалюты биткойн никак не сообщаются с внешним миром. Майнеры интересуются не только валютами, но и товарами особо рода: оружием, наркотическими веществами и т.п. Что логично в силу вышеназванных преимуществ. Тем не менее, существует точка зрения, что между внешним и внутренним миром криптовалют всегда есть особые «коридоры», которые программисты могут вычислить и тем самым идентифицировать непосредственно тех, кто использует «коридоры» [12].

Таких примеров уже весьма много: недавно турецкая полиция, применив вышеописанный способ, предотвратила крупное вымогательство, связанное с биткоином [13]; в 2013 г. ФБР США раскрыла организацию «Шёлковый путь», которая торговала наркотическими веществами, используя биткоин [14].

По данным агентства Bloomberg, объем похищенных мошенниками цифровых монет за примерно последние 10 лет составляет сумму $1,2 млрд (десятая часть вложенных в криптовалюту денег) [15]. Японская криптовалютная биржа Coincheck была взломана хакерами в начале февраля текущего года: похищена криптовалюта NEM на сумму в $530 млн [16].

Кроме того, бытует мнение, что биткоин придумал и обосновал совсем не Сатоши Накамото [17] (отмечу: никто никогда его не видел; признанный факт: данное имя является псевдонимом,

т.е. это может быть не один учёный, а целая группа таковых), а был разработан в лабораториях США, т.е. понятно: если принять к сведению данный факт, то анонимность участников закономерно ставится под сомнение [18]. а 29 ноября 2017 г. суд в США вынес решение, которое лишний раз доказывает, что анонимность и криптовалюты — понятия несовместимые: криптовалютная биржа Coinbase теперь обязана предоставить все данные 14000 пользователей названной биржи налоговому управлению США [19]. и о какой супер-анонимности может идти речь?

Как уже о тмечалось, Центробанк разрабатывает крипторубль. Но обладают ли криптовалюты признаками, характерными для денег? На мой взгляд, нет, хотя, безусловно, вопрос сложнейший и крайне дискуссионный. Некоторое время назад под феноменом денег понимали непосредственно товар, сегодня же данный «товар» утратил связь с драгоценными металлами, поэтому сейчас принято считать деньги «знаком» (фидуциарные (фиатные) деньги). При этом, общепризнанным является факт, что деньги — измеритель стоимости товаров и услуг.

Возникает закономерный вопрос: в состоянии ли выполнять названную функцию криптовалюта биткоин? Ответ, к сожалению, отрицательный, что объясняется крайне высокой волатильностью биткойна по сравнению с иными обычными валютами. Эмиссия биткойна началась в 2009 г. и тогда данная криптовалюта обменивалась на доллар США по курсу: 1 биткойн = 0,01 цента. Затем, в течение весьма короткого промежутка времени покупательная способность криптовалюты биткойн стабильно росла: сначала за неё давали несколько долларов США, затем несколько десятков. а в 2013 г. биткойн стал оцениваться в 1000 долларов США. Как я уже отмечал, в ноябре 2017 г. зафиксирован абсолютный рекорд: 1 «монета» оценивается в целых 20000 долларов США. Согласитесь, какая-то невероятная космическая скорость роста обменного курса по отношению к обычной валюте, в частности, к американскому доллару. Данный факт не может не настораживать: становится непонятно, как можно использовать такую «цифровую валюту» в качестве меры стоимости?

Отмечу, для биткойна характерны не только стабильные (относительно) и резкие взлёты обменного курса, но и внезапные весьма ощутимые падения. Например, называется цифра в плюс-минус 20% от среднего значения [20]. Сразу вспоминается июнь-июль 2017 г., когда в июне биткойн оценивался в 3000 долларов, а в июле показатели резко упали до 1300 долларов США.

Такова волатильность биткойна, и она крайне высокая. При этом, отмечу: подобная волатильность характерна и для альткойнов. На мой взгляд, основная причина таких показателей следующая: обычные деньги в отличие криптовалюты биткойн напрямую связаны непосредственно с товарами, которые выступают мощным регулятором, способствующим уравнению валютных курсов.

Все вышеназванные факты свидетельствуют о том, насколько несовершенен биткоин. Несовершенства порождают мошенничество. Криптовалюта биткойн — не исключение: риски утраты криптовалюты путём кражи, различных мошеннических схем и иных обстоятельств, не зависящих от майнера, весьма велики. Если майнер не знает личность контрагента, то не исключено, что последний не выполнит своё обязательство, например, оплаты товара, при этом, никакой механизм компенсаций ещё не разработан [21; 493].

Кроме того, стоит помнить, что утрата виртуальных единиц может быть не только вследствие мошенничества, хакерских атак, но и банальной неисправности или потери компьютерного средства, что тоже является своего рода риском.

Резюмируя, важно сделать следующие выводы.

1. Сделки с биткойном — крайне рисковая деятельность, никак не регулируемая (сейчас) на законодательном уровне. Безусловно, некоторые преимущества майнинга назвать можно, но и они, как выяснилось, весьма дискуссионные.
2. Биткойн не обеспечивает высокого уровня анонимности участникам сделок.
3. Биткойн — не деньги, т.к. не в состоянии выполнять функцию измерителя стоимости товаров и услуг в силу его крайне высокой волатильности.
4. Волатильность криптовалюты биткойн несравнимо выше, чем у обычной валюты.
5. Риски утраты биткойна вследствие мошеннических действий велики.

Не может не настораживать тот факт, что разработкой крипторубля занимаются организации, регулирующие оборот денежных средств. Однако, на фоне довольно большого числа негативных высказываний в доктрине относительно целесообразности легализации биткойна, такие организации, к сожалению, игнорируют их: процесс разработки продолжается. Считаю: денежные власти должны заниматься непосредственно деньгами, а биткойном должно заниматься, как минимум, новое ведомство.

Считаю, самый главный вывод: криптовалюта по своей сути — новый инструмент азартной игры: слишком уж велик простор для мошенничества (по крайней мере сейчас).

Импонирует сравнение В.Ю. Катасонова: регулирование оборота биткойна денежными властями — регулирование оборота наркотиков: и то, и другое необходимо запрещать в силу идентичности их сущности [22].

Итак, криптовалюты — если не всемирная, то национальная угроза точно. Биткойн — своего рода проигрыш денежных властей, которые слишком много внимания уделяют биткойну в ущерб национальной валюте, фактически признавая биткойн деньгами, что спорно.

Убеждён: разработав правила использования криптовалют с оглядкой, в частности, на европейский, японский, австралийский, американский опыт, ЦБ РФ, Минфин и иные вовлечённые в процесс организации нанесут очередной серьёзный удар по российскому рублю. Нужно ли это российской экономике и без того переживающей не самые лучшие времена? Не думаю.

Список использованной литературы: Уоррен Баффет: ценность биткоина — «просто шутка» // CoinCpot.io. URL: https://coinspot.io/analysis/uorren-baffet-cennost-bitcoina-prosto-shutka/ (дата обращения: 25.11.2017).

6. Янковский Р.М. Почему юристы никак не договорятся о криптовалютах // Geektimes. URL: https://geektimes.ru/post/290953/%2C+vkontakte%2BclubIP_CLUB/ (дата обращения: 25.11.2017).
7. Проект Федерального закона «О цифровых финансовых активах» (подготовлен Минфином России) (не внесен в ГД ФС РФ, текст по состоянию на 25.01.2018) // СПС «Консультант Плюс».
8. Путин: без цифровой экономики у страны нет будущего // РИА Новости. URL: https://ria.ru/economy/20170615/1496585016.html (дата обращения: 25.11.2017).
9. Могилевская А. Медведев призвал задуматься о регулировании блокчейна // РБК. URL: https://www.rbc.ru/economics/17/05/2017/591c28259a79471d2ecbbf7b (дата обращения: 25.11.2017).
10. ЦБ РФ начал работу над созданием виртуальной национальной валюты // ИНТЕРФАКС. URL: http://www.interfax.ru/forumspb/564986 (дата обращения: 25.11.2017).
11. ЦБ РФ предложил рассматривать криптовалюты как цифровой товар // ИНТЕРФАКС. URL: http://www.interfax.ru/business/563859 (дата обращения: 25.11.2017).
12. Минфин предложил регулировать криптовалюты как «иное имущество» // РИА Новости. URL: https://ria.ru/economy/20170608/1496121430.html (дата обращения: 25.11.2017).
13. Стоимость биткоина за два дня превысила 11 тысяч долларов // РИА Новости. URL: https://ria.ru/economy/20171129/1509866263.html (дата обращения: 29.11.2017).
14. Биткоин снова ниже 10 000$, криптовалюты в небольшом плюсе // Stock Markets Group. URL: http://stock-maks.com/analitika-i-prognoz-kriptovalyut/35896-bitkoin-snova-nizhe-10-000-kriptovalyuty-v-nebolshom-plyuse.html (дата обращения: 26.02.2018).
15. Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд. М.: Статут, 2016. С. 490–492.
16. «Финансы по Катасонову» №12. Что такое криптовалюты? // YouTube. URL: https://www.youtube.com/watch?v=wiHcPvdsffs (дата обращения: 26.11.2017).
17. Турецкая полиция поймала банду похитителей владельцев биткоинов // Bits.Media. URL: https://bits.media/news/turetskaya-politsiya-poymala-bandu-pokhititeley-vladeltsev-bitkoina/ (дата обращения: 26.11.2017).

18. Биткоины, изъятые у владельца криминального сайта «Шелковый путь», ФБР хранит в интернет бумажнике blockchain // CryptoRussia. URL: https://cryptorussia.ru/zametki/bitkoiny-izyatye-u-vladelca-kriminalnogo-saytashelkovyy-put-fbr-hranit-v-internet-bumazhnike (дата обращения: 30.11.2017).
19. Kharif O. Hackers Have Walked Off With About 14% of Big Digital Currencies // Bloomberg. URL: https://www.bloomberg.com/news/articles/2018-01-18/hackers-have-walked-off-with-about-14-of-big-digital-currencies (дата обращения: 10.02.2018).
20. Хакеры ограбили криптовалютную биржу // Euronews. URL: http://ru.euronews.com/2018/01/27/cryptocurrency-exchange-hacked?utm_source=ip_club%2C+vkontakte&utm_term=ip%2Bclub&utm_campaign=IP_CLUB (дата обращения: 10.02.2018).
21. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. P. 3 // Bitcoin.org. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 25.11.2017).
22. «Финансы по Катасонову» № 12. Что такое криптовалюты? // YouTube. URL: https://www.youtube.com/watch?v=wiHcPvdsffs (дата обращения: 26.11.2017).
23. Суд обязал криптобиржу Coinbase предоставить налоговой США данные 14 тысяч пользователей // VC.ru. URL: https://vc.ru/29901-sud-obyazal-kriptobirzhu-coinbase-predostavit-nalogovoy-ssha-dannye-14-tysyach-polzovateley (дата обращения: 30.11.2017).
24. «Финансы по Катасонову» № 12. Что такое криптовалюты? // YouTube. URL: https://www.youtube.com/watch?v=wiHcPvdsffs (дата обращения: 03.03.2018).
25. Савельев А.И. Указ. соч. С. 493.
26. «Финансы по Катасонову» №12. Что такое криптовалюты? // YouTube. URL: https://www.youtube.com/watch?v=wiHcPvdsffs (дата обращения: 03.12.2017).

ЦАПЕШ АЛЕКСАНДА
выпускница факультета бизнес и менеджмента
НИУ ВШЭ, г. Москва
E-mail: tsapeshsasha@mail.ru

АНАЛИЗ ДЕЯТЕЛЬНОСТИ ОДНОГО ИЗ ЛИДЕРОВ МИРОВОЙ ИНДУСТРИИ БЕЗОПАСНОСТИ НА ПРИМЕРЕ КОМПАНИИ ADT INC

TSAPESH ALEXANDRA
Bachelor Alumni, faculty of business and management
National Research University «Higher School of Economics», Moscow

ANALYSIS OF THE ACTIVITIES OF ONE OF THE LEADERS IN THE GLOBAL SECURITY INDUSTRY ON THE EXAMPLE OF ADT INC

Аннотация: Темой данной статьи является анализ мировой корпорации АДТ – Американ Дистрикт Телеграф, входящую в холдинг Аполло Холдинг Менеджмент, который приобрел компанию в феврале 2018 года за 7$ млрд. Анализ компании заключался в исследовании компании через определение сферы ее деятельности, анализ предоставляемых услуг и обзор кейса, который представляет собой проблемы, с которой столкнулась компания в ходе своей деятельности, а также деятельность компании на сегодняшний день.

Abstract: The subject of this article is an analysis of the global ADT Corporation -American District Telegraph, part of the Apollo Global Management holding, which acquired the company in February 2016 for $ 7 billion. The analysis consisted in the study of the company through the definition of its scope of activities, analysis of the services provided and a review of the case, which represents the problems that the company has faced in the course of its activities, also the company's current activities.

Ключевые слова: электронная безопасность, индустрия безопасности, ADT

Keywords: electronic security, security industry, ADT.

Введение

Проанализировав большое количество ресурсов на тему лидерства в сфере безопасности, ключевым фактором при выборе компании ADT для исследования было то, что эта компания славится одним из первых мест в рейтинге мировых лидеров на рынке предоставления услуг безопасности и контроля жизнедеятельности, а также номером один на европейском рынке. Однако, ее рынок не ограничивается Европой и Америкой - спектр продукции представлен еще на Ближнем Востоке и в Африке, и включает в себя охранные сигнализации, кабельное телевидение, системы видеонаблюдения, контроля доступа, противокражные системы, системы контроля перемещений, противопожарные системы, а также комплексные решения по обеспечению безопасности.

При выборе компании для исследования я руководствовалась не только рейтингами, а также масштабами компании и благополучностью ее деятельности - ADT является огромной корпорацией с общей численностью сотрудников более 100 000 человек, а также с количеством потребителей, превышающих количество 7,5 млн более чем из 100 стран.

ADT Corporation (ADT) является американской компанией, которая занимается разработкой и установкой систем электронной безопасности, интерактивного дома и деловой автоматизации, а также услуг наблюдения и контроля для физических лиц и бизнеса, в Соединенных Штатах

и Канаде. До 2016 года ADT входила в состав Tyco Fireand Security, которая является крупнейшим в мире поставщиком решений по безопасности бизнеса и противопожарной безопасности. в феврале стало известно, что фонд Apollo Global Management приобрел компанию за $7 млрд.

Практическая значимость моей работы заключается в анализе современной компании ADT (American District Telegraph Company), входящую в холдинг Apollo Global Management. Основное содержание работы содержит в себе исследование этой компании на рынке предоставления услуг безопасности через подробное определение сферы ее деятельности, анализ предоставляемых услуг и обзор кейса – проблемы, с которой столкнулась компания в ходе своей деятельности.

Было бы несправедливо не упомянуть тот факт, что подобный анализ этой компании в формате исследования еще не проводился (к этому выводу я пришла после подробного поиска в интернете этой тематики) – в этом заключается новизна моей работы.

Введение в историю

История компании ADT берет своё начало в далеком 1874 году с появлением нового технического телекоммуникационного прибора - телеграфа. в конце 19 века, когда телеграф стал использоваться в коммерческих целях, стало возможно его использование в обеспечение безопасности собственности. Система работала таким образом, что офисы компаний могли отправлять в определенное время в офис ADT сигнал, который означал, что все в порядке и помощи не требуется. Как только такого сигнала не поступало – это означало, что случилась непредвиденная ситуация и требуется помощь, тогда сотрудники ADT оперативно оказывали необходимые действия включая связь с отделением полиции. с быстрым развитием технологий ADT не стояла на месте, и постепенно добавляла новые дополнения в перечень своих услуг – так они добавили категории продуктов для охранно-пожарной сигнализации в 1910 гг. к 1930 году компания ADT стала лидером в области охранного мониторинга.

Вторая мировая война стала катализатором прогресса в области охраны и безопасности – в эти года остро ощущалась нехватка человеческих ресурсов, что вызвало необходимость в автоматизации процессов передачи сигнала и последующей реакции. в результате компания стала первой в разработке систем Teletherm - автоматических систем охранно-пожарной сигнализации.

В своем роде компания ADT является важнейшим первооткрывателем в сфере безопасности. Так уже в 1970 году они установили первую автоматическую центральную станцию ADT, ставшей прямой предшественницей сегодняшней интеллектуальной интегрированной сети для мониторинговых центров.

В 1990-х гг. продолжался технологический прорыв, начатый в 1980-х, с активным внедрением таких направлений, как беспроводные системы, контроль доступа и системы видеонаблюдения.

Уже в 1990 году случилось важное событие в жизни компании – впервые количество потребителей перевалило за 1 миллион человек. Стоит отметить, что с 1964 года компанией активно поглощаются мелкие участники рынка для завоевания большой доли этого сектора. в этом же году ADT была признана монополией, так как обслуживали 80% всего рынка, так как они устанавливали цены ниже среднего, что ставило в невыгодное положение конкурентов. в некоторых городах, таких как Нью-Йорк и Мемфис, штат Теннесси, они были единственным поставщиком. ADT был вынужден принять национальный прейскурант, который не мог быть изменен, чтобы помочь создать конкурентов центральной станции в городах без конкуренции и выплатить штрафы и тройной ущерб федеральному правительству, клиентам и местным конкурентам.

В 2002 году филиалы Великобритании и Центральной Европы объединили свои усилия для увеличения объемов поставки широкого спектра продуктов и услуг на территории всей Европы, образовав единую ADT Europe, как подразделение компании Tyco Fire and Security, в свою очередь входящую в международный холдинг Tyco International. Таким образом, за более чем сто лет своего развития ADT стала бесспорным лидером в индустрии электронных систем безопасности.

ADT сегодня

На сегодняшний день компания ADT обладает мощнейшей клиентской базой в 7,5 млн человек. Компания предлагает свои продукты в основном под брендом ADT и ADT Pulse для частных клиентов, в том числе владельцев домов для одной семьи, а также для розничных предприятий, поставщиков продуктов питания и напитков, медицинских офисов и клиник, механических и автомобильных магазинов, профессиональных поставщиков услуг и небольших коммерческих объектов, различных сфер бизнеса, а также государственным структурам. Под защиту компании ADT входят более 5 млн домов по всему миру, 300 мировых аэропортов и защита около 80% морских судов мира. Помимо этого, ADT являлась официальным спонсором летних Олимпийских игр в 1996 г. в Атланте и зимних Олимпийских игр 2002 г. в Солт-Лейк-Сити. Создание и поддержка такой гигантской системы были бы невозможным без продуманной внутренней структуры компании. в ее владения входят 35 производственных площадок, 1200 офисов более чем в 100 странах мира, более 600 новых и улучшенных продуктов ежегодно, 950 ученых, инженеров-исследователей и разработчиков, а также 33 000 сервис-инженеров. Этот бизнес приносит около 11$ млрд ежегодно. Штаб-квартира компании находится в Бока-Ратон, штат Флорида.

Контролируемые компанией системы безопасности и предложения для автоматизации дома и бизнеса включают в себя установку и мониторинг безопасности жилых и деловых помещений и систем автоматизации помещений, предназначенных для обнаружения вторжений, контроля доступа и реагирования на движение, дым, угарный газ, наводнения, температуру и другие условия окружающей среды и опасностей, а также для решения проблем, связанных с личными чрезвычайными ситуациями, таких как травмы, неотложная медицинская помощь или нетрудоспособность. Он также предоставляет различные альтернативные и резервные методы передачи сигналов тревоги, включая сотовый и широкополосный Интернет; центр мониторинга оказал поддержку персональным системам реагирования на чрезвычайные ситуации; и обслуживание клиентов для обслуживания и установки модернизированного или дополнительного оборудования.

После подробного изучения сайта компании я определила точный спектр услуг, предоставляемые потребителям:

- домашние системы безопасности (в том числе пожарная и спасательная);
- домашние услуги автоматизации;
- обнаружение окиси углерода;
- информационная безопасность;
- удаленный доступ и автоматические дверные замки;
- пользовательские системы домашней безопасности (в том числе пожарная и спасательная);
- домашние системы здравоохранения;
- домашнее видеонаблюдение;
- домашнее дистанционное интерактивное управление и системы автоматизации;
- обнаружение вторжений в бизнес;
- бизнес-видеонаблюдение;
- управление электронным доступом в бизнесе;
- дистанционное интерактивное управление и системы автоматизации в бизнесе.

Помимо этого, есть возможность отдельно приобрести товары и продукты для самостоятельного видеонаблюдения.

Компания ADT несомненно гордиться своей столетней историей, тем самым влияя на лояльность потребителей – это подтверждает отдельные страницы сайта с историей бренда, а также с отзывами своих клиентов.

У компании четко отработанный план продаж, они также предоставляют бесплатную установку своих систем в течение 1 дня после подписания контракта.

Обзор кейса

В 2015 году компания ADT столкнулась с проблемой недостаточной защищенности соб-

ственных данных. Суть иска состоит в том, что поставляемое компанией беспроводное охранное оборудование использует незащищённую передачу данных и потому может быть взломано злоумышленниками. Несмотря на то, что иск был подан лишь одним пользователем, в нем шла речь о всей базе данных клиентов. в исковом заявлении приводятся цитаты из статьи, опубликованной в журнале Forbes в июле 2014 года — согласно материалам журналистского расследования, анонимный испытатель для получения полного доступа к беспроводным системам ADT использовал прибор, купленный в магазине бытовой электроники за десять долларов. в результате перехвата коммуникации злоумышленник получает возможность отключить охранную систему в нужный момент либо вести наблюдение за обстановкой в охраняемом жилище в собственных интересах. Основанием для обращения в суд истец счёл два ложных вызова полиции в результате ошибочных срабатываний охранной сигнализации, установленной ADT по контракту.

ADT оказались в ситуации, когда их рекламные посты об абсолютной безопасности собственности и информации шли вразрез с действительностью. Так как в региональных законах штата Иллинойс (где был подан иск) есть статья о недобросовестных практиках в торговле, то компанию обязали выплатить истцу от $15 либо $45, в зависимости от того, сколь долго он был клиентом ADT.

Эксперты особо выделяют тот факт, что, несмотря на широкую распространённость услуг ADT в США, не зафиксировано ни одного случая, когда хакеры действительно использовали уязвимость её систем охранной сигнализации. Таким образом, ADT заплатила не за ущерб, полученный клиентами, а за его потенциальную возможность.

Заключение

Сегодня о компании ADT пишут мировые СМИ, она по праву считается гигантом и лидером в индустрии безопасности. Проанализировав сайт, я сделала выводы, что у компании ADT внушительная репутация, которая подкреплена многолетней корпоративной культурой – это побуждает не только постоянно наращивать базу новых потребителей, а также и возвращаться к ним вновь и вновь уже давних клиентов. Они ежедневно работают над усовершенствованием собственных услуг и продукции, что делает их на шаг дальше от конкурентов.

Сфера деятельности компании сегодня заключается в производстве продукции систем контроля перемещений объектов, комплексных систем безопасности, которые объединяют системы контроля доступа, системы видеонаблюдения и мониторинга и противокражные системы, системы RFID и оборудование для применения в программе UPP. Решения ADT используются для защиты людей, потребительских товаров и недвижимости. Дополнительно к этому ADT предлагает также продукцию и услуги для противопожарной защиты.

Подводя итоги кейса, можно сказать, что компании ADT еще есть куда расти и совершенствовать защиту и безопасность данных своих потенциальных клиентов, однако, несмотря на это, фактических случаев взлома их систем безопасности никогда не было – это говорит о высоком уровне профессионализма и уровне ответственности перед клиентами.

Список использованных источников и литературы:

1. Энциклопедия брендов: ADT [Электронный ресурс]: Журнал «Системы безопасности» #3, 2006 г. URL: http://www.lib.tsu.ru/win/produkzija/metodichka/6_6.html
2. Company Overview of The ADT Corporation [Электронный ресурс]: BLOOMBERG. URL: https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=184157327
3. The ADT Corporation [Электронный ресурс]: Wikipedia, the free encyclopedia URL: https://en.wikipedia.org/wiki/The_ADT_Corporation
4. ADT Home Security [Электронный ресурс]: главная страница компании. URL: https://www.adt.com/
5. Security News [Электронный ресурс]: Информационно-аналитическое издание по техническим средствам и системам безопасности. URL: http://www.secnews.ru/foreign/23429.htm#axzz5EB61LQfD

ЧЕРНЫШЕВА АННА ДМИТРИЕВНА
студентка факультета социальных наук
НИУ ВШЭ, г. Москва
E-mail: annadchernysheva@gmail.com

МОШЕННИЧЕСТВО КАК СОСТАВ УГОЛОВНО НАКАЗУЕМОГО ДЕЯНИЯ В ОТЕЧЕСТВЕННОМ ПРАВЕ

CHERNYSHEVA ANNA DMITRIEVNA
student, faculty of social sciences
National Research University «Higher School of Economics», Moscow

FRAUD AS A PART OF A CRIMINAL ACT IN NATIONAL LEGISLATION

Аннотация: С развитием общества и информационных систем растет количество способов осуществления мошеннических действий. На сегодняшний день применяется мошенничество с помощью банковских карт, компьютерных систем (через вредоносное ПО), фишинговые сайты. в статье представлена теоретическая база и схема мошеннического деяния, рассмотрена история мошенничества в России, современные методы, а также правовые основы темы и уголовная ответственность за мошеннические действия. в заключении приведены рекомендации по тому, как обезопасить себя и организацию от злоумышленников.

Abstract: With the development of society and information systems, the number of ways to perform fraudulent activities is growing. Today, frauds using bank cards, computer systems (via malware), phishing sites are used. The article presents the theoretical basis and scheme of a fraudulent act, considers the history of fraud in Russia, modern methods, as well as the legal basis of the topic and criminal liability for fraudulent actions. The conclusion contains recommendations on how to protect yourself and your organization from intruders.

Ключевые слова: мошенничество в УК РФ, фишинг, скимминг, ливанская петля.

Keywords: fraud in the Criminal Code of the Russian Federation, phishing, skimming, Lebanese loop.

Введение

Еще в Российской империи второй половины XIX века применялась практика привлечения к уголовной ответственности за преступления в экономической и финансовой сферах. в Уложении о наказаниях уголовных и исправительных (1869) [Таганцев, 2013] указано, что к уголовной ответственности привлекались лица, повинные в насильственным завладении или повреждении чужой собственности, а также ее хищения путем кражи, разбоя, грабежа и мошенничества. Таким образом, государство признавало частное имущество и защищало его с помощью определенных мер.

Значимость темы мошенничества для России обоснована тем, что российский бизнес зарождался в крайне некомфортных для этого условиях [Шульц, Юрченко, Рудченко, 2016]. Во времена становления рыночной экономики в 1990-е гг. государство столкнулось, помимо «шоковой терапии», с большим количеством макроэкономических угроз. Сюда относятся, кроме массового мошенничества, рэкет и шантаж, нечестная приватизация, хищения бюджетных средств в огромных масштабах, коррумпированность властных структур и тому подобные действия, вплоть до похищений и убийств бизнесменов и политиков. Эти особенности постсоветского периода связаны с повсеместным упадком морально-этических ценностей на фоне кризиса, девальвации, ми-

граций. Также произошло освобождение от жесткого административно-правового режима Союза, в результате чего все негативные силы смогли себя проявить.

Кроме того, чтобы осуществлять успешную практику защиты предприятия от различных угроз и овладеть методами противодействия им, необходимо в полной мере осознавать состав мошенничества, знать все тонкости государственного регулирования данного вопроса, меры наказания.

Целью моей работы является выявить, какие способы противодействия мошенничеству наиболее эффективны в нашей стране. Для этого мною будут решены следующие задачи:

- проанализировать нормативно-правовые документы касаемо мошенничества;
- выявить виды мошенничества и охарактеризовать их;
- взглянуть на историю мошенничества в современной России;
- привести конкретные примеры мошеннических действий.

Правовая сторона вопроса

С 1997 года и по сей день ответственность за мошенничество регулируется Уголовным Кодексом, принятым 24 мая 1996г. (далее – УК 1996г.). Информация об уголовной ответственности содержится в разделе VIII УК РФ «Преступления в сфере экономики», главе 21 «Преступления против собственности».

В вышеуказанной главе мошенничество определяется как «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием». Меры наказания представлены в таблице 1.

В таблице 2 можно увидеть информацию о том, какой ущерб оценивается в качестве значительного, крупного и особо крупного.

На данный момент российское законодательство различает пять видов мошенничества:

1. в сфере кредитования – осуществляется через предоставление кредитору заведомо ложной или недостоверной информации.
2. при получении выплат – ложная информация при получении пособий, компенсаций, субсидий; сюда же относится утаивание фактов, способствующих прекращению этих выплат.
3. с использованием платежных карт – обман сотрудников кредитной/торговой/другой организации путем использования фальшивой или чужой платежной карты (кредитной, расчетной).
4. в сфере страхования – обман относительно наступления страхового случая или же размера выплаты.
5. в сфере компьютерной информации – овладение чужим имуществом через любое вмешательство (ввод, удаление, блокирование, изменение) в компьютерную информацию или влияние на информационно-телекоммуникационные сети и другие средства хранения, обработки, передачи данных.

Примечательно, что в отношении пунктов 1, 3, 4 и 5 действуют другие стандарты для оценки ущерба. Крупным считается имущество стоимостью более 1 500 000 рублей, а особо крупным – 6 000 000 рублей.

Степень тяжести / Меры наказания	Штраф	Обязат работы	Исправит. работы	Принудит. работы	Арест	Ограничч. свободы	Лишение свободы
Мошенничество	до 120 т.р. ИЛИ з/п за период до 1 года	до 360 ч	до 1 года	до 3-х лет	до 4-х мес.	до 2-х лет	до 2-ух лет
Группа лиц по предварительному стоворуЗначительный ущерб	до 300 т.р. ИЛИ з/п за период до 2-х лет	до 480 ч	до 2-х лет	до 5-и лет (с/без огр. св. до 1 года)	–	до 1 года или без такового	до 5-и лет (с/ без огр. св. до 1 года)
С использованием служебного положенияКрупный размер	100-500 т.р. ИЛИ з/п за период 1-3 лет	–	–	до 5-и лет (с/без огр. св. до 2-х лет)	–	до 2-х лет или без такового	до 6-и лет (с/ без штр. до 80 т.р. и огр. св. до 1,5 лет)
Организованная группаОсобо крупный размерЛишение права на жилье	лиш. св. + до 1 млн р. ИЛИ з/п за период до 3-х лет	–	–	–	–	до 2-х лет или без такового	до 10-и лет
Преднамеренное неисполнение договорных обязательств в сфере предпринимательской деятельности:							
Значительный ущерб	до 300 т.р. ИЛИ з/п за период до 2-х лет	до 480 ч	до 2-х лет	до 5-и лет (с/без огр. св. до 1 года)	–	до 1 года или без такового	до 5-и лет (с/ без огр. св. до 1 года)
Крупный размер	100-500 т.р. ИЛИ з/п за период 1-3 лет	–	–	до 5-и лет (с/без огр. св. до 2-х лет)	–	до 2-х лет или без такового	до 6-и лет (с/ без штр. до 80 т.р. и огр. св. до 1,5 лет)
Особо крупный размер	лиш. св. + до 1 млн р. ИЛИ з/п за период до 3-х лет	–	–	–	–	до 2-х лет или без такового	до 10-и лет

Таблица 1. Соотношение степени тяжести деяния и наказания за него. Составлена автором на основании ст.159 УК РФ

Название	Значительный	Крупный	Особо крупный
Размер, руб.	10 000 – 3 000 000	3 000 000 – 12 000 000	свыше 12 000 000

Таблица 2. Оценка ущерба. Составлена автором на основании ст.159 УК РФ

Структура мошенничества

Обратим внимание на объективную и субъективную стороны мошенничества. Из понятия, представленного в УК РФ, можно вычленить следующие характеристики мошеннических действий:

- изъятие имущества из владения собственника;
- корыстный умысел;
- противоправный характер деяния;
- безвозмездность изъятия;
- общественно опасные последствия.

Причем основными для субъективной стороны здесь являются первые два пункта, а именно – их взаимосвязь. Процесс изъятия собственности своеобразен тем, что жертва, смотря на вещи через призму измененного сознания, «добровольно» отчуждает свое имущество в пользу преступника. Также действие не может быть признано мошенническим, если лицо его осуществляющее (субъект) не осознает связи между собственными действиями и ущербом для другого человека. Иными словами, мошенником нельзя стать «случайно».

Из способов мошенничества нам известны обман и злоупотребление доверием. в обоих случаях целью выступает ввести человека в заблуждение, что мошенник действует в рамках закона и в интересах человека. Обман заключается в искажении действительности через предоставление заведомо ложных фактов или же сокрытие правдивых. Мошенник может предлагать поддельный товар, использовать несправедливые методы расчета. Злоупотребление доверием – это использование доверительных или должностных взаимоотношений при намерении незаконно завладеть имуществом или средствами собственника.

Стоит обратить внимание, что субъект всегда будет являться физическим лицом или группой лиц, в то время как потерпевший может быть как физическим, так и юридическим лицом (зависит от того, кому принадлежит объект посягательств). При этом понятие объекта мошенничества включает в себя не только сам предмет преступления (имущество), но и нематериальная составляющая – отношения собственности.

Мошенничество в России

Несмотря на то, что название дисциплины предусматривает рассмотрение угроз в сфере бизнеса, наверняка каждый в своей жизни не раз сталкивался с мошенниками. Возможно, кто-то даже от них серьезно пострадал. Обратимся к наиболее ярким примерам мошенничества в прошлом.

Нигерийское мошенничество – письма, поступавшие в Россию в начале 90-х годов, оповещавшие получателя о том, что он стал наследником большой суммы денег. Под предлогом вступления в право на наследство, злоумышленники требовали полную информацию о человеке (Ф.И.О., адрес проживания и работы, контактные телефоны и номера счетов), после получения которой заключали сделки от имени «наследника».

В 1990-х – 2000-х гг. были популярны финансовые пирамиды, в результате работы которых вкладчики теряли свои средства. Самой известной стала организация АООТ «МММ», основанная Сергеем Мавроди и обманувшая за свое существование около 10 млн человек.

На современном этапе развития технологий и общества наиболее опасными видами мошенничества можно назвать мошенничество с использованием магнитных карт и в сфере компьютерной информации, поэтому в своей работе я подробно рассмотрю именно их.

Все чаще люди пользуются именно картами, а не наличными деньгами. с появлением таких платежных систем, как ApplePay и SamsungPay, эта тенденция распространилась еще сильнее. Практически любую покупку, будь то продукты в супермаркете или частном магазине рядом с домом, доставка, услуга, покупка в режиме онлайн, можно оплатить с помощью банковской карты. Работодатели в основном перечисляют заработные платы на карты. с помощью карт можно оплатить счета или за секунды перевести кому-то деньги. Это значительно упрощает жизнь, но несет

и некоторые отрицательные последствия.

Пластиковые карты

Поговорим о нескольких распространенных способах мошенничества с использованием пластиковых карт [Бегишев, 2016]. Стоит обратить внимание, что многие из них сопряжены с преступлениями в сфере компьютерных данных. Дело в том, что, при введении информации в банкомат или заполнении формы на оплату, данные модифицируются.

Фишинг – это система похищения («выуживание») данных и средств через интернет и другие источники. Сюда относят использование бренда, например, поддельные сообщения или сайты, содержащие информацию о том, что пользователь выиграл в конкурсе/лотерее от компании Microsoft. Злоумышленники могут требовать отправить личные данные, отвечать на такие сообщения ни в коем случае нельзя. Существуют программы, которые выглядят так, будто защищают компьютер, но на самом деле генерируют ложные угрозы и пытаются завлечь в мошеннические транзакции.

Для защиты от фишинга можно отмечать подозрительные сообщения и веб-страницы при помощи Hotmail, Microsoft Office Outlook, фильтра SmartScreen. При ответе на фишинговое сообщение минимизировать потенциальный ущерб можно следующим образом:

1. сменить пароль и PIN-код во всех аккаунтах;
2. обратиться в банк или к финансовому консультанту, чтобы добавить предупреждение о мошенничестве в кредитные отчеты;
3. закрыть счета, если поступила информация о доступе к ним;
4. регулярно проверять банковские выписки и отчеты по операциям.

Следующий вид мошенничества – «ливанская петля». Небольшой отрезок фотопленки складывается особым образом и вставляется в банкомат так, чтобы не мешать проведению транзакции. Владелец вставляет карту и совершает операцию, в то время как рядом стоит человек, следящий за «жертвой» при наборе ПИН-кода. По окончанию операции владелец не может извлечь карту, в это время подходит мошенник и производит отвлекающий маневр. Когда владелец отходит от банкомата, мошенник достает карту и снимает деньги. Единственный способ избежать такой ловушки – быть максимально внимательным и минимально наивным, не поддаваться панике, если банкомат «зажевал» карту и ни в коем случае не оставлять его без присмотра до тех пор, пока карта не будет извлечена.

Огромные доходы мошенникам приносит скимминг. Скиммер – маленькое считывающее устройство, которое крепится к банкомату. с помощью него можно получить доступ ко всей информации, записанной на магнитной карте. Скиммером может быть специальная накладка на картридере или панели набора ПИН-кода, даже крохотная камера.

Устройство сложно обнаружить, поэтому стоит пользоваться банкоматами в отделениях, больших торговых центрах, на охраняемых территориях. Также преимущество имеют чиповые карты, так как скиммер не способен украсть информацию с чипа.

Компьютерная информация

Перейдем к преступлениям в сфере компьютерной информации. Мошенническое программное обеспечение оказывает деструктивное воздействие на компьютерные данные [Шульц, Юрченко, Рудченко, 2016]. к таким программам относят:

- баннеры (всплывающие окна);
- блокираторы (блокируют доступ в интернет, возможности операционной системы);
- шифровальщики (шифруют файлы и данные).

Сегодня существует множество программ, которые помогают выявлять подозрительные файлы, программы и сайты (защитные системы Microsoft, антивирусные программы, встроенные

функции браузеров). Однако даже они не способны обеспечить полную защиту данных. к тому же многие пользователи не имеют желания или возможности платить за антивирусные программы, тем самым подвергая себя еще большей опасности.

Вдобавок, возникают вопросы и проблемы с квалификацией мошеннических действий, связанных с компьютерными данными. Сложности квалификации могут быть редуцированы путем заполнения пробелов в российском законодательстве.

Заключение

Подводя небольшой итог, хотелось бы сказать о правилах поведения, которые помогут любому избежать попадания в ловушку мошенников:

1. Не паниковать. Мошенники часто пытаются загнать человека в состояние цейтнота. Создавая видимость, что времени на размышления нет, они вводят жертву в панику и заставляют принять нерациональные решения.
2. Всегда следует перепроверять информацию и лишний раз усомниться в достоверности данных.
3. Не стоит поддаваться обаянию и навыкам общения. Некоторые мошенники при общении с потенциальной жертвой настолько входят в роль, что люди безоговорочно верят им, находясь под влиянием собеседника.
4. Никому не сообщать своих личных данных (номер и серия паспорта, номер карты и счета, ПИН-коды и пароли). в случае их утечки реагировать максимально быстро.
5. Не пользоваться услугами непроверенных организаций и не покупать товары у подозрительных продавцов [Быкова и Изотов, 2015].

В плане общих рекомендаций для бизнеса (выбор контрагентов) можно выделить следующие:

- В организации должен быть разработан и закреплен разумный порядок выбора контрагентов, с которым должны быть ознакомлены сотрудники.
- Контрагенты должны отвечать экономическим и профессиональным требованиям, быть тщательно изучены.
- Действия по выполнению контракта необходимо контролировать и назначать справедливое наказание за невыполнение условий.

Список использованной литературы

1. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 19.02.2018, с изм. от 25.04.2018)
2. Таганцев Н. С. Уложение о наказаниях уголовных и исправительных. – Рипол Классик, 2013.
3. Шульц, В. Л. Безопасность предпринимательской деятельности в 2 ч. Часть 1 : учебник для академического бакалавриата / В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко ; под ред. В. Л. Шульца. — М. : Издательство Юрайт, 2018. — 288 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-02331-2.
4. Бегишев И. Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации // Вестник казанского юридического института МВД России. – 2016. – №3. – С. 112-117.
5. Быкова Н. Н., Изотов Д. С. Виды мошенничества с банковскими картами // Вестник НГИЭИ. – 2015. – №3. – С. 49-53.

ШВАРЦМАН АЛЕКСАНДРА ОЛЕГОВНА
студентка факультета права
НИУ ВШЭ, г. Москва
E-mail: aoshvarts@gmail.com

ИСПОЛЬЗОВАНИЕ САЙТА ФЕДЕРАЛЬНОЙ НАЛОГОВОЙ СЛУЖБЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В ИНТЕРЕСАХ КОНКУРЕНТНОЙ РАЗВЕДКИ

SHVARTSMAN ALEKSANDRA OLEGOVNA
student, faculty of law
National Research University «Higher School of Economics», Moscow

THE USE OF THE SITE OF THE FEDERAL TAX SERVICE OF THE RUSSIAN FEDERATION IN THE INTERESTS OF COMPETITIVE INTELLIGENCE

Аннотация: В данной статье рассмотрен механизм сбора информации с помощью сайта ФНС РФ в процессе осуществления деловой разведки. Выявлены и проанализированы основные виды информации, предоставленные сайтом ФНС РФ, и установлена значимость полученной информации в рамках оценки добросовестности контрагента. Особое внимание обращено на правовую составляющую последствий ведения бизнеса с юридическими лицами, недобросовестность которых подтверждена информацией с сайта ФНС РФ.

Abstract: The article is aimed to describe the mechanism for collection of information using the site of the Federal Tax Service in the process of conducting business intelligence. Tha article identify and analyze the main types of information provided by the site of the Federal Tax Service and the significance of the received information. Particular attention is paid to the legal component of the consequences of doing business with firms, the dishonesty of which is confirmed by information from the site of the Federal Tax Service of Russia.

Ключевые слова: деловая разведка, конкурентная разведка, проверка контрагента, добросовестность, ФНС РФ, бизнес, сбор информации, официальный источник

Keywords: business intelligence, competitive intelligence, counterparty checking, counterparty acting in a good faith, Federal Tax Service, business, collection of information, official source.

Гражданский кодекс РФ определяет предпринимательскую деятельность как самостоятельную, осуществляемую на свой риск деятельность, направленную на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг. Так, основной нормативно-правовой акт РФ, направленный на регулирование отношений в сфере предпринимательской деятельности, устанавливает такой критерий предпринимательской деятельности как «риск».

Риск в предпринимательской деятельности является широким понятием, охватывающим множество аспектов, в том числе и риск убытков от действий недобросовестного контрагента, оппортунистического поведения контрагента.

С целью минимизировать риски предпринимательской деятельности коммерческое юридическое лицо или индивидуальный предприниматель должны предпринимать действия для обеспечения своей экономической безопасности. «Экономическая безопасность предприятия – это состояние наиболее эффективного использования корпоративных ресурсов для предотвращения угроз и обеспечения стабильного функционирования предприятия в настоящее время и в будущем». Конкурентная (деловая) разведка является одним из инструментов, позволяющих обеспе-

чить безопасность предпринимательской деятельности.

Рассматривая механизм получения информации о юридических и физических лицах, можно отметить четыре категории источников информации: официальные, открытые, конфиденциальные и частные. Как отметил в своей работе Карл Андерсон, качество данных является ключевым элементом при принятии верных бизнес решений. Именно поэтому использование при сборе информации в целях деловой разведки официальных источников информации, которые обладают высоким уровнем точности, надежности и достоверности, способствует выработке подходящих стратегий ведения бизнеса и решения поставленных задач.

Сайт Федеральной налоговой службы Российской Федерации (далее – ФНС РФ) является одним из основных официальных источников информации о юридических и физических лица.

Согласно п. 10 Постановление Пленума ВАС РФ от 12.10.2006 № 53, налоговая выгода может быть признана необоснованной, если налоговым органом будет доказано, что налогоплательщик действовал без должной осмотрительности и осторожности и ему было известно о нарушениях, допущенных контрагентом.

Таким образом, чтобы избежать возникновения неблагоприятных последствий от действий контрагента, важно на момент совершения сделки провести тщательную проверку.

Необходимо отметить, что в Письме ФНС РФ от 12.05.2017 N АС-4-2/8872 содержатся рекомендации налогоплательщикам о том, на какие признаки недобросовестности контрагентов необходимо обратить внимание: отсутствие информации о государственной регистрации контрагента в ЕГРЮЛ; регистрация по адресу «массовой» регистрации; отсутствие информации о фактическом местонахождении контрагента, а также о местонахождении его складских, производственных, торговых площадей и т. д. Большую часть информации, в том числе данные о регистрации в ЕГРЮЛ и о регистрации по «массовому» адресу, можно получить на сайте ФНС РФ.

Используя сайт ФНС РФ в целях поиска информации о контрагенте, на главной странице сайта необходимо в разделе «Электронные сервисы» перейти по ссылке «Риски бизнеса: проверь себя и контрагента». После перехода перед лицом, осуществляющим деловую разведку, предстает раздел «Сведения о государственной регистрации юридических лиц, индивидуальных предпринимателей, крестьянских (фермерских) хозяйств». После ввода в специальные окна одного из вида данных о юридическом лице (далее – ЮЛ), индивидуальном предпринимателе (далее – ИП) или крестьянском (фермерском) хозяйстве (далее – КФХ): ОГРН (для ЮЛ), ОГРНИП (для ФЛ или КФХ) или ИНН или наименование ЮЛ, ФИО и регион места жительства; лицо, занимающееся сбором информации о контрагенте может получить следующие данные: информация о наименовании, адрес (место нахождения), ОГРН, сведения о регистрации, ИНН, КПП, сведения об уставном капитале, сведения об учредителях (участниках) ЮЛ, статус ЮЛ на дату запроса, сведения о видах экономической деятельности ИП.

На некоторые данные, собранные в данном разделе, стоит обратить особое внимание.

Длительность существования фирмы является одним из критериев для квалификации контрагента в качестве надежного и добросовестного. В законодательстве РФ отсутствует определение понятию «фирма-однодневка». «Вместе с тем, фирмами-однодневками принято называть юридические лица, создаваемые под конкретную операцию или на конкретный срок, как правило, на квартал».Недавнее присвоение компании ОГРН и регистрация фирмы меньше года является одним из признаков «однодневки». Ведение предпринимательской деятельности с фирмами-однодневками влечет за собой такие последствия как объявление затрат по сделкам с такими контрагентами необоснованными, отказ в применении вычетов по НДС, уплаченному спорным контрагентам, с таких расходов и сумм НДС доначисляются налоги, а также штрафы и пенни.

Небольшой размер уставного капитала не является признаком фирмы-однодневки и не говорит о ненадежности контрагента. так как российское законодательство для ООО устанавливает минимальный размер уставного капитала в 10 000 рублей. В свою очередь большой размер уставного капитала повышает вероятность того, что проверяемое ЮЛ является добросовестным.

Если по итогам сбора информации в данном разделе было выявлено, что данные о ЮЛ или ИП отсутствуют в ЮГРЮЛ и ЕГРИП, что ЮЛ или ФЛ прекратило свою деятельность, данного контрагента необходимо признать недобросовестным и ненадежным, принять решение об отказе

ведения предпринимательской деятельности с таким контрагентом.

Далее, если контрагент находится в процессе государственной регистрации или в процессе внесения изменений в учредительные документы сайт ФНС предоставляет возможность получить такие данные в специальном разделе «Сведения о юридических лицах и индивидуальных предпринимателях, в отношении которых представлены документы для государственной регистрации». Данный сервис позволяет информацию о характере изменений в ЕГРЮЛ и ЕГРИП.

На сайте ФНС РФ также возможно обращение к специализированным разделам, содержащим сообщения и сведения, опубликованные в журнале «Вестник государственной регистрации». В указанном разделе размещена информация о наличии решения о ликвидации фирмы или ее реорганизации, об уменьшении уставного капитала, о принятом решении исключить ЮЛ из ЕГРЮЛ, а также иные виды данных, которые ЮЛ обязаны публиковать в соответствии с российским законодательством. Для получения перечисленных выше сведений необходимо ввести ИНН или ОГРН. При отсутствии подобного рода сообщений в журнале «Вестник государственной регистрации» сайт укажет на невозможность обнаружения запрашиваемой информации, в данном случае причин для признания контрагента недобросовестным становится меньше. Однако, если

ЮЛ, являющееся потенциальным контрагентом, зарегистрировало сообщение об уменьшении уставного капитала или находится в стадии реорганищации, необходимо провести более подробный сбор информации для оценки такого ЮЛ. В случаях, когда в журнал содержит данные о ликвидации ЮЛ или о решении исключить ЮЛ из ЕГРЮЛ, необходимо обратить внимание на эти стоп-сигналы. Организации при выборе контрагентов предпочитают не иметь дело с теми компаниями, которые находятся на этапе реорганизации (и уже тем более в процессе ликвидации) или в отношении которых возбуждена процедура банкротства. Опасения эти не напрасны:

Риски, которые существуют при ведении дел и заключении соглашений с ЮЛ, находящими в процессе реорганизации или ликвидации, заключаются в следующем. ЮЛ, которое вступило в процесс реорганизации, вскоре прекратит свое существование, а права и обязанности ЮЛ перейдут к новому (новым) ЮЛ. Переход прав и обязанностей к новому ЮЛ-правопреемнику может повлечь убытки и дополнительные издержки, так как правопреемник может быть более слабым в экономическом плане и с меньшим количеством активом (например, при реорганизации в форме разделения).

ЮЛ, находящееся в процессе ликвидации, по завершении прекратит свое существование, и все обязательства будут прекращены на основании ст. 419 ГК РФ. С момента назначения ликвидационной комиссии по п. 2 ст. 62 ГК РФ к ней переходят полномочия по управлению делами юридического лица (п. 3 ст. 62 ГК РФ). Следовательно, с момента принятия решения о ликвидации полномочия на заключение гражданско-правовых сделок имеются лишь у ликвидатора, директор общества и иные лица, обладавшие полномочиями до назначения ликвидатора, не праве выступать от имени ЮЛ в правоотношения с другими лицами, в том числе и в гражданско-правовых сделках. В таком случае сделка будет признана ничтожной (на основе ст. 168 ГК РФ).

Затрагивая вопрос дисквалифицированных лиц, на сайте ФНС РФ можно проверить конкретное физическое лицо в реестре дисквалифицированных лиц. При отсутствии необходимых реквизитов для ввода сайт ФНС РФ выдает полный список всех дисквалифицированных лиц в алфавитном порядке. Результат поиска выдается в виде таблицы, в которой указаны фамилия, имя, отчество дисквалифицированного лица, номер записи в реестре дисквалифицированных лиц, организация, должность, статья КоАП РФ, наименование органа, составившего протокол об административном правонарушении, фамилия судьи, вынесшего решение, сведения о дисквалификации - срок дисквалификации.

Также, на сайте ФНС РФ можно проверить состав исполнительного органа ЮЛ на предмет отсутствия в нем дисквалифицированных лиц. При отсутствии реквизитов поиска выдается весь список юридических лиц, в состав исполнительных органов которых входят дисквалифицированные лица.

«Дисквалификация заключается в лишении физического лица права … занимать должности в исполнительном органе управления юридического лица, входить в совет директоров (наблюдательный совет), осуществлять предпринимательскую деятельность по управлению юридическим

лицом, осуществлять управление юридическим лицом в иных случаях, предусмотренных законодательством Российской Федерации».

Налоговыми инспекциями и арбитражными судами факт подписания договоров и иных актов дисквалифицированным руководителем признается доказательством получения налогоплательщиком необоснованной налоговой выгоды в совокупности с другими признаками, подтверждающими отсутствие реальных хозяйственных операций и непроявлением должной осмотрительности налогоплательщиком.

Гражданско-правовым последствием сделки, заключенной с дисквалифицированным лицом, будет ее недействительность по ст. 183 ГК РФ.

Согласно Письму ФНС России от 11.02.2010 № 3-7-07/84, под «фирмой-однодневкой в самом общем смысле понимается юридическое лицо, не обладающее фактической самостоятельностью … зарегистрированное по адресу массовой регистрации». Для проверки адреса ЮЛ через сайт ФНС РФ необходимо ввести все реквизиты адреса, после чего сайт предоставит данные из реестра адресов, указанных при регистрации, по которым зарегистрировано несколько ЮЛ. Данный раздел позволяет выявить недобросовестные фирмы и фирмы-однодневки, зарегистрированные по «массовым» адресам (сотни зарегистрированных ЮЛ по одному адресу – см. Приложение 1). Однако, при проверке адреса в настоящем разделе стоит учитывать, что большое количество зарегистрированных ЮЛ по адресу регистрации контрагента не обязательно указывает его недобросовестность, так здания, находящее по проверяемому адресу, может являться офисным бизнес-центром, который предполагает возможность регистрации десятков или сотен ЮЛ по одному адресу (см. Приложение 2).

Федеральный закон от 01.05.2016 № 134-ФЗ снял режим налоговой тайны с некоторых сведений, к которым имеет доступ ФНС. Так, с 1 июня 2016 года не являются налоговой тайной следующие сведения: о среднесписочной численности работников; об уплаченных организацией суммах налогов и сборов; о налоговых нарушениях, в том числе о суммах недоимки и задолженности по пеням, штрафам при их наличии; о суммах доходов и расходов по данным бухгалтерской (финансовой) отчетности. Сайт ФНС РФ предоставляет возможность быстро проверить контрагента на предмет уплаты налогов и предоставления налоговой отчетности, для проверки необходимо ввести только номер ИНН ЮЛ. Если по итогу поиска ЮЛ не имеет задолженность, превышающую 1000 рублей по уплате налогов и вовремя предоставляет налоговую отчетность, данный контрагент может быть рассмотрен в качестве добросовестного (если в иных параметрах поиска также отсутствует информация, вызывающая опасение оппортунистического поведения ЮЛ).

Недобросовестное поведения контрагента по уплате налогов может повлечь за собой указанные ранее последствия: отказ в применении вычетов по НДС, доначисление налогов, штрафов и пенни. Также, контрагент, являющийся злостным задолжником, то есть ЮЛ, нарушающее свои обязательства перед государством, может с такой же степенью безразличия относиться к своим обязательства по сделке.

Сайт ФНС обладает относительно новым сервисом: «Сведения о физических лицах, являющихся руководителями или учредителями (участниками) нескольких юридических лиц». В сервисе представлены сведения о лицах, являющихся руководителями или участниками в 10 и более ЮЛ. Для проверки данных по контрагенту необходимо ввести его фамилию, имя, отчество и ИНН (допустим ввод части имеющихся реквизитов).

Массовые учредители и руководители – это, по мнению ФНС РФ, признак того, что такое ЮЛ является фиктивным, иными словами не ведет реальную предпринимательскую деятельность. Массовость учредителя или руководителя не является основанием для применения каких-либо санкций со стороны государства, однако, такой критерий является сигналом для налоговых служб по проведению контрольных мероприятий, а также для потенциальных контрагентов о недобросовестности и ненадежности ЮЛ.

Последним электронным сервисом по проверке контрагента, представленным на сайте ФНС РФ, является сервис «Сведения о лицах, в отношении которых факт невозможности участия (осуществления руководства) в организации установлен (подтвержден) в судебном порядке». Ввод

двух реквизитов ОРГН и ИНН позволяет моментально проверить ЮЛ на наличие лиц, участие в организации которых невозможно.

Таким образом, сайт ФНС РФ обладает широким набором инструментов, находящихся в свободном доступе, которые позволят выявить недобросовестного контрагента и предупредить оппортунистическое поведение ЮЛ в совместном ведении бизнеса. Однако необходимо отметить, что процесс деловой разведки в целях обеспечения экономической безопасности фирмы не может быть ограничен одним информационным ресурсом. Обращения к данным на сайте ФНС РФ является первым базовым шагом в процессе оценивания надежности контрагента.

Список использованных источников и литературы

I. Нормативно-правовые акты

1. «Гражданский кодекс Российской Федерации (часть первая)» от 30.11.1994 N 51-ФЗ (ред. от 29.12.2017) // Российская газета. 1994 г. № 238-239.
2. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 05.02.2018) // Парламентская газета. 2002 г. № 2-5. Ст. 3.11
3. Федеральный закон от 08.02.1998 N 14-ФЗ (ред. от 31.12.2017) «Об обществах с ограниченной ответственностью» (с изм. и доп., вступ. в силу с 01.02.2018) // Российская газета. 1998 г. № 30.
4. Федеральный закон от 01.05.2016 N 134-ФЗ «О внесении изменений в статью 102 части первой Налогового кодекса Российской Федерации» // Российская газета. 2016 г. № 97.
5. Письмо ФНС РФ от 11.02.2010 N 3-7-07/84 «О рассмотрении обращения» // «Официальные документы» (еженедельное приложение к газете «Учет, налоги, право»). 2010 г. № 9.
6. Вопрос: О подтверждении должной осмотрительности в выборе контрагентов; о правах налогоплательщика при назначении и проведении экспертизы. (Письмо ФНС России от 12.05.2017 N АС-4-2/8872) // «Официальные документы» (приложение к «Учет. Налоги. Право»). 2017 г. № 20.
7. Письмо МНС России от 30 декабря 2003 г. № БГ-6-09/1390 // Главбух URL: https://www.glavbukh.ru/npd/edoc/99_901888708 (дата обращения: 06.03.2018).

II. Судебная практика:

1. Постановления Пленума ВАС РФ №53 от 12.10.2006 года «Об оценке арбитражными судами обоснованности получения налогоплательщиком налоговой выгоды» // Федеральные арбитражные суды Российской Федерации URL: http://www.arbitr.ru/as/pract/post_plenum/3151.html (дата обращения: 06.03.2018).
2. Постановление ФАС Северо-Кавказского округа от 13.08.2009 по делу N А53-12650/2008-С3-15 // Решения и постановления судов URL: http://www.resheniya-sudov.ru/2009/97687/ (дата обращения: 07.03.2018)
3. Постановление ФАС Северо-Кавказского округа от 26 января 2016 г. по делу № А53-13109/2013 // Судебные и нормативные акты РФ URL: http://sudact.ru/arbitral/doc/1Aijz4D9jMm/ (дата обращения: 07.03.2018).

III. Диссертации и авторефераты:

1. Денисов Р. В. Деловая разведка как фактор повышения конкурентоспособности предприятия: автореф. дис. ... канд. экон. наук: 08.00.05. М., 2012.

IV. Монографии, справочная и учебная литература:

1. Андерсон К. Аналитическая культура: От сбора данных до бизнес-результатов. М.: Манн, Иванов и Фербер, 2017.
2. Воронов Ю.П. Конкурентная разведка: Учеб. пособ. Новосибирск: Издательство Новосибир-

ского гос. университета, 2007.
3. Муратова Н. К. Экономическая безопасность предприятия как успешная составляющая современного бизнеса // Государственное управление. Электронный вестник. 2012. №32. С. 2.
4. Серебряник И. А., Золотухина Д.М. Проверка контрагента: дополнительные возможности для бизнеса // Дискуссия. 2016. №11 (74).
5. Ярочкин В.И., Бузанова Я.В. Корпоративная разведка. М.: Ось-89, 2005.

V. Электронные ресурсы:

1. Федеральная налоговая служба URL: https://www.nalog.ru/rn77/ (дата обращения: 06.03.2018-08.03.2018).
2. Какие последствия влечет договор, подписанный дисквалифицированным руководителем? (Куприна Н.) // Закон.ru URL: https://zakon.ru/discussion/2017/3/2/kakie_posledstviya_vlechet_dogovor_podpisannyj_diskvalificirovannym_rukovoditelem (дата обращения: 06.03.2018)
3. Режим налоговой тайны снят с части сведений, имеющихся в распоряжении налогового органа // КонсультантПлюс URL: http://www.consultant.ru/law/hotdocs/46315.html (дата обращения: 07.03.2018). и сам ФЗ ;
4. В ФНС России подвели предварительные итоги работы по борьбе с фиктивными компаниями // Федеральная налоговая служба URL: https://www.nalog.ru/rn77/news/activities_fts/6979157/ (дата обращения: 07.03.2018).
5. На сайте ФНС теперь можно вычислить «массовых» директоров // Налог-налог.ру URL: http://nalog-nalog.ru/spravochnaya_informaciya/na_sajte_fns_teper_mozhno_vychislit_massovyh_direktorov/ (дата обращения: 07.03.2018).

Приложения

1. Ленинский проспект, д. 95 – жилой дома в юго-западном административном округе.

№ п.п	Адрес, указанный в качестве места нахождения при государственной регистрации юридического лица	Количество зарегистр. ЮЛ
1	МОСКВА Г,ЛЕНИНСКИЙ ПР-КТ, дом (владение) 95	293

2. Пресненская набережная, д. 12 – бизнес-центр «Башня Федерации».

РЕЗУЛЬТАТЫ ПОИСКА (ДАТА ФОРМИРОВАНИЯ СВЕДЕНИЙ 07.03.2018)

Всего записей в реестре: 25670, найдено записей: 12, представлено записей: 12

Выгрузка полного списка найденных записей в формате Excel

№ п.п	Адрес, указанный в качестве места нахождения при государственной регистрации юридического лица	Количество зарегистр. ЮЛ
1	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12, квартира (офис) А1	10
2	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12, квартира (офис) ЭТ.41	10
3	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12, квартира (офис) 45, КОМН. 10	107
4	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12, квартира (офис) 10	15
5	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12	78
6	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12, квартира (офис) А30	16
7	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12, квартира (офис) 45 К. 82	11
8	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12, квартира (офис) 82	34
9	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12, квартира (офис) 29 КОМ. А30	13
10	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12	62
11	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12, квартира (офис) А28	19
12	МОСКВА Г,ПРЕСНЕНСКАЯ НАБ, дом (владение) 12, квартира (офис) 4403	10

АЛЬПЕРТ ОЛЕГ ДМИТРИЕВИЧ
студент факультета права
НИУ ВШЭ, г. Москва
E-mail: odalpert@edu.hse.ru

БЫЛЬБА МАКСИМ СЕРГЕЕВИЧ
студент факультета права
НИУ ВШЭ, г. Москва
E-mail: mbylba@edu.hse.ru

ОТЕЧЕСТВЕННАЯ ПРАКТИКА ЗАЩИТЫ БИЗНЕСА ОТ РЕЙДЕРСКИХ ЗАХВАТОВ

ALPERT OLEG DMITRIYEVICH
student, faculty of law
National Research University Higher School of Economics, Moscow

BYLBA MAXIM SERGEEVICH
student, faculty of law
National Research University Higher School of Economics, Moscow

DOMESTIC PRACTICE OF PROTECTING BUSINESS FROM RAIDER ATTACKS

Аннотация: Возникшее на рубеже 20-го и 21-го веков в России рейдерство до сих пор является серьезной проблемой и угрозой экономической деятельности и конкуренции на отечественном рынке. Однако, на данный момент законодательно установленные механизмы противодействия данному явлению отсутствуют, в связи с чем вопрос рейдерства остается актуальным. в результате слабого реагирования государственных структур на действия рейдеров отечественные предприниматели вынуждены принимать меры самозащиты от рейдерских захватов. в данной статье авторами рассматриваются существующие практики противодействия данному явлению, а также их эффективность.

Abstract: Raiding that emerged at the turn of the 20th and 21st centuries in Russia is still a serious problem and threat of economic activity and competition in the domestic market. However, at the moment there are no legally established methods to counteract this phenomenon, and therefore the issue of raiding remains relevant. As a result of weak response of state structures to the actions of raiders, domestic entrepreneurs are forced to take measures to protect themselves from raider seizures. In this article authors analyze existing practices of counteraction to the given phenomenon, and also their efficiency.

Ключевые слова: рейдерство, рейдерский захват, предприниматели, противодействие рейдерству, самозащита, субъекты, осуществляющие предпринимательскую деятельность, практика защиты.

Keywords: raiding, raider seizure, entrepreneurs, countering of raiders, measures of self-protection, business owners, practices of counteraction.

Возникшее на рубеже 20-го и 21-го веков в России рейдерство до сих пор является серьезной проблемой и угрозой экономической деятельности и конкуренции на отечественном рынке. Однако, в национальном законодательстве до сих пор отсутствует как определение, так и состав уголовно наказуемого деяния для рейдерства (или рейдерского захвата). Вместе с тем, проблема рейдерства по-прежнему актуальна несмотря на попытки его пресечения государством. Так, на 2017 год из 557 жалоб бизнесменов в Генпрокуратуру 202 пришлось на рейдерские захваты, что говорит о существенности и масштабе данного явления. в результате слабого реагирования государственных структур на действия рейдеров отечественные предприниматели вынуждены принимать меры самозащиты от рейдерских захватов. Очевидно, что основным субъектом противодействия рейдерству должно быть государство в лице государственных органов, устанавливающих императивные нормы, однако в силу отсутствия эффективного регулирования ключевым механизмом борьбы является самозащита права собственности. Поэтому в данной работе будут проанализированы методы защиты бизнеса от рейдерства в России, а также будет рассмотрена конструкция и механизм функционирования самого рейдерства.

Проблема неопределенности рейдерских захватов и недостатка мер по противодействию рейдерству на государственном уровне поднималась не раз различными государственными структурами. Так, в 2008 году Правительство РФ в «Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года» в рамках развития российского финансового рынка сделало упор на необходимость предотвращения и пресечения рейдерства.

Помимо этого, и Президент РФ также обращал внимание на рейдерство в различных нормативно-правовых актах. Так, в пп. 2 п. 22 «Стратегии экономической безопасности Российской Федерации на период до 2030 года» указывалось, что одним из факторов и задач обеспечения экономической безопасности бизнеса является профилактика и предотвращение рейдерских захватов. Вместе с тем, в своем Послании Федеральному Собранию в 2018 году Президент РФ также подчеркнул необходимость установления жестких норм в Уголовном Кодексе по отношению к рейдерским захватам. Не остался в стороне и бизнес-омбудсмен Б.Ю. Титов. Свидетельством вышесказанному может служить доклад о положении дел с правами человека в предпринимательской сфере предоставленный уполномоченным по защите прав предпринимателей Борисом Титовым Президенту 27 мая 2019 года. Наиболее наглядным и интересным является приложение к докладу, в котором представлен экспертный опрос Федеральной службы охраны. в рамках опроса специалисты (адвокаты, ученые-юристы, прокуроры и правозащитники) давали оценку бизнес-климату, также были опрошены предприниматели, подвергшиеся уголовному преследованию. Таким образом, были опрошены 181 специалист и 211 предпринимателей в 37 регионах.

По мнению подавляющего большинства респондентов, заниматься бизнесом в России небезопасно, и перспектива исправления не утешающая. Так, данной позиции придерживается 69,2% специалистов и 84,4% бизнесменов. Также, в соответствии с опросом лишь 43,3% участников опроса доверили бы разрешение хозяйственных споров государственному суду, чуть больше 30% — третейскому, а почти 11% — вообще никому. Больше 70% респондентов считают, что российские законы не гарантируют защиту бизнеса от необоснованного возбуждения уголовных дел (цифра с прошлого года почти не изменилась).

Во многом, данная негативная тенденция обусловлена отсутствием эффективных механизмов противодействия рейдерству и появлением его новых видов, в том числе благодаря наличию пробелов в законодательстве.

Так, в марте 2012 года Банк России утвердил положение № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов». с принятием данного положения кратно возросло количество блокировок счетов на основании Закона о противодействии легализации преступных доходов – 115-ФЗ. в связи с широким перечнем подходящих признаков и интенсивностью применения данного инструмента, стали возникать ситуации злоупотребления банками, что еще более актуально в условиях затруднения привлечения их к ответственности.

В связи с этим, бизнес-омбудсмен усматривает в действиях некоторых банков «прямое рейдерство» и приводит в пример случаи, когда банки требовали от клиентов за разблокировку счёта

15% от остатка средств. в связи с чем, Б.Ю. Титов отмечает: «если у вас есть подозрения в том, что деньги какие-то неправильные, «черные», тогда нужно подавать заявление в правоохранительные органы». По мнению бизнес-омбудсмена, проблема обусловлена тем, что межведомственная комиссия при ЦБ, которая рассматривает жалобы на необоснованные блокировки, работает закрыто и в неё не входят представители общественности. Также, замечание относительно действий банков, на наш взгляд, относится к пробелу в законодательстве в той мере, в которой допускаются подобные злоупотребления.

Для преломления отрицательной тенденции Б.Ю. Титовым в качестве одного из возможных решений предложено наделить представителей бизнес-омбудсмена объемом полномочий, который имеет адвокат, что должно обеспечить полноценную защиту предпринимателей в судах.

Однако, возвращаясь к нынешнему законодательству, на данный момент конкретного состава рейдерства или рейдерского захвата в УК РФ нет. в целом данное деяние характеризуется как преступный захват чужой собственности. При этом, объектом данного противоправного посягательства являются корпоративные и иные правоотношения внутри организации, которые возникают в процессе осуществления уставной деятельности. Предметом же посягательства является имущество предприятия, которое находится в собственности данной организации (или на основании иного вещного права). На практике рейдерство может квалифицироваться как различные преступления или по совокупности. Например, рейдерский захват или рейдерство можно квалифицировать как мошенничество (ст. 159 УК), вымогательство (ст. 163 УК), принуждение к совершению сделки (ст. 179 УК), организацию преступного сообщества (ст. 210 УК), самоуправство (ст. 330 УК) и т.п. При этом рядом авторов отмечается, что рейдерство совершается в совокупности с подделкой документов.

Пример такой квалификации привел официальный представитель СК России В.И. Маркин в 2016 году. Например, Г. Пирумов был признан виновным в совершении рейдерского захвата по ст. 159 УК РФ (мошенничество). Виновный в сговоре со своим адвокатом разработали план, предусматривающий нарушение договоров, включая инициирование судебных разбирательств. Целью являлось незаконное завладение зданием.

Неэффективность такого регулирования иллюстрируется длительной практикой. Так, в среднем лишь одно уголовное дело возбуждалось на 173 рейдерских захвата. Только одно дело из тысячи дошло до судебного разбирательства. Один обвинительный приговор был вынесен на 5500 рейдерских захватов.

Таким образом, отсутствие прямых материальных и процессуальных норм является серьезным фактором функционирования рейдерства, однако не единственным. Анализируя практику рейдерских захватов, можно прийти к выводу о наличии других катализирующих факторов. Речь идет о коррупции и неэффективной деятельности правоприменительных органов.

Непосредственным результатом самого рейдерства является завладение чужим имуществом. Вместе с тем, цели, для достижения которых применяется рейдерство, могут быть разными: устранение конкурентов, завладение желаемыми правами или материальными благами и др. Такое рейдерство используется участниками рынка – компаниями и их бенефициарами. Также рейдерство может совершаться в личных преступных интересах. в таком случае целью рейдеров является получение дохода в виде разницы между ценой приобретения и ценой последующей продажи, так как цена приобретения в ходе рейдерства существенно снижена («недокапитализация» активов).

Для первого случая, когда к рейдерству прибегают участники рынка, для планирования рейдерского захвата привлекаются специальные структуры, обладающие опытными юристами. Такие юристы сопровождают рейдерский захват на всех его этапах. Для всех задач выделяются крупные денежные средства, которые в основном идут на подкуп государственных органов и на иные аспекты реализации рейдерства.

Тем не менее, для всех случаев схемы и способы рейдерских захватов, в целом, одинаковы. Так, к основным средствам, применяемых рейдерами, можно отнести следующие:

1. подделка документации, как, например, учредительные документы, решения собраний, судебные решения и др.;

2. трансфер (перевод с лицевого счета/счета депо законного владельца на счет рейдера) акций на основании поддельных документов или иным образом;
3. получение решений суда по несуществующим обязательствам;
4. обход закона и злоупотребление правом с помощью недостатков законодательства, как, например, закона о несостоятельности (банкротстве);
5. блокирование работы органов управления организации;
6. силовой захват.

Данный перечень не является исчерпывающим, так как с развитием общества и технологий появляются новые способы для рейдерства.

Также одним из способов рейдерства может быть доведение компании до предбанкротного состояния путем конструирования вокруг собственника и самой компании некой обстановки отчуждения, воздействуя на клиентов и контрагентов компании. в результате капитализация активов резко падает, так как собственник осознает то, что находится на грани банкротства. в этот момент рейдер направляет оферту о приобретении активов предприятия, на что собственник и соглашается.

К силовым методам захвата можно отнести психологическое давление, как, например, угрозы собственнику компании и его семье, слежка, звонки с угрозами физической расправы, рассылка писем с соответствующим содержанием и т.д. Также это могут быть и действия, носящие насильственный характер: причинение материального ущерба имуществу компании; похищение или причинение физических повреждений собственнику или членам его семьи; убийство собственника.

Таким образом, осуществление рейдерского захвата с причинением экономического вреда невозможно без оказания воздействия на корпоративное управление компании. Результатом же рейдерских захватов, как показывает практика, является снижение экономических показателей компании, прекращение осуществления деятельности юридического лица (либо приостановление деятельности), обогащение рейдеров или лиц, приобретавших услуги рейдеров и т.п.

За пару десятилетий существования явления рейдерства на российском рынке в бизнес-среде сформировались различные способы защиты от рейдерских атак. Помимо этого, различные рекомендации публикуют и СМИ. Так, например, издание «Ведомости» убеждает в том, что эффективны лишь системные действия. в первую очередь рекомендуется в случае наличия угрозы бизнесу обращаться к специалистам. Однако, необходимо принять некоторые меры самостоятельно. Так, сложности у рейдеров вызовет грамотная и проработанная схема управления. в то же время особое внимание уделяется внутренней документации и крупным сделкам. Данные меры являются основой противодействия рейдерам. Ведь недостатки корпоративного управления и документации (наличие противоречий закону, излишние либо наоборот непроработанные процедуры) облегчают рейдерский захват. Например, в одной компании полномочия гендиректора были безграничными, что позволило рейдерам захватить активы, лишь поставив своего человека в должность гендиректора компании. Подобное внимание также должно уделяться процедуре принятия решений на собраниях акционеров, размещению дополнительных ценных бумаг. Однако, решения вопроса акционеров не столь однозначны. в одних источниках рекомендуется компании выйти на IPO (публичное размещение акций), тем самым увеличив количество акционеров-миноритариев. Вместе с тем, Н.С. Киселев в своей работе убеждает в неэффективности данной меры. Данный автор пишет, что именно миноритарии являются слабым звеном в обеспечении безопасности от угрозы рейдерских атак. в качестве примера он приводит скупку несколькими конкурентами акций у миноритариев Новосибирского авиаремонтного завода в 2005 году. Когда приобретатели направили оферту о приобретении остальных пакетов акций у мажоритарных акционеров, они отказали. в результате, владея крупным пакетом акций, скупленных у миноритариев, новые акционеры начали блокировать деятельность собрания акционеров, оспаривать их решения в суде. Такие действия поставили компанию на грань банкротства.

Интересна также стратегия диверсификации активов в целях снижения риска рейдерского захвата. Суть ее состоит в том, чтобы разделить основные активы между разными компаниями. Например, одна компания будет собственником недвижимого комплекса, тогда как вторая

будет владеть оборудованием и т.д. Очевидно, что такая стратегия усложняет хозяйственную деятельность, однако, вместе с тем значительно снижает риски при рейдерских атаках. Аналогичная схема носит название холдинговой структуры. Отличие такой реструктуризации заключается в разграничении не имущества, а функций деятельности. То есть, хозяйственные функции осуществляет не одна структура, а четыре самостоятельные компании: владельческая, производственная, торговая и управленческая. Иначе такая схема называется схемой четырех углов.

Также необходимо ликвидировать возможные источники утечки корпоративной информации. Необходимо поддерживать благожелательные отношения внутри коллектива: между сотрудниками и руководителями. в то же самое время проводится проверка безопасности среди нового персонала, особенно владеющего доступом к информации, имеющей значимость. Помимо этого, защитной мерой будет являться обеспечение безопасности информационных данных от атак хакеров. Однако, российская специфика рейдерских захватов предусматривает и силовые методы завладения конфиденциальными корпоративными данными. Например, в случае с пермским крупным заводом по производству турбогенераторов в 2005 году, группа рейдеров силовым путем проникла на территорию завода с целью завладения корпоративной документацией. Атака была отбита старанием сотрудников завода, один из которых даже получил пулевое ранение в живот. Поэтому, исходя из отечественной практики, стоит обеспечить безопасность предприятия путем формирования внутренней службы безопасности, которая смогла бы предотвратить и силовые методы рейдеров. Однако, в настоящее время такие пути используются рейдерами редко.

Немаловажным фактором предостережения от угрозы рейдерского захвата является сбор информации и мониторинг конкурентов. Такой сбор и анализ информации позволит обнаружить признаки угрозы рейдерства. Такими индикаторами могут служить излишняя заинтересованность и предложения о продаже долей в уставном капитале или акций со стороны инвестиционных компаний, инициирование судебных дел и проверок со стороны государственных органов или внезапный интерес у СМИ, результатом которого является ухудшение имиджа компании, а также трудности с контрагентами.

Данные меры являются превентивными, т.е. мерами предосторожности, когда рейдерского захвата еще не произошло. Такие способы защиты сводятся к прогнозированию и мониторингу рисков, а также позволяют создать систему защиты. По мнению некоторых авторов, как, например, Е.В. Борисовой и Н.С. Киселева, большинство отечественных предпринимателей недооценивают такие меры защиты. Это связано, в основном, с затратностью либо простым халатным отношением к угрозе рейдерского захвата. Результатом такой неосмотрительности является реальная угроза рейдерских атак.

Тем не менее, на практике существуют и экстренные меры, применяемые непосредственно в процессе рейдерского захвата. Однако, в отличие от превентивных данные способы защиты не являются столь эффективными. Одним из таких способов, является активное вовлечение СМИ. Таким образом, масштабная PR-кампания позволит отбить желание рейдеров продолжать захват. Помимо этого, необходимо привлечь юристов, а также, в случае наличия криминальных способов рейдерства, необходимо обращаться в органы внутренних дел или в прокуратуру.

Рейдерство до сих является серьезной угрозой отечественному бизнесу. Это завладение имуществом помимо воли собственника, что, таким образом, носит негативный характер не только в бизнес-сообществе, но и во властных структурах. Однако, в отечественном законодательстве до сих пор отсутствует легальное определение рейдерства и рейдерских захватов. Также, уголовное законодательство не содержит и норм об ответственности за совершение рейдерства. Такие деяния обычно квалифицируют по различным статьям УК РФ, в т.ч. мошенничество, организация преступного сообщества и т.д. Хотя вопрос о включении в УК состава преступления за рейдерство поднимался на разных уровнях государственной власти неоднократно, по существу ничего не изменилось. Похожая ситуация касается и правоприменительной практики. Несмотря на большое количество жалоб на рейдерство со стороны отечественных предпринимателей, до суда доходит лишь небольшое количество дел. При этом, новеллы принимаемые на законодательном уровне, хотя и служащие борьбе с другими преступными явлениями, могут напрямую влиять на ведение бизнеса. Так, нормы, принятые для борьбы с отмыванием денег, стали очередной воз-

можностью для рейдерских захватов.

Современные рейдеры используют различные методы приобретения чужих активов. Однако, все они так или иначе связаны с корпоративным управлением компании-цели. в результате у компании, ставшей жертвой рейдерской атаки падают экономические показатели, имидж, и появляется угроза банкротства. Компания и вовсе может прекратить свою деятельность, что в целом и является целью многих рейдерских атак.

В силу отсутствия эффективного противодействия рейдерству со стороны государственных структур, отечественные предприниматели осуществляют защиту своего бизнеса самостоятельно. Однако, многие бизнесмены зачастую не придают должного значения угрозе рейдерских захватов, что, несомненно, упрощает функционирование рейдерства на практике. Поэтому, практические рекомендации самозащиты публикуются и СМИ. Отечественные авторы выделяют превентивные и экстренные меры защиты. При этом, наиболее эффективными являются именно превентивные меры безопасности. к ним относятся сбор информации, обеспечение информационной и внутренней безопасности, изменение в системе управления и т.д. Обращение в государственные органы и громкая PR-акция с целью привлечения внимания являются экстренными мерами, которые, все-таки, являются менее эффективными.

Список использованных источников и литературы:

Нормативно-правовые акты:

1. Указ Президента РФ от 13 мая 2017 г. N 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // Собрание законодательства Российской Федерации от 15 мая 2017 г. N 20 ст. 2902;
2. Распоряжение Правительства РФ от 17.11.2008 N 1662-р «О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года» // Собрание законодательства РФ от 24 ноября 2008 N 47 ст. 5489;
3. Послание Президента РФ Федеральному Собранию от 01.03.2018 «Послание Президента Федеральному Собранию» // Российская газета от 02 марта 2018 N 46;
4. “Положение о требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма” (утв. Банком России 02.03.2012 N 375-П) (Зарегистрировано в Минюсте России 06.04.2012 N 23744) // “Вестник Банка России”, N 20, 18.04.2012.

Источники:

5. Рейдерство стало самой частой причиной жалоб бизнеса в Генпрокуратуру // РБК URL: www.rbc.ru/politics/07/02/2017/5898adac9a7947096696dc48;
6. Закрытый опрос ФСО показал рекордное недоверие бизнеса к силовикам // URL: https://www.rbc.ru/society/28/05/2019/5cebe7939a794754023bf449?from=from_main;
7. Титов: уголовные экономические дела должны начинаться только после арбитража // Право.Ru URL: https://pravo.ru/news/210508/?desc_search=;
8. Титов хочет получить полномочия, приближенные к адвокатским // Право.Ru URL: https://pravo.ru/news/211140/?desc_search=;
9. Интервью официального представителя СК России Владимира Маркина интернет-изданию ПАСМИ // СК РФ URL: https://sledcom.ru/press/interview/item/1067116/?pdf=1;
10. Как дать отпор рейдерам (и не дать себя поглотить) // Интернет-сайт Inc.Russia URL: https://incrussia.ru/understand/kak-dat-otpor-rejderam-i-ne-dat-sebya-poglotit/;
11. Как защититься от современных рейдеров // Ведомости URL: https://www.vedomosti.ru/management/blogs/2017/06/23/695696-zaschititsya-ot-reiderov;

12. Защита от рейдерского захвата: правовые методы // Интернет-сайт VEGAS LEX URL: https://www.vegaslex.ru/analytics/publications/60789/.

Научная литература:

13. Борисова Е.В. Защита финансовой системы от рейдерских захватов организаций // Альманах современной науки и образования, № 8, 2015 – С. 33-35;
14. Бурынин С.С. Практика противодействия рейдерским захватам имущества предприятия // Российский следователь. - 2017. - N 18. - С. 11-14;
15. Воеводкин А.В. о понимании рейдерства в России // «Российское право: образование, практика, наука», N 1, 2016 г. URL: http://study.garant.ru/#/document/57244771;
16. Воеводкин А.В. Юридическая конструкция рейдерства // СПС «Консультант Плюс» URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=CJI&n=106007#08952844465289469;
17. Габов А.В., Молотников А.Е. Рейдерство как правовое явление // "Законодательство", N 7, июль 2009 г. URL: http://study.garant.ru/#/document/5751275;
18. Киселев Н. С. Превентивная защита от рейдерских атак // Национальная безопасность / Nota bene. 2013. № 1. С. 171-178;
19. Мацкевич И.М. Причины экономической преступности: учебное пособие. - М.: "Проспект", 2017. - 272 с. URL: http://study.garant.ru/#/document/77771933.

БАЛАКШИН ИЛЬЯ СЕРГЕЕВИЧ
студент факультета бизнеса и менеджмента
НИУ ВШЭ, г. Москва
E-mail: isbalakshin@mail.ru

АНАЛИЗ ДЕЯТЕЛЬНОСТИ КРУПНОГО ИГРОКА НА МЕЖДУНАРОДНОМ РЫНКЕ БЕЗОПАСНОСТИ – КОМПАНИИ MOBOTIX

BALAKSHIN ILYA SERGEEVICH
student, faculty of business and management
National Research University «Higher School of Economics», Moscow

ANALYSIS OF THE ACTIVITIES OF A MAJOR PLAYER IN THE INTERNATIONAL SECURITY MARKET – MOBOTIX

Аннотация: В статье рассматриваются вопросы по внедрению различных систем безопасности от видеонаблюдения, датчиков движения до биометрических и автоматических роботизированных устройств. Проведен анализ крупной международной компании в сфере безопасности и ее кейсов по внедрению различных систем безопасности.

Abstract: The article discusses the implementation of various security systems from video surveillance, motion sensors to biometric and automatic robotic devices. The analysis of a large international security company and its cases on the implementation of various security systems is performed.

Ключевые слова: Бизнес, биометрия, системы видеонаблюдения, роботы, кибербезопасность.

Key words: Business, biometrics, CCTV, robots, cybersecurity.

В наше время для большинства крупных и малых компаний становится один из главных вызовов, как и каким образом обеспечить безопасность материальных ресурсов своего бизнеса, защитить своих работников, информацию на физических носителях и так далее. Здесь выход только один – внедрение различных систем безопасности от видеонаблюдения, датчиков движения до биометрических и автоматических роботизированных.

Данная тема является весьма перспективной, так как проблема физической и инженерно-технической безопасности всегда были одними из главных, что 20 лет назад, когда еще не были развиты устройства Четвёртой промышленной революции, что сейчас – с их созданием и новыми вызовами. Поэтому, очень важно, чтобы проблемы данной сферы решались новаторскими методами, отвечающим современным требованиям. Также, эта тема становится одной из главных среди обсуждений во многих бизнес и IT исследованиях, что еще раз подтверждает ее актуальность. Например, такие журналы, как: Forbes, РБК, VC и так далее, часто проводят исследования по анализу рынка устройств и услуг по безопасности, часто организуют встречи и конференции по обсуждению текущих проблем в этой сфере и методов их решения.

Предметом исследования является анализ возможностей и предложений компанией Mobotix – одного из лидеров сегмента систем видеонаблюдения, а объектом – общий анализ рынка в сегменте устройств и систем видеонаблюдения.

Цель этой работы состоит в том, чтобы определить ключевых игроков в сегменте систем видеонаблюдения, проанализировать деятельность одного из них и провести бенчмаркинг проанализированной информации.

Основные задачи работы:

1. Определить нынешнюю ситуацию на рынке систем видеонаблюдения;
2. Изучить аспекты деятельности компаний на этом рынке;

3. Проанализировать деятельность одной из выбранных компаний-лидеров;
4. Провести бенчмаркинг проанализированной информации.

На данный момент существует множество компаний, которые занимаются предоставлением услуг в сфере физической и инженерно-технической безопасности, но лидеров, которые предоставляют по праву качественные и современные услуги не так много. Ничем не отличается сегмент систем видеонаблюдения на данном рынке. Некоторые эксперты выделяют среди лидеров такие компании, как: Hikvision Digital Technology, Axis Communications, Bosch Security Systems, Mobotix и так далее. Деятельность последней – Mobotix – будет рассматриваться дальше в работе.

Почему важны только лидеры, помимо стороны качества? Ответ очевиден, более 60% доходов приходятся на топ-15 компаний по состоянию на 2018 год.

Самыми быстрыми темпами в период с 2016 по 2022 годы увеличатся продажи систем видеонаблюдения для коммерческого сектора. Высокий спрос на системы безопасности в крупной и мелкой розничной торговле обусловлен необходимостью противостоять кражам в розничных сетях и бороться с потерями по всей цепочке предприятия. в финансовом секторе, особенно в банках, системы видеонаблюдения срочно необходимы для защиты зданий, управления движением и хранением наличных денег, мониторинга действий клиентов и персонала. Все это требует систематического расширения функциональности систем видеонаблюдения в соответствии с прогрессом технологий.

Регион, в котором рынок видеонаблюдения будет расти самыми быстрыми темпами – Азиатско-Тихоокеанский. Он концентрирует значительную часть производственных ресурсов в области видеонаблюдения, в том числе многих из наиболее важных игроков на этом рынке. с другой стороны, в регионе высокий уровень преступности и степень террористической угрозы.

Но, перед тем как перейти к анализу деятельности компании, стоит разобраться с различными общими аспектами работы компаний на этом рынке.

Известно, что системы видеонаблюдения занимают около 20% мирового рынка устройств физической и инженерно-технической безопасности, поэтому очень важно выделить те тренды, на которые сейчас акцентируют внимание многие компании при внедрении таких устройств.

Сейчас выделяют несколько трендов:

- Беспроводные системы видеонаблюдения,
- Кибербезопасность в видеонаблюдении,
- Революция в видеоаналитике,
- Роботы в видеонаблюдении,
- HD CCTV.

Имеет смысл описать и проанализировать каждый из них, чтобы сравнить с теми возможностями Mobotix, которые они могут предоставить клиенту.

Беспроводные системы видеонаблюдения.

Сегмент беспроводных систем видеонаблюдения (wireless video surveillance или WVS) демонстрирует высокую динамику развития на мировом рынке систем видеонаблюдения со среднегодовыми темпами роста 21% в период 2017-2021 годов.

Среди основных драйверов аналитики TechNavio называют низкую стоимость монтажа, низкую стоимость обслуживания дешевой рабочей силой и низкую совокупную стоимость владения.

Беспроводные системы видеонаблюдения (WVS) преобладают в жилом и коммерческом секторе, и будут пользоваться наибольшим спросом у владельцев небольших розничных магазинов. Что касается географической сегментации – наибольшую популярность видеокамеры WVS получают в Северной Америке.

Данный тренд говорит только о том, что сейчас видеонаблюдение как инструмент физической защиты предприятия не может нормально функционировать без учета кибер безопасности, о чем и будет сказано далее.

Кибербезопасность в видеонаблюдении.

Уязвимость камер видеонаблюдения и видеорегистраторов стала трендом еще в 2017 году, в 2018 градус внимания к ней по-прежнему был очень высок. Точка накала произошла в 2016, когда огромное количество пораженных вирусами устройств, включая оборудование для систем видеонаблюдения, были использованы для DDoS-атак ботнетом Mirai. Это нарушило работу сервисов нескольких интернет-гигантов, таких как Netflix, Twitter, Spotify и нескольких крупных интернет провайдеров США.

Кибербезопасность имеет большое значение для производителей систем видеонаблюдения, как представителей больше физической стороны. с внедрением подключенных к сети интернет цифровых видеорегистраторов (DVR) и камер видеонаблюдения, системы видеонаблюдения перестали быть «закрытыми». Сетевые технологии сделали видеонаблюдение более интеллектуальным, видеоархив доступным из любой точки мира, а системы видеонаблюдения в целом еще более масштабируемыми.

Информационная безопасность для оборудования, последнее время всегда на первом месте в повестке дня на многих мероприятиях индустрии видеонаблюдения. Индустрия в целом предпринимает согласованные усилия для обучения пользователей и внедрения передового опыта с целью обеспечения безопасности сетевого оборудования в системах видеонаблюдения. Тем не менее, изменение поведенческой модели часто является не таким быстрым процессом.

Выделение кибербезопасности систем видеонаблюдения, как отличительной характеристики продукта или монетизация сервиса физической защиты могут быть проблемой для поставщиков оборудования систем видеонаблюдения.

Прогресс в кибербезопасности может привести к возникновению у пользователей вопросов по информационной защите оборудования, которое уже установлено. Более того, есть опасения, что компания, рекламирующая информационную защиту своего оборудования, побудит хакеров к атакам на такое оборудование. Продукты информационной защиты, предназначенные для систем видеонаблюдения, по-прежнему встречаются редко. Есть всего лишь несколько таких примеров, например, протокол DirectIP, разработанный компанией IDIS.

В будущем мы увидим рост предложений с увеличенной добавленной стоимостью от поставщиков систем видеонаблюдения, сфокусированных именно на кибербезопасности. Это должно привести к появлению новых решений, сфокусированных больше на активных, упреждающих подходах к кибернетическим угрозам к казалось бы устройствам никак не связанным с кибер- тематикой, но современные вызовы требуют современных решений.

Революция в видеоаналитике.

Данный тренд является опять же развитием физических систем безопасности, реагируя на современные вызовы. Что же тут примечательного? Системы с видеоаналитикой могут в режиме реального времени изучать тот или иной объект и давать ему оценку. Условно, камера перед входом оценивает кто заходит: работник IT-отдела, его начальник или уборщица, записывает эти данные, а в случае проникновения «неизвестного», сообщит сотрудникам ЧОПа.

В 2016 году впервые можно было увидеть такие системы в деле. Китайские производители уже установили такие продукты для контроля и наблюдения в городе. Людям дают оценку: у кого хороший рейтинг, может пользоваться всеми благами, льготами и тд., а у кого наоборот, не может даже купить билет на самолет. Также, и в компаниях, такие системы глубинного обучения смогут защитить, вовремя сообщив сотрудникам о существующей проблеме.

Роботы в видеонаблюдении.

Еще в 2016 году было заметно значительное увеличение количества беспилотных транспортных решений, представленных на выставках по безопасности. в первую очередь это автономные беспилотные летательные аппараты – АБПЛА и автономные беспилотные наземные

транспортные средства – АБНТС. Интересно, что беспилотники раньше использовались только в военных целях, а сейчас уже растет рынок потребительских летательных аппаратов, перспективы коммерческого применения которых в сфере безопасности предприятия крайне интересны и имеют хорошие возможности для роста. Пока коммерческих предложений таких продуктов в сфере безопасности крайне мало ввиду новизны. Эксперты утверждают, что беспилотные летательные аппараты будут востребованы на большинстве крупных промышленных производств, в энергетике, в фармацевтических компаниях, в нефтяной и газовой отраслях, в аэропортах, и на правительственных объектах. Идеальное решение по безопасности должно иметь стопроцентное покрытие территории учреждения, предприятия или организации. Пока стационарное оборудование не будет способно обеспечить стопроцентный охват, дроны и роботы способны выступать в качестве «мультипликаторов повышения эффективности» для содействия охранным подразделениям.

При этом беспилотные устройства осуществляют выполнение обычных рутинных задач, а персонал службы охраны выполняет более специфические, требующие участия человека задачи.

Есть две основные функции, предусмотренные для дронов и роботов в коммерческой безопасности: обход и сигнализация. и дроны, и роботы могут быть использованы для предварительно программируемого обхода объекта, для постоянного круглосуточного патрулирования.

Есть свои плюсы и минусы у каждого из типов беспилотных аппаратов. Дроны могут летать на высоте и таким образом обеспечивать обзор большой территории объекта, в то время как робот на земле может только покрывать такой же обзора, как и человек. Но, дрон может работать не более 1 часа, а работ имеет преимущество по временному показателю – может работать более 8 часов. к примеру, робот Sharp’s INTELLOS (АБНТС).

Другое преимущество роботов перед дронами – их возможность переносить на себе многочисленные сенсоры и различные камеры. Дроны могут иметь только одну профессиональную основную камеру, и, может быть, дополнительный источник света или тепловизор. в то время робот может иметь любое количество камер, обеспечивая поле зрения на 360 градусов, дополнительные датчики, такие как радиолокационная станция, лазерный эхолокатор, датчики радиационного, биохимического контроля, радиосвязь и так далее. Но минус работы роботов – это оповещение и сигнализация.

Дроны довольно мобильны и быстры, и, когда тревога включается при нарушении периметра, они могут прибыть на место происшествия сразу же и обеспечить передачу видеосигнала. Это может также сдерживать нарушителей или обеспечить визуальный контроль над ситуацией до прибытия работников службы охраны для задержания нарушителей.

Многие эксперты отрасли утверждают, что компании-производители дронов и роботов будут работать в тесном сотрудничестве с поставщиками оборудования систем видеонаблюдения. Потому что очень важно интегрировать встроенную запись видео, разные сенсоры и статус такого транспортного средства в единой системе управления видеонаблюдением.

HD CCTV.

HD CCTV (High Definition Closed-Circuit Television) это технология, предоставляющая изображение высокого качества по коаксиальному кабелю нескольких стандартов. Это: RG-59, RG-6, RG-11, с разрешением 720p и 1080p. Спрос на данную технологию в видеокамерах и регистраторах в соответствии с прогнозами будет стремительно расти в 2018-2020 годах.

Почему HD CCTV оборудование?

- Низкая стоимость;
- Максимальная длина магистрали больше чем в IP решениях;
- Уже запущены в серию камеры с большей разрешающей способностью, включая камеры с разрешением 4К;
- Хорошими на небольших предприятиях, так как они не так масштабируемы как IP;
- Возможность обеспечивать питание видеокамер через коаксиальный кабель. Данный кабель

практически незаменим, если требуется решить вопрос с большими расстояниями. Его можно использовать даже на расстояниях больше 600 метров.

- Возможность использовать в сложных условиях, при использовании коаксиального кабеля.

Суммируя, можно сказать, что сейчас наблюдается множество современных трендов, требующих современного решения от производителей физических и инженерно-технических устройств, видеонаблюдение тому не исключение. Поэтому, стоит рассмотреть предложения нынешних лидеров рынка в данном сегменте, проанализировать и оценить их деятельность. Для анализа была выбрана немецкая компания – Mobotix.

Компания Mobotix занимает пятое место на рынке видеонаблюдения в мире. в регионе EMEA («Европа, Ближний Восток, Африка») доля рынка компании составляет 16,3 процента, и она занимает второе место. в сегменте мегапиксельных камер видеонаблюдения Mobotix является лидером мирового рынка. Именно поэтому выбор данной компании для анализа ее деятельности был неслучайным.

Чтобы более точно оценить работу компании, важно идти по определенной структуре, описав каждый пункт. в первую очередь – это:

- Общая информация
- Продукция и услуги компании
- Особые кейсы

Начать стоит с базового – с общей информации. Компания основана в 1999 году. Mobotix ведет продажи по всему миру. Штаб-квартира компании находится в городе Лангмайль, земля Рейнланд-Пфальц, Германия. Имеется филиал в Нью-Йорке, США.

Компания Mobotix AG выпускает сетевые камеры высокого разрешения, а также аксессуары для их установки и ПО для управления их работой.

Также, предоставляет продукцию более чем в 70 странах, имеет около 350 сотрудников и достигла в 2016 финансовом году оборота в 63,1 миллиона евро. Компания Mobotix имеется ряд дистрибьюторов в России, Украине и Белоруссии.

В Mobotix концепция видеонаблюдения децентрализована. IP-камеры видеонаблюдения производства Mobotix являются интеллектуальными – они снабжены встроенным процессором. Децентрализованный подход был настолько революционным, что навсегда изменил индустрию видеонаблюдения, а Mobotix здесь первопроходец. Поскольку их камеры полностью управляет сами собой, дорогие централизованные системы больше не требуются. Платформа децентрализованной системы Mobotix потребляет сравнительно небольшую вычислительную мощность, даже в мегапиксельных разрешениях, поэтому она более экономична и масштабируема по сравнению с традиционными. Эта система недорога в обслуживании, практически его не требует, система экономит значительные средства на протяжении всего срока эксплуатации.

Компания предоставляет следующие продукты и услуги по безопасности:

- Наружные камеры
- Камеры для помещений
- Тепловизионные камеры
- Камеры MOBOTIX MOVE
- Контроль за доступом к объекту

Камеры снимают в нескольких разрешениях и бывают разного функционала:

- 180° Fisheye
- 103° Ультраширокоугольный
- 90° Сверхширокоугольный
- 60° Широкоугольный
- 45° Стандартный
- 15° Дистанционный телеобъектив
- 31° Tele
- 8° Сверхширокоугольный

Реализовала свои услуги и продукты в следующих отраслях:

- Промышленность
- Розничная торговля
- Образование и наука
- Здравоохранение
- Логистика и на всей цепями поставок
- Государственные учреждения
- Туризм
- Общепит

Также предлагает свою систему кибербезопасности видеокамер «Кактус». Это уникальная разработка в сфере безопасности видеокамер. Она используются для надежной и полной защиты комплексных охранных видеосистем. Защитит от серьезных хакерских атак с помощью интеллектуальной архитектуры, которая всегда готова к работе и может противостоять любым вызовам и DDoS-атакам. Чтобы повысить уровень сетевой безопасности и защитить частную жизнь, в IP-камеры Mobotix встроила большое количество специальных технологий безопасности.

Помимо всего этого, видеосистемы являются одними из самых качественных и прочных в отрасли к тому же с очень выгодными предложениями. Многие модели камер видеонаблюдения Mobotix рассчитаны на работу в экстремальных условиях. Уличные камеры Mobotix помещаются в корпус из пластмассы, армированной стекловолокном. Профессиональная система управления видео и анализом видеоданных являются частью комплексной системы, которая предлагается бесплатно и без каких-либо лицензионных сборов. Также бесплатно предоставляются обновления для загрузки.

Примечательно, что помимо всего этого, предоставляется ПО (MxMC) MxManagementCenter компании MOBOTIX — программное обеспечение для управления видеосистемами на любых носителях. MxAnalytics — интегрированный в камеру анализ видеоданных. Позволяет сохранять статистические данные о поведении людей и объектов. MxApp — мобильное управление видеосистемами. Благодаря ему, с телефона можно наблюдать за тем, что происходит у Вас в компании из любой точки планеты.

Также, в компании предоставляют услуги по контролю за доступом к объекту. Благодаря интеллектуальной системе видеоанализа видеокамеры регистрируют движения в поле зрения и подозрительные шумы, автоматически включая видеозапись для обеспечения доказательств и немедленно отправляет сообщение жильцам или в ЧОП.

Наглядно видно, что данная компания по праву является одним из лидеров сегмента. Далее стоит рассмотреть кейсы, которые были реализованы в некоторых сферах.

Первый кейс – Montebello USA.

Городская автобусная компания Montebello (MBL) является третьим по размеру оператором общественного транспорта в городе Лос-Анджелес, штат Калифорния, с годовым пассажиропотоком более 8,2 миллиона человек. в рамках своей обязанности заботиться и обеспечивать безопасность своих пассажиров и водителей автобусов агентству требовалось подходящее решение для обеспечения физической и инженерно-технической безопасности, которое позволило бы быстрее реагировать на инциденты. Вдохновленный желанием использовать как можно меньше камер на каждой машине, а также потребностью в системе, достаточно надежной, чтобы выдерживать каждый день постоянную вибрацию, высокую температуру и пыль, компания MBL выбрала системное решение Mobotix. Каждая машина, оснащенная системой видеонаблюдения, имеет пять камер FlexMount S15 с двумя 6-мегапиксельными датчиками изображения. Они обеспечивают детальный обзор внутренней и внешней зоны автобуса и даже могут обнаружить людей и номерные знаки. MBL тесно сотрудничал с Transit Security Systems Inc. для разработки платформы управления, которая включает в себя решение для просмотра и архивирования видео, а также возможности отслеживания и оповещения об инцидентах. Таким образом, любая машина

может отслеживаться в реальном времени, а любая информация сохраняется и остается для расследования инцидентов или для глубокого обучения видеокамер.

В пилотном проекте систему установили на семи автобусах, и реакция была чрезвычайно положительной. Именно поэтому компания MBL заключила контракт на установку видеосистем с Mobotix.

Следующий, не менее интересный кейс связан с одной из крупнейших транспортно-логистических компаний мира – Bolloré Logistics.

Складские и транспортные мощности вблизи аэропорта Окленда, Новая Зеландия, в последние годы значительно выросли и зачастую обрабатывают более 2000 единиц продукции в день. Там расположен склад под таможенной пломбой, именно поэтому на этой территории действуют строгие правила безопасности. Поэтому все перемещения и обработка на складе должны тщательно контролироваться, так как последствия повреждения оборудования или потери запасов могут иметь катастрофические последствия. Сочетание камер полусфер конфигураций c25, v25 и i25, а также нескольких камер Mobotix Dual D15 обеспечивают полное покрытие участка площадью 6 600 квадратных метров. Новая система обеспечивает полную видимость проходов склада, чтобы защитить как сотрудников, так и клиентов в случае возникновения инцидентов.

Система безопасности, которая позволяет отслеживать бизнес-процессы и гарантирует доступность отснятого материала, может помочь компаниям избежать дорогостоящих исков о компенсации. Таким образом, система Mobotix является бесценным инструментом для управления рисками, обеспечивает соблюдение прав сотрудников, их защиту и разрешение споров с контрагентами. Более того, такая система безопасности помогла сэкономить деньги логистическому оператору: некоторые страховые компании уменьшают проценты по страховым взносам, когда эта система установлена.

Брайан Клоу, специлист Auckland Security Cameras сказал: «Это лучший пользовательский интерфейс, который я когда-либо видел, с точки зрения конечного пользователя. Это очень интуитивно понятно. Он отлично работает и очень прост в использовании.» Что несомненно говорит о том, что услуги и продукты компании Mobotix ценят даже конкуренты.

Подытожив все проанализированное выше, можно сделать вывод, что компания предоставляет целый ряд услуг по физической и инженерно-технической безопасности: от защиты персонала до наблюдения в реальном времени из любой точки планеты за нужным объектом.

Помимо этого, компания имеет все возможности чтоб себя реализовываться дальше, их всех озвученных трендов, они еще не используют беспилотники и роботов, но по инсайдерской информации, они рассматривают в будущем подобные кроссоверы. Как отмечают многие конкуренты, подобных технологий как Mobotix просто еще нет на рынке.

Слова коммерческого директора IBC Raif GmbH Норберта Э. Райфа это подтверждают: «После установки камер продолжительность простоев на складах в среднем сократилась на 25-30 %. По-моему, на рынке сейчас просто нет систем со сравнимыми возможностями.»

В данном исследовании были решены вышеупомянутые задачи об определении нынешней ситуации на рынке систем видеонаблюдения, изучении аспектов деятельности компаний на этом рынке, анализа деятельности одной из выбранных компаний-лидеров и оценки этой деятельности.

Также, в ходе представленной работы были сделаны выводы о том, как работают различные системы видеонаблюдения, в каких сферах экономики они задействованы. Были рассмотрены примеры того, как они используются и дана оценка не только моя, но и известных в этой сфере специалистов, что только подтверждает актуальность темы и перспективность той компании, которой говорилось в работе.

Исходя из описанного выше, был сделан вывод, что мировой рынок устройств физической и инженерно-технической безопасности постоянно развивается и каждый сегмент отвечает на современные требования, в частности сегмент систем видеонаблюдения.

Что же можно предложить в данной ситуации, описанной в работе? Каждый пользователь систем видеонаблюдения должен с трепетом и осторожностью относится к их работе. Многие специалисты отмечают, что люди не относятся со всей серьезностью к процессу видеонаблю-

дения ввиду своей необразованности в этой сфере. Многие компании переучивают сотрудников и объясняют им всю «соль» того, если они будут вводить простые пароли на доступ к камерам, не следить за их состоянием, не отвечать вовремя на инциденты; камера бесперебойно сработает и сделает оповещение, а как это воспримет сотрудник охраны зависит уже от его квалификации.

Помимо этого, я считаю, что любая компания, если ей важна безопасность ее материальных ресурсов, ее персонала, то она просто обязана заниматься установкой видеосистем, дабы предупреждать различного рода инциденты и споры.

Слова коммерческого директора IBC Raif GmbH Норберта Э. Райфа это подтверждают: «После установки камер продолжительность простоев на складах в среднем сократилась на 25-30 %. По-моему, на рынке сейчас просто нет систем со сравнимыми возможностями.»

Список использованных источников:

1. Шульц В.Л., Рудченко А.Д., Юрченко А.В. Безопасность предпринимательской деятельности: учебник для академического бакалавриата / В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко ; под науч. ред. В. Л. Шульца. — М. : Издательство Юрайт, 2016. — 237с.;
2. 2016 Финансовый отчет/ Jahresabschluss zum Geschäftsjahr vom 1. Oktober 2014 bis zum 30. September 2015 der Mobotix AG. In: https://www.bundesanzeiger.de [Электронный ресурс], 1. April 2016, abgerufen am 1. August 2016, свободный;
3. Блог компании Интемс: [Электронный ресурс] – 2018. – Режим доступа: https://securityrussia.com/blog/cctv-trendy.html, свободный;
4. Security News. Информационно-аналитическое издание по техническим средствам и системам безопасности: [Электронный ресурс] – 2016. – Режим доступа: http://www.secnews.ru/foreign/22525.htm#axzz5m6TxwkSB, свободный;
5. Security News. Информационно-аналитическое издание по техническим средствам и системам безопасности: [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/company/mobotix#axzz5m6TxwkSB, свободный;
6. Mobotix. Кейс компании Montobello: [Электронный ресурс]. – Режим доступа: https://www.mobotix.com/en/solutions/transport-and-mobility/montebello, свободный;
7. Mobotix. Кейс компании Bolloré Logistics: [Электронный ресурс]. – Режим доступа: https://www.mobotix.com/en/solutions/logistics-shipping/bollore, свободный;
8. Mobotix. Инструмент Kardex MLOG: [Электронный ресурс]. – Режим доступа: https://www.mobotix.com/ru/kardex-mlog, свободный;
9. Mobotix – Aktuelle Meldungen im Überblick: [Электронный ресурс] – 2007. – Режим доступа: https://www.mobotix.com/de/node/2007, свободный;
10. Mobotix – eine Nischenfirma wächst um das Siebzigfache. In: Wirtschaftswoche: [Электронный ресурс] – 2014. – https://www.wiwo.de/unternehmen/mittelstand/mittelstand-mobotix-eine-nischenfirma-waechst-um-das-siebzigfache-/7662326.html, свободный.

ВЕТРОВА ВИКТОРИЯ ОЛЕГОВНА
студентка факультета социальных наук
НИУ ВШЭ, г. Москва
E-mail: vovetrova@edu.hse.ru

АНАЛИЗ ПРОФЕССИОНАЛЬНОЙ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ В ЯПОНИИ.

VETROVA VIKTORIA OLEGOVNA
student, faculty of social sciences
National Research University «Higher School of Economics», Moscow

THE ANALYSIS OF PROFESSIONAL CRIMINAL ACTIVITY IN JAPAN.

Аннотация: Данная работа посвящена японской организованной профессиональной преступной деятельности, которая называется якудза. в статье описаны история появления якудза, ее характеристики и известные традиции. Также в работе рассматриваются основные направления деятельности преступных группировок в Японии и причины недостаточно эффективных способов борьбы с ними. Особое внимание уделяется вопросу основных отличий преступных группировок Японии от преступных формирований в остальном мире. в работе сделана попытка ответа на следующий исследовательский вопрос: что способствует столь продолжительному существованию организованной профессиональной преступной деятельности в Японии? В статье названы основные причины, которые способствовали сохранению организованных преступных группировок на территории Японии в период с 17 века до наших дней, а также указаны причины неэффективной борьбы с ними.

Abstract: This work is devoted to Japanese organized professional criminal activity, which is called Yakuza. The article describes the history of the Yakuza, its characteristics and well-known traditions. The paper also discusses the main activities of criminal groups in Japan and the reasons for the lack of effective ways to combat them. Special attention is paid to the main differences between criminal groups in Japan and criminal groups in the rest of the world. The paper attempts to answer the following research question: what contributes to such a long existence of organized professional criminal activity in Japan? The article identifies the main reasons that contributed to the preservation of organized criminal groups on the territory of Japan in the period from the 17th century to the present day, as well as the reasons for the ineffective fight against them.

Ключевые слова: Якудза, японская мафия, главные особенности якудза, борьба с организованной преступностью в Японии.

Key words: Yakuza, the Japanese mafia, the main features of the Yakuza, the fight against organized crime in Japan

Введение

Организованная профессиональная преступная деятельность в Японии, якудза, появилась еще в 17 веке и продолжает существовать до сих пор. Это свидетельствует о том, что преступные группировки Японии имеют свои характерные черты, которые позволяют им продолжать легально существовать и заниматься активной деятельностью в стране. Несмотря на то, что якудза занимается запрещенными азартными играми, вымогательством, проституцией, продажей наркотических средств и т.д., у нее все равно есть довольно прочная взаимосвязь с правоохранительными органами страны. Для того чтобы понимать, какие есть способы борьбы с преступной деятельностью в Японии и почему они до сих пор не работают в полной мере, необходимо разобраться

в источниках могущественности якудза и определить, что позволяет ей легально существовать столь продолжительный период времени на территории страны.

В настоящий момент существует недостаточное количество работ, которые посвящены японской организованной преступности, которая называется якудза. Существующие работы основываются либо на определенных видах деятельности преступных формирований в Японии, либо рассказывают

о современных тенденциях якудза. При этом, практически нет работ, в которых бы выделялись конкретные характеристики, отличающие организованную преступную деятельность в Японии от других преступных группировок. в данной работе сделана попытка ответить на следующий исследовательский вопрос: что способствует столь продолжительному существованию организованной профессиональной преступной деятельности в Японии?

Цель работы – выделить основные характеристики, отличающие якудза от других преступных группировок мира, и позволяющие ей существовать на территории Японии такой продолжительный период времени.

Для того чтобы ответить на исследовательский вопрос, были поставлены следующие задачи:

- составить историческую справку о профессиональной преступной деятельности в Японии;
- рассмотреть ключевые сферы деятельности якудза;
- охарактеризовать основные отличительные черты японских преступных группировок;
- проанализировать причины неэффективности борьбы с якудза в Японии.

В данной работе используется информация из существующих статей, написанных по теме организованной профессиональной преступной деятельности в Японии. Для написания работы были использованы следующие статьи:

- Квашис В.Е., Морозов Н.А. Организованная преступность в Японии // Научный портал МВД России. №4. 2013. С.121-130.

В данной статье авторы обращают особое внимание на основные отличия преступных групп в Японии от организованных преступных формирований в других странах, а также делают акцент на причины вовлеченности молодежи из беднейших слоев населения в организованные преступные группировки Японии.

- Куршев М. Характеристики японской мафии якудза // Уголовное право. №1. 2006. С.133-139.

В своей статье автор приводит подробный анализ основных новых тенденций в деятельности якудза. Кроме того, Куршев М. пишет об отличительных характеристиках японской мафии, которые выделяют ее среди других преступных группировок в мире.

- Коробеев А.И., Морозов Н.А. Особенности современной организованной преступности в Японии // Криминологический журнал Байкальского государственного университета экономики и права. №3. 2013. С.159-164.

В данной работе авторы обращают особое внимание на особенности сфер деятельности якудза на современном этапе развития Японии. Коробеев А.И. и Морозов Н.А. анализируют различные события, связанные с деятельностью якудза, начиная с момента появления этих преступных группировок до 2012 года.

Для написания работы были дополнительно использованы различные интернет-ресурсы, находящихся в свободном доступе, которые предоставили выборочную информацию по теме работы.

Основная часть

Организованная преступность не является чем-то необычным в настоящее время и может встретиться в любой точке нашей планеты. Под организованной преступностью стоит понимать негативное социальное явление, которое характеризуется сплочением криминальной среды. По-

нятие организованной преступности подразумевает под собой уголовные виды деятельности, осуществляющиеся группами, имеющими внутреннюю структуру. Выполнение данных видов уголовной деятельности дает возможность членам организованных профессиональных преступных групп получать финансовую прибыль и приобретать власть. в докладе Генерального секретаря ООН «Воздействие организованной преступной деятельности на общество в целом» (1993) приведена обобщенная характеристика организованной преступности:

1. Организованная преступность предоставляет законные товары и услуги в незаконной форме или же предоставляет незаконные товары, извлекая из данного вида деятельности экономические выгоды.
2. Под организованной преступностью предполагается конспиративная преступная деятельность, которая осуществляется структурами, имеющими четкую иерархию. в результате данной деятельности происходит планирование и осуществление незаконных деяний или достижение законных целей, но при помощи незаконных средств.
3. Организованные преступные группы стремятся к получению более высоких доходов, путем установления частичной или полной монополии на поставку товаров или предоставление услуг.
4. Организованная преступность занимается не только незаконными видами деятельности или предоставлением незаконных услуг, но и специфическими видами деятельности, как, например, «отмывание» денег через законные экономические структуры.

Организованные преступные группировки можно встретить по всему миру. Самые известные из них — это Сицилийская мафия, Коза Ностра, а также Русская мафия, известная как «воры в законе».

Якудза – так называется традиционная форма организованной преступности в Японии, группировки которой занимают лидирующее положение в криминальном мире страны. Членов данной организованной преступной группировки называют «гокудо». в настоящее время можно услышать официальное название преступных группировок

в Японии - «boruokudan» (слово «boruoku» означает насилие, а слово «dan» означает банду). Стоит отметить интересный факт, что слово якудза означает цифры 8 («ya»), 9 («ku»), 3(«za»), которые в свою очередь считаются худшей комбинацией цифр в японской традиционной карточной игре «hanafuda». Изначально, слово «якудза» означало «ненужный» («ya-ku-ta-ta-za») и применялось к людям, которые ничего не значили в обществе [Куршев, 2006].

Появление якудза, ее главные особенности и иерархическая структура

Как известно, появление якудза датируется серединой 17 века. «Ее предшественниками являются три группы полукриминальных и криминальных сообществ: городские стражи – мати-ёко, торговцы-«коробейники» - тэкияи, профессиональные картежники – бакуто» [Коробеев, Морозов, 2013]. Члены данных полукриминальных сообществ были бедными людьми, которые постоянно шли против закона. Спустя некоторое время они объединились в своего рода «семьи» и начали заниматься грабежами. к началу 20 века организованная преступность глубоко проникла во всех сферы жизни Японии. Однако наиболее ускоренные темпы развития преступности связаны с послевоенным временем. Вторая мировая война сильно ослабила Японию. Из-за войны в Японии начался экономический и политический кризисы, население страны пребывало в подавленном настроении, а высокий уровень безработицы в послевоенное время привел к развитию черного рынка.

Примерно с конца 1970х годов и до 1985 года можно говорить о «золотом веке» профессиональной организованной преступности в Японии [Квашис, Морозов, 2013]. в этот промежуток времени якудза начала активно включаться в систему международной преступности. Взаимодействуя с партнерами из зарубежных стран, члены японских преступных группировок занимались нелегальным ввозом в страну иностранной рабочей силы, налаживанием контактов с российски-

ми группировками, которые работали в сфере торговли оружием, биоресурсами и автомобилями. в эти годы полиция не могла справиться с японской мафией, в то время как деятельность якудза становилась все масштабнее.

К 1980 году Япония была охвачена наркоманией. Якудза получала колоссальную прибыль от торговли наркотическими веществами. При этом, полиция выявляла лишь примерно 5% от всего объема поставляемых наркотических средств в страну. Основным слоем населения, который приобретал наркотики у якудза, оставались бедные люди. При этом, закупка одного грамма наркотического вещества за границей обходилась в 3 тыс. иен., в то время как покупка в Японии была равна 130 тыс. иен [Коробеев, Морозов, 2013]. Такая сильная разница в стоимости наркотиков за границей и в Японии приносила якудза огромные доходы. к концу 20 века организованная преступность в Японии получала годовой доход, который не уступал выручке концерна «Тойота». Такие колоссальные доходы якудза заставляли обычных граждан верить в законность деятельности преступных группировок.

Главные особенности деятельности членов преступных группировок в Японии были заложены еще в феодальный период. Существует два принципа, которых придерживается якудза: «вовремя появиться там, где возникают трудности с решением тех или иных проблем» и «сотрудничество с властями» [Квашис, Морозов, 2013]. Особенностями якудза от других преступных образований является то, что она не имеет четких территориальных зон влияния, не опирается на родственные связи как на структурную основу своей организации и не старается держать в тайне свою внутреннюю иерархию, численность и состав руководства.

Можно услышать, что объединения якудза называют семьями, но это лишь символически. На самом деле между членами профессиональных преступных группировок, как правило, нет никакого родства. Отношения, которые связывают между собой членов преступной группировки, можно назвать квазисемейными. В данном случае подразумевается система «оябун – кобун», где оябун – это условно отец, а кобун – условно сын. «Такая иерархическая система характерна не только для якудза: по такому же принципу свои неформальные отношения строят компании, политические партии, общественные организации в Японии» [Маков, 2013]. Взаимоотношения среди членов профессиональных преступных группировок иногда рассматриваются как более крепкие, чем отношения в других коллективах. Крепость взаимоотношений особенно хорошо видна, когда речь идет об исполнении приказа главы преступной группировки. Для члена преступной группы ослушаться главу банды (оябуна) считается страшной провинностью. Если же якудза по каким-то причинам не выполнил задание главы группировки, для искупления своей вины он совершает ритуал — отрезает последнюю фалангу мизинца. Если же это не первый проступок, то отрезается безымянный палец. Этот ритуал называется юбитсуме, и появился он еще в древней Японии. в те времена ритуал имел не только символическое, но и практическое значение: «без мизинца или его части воину было гораздо сложнее орудовать мечом, что делало его более зависимым от хозяина и других участников коллектива, перед которыми он провинился» [Маков,2013]. Заступиться за своего товарища – поступок, заслуживающий уважения среди членов преступной группы в Японии.

На рисунке 1 представлена иерархическая структура, которая свойственна японским организованным преступным группировкам. Как видно на рисунке, самым главным во всей иерархии считается оябун. Ему непосредственно подчиняются сайко комон, а также главы низовых подразделений (вака-гасира, который считается главным у нескольких групп бандитов одного региона, и сятэй-гасира). Сингиин и кайкэй подчиняются непосредственно сайко комон. Вака-гасира и сятэй-гасира командуют командирами различных рангов (кё дай и сятэй), новичками и стажерами.

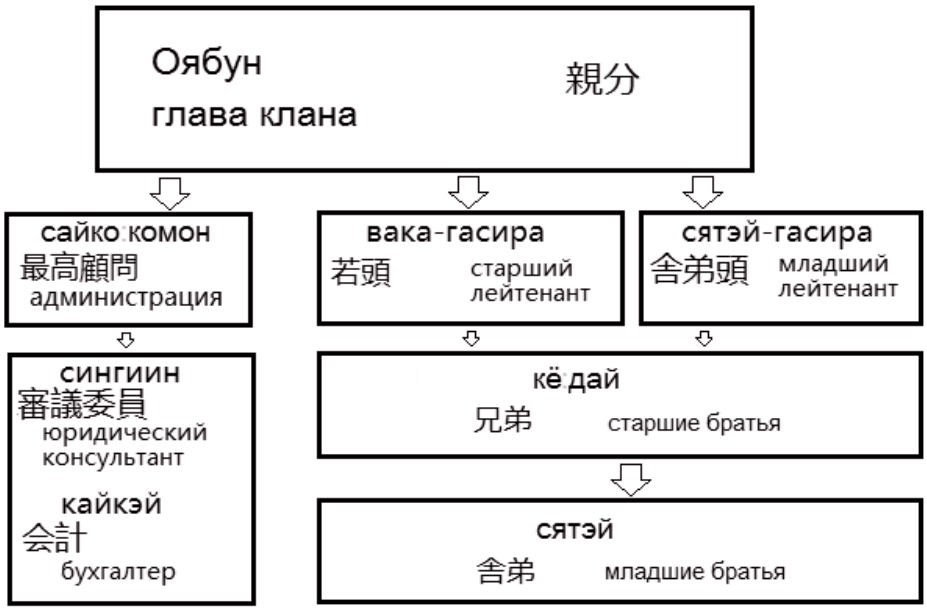


Рисунок 1. Иерархия якудза. Источник: https://upload.wikimedia.org/wikipedia/commons/a/a9/Yakuza_hierarchy_ru.png

Сферы деятельности якудза

Организованная преступность в Японии слишком глубоко пронизывает все сферы общества еще с давних времен, поэтому в массовом сознании стало явлением практически естественным. В публицистике феномен якудза часто рассматривается как модель мирного сосуществования государства и «мафии». Еще с момента появления якудза государство прибегало к ее помощи, для того чтобы утихомирить недовольных постоянным голодом бедняков или подавить бунт крестьян, которые были возмущены слишком высокими поборами. Например, еще в 1934 году государство обратилось за помощью к якудзе, чтобы прекратить бунт портовых рабочих в Кобе. в результате все профсоюзные лидеры были убиты членами преступных группировок. Правительству Японии достаточно выгодно было сотрудничество с преступными группировками, так как они могли применить силу в тех ситуациях, когда определенные действия могли скомпрометировать правящих лиц [Новикова,2012].

В настоящее время самыми крупными синдикатами якудза являются Ямагути-гуми, Сумиёси-кай, Инагава-кай. Эти три синдиката образуют так называемую «большую тройку». в «большую тройку» входят более 70% членов всей японской организованной преступности. При этом, только один синдикат Ямагути-гуми включает в себя примерно 45% всех членов организованных профессиональных преступных группировок. Синдикат Ямагути-гуми основали в 1915 году. Своё название синдикат получил в честь основателя – Харукити Ямагути. в период с 1946 по 1981 г. синдикат

Ямагути-гуми возглавлял Кадзуо Таока. Он считается одним из самых легендарных боссов якудза. Благодаря этому человеку, Ямагути-гуми стал самым мощным синдикатом, который контролировал огромное количество нелегальных областей деятельности в Японии.

Деятельность якудза включает запрещенные азартные игры, торговлю наркотиками и оружием, вымогательство, контрабанду, а также проституцию. Довольно часто якудза занимается специализированной японской формой вымогательства, которая называется «сокайя». Якудза запугивают акционеров крупных компаний, таким образом получая право на участие в совещаниях, а также право на небольшую покупку акций.

Якудза оказывают сильное влияние на профессиональную японскую борьбу, которая назы-

вается «пурорэсу». Поддержка бойцов и проведение данного рода мероприятий имеет для якудза чисто финансовый интерес, так как члены преступных группировок получают некий процент от сборов [Kaoru, 2011].

Расследовать дела, связанные с деятельностью якудза, особо сложно, так как попасть в данное закрытое общество практически невозможно. Якудза – это общество с строжайшей системой наказаний и кодексом молчания. Специфика японской модели организованной преступности в том, что преступные организации функционируют вполне легально, подобно обычным фирмам. Члены организованных преступных группировок имеют визитные карточки, которые украшены эмблемой банды. Символ клана может быть также изображен на одежде, различной сувенирной продукции. На рисунке 2 представлены эмблемы самых крупных синдикатов, действующих в Японии. Адреса штаб-квартир преступных группировок печатаются в различных справочниках. Каждая преступная группа имеет свой официальный гимн, а также выплачивает членам преступной группировки пенсионные пособия. Самые крупные синдикаты в Японии владеют собственными печатными изданиями. Все это указывает на то, что профессиональные преступные группировки ни от кого не скрываются и действуют на территории максимально открыто.

Рисунок 2. Эмблемы крупнейших синдикатов якудза. Источник: https://upload.wikimedia.org/wikipedia/commons/thumb/5/5a/Yamabishi.svg/1280px-Yamabishi.svg.png

Стоит отметить интересный факт: количество организованных преступников на душу населения, действующих на территории Японии, очевидно больше, чем в таких странах, как: Россия, США или Италия. При этом, вред, наносимый обществу от японских организованных профессиональных преступных группировок значительно ниже. Японская полиция рассматривает членов организованных преступных группировок не как бандитов, которые стремятся нанести максимальный ущерб обществу, а как своих возможных союзников в области сдерживания неорганизованной преступности. На примере Японии можно увидеть возможность сосуществования общества и организационной преступности. При этом, и та, и другая сторона считает данное сосуществование оптимальным.

Якудза можно сравнить с мафией. Она состоит из отдельных «семей», в которых четко соблюдается иерархический порядок. Несмотря на то, что якудза схожа с мафией, существует значительное отличие. в Японии существует около 4000 официальных бюро, принадлежащих якудза, что характеризует деятельность данной преступной группировки как обычной организации. Кроме того, в отличие от мафии, якудза могущественнее, особенно в политической сфере.

Субкультура якудза

Обращаясь к субкультуре якудза, стоит отметить тот факт, что члены данной организованной преступной группировки воспринимают ее как «настоящую» семью. По негласному кодексу якудза должен терпеливо переносить боль, голод, обязан хранить в строжайшем секрете информацию о группировке, исполнять все приказы и с особым уважением относиться к членам группы, которые старше по рангу. Кроме того, якудза не имеет права употреблять наркотики, совершать противоправные действия против посторонних граждан. Данная субкультура также характеризуется враждебностью к чужакам, презрением к боли, страху. Членам данной преступной организации запрещены контакты с деятелями из экономической и политической сферы деятельности. Все члены преступной группировки обязаны работать до самой смерти [Куршев,2006].

Еще одной известной отличительной чертой якудза являются громадные татуировки, кото-

рые могут покрывать все тело члена профессиональной преступной группировки. Первая причина, по которой якудза хотят нанести на свое тело как можно больше татуировок, — это стремление показать свою силу духа и отсутствие страха перед физической болью. Стоит обратить внимание на тот факт, что такие татуировки наносятся на тела членов преступных группировок вручную, без использования специальной техники. Именно поэтому процесс нанесения татуировки может занять даже несколько лет. в большинстве случаев, члены группировок тщательно скрывают эти татуировки от посторонних людей [Маков, 2013]. Татуировки являются традицией, они наносятся в виде драконов, змей, мифических фигур.

Стоит отметить тот факт, что якудза разработала свой собственный секретный язык, который называется «ingo». Этот язык может подвергаться изменениям в зависимости от места и времени его использования. в данном языке используются сокращенные слова; фразы, произнесенные на китайский манер; совершенно новые слова. Невербальный секретный язык якудза состоит из целого набора телодвижений, которые имеют свое значение [Куршев, 2006].

Борьба с якудза

Каждое государство ставит перед собой цель – эффективная борьба с преступностью. Борьба с якудза представляла ряд сложностей еще в период ее расцвета. На данный момент противодействие организованным преступным группировкам все так же остается затрудненным. Есть ряд объективных факторов, которые в ощутимой мере усложняют борьбу с якудза.

Стоит отметить, что 1991 год является особо важным для Японии в области противодействия организованной профессиональной преступности. Именно в этом году появился «Закон о предотвращении противоправных деяний членами преступных банд». В этом законе был определен ряд понятий преступной группировки, который был значительно ограничен определением – «совершающая насильственные действия». Появление данного закона в некотором роде дало успех. С 1991 года значительно снизилось количество членов преступных группировок в Японии. Из-за того, что деятельность якудза стала ограничиваться законом на территории страны, члены преступных группировок стали активно перебираться за рубеж. На данный момент якудза охватывает почти все страны Юго-Восточной Азии, проводит активную деятельность в США (Гавайи) и в Европе [Куршев,2006]. Например, якудза использует Гавайи как промежуточный пункт между Японией и США, для того чтобы вести деятельность по сбыту наркотических средств в США и вывозу огнестрельного оружия в Японию.

Якудза может заниматься подкупом полицейских, которые в дальнейшем будут за одно с членами преступных групп. Низовые чины полиции и якудза ведут порой взаимовыгодное сотрудничество, в сфере борьбы с насилием, преступностью, беспорядками. Именно это приводит к тому, что иногда полиция просто может закрыть глаза на деятельность якудза или даже заранее предупредить о готовящихся облавах на группировку. Очевидно, что такое сотрудничество якудза и полиции затрудняя борьбу с организованной преступностью в стране [Коробеев, Морозов, 2013].

Кроме того, организованные преступные группировки в Японии занимаются спонсированием правящей партии. Например, Демократическая партия Японии за 2 года до прихода к власти получила одобрение со стороны двух крупных синдикатов: «Ямагути-гуми» и «Инагава-кан». Соответственно, преступные группировки пообещали отдать свои голоса за Демократическую партию Японии в обмен на то, что она не пропустит новые законы против организованных преступных групп [Коробеев, Морозов, 2013]. Политические деятели сотрудничают с якудза для того, чтобы получить финансирование в крупных размерах или же найти компромат на своих политических соперников.

Затруднение в борьбе с якудза так же вызывает страх жителей страны перед возможными репрессиями со стороны преступных группировок. Именно этот страх снижает готовность населения давать показания правоохранительным органам. Лишь в 2011 году был создан отряд «антиякудза», целью которого является защита граждан от возможного нападения со стороны членов преступных группировок.

Заключение:

Профессиональная организованная преступность в Японии заслуживает к себе особого внимания. Якудза зародилась еще 17 веке и существует до настоящих дней. Это означает, что данная организованная преступная группировка настолько могущественная, что с ней не могут справиться даже власти страны. Если посмотреть на данный аспект с другой стороны, то становится ясно, что порой для властей даже не выгодно бороться с якудза. Эта профессиональная организованная преступная группа, не имея четко прописанного кодекса, справляется с сохранением строжайшей дисциплины и обычаев. Якудза показывает обществу, что она опирается на ценности патриархальной семьи, на принципы четкого выполнения поручений вышестоящих лиц. Исходя из статистических данных, число преступлений, совершаемых в Японии, постепенно снижается, что является положительным трендом. Кроме того, можно заметить, что организованная преступность в современном мире является специфической сферой бизнеса, которая базируется на предоставлении нелегальных товаров и услуг. Главной особенностью данной организованной преступной группировки в Японии считается то, что она действует вполне легально, совсем как обычная фирма. Несмотря на то, что якудза – это организованная преступная группировка, стоит отметить один факт, который показывает якудза немного с другой стороны. Во время землетрясения в Кобе, якудза пришла на помощь населению и предоставила жителям безопасное убежище, воду и продукты. Якудза среагировали на чрезвычайное происшествие даже более оперативно, чем правительство Японии. Возможно, данное стремление к оказанию помощи людям в трудной ситуации можно объяснить тем, что члены якудза в основном изгои общества, которые умеют сочувствовать другим. в настоящее время отмечается снижение количества членов профессиональных преступных группировок в Японии, по сравнению с их числом во время «золотого века» якудза, но при этом количество членов преступных формирований все еще остается довольно внушительным. Таким образом, можно прийти к выводу, что якудза необычный вид организованной преступности, который имеет ряд своих отличительных особенностей. Борьба с якудза является не особо эффективной, так как эти организованные преступные группировки проникли глубоко во всех сферы жизни общества и имеют особую силу в политической сфере. Именно эти факторы позволяют якудза существовать в Японии и других странах мира уже на протяжении столь большого периода времени.

Список литературы:

1. Квашис В.Е., Морозов Н.А. Организованная преступность в Японии // Научный портал МВД России. №4. 2013. С.121-130.
2. Коробеев А.И., Морозов Н.А. Особенности современной организованной преступности в Японии // Криминологический журнал Байкальского государственного университета экономики и права. №3. 2013. С.159-164.
3. Куршев М. Характеристики японской мафии якудза // Уголовное право. №1. 2006. С.133-139.
4. Латов Ю. (2005) Мафия, организованная преступность. Энциклопедия Кругосвет. Универсальная научно-популярная энциклопедия. Получено из https://www.krugosvet.ru/enc/gumanitarnye_nauki/sociologiya/MAFIYA_ORGANIZOVANNAYA_PRESTUPNOST.html
5. Маков В. (2013, Июль 27). Их бог – оябун. Lenta.ru. Получено из https://lenta.ru/articles/2013/07/27/yakuza/
6. Новикова А.А. 2012.03.070 Синявер Э. Достойные партнеры: якудза и государство Японии нового времени // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 9: востоковедение и африканистика. Реферативный журнал. №3. 2012. С.212-216.
7. Kaoru (2011, Сентябрь 16). Справка (об особенностях преступного мира и др.). Tokyo Decadence. Получено из http://xkingdom.rolka.su/viewtopic.php?id=992
8. NEWSru.com (2013). в Японии 65-летний босс крупнейшего клана якудза получил 6 лет тюрьмы за вымогательство. Получено из https://www.newsru.com/crime/22mar2013/snt6yyakuzaboss.html

ДОЛГОПОЛОВА ЮЛИЯ СЕРГЕЕВНА
студентка факультета экономических наук
НИУ ВШЭ, г. Москва
Email: dolgopolovayuliya3@gmail.com

МЕШКОВА ЛЮДМИЛА НИКОЛАЕВНА
студентка факультета экономических наук
НИУ ВШЭ, г. Москва
Email: mila20.01@mail.ru

ПЕРМЯКОВА ВАЛЕНТИНА АНДРЕЕВНА
студентка факультета социальных наук
НИУ ВШЭ, г. Москва
Email: vapermyakova@edu.hse.ru

СЕТЕЦЕНТРИЧЕСКИЕ ПРОТИВОБОРСТВА НА ФИНАНСОВЫХ РЫНКАХ: ПРИЧИНЫ РАСПРОСТРАНЕНИЯ И МОДЕЛИРОВАНИЕ КОНЦЕПЦИИ

DOLGOPOLOVA YULIA SERGEEVNA
student, faculty of economic sciences
National Research University «Higher School of Economics», Moscow

MESHKOVA LYUDMILA NIKOLAEVNA
student, faculty of economic sciences
National Research University «Higher School of Economics», Moscow

PERMIAKOVA VALENTINA ANDREEVNA
student, faculty of social sciences
National Research University «Higher School of Economics», Moscow

NETWORK-CENTRIC WARFARE IN FINANCIAL MARKETS: THE REASONS FOR THE SPREAD AND CONCEPT MODELING

Аннотация: Данное исследование посвящено изучению проблемы сетецентрических противоборств на финансовых рынках. Цель работы состояла в создании обобщенной модели таких противоборств и выявлении причин их распространения. Теоретический анализ позволил проанализировать существующие подходы к классификации манипуляций на финансовом рынке. Кроме того, обзор литературы дал возможность выявить такие эффекты, как эффект подражания, эффект раскачивающейся лодки, коммуникационный эффект и другие, которые объясняют, почему количество людей, вовлеченных в финансовые манипуляции, не уменьшается, а, напротив, увеличивается с каждым годом. Эмпирический анализ состоял в изучении различных кейсов сетецентрических противоборств на финансовых рынках по всему миру. в результате такого анализа удалось выявить общие закономерности и построить обобщенную модель сетецентрических противоборств.

Abstract: This research is devoted to the study of the problem of network-centric confrontation in financial markets. The paper was aimed to create a generalized model of the studied confrontations and identify the reasons for their spread. The theoretical analysis made it possible to get acquainted with existing approaches to classifying manipulations in the financial market. In addition, a review of the literature helped to identify such effects as the imitation effect, the rocking boat effect, the communication effect and others that explain why the number of people involved in financial manipulation increases every year. The empirical analysis consisted of studying various cases of network-centric conflicts in

financial markets around the world. As a result of this analysis, it was created a generalized model of network-centric confrontations.

Ключевые слова: сетецентрические противоборства, информационное поле, генератор, сенсоры, информационные и биржевые противоборства, «клиповость» мышления, эффект толпы.

Keywords: network-centric warfare, information field, generator, sensors, information and exchange confrontations, «clip» thinking, crowd effect.

Введение

Феномен сетецентрической войны (или сетецентрических противоборств) возник сравнительно недавно и применялся лишь к военной сфере. Основоположниками концепции сетецентрических противоборств принято считать А. Сербовски, Дж. Гарстка и Дж. Джонсона. По их мнению, главным элементом такого рода противоборств является достижение информационного и коммуникационного превосходства над противником, которое позволяет увеличить скорость командования [16]. Со временем данная теория развивалась и нашла свое отражение в трудах Ковалева В. И., Малинецкого Г. Г., Матвиенко Ю. А. (2015) [4], Макаренко С. И. (2017) [6], Fewell M. P., Hazen M. G. (2003) [17], которые также изучали процесс проведения сетецентрической войны. Однако до настоящего момента применение сетецентрических противоборств в других сферах деятельности не рассматривалось. в данной работе нами был восполнен существующий пробел, и была предпринята попытка применить концепцию сетецентрической войны к финансовой сфере. Кроме того, помимо создания модели сетецентрических противоборств на финансовом рынке в данном исследовании особое внимание уделяется причинам вовлечения людей в такого рода противоборства. Особый вклад в выявлении причин происходящего внесли работы Елякова А. Д. (2005) [2], Радаева В.В. (2002) [10], Штомпки П. (2015) [14].

В текущем исследовании можно выделить несколько проблем. Во-первых, сложность состоит в том, чтобы научиться распознавать сетецентрические противоборства на финансовых рынках. Во-вторых, необходимо понять мотивацию людей, которые участвуют в данных противоборствах. Ведь умение вовремя выявить сетецентрические противоборства на финансовых рынках позволит лучше понять, как противодействовать такого рода манипуляциям и минимизировать потери от них.

Таким образом, цель данной работы заключалась в решении двух перечисленных выше проблем. Первая была решена с помощью построения обобщенной модели сетецентрических противоборств, а вторая – на основе изучения разнообразных социо- и психологических эффектов, которым поддаются люди, вовлеченные в финансовые манипуляции.

Актуальность данной темы связана с широким распространением рыночных правонарушений на мировых финансовых рынках. Так, например, в России лишь за 2019 год было выявлено 15 случаев неправомерного использования инсайдерской информации и манипулирования рынком. Там, где финансовые рынки более развиты, например, в США количество таких правонарушений гораздо больше. При этом данные манипуляции осуществляются главным образом с помощью достижения информационного превосходства над остальными участниками рынка, что обуславливает применимость термина «сетецентрических противоборств» к финансовой сфере. Таким образом, в данной работе впервые было рассмотрено применение концепции сетецентрической войны к финансовому сектору.

Структура работы такова. Сначала речь пойдет о применимости термина сетецентрические противоборства к финансовым рынкам, затем будет рассмотрена модель совершения таких противоборств. Далее будет дана новая, разработанная нами, классификация сетецентрических противоборств на финансовых рынках. На заключительном этапе будут перечислены основные причины распространения такого рода правонарушений.

Сетецентрические противоборства на финансовых рынках: модель и классификация

Изначально термин «сетецентрические противоборства» появился в военной сфере и представлял из себя новый способ ведения войны. Главным элементом здесь выступает телекоммуникационная сеть обмена данными, которая объединяет средства разведки и наблюдения, средства автоматизации управления и связи, а также боевые платформы в единую систему, что способствует более эффективному ведению войны [4]. Таким образом, сетецентрическая война – это война, направленная на достижение информационного превосходства, которое ведет к ускоренному процессу принятия решений и разработки стратегий. Фактически, нечто похожее можно наблюдать и в финансовой сфере. На финансовых рынках также существуют и создаются новые сети, которые объединяют трейдеров, торговые площадки и платформы, эмитентов и других участников финансового рынка в единую систему. Так, оказывая влияние на информацию, поступающую в эту сеть, можно совершать различные противоборства. в результате одна сторона будет проигравшей и потеряет свои вложения и активы, другая, напротив, получит свой выигрыш.

Ярким примером сетецентрических противоборств на финансовых рынках являются манипуляции. в ходе работы была собрана выборка из 40 различных манипуляций, проводившихся на фондовых рынках по всему миру, в том числе и в России. Эмпирический анализ данных кейсов, а также изучение теоретических материалов позволили создать модель сетецентрических противоборств на финансовых рынках, которая очень похожа на обобщенную модель сетецентрической войны (рис. 1) [4].

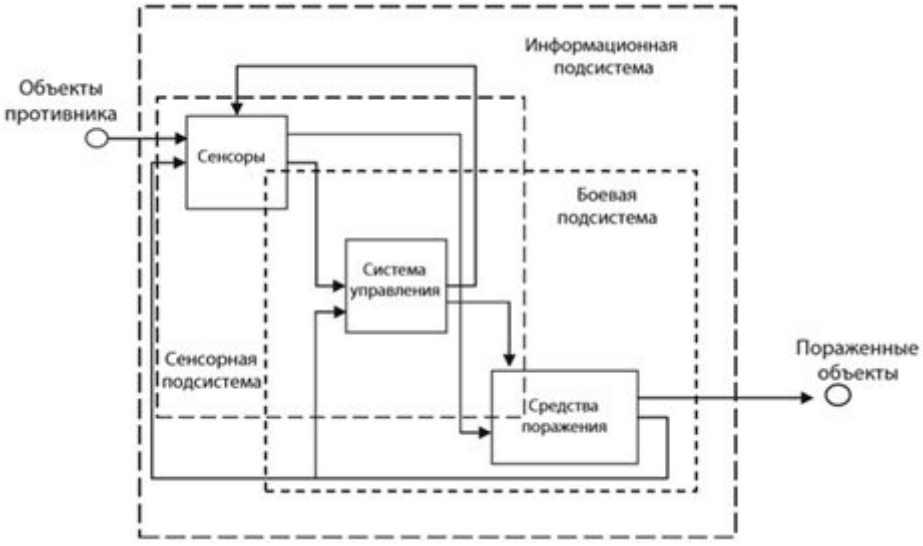


Рисунок 1. Обобщенная модель концепции сетецентрической войны

В нашей модели предполагается, что существует бенефециар, целью которого является увеличение своего экономического и финансового потенциала по сравнению с другими агентами. Сетецентрическое противоборство происходит в три этапа. На первом этапе бенефициар, имея информационное превосходство, выбирает объект манипуляции. Затем, используя различные стратегии, такие как «айсберг», «spoofing», либо ложную информацию агент совершает сетецентрическое противоборство. Через генератор (вспомогательные счета, акции компаний-пустышек и т.д.) он создает информационное поле. Изменения, которые вызваны действиями бенефициара, отражаются как на информационном поле, так и на сенсорах. в качестве сенсора, как правило, выступает биржа. в свою очередь участники финансового рынка принимают решения, ориентируясь на сенсоры, а так как информация на сенсорах искажена, то и решения, принимаемые DMU (decision making unit), заведомо ведут их к поражению и потере своих активов.

Рисунок 2. Модель сетецентрических противоборств на финансовых рынках

Все изученные кейсы были описаны с помощью данной модели, что позволило создать для них единую классификацию.

Для начала стоит отметить, что единого подхода к определению манипулятивных сделок на фондовом рынке не существует. Согласно российскому законодательству, Закону от 27.07.2010 №224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком» [12], выделяют следующие виды манипулирования:

1. распространение ложной информации, в результате которой «цена, спрос, предложение и объем торгов финансового инструмента существенно отличаются от того уровня, который бы сформировался без распространения таких сведений»;
2. совершение операций по предварительному соглашению между участниками торгов;
3. совершение сделок, обязательства сторон по которым исполняются за счет или в интересах одного лица. Применяется к организованным торгам, сделки на которых заключаются на основании заявок, адресованных всем участникам торгов;
4. неоднократное в течение торгового дня совершение на организованных торгах за счет или в интересах одного лица сделок в целях введения в заблуждение относительно цены финансового инструмента;
5. и другие.

Кроме того, существует не законодательный подход к классификации манипуляций на фондовом рынке. Виды манипуляций представлены в таблице 1 [18].

Виды манипулятивной торговли

Таблица 1

Классические виды	Новые виды
Корнер, сжатие, забегание вперед, тактика «бойлерной фирмы», накачка и сброс, манипулирование предложением, стабилизация цен, воздействие на цену закрытия и открытия, исходное искажение	Pinging, spoofing, electronic front running, mass misinformation

В данной работе был разработан новый подход к классификации манипуляций на фондовом рынке, который можно представить следующим образом (рис. 3).

Рисунок 3. Классификация манипуляций на основе модели сетецентрических противоборств

Данная классификация была построена на основе тех сенсоров, которые влияют на принятие решений участниками финансового рынка. Итак, данные сенсоры условно можно разделить на две группы: информационные и биржевые. Другими словами, DMU принимают решения либо на основе информационных сообщений, например, о слиянии и поглощении, либо пресс-релизов и т.д., либо на основе данных биржи, где, как правило, транслируется объем торгов, цена и количество заявок того или иного финансового инструмента. Итак, рассмотрим для начала информационные виды манипуляций.

Ещё в 19 веке Ротшильд сказал: «Кто владеет информацией, тот владеет миром», - и эта фраза актуальна и по сей день. Информация является ценнейшим ресурсом, и именно на её основе принимаются важные стратегические решения. Применимо к финансовым манипуляциям стоит разграничивать официальные и неофициальные источники информации. к официальным источникам относятся сайты государственных служб, а также регуляторов финансового рынка. к неофициальным - мнения экспертов, бизнесменов, различные форумы и т.д. Таким образом, агенты используют эти информационные ресурсы для размещения ложных сведений и проведения сетецентрических противоборств.

В качестве примера информационных манипуляций, где сенсор – неофициальный источник, можно привести следующую ситуацию. в 2018 году в своем личном Twitter аккаунте глава компании Tesla Илон Маск заявил о решении сделать Tesla частной фирмой и о том, что уже нашел финансы для выкупа акций. в сообщениях он также указал на то, что планирует выкупить ценные бумаги из расчёта 420 $ за акцию, то есть выше их рыночной стоимости. в результате цена акций поднялась с $340 до $370. Осенью 2018 года ряд трейдеров и акционеров Tesla подали в суд на Маска и обвинили главу компании в нарушении закона о ценных бумагах. в иске утверждалось, что Маск намеренно выдавал ложную информацию в Twitter-аккаунте, чтобы повлиять на цену акций Tesla. Кроме того, он должен выплатить штраф в размере 20 миллионов долларов. Такой же штраф наложен на компанию Tesla [7].

Далее рассмотрим подробнее информационные манипуляции, где сенсор – официальный источник. Ярким примером манипуляций такого типа может служить случай с компанией Avon, произошедший 14 мая 2015 года. Так, акции косметической компании Avon подскочили в четверг, 14 мая, на 20% после того, как на сайте Комиссии по ценным бумагам и биржам США (SEC) появился документ, в котором компания по имени PTG Capital Partners заявляла, что собирается купить Avon за $8 млрд. Сумма почти в три раза превышала рыночную стоимость компании (до скачка котировок она составляла $2,87 млрд), а сама Avon вскоре заявила, что не получала никаких предложений о поглощении. Заявка PTG Capital Partners оказалась фальшивой, в документе содержалось большое количество ошибок, в том числе и опечаток в названии компании. Но все это не смутило инвесторов, которые взвинтили стоимость акций Avon с $6,6 до $8 за бумагу.

к закрытию торгов, уже после разоблачения фальшивой заявки, котировки опустились до $7,07, а капитализация - до $3 млрд [11].

Стоит отметить, что к манипуляциям информационного типа можно отнести:

- распространение ложной информации (используются как официальные, так и неофициальные источники);
- исходное искажение (benchmark distortion), которое связано с предоставлением ложной информации относительно какого-либо индикатора или метрики, например, индекса S&P500 или ставки LIBOR, и др.;
- массовая дезинформация (mass dismissing), которая направлена на распространение неверных данных и новостей, призванная исказить информацию, подаваемую на финансовый рынок, в беспрецедентном масштабе.

Далее рассматривается, как работают манипуляции биржевого типа.

Традиционные манипуляции на фондовом рынке направлены на искажение цен или объёмов определенных ценных бумаг и финансовых инструментов в пользу манипулятивной стороны. Данные манипуляции могут иметь различные формы.

1. Корнер и сжатие (cornering, squeezing)

Корнер-ситуация обычно возникает, когда одна или несколько сторон приобретают большой объем ценной бумаги или финансового инструмента, а затем диктуют рыночные цены, тем самым манипулируя естественным ценовым состоянием рынка. Сжатие работает аналогичным образом, создавая искусственный дефицит ценной бумаги с целью контроля спроса. Подобные схемы требуют значительные суммы капитала для захвата доминирующего положения на определенном рынке. Несмотря на снижение числа данных манипулятивных схем из-за регулирования и развития рынка, они по-прежнему существуют на рынках у неликвидных эмитентов с низким free-float, где одна или несколько конкретных сторон могут получить доминирующее положение [3].

Подобных способов манипуляций немало. Можно назвать ещё забегание вперед (front running), тактику «бойлерной фирмы» (wash trading, painting the tape), манипулирование предложением и стабилизацию цен (parking), воздействие на цену закрытия/открытия (marking the close/open), исходное искажение (benchmark distortion), pinging и spoofing, но в данной работе рассматриваются самые распространенные и чаще других встречающиеся виды манипуляций.

2. Pump & Dump

Это схема манипулятивного повышения курса на рынках ценных бумаг или иных подобных активов с последующим обвалом. в основу заложена попытка увеличить стоимость при помощи ложных, ни на чём не основанных рекомендаций. Данная манипуляция особенно распространена на рынке криптовалют. Из-за отсутствия регуляции рынка криптовалют в большинстве стран на сервисах обмена криптовалют такая схема встречается очень часто. Как и на фондовом рынке, в афере два действующих лица - трейдер-промоутер и трейдер-инвестор. Трейдер-промоутер - организатор схемы манипуляции, делящийся «инсайдерской» информацией, и трейдер-инвестор - привлеченный промоутером, как правило, неопытный участник, который должен поверить в предоставляемую информацию. Основным каналом привлечения является мессенджер Telegram. Популярность данного канала, прежде всего, обусловлена использованием в приложении end-to-end шифрования, позволяющего участникам сохранять анонимность. Сообщества публикуют призывы об организованной скупке (памп) какой-либо криптовалюты с целью привлечь внешних покупателей и продаже (дамп) ее в несколько раз дороже. Сам процесс пампа и дампа организован следующим образом: участникам, состоящим в группах Телеграм, заранее сообщают время проведения пампа, дают ссылку, где будут проходить торги, затем в назначенное время выходит сообщение с призывом о покупке криптовалюты, что провоцирует пользователей одновременно

покупать криптовалюту. Таким образом, цена криптовалюты резко увеличивается, а через время падает до отметки ниже, чем была в самом начале [9].

Так, два трейдера из Нью-Джерси были арестованы в понедельник за то, что якобы манипулировали ценами более 2000 акций, зарегистрированных на Нью-Йоркской фондовой бирже и Nasdaq, что привело к незаконной прибыли в размере более 26 миллионов долларов в течение двухлетнего периода. Манипулятивная торговля происходила более 23 000 раз и часто длилась всего несколько минут. Джозеф Тауб (37 лет, Клифтон, штат Нью-Джерси) и Элазар Шмало (21 год, Пассаик, штат Нью-Джерси), иногда контролировали по меньшей мере 80% объема целевых акций и торговали на нескольких счетах одновременно. Тауб, зарегистрированный брокер, и Шмало, который являлся безработным, якобы координировали торговлю ценными бумагами на сумму более 10 миллиардов долларов на десятках брокерских счетов. Они искали компании с низкими объемами торговли, а затем вели многочисленные сделки, используя «вспомогательные» счета, которые сигнализировали о ложной информации на рынке, искусственно завышая их цены. Позже они продавали акции по искусственно завышенным ценам после накопления позиций по более низким ценам. Тауб использовал две компании, которыми он управлял, EAC Capital LLC и LNW Direct LLC для совершения некоторых сделок. Некоторые учетные записи были проведены на имена Тауб и Шмало, а другие были на имена членов семьи. Многие из счетов были открыты на имена физических лиц, которые не контролировали эти счета и не торговали ценными бумагами, чтобы скрыть схему от регулирующих и правоохранительных органов [19].

3. Предварительный сговор

Данный вид манипуляций предполагает совершение операций с финансовым инструментом, иностранной валютой и (или) товаром по предварительному соглашению между участниками торгов и (или) их работниками и (или) лицами, за счет или в интересах которых совершаются указанные операции, в результате которых цена, спрос, предложение или объем торгов финансовым инструментом, иностранной валютой и (или) товаром отклонились от уровня или поддерживались на уровне, существенно отличающемся от того уровня, который сформировался бы без таких операций [15].

Например, с марта 2013 г. по июнь 2014 г. рыночная стоимость ЗПИФ «Земли Подмосковья» искусственно поддерживалась с помощью манипулятивных сделок по предварительному сговору между компаниями ООО «Универ Капитал» и ООО «ИК «Ди Си Кэпитал», доля которых составляла более 70% общего объема торгов [1].

4. Кросс-сделки

Кросс-сделка - сделка, в которой одна и та же компания выступает одновременно и продавцом, и покупателем одного и того же актива по одной и той же цене. с помощью кросс-сделки можно показать, что по данному инструменту резко возросли объемы торгов. Или, используя кросс-сделки, брокер мог купить актив у клиента, продающего по низкой цене, а потом продать другому клиенту, покупающему за высокую цену. Манипулировать ценами путем кросс-сделок от имени одного клиента на бирже запрещено. При этом разные клиенты одного брокера беспрепятственно могут совершить сделку по одной и той же цене, потому что биржа видит, что источником заявок являются разные клиенты брокера [5].

Например, в США в 2007-2008гг. Михаел Таксон и Итамар Коен искусственно завышали кросс-сделками цены акций компаний Raven Gold Corporation (на 175%) и Kentucky USA Energy Inc. (на 562%). Распространяли буклеты с ложными данными о перспективах развития компаний [1].

Все вышеперечисленные манипуляции можно считать механизмом сетецентрического противоборства, и их можно описать по одной модели, которая была представлена выше (рис. 2).

Почему люди хотят легких и быстрых денег
или почему распространен сетецентризм?

Финансовые манипуляции на рынках и биржах одинаковы для всех стран, людей с разным образованием, социальным статусом и заработком, и они «приравнивают» всех на своем пути. Почему же люди покупаются на это и начинают действовать нерационально? Для этого есть несколько объяснений.

В первую очередь, суть каждой успешной финансовой манипуляции заключается в разном уровне владении информацией между участниками, незнанием сути махинаций и мотивов злоумышленников, что в экономике принято называть «асимметрией информации». Часто этому способствует низкая финансовая грамотность населения, поэтому они не могут распознать мошеннические действия от правомерных. Так, например, в России, почти половина, а именно 46% населения оценивают себя как финансово неграмотных. Тем временем, выше уровень финансовой грамотности у тех, кто получает или получил экономическое образование [13]. Кроме финансовой неграмотности, одной из наиболее частых причин попадания в финансовые ловушки называют российский менталитет с его характерным желанием заработать деньги быстро и не вкладывая труда, однако, по нашему мнению, легких денег хотят получить все, вне зависимости от национальности.

Тогда что же побуждает людей участвовать в финансовых манипуляциях? Ответ на это можно найти в работах психологов и социологов, которые выявили некоторые эффекты, влияющие на поведение человека на финансовой арене.

Во-первых, с появлением интернета, появилась возможность для создания виртуальных толп и новых обманов. Кроме этого, интернет создает условия информационного шума. Информационный шум оказывает негативное воздействие на психическое здоровье, вызывая у личности психоэмоциональное напряжение, трудности понимания информации и принятия решений, заставляя организм сопротивляться, включая фильтры понижения внимания и восприятия, вплоть до полного отказа от восприятия информации, вызывая «информационный стресс» [8]. Характерной чертой современности является «клиповость» мышления, как особенность восприятия человеком информации через короткие яркие образы и послания, вырванные из контекста. Поверхностность восприятия информации возникает из-за информационной перегруженности мозга. Такой способ восприятия не требует подключения рефлексии, осмысления информации, дробит информацию, вырывает из контекста, у людей теряется способность к анализу и выстраиванию логических цепочек, связей между объектами мира. Также, в условиях информационного шума человек воспринимает информацию в искаженном свете или просто отказывается от ее восприятия, а если информация воспринимается не в полном объеме, то она дает ложное представление о фактах, а отсюда становится причиной неточных и даже ошибочных, федеральных, групповых, индивидуальных решений [2]. Все это может привести к неправильным решениям индивида относительно участия в той или иной финансовой манипуляции, а также помогает злоумышленникам манипулировать людьми.

Вернемся к конкретным эффектам, которые побуждают людей участвовать в финансовых манипуляциях. Как уже говорилось, интернет дал возможность созданию масс и толп. Отсюда появляется такое понятие, как конформность. Люди следуют за своим окружением, механизмы коллективной мобилизации оказываются сильнее личного опыта и переламывают рационализм индивидуальных расчетов – это есть эффект подражания. Однако исключительно на имитации чужого поведения специфика толпы [10] не ограничивается. Также имеет место быть коммуникационный эффект, который заключается в убыстренном распространении информационных сигналов, причем чем более необычна и даже нелепа информация, тем быстрее она распространяется, именно это чаще всего происходит в интернете. Главная черта человека толпы - неустойчивость мнений, быстрая смена настроений и способов действий, отбрасывание вчерашней информации в пользу сегодняшней. Попадая в зону сильной неопределенности, задаваемой игрой, индивиды ведут себя не так, как предписано моделью рационального «экономического человека». к специфике толпы можно также отнести эффект раскачивающейся лодки, при котором появляются резкие колебательные движения между позитивными и негативными оценками ситуации, опти-

мистическими и пессимистическими настроениями с увеличением амплитуды этих колебаний. Эффект единения или разрядки - тенденция к ликвидации социальных различий в актах массового поведения. а также периодическое возникновение и исчезновение массовых форм поведения - эффект возвращения.

Кроме того, люди внушаемы, они готовы согласиться с тезисами, которые им транслируются от окружения / СМИ, поэтому побудить поучаствовать в той или иной финансовой манипуляции их может удачная вирусная реклама (эффект вирусной рекламы) финансовых организаций, предлагающих быстрое обогащение (букмейкерские конторы, финансовые пирамиды, онлайн казино и т.д.), а также для них свойственно доверие харизматическому лидеру.

Важным эффектом является «синдром собственной исключительности». в людях преобладает оптимизм, они верят в собственную исключительность: «случится со всеми, но не со мной / со мной ничего плохого не произойдет, я выиграю». Важно то, что горизонты безопасности не остаются неизменными. Напротив, они постоянно движутся, могут удаляться или приближаться. Чаще всего после обвала субъективные пороги безопасности резко приближаются, становятся минимальными. Пережитый шок оставляет осадок в виде чувства опасности. Затем срабатывает эффект привыкания, и происходит постепенное отодвигание субъективных порогов безопасности. Это эффект привыкания к игре, который сослужил многим столь печальную службу.

Еще один эффект, влияющий на участие людей в сетецентрических противоборствах – это доверие к финансовым институтам. Существуют три базовых основания, по которым мы определяем имманентную добросовестность адресатов доверия: репутация, актуальные (фактические) достижения и образ, и вторичные основания: рекомендации и референции (символические знаки достоверности) [14].

Синдром обворованного также подталкивает людей к нерациональному поведению, а именно, к участию в новой «игре» (нужно отыграться, вернуть потерянное). в случае потери средств меняется мотив вложений: теперь главное – не накопить остаточную сумму, а вернуть потерянное, а также овладеть механикой игры. Вернуть себе возможность понимать происходящее для человека порою важнее отдельного выигрыша или проигрыша.

Таким образом, можно выявить несколько точек зрения, относительно участия в финансовых манипуляциях.

Социальные психологи, социологи: участники игры не в состоянии выработать рациональных стратегий и становятся легкой добычей манипуляторов. Иными словами, люди ведут себя иррационально, глупо, и потому их обманывают.

Экономисты скорее всего встанут на противоположную точку зрения, утверждая, что каждый человек толпы вполне рационально следует своим интересам, а вот общий результат эгоистических усилий участников толпы оказывается иррациональным - большинство проигрывают. Такова традиционная проблема коллективного действия.

Позиция эконом-социолога: под воздействием разных факторов (в том числе под воздействием эффектов толпообразования) схема поведение может переключаться, и тогда - непоследовательно, вопреки собственным интересам и предпочтениям.

Так что, причина в жажде быстрого обогащения - это сложная констелляция социально-экономических, политических и культурных факторов, превращающих индивида сначала в атомарное существо, анонимного представителя безликой публики, а затем в человека толпы. Здесь и влияние утвердившейся этики успеха, и увлечение практиками азартных финансовых игр, и периодический обман населения государством, и массированный удар средств массовой коммуникации, и, конечно, стратегические действия организаторов, нацеленные на создание толп и манипулирование толпами.

Заключение

В ходе данной работы было проанализировано 40 кейсов финансовых манипуляций в различных странах мира. Эмпирический анализ показал возможность применения термина сетецентрических противоборств к финансовым рынкам. Так, сетецентрические войны, которые ос-

нованы на инфокоммуникационном превосходстве, можно наблюдать и на финансовых рынках, где бенефициары обладают большей информацией, чем DMU, и благодаря этому выигрывают в сетецентрических противоборствах на финансовых рынках.

Кроме того, было выявлено, что все кейсы, рассмотренные в работе, имеют ряд схожих особенностей и неплохо согласуются с концепцией сетецентрической войны. Данная особенность позволила обобщить полученный результат в виде модели сетецентрических противоборств на финансовых рынках. Суть данной модели состоит в том, что бенефициары, имея информационное превосходство, с помощью генератора искажают реальную информацию. в свою очередь, недостоверные сведения поступают в информационное поле и отражаются на сенсорах. в результате, лица, принимающие решения, обладают ложной информацией и осуществляют сделки с убытком, принося прибыль бенефициарам.

На основе данной модели, а точнее на основе сенсоров, которые влияют на принятие решений, была разработана классификация сетецентрических противоборств на финансовых рынках. Так, было выявлено два основных вида противоборств: информационные, осуществляемые с помощью официальных и неофициальных источников информации, и биржевые, которые выражены в искажении цены или объема финансовых активов (инструментов).

В ходе теоретического анализа были выявлены эффекты, из-за которых люди участвуют в махинациях на финансовых рынках. Главными эффектами в данном случае выступают:

- эффект подражания;
- коммуникационный эффект;
- эффект раскачивающейся лодки;
- эффект единения или разрядки;
- эффект возвращения;
- эффект вирусной рекламы;
- «синдром собственной исключительности»;
- эффект привыкания;
- синдром обворованного.

Таким образом, в ходе данного исследования удалось создать обобщенную модель сетецентрических противоборств и выявить причины их распространения. в свою очередь, полученные результаты могут стать хорошей основой для более глубокого изучения данной проблемы в будущем.

Список литературы

1. Володин С. Н., Емелькина А. И. Борьба с рыночным манипулированием в развивающихся странах: используемые методы и возможность их применения в России //Управление финансовыми рисками. 2017. №. 3.
2. Еляков А.Д. Информационная перегрузка людей // Экономическая социология. 2005.
3. Заборовский В. Е., Заборовская А. Е., Плетнев К. В. Необходимость и направления государственного регулирования и предотвращения манипулятивных сделок на фондовом рынке // Вестник УрФУ. Серия: Экономика и управление. 2018. № 5.
4. Ковалев В. И., Малинецкий Г. Г., Матвиенко Ю. А. Концепция «сетецентрической» войны для армии России: «множитель силы» или ментальная ловушка? //Вестник академии военных наук. 2015. №. 1.
5. Кросс-сделка // Инвестиционная Палата URL: https://investpalata.ru/%D0%BA%D1%80%D0%BE%D1%81%D1%81-%D1%81%D0%B4%D0%B5%D0%BB%D0%BA%D0%B0/ (дата обращения: 09.03.2020).

6. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография // СПб.: Наукоемкие технологии. 2017.
7. Маск объяснил стоившее ему должности в Tesla сообщение в Twitter // РБК URL: https://www.rbc.ru/technology_and_media/24/11/2019/5dd9af7f9a794715d15e0df1 (дата обращения: 09.03.2020).
8. Наше будущее - выживание в условиях информационного шума // Медиа. Информация. Коммуникация URL: http://mic.org.ru/3-vyp/663-nashe-budushchee-vyzhivanie-v-usloviyakh-informatsionnogo-shuma (дата обращения: 09.03.2020).
9. Незаконная игра. Как работает схема «Pump and Dump» на рынке криптовалют // РБК URL: https://www.rbc.ru/crypto/news/5bbf2a459a7947f7ac3a048a (дата обращения: 09.03.2020).
10. Радаев В.В. Уроки «финансовых пирамид» или что может сказать экономическая социология о массовом финансовом поведении // Мир России. 2002. № 2.
11. Подделка на миллион: как фейковые новости влияют на котировки компаний // РБК URL: https://www.rbc.ru/photoreport/15/05/2015/5555e9089a794704a5b8298a (дата обращения: 09.03.2020).
12. Федеральный закон от 27.07.2010 N 224-ФЗ (ред. от 27.12.2018) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» // КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_103037/f7ff18209caf8927a5ebf06a12838837b333c5f3/ (дата обращения: 09.03.2020).
13. Финансовая неграмотность бьет по карману // IQ HSE.ru URL: https://iq.hse.ru/news/205933107.html (дата обращения: 07.03.2020).
14. Штомпка П. Доверие — основа общества. М.: Логос. 2015
15. Якупов В. Р. Манипулирование рынком: совершение незаконных сделок на организованных торгах //Вестник Южно-Уральского государственного университета. Серия: Право. 2013.
16. Cebrowski A. K., Garstka J. J. Network-Centric Warfare: Its Origin and Future, U.S. Naval Institute Proceedings. Annapolis, Maryland. 1998. Vol. 124. No.1.
17. Fewell M. P., Hazen M. G. Network-centric warfare-its nature and modelling. – Defence science and technology organisation salisbury. Australia: Systems sciences lab. 2003.
18. Lin, Tom C. W The new market manipulation // Emory Law Journal. 2016. Vol. 66 No. 6.
19. Two traders arrested over alleged manipulation of more than 2,000 stocks // MarketWatch URL: https://www.marketwatch.com/story/two-traders-arrested-over-alleged-manipulation-of-more-than-2000-stocks-2016-12-12 (дата обращения: 08.03.2020).

КОЛЯДА МАКАР ВАДИМОВИЧ
студент факультета права
НИУ ВШЭ, г. Москва
E-mail: mvkolyada@edu.hse.ru

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ АРБИТРАЖНЫХ СУДОВ В ИНТЕРЕСАХ ДЕЛОВОЙ РАЗВЕДКИ

MAKAR KOLIADA VADIMOVICH
student, faculty of law
National Research University «Higher School of Economics», Moscow

THE USING OF RUSSIAN ARBITRATION COURTS' INFORMATION SYSTEM FOR BUSINESS INTELIGENCE PURPOSES

Аннотация: В настоящей статье автор изучает вопрос о том, каким образом информационная система арбитражных судов Российской Федерации, также известная как Картотека арбитражных дел или КАД «Арбитр» может быть использована при выполнении задач деловой разведки, насколько такое использование эффективно с точки зрения сбора сведений о человеке или организации. На примере изучения конкретной организации – известного в России публичного страхового общества, исследуются достоинства и недостатки применения Картотеки арбитражных дел в целях деловой разведки.

Abstract: In the present article the author studies the question of how the Russian arbitration courts' information system, also known as the Arbitration cases cards file, or KAD "Arbitr", can be used while business intelligence performance. Also the question arises: is such using effective for the purposes of collecting information about a person or about an organization. Performing the researching of a well-known Russian insurance company, the author tries to analyze the benefits and disadvantages of using the Arbitration cases cards file for business intelligence purposes.

Ключевые слова: КАД Арбитр, арбитражные суды, деловая разведка, изучение контрагента, Due Diligence

Key words: KAD "Arbitr", arbitration courts, business intelligence, counter-party research, Due Diligence

Введение

Любое дело требует опыта, профессионализма, в той или иной степени специальных знаний, умений и подготовки. Деловая (конкурентная) разведка не исключение. Жизнь, однако, диктует свои правила, которым приходится следовать. И, зачастую, в силу различных обстоятельств, будь то необходимость выживания или неудовлетворительная ситуация в определённом сегменте рынка труда, люди занимаются профессиональной деятельностью из сферы, отличной от той, в которой они получали высшее образование или в которой хорошо разбираются в силу особенностей личности, темперамента, увлечений. При этом, однако, занимаясь не вполне свойственным ему родом деятельности, человек всегда будет предпринимать попытки использовать накопленные в течение жизни знания и жизненный опыт при выполнении своих должностных обязанностей. Так, если поручить человеку, окончившему юридический факультет и не имеющему опыта работы в сфере поиска и анализа информации о человеке или организации, выполнить задание из области деловой (конкурентной) разведки, первое, что придёт ему в голову – воспользоваться данными публичного доступа, содержащимися в ЕГРЮЛ и в информационной систе-

ме арбитражных судов (КАД Арбитр). При определённых обстоятельствах такой подход может принести результат. о том, как использование системы КАД Арбитр может послужить интересам деловой разведки, пойдёт речь в настоящей статье.

Целью настоящей статьи является поиск ответа на вопросы о том, каким образом информационно-справочная система арбитражных судов РФ может быть использована при выполнении задач деловой разведки, насколько такое использование эффективно с точки зрения сбора сведений о человеке или организации. Работа представляет собой аналитическое исследование, проведённое автором на основе собственных знаний, полученных в ходе получения высшего профессионального образования по специальности «Юрист», а также в ходе освоения дисциплины общеуниверситетского пула Маголего НИУ ВШЭ «Актуальные проблемы конкурентной (деловой) разведки» и опыта, полученного во время работы в сфере практической юриспруденции. Выводы, сделанные автором по результатам проведённого исследования, подкрепляются мнениями практикующих юристов и специалистов в области повышения эффективности бизнеса, полученных из общедоступных источников, перечень которых приводится в первой части настоящей работы.

Объектом исследования является система КАД Арбитр, а также публикации, касающиеся её использования, находящиеся в публичном доступе в сети Интернет.

Актуальность и новизна настоящего исследования обусловлены тем, что в настоящее время в большинстве общедоступных источников система КАД Арбитр не рассматривается как источник сведений, которые могут представлять интерес для специалиста в области деловой разведки. Настоящая работа представляет собой попытку обобщения материала, содержащегося в различных источниках, в целях облегчения удобства пользования таким материалом. Выводы настоящего исследования могут быть использованы людьми, сталкивающимися с необходимостью решения задач деловой разведки, для разрешения вопроса о том, стоит ли использовать при разрешении таких задач систему КАД Арбитр и, если да, то каким образом можно получить нужную информацию с использованием данного ресурса.

Настоящая статья состоит из информационно-аналитической и практической частей. в информационно – аналитической части представлены общие сведения о системе КАД Арбитр, а также обзор публикаций о её функционале и способах работы с ней. в практической части описывается механизм поиска информации в системе на примере поиска информации о контрагенте при разрешении определённой задачи. в заключительной части исследования проводится разбор достоинств и недостатков системы с позиций разведки, приводятся выводы автора о возможностях использования системы в интересах деловой разведки.

Информационно-справочная система арбитражных судов (КАД Арбитр)

Информационно – справочная система КАД Арбитр была запущена в 2009 году в рамках проекта по созданию в стране т.н. «электронного правосудия». Сервис предоставляет любому желающему возможность на безвозмездной основе отслеживать ход рассмотрения любого дела в любом арбитражном суде России. Кроме того, в системе публикуются все акты, вынесенные арбитражными судами, что многократно снижает затраты времени и ресурсов на поиск таких актов и выгодно отличает КАД Арбитр от, к примеру, справочно – правовых систем, в которых опубликованы лишь судебные акты, вступившие в законную силу, как правило, акты высших судебных инстанций. Помимо этого, КАД Арбитр предоставляет возможность подачи сканированных копий процессуальных документов в арбитражный суд, то есть подать иск можно не выходя из дома или офиса. Всё это делает КАД Арбитр одним из главных рабочих инструментов практикующих юристов, которые используют его ежедневно.

Использование КАД Арбитр в интересах деловой разведки: обзор публикаций

Простота и удобство использования системы КАД Арбитр обусловливают тот факт, что на информацию, полученная с использованием данной системы, обсуждается в профессиональных

сообществах, форумах постоянно, но практически никто не пишет о самой системе. Это очевидно: никому не интересно читать о том, что знают все. Публикации, посвящённые системе КАД Арбитр чаще всего встречаются в сети Интернет на сайтах, редактируемых и используемых профессиональными юристами.

Практически во всех источниках подобного рода можно встретить одну или несколько фраз общего характера о том, что «используя систему КАД Арбитр можно получить информацию о рассмотрении дел с участием контрагента». о том, почему такая информация может быть полезна и какие выводы можно сделать на её основе, в большинстве публикаций, впрочем, не уточняется.

Количество публикаций, в которых описывается, каким образом информация с КАД Арбитр может использоваться при изучении контрагента, относительно невелико. Так, например, автор одной из публикаций на портале «Арбитр ру» не рекомендует сотрудничество с организациями, которые часто участвуют в судебных процессах, а одна из компаний, предоставляющих услуги в области обеспечения безопасности бизнеса, отмечает, что компания, участвовавшая в нескольких судебных процессах в арбитражных судах, требует дополнительной проверки на благонадёжность. «Центр экспертиз при институте судебных экспертиз и криминалистики» указывает, что проверка контрагента важна не только на этапе заключения договора, но и на всём протяжении сотрудничества – это позволит выяснить, не использует ли бизнес-партнёр накапливающуюся дебиторскую задолженность для расчёта с другими кредиторами, не вступил ли он в стадию банкротства. Такие сведения помогут вовремя отреагировать на неблагоприятные изменения в хозяйственной жизни контрагента и, возможно, сохранить ресурсы.

Теперь перейдём к поиску информации в системе КАД Арбитр.

Для примера проведём небольшое исследование крупной страховой компании, с которой, образно говоря, планируется заключение договора страхования имущества нашей условной компании. Очевидно, что нам, как страхователям имущества, хочется иметь уверенность в том, что при наступлении страхового случая страховщик выплатит положенную сумму добровольно, а не в судебном порядке. Поэтому проверим, насколько часто страховщик привлекается в качестве ответчика – это поможет оценить вероятность риска, что и нам придётся обращаться в суд и требовать от страховщика выплаты положенной по договору суммы. Первое, что обращает на себя внимание – удобство пользовательского интерфейса: полей для заполнения немного, крупные иконки обозначают разделы. Для пользователей, не имеющих опыта работы с системой, предусмотрены сразу две ссылки, по которым доступно Руководство пользователя, в котором в сжатой форме описан механизм поиска информации в системе.

Для поиска дел с участием изучаемой компании нужно ввести наименование в строке «Участник дела» в левом верхнем углу. Начинаем вводить наименование и сталкиваемся с тем, что в картотеке дел встречаются различные наименования одной и той же организации. Выбрав из всплывающего окна одно из наименований, наиболее, на наш взгляд, подходящее, получаем возможность сократить количество отображаемых по запросу карточек дел, выбрав процессуальное положение интересующей нас компании по делу – ответчик.

По запросу найдено 2102 карточки дел. Результаты поиска сортируются по дате последнего обновления карточки дела, при этом в карточке дела находятся не только судебные решения, оканчивающие спор по существу, но и промежуточные акты, например, определения о принятии дела к производству. Определить, окончено ли дело, не заглянув в карточку, нельзя, но в рассматриваемом примере помогает номер дела. Последнее число – год поступления искового заявления в суд, первое – входящий номер искового заявления за этот год. Поскольку мы ищем информацию в марте 2019 года, очевидно, что дела, находящиеся на первой странице результатов поиска, на момент изучения не рассмотрены, а только приняты к производству. То есть мы не можем узнать, взыщет ли в итоге суд с объекта изучения что-либо, но количество подаваемых «против» него в суд исков в день само по себе повод для размышлений. Сузить круг поиска можно, выбрав одну из категорий дел в верхней части экрана. Но нас интересуют дела о взыскании страхового возмещения (гражданские), а таких абсолютное большинство.

Теперь вспомним, что в начале поиска в выпадающем окне было несколько строк, вклю-

чающих наименование изучаемой компании. в таком случае, возможно, выбрав один из вариантов наименования компании, мы увидели лишь часть интересующих нас дел. Проверим это, введя в поисковую строку ИНН изучаемого объекта, который, как известно, является уникальной характеристикой. Узнать ИНН не проблема. Можно использовать официальный сайт компании, можно, как в рассматриваемом примере, не уходя с сайта КАД Арбитр, открыть любую из карточек дел, открыть любой судебный акт и скопировать ИНН оттуда, поскольку в «шапке» большинства судебных актов ИНН стороны по делу есть. Поиск по ИНН в большинстве случаев подтверждает, что сомнения не напрасны. в рассматриваемом примере по запросу выдается более 14 000 результатов.

Система КАД Арбитр единая для арбитражных судов всей страны. Масштаб бизнеса изучаемой в данном примере компании предполагает, что процессы с участием компании проходят по всей стране. Если мы хотим получить информацию о привлечении компании к суду в каком-то конкретном регионе, мы можем легко это сделать, выбрав конкретный арбитражный суд в соответствующей строке поиска. Это удобно, учитывая, что в каждом субъекте РФ есть только один арбитражный суд. Правда, стоит учитывать, что подсудность можно изменить соглашением сторон, что, впрочем, страховым спорам не очень свойственно.

Кроме того, поиск выдал нам все дела с участием целевого страховщика, зарегистрированные в системе за все 10 лет её существования. Сузим поиск, установив дату регистрации дела в суде за последние три года и только в Арбитражном суде города Москвы. Найдено 909 дел. Среди этих дел 769 – споры по гражданским делам, большинство из которых споры о взыскании страхового возмещения, 139 – административные дела. Выбрав административные споры, выясняем, попутно с решением основного поставленного вопроса, что за последние три года изучаема организация по заявлениям Центрального Банка почти 100 раз привлекалась к административной ответственности по ч. 3 ст. 14.1 КоАП РФ – нарушение условий лицензии.

Из найденной информации невозможно сделать однозначных выводов о надёжности и добросовестности изучаемой компании. с одной стороны, компания привлекается к суду тысячи раз. с другой стороны, это особенности страхового дела: огромное количество жизненных ситуаций невозможно однозначно признать или не признать страховым случаем, необходима правовая квалификация, которую может легально осуществлять только суд, очень часто предпринимаются попытки страхового мошенничества, и нет ничего удивительного в том, что крупная страховая компания является «постоянным клиентом» арбитражных судов по всей стране.

Для формирования целостной картины нам необходимо бегло ознакомиться с каждым из хотя бы «московских» дел, прочитать финальные судебные акты, определить, что произошло и сделать какие-то более – менее правдоподобные выводы о модели делового поведения изучаемого контрагента. Делать этого мы, конечно, не будем. Во-первых, это неоправданная трата времени. Во-вторых, судебные решения написаны сухим формальным языком, для того чтобы понять написанное нужно обладать определёнными знаниями либо опять-таки потратить колоссальное количество времени. Так, если автору настоящего исследования, являющемуся профессиональным юристом, на изучение одного судебного акта объёмом в пять страниц потребуется 1 – 2 минуты, то деловому разведчику, не имеющему практического опыта в юридической сфере – 10 -15 минут. а дел сотни (!). Кроме того, большинство страховых споров рассматриваются в порядке упрощённого производства. По таким делам без ходатайства сторон не составляется мотивированное решение. Соответственно, всё, что можно увидеть на КАД Арбитр – это один лист, не несущий почти никакой информативной нагрузки для лица, не участвовавшего в деле.

В таком случае, возможно, ответ на вопрос о том, является ли огромное количество арбитражных дел с привлечением изучаемого объекта ответчиком обычным явлением для компании – страховщика, поможет получить сравнительный метод. Введём в строки поиска аналогичный вышеуказанному запрос на прямого конкурента. Вводим ИНН с указанием процессуального положения по делу «ответчик», арбитражный суд Москвы, период с 01 января 2017 по 03 марта 2019 года. Найдено 474 дела, то есть почти в два раза меньше, чем у изучаемой компании, из них о привлечении к административной ответственности – 11, что в 10 раз меньше аналогичного показателя потенциального контрагента. На основе полученной информации всё равно не полу-

чится сделать неоспоримых выводов, но это информация к размышлению.

Подводя итог проведённому поиску информации о страховой компании в системе КАД Арбитр, можно констатировать несколько фактов. Компания часто участвует в судебных заседаниях арбитражных судов по всей стране, в Москве, в частности, примерно в 300 делах в год. За прошедшие три года около 100 раз привлекалась к административной ответственности за нарушение условий лицензии на осуществление страховой деятельности. Данные показатели не являются запредельными для страховой компании, но они выше, чем у некоторых других крупных страховщиков. Поскольку полученной информации недостаточно для предоставления убедительных выводов, руководству в отчёте будет рекомендовано провести дополнительную проверку контрагента.

Удобная опция, предоставляемая системой КАД Арбитр – календарь предстоящих судебных заседаний, можно в один клик перенести записи из календаря в рабочий Outlook или в Google Calendar. «Центр экспертиз при институте судебных экспертиз и криминалистики» указывает, что непосредственное посещение судебных заседаний может быть полезно при изучении контрагента. с этим следует согласиться. в заседании стороны заинтересованы в победе, и будут отвечать на любые вопросы судьи, возможно, вынуждены будут озвучить информацию о деятельности компании, которую при других обстоятельствах разглашать не стали бы. Впрочем, в большинстве случав, судья, разумеется, ограничивается одним – двумя вопросами, уточняющими суть и размер исковых требований. в таком случае экскурсия в суд окажется для делового разведчика бесполезной тратой времени.

Заключение

Таким образом, мы бегло изучили функционал информационно – справочной системы арбитражных судов РФ (КАД Арбитр) и провели небольшое исследование контрагента с её использованием, т.н. «арбитраж-проверку». По итогам проведённой работы можно сделать следующие выводы. к достоинствам системы КАД Арбитр следует отнести:

Удобство пользования. Даже впервые используя систему, можно без труда разобраться, как искать интересующую информацию, фильтры позволяют группировать результаты поиска по интересующим разделам;

Достоверность сведений. Факты, установленные решением суда, обладают высоким убедительным эффектом. Более того, могут использоваться при взаимодействии с государственными органами, поскольку установленные судом факты имеют силу бесспорных доказательств – ст. 69 АПК РФ. Исключения составляют судебные решения, не вступившие в законную силу, а также отменённые или изменённые вышестоящими судами;

Актуальность информации. Сведения в системе обновляются ежедневно. Помимо решений судов можно видеть актуальную информацию о принятии дел к производству, привлечении третьих лиц, назначении даты судебных заседаний и проч. Наиболее значимыми в данном аспекте являются сведения о вступлении контрагента в одну из процедур банкротства, например, подача заявления в арбитражный суд о признании должника банкротом.

В то же время использование КАД Арбитр в интересах деловой разведки предполагает наличие следующих существенных недостатков:

Арбитражные суды рассматривают исключительно споры между предпринимателями, вытекающие из предпринимательской деятельности. Впрочем, сложно представить, что деловую разведку могут заинтересовать споры с физическими лицами. (Корпоративные споры входят в компетенцию арбитражных судов – глава 28.1 АПК РФ);

По многим делам не представляется возможным получить никаких сведений, кроме их существования. к примеру, к таким делам относятся дела, рассматриваемые в порядке упрощённого производства;

Поиск по наименованию контрагента может не дать исчерпывающего перечня результатов, поскольку различные судьи и сотрудники аппарата судов могут вносить различные наименования одной и той же компании в карточки дел. Проблема решается с помощью поиска по ИНН, узнать который не составляет труда;

Для того чтобы эффективно использовать найденную информацию, особенно изучать су-

дебные акты, крайне желательно обладать знаниями и/или опытом в сфере юриспруденции.

В целом, по итогам проведённого исследования можно сделать вывод о том, что система КАД Арбитр функционально не предназначена для поиска информации о гражданах и организациях, но в интересах деловой разведки использоваться может. При этом необходимо иметь в виду, что КАД Арбитр при разрешении задач деловой разведки является вспомогательным, но никак не основным инструментом. Обратиться к системе целесообразно в случае обнаружения в иных источниках сведений об участии проверяемого объекта в арбитражном судопроизводстве, особенно в качестве ответчика. Используя КАД Арбитр, можно получить информацию о том, по какого рода спорным ситуациям изучаемый контрагент привлекается к суду, прочитать вынесенные судами решения, из которых выяснить, в силу каких особенностей бизнес – политики контрагента его приходится понуждать к исполнению обязательств в судебном порядке, выявить возможные риски сотрудничества с таким контрагентом.

Так же нужно принимать во внимание, что информация, размещённая в системе КАД Арбитр создаётся профессиональными юристами с большим опытом работы и не адаптируется под восприятие среднестатистического человека. Поэтому человеку, имеющему определённые познания в сфере юриспруденции, значительно проще использовать весь потенциал системы, нежели человеку, такими познаниями не обладающему. Поэтому, если среди людей, занимающихся деловой разведкой в конкретной компании, имеется человек, разбирающийся в праве, то анализ контрагента с использованием системы КАД Арбитр лучше всего поручить именно такому человеку.

Список использованных источников

1. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 г. № 95-ФЗ. «Собрание законодательства РФ», 29.07.2002 г., № 30, ст. 3012. Доступен онлайн в СПС «Консультант-Плюс».
2. URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=314404&fld=134&dst=1000000001,0&rnd=0.44000014307648727#006994412045886778 (дата обращения 03.03.2019);
3. Картотека арбитражных дел арбитражных судов Российской Федерации (КАД Арбитр). URL: http://kad.arbitr.ru/ (дата обращения 03.03.2019);
4. Портал «ЦентрИнформ». Статья на тему «Регистрация и работа в системах «Мой арбитр» и «Правосудие» (документооборот в рамках судебных процессов)» URL:https://torgi.center-inform.ru/tehpod/faq/Регистрация%20и%20работа%20в%20системах%20»Мой%20арбитр»%20и%20»Правосудие»%20%28документооборот%20в%20рамках%20судебных%20процессов%29/ (дата обращения 03.03.2019);
5. Юридический блог «Legal-IT». Статья на тему «FAQ: изменения в процессе подачи документов в системе «Мой Арбитр» URL: https://blog.casebook.ru/faq-izmeneniya-v-processe-podachi-dokumentov/ (дата обращения 03.03.2019);
6. Юридический форум «Конференции ЮрКлуба», тема обсуждения «О порядке размещения информации в КАДе». URL:http://forum.yurclub.ru/index.php?showtopic=355292 (дата обращения 03.03.2019);
7. Портал «Арбитр ру». Статья «КАД Арбитр ру — картотека арбитражных дел: электронное правосудие в действии». URL: https://arbitrru.ru/kad-arbitr-ru (дата обращения 03.03.2019)
8. Официальный сайт ООО «Альфа-развитие», раздел «Арбитраж-проверка контрагента». URL:https://proverk.ru/arbitrazh-proverka-kontragenta/# (дата обращения 03.03.2019)
9. Центр экспертиз при институте судебных экспертиз и криминалистики. Официальный сайт. Статья «Как Arbitr.ru помогает бизнесу и юристам?». URL:https://ceur.ru/library/articles/pravo/item317459/ (дата обращения 03.03.2019).

КРУПЕНИЧ ЕЛИЗАВЕТА АЛЕКСЕЕВНА
студентка факультета бизнеса и менеджмента
НИУ ВШЭ, г. Москва
E-mail: eakrupenich@gmail.com

КИМ НАТАЛЬЯ
студентка факультета бизнеса и менеджмента
НИУ ВШЭ, г. Москва
E-mail: natalyakim.edu@gmail.com

ПРЕГРАДЫ И ПЕРСПЕКТИВЫ ЦИФРОВОЙ БЕЗОПАСНОСТИ БИЗНЕСА

KRUPENICH ELIZAVETA
student, faculty of business and management
National Research University «Higher School of Economics», Moscow

KIM NATALYA
student, faculty of business and management
National Research University «Higher School of Economics», Moscow

PREDICAMENTS AND PROSPECTS OF CYBERSECURITY FOR BUSINESS

Аннотация: Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации поставило перед собой задачу к 2024 году достичь определенных показателей, среди которых ключевые - 90% сетевого трафика российского сегмента сети «Интернет» будут маршрутизироваться на территории России, а 97% населения будут использовать средства защиты информации. Изучая сферу безопасности предпринимательской деятельности и, в частности, процесс цифровой трансформации бизнеса в текущей мировой обстановке, невозможно не учитывать приоритетность цифровой безопасности, которая затрагивает все больший спектр деятельности человека. Данная статья посвящена изучению перспектив и проблем цифровой безопасности бизнеса как наиболее активно развивающегося направления в России. Цель данного исследования заключается в выявлении тенденций и решений, которыми оперирует бизнес на сегодняшний день для предупреждения и предотвращения возникновения риска безопасности данных. Методология исследования предполагает анализ релевантных исследований в сфере цифровой безопасности бизнеса, изданных в последние пять лет, а также соответствующие отчеты опроса и исследований в различных отраслях экономики. в ходе системного анализа существующих исследований и отчетов стал очевиден тот факт, что предприниматели все больше озабочены сохранностью и конфиденциальностью данных, а также заинтересованы в персонализации технологий под потребности конкретной компании. Таким образом, были выявлены наиболее острые проблемы безопасности в различных отраслях бизнеса, а также перспективные с точки зрения области применения и надежности решения, которые могут предложить технологии на сегодняшний день.

Abstract: While examining the process of digital transformation of a business in the current world environment it is impossible not to take into account the priority of cybersecurity, which affects a wider range of human activities. The Ministry of Digital Development, Telecommunications and Mass Media of the Russian Federation set a goal to achieve certain indicators by 2024, among which the key ones are “90% of the Russian segment of the Internet network traffic will be routed in Russia” and “97% of the population will use information security tools”. This article is devoted to studying the prospects and problems of cybersecurity of business as one of the most actively developing area in Russia. It became

apparent from the analysis of existing studies and reports that entrepreneurs are increasingly concerned about the safety and confidentiality of data and interested in personalizing technology to the needs of a particular company. Thus, the most acute security problems in various business sectors were identified, as well as promising solutions from the point of view of application and reliability that technologies can offer today.

Ключевые слова: цифровая безопасность бизнеса, проблемы безопасности бизнеса, цифровая трансформация бизнеса.

Keywords: cybersecurity for business, business security issues, digital business transformation.

Цифровая безопасность бизнеса является довольно актуальной областью исследований, поскольку технологии как основная составляющая нашей современной жизни подвержены ежедневному обновлению и в то же время оказывают сильное влияние на понимание актуальных проблем и стратегий их решения.

В ходе исследования PWC, проведенного в рамках 23-го ежегодного глобального опроса CEO (1581 CEO из 83 стран), была выявлена тенденция уменьшения уверенности в будущем дне: всего за 2 года процент неуверенности относительно благополучия экономической обстановки среди CEO увеличился с 5% до 53%. Основной причиной стал рост обеспокоенности относительно изменения климата, появления новых киберугроз, роста торговых конфликтов и расширения спектра проблем, вызванных недостаточной защищенностью бизнеса. Лишь 27% директоров высказали уверенность относительно роста своих компаний в 2020 году.

Интернет является «глобальным связующим элементом» бесчисленного количества информации. с одной стороны, новые цифровые технологии привносят большое количество положительных изменений в действующие бизнес-модели и условия ведения предпринимательской деятельности. с другой стороны, отсутствие грамотного и эффективного управления такой глобальной структурой (а также отсутствие как таковых глобальных организаций, следящих за цифровой безопасностью) актуализирует проблемы, связанные с кибербезопасностью и конфиденциальностью данных в сети.

Прежде всего, возникает вопрос: где находятся границы цифровой безопасности? Действует ли на них императив национальной безопасности или данная сфера должна регулироваться совместно всеми государствами? Кто ответственен за модерацию контента, защиту конфиденциальности данных, установление границ защиты предпринимательной деятельности в диджитал-среде? По нашему мнению, данные задачи должны быть возложены на надгосударственные структуры.

Согласно другому исследованию, проведенному IDG в 2019 году, были выявлены следующие тенденции относительно изменения приоритетов компаний в сфере кибербезопасности:

Отмечается рост финансирования программ кибербезопасности.

- 25% бюджета выделяется на обучение и профессиональную подготовку квалифицированных кадров в сфере информационной безопасности.
- 23% и 22% бюджета выделяется соответственно на технологическое и инфраструктурное оборудование.
- Уже сейчас более 2/3 всех организаций (88% крупных и 51% малых и средних предприятий) имеют специалиста по кибербезопасности.
- 38% рабочих в сфере IT и информационной безопасности ожидают увеличения расходов на обеспечение кибербезопасности.

Наиболее распространенными инструментами и технологиями в рамках стратегий безопасности опрошенных компаний являются: Zero Trust (47%), технологии обмана (40%) и мониторинг и анализ поведения (39%).

Согласно исследованию Forbes относительно прогнозов кибербезопасности на 2020 год, проблемы безопасности будут расти по мере расширения использования искусственного интеллекта (когнитивных систем) и иных новых технологий в сфере обеспечения информационной безопасности. Так, по словам вице-президента IBM Security Аарти Боркара, уже сейчас появляется большое количество «слепых зон безопасности», которые уже приводят и потенциально могут привести к серьезным угрозам, упущениям системами, равно как и к ложным срабатываниям. Преодоление данного рода проблемы должно подкрепляться обеспечением разнообразия механизмов поиска киберугроз и ученых, которые над ними работают.

Наиболее опасными кибератаками, по мнению генерального директора Theta Ray Марка Газита, признаны атаки на банки и другие финансовые организации: например, в последнее время появилось большое количество случаев утечки персональных данных пользователей банковских карт. Это не только нарушает право человека на конфиденциальность, но и влечет другие связанные с этим проблемы, в частности недоверия людей банковским системам. За последнее десятилетие стоимость и последствия киберпреступлений тревожно возросли.

Например, общие финансовые и экономические потери от атаки WannaCry 2017 года оцениваются в 8 миллиардов долларов. в 2018 году Marriott обнаружил, что нарушение системы бронирования дочерней компании Starwood потенциально могло раскрыть личную информацию и данные кредитной карты 500 миллионов гостей. Хакеры, кажется, продолжают становиться более эффективными. Томас Дж. Паренти и Джек Дж. Домет, соучредители Archefact Group, предполагают причину, по которой компании так восприимчивы к угрозам от взлома: отсутствие знания и понимания своих критических киберрисков, потому что они по-прежнему сосредоточены на своих технологических уязвимостях.

Более того, согласно мнению Джастина Сильвера, руководителя безопасности PROS, опасны любые проникновения в деловой мир, поскольку все они влияют на принятие управленческих решений. Необходимо уделять больше внимания аудиту алгоритмов искусственного интеллекта на предвзятость (например, недавняя ошибка алгоритма Apple Credit Card), особенно при процессе организационного принятия решений.

По нашему мнению, любой алгоритм выявления потенциальных кибер-угроз должен опираться на различные системы и механизмы, способные не только выявить кибер-угрозы, но и предотвратить их. Обширное количество используемых технологий и инструментов, адаптированных под одновременную совместную работу, позволит найти максимально возможное количество «слепых зон» и не допустить нарушения безопасности в данной сфере.

Проанализировав отчеты и исследования в динамике за последние 5 лет, мы пришли к выводу что традиционных методов защиты становится недостаточно и все чаще на их смену приходят такие как блокчейн и интернет вещей Internet of Things (IoT). IoT меняет концепцию ведения бизнеса в реальном мире, одновременно обеспечивая беспроводную связь между повседневны-

ми объектами в организациях. Технология, безусловно, запускает новые инновации в различных вертикалях. Это помогает предприятиям оптимизировать свои процессы, повысить производительность, а также повысить эффективность работы в различных отраслях. Компании, которые приняли эту технологию, могут предложить своим клиентам более качественные и улучшенные продукты и услуги.

Одним из основных направлений деятельности Honeywell является промышленный Интернет вещей (IIoT), интеграция цифровых технологий в производство. Это делает упор на информацию, а не на физические механизмы, даже в тех областях, где традиционно требуется физический труд.

В 2019 году Honeywell выпустила программное решение под названием Honeywell Forge, которое помогает отраслям собирать, анализировать и обрабатывать данные, поступающие из различных частей их операций. Это могло бы хорошо позиционировать компанию для будущего IIoT. Согласно исследованию Honeywell, в котором приняли участие 600 американских бизнес-профессионалов, 70% инвестировали «значительные» суммы в IIoT, а 9 из 10 считают, что IIoT окупит себя. Использование промышленного интернета вещей (датчики на оборудовании) позволило Schneider Electric сократить потребление на 12% в третий год и на 10% в четвертый год.

Продолжающийся рост IoT-индустрии станет трансформирующей силой для всех организаций. Интегрируя современные устройства с подключением к Интернету, рынок IoT стремительно растет к 2026 году в год до более чем 3 триллионов долларов США. Прогнозируемая доля глобальных расходов на IoT к 2020 году составит 50–60% в сфере предпринимательства / промышленности, 20–25% в потребительском секторе и 20–25% в сфере услуг / государственном секторе.

Потребность в IoT - это легкое, масштабируемое и распределенное решение для обеспечения конфиденциальности и безопасности. Блокчейн в свою очередь обладает потенциалом для преодоления этих проблем благодаря своему распределенному, безопасному и частному характеру. Данная технология, которая получает все большее развитие может обогатить IoT, предоставляя услугу надежного совместного использования, где информация является надежной и может отслеживаться. Сочетание Blockchain и IoT может быть довольно мощным, поскольку Blockchain может обеспечить устойчивость к кибератакам и возможность взаимодействовать с коллегами без доверия, надежным и проверяемым способом с высокой оперативностью процесса. Непрерывная интеграция Blockchain с IoT приведет к значительным преобразованиям во многих отраслях, что приведет к появлению новых бизнес-моделей.

Распределенный регистр в системе блокчейнов защищен от несанкционированного доступа, что устраняет необходимость доверия между вовлеченными сторонами. Ни одна организация не может контролировать такое огромное количество данных, генерируемых устройствами IoT, с помощью традиционных средств.

Использование блокчейна для хранения данных IoT добавит еще один уровень безопасности, который хакерам придется обойти, чтобы получить доступ к сети. Блокчейн обеспечивает гораздо более надежный уровень шифрования, что делает практически невозможным перезапись существующих записей данных.

Технология обеспечивает прозрачность, позволяя любому, кому разрешен доступ к сети, отслеживать транзакции, которые произошли в прошлом. Это позволяет предупредить и заранее предусмотреть возможные источники любых утечек данных и принятия, применяя быстрые меры по исправлению положения.

Блокчейн может обеспечить быструю обработку транзакций и координацию между миллиардами подключенных устройств. По мере роста числа взаимосвязанных устройств технология распределенного регистра предоставляет жизнеспособное решение для поддержки обработки большого количества транзакций.

Предоставляя способ обеспечить доверие между заинтересованными сторонами, блокчейн может позволить компаниям IoT снизить свои затраты за счет устранения накладных расходов на обработку, связанных со шлюзами IoT (например, затраты на традиционные протоколы, оборудование или накладные расходы на связь). Над поиском оптимальных вариантов сочетания двух

технологий работает так называемый Chain of Things (CoT), который представляет собой консорциум технологов и ведущих блокчейн-компаний. Он исследует наилучшие возможные случаи использования, когда комбинация блокчейна и IoT может предложить значительные преимущества для промышленных, экологических и гуманитарных целей. Консорциум разделяет три варианта направления разработок решений: «Цепочка безопасности», «Цепочка солнечной энергии» и «Цепочка доставки».

IoT может потенциально улучшить качество жизни в различных областях, включая медицинские услуги, умные города, строительную отрасль, сельское хозяйство, управление водными ресурсами и энергетику. Говоря о направлении «Цепочка солнечной энергии», интеграция технологии IoT позволяет не только включать больше систем в сеть, но также улучшает общее управление сетью. Размещая датчики на подстанциях и вдоль распределительных линий, компании могут собирать данные о потреблении электроэнергии в режиме реального времени. Энергетические компании могут использовать эти данные для принятия эффективных решений о контроле напряжения, переключении нагрузки и конфигурации сети. Датчики, расположенные на сети, также могут помочь операторам оповещать о сбоях в режиме реального времени. Доступность данных в реальном времени позволяет работникам быстро отключать питание поврежденных линий. Это предотвращает возможные случаи поражения электрическим током, пожары или другие опасности.

IoT даже позволяет некоторым из этих решений стать автоматизированными. Автоматизированная система оказывается более эффективной, чем зависимая от человека. в случае сбоя интеллектуальные коммутаторы могут автоматически изолировать проблемные зоны. Устройства IoT могут перенаправить питание, чтобы быстро включить свет. Это приводит к экономии драгоценного времени и человеческих ресурсов. Данные об энергопотреблении также могут служить основой для прогнозирования нагрузки. IoT помогает в управлении перегрузками вдоль линий электропередачи. Они помогают обеспечить соответствие всех генерирующих установок требованиям, связанным с контролем частоты и напряжения. Эти данные о потреблении энергии также могут помочь компаниям решить, где построить новую инфраструктуру или обновить существующие.

Соединенное Королевство было одним из первых пользователей технологии интеллектуальных сетей. в рамках проектов Фонда низкоуглеродных сетей и конкурса инноваций в электроэнергетических сетях правительства приняли решения по интеллектуальным сетям и интеллектуальным счетчикам. Эта система обеспечивает наблюдаемую, автоматизированную и контролируемую электрическую сеть.

Интеллектуальные энергосистемы - это современные энергосистемы, в которых используются наиболее безопасные и надежные информационно-коммуникационные технологии для управления и оптимизации энергопотребления, электрических сетей передачи и распределения, а также конечного использования. Соединив много интеллектуальных счетчиков, интеллектуальная сеть развивает разнонаправленный поток информации, который может использоваться для оптимального управления системой и эффективного распределения энергии. Применение интеллектуальной сети может быть выделено в разных подсекторах энергосистемы индивидуально, например, в производстве энергии, зданиях или транспорте, или их можно рассматривать в целом.

Список использованных источников:

1. Исследование приоритетов компаний в сфере кибербезопасности IDG 2019. Режим доступа: https://www.idg.com/tools-for-marketers/2019-security-priorities-study/
2. Сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. Режим доступа: https://digital.gov.ru/ru/activity/directions/874/

3. Сайт Forbes. Режим доступа: https://www.forbes.com/sites/gilpress/2019/12/03/141-cybersecurity-predictions-for-2020/#44f5a4621bc5
4. Alladi, T.; Chamola, V.; Rodrigues, J.J.; Kozlov, S.A. Blockchain in Smart Grids: A Review on Different UseCases. Sensors 2019, 19, 4862.
5. Anjana, K.; Shaji, R. A review on the features and technologies for energy efficiency of smart grid. Int. J. Energy Res. 2018, 42, 936–952.
6. Bandyopadhyay, D.; Sen, J. Internet of Things: Applications and Challenges in Technology andStandardization. Wirel. Pers. Commun. 2011, 58, 49–69.
7. Chow, R. The Last Mile for IoT Privacy. IEEE Secur. Priv. 2017, 15, 73–76.
8. Hossain, M.; Madlool, N.; Rahim, N.; Selvaraj, J.; Pandey, A.; Khan, A.F. Role of smart grid in renewableenergy: An overview. Renew. Sustain. Energy Rev. 2016, 60, 1168–1184.
9. Hossein, N., Mahsa Mohammadrezaei, M., Hunt, J., & Zakeri, B., 2020. "Internet of Things (IoT) and the Energy Sector", Energies, vol. 13, pp. 494.
10. Lee, C.; Zhang, S. 2016. Development of an Industrial Internet of Things Suite for Smart Factory towards Re-industrialization in Hong Kong. In Proceedings of the 6th International Workshop of Advanced Manufacturing and Automation, 10–11.
11. Navigating the rising tide of uncertainty, PwC's 23rd Annual Global CEO Survey, 2020 PwC, 2019. New world. New skills. Режим доступа: https://www.pwc.com/gx/en/issues/upskilling.html
12. Nicole Perlroth, Amie Tsang and Adam Satariano "Marriott Hacking Exposes Data of Up to 500 Million Guests". Режим доступа: https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html
13. Oracle and KPMG cloud threat report 2019 Defining Edge Intelligence: Closing Visibility Gaps with a Layered Defense Strategy.
14. Parenty, T. J., & Domet, J. J., 2019. "Sizing Up Your Cyberrisks", Harvard Business Review, November–December 2019.
15. Porambage, P.; Ylianttila, M.; Schmitt, C.; Kumar, P.; Gurtov, A.; Vasilakos, A.V. The quest for privacy in the internet of things. IEEE Cloud Comput. 2016, 3, 36–45.
16. Poyner, I.; Sherratt, R.S. Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT—2018, 28–29 March 2018; pp. 1–5.
17. Schwab, K., 2019. Global Competitiveness Report 2019: How to end a lost decade of productivity growth, World Economic Forum. Режим доступа: https://www.weforum.org/reports/how-to-end-a-decade-of-lost-productivity-growth
18. Stergiou, C.; Psannis, K.E.; Kim, B.G.; Gupta, B. Secure integration of IoT and Cloud Computing. Future Gener. Comput. Syst. 2018, 78, 964–975.
19. Sigfox, Inc. Utilities & Energy. 2019. Режим доступа: https://www.sigfox.com/en/utilities-energy/
20. Thomas, R., Devan, P., & Khan, A. 2018. The Internet of Things: A technical primer, Deloitte Insights.

ЛЕКАРЕВ ЕВГЕНИЙ ЕВГЕНЬЕВИЧ
студент факультета бизнеса и менеджмента
НИУ ВШЭ, г. Москва
E-mail: lekarev.evgeniy@gmail.com

РИСКИ И УГРОЗЫ В ОБЛАСТИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ПРИМЕНЕНИЕ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА

LEKAREV EVGENIY EVGENEVICH
student, faculty of business and management
National Research University «Higher School of Economics», Moscow

THE RISKS AND THREATS IN THE FIELD OF ECONOMIC SECURITY OF THE ENTERPRISE APPLICABILITY OF THE RISK-ORIENTED APPROACH

Аннотация: В современных условиях глобальной экономической нестабильности, одной из важнейших задач, стоящих перед коммерческими организациями и иными субъектами хозяйствования, является адаптация к условиям политической и социально-экономической нестабильности, а также поиск эффективных решений и выработка оптимальной реакции на возникающие угрозы. Важнейшим фактором, определяющим эффективность предпринимательской деятельности, является разработка и реализация комплексной системы обеспечения экономической безопасности предприятия. в данной статье раскрыто значение и описаны основные подходы к определению понятия экономической безопасности, описаны функциональные составляющие данного понятия, а также определены факторы, риски и угрозы, оказывающие влияние на экономическую безопасность предприятия. Помимо этого, в статье рассматриваются теоретические основы «риск-ориентированного подхода», а также его роль и значение в управлении бизнесом.

Abstract: In a world of continuing global instability, the most important challenge that commercial organizations and other economic entities are facing is adaptation to a prevailing political and socio-economic instability as well as finding effective solutions and best response to emerging threats. The key factor that will determine business performance and efficiency is development and implementation of a complex system of economic business security. This paper outlines and defines major concepts of economic business security, its functional components and determines various factors, risks and threats affecting business security. Additionally, the research looks into theory of “risk-orientated approach” and its role in running a business.

Ключевые слова: экономическая безопасность, предприятие, безопасность предпринимательской деятельности, управление рисками, риск-менеджмент

Keywords: economic security, enterprise, entrepreneurship security, risk-management

Введение

В современном мире, где функционирование предприятия подвержено влиянию огромного количества факторов, связанных как с внешней, так и с внутренней средой организации, остро встает вопрос обеспечения безопасности. Отрицательное воздействие на деятельность организации оказывают такие макроэкономические факторы, как несовершенство законодательства в сфере малого и среднего бизнеса, недостатки правового регулирования, нестабильная экономика, мошенничество и коррупция, дефицит информации. к микроэкономическим факторам, оказыва-

ющим влияние на организационную деятельность, относятся факторы производства, корпоративная культура, менеджмент и кадры.

Предпринимательская среда всегда носит неопределённый характер, а сами организации развиваются и функционируют в условиях ограниченности ресурсов. Экономическая деятельность, осуществляемая без учета факторов неопределенности и риска, не способствует достижению устойчивого развития предприятия. Таким образом, осуществляя управление бизнесом, предприниматели сталкиваются с различными управленческими проблемами, требующими адекватной оценки и принятия управленческих решений для защиты законных интересов своего бизнеса от рисков и угроз в различных сферах. Состояние защищенности интересов организации от внутренних и внешних угроз, достигаемое за счет анализа профильных рынков, оценки уровня конкуренции и состояния конкурентной среды, обработки и анализа полученных данных и информации с целью принятия соответствующей системы мер является экономической безопасностью предприятия [Шульц В.Л. 2019, С. 32]. Под системой мер в данном случае подразумевается комплекс мероприятий, принимаемых предприятием с целью достижения стабильности функционирования его организационных структур, устойчивого финансового положения, использования современных бизнес-технологий независимо от состояния внешней и внутренней среды, что в последствии определяет его устойчивость, а также надежное функционирование всех бизнес-процессов. Ранее термин экономическая безопасность использовался в более узком смысле и означал обеспечение надежности информации, составляющей коммерческую тайну, в настоящее же время большинство авторов рассматривает экономическую безопасность, как некое состояние, при котором предприятие добивается защищенности его имущества, информации, научно-технических достижений, а также других жизненно важных интересов путем предотвращения или ослабления угроз, а также минимизации рисков [Грунин О.А., 2002]. к основным задачам системы экономической безопасности предприятия можно отнести мониторинг и прогнозирование угроз, оценку рисков, а также разработку механизмов и методов их нивелирования для поддержания стабильного функционирования предприятия и постоянное совершенствование данных механизмов.

Актуальность проблемы

За последние годы в России было ликвидировано значительное количество предприятий, что говорит о том, что вне зависимости от организационно-правовой формы многие предприятия не способны справиться с предпринимательскими рисками и угрозами и вынуждены прекращать свою деятельность. По результатам исследования аудиторско-консалтинговой сети FinExpertiza, основанного на данных Росстата, в 2018 году в России на основании признания несостоятельности было ликвидировано в 2 раза больше предприятий (свою деятельность прекратили более 600 тыс. организаций), чем открыто за тот же период. Основные трудности, с которыми сталкивались предприниматели, включают в себя проблемы с деловым климатом и убыточностью бизнеса в виду высоких кредитных ставок и ограниченного доступа к финансовым ресурсам и рынкам сбыта, дефицит кадров и другие. в настоящий момент в России наблюдается острая проблема с устойчивостью бизнеса, которая может усилиться в текущем году на фоне общей нестабильности глобальной и российской экономик, вынужденного закрытия многих предприятий вследствие пандемии, негативной конъектуры на рынке, роста валютного курса, сокращения потребительского спроса, деловой и инвестиционной активности. Другие проблемы, с которыми сталкиваются предприятия в настоящий момент – это увеличение себестоимости продукции, приостановка и закрытие производственных компаний поставщиков сырья и комплектующих, как следствие задержка поставок сырья. в условиях тотальной неопределенности предпринимателям непросто просчитывать сценарии развития бизнеса, а также осуществлять планирование логистической деятельности, распределение и маневрирование оборотными средствами и принимать другие управленческие решения, что в последствии может привести к полной остановке деятельности еще большего числа предприятий. Помимо этого многие компании не уделяют должного внимания своей экономической безопасности, в частности анализу и оценке рисков, и оказываются

неготовыми к резким изменениям в их внутренней и внешней среде, а также неспособными поддерживать стабильное функционирование в таких условиях. По данным исследования оценки уровня зрелости управления рисками в России, проведенного исследовательским центром компании «Делойт», в большинстве организаций уровень зрелости управления рисками оценивается, как низкий (40%) или средний (42%). При этом по большей части управление рисками в организациях (84%) не интегрировано с ключевыми бизнес-процессами, а также процессами принятия решений. Основными проблемами, связанными с управлением рисками, являются нежелание или незаинтересованность руководителей в проведении анализа существующих рисков и угроз и внедрении системы управления рисками, а также отсутствие навыков и компетенций для проведения анализа и оценки.

Понятие рисков и угроз в области экономической безопасности

С рисками и угрозами предприниматели сталкивались во все времена, однако именно сейчас появилась реальная возможность идентифицировать их, оценивать различные последствия их реализации и принимать необходимые меры для минимизации и нивелирования негативных последствий их влияния [Авдийский В.И., Безденежных В.М., 2013]. с точки зрения экономической безопасности, риски и угрозы – это характеристики категорий разного уровня. Для выявления наиболее характерных различий между рисками и угрозами в области экономической безопасности, необходимо рассмотреть обе категории отдельно друг от друга.

Угрозы – это совокупность условий и факторов, которые создают опасность жизненно важным интересам предприятия и способны негативно повлиять на его экономическую безопасность в настоящем или будущем. Выделяют три главных внешних источника угрозы: государственная политика в сфере экономики, способствующая неблагоприятной экономической ситуации в стране; конкурентная среда, в случаях, когда речь идет о недобросовестной конкуренции, и кризисные явления в мировой экономике. По типам угрозы делятся на внешние и внутренние, случайные и преднамеренные, нацеленные против собственности, исходящие от персонала организации, направленные против сотрудников, административные и уголовные, управленческие, информационные, структурно-функциональные, кредитно-финансовые, технологические, товарно-распределительные и экологические [Ильных А.С., 2016].

В свою очередь, предпринимательский риск в общем понимании – это вероятность наступления неблагоприятного события или неудачного исхода производственно-хозяйственной деятельности. Согласно другому определению, риск является волатильностью доходности, ведущей к непредвиденным расходам. Риски можно разделить на операционные (риск убытка по причине ошибочных действий персонала, ошибок в процессах и системах управления, а также риски внешней среды, включая политические и финансовые); рыночные (валютные, товарные, риск изменения цены акций), а также кредитные, деловые, репутационные, стратегические риски и риски ликвидности (риск ликвидности фондирования и активов) [Гэлаи Д., Кроуи М., Минасян В. Б., Марк Р., 2019; Авдийский В.И., Безденежных В.М., 2013].

По мере и времени возникновения риски можно разделить на ретроспективные (продолжающиеся длительный период времени), текущие и перспективные; по причинам появления – на природно-естественные, политические, экономические, технические, имущественные, транспортные, коммерческие и экологические. Также риски условно можно разделить на две большие категории: чистые и спекулятивные. в результате реализации чистых рисков результат может быть нулевым или отрицательном, в то время как спекулятивные могут привести как к положительному, так и к отрицательному результату.

Не существует безрисковых видов деятельности - любая форма деятельности подразумевает те или иные риски, которые в определенных ситуациях могут проявляться и приводить к негативным последствиям, что говорит о всеохватности риска. Каждая интеллектуальная система оценивает величину риска, а также формирует границы его приемлемости путем категоризации полей риска, основываясь на особенностях, закономерностях, установках и критериях своей внутренней деятельности. Субъективность в оценке риска определяется индивидуальными осо-

бенностями личности человека, ответственного за принятие управленческого решения. Однако риски существуют и проявляются вне зависимости от желания и намерений данного индивидуума, что свидетельствует об объективности причин их существования. Последнее свойство риска – это неповторимость: каждая ситуация, с которой сталкиваются предприниматели, уникальна, риск зависит от множества факторов и его повторение невозможно [Шульц В.Л., 2019].

Риск является более широким понятием, нежели угроза, и можно с уверенностью сказать, что управление рисками должно лежать в основе формирования эффективной системы обеспечения экономической безопасности предприятия, а сама экономическая безопасность является риск-ориентируемой, так как характеризует способность бизнеса развиваться и функционировать в условиях постоянно изменяющейся внутренней и внешней среды. Принятие большинства управленческих решений должно быть основано на идентификации и выявлении риска, измерении и оценке уровня подверженности риску, а также оценке его эффектов. в данном случае риск-менеджмент или управление рисками рассматривается как непрерывный процесс снижения уровня корпоративного риска, а также выбор организацией приемлемого для себя типа и уровня риска [Гэлаи Д., Кроуи М., Минасян В. Б., Марк Р., 2019].

Управление рисками

В последние несколько десятилетий в современной экономической науке, в частности в организационном менеджменте, набирает все большую популярность теория управления рисками организации. Система управления рисками предоставляет различные инструменты структурирования видения будущего, а также решения проблем неопределенности, с которыми так часто сталкиваются предпринимали. Использование данной теории на практике способствует обеспечению стабильного функционирования предприятия в рыночных условиях, увеличению продолжительности жизненных циклов, а также повышению финансовой устойчивости предприятия [Уродовских В.Н., 2010]. Согласно результатам исследования практик управления рисками в России, проведенного одной из крупнейших аудиторско-консалтинговых организаций KPMG Россия, основные цели внедрения систем управления рисками в крупных российских компаниях это – достижение стратегических целей (82%), сохранение активов, приносящих доход и повышение эффективности деятельности (75%), а также обеспечение соответствия регуляторным требованиям (36%). в 65% участвующих в исследовании компаниях создано отдельное структурное подразделение, отвечающее за координацию процессов управления рисками.

Процесс управления риском включает в себя несколько этапов (Рис. 1):

Рисунок 1. Основные этапы управления рисками

Далее данные этапы будут описаны более подробно:

1. Идентификация риска (составление четкой и полной картины рисков, с которыми сталкивается предприятие, формирование реестра рисков);
2. Анализ и оценка риска (измерение и оценка вероятности рисков, уровня подверженности рискам, их приоритезация посредством разработки матрицы рисков, составления дерева событий);
3. Поиск, оценка преимуществ и стоимости реализации различных альтернатив управления риском;
4. Выбор одной из стратегий управления риском:
   - Избежание риска (прекращение или отказ от деятельности, которая повышает вероятность возникновения риска, что также предполагает отказ от связанных с данной деятельностью выгод)
   - Передача или разделение риска (разделение риска с одной или несколькими сторонами, посредством аутсорсинга или страхования)
   - Снижение или смягчение риска (минимизация вероятности возникновения событий или их последствий, например, через ликвидацию источника их возникновения)
   - Допущение или принятие риска (признание наличия риска, но отказ от принятия мер по снижению его вероятности).
5. Исполнение выбранной стратегии управления риском и реализация программы, разработанной на предыдущем этапе (определение сроков исполнения и ответственных за реализацию лиц, определение источников ресурсов, проведение конкретных мероприятий)

Заключительным неформальным этапом является мониторинг результатов реализации той или иной программы, тщательный анализ реализованных рисков, а также постоянное совершенствование системы управления рисками.

Заключение

В настоящее время риск-ориентированный подход при управлении бизнесом является одним из наиболее перспективных направлений экономической деятельности, ведущим к минимизации издержек и улучшению финансовых показателей путем снижения вероятности наступления возможных рисков. От уровня экономической безопасности предприятия напрямую зависят его финансовое состояние, уровень экономической эффективности и положение организации на рынке. Для того, чтобы оценить экономическую безопасность предприятия, необходимо провести комплексную интегральную оценку индикаторов и показателей безопасности с учетом анализа риска и угроз на всех уровнях (персонал, различные подразделения и службы, менеджмент) и во всех направлениях деятельности хозяйствующих субъектов, включая финансовую, управленческую, коммерческую, производственную и снабженческую. Управление рисками – важнейший элемент механизма обеспечения экономической безопасности предприятия. Оценка рисков и угроз должна проводиться на всех этапах начиная с формирования основ обеспечения экономической безопасности (формирование стратегии, целей, функций и методов управления организацией) [Богомолов В.А., 2012], заканчивая разработкой управленческих решений и рекомендаций. в то же время управление рисками не является единственным важным элементом, так как анализ экономической безопасности должен проводиться комплексно. в рамках экономической безопасности проводится мониторинг контрагентов, анализ конкурентов и конкурентной среды, ведется противодействие мошенничеству. Помимо экономической безопасности предприятие должно уделять большое внимание финансовой, информационной, физической, инженерно-технической и кадровой безопасности.

Список литературы

1. Авдийский, В. И., Безденежных, В.М., «Риски хозяйствующих субъектов: теоретические основы, методология анализа, прогнозирования и управления.» ВИ Авдийский, ВМ Безденежных (2013): 2013-368.
2. Богомолов, В.А., 2012. Экономическая безопасность.
3. Грунин, О. А. «Экономическая безопасность организации/ОА Грунин, СО Грунин.» (2002).
4. Гэлаи Д., Кроуи М., Минасян В. Б., Марк Р.-ОСНОВЫ РИСК-МЕНЕДЖМЕНТА-М.: Издательство Юрайт, 2019-390-Бакалавр. Академический курс-978-5-534-02578-1: -Текст электронный // ЭБС Юрайт - https://biblio-online.ru/book/osnovy-risk-menedzhment..
5. Ильиных, А.С., 2016. Экономическая безопасность предприятия. Международный журнал гуманитарных и естественных наук, 7(1).
6. Уродовских, В. Н.. «Управление рисками предприятия.» (2010).
7. Шульц, В. Л. Безопасность предпринимательской деятельности: учебник для вузов / В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко ; под редакцией В. Л. Шульца. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 585 с. — (Высшее образование). — ISBN 978-5-534-12368-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/447405
8. Практики управления рисками в России: сильные стороны и области для развития URL: https://assets.kpmg/content/dam/kpmg/pdf/2015/11/S_CG_10r.pdf (Дата обращения 13.04.20)
9. Управление рисками в системах нормативного регулирования URL: https://www.unece.org/fileadmin/DAM/trade/Publications/WP6_ECE_TRADE_390R.pdf (Дата обращения 10.04.20)
10. Оценка уровня зрелости управления рисками в России URL: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/maturity-level-of-risk-management.pdf (Дата обращения 13.04.20)
11. Смертность бизнеса: за 2018 год в России закрылось в два раза больше компаний, чем открылось URL: https://finexpertiza.ru/press-service/researches/2019/smertnost-biznesa-za-2018/ (Дата обращения: 05.04.2020)ё

ЛЕКАРЕВ ЕВГЕНИЙ ЕВГЕНЬЕВИЧ
студент факультета бизнеса и менеджмента
НИУ ВШЭ, г. Москва
E-mail: lekarev.evgeniy@gmail.com

МАРТЫНОВ КИРИЛЛ ДМИТРИЕВИЧ
студент факультета бизнеса и менеджмента
НИУ ВШЭ, г. Москва
E-mail: kdmartynov@mail.ru

ТРОШИНА КРИСТИНА АНДРЕЕВНА
студенка школы иностранных языков
НИУ ВШЭ, г. Москва
E-mail: kristina.troshina98@gmail.com

МИНГАЗОВ АЗИЗ РИНАТОВИЧ
студент факультета права
НИУ ВШЭ, г. Москва
E-mail: aamingazov@mail.ru

ХОМУШКУ СЫРГА ВЛАДИМИРОВНА
студентка факультета права
НИУ ВШЭ, г. Москва
E-mail: syrgapinansj@yandex.ru

ЧЕРНЫШЕВА АННА ДМИТРИЕВНА
студентка факультета социальных наук
НИУ ВШЭ, г. Москва
E-mail: anncherka@gmail.com

ДЕЯТЕЛЬНОСТЬ ЦЕНТРАЛЬНОГО БАНКА РОССИЙСКОЙ ФЕДЕРАЦИИ В ПРОТИВОДЕЙСТВИИ ЛЕГАЛИЗАЦИИ ПРЕСТУПНЫХ ДОХОДОВ

LEKAREV EVGENIY EVGENEVICH
student, faculty of business and management
National Research University
«Higher School of Economics», Moscow

MARTYNOV KIRILL DMITRIEVICH
student, faculty of business and management
National Research University
«Higher School of Economics», Moscow

TROSHINA KRISTINA ANDREEVNA
student, school of foreign languages
National Research University
«Higher School of Economics», Moscow

MINGAZOV AZIZ RINATOVICH
student, faculty of law
National Research University
«Higher School of Economics», Moscow

KHOMUSHKU SYRGA VLADIMIROVNA
student, faculty of law
National Research University
«Higher School of Economics», Moscow

CHERNYSHEVA ANNA DMITRIEVNA
student, faculty of social sciences
National Research University
«Higher School of Economics», Moscow

THE ACTIVITIES OF THE CENTRAL BANK OF THE RUSSIAN FEDERATION IN COMBATING MONEY LAUNDERING

Аннотация: Механизмы отмывания денег разнообразны и широко распространены в современном мире. Такие практики приводят к ряду негативных последствий для мировой экономики, поэтому борьба с ними – первостепенная задача государств и международных организаций. В российской финансовой системе особое место занимает Центральный Банк Российской Федерации. В данной статье изучена роль и непосредственная деятельность Центрального банка в борьбе с легализацией (отмыванием) доходов, полученных преступным путем. Исследованы механизмы влияния Банка России на законодательную и нормативно-правовую базу в сфере борьбы с легализацией преступных доходов. Для исследования были изучены нормативно-правовые акты российского законодательства и иные официальные документы, учебники, монографии и публикации в научных журналах, проведен качественный контент-анализ СМИ. Рассмотрена национальная система противодействия отмыванию преступных доходов и финансирования тер-

роризма (ПОД/ФТ) Российской Федерации. Приведена статистика по легализации преступных доходов. Проанализированы примеры из реальной судебной практики, рассмотрены конфликты с участием «Мастербанка», «Внешпромбанка» и «Deutsche Bank». Исследователями выявлены проблемы, возникающие в данной сфере, предложены рекомендации, которые могут улучшить текущую ситуацию.

Abstract: the mechanisms of money laundering are diverse and widespread in the modern world. Such practices lead to a number of negative consequences for the global economy, therefore, the fight against these actions is the primary task of states and international organizations. In the Russian financial system, the Central Bank of the Russian Federation plays the major role. This article examines the role and direct activities of the Central Bank of Russia in the fight against the legalization (money laundering) of proceeds of crime. The mechanisms of the Bank of Russia influence on the legislative and regulatory framework in the field of combating money laundering are investigated. For the study, the regulatory legal acts and other official documents, textbooks, monographs and publications in scientific journals were studied, media content analysis was also conducted. The national anti-money laundering and counter-terrorist financing (AML / CFT) system of the Russian Federation is considered. The statistics on the legalization of criminal income is provided. Examples from real judicial practice are analyzed, conflicts with the participation of Masterbank, Vneshprombank and Deutsche Bank are examined. The researchers have identified problems encountered in the field of study and suggested solutions that can improve the current situation.

Ключевые слова: Центральный Банк, противодействие отмыванию доходов, легализация преступных доходов, отмывание денег, регулирование, законодательство, ПОД/ФТ

Keywords: Central Bank of Russia, anti-money laundering regulations, AML/CFT, money laundering, law

Введение

На сегодняшний день тенденции глобализации не оставляют в стороне ни одно государство. Происходят качественные и количественные изменения во всех сферах общественных отношений, будь то экономика, политика, здравоохранение. Данные изменения имеют как положительные, так и отрицательные черты. Во взаимоотношениях государств ключевой фактор выражен в притоке и оттоке капитала. Обмен капиталом проистекает как через легальные способы, так и нелегальные. Последние весьма разнообразны и распространены в современном мире. Такие практики несут за собой ряд негативных последствий для национальных экономик, проблема выходит на мировой уровень, поэтому борьба с данными противозаконными действиями – первостепенная задача государств и международных организаций.

Легализация преступных доходов напрямую связана с такими явлениями, как коррупция, бандитизм, терроризм, и до сих пор считается актуальной глобальной проблемой и серьезной угрозой для экономической, политической, социальной устойчивости и национальной безопасности большинства стран мирового сообщества. Являясь одним из ключевых аспектов деятельности организованных преступных групп и крупных криминальных сообществ, отмывание денег может повлечь тяжкие последствия для государственной экономики и нарушить функционирование рыночного аппарата.

В российской финансовой системе одну из главных ролей по борьбе с отмыванием доходов, полученных преступным путем, играет Центральный Банк Российской Федерации, который является объектом данного исследования. Предметом исследования является деятельность Центрального Банка в процессе противодействия легализации (отмыванию) средств, полученных преступным путем.

Актуальность проблемы

Отмывание денег (англ. money laundering) – придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученных в результате совершения преступления [37], то есть перевод неправомерно добытых денежных средств и имущества из теневой экономики в легальное поле. В официальных документах используется формулировка «легализация (отмывание) денежных средств или иного имущества, полученных преступным путем». В процессе легализации преступные деньги (“черный нал”) или электронную валюту встраивают в поток легальных денежных средств или трансформируют в иную форму собственности – имущество, ценные бумаги, объекты интеллектуального права с целью полноценного открытого использования, истинное же происхождение доходов тщательно скрывается путем осуществления формальных сделок [25].

Самая популярная причина легализации – обеспечение безопасности ресурсов в плане их сохранности. Не менее важным аспектом является мобильность – возможность удобного гибкого доступа к средствам в любое время и при любых обстоятельствах. Ключевую роль играет также персональная безопасность владельца денежных средств, так как при обнаружении значительных расхождений между тратами и легальными доходами неизбежно последуют процедуры разбирательств и ответственность перед регуляторами.

По данным Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН) [27], ежегодный объем легализованных активов в мире колеблется в диапазоне от 800 млрд. до 2 трлн. долларов США (2 – 5% мирового ВВП), однако реальные показатели гораздо выше, и их практически невозможно оценить, так как речь идет о бизнесе, имеющем высокую степень латентности.

Растущие объемы легализации преступных денежных средств говорят о необходимости повышения эффективности функционирования финансовых и правоохранительных органов стран мирового сообщества на национальном и международном уровне, поэтому процессу противодействия отмыванию преступных доходов уделяется значительное внимание, в законы вносятся необходимые поправки, проводятся глобальные конференции. Россия также заинтересована в пресечении подобных экономических преступлений и ведет собственную борьбу с легализацией денежных средств. Отмывание преступных доходов опасно не только само по себе, но и по причине косвенных последствий теневой деятельности. Их можно разделить на четыре группы: экономическая, коррупционная, криминальная и террористическая [8, с. 76-77]. Далее приводится краткое объяснение каждой из причин потенциальной опасности [13].

Экономическая причина. Легализация создает отдельный сектор экономики, над которым государство не имеет власти и не может его контролировать. Это происходит в результате нарушения установленного порядка экономической деятельности и распространения форм нелегального предпринимательства. Нелегальный сектор нарушает правила конкуренции, так как деньги, полученные преступным путем, вкладываются в легальный бизнес и дают ему преимущество, увеличивая сферу его влияния и тем самым ухудшая инвестиционный климат [1, с. 31]. По данным МВФ, каждый год общемировой ВВП теряет около 2—3% от своего объема именно из-за легализации преступных доходов [8, с. 75].

Коррупционная причина. Наличие механизмов отмывания денег стимулирует коррупцию, ведь без способов легализации взяток пропадает смысл коррупционных действий. Чтобы потратить доходы, полученные преступным путем, нужно сначала их легализовать.

Криминальная причина. Отмывание доходов часто является не только направлением, но условием и основным стимулом преступной деятельности [9, с. 14 – 16.].

Террористическая причина. Легализованные средства часто являются источником финансирования вооруженных формирований.

Анализ статистических данных

Ситуация с отмыванием денег в России весьма неоднозначная – борьба с отмыванием преступных доходов и финансированием терроризма ведется давно, но все еще недостаточно эф-

фективно. В период с 2000 по 2019 год суммарный отток капитала из России составил более 800 млрд. долл. США [см. Табл. 1]. По результатам исследования консалтинговой компании PwC, легализация преступных доходов составляет 15% экономических преступлений в России против 9% в мире [23]. В 2016 году показатели составляли 12% и 11% соответственно [5], однако нельзя однозначно сказать, что преступность по этому направлению в России возросла – скорее, повысилась раскрываемость.

За 2016 год Росфинмониторингу совместно с ЦБ удалось пресечь деятельность 12 теневых потоков и наложить арест на имущество финансовых пирамид и кредитных кооперативов на сумму около 1,7 млрд рублей [28]. В 2017 году положительный тренд сохранился, 22 площадки обслуживания теневых денежных потоков были закрыты, сумма выявленных средств превысила 80 млрд рублей, а по ст. 172 УК РФ возбуждено более 60 уголовных дел [29].

Обратимся к статистике, иллюстрирующей объемы вывода нелегальных денег из Российской Федерации. Заметен пик в 2014 году, что может быть связано с деятельностью так называемой российской «мегапрачечной», через которую начиная с 2011 года выводились огромные суммы российских денег [22]. Именно на начало 2014 приходятся значительные объемы легализованных средств. В следующей таблице представлены данные о притоке / оттоке денежных средств в России в период с 2000 по 2019 год:

Год	Отток (-) / Приток (+) капитала, млрд. долл. США	Год	Отток (-) / Приток (+) капитала, млрд. долл. США
2000	-24,8	2010	-30,8
2001	-15	2011	-81,4
2002	-8,1	2012	-53,9
2003	-1,9	2013	-61
2004	-8,9	2014	-154,1
2005	-0,3	2015	-56,9
2006	43,7	2016	-15,4
2007	87,8	2017	-31,3
2008	-133,6	2018	-76
2009	-57,5	2019	-35

Таблица 1. Показатели притока и оттока капитала в России с 2000 по 2019 год

Стоит отметить, что отток капитала в России необязательно свидетельствует об отмывании денег, особенно в нестабильные для экономики кризисные года, так как средства могут перемещаться за рубеж вполне законными способами. Кроме того, легализация преступных доходов возможна и на территории России в национальной валюте. По данным ЦБ РФ, в России, по сравнению с выводом денег за границу, в структуре сомнительных операций значительно преобладают операции по обналичиванию денежных средств [31]. Суммарный объем сомнительных операций составил в 2017 году более 100 млрд. руб. [17].

Анализ российского законодательства в сфере отмывания денег

Правовые основы регулирования легализации преступных доходов были заложены федеральным законом № 115-ФЗ от 7 августа 2001 года. Как следует из официального текста акта, «Закон направлен на защиту прав и законных интересов граждан, общества и государства путем создания правового механизма противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.» [37].

В первой главе данного закона определяется сущность понятий «доходы, полученные преступным путем», «легализация», «уполномоченный орган» и т. д.

Во второй главе говорится о мерах предупреждения отмывания преступных доходов. Перечислены организации по видам деятельности, ответственные за исполнение закона: страховые и

инвестиционные компании, лизинговые операторы, кредитные организации, агентства недвижимости, ломбарды, почтовые сервисы и др. При совершении сделок на сумму более 600 тыс. руб. организации должны исполнять процедуру контроля, в случае операций с недвижимостью цена объекта должна быть не менее 3 млн. руб. В этой же главе определяется порядок контроля сделок, если хотя бы одна из сторон причастна к террористической и / или экстремистской деятельности. Определяется порядок идентификации личности клиента (по запросу регулятора) и бенефициара. Пороговым значением сделки при идентификации лица является сумма в 30 тыс. рублей, при обмене наличности – 15 тыс. При превышении данных лимитов идентификация обязательна. Помимо этого, определяется порядок внутреннего контроля, права и обязанности адвокатов, нотариусов, лиц, осуществляющих предпринимательскую деятельность в сфере оказания юридических или бухгалтерских услуг.

Глава 3 всецело посвящена методологии противодействия легализации доходов, полученных преступным путем. Дается понятие уполномоченного органа, его обязанности и возможности.

Глава 4 повествует о важности международного сотрудничества при борьбе с отмыванием денежных средств и затрагивает процессы обмена информацией, выдачи преступников и т. д.

Заключительная, пятая глава, говорит об административной и уголовной ответственности за несоблюдение законодательства в сфере отмывания доходов, о прокурорском надзоре за его соблюдением и порядке обжалования решений уполномоченного органа.

На текущий момент на основании закона № 115-ФЗ функционирует национальная система противодействия легализации преступных доходов и финансированию терроризма (ПОД/ФТ), концепция которой была утверждена указом Президента Российской Федерации от 11 июня 2005 г. N Пр-984. Система объединяет государственные органы и организации, осуществляющие противодействие легализации преступных доходов и финансированию терроризма. Чтобы борьба с отмыванием денег имела успех, необходимо наладить эффективную коммуникацию между всеми участниками системы, задействованными в процессе. Сюда можно отнести:

- органы законодательной власти;
- органы исполнительной власти;
- органы судебной власти;
- правоохранительные органы – прокуратура, ФСБ, МВД, ФСКН;
- подразделения финансовой разведки;
- контрольно-надзорные органы, регуляторы – центральный банк, а также другие финансовые и нефинансовые организации;
- частные учреждения – банки; нотариальные конторы и тд.

Органы и организации наделены соответствующими полномочиями и действуют на основании нормативно-правовых актов РФ. Основная цель подобной системы – создать необходимые условия для проведения единой государственной политики в отношении противодействия отмыванию денежных средств, независимо от сопутствующей цели, которой может являться совершение преступлений, проведение террористических атак, личное противозаконное обогащения, коррупционная деятельность и т. д. Деятельность ПОД/ФТ ориентирована на защиту прав и свобод граждан, а также обеспечение национальной безопасности и охрану экономических интересов России.

Система по своему составу двухуровневая, содержит подсистемы: правоохранительный блок и финансовый мониторинг. Финансовый мониторинг, в свою очередь, бывает первичный и государственный. Отношения между субъектами внутри правоохранительного блока регулируются нормами уголовного, уголовно-процессуального законодательства и федеральными законами. Деятельность правоохранительной подсистемы сосредоточена на выявлении, пресечении и расследовании преступлений в сфере отмывания денег и финансирования терроризма.

К субъектам первичного финансового мониторинга относят организации, которые проводят операции с денежными средствами / другим имуществом. Они обязаны надлежащим образом проверять клиентов, выявлять подозрительные транзакции и по запросу представлять необходимую информацию уполномоченному органу – Росфинмониторингу. Именно на уровне первично-

го финансового мониторинга и возникает необходимость предупреждения отмывания преступных доходов и финансирования терроризма.

Государственный мониторинг осуществляется преимущественно Росфинмониторингом. При получении информации от первичного финансового мониторинга и наличии необходимых оснований, принимаются соответствующие меры, и информация передается правоохранительным органам. В данном случае субъектами выступают контрольно-надзорные органы, контролирующие исполнение требований закона № 115-ФЗ, касающихся фиксирования, хранения и представления информации. юридическими и физическими лицами. Вся подсистема финансового мониторинга регулируется преимущественно положениями административного и финансового права.

Ключевым регулирующим элементом национальной системы ПОД/ФТ является федеральный орган исполнительной власти - Росфинмониторинг, обеспечивающий синергетический эффект между финансовым мониторингом и правоохранительным блоком.

Деятельность государственных органов и организаций, задействованных в противодействии легализации доходов, полученных преступным путем и финансированию терроризма, регулируется Конституцией Российской Федерации, Федеральным законом от 7 августа 2001 г. № 115-ФЗ, другими федеральными законами (в том числе КоАП РФ, УК РФ), актами и постановлениями Правительства РФ (основные: № 82, № 667, № 58, № 209, № 492, № 804, № 1052), приказами Росфинмониторинга (№ 103, № 203, № 59, № 361, № 191, №207, №110), приказами Минфина РФ (№ 108н, № 5н), нормативными актами Центрального Банка РФ (Положение ЦБР от 29 августа 2008 г. № 321-П «О порядке представления кредитными организациями в уполномоченный орган сведений, предусмотренных Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»)

Положения нормативно-правовых актов рассматривают два аспекта трактовки термина легализация преступных доходов: совершение преступных действий (незаконное использование средств) и преследование цели сокрытия или утаивания преступного источника доходов, а также оказание помощи лицу, участвующему в совершении преступления, результатом которого становится процесс отмывания денежных средств (наличие нелегального источника доходов).

Административная ответственность за легализацию преступных доходов регламентируется статьей № 15.27 КоАП РФ «Неисполнение требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма)». Как и следует из названия, статья обязывает граждан – физических лиц и юридических организаций, своевременно предоставлять сведения об операциях, подлежащих обязательному контролю, а также операциях, которые вызывают подозрения в их осуществлении для легализации доходов, полученных преступным путем, или финансирования терроризма. Кроме того, закон обязывает предоставлять информацию по запросу уполномоченного органа и запрещает попытки воспрепятствования проведению проверок уполномоченным органом. Мера наказания варьируется в зависимости от части статьи от предупреждения до наложения штрафов (максимальные штрафы по данной статье – 50 тыс. руб. для должностных лиц, 1 млн. руб. – для юридического лица). Альтернативной мерой может стать дисквалификация должностного лица, либо административное приостановление деятельности организации. В 2018 году в России по результатам рассмотрения дел об административных правонарушениях по I инстанции по статье 15.27 КоАП РФ наказанию было подвергнуто 1056 лиц [30].

К административной ответственности могут также привлечь по статье № 15.39 КоАП РФ (ч.6, ч.7) за нарушение требований законодательства Российской Федерации в части открытия в кредитной организации счетов и вкладов. В статье приведены обязательные к исполнению рекомендации по предоставлению достоверных сведений в федеральный орган исполнительной власти. За несоблюдение указанных требований может последовать штраф в размере до пятидесяти тысяч рублей для должностных лиц государственных корпораций и до шестидесяти миллионов рублей для юридических лиц соответственно.

Контролирующие исполнение законодательство органы указаны в статье № 23.62 КоАП РФ «Органы, осуществляющие контроль за исполнением законодательства о противодействии лега-

лизации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (введена Федеральным законом от 30.10.2002 N 130-ФЗ)».

Уголовная ответственность за отмывание денег в соответствии с законодательством предусмотрена ст. № 174 и 174.1 УК РФ, согласно которым предметом преступления являются денежные средства или иное имущество, заведомо приобретенные лицом, совершившим преступление (ст. 174.1 УК РФ), или средства, приобретенные другими лицами преступным путем (ст. 174 УК РФ). Однако, это не единственные нормативно-правовые акты, связанные с легализацией преступных доходов.

Так, весьма часто с отмыванием денег сталкиваются при расследовании дел по статье № 200.1 УК РФ (Контрабанда наличных денежных средств и (или) денежных инструментов), ст. № 205.1 УК РФ (Содействие террористической деятельности), ст. № 193.1 УК РФ (Совершение валютных операций по переводу денежных средств в иностранной валюте или валюте Российской Федерации на счета нерезидентов с использованием подложных документов), ст. № 172 УК РФ (Незаконная банковская деятельность) и др.

Преступный доход, выявленный правоохранительными органами, проверяется Росфинмониторингом, способным обнаружить и отследить подозрительные операции и установить факт легализации (отмывания) денежных средств. Подобное взаимодействие весьма эффективно и оправдано, так как именно мониторинг финансовых операций часто становится отправной точкой, откуда можно отследить цепь событий и выйти на первичное преступление. Обратная ситуация также возможна: в процессе расследования уголовных дел по основным преступлениям устанавливается факт получения нелегальных доходов с последующей легализацией. Однако в данном случае важна специфика преступлений, так как отмывание доходов, полученных преступным путем, обычно связано с делами о мошенничестве, контрабанде, незаконном предпринимательстве, наркоторговле и так далее.

Анализ роли Центробанка в системе противодействия отмыванию преступных доходов

Российская система борьбы с выводом нелегальных средств представлена следующими основными участниками:

1. Федеральная служба по финансовому мониторингу;
2. Банк России;
3. Министерство Финансов РФ;
4. Федеральное казначейство.

Как часть механизма общей системы, ЦБ выполняет ряд функций: контрольную, нормативную, консультативную, аналитическую, инспекционную. В противодействии легализации преступных доходов также участвуют:

- Российская государственная пробирная палата;
- Роскомнадзор;
- Федеральная налоговая служба;
- Прокуратура РФ.

После ратификации Российской Федерацией в июне 2002 года международной Конвенции «О борьбе с финансированием терроризма» в 2003 г. Россия стала полноправным членом ФАТФ, в следствие чего началась имплементация рекомендаций ФАТФ по борьбе с финансированием терроризма: были предприняты меры по совершенствованию национального законодательства, в частности уголовного и административного. В КоАП РФ включили ст. 15.27 «Нарушение законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

В целях адаптации законодательной базы требованиям времени был принят Закон N 115-ФЗ «О противодействии легализации…», как уже было сказано ранее, регламентировавший правовые и организационные основы полномочий государственных органов, которые непосредственно или опосредованно принимают участие в предупреждении совершения операций с денежными

средствами или иным имуществом, добытым преступным путем.

По состоянию на 1 декабря 2018 года 104 кредитных организаций, соответствуют требованиям, установленным частями 1–1.2 и 1.5 статьи 2 Федерального закона от 21.07.2014 № 213 ФЗ, и постановлению Правительства Российской Федерации от 20.06.2018 № 706. Из них только 26 находятся под прямым или косвенным контролем Банка России. Управление ООН по наркотикам и преступности (УНП ООН), в своем докладе отмечает, что из всеобщего оборота незаконных денег, получаемых от всех форм трансграничной организованной преступности, не менее 70% производится с помощью финансовых институтов государства [34].

В свете этого на Центральный банк возложены контрольно-надзорные функции в банковском секторе. Это наделяет ЦБ полномочиями по пресечению отмывания денежных средств через кредитные организации, оздоровлению финансовых организаций и банковских групп, а также снижению рисков на финансовом рынке. На основании Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» в сфере противодействия легализации преступных доходов Банк России осуществляет надзор за соблюдением кредитными организациями законодательства о противодействии легализации преступных доходов и проводит мониторинг общего состояния банковской системы с целью обнаружения предпосылок к отмыванию денежных средств.

Действия Центробанка

Для проверки документации по исполнению требований Федерального закона «О противодействии легализации (отмыванию) доходов…» при проведении проверок кредитных организаций и их филиалов, создается рабочая группа из уполномоченных представителей ЦБ РФ, которые проводят комплексную проверку внутренних документов кредитной организации и ее филиалов. В случае обнаружения нарушений выносится предписание об их устранении, либо более жесткие санкции. Далее будут детально рассмотрены полномочия ЦБ РФ.

В соответствии со ст. № 74 Закона «О Банке России» в рамках противодействия легализации преступных доходов ЦБ РФ наделен следующими полномочиями: взыскивать с кредитной организации штраф; вводить запрет на осуществление кредитной организацией отдельных банковских операций, в рамках выданной ей лицензией на срок до одного года, а также на открытие ею филиалов; назначать временную администрацию по управлению кредитной организацией на срок до шести месяцев и др. Необходимо отметить, что при принятии решения о применении мер воздействия на кредитные организации, ЦБ РФ руководствуется принципом соразмерности санкций выявленным нарушениям банками законодательства о ПОД/ФТ. Начиная с 2011 года, на Центральный банк возложены обязанности органа банковского надзора по рассмотрению дел об административных правонарушениях, предусмотренных статьей 15.27 КоАП РФ.

На рисунке ниже представлена статистика по отзыву Центробанком лицензий у кредитных организаций. За 2007-2016 гг. орган отозвал и аннулировал около 556 лицензий у коммерческих банков. При этом за последние три года Центральным Банком были отозваны лицензии 276 кредитных организаций [24].

Рис. 1. Статистика административных правонарушений и отзыва лицензий коммерческий банков. Источник: ЦБ РФ.

Банк России ежегодно публикует данные о проделанной им работе в сфере противодействия легализации преступных доходов и финансированию терроризма. На банках в соответствии с ФЗ №115-ФЗ лежит обязанность по выявлению и представлению в уполномоченный орган (Росфинмониторинг) сведений об операциях по банковским счетам (вкладам) клиентов банка, носящих сомнительный характер. К критериям сомнительных сделок ЦБ РФ относит следующие элементы: необычное для конкретной ситуации поведение клиента; наличие нестандартных или сложных инструкций по порядку проведения расчетов; игнорирование клиентом выгодных условий оказания услуг; операции, не имеющие явного экономического смысла. Экспертами отмечается, что издаваемые ЦБ РФ рекомендации, на основе которых выявляются подозрительные операции, носят порой «нечеткий характер, что приводит к неэффективному использованию их со стороны банков. Перед страхом лишения лицензии, в одно время некоторые кредитные организации присылали в рамках обязательного контроля информацию о суммах от 2 рублей, к примеру, по благотворительным сборам на детей.

На первый взгляд кажется, что со стороны Банка России предпринимаются все меры для предотвращения отмывания «грязных» денег, однако есть и обратная сторона. Жесткие требования, предъявляемые Центральным банком, приводят к тому, что банки из финансово-кредитных организаций превращаются в надзорный орган, который держит под «колпаком» деятельность предпринимателей, опираясь на многочисленные рекомендации, предложенные Банком России.

Руководствуясь положениями международных стандартов и статистическими данными, Банк России создает методические рекомендации по разработке кредитными организациями правил внутреннего контроля в целях ПОД/ФТ. Они способствуют совершенствованию методов и программ внутреннего контроля в кредитных организациях. Необходимо отметить, что правила внутреннего контроля, кроме рекомендаций ЦБ РФ, должны опираться на научно обоснованную систему рекомендаций криминалистического характера. Банки должны активно использовать данные криминалистической методики, которые относятся к способу совершения и сокрытия преступления, но на практике это встречается весьма редко.

Анализ кейсов из реальной практики

В качестве примера деятельности Банка России в области ПОД/ФТ представлены реальные случаи, участниками которых стали две российские корпорации (Мастер-банк и Внешпромбанк) и международный банк Deutsche Bank.

Мастер-банк являлся крупной организацией, имевшей 12 отделений в 10 регионах России. Он входил в отечественные и международные рейтинги – к примеру, в 2002 году занял 993 место в рейтинге крупнейших банков мира The Banker TOP 1000. Еще в 2011 году прошли первые расследования в отношении сотрудников, вовлеченных в схемы по легализации преступных доходов (менеджеры Санкт-Петербургского отделения и ведущий специалист Мери Таванян). В 2012 году были возбуждены дела против двух бывших менеджеров, а в июле того же года МВД сообщило о раскрытии группировки, за последние пять лет легализовавшей и обналичившей 36 млрд рублей. 20 ноября 2013 года банк прекратил свою деятельность в связи с отзывом лицензии Центробанком [12].

Данная ситуация сопровождалась масштабным общественным беспокойством, так как клиентами банка были известные компании (среди них ритейлеры, турфирмы, гостиничные комплексы, рестораны и авиаперевозчики). Лишились средств партия «Яблоко», фонд «Доктор Лиза»; по картам банка получали зарплату сотрудники «ВГТРК» и Первого канала [26]. Тем не менее, вклады Мастер-банка были застрахованы, поэтому все убытки впоследствии были возмещены вкладчикам.

Второй пример иллюстрируется на случае с Внешпромбанком, у которого в январе 2016 года была отозвана лицензия в связи с обнаружением незаконного вывода капитала в размере более 1 млрд рублей. На тот момент превышение обязательств над активами было оценено в 210,1 млрд руб., что является огромной по российским меркам суммой. Руководством банка была раз-

работана целая схема по фальсификации отчетности [10]. В результате было возбуждено уголовное дело по ст. 159 УК РФ [29]. После отзыва лицензии в банке «зависли» средства Транснефти, Олимпийского комитета России и Русской православной церкви [11].

Начиная с 2015 года разрастался скандал вокруг крупнейшего немецкого банка – Deutsche Bank, в котором Центральный Банк России играл не последнюю роль. В 2014 году Центробанк РФ обратил внимание на подозрительные транзакции немецкого банка [21]. В российском подразделении банка происходила покупка ценных бумаг за рубли, которые сразу же выкупались лондонским подразделением уже за валюту, в том числе доллары. Подобные действия именуются «зеркальными сделками» и имели место в банке примерно с 2011 года. ЦБ РФ заподозрил, что такие операции могут применяться для незаконного вывода российского капитала. Осенью 2014 ЦБ РФ порекомендовал Deutsche Bank провести внутреннее расследование с целью выявления отмывания доходов, что банк и сделал в мае 2015. В результате некоторое количество московских сотрудников было отстранено от работы, так как они имели отношение к внебиржевым сделкам, имеющим признаки отмывания денег. В числе уволенных оказался один из топ-менеджеров банка, Тим Уиксвелл, который руководил отделом акций Deutsche Bank в России [19].

Проблема привлекла внимание других стран-партнеров банка, и постепенно они стали принимать участие в расследовании этого дела [18]. В 2015 году на проблемы в области соблюдения законодательства против отмывания денег обратил внимание Центральный банк ЮАР. Позднее к расследованию дела присоединились США и Великобритания. Министерство юстиции США и нью-йоркский департамент финансовых услуг отметили тесную связь между покупателями и продавцами акций: часто у них были одни бенефициары, менеджеры и агенты [20].

История развивалась в течение нескольких лет, и в 2018 году выяснилось, что «Дойче банк» замешан не только в отмывании российских денег, но является «прачечной» мирового уровня – он был задействован в ситуации с «панамским архивом» [14], а через американское подразделение были реализованы сотни миллионов долларов [16]. Несмотря на все скандалы, банк лишь урезал объем своей деятельности в России, но остался действующим.

Проблемы, возникающие в деятельности ЦБ в области ПОД/ФТ

В рамках данной темы нельзя обойти стороной вопрос, связанный с проблемами, возникающими в процессе деятельности ЦБ РФ. В настоящей главе рассмотрим основные из них. Очевидно, что далеко не во всех странах существует идеально сформированный механизм банковской системы, в том числе и по борьбе с отмыванием нелегальных доходов. В российских реалиях вопрос эффективности ПОД/ФТ ЦБ РФ особенно актуален в связи не столько с существующими недостатками самой системы, сколько из-за несовершенства законодательства.

Во-первых, по мнению исследователей, процесс противодействия чрезмерно детализирован правилами, регламентами и процедурами, предусмотренными Федеральным законом №115-ФЗ «О противодействии легализации (отмыванию) преступных доходов, полученных преступным путем, и финансирования терроризма» и другим нормативно-правовыми актами, регулирующими названную деятельность. Детализация проявляется в том, что из-за большого массива установленных норм банки оказываются «закованными» формальными требованиями, за неисполнение которых предусмотрена несоразмерная проступкам ответственность [4]. При всей детализации процедур все еще не существует четкого понятия подозрительных операций. В марте 2012 года Банком России было утверждено положение № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов», исходя из которого определяются основные признаки таких операций. Однако данный список с каждым годом неуклонно растет, что ведет к ущемлению прав добросовестных клиентов, которые попадают под некоторые из этих признаков по стечению обстоятельств [15].

Другая проблема возникает из-за ограниченности банков в своих действиях. Например, они не могут самостоятельно отказать в проведении операции, прекратить обслуживание по счету клиентов, действия которых могут показаться подозрительными. Данные полномочия принадлежат Банку России и Росфинмониторингу. С одной стороны, так защищаются интересы клиентов,

однако с другой стороны, это создает дополнительный канал отмывания нелегальных доходов. Безусловно, существует перечень исключений в действиях банков, но они не позволяют решить проблему полностью.

Проанализировав действия ЦБ РФ и всей банковской системы в целом по ПОД/ФТ в контексте существующего законодательства, можно заметить несоответствие поставленных в нем целей существующим реалиям. Так, уместно сказать о том, что законодателем были установлены правовые рамки, однако методическое и организационное обеспечение в части реализации банковскими организациями требований Банка России было произведено с большой задержкой. Центральному банку РФ потребовалось длительное время для разработки и передачи коммерческим банкам всей необходимой информации о порядке предоставления ими в Росфинмониторинг сведений, закрепленных в законодательстве о ПОД/ФТ. После этого понадобилось еще больше времени на то, чтобы ЦБ РФ предоставил закрепленный перечень правил, в соответствии с которыми коммерческие банки должны были оформить свою работу по нормам закона и квалифицировать кадры, чтобы они, в свою очередь, были компетентны в вопросе противодействия легализации преступных доходов. Итогом координационной деятельности Банка России стало предоставление полного перечня нарушений в области ПОД/ФТ и меры по их устранению. В число последних вошли не только штрафы в отношении банков, но также отзыв их лицензии, одновременно с чем, по сути, прекращается банковская деятельность.

При таком раскладе банки оказались не в самой благоприятной ситуации. В действительности им необходимо было с нуля проработать всю систему по противодействию легализации доходов, обобщить большой массив информации с целью выявления подозрительных действий клиентов, провести мероприятия по устранению ошибок. Результатом такой поспешной работы стала череда отзывов лицензий Банком России у коммерческих банков, которые впоследствии признавались причастными к отмыванию преступных доходов.

Заключение

Реализация комплекса мер по выявлению, раскрытию и расследованию преступлений, связанных с легализацией (отмыванием) преступных доходов и финансированием терроризма, предполагает необходимость повышения эффективности функционирования правоохранительных и финансовых органов различных государств мирового сообщества и требует от них согласованной деятельности как на национальном, так и на международном уровне.

В настоящее время борьба с отмыванием денег ведется во всем мире, но больших успехов не приносит. FATF активно работает над этой проблемой, но отчеты о деятельности как правило сводятся к анализу результатов апостериори, то есть разъяснению ситуации с легализацией преступных доходов в мире. При этом мир динамичен, и требует постоянной разработки актуального комплекса мер по противодействию отмывания денег, в особенности превентивных – на этапе финансового мониторинга.

За последние 10 лет российское законодательство в сфере ПОД/ФТ стало более эффективным и конкретным, однако до сих пор существуют проблемные места и спорные аспекты. Так, например, по судебной статистике Верховного суда РФ за 2018 год приговор по статье 174 УК РФ и 174.1 УК РФ суммарно вынесли всего по 33 делам, хотя объемы легализованных денежных средств за 2018 год возросли почти в 2 раза, по сравнению с 2017. Отсюда можно сделать вывод, что, либо большинство дел, так или иначе связанных с легализацией, выносится совсем по другим статьям – например, Незаконное предпринимательство, Контрабанда, Незаконная банковская деятельность и т. д., либо финансовый мониторинг в стране нуждается в серьезной доработке.

Детально проанализировав все нормативно-правовые акты и иные источники, авторы пришли к следующим выводам:

1. На сегодняшний момент проблема легализации денежных средств является значимой, поскольку потенциальный вред от подобных действий разнонаправлен. Последствия опасны как для локальных бизнес-предприятий и национальных экономик, так и для мирового сообщества.
2. Данный вид преступной деятельности не является самым распространенным в России или мире, однако характеризуется очень низкой раскрываемостью.
3. Центральный Банк играет одну из важнейших ролей в борьбе с отмыванием денег в России. Существуют примеры того, как ЦБ оказал влияние на раскрытие заграничных «прачечных» (пример Deutsche Bank).
4. Существующее законодательство нуждается в принятии новых мер, в частности:
   - ужесточение уголовного законодательства (необходимо связать легализацию денежных средств со смежными первичными преступлениями, доходы от которых отмываются);
   - ужесточение законодательства в сфере регулирования наличных денежных средств и электронной валюты, в том числе виртуальной.;
   - закрепление четко обозначенного перечня сомнительных (подозрительных) операций и облегчение процедур по обращению банками с запросами в уполномоченные органы, в том числе в ЦБ РФ;
   - предоставление банковским организациям разумных сроков для устранения ошибок.

Источники

1. Букарев В. Б. Легализация (отмывание) доходов, приобретенных преступным путем: общественная опасность и вопросы квалификации: дис. – М.: ВГ Букарев, 2006.
2. Гобрусенко К.И, Глотов В.И., Аржанова И. М. Национальная система противодействия легализации преступных доходов и финансированию терроризма/ редкол.: Каратаев М. В. (отв. ред) [и др.] – Москва. – 20 стр.
3. Гудкова М. В. К вопросу об осуществлении деятельности в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма Центральным банком Российской Федерации //Право: современные тенденции. – 2016. – С. 51-54.
4. Заернюк В. М. Оценка существующего механизма противодействия отмыванию преступных доходов в банковской сфере России //Дайджест-финансы. – 2012. – №. 12.
5. Оутен Д. и др. Российский обзор экономических преступлений за 2016 год //М.: PwC Россия. – 2016.
6. Понаморенко В. Е. О рисках вовлечения банков в незаконные финансовые операции в условиях региональной интеграции //Экономика. Налоги. Право. – 2016. – №. 3.
7. Ревенков П. В., Дудка А.Б., Воронин А. Н., Каратаев М. В. Финансовый мониторинг: управление рисками отмывания денег в банках. / Монография. - М.: КНОРУС, ЦИПСиР, 2012. – 279 с.
8. Русанов Г. А. Противодействие легализации (отмыванию) преступных доходов. – 2017.
9. Третьяков В. И. Организованная преступность и легализация преступных доходов: дис. ... д-ра юрид. наук. – Волгоград, 2009. – С. 14 – 16.

Электронные ресурсы

10. Банки.ру [Электронный ресурс]. Внешпромбанк лишился лицензии. URL: https://www.banki.ru/news/lenta/?id=8599468 (Дата обращения: 30.05.2019)
11. Банки.ру [Электронный ресурс]. Во Внешпромбанке зависли деньги Русской православной церкви. URL: https://vk.cc/axRYhw (Дата обращения: 30.05.2019)
12. Банки.ру [Электронный ресурс]. Книга памяти: «ОАО «Коммерческий банк «Мастер-Банк». URL: https://www.banki.ru/banks/memory/bank/?id=5876138
13. Ведомости. [Электронный ресурс]. Опасно: легализация! URL: https://vk.cc/axRW8k

14. Новая газета [Электронный ресурс]. «Панаму» натянули на Германию. Deutsche Bank вновь оказался в центре скандала, связанного с отмыванием денег. URL: https://vk.cc/axRXiO
15. Право.ру. [Электронный ресурс]. Банки против бизнеса: как применяются нормы о противодействии отмыванию средств. URL: https://pravo.ru/story/201558/ (Дата обращения: 25.05.2019)
16. Рамблер [Электронный ресурс]. Deutsche bank оказался крупнейшей мировой прачечной денег наркокартеля? URL: https://vk.cc/axON98
17. РБК. [Электронный ресурс]. ЦБ впервые раскрыл оценку объемов и структуры сомнительных операций. URL: https://vk.cc/axRWvu
18. РИА Новости [Электронный ресурс]. Минюст США проводит расследование по сделкам в Deutsche Bank. URL: https://vk.cc/axRWRv
19. РИА Новости [Электронный ресурс]. США подозревают Deutsche Bank в нарушении режима санкций против России. URL: https://vk.cc/axRYAQ
20. Тасс [Электронный ресурс]. США расследует операции Deutsche Bank на предмет нарушения санкций против РФ - Экономика и бизнес – ТАСС. URL: https://tass.ru/ekonomika/2378462(Дата обращения: 30.05.2019)
21. Deutsche Welle. [Электронный ресурс]. Три самых громких юридических скандала вокруг Deutsche Bank. URL: https://vk.cc/axON1w
22. OCCRP [Электронный ресурс]. Российская финансовая «мегапрачечная» в действии. URL: https://vk.cc/axRWU5 (Дата обращения: 28.05.2019)
23. PwC [Электронный ресурс]. Российский обзор экономических преступлений за 2018 год. URL: https://vk.cc/axRWN6 (Дата обращения: 25.05.2019)
24. PwC [Электронный ресурс]. Форензик. URL: https://vk.cc/axRX6C
25. TJ. [Электронный ресурс]. Индустрия отмывания денег: становление и развитие в прошлом и современности. URL: https://vk.cc/axONbf
26. The New Times. [Электронный ресурс] Прачечная закрыта. Стирка продолжается. URL: https://newtimes.ru/articles/detail/74564
27. United Nations [Электронный ресурс]. Money-Laundering and Globalization. URL: https://vk.cc/axRX32
28. Отчет о деятельности Росфинмониторинга за 2016 год. URL: http://www.fedsfm.ru/content/files/documents/2017/otchet_final.pdf
29. Отчет о деятельности Росфинмониторинга за 2017 год. URL: https://vk.cc/axON4n (Дата обращения: 25.05.2019)
30. Отчет о работе судов общей юрисдикции по рассмотрению дел об административных правонарушениях за 12 месяцев 2018 г. [Электронный ресурс]. URL: https://vk.cc/axRX8s
31. Отчет ЦБ РФ «Структура сомнительных операций в банковском секторе в 2018 году» (Дата обращения 25.05.2019)
32. Официальный сайт Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ). [Электронный ресурс]. URL: https://www.fatf-gafi.org/
33. Официальный сайт Судебного департамента при Верховном суде Российской Федерации. [Электронный ресурс]. URL: http://www.cdep.ru/index.php?id=79
34. Официальный сайт Федеральной службы государственной статистики (Росстат) URL: http://www.gks.ru/. (Дата обращения: 28.05.2019)
35. Официальный сайт Федеральной службы по финансовому мониторингу (Росфинмониторинг). [Электронный ресурс]. URL: http://www.fedsfm.ru/
36. Официальный сайт Центрального Банка Российской Федерации (ЦБ РФ). [Электронный ресурс]. URL: https://www.cbr.ru/today/resist/resist_sub/ Нормативные акты ЦБ РФ: https://www.cbr.ru/today/anti_legalisation/acts_resist/
37. Федеральный закон от 07.08.2001 N 115-ФЗ (ред. от 18.03.2019) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». URL: https://vk.cc/ajLa93

МОВСЕСОВ АЛЕКСАНДР ЖАНОВИЧ
аспирант кафедры ИУ-8
МГТУ им. Баумана, г. Москва
E-mail: alexmovsesov93@gmail.com

МОНИТОРИНГ УГРОЗ БИЗНЕСА В ИНТЕРНЕТЕ ПРИ ПОМОЩИ АНАЛИЗА ИСХОДНОГО КОДА

MOVSESOV ALEKSANDER JANOVICH
postgraduate student, the department IU-8
Bauman Moscow State Technical University, Moscow

MONITOR BUSINESS THREATS ON THE INTERNET BY SOURCE CODE ANALYSIS

Аннотация: В данной работе рассматривается проблематика обнаружения и предотвращения угроз бизнеса в сети Интернет при помощи непрерывного мониторинга в виде анализа исходного кода на уязвимости. Большая часть угроз бизнесу в сети возникает вследствие наличия программных ошибок и уязвимостей в используемых сервисах. в работе рассмотрен принцип работы анализаторов исходного кода и структура поиска уязвимостей. Определен класс уязвимостей, который можно обнаружить при применении данных анализаторов. Было проведено тестовое внедрение анализатора на предприятие. в работе предоставлены результаты данного внедрения, приведены выявленные сильные и слабые стороны мониторинга исходного кода.

Abstract: This work discusses the problem of detecting and preventing business threats on the Internet using continuous monitoring in the form of vulnerabilities searching by source code analysis. Most of the threats to business on the Internet arise from the presence of software bugs and vulnerabilities in the services used. The work considers the concept of source code analyzers and the structure of vulnerability searchers. The class of vulnerabilities that can be detected was defined. A test implementation of the analyzer at the enterprise was conducted. The paper presents the results of this implementation, identifies the strengths and weaknesses of source code monitoring.

Ключевые слова: taint анализ, анализ исходного кода, поиск уязвимостей, мониторинг безопасности.

Keywords: taint analysis, source code analysis, vulnerability searching, security monitoring.

Введение

В настоящее время, в связи с глобальным выходом российского бизнеса в сеть Интернет, появились новые угрозы его информационной среде, как у клиентов, так и у владельцев бизнеса.

В случае если бизнесом является банк или предприятия, обрабатывающие конфиденциальные данные, риски значительно возрастают, и данные угрозы могут нанести большой ущерб.

Некоторые виды угроз способны остановить работу системы полностью. Работоспособность бизнеса в сети Интернет зависит от его защищенности.

Цель данной работы заключается в исследовании возможности снизить размер возможного ущерба предприятию при помощи детектирования и предотвращения уязвимостей, используя непрерывный анализ исходного кода.

Для осуществления данной цели были поставлена следующая задача: определить эффективность мониторинга на основе анализа исходного кода, при помощи внедрения анализатора на предприятие.

В данной работе предоставлена классификация уязвимостей, рассмотрен принцип работы статического анализа и приведены результаты внедрения мониторинга на предприятии.

Основная часть

Классификация атак информационной среды бизнеса в Интернете :

Сетевые атаки.

Представляют из себя атаки на сетевую подсистему бизнеса и возникают из-за некорректных настроек сетевых служб, либо использования уязвимых версий библиотек. Также угрозы возникают при недостаточном шифровании каналов связи. Системы IPS (предотвращения вторжения) предоставляют средства мониторинга и предупреждения атак данного класса.

Социальная инженерия.

Данный вид атак является одним из наиболее опасных и проблемных с точки зрения его предотвращения. в общем случае, это шпионаж за сотрудниками компании с целью получить доступ к системе или узнать ее внутренние особенности. Уязвимостью является человеческий фактор. Для предотвращения подобных атак следует устанавливать мониторинг безопасности предприятия от вторжения, проводить внутреннюю разведку на поиск закладок, анализировать поведение сотрудников.

Атаки на поведение системы.

Данные атаки могут быть осуществлены при наличии уязвимостей в системе.

1. Уязвимости конфигурации.
2. Уязвимости архитектуры системы.
3. Уязвимости кода.

Подобные уязвимости могут появляться при некорректном процессе разработки и недостаточном мониторинге и аудите безопасности системы.

Аудит безопасности представляет собой тестирование системы с помощью имитирования поведения злоумышленника и проведения поиска потенциальных проблем и тестирующих атак.

Данные виды атак приводят к следующим угрозам:

1. Отказ в обслуживании.
2. Превышении полномочий заданной роли пользователя.
3. Получение доступа к базе данных (утечка данных).
4. Расшифровка конфиденциальной информации пользователей.
5. Внедрение произвольного кода на выполнение.
6. Уничтожение системы.

В сфере сетевых вторжений существует большое количество средств мониторинга (IPS) и сбора информации о потенциальных угрозах, а также средства оценки рисков.

Однако, защищая только сеть организации и проверяя систему только на известные вирусы, возникают рассмотренные выше угрозы использования собственного программного обеспечения бизнеса.

Чем крупнее компания, тем больше вероятность необходимости использования программного обеспечения собственного производства, основываясь на нуждах компании.

Представленные выше средства защиты не гарантируют защищенность системы с потенциально уязвимыми собственными сервисами. Для того, чтобы обеспечить целостность системы, необходимо производить автоматизированный анализ кода.

Сам код может быть источником багов, логических проблем в проведении различных операций, например транзакций, а также представлять из себя всевозможные уязвимости из приведенной выше классификации. По этой причине возможность отслеживать и минимизировать возникающие риски, является важной проблемой.

Анализ кода в общем случае — это проверка исходного или скомпилированного кода на удовлетворение какого-либо условия. Например, это может быть проверка на хранение пароля в константе. Если условие выполняется, то данная константа является потенциальным источником проблем. Узнать, что в константе хранится пароль, довольно просто, изучив, где он был использован и нет ли в данных областях контекста передачи пароля.

Процесс анализа разбивается на несколько фаз: лексический анализ, синтаксический и семантический [Ахо, Лам, Сети, Ульман, 2016].

Лексический анализ представляет собой разбор исходного кода на токены при помощи регулярных выражений. Среди токенов могут быть ключевые слова рассматриваемого языка, пробелы (которые обычно игнорируются), идентификаторы и различные литералы. Он необходим для упрощения последующих фаз анализа и построения необходимых структур данных.

Синтаксический анализ заключается в парсинге полученных токенов и построении из них абстрактного синтаксического дерева. Решается данная задача при помощи методов рекурсивного спуска или алгоритма сортировочной станции. После выполнения данной фазы, на выход подается набор деревьев, каждое из которых представляет файл или инструкцию исходного кода. Дерево строится согласно контекстно-свободной грамматике, которая определяет синтаксис языка. Анализировать подобное дерево намного проще, чем анализировать код с помощью регулярных выражений. Также это позволяет построить различные семантические модели.

Семантический анализ позволяет производить различные проверки исходного кода, его преобразования. Для проведения данного вида анализа обычно строят дополнительные модели, называемые графом потока управления и графом потока данных.

Граф потока управления является графом, в котором инструкции соединены друг с другом во всех возможных последовательностях их выполнения, например, для условного оператора могут быть переходы вперед с точки оператора на его различные ветви, а в циклах возможны переходы на предыдущие инструкции.

Граф потока данных является глобальным графом передачи данных из переменных внутрь вызовов функций. Благодаря данному графу можно изучить какие функции могли быть вызваны из анализируемой, с какими аргументами.

Одним из вариантов поиска уязвимостей является поиск обнаруженных раннее сигнатур. Системы, использующие данный вид анализа, используются в антивирусах. к проблемам данных систем можно отнести то, что они не анализируют код программного обеспечения и работают на основе ранее обнаруженной информации.

Универсальным видом анализа на уязвимости является taint анализ [Boxler, Walcott, 2016]. Он представляет собой анализ актуального исходного кода на наличие проблем безопасности.

Рассмотрим концепцию taint анализа. Уязвимостью является попадание непроверенных данных в какую-либо критическую функцию. Например, если данные, прочитанные из файла, не были достаточно отфильтрованы и попали на запись в базу данных, возникает потенциальная уязвимость в системе.

Для того, чтобы автоматизировано определять подобные уязвимости, необходимо находить данные, которые нужно фильтровать. Подобные данные возникают при чтении из внешних источников, например базы данных или при получении данных пользователя из http запроса. На языках программирования получение подобных данных выглядит как вызов функции, присвоение данных из вызова обозначает сохранение неотфильтрованных, грязных данных в переменную. Данная переменная должна быть профильтрована или обработана санитизаторами (очистителями данных от потенциальных загрязнений). в случае, если грязные данные из этой переменной дойдут до критической функции, например, операции записи в базу данных, потенциально произвольные данные могут быть переданы пользователем на запись в систему. в качестве наиболее просто обнаруживаемых уязвимостей с помощью данного вида анализа стоит выделить SQL и XSS инъекции.

Цель данного анализа заключается в отслеживание всех возможных путей от пятна до стока (критических функций).

В качестве статических анализаторов уязвимостей исходного кода автор данного доклада приводит следующие системы: PVS-studio, AppChecker и ircmaxell/php-security-scanner.

Проблемой статического анализа является невозможность полноценно проанализировать актуальные данные, попадающие в систему.

Для решения данной проблемы существуют системы динамического анализа кода, которые внедряются в код программы или в ее интерпретатор. Для быстрого воспроизведения возможных

сценариев использования информационной системы, применяют генераторы входных данных.

Заключение

Автором данной работы было осуществлено внедрение рассмотренных систем поиска уязвимостей на предприятие.

По результатам внедрения были выявлены сильные и слабые стороны данных систем с точки зрения возможности снижения рисков и размера ущерба предприятию от возникающих угроз в сети Интернет.

Плюсы данных систем:

1. Благодаря анализаторам кода на уязвимости появляется возможность предотвращать большой спектр угроз бизнесу в современных условиях.
2. Упрощение анализа системы на проникновение, так как анализаторы определяют проблемные места кода, по которым проще производить тестирование.
3. Исключается возможность внедрения кода, содержащего уязвимости, так как система работает непрерывно и при обнаружении данной проблемы может сигнализировать о наличии опасности.
4. Минусы данных систем:
5. Большое количество ложных срабатываний и сложность автоматизированного развертывания системы с последующим анализом результатов ее работы.
6. В случае, если анализируемая система достаточно большая, изучение результатов анализа затруднено огромным количеством путей распространения пятен от их появления в коде до стоков.
7. Данный вид анализа подразумевает анализ кода в глубину вызовов и обычно занимает продолжительное время.
8. Рассмотренные системы подходят для дополнительной защиты предприятий при невнимательном подходе к безопасности со стороны разработчиков и от действий злоумышленников.
9. Анализаторы кода позволяют предотвратить возможные ошибки в коде и увеличить уровень защищенностиы во время разработки программного обеспечения предприятия.

Список литературы

1. Альфред В. Ахо, Моника С. Лам, Рави Сети, Джеффри Д. Ульман «Компиляторы: принципы, технологии и инструменты». Вильямс, 2016.
2. OWASP Vulnerabilities // Официальный сайт Open Web Application Security Project. URL: https://owasp.org/www-community/vulnerabilities/ (Дата обращения: 07.03.2020)
3. Static Taint Analysis Tools to Detect Information Flows // Int'l Conf. Software Eng. Research and Practice | SERP'18 / Dan Boxler, Kristen R. Walcott

ПОЗДНЯКОВА ТАТЬЯНА СЕРГЕЕВНА
студентка факультета анализа рисков и экономической
безопасности имени профессора В. К. Сенчагова
Финансовый университет при Правительстве РФ, г. Москва
E-mail: tatyana_pozdnyakova98@mail.ru

РАЗРАБОТКА ИНДИКАТОРОВ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ ПИЩЕВОЙ ПРОМЫШЛЕННОСТИ

POZDNYAKOVA TATYANA SERGEEVNA
student, Professor Senchagov Faculty of Risk Analysis and Economic Security
Financial University under the Government of the Russian Federation, Moscow

DEVELOPMENT OF ECONOMIC SAFETY INDICATORS FOR THE FOOD INDUSTRY

Аннотация: В настоящее время проблема экономической безопасности занимает центральное место. Экономическая безопасность делится на 3 уровня: экономическая безопасность государства, региональная экономическая безопасность и экономическая безопасность хозяйствующего субъекта. Ввиду нестабильности окружающей среды, экономических и социальных проблем хозяйствующие субъекты вынуждены адаптироваться к этим условиям. Именно разработка индикаторов позволит разработать подход, способный выявить уязвимые места предприятия и выработать меры, способствующие устранению проблем. в работе представлен механизм обеспечения экономической безопасности на ООО «КМК» на основе разработки индикаторов. Автор рассчитал индикаторы и выявил наиболее уязвимую составляющую ЭБ для ООО «КМК».

Abstract: Now the problem of economic security occupies a central place. Economic security is divided into 3 levels such as government economic security, regional economic security and economic security of the economic entity. Due to the instability of the environment, economic and social problems, economic entities are forced to adapt to these conditions. The development of indicators can allow us to develop an approach that can identify vulnerabilities of the enterprise and develop measures that help to eliminate problems. The author presents a way for ensuring economic security at KMC LLC based on the development of indicators. The author calculated the indicators and identified the most vulnerable component of the economic security for LLC KMK.

Ключевые слова: экономическая безопасность, индикаторы, кадровая безопасность, пищевая промышленность, технико-технологическая безопасность, стабильность.

Keywords: economic security, indicators, personnel security, food industry, technical and technological security, stability.

В настоящее время недостаточно внимания уделяется защите экономических интересов предприятия. Хотя в условиях развития рыночной экономики, роста частного предпринимательства и конкуренции важной задачей хозяйствующего субъекта является обеспечение его экономической безопасности.

Экономическая безопасность – это состояние субъекта, при котором обеспечивается его способность к выживанию и развитию в условиях внешних и внутренних угроз.

Исходя из функциональных целей и имеющихся у предприятия ресурсов можно выделить семь функциональных составляющих экономической безопасности: финансовая, кадровая, технико-технологическая, экологическая, информационная, силовая и правовая. Данные составляю-

щие могут изменяться в зависимости от специфики деятельности предприятия.

Но для определения уровня экономической безопасности необходимо выделить комплекс критериев, пороговые значения которых помогут выявить несовершенства в составляющих экономической безопасности. Ведь предприятие обладает ограниченными ресурсами, поэтому не способно устранить несовершенства в экономической безопасности во всех составляющих одновременно.

Индикаторы – это показатели, имеющие пороговые значения, при превышении которых возникает угроза хозяйственной деятельности предприятия.

Для оценки уровня безопасности на предприятии используются как качественные, так и количественные методы. Качественные методы прежде всего связаны с мнением экспертов, но они имеют недостаток – субъективная оценка. Поэтому необходимо разработать спектр критериев, которые дают объективную оценку уровня экономической безопасности. При комплексной оценке экономической безопасности используют комбинированные подходы, применяя различные формы, такие как вопросный, анкетный, табличный, матричный, графический, портфельный, математический.

Объектом нашего исследования является ООО «КМК» - это предприятие, основным видом деятельности которого является производство молока и молочной продукции. Миссия ООО «КМК» состоит в обеспечении населения Ставропольского края и других регионов качественной натуральной молочной продукцией, в которой сохранены все полезные свойства и витамины.

Главное преимущество ООО «КМК» заключается в том, что оно расположено вблизи от фермерских хозяйств, которые непосредственно поставляют молоко для производства. Технологи постоянно следят за состоянием животных. в отличие от других хозяйств, ООО «КМК» не кормит коров антибиотиками и вредными добавками. Благодаря природному изобилию Ставропольского края, летом коровы получают возможность пастись на лучших пастбищах, получая всё от природы. Ежедневный контроль над производством молочной продукции осуществляется на всех этапах технологической цепочки – от обработки земли, кормопроизводства и кормления до получения, хранения и сдачи молока на молочный комбинат. Предприятие оснащено современной лабораторией, которая затем отслеживает качество изготавливаемой продукции. Что касается трудовых ресурсов, то предприятие состоит из 18 отделов, среди которых есть и отдел экономической безопасности, состоящий из 1 специалиста. Всего на предприятии работает 192 человека, среди которых 53% — это мужчины, а 47% - это женщины.

Прежде чем переходить к механизму обеспечения экономической безопасности, необходимо дать анализ составляющих экономической безопасности, а именно материальных и трудовых ресурсов предприятия. Так как предприятие обладает ограниченными финансовыми ресурсами, необходимо выбрать наиболее «значимую» для механизма обеспечения экономической безопасности составляющую и уже затем вырабатывать механизмы по минимизации угроз.

Нами были разработаны индикаторы экономической безопасности в отрасли пищевой промышленности и на основании них выявлена «значимая» составляющая. (Приложение 1)

В финансовой безопасности была выявлена большая зависимость от заёмных средств. Действительно, предприятие взяло кредит на сумму 600000000 рублей. в правовой, информационной, пожарной составляющих угроз не было выявлено. Работники соблюдают технику безопасности, ведётся контроль над её соблюдением. Информация, предоставленная покупателем истина и полна. Наличие ливневой канализации, локально-очистительных сооружений говорит о соблюдении экологической безопасности.

На предприятии разработана Программа производственного контроля – документ, в котором прописаны мероприятия по оценке качества продукции и ответственные лица. Безопасность продукции начинается с чёткой организации заготовки кормов, составлении правильного рациона. Соблюдение пищевой безопасности осуществляется согласно ХАССП и ТР ТС 021/2011.

Для анализа технико-технологической безопасности оценим показатель степени загрузки мощностей. в декабре этот показатель увеличился в 22 раза по сравнению с апрелем 2018 года!

В ходе анализа экономической безопасности была выявлена составляющая с наибольшим количеством угроз. Это кадровая. Были выявлены проблемные зоны, а именно:

Текучесть кадров. в 2018 году выбыло 9 человек, среди которых 6 ушли на пенсию.

Демотивация и неудовлетворённость условиями труда. Это говорит такой индикатор, как удовлетворённость заработной платой на 39%.

Низкая заработная плата у персонала производственного отдела. Дифференциация заработной платы составляет 68%.

Отсутствие персонала в производственной сфере.

Эти угрозы подрывают кадровую безопасность предприятия, тем самым нанося вред экономической безопасности ООО «КМК».

Были приняты меры по совершенствованию кадровой безопасности:

Увеличение заработной платы работникам производственного отдела в зависимости от стажа работы. Это будет прописываться в Положении ООО «КМК» об оплате труда. Исполнителем является главный бухгалтер.

Дополнительный набор персонала в производственный отдел. Исполнителем является специалист по работе с персоналом.

Выплата «ипотечных» процентов за счёт предприятия для молодых семей, что привлечёт молодых специалистов. Это прописывается в трудовом договоре. Исполнителем является генеральный директор.

Таким образом, безопасность материальных и трудовых ресурсов предприятия имеет важное значение для обеспечения экономической безопасности. и только безопасность всех составляющих может обеспечить высокий уровень экономической безопасности предприятия.

Список используемой литературы

1. Единые государственные стандарты по обеспечению экономической безопасности хозяйствующих субъектов Российской Федерации. / Под общ. ред. В. И. Авдийского, В. М. Безденежных и В. К. Сенчагова. -Спб.: Образовательный центр «СоветникЪ», 2013. -148с.
2. Кузнецова Е.И. Экономическая безопасность: учебник и практикум для вузов/ Е.И.Кузнецова. - М.:Издетельство Юрайт,2019.-294 с.
3. Экономическая безопасность России: Общий курс: учебник / под ред.В.К.Сенчагова. 3-е изд., перераб. и доп. 2009. С.738-740
4. Денисова О. К., Кобенко А. С. Показатели оценки уровня экономической безопасности предприятия// Вестник университета Туран, №4(80), 2018, С.186-190
5. Кротенко Т. Ю. Методические подходы к разработке индикаторов экономической безопасности организации// Вестник университета, №11, 2018, С.18-22
6. Официальный сайт ООО «КМК» [Электронный ресурс] URL: http://kazminmilk.ru (дата обращения: 15.05.2019)

Приложение

Индикаторы экономической безопасности на ООО «КМК»

Составляющая ЭБ	Индикаторы	Значения для ООО «КМК»	Контрольные периоды
Финансовая безопасность	Показатели платежеспособности		
	коэффициент абсолютной ликвидности	0,27057	2 раза в год – при составлении Бухгалтерского баланса, Отчёта о финансовых результатах
	коэффициент быстрой ликвидности	1,400465	
	коэффициент текущей ликвидности	2,755481	
	коэффициент манёвренности капитала	0,288343	
	коэффициент обеспеченности СОС	0,637087	
	Показатели финансовой устойчивости		
	плечо финансового рычага	4,043198	
	коэффициент автономии	0,198287	
	коэффициент финансовой устойчивости	0,967431	
	Показатели деловой активности		
	фондоотдача	0,077988	
	оборачиваемость активов	0,068441	
	оборачиваемость собственного капитала	0,345161	
	оборачиваемость дебиторской задолженности	1,859818	

	оборачиваемость кредиторской задолженности	2,308966	
	оборачиваемость запасов	2,030927	
	Показатели рентабельности		
	рентабельность продаж	0,055634	
	рентабельность активов	0,002488	
	рентабельность собственного капитала	0,012547	
Кадровая безопасность	Показатели состава и движения персонала		2 раза в год
	Коэффициент выбытия	0,125	
	Коэффициент приёма	0,444	
	Процент сотрудников с высшим образованием	32%	
	Средний стаж рабочих	3 года	
	Обеспеченность рабочей силой	60%	
	Показатели мотивации		
	степень удовлетворённости оплатой труда	39%	2 раза в год
	коэффициент дифференциации среднемесячной номинальной заработной платы	68%	
	удельный вес затрат на оплату труда в общих издержках предприятия	72%	
	Показатели условий труда		
	автоматизация труда	82%	1 раз в год
	уровень травматизма	5-10%	2 раза в полгода

	Личностные показатели		
	процент нарушений трудовой дисциплины от общего числа сотрудников	5-10%	1 раз в месяц
	вероятность сохранения коммерческой тайны	85%	1 раз в полгода
	Количество созданных за год новых рабочих мест	7	2 раза в год
Технико-технологическая безопасность	Показатель выбытия основных средств	0,03	2 раза в год
	Коэффициент обновления основных средств	0,9	
	Материалоёмкость	0,907	
	Фондоотдача	0,077988	
	Уровень брака	5-10%	ежемесячно
	Показатель износа основных средств	0,05	2 раза в год
	Уровень технологий и использование передовых технологий	82%	
	Фондовооружённость	0,81	
	Уровень загрузки производственных мощностей	73%	1 раз в месяц
Силовая безопасность	Коэффициент защищённости транспорта	-	Раз в полгода
	Коэффициент защищённости персонала и имущества	-	Проверка специального оборудования – раз в 3 месяца
	Доля нарушений техники безопасности	5-10%	1 раз в месяц
Правовая безопасность	Удельный вес судебных дел в общей численности договоров предприятия	Не выявлено	Раз в год
	Удельный вес уплаченных штрафных санкций в общей сумме обязательств		
	Коэффициент качества юридических услуг		

Информационная безопасность	Коэффициент полноты информации	87%	2 раза в год
	Коэффициент точности информации	85%	
	Коэффициент противоречивости информации	5-10%	
	Коэффициент защищённости информации	85%	
	Коэффициент оснащённости информацией потребителей	92%	
Экологическая безопасность	Степень экологичности продукции	83%	Ежедневно
	Степень экологичности производства	69%	Раз в месяц
Пищевая безопасность	Степень безопасности продукции	94%	Ежедневно
Сырьевая безопасность	Самообеспеченность ресурсами	90%	Два раза в месяц
	Выход готовой продукции	5,76%	Раз в месяц

Источник: разработано автором

РАДЗИХОВСКАЯ МАРИЯ АЛЕКСАНДРОВНА
студента факультета бизнеса и менеджмента
НИУ ВШЭ, г. Москва
Email: kkarma27@mail.ru

ГЕОГРАФИЯ КИБЕРПРЕСТУПНОСТИ: ПРЕСТУПЛЕНИЕ И НАКАЗАНИЕ

RADZIHOVSKAYA MARIA ALEKSANDROVNA,
student, faculty of business and management
National Research University «Higher School of Economics», Moscow

GEOGRAPHY OF CYBERCRIME: CRIME AND PUNISHMENT

Аннотация: Данная статья затрагивает вопрос распространения киберпреступности в различных странах мира, дает представление о появлении понятия киберпреступность, его общих тенденциях, проблемах и важнейших угрозах в условиях динамично развивающегося информационного пространства. Помимо этого, в статье представлен сравнительный анализ наиболее опасных стран мира с точки зрения нарушения целостности мирового киберпространства, а также описаны государственные методы защиты от кибератак в разных странах мира, даны краткие описания наиболее известных киберпреступлений в анализируемых странах.

Abstract: This article addresses the issue of the spread of cybercrime in various countries around the world and provides an overview of the emergence of the concept of cybercrime, its general trends, problems and major threats in a dynamic information space. Besides, the article presents a comparative analysis of the most dangerous countries of the world from the point of view of violation of integrity of the world cyberspace, describes state methods of protection against cyberattacks in different countries of the world, and gives brief descriptions of the most famous cybercrimes in the countries under analysis.

Ключевые слова: киберпространство, информационная безопасность бизнеса, киберпреступник, организованная преступность, география киберпреступлений, виртуальное пространство, кибератака

Keywords: cyberspace, business information security, cybercriminal, organized crime, geography of cybercrime, virtual space, cyberattack

Введение

В настоящее время глобальная информатизация затронула многие аспекты жизни современного человека: информационные технологии встречаются и, более того, используются везде – начиная от рутинных ежедневных дел, включающих в себя покупку продуктов, выбор одежды в интернет-магазинах, оплату коммунальных счетов и других процессов, заканчивая более широкомасштабными аспектами, связанными с политическими, экономическими и социальными вопросами мировых сообществ в целом. Нельзя не заметить, что данная тенденция повсеместного внедрения информационных технологий в современном обществе привела к появлению мирового киберпространства, которое в свою очередь не является географическим в общепринятом смысле этого слова, однако является международным. в процессе интеграции мирового информационного сообщества, все чаще государства разрабатывают методы активного противодействия информационным атакам, наносящим ущерб государству в целом. к ущербу можно отнести, на мой взгляд, любую важную информацию: конфиденциальные данные, связанные с микроэкономическими показателями, военными и космическими разработками и так далее. Можно предположить, что в данный момент любая информация, каким-то образом связанная с IT-технологиями, например, имеет риск быть незащищенной под натиском представителей киберпреступности.

Наряду с этим возникает вопрос – каким образом правительство может защитить общество

от кибератак и как осуществить этот процесс наиболее эффективно без лишних затрат? Одним из решений данного вопроса, по моему мнению, является формирование базы данных киберпреступлений посредством анализа действующей киберпреступности как в стране, так и в мире в целом. Однако логично задать следующий вопрос – что подразумевается под миром? Неужели лучшим программистам, разработчикам и специалистам по обеспечению информационной безопасности государства стоит досконально изучать всю историю киберпреступлений, модели угроз и принципы, схемы похищения информации каждой страны в мире? Отвечая на данный вопрос, можно говорить о том, что необходимо выделить самые активные, то есть предоставляющие наиболее высокий уровень киберопасности страны, где чаще всего наблюдались случаи похищения информации государственной важности, распространения вредоносных программ и других угроз киберпространства и рассмотреть активность киберпреступности каждой выделенной страны на нескольких реальных примерах, кейсах. Таким образом, вопрос, стоящий на повестке дня – это изучение географии киберпреступности на примере происходящих в реальности случаев похищения, заражения и замены важнейшей информации.

Основная часть

1. Киберпреступность как важнейшая угроза мировому информационному сообществу

1.1. Понятие киберпреступности

Прежде чем обращаться к анализу наиболее кибератиных стран мира и оценке их существующего положения, степени опасности для всего мирового сообщества, стоит разобраться с терминологической, базисной частью данного вопроса. Изучение основных понятий, таких как киберпреступность, и, следовательно, следующие за ней киберпространство, существенно прояснят дальнейшее ознакомление с проблемой анализа географии киберпреступности.

Как было указано ранее, в настоящее время глобализация информационных технологий и информатизация общества в целом предоставляет неограниченные возможности для оказания воздействия на личность. Нельзя не осознавать, что за видимыми преимуществами технологий скрывается масштабный недостаток информационной глобализации мира – появление новой формы преступности в сфере высоких технологий. Как отмечает Бондарь В.В., объектами защиты выступают не физические лица, а компьютеры, базы данных, сетевые носители, жесткие диски и другие IT-устройства. к киберпреступлению можно отнести любое неправомерное действие, совершаемое с помощью компьютерной сети. Преступление, совершенное в киберпространстве, — это противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ. Таким образом, понятие киберпреступности сопряжено с понятием виртуального пространства, или же киберпространства. Номоконов В. А. убеждает, что киберпространством можно охарактеризовать информационное пространство, в котором находятся данные о предметах, события, лицах, процессах, представленные в символьном виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого реального или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи.

1.2. Общие тенденции киберпреступности в наше время: источники киберугроз и основные проблемы

Разобравшись с определением киберпреступности, необходимо обратиться к рассмотрению глобальных тенденций кибератак в мировом сообществе: какие общие черты имеют киберпреступления в настоящее время, а также какие распространены источники киберугроз. Так, например, интеграция телекоммуникационных сетей, повсеместное использование Интернета, переход банковской сферы в иной формат – формат мобильного банкинга и многое другое, привели

к преступным посягательствам, которые имеют в целом общие черты. Во-первых, к ним относится интеллектуальный

характер преступной деятельности: это означает то, что преступник без должной подготовки и уровня образования, научных знаний, без специфических навыков и умений вряд ли сумеет совершить преступление, ему необходимо знать базовые ключи к программированию, шифрованию информации в киберпространстве. Во-вторых, преступник и объект нападения могут находиться вдалеке друг от друга, на разных континентах или на территории различных государств, так как для совершения преступного деяния в киберпространстве необходимо лишь подключение к локальной компьютерной сети, а не прямое личное взаимодействие. В-третьих, одной из черт киберпреступления является возможность совершать кибератаку на множестве устройств, а также возможность совмещать относительно слабые мобильные ресурсы многих компьютеров в одно мощное орудие совершения преступления. Помимо этого, к общим чертам кибератак относится возможная неосведомлённость потерпевших о том, что они подверглись преступному воздействию. Далее идет дистанционных характер преступных действий при отсутствии физического контакта – также особенность множества совершаемых кибератак. И, наконец, к отличительным чертам киберпреступлений я бы отнесла тот факт, что зачастую потерпевшие не могут обладать информацией о киберпреступниках в силу всех вышеперечисленных факторов: лица, совершившие преступление в виртуальном пространстве, точно знают, каким образом скрыть свое деяние, то есть зашифровать свое местонахождение, личные данные и другую важную информацию о себе, так как для большинства преступлений, совершаемых в виртуальном пространстве характерна повышенная скрытность совершения преступления, обеспечиваемая спецификой информационного пространства.

Кроме того, важно выделить основные источники киберугроз, зафиксированные в мировом киберпространстве. Источники киберугроз подразделяются на внешние и внутренние; в 2015 году компанией IBM было проведено исследование разновидностей кибератак всех стран мира, в исследовании учитывались данные о 2700 крупнейших компаниях и корпорациях мира, в следствие чего было установлено, что более 60% кибератак были проведены теми лицами, которые имели доступ к ознакомлению с инсайдерской информацией и системам определённой организации. к другим источникам можно отнести внешние вредоносные источники, случайные инциденты и вредоносные инсайдеры. Для подтверждения данной информации снова обратимся к изучению исследования IBM: в соответствии с данными о соотношении внутренних и внешних угроз, в 2016 году 55% процентов приходилось на внутренние, к ним относились случайные инциденты – 23,5%, вредоносные инсайдеры – 31,5%, а также внешние угрозы – 45%. к 2017 году уровень внутренних угроз вырос на 5% и составил 60%: 44,5% -вредоносные инсайдеры, и 15,5% на случайные инциденты, уровень же внешних угроз снизился на 5% и составил 40% соответственно. Исходя из вышесказанного, можно делать вывод о том, что крупным компаниям и организациям стоит усиливать внутреннюю систему безопасности, модернизировать проверку сотрудников, имеющих

доступ к инсайдерской информации и сфокусироваться более на внутренних киберугрозах, чем на внешних.

2. Формирование глобального киберпространства: наиболее опасные страны

2.1. География распространения кибератак: кто могущественнее и сильнее?

Ознакомившись с понятием киберпреступности, основными чертами всех совершаемых киберспреступлений, важнейшими источниками киберугроз, перейдем к основной задаче, описанной ранее: изучении географии киберпреступности на примере реальных кейсов. Классификация самых опасных стран будкт производиться с точки зрения общего количества кибератак, приходящихся на страну. По праву лидером среди всех стран, чьей сильной стороной является развитая киберпреступность, является США: 24,7% всех мировых киберпреступлений совершается именно там. Вполне логичным подтверждением лидирующего положения США среди наиболее опасных стран является ряд факторов. Во-первых, наиболее атакуемыми операционными системами

являются Windows, Android, Mac OS X, которые непосредственно были разработаны в Соединенных Штатах. Во-вторых, общее количество интернет-пользователей в США составляет 245 млн., уровень проникновения интернета в Северной Америке составляет 78,6% - 1 место в мире. Помимо этого, уровень лидирующее положение США достигается за счёт не прекращающего роста кибератак: крупнейшая телекоммуникационная японская компания NTT Group в своем годовом отчёте «Global Threat Intelligence Report 2016» показала, что 65% обнаруженных кибератак против клиентской базы производились с IP-адресов в Соединенных Штатах, причем прошлый анализ показал, что в 2013 году 49% нападений происходили из США, а в 2014 г. – уже 56%, то есть заметен стремительный рост кибератак. в 2016 году жертвами киберпреступников стали 143 млн человек, более половины взрослого населения страны. Относительно вопроса наказаний за хакерские атаки и неправомерных действий киберпреступников в США, важно отметить существование закона «О мошенничестве и злоупотреблении с использованием компьютеров» 1984 года, который предусматривает семь разных составов преступлений в сфере информационно-компьютерной информации. Однако особенностью правового регулирования кибепреступлний в США является то, что в соответствии с решением 2016 года Федерального апелляционного суда США, американское правительство и спецслужбы не имеют возможности направить запрос операторам связи и крупным компьютерным корпорациям, например, таким как Microsoft.

По данным Symantec, крупнейшей калифорнийской компании по разработке программного обеспечения в области информационной безопасности и защиты информации, второе место среди самых опасных стран в области киберпреступлений занимает Китай – около 9,6% всех мировых кибератак приходятся на эту страну. Подтверждением данного утверждения может являться тот факт, что именно Symantec уведомил в июне 2018 года мировое сообщество о крупнейшей кибератаке китайских хакеров группировки Thrip на объекты США и Юго-Восточной Азии. Целью данной кибератаки являлся шпионаж и перехват гражданской и военной информации. Преступники заразили компьютеры, используемые для управления спутниками: это дало им возможность менять орбитальную позицию устройств и вмешиваться в обмен данными. Помимо этого, другим случаем беспецедентного вмешательсва акеров в инфомационную базу государства является другая кибератака, произошедшая в марте 2014 года. Так, китайские хакеры организовали кибератаку на компьютерные сети правительства США и получили доступ к некоторым базам данных федеральных госслужащих. Атака проводилась для кражи персональных данных десятков тысяч человек, проходивших проверку с целью получения разрешения на работу с секретной информацией.

На третьем месте находится Бразилия – 5,84% всех киберпреступлений мира совершено именно в этой стране. Так, например, в мае 2017 года бразильская кибератака хакеров вывела из строя электронную судебную систему страны. Действия бразильских киберпреступников в большей степени направены на соотечественников, например, хакеры копируют номера банковских карт, тем самым снимая наличность с карты без ведома владельцев. Преступники осуществялют поиск данных разными способами, к примеру, с помощью скиммеров, устанавливаемых в банкоматах и платежных терминалах, а также клавиатурных шпионов. Другое направление запрещенной деятельности бразильских хакеров — это IT-ресурсы государственных учреждений и корпораций. в настоящему времени официально установлено, что от масштабных утечек информации пострадали базы данных правительства, Федеральной налоговой службы и других организаций. Например, в 2011 году две вредоносных носителя, управлемые бразильскими киберпреступниками, на сайте Министерства труда выложили на всеобщее обозрение личные данные и контакную информацию обо всех гражданах страны за шесть месяцев. Другим фактическим подтверждением активности бразильских киберпреступности является случай фишинговой атаки на государственный ресурс. Результатом атаки стало проведение незаконной вырубки лесов Амазонии и нелегальная добыча древесины на 11 миллионов долларов США.

На четвертом месте по количеству кибератак находится Индия – примерно 5,11% от общего зафиксированного количества киберпреступлений прходятся на эту страну. Например, жертвами атак стали в 2017 году 186 млн человек. Фактическим подтверждением нахождения Индии в пятерке стран-лидеров в киберпреступлениях, является случай, произошедший с компаний Hitachi

Payment Services в 2016 году. Компьютерная сеть была взломана индийскими хакерами, в результате кибератаки системы компании были заражены вредоносным программым обеспечением, что стало причиной утечки данных, затронувшей примерно 3,25 млн банковских карт. Из-за утечки данных пострадали карты индийской системы RuPay, а также Visa и MasterCard, выпущенные 19 крупными банками страны. Помимо всего прочего, в перечень стран входит Германия - 3, 35%, Россия – 3,07%, Великобритания – 2,06%, Франция – 2%, Япония – 2,25%, Вьетнам – 2,13%.

Кроме того, на мой взгляд, проводить анализ георгафии киберпреступлений можно не с точки зрения общего количества всех зафиксированных киберпреступлений в виртуальной сети по миру, а с точки зрения сетевых и локальных кибератак отдельно. Обратимся снова к достоверной информации из годового отчёта «Global Threat Intelligence Report 2016»3. NTT Group обнаружила атаки в общей сложности из 217 различных стран в течение 2015 г. в том числе, на каждую из 197 стран по отдельности приходится менее одного процента от кибератак. Рассматривая общий объем интернет-трафика и блокирующую активность4 (отчет Kaspersky Security Bulletin), можно сделать вывод о том что по итогам 2016 г., крупнейшими источниками заблокированного трафика стали страны Европы и Востока, а в Азиатско-Тихоокеанском регионе список возглавила Австралия.

Иначе выглядит география локальных кибератак. в одной из глав отчета Kaspersky Security Network предоставлена информация о частоте локальных кибератаках в 2016 году. в среднем в группе стран из top-10 вредоносный объект хотя бы раз был выявлен на компьютере (на жестком диске или на съемном носителе, который присоединен к жесткому диску или самому компьютеру) – у 67,7% пользователей, тогда как в 2015 г. – у 58,7%. Первое место в этом рейтинге третий год подряд занимает Вьетнам (70,83%). Монголия и Бангладеш в 2016 году поменялись местами: Монголия (66,30%) опустилась со второго на четвертое место, а Бангладеш (69,55%) поднялся с четвертого на второе. Россия (68,81%), не вошедшая в top-10 в прошлом году, в 2016 году оказалась на третьем месте.

2.2. Государственные методы защиты от кибератак в разных странах мира

Вполне закономерно предположить, что изучение географии киберпреступности должно иметь особый уровень результативности для изменения вектора противодействия всего международного сообщества против такой разновидности виртуальной преступности. Более того, многие государтсва уже сейчас признали особую важность объединения сил с другими ведущими странами против киберпреступности, ведь, как известно, рост киберпреступности растет с увеличением числа пользователей Интернета, и на данный момент темпы роста преступности в Интернете и в любых других компьютерных сетях являются самыми быстрыми на планете. Основной целью международного сотрудничества является совершение международного законодательства в области обеспечения информационной безопасности, а также создание в первую очередь гибких инструментов по предотвращению атак в киберпространстве; также крайне важно единство действий государств в лице проавоохранительных органов при расследовании преступлений подобного типа, ведь как было указано ранее, зачастую объект, подвергшийся кибератаке, не может определить месторасположение преступника в силу дистанционного характера нанесения ущерба. Примером договороного-правового сотрудничества ведущих стран мира является появление универсальных международных договоров заданной тематики, например, Конвенция ООН против транснациональной организованной преступности, Европейская конвенция о киберпреступлением, принятая в Будапеште в 2001 году. Также существует определлная разновидность региональных международных соглашений – к примеру, Соглашение СНГ о борьбе с преступлениями в сфере компьютерной информации. в целом можно заключить, что транснациональный характер киберпреступности требует определенных мер по защите информации как внутри страны, так и в мире в целом, к которым я бы отнесла в первую очередь постоянное сотрудничество ведущих стран мира. к примеру, если на основании статистических данных было выявлено, что самые опасные страны по количеству кибератак – это США Бразилия, Индия и Китай, то именно специалистам из этих стран следует сотрудничать на регулярной основе, возможно, выстраивать некие

международно-правовые отношения путем заключения договоров, связанных с обеспечением информационной безопасности.

Заключение

Несмотря на вышеперечисленные факторы, которые свидетельствуют о том, что мировое сообщество максимально сосредоточило свое внимание на создании новейших методов по борьбе с киберпреступностью, создании конвенций и договоров, правовое, государственное и социальное регулирование не может в полной мере противостоять нахлынувшему количеству киберпреступлений на различных информационных платформах. Подводя итоги, необходимо отметить, что становление и развитие информационных технологий открыло перед людьми не только обширные возможности, но и новые виды информационных угроз. Как уже было отражено в данном анализе, на сегодняшний день страны столкнулись с крайней необходимостью обобщения мировой практики для предотвращения возрастающего роста кибер-преступлений. Основываясь на сегодняшней тенденции, сложно строить оптимистический прогноз по улучшению ситуации в сфере защиты данных, однако стоит отметить, что все же можно выделить некоторые положительные аспекты в данной области, а именно улучшения систем безопасности, привлечения на защиту данных бывших хакеров, а также в целом увеличение штаба по информационной безопасности. Данные изменения позволяют нам надеяться на становление в будущем глобальной сети, которая предоставит нам не только огромные возможности, но и нашу безопасность.

Список Литературы

1. Бондарь Владимир Владимирович Киберпреступность – современное состояние и пути борьбы // Юридические записки. 2013. №2
2. Валько Д.В. Киберпреступность в России и мире: сопоставительная оценка // Управление в современных системах. 2016. №3 (10)
3. Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями. [Электронный ресурс]
4. Информационная безопасность // Kaspersky Security Lab. [Электронный ресурс] - URL: http://www.kaspersky.ru/images/Bezopasnost_Screen.pdf
5. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. №24.
6. Global Threat Intelligence Report 2016 // NTT Group. [Электронный ресурс] - URL: https://www.solutionary.com/_assets/pdf/research/2016-gtir.pdf
7. Kaspersky Security Bulletin 2015// Kaspersky Security Lab. [Электронный ресурс] - URL:https://securelist.ru/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_RUS.pdf
8. Kaspersky Security Bulletin 2015// Kaspersky Security Lab. [Электронный ресурс] - URL:https://securelist.ru/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_RUS.pdf

РЕДЬКИН ИГОРЬ АЛЕКСЕЕВИЧ
студент факультета бизнеса и менеджмента
НИУ ВШЭ, г. Москва
E-mail: igorred99@mail.ru

ОТЕЧЕСТВЕННАЯ ПРАКТИКА ЗАЩИТЫ БИЗНЕСА ОТ РЕЙДЕРСКИХ ЗАХВАТОВ

REDKIN IGOR ALEKSEEVICH
student, faculty of business and management
National Research University «Higher School of Economics», Moscow

Аннотация: В данной статье автор рассматривает проблему защиты бизнеса от рейдерских захватов в контексте Российской Федерации. Целю работы является рассмотрение отечественной практики защиты бизнеса от рейдерских захватов. Вопрос, который автор поднимает в своем исследовании: Какие механизмы защиты от захватов и поглощений являются наиболее действенными на территории Российской Федерации? в качестве методологии получения данных, автор использовал научные труды по теме исследования, нормативно-правовые акты Российской федерации, сведения сайтов компании о текущих слияния-поглощениях, а также табличные и графические методы финансового анализа, горизонтальный и факторный анализы. Результатами исследования являются выявленные механизмы защиты от захватов и поглощений в современной России, основанные на изученной практике рейдерских захватов на территории Российской Федерации.

Abstract: In this article, the author considers the problem of protecting businesses from raider attacks in the context of the Russian Federation. The aim of the work is to review domestic practice of protecting a business from raider attacks. The question that the author raises in his study: What are the most effective defense mechanisms against seizures and acquisitions in the Russian Federation? As a methodology for obtaining data, the author used scientific papers on the topic of research, regulatory legal acts of the Russian Federation, information on the company's websites on current mergers and acquisitions, as well as tabular and graphical methods of financial analysis, horizontal and factor analysis. The results of the study are the identified mechanisms of protection against seizures and acquisitions in modern Russia, based on the studied practice of raider seizures in the Russian Federation.

Ключевые слова: Рейдерство, Рейдерский захват, Бизнес

Key words: Raiding, Raider seizure, Business

Введение

Одним из актуальных вопросов современной экономики является изучение рейдерских захватов компании, что обусловлено глобализацией экономического пространства и, как следствие, увеличением количества угроз в виде волатильности финансовых рынков, существенных колебаний цен и так далее.На сегодняшний день, реорганизация компаний является допустимым направлением в управлении компании, с целью привлечения в свой капитал новых ресурсов.

Целью данной работы является рассмотрение отечественной практики защиты бизнеса от рейдерских захватов.

Задачи:

- рассмотреть понятие рейдерских захватов их виды,
- проанализировать практику рейдерских захватов в России,
- выявить механизмы защиты от захватов и поглощений в современной России.

Бизнес играет важную роль в развитии экономики любой страны, от того на сколько комфортными будут условия развития бизнеса, зависит будущее различных сфер экономики и отраслей.

Методологической основой данного исследования являются табличные и графические методы финансового анализа, горизонтальный и факторный анализ.

Нормативно-правовой базой исследования являются нормативные и правовые акты Российской Федерации, органов региональной власти, регламентирующие деятельность финансовой сферы.

Теоретическую базу исследования составляют научные труды по теме исследования.

Эмпирическую базу исследования составляют данные, характеризующие экономическое состояние организаций при реализации стратегии слияния/поглощения, компьютерная и электронная информация, сведения сайтов компаний и пр.

Понятия рейдерских захватов их виды

Острыми проблемами для осуществления деятельности компаний в настоящее время стала реструктуризация компаний, которая охватывает несколько эффективно работающих организаций во многих отраслях экономики, а также коррупция.

Способность компании противостоять негативным воздействиям и угрозам зависит напрямую от её финансового состояния и финансовой устойчивости, так как для реализации каких-либо мероприятий требуются финансовые ресурсы.

Рейдерский захват — это процесс поглощения предприятия обманным методом, против воли его собственника, в результате чего захватчики приобретают контроль над активами предприятия и продают их. Рейдерство все время изобретает новые способы захвата, становится все более изощрёнными и его сложнее опознать и выделить как противозаконное действие. [3, с.89]

В России рейдерство принято делить на три категории: «белое», «серое» и «черное». Рассмотрим их.

На рисунке 1 представлены типы рейдерства.

Рисунок 1 – Типы рейдерских захватов (Автор: Редькин И.А.)

- **«Белое» рейдерство** - реализовывается в пределах закона. Основной метод – корпоративный шантаж. Для этого создаются помехи нормальной работы при помощи миноритарного пакета акций с расчетом на то, что руководство предприятия в целях избавления от шантажа выкупит данный пакет по завышенной цене. Обычно такой рейдерский захват компании происходит из-за финансовых трудностей и малоэффективного корпоративного управления. [2, с.78]
- **«Серое» рейдерство** - деятельность захватчиков с нарушением гражданских правовых норм. На первый взгляд такое действие выглядит законным. Но при анализе применяемых методов становится понятно, что эта схема - мошенничество. Происходит подделка документов и подкуп должностных лиц. Этот способ можно использовать на любых предприятиях.
- **«Черное» рейдерство** – это самый жесткий способ захвата предприятий. Рейдерский захват УК РФ связывает с нарушением норм уголовного законодательства. Люди, которые действуют таким способом, используют насильственные методы захвата власти: шантаж, силовой вход на предприятие, подкуп, подделку реестра акционеров и т. д. Обычно такой вид рейдерства

применяется к непубличным предприятиям, хотя применим к любым. [6, с.65]

Отметим, что год от года рейдерский захват постоянно совершенствуется в своей схеме, видоизменяется, становится еще более завуалированным и по своим действиям практически полностью законным.

Практика рейдерских захватов в России

В течение последнего десятилетия 20-го века прослеживалась как за рубежом, так и в Российской Федерации, тенденция роста сделок по слияниям и поглощениям компаний, а также тенденция рейдерских захватов.

Процесс слияний и поглощений в России имеет ярко выраженную специфику. к российским особенностям относятся формы и этапы процессов поглощений, методика оценки стоимости, характер ведения переговоров при заключении сделок, мотивы компаний-инициаторов.

Преобладающий в мировой практике мотив получения синергетического эффекта не характерен для российских компаний. Большое количество недружественных поглощений и захватов породило специфические меры корпоративной защиты – превентивные и тактические. [3, с.45]

Организаторами поглощения или захвата бизнеса обычно являются:

- традиционные заказчики;
- специализированные рейдерские ОПГ;
- профессиональные агрессивные компании-рейдеры, выгодно реализующие коррупционный административный ресурс.

В современной России началом корпоративного рейдерства считается приватизация, когда через процедуры банкротства предприятия со стоимостью активов в миллиарды долларов были куплены за миллионы (ЗИЛ — 4 миллиона долларов, Уралмаш — 3,72 миллиона).

В результате реформ, проводимых Правительством России, открылось свободное и частное предпринимательство.

Размах рейдерства возрос в начале XXI века и доминирует среди поглощений: в 2002 году в России состоялось 1870 поглощений, из них три четверти (76 %) недружественных. с 2004 по 2007 год сумма недружественных сделок возросла более чем в четыре раза. Только за 2008 год МВД зарегистрировало более 3000 обращений о рейдерских захватах.

В России существует два основных метода, которые используют в рейдерских атаках:

1. коррупционные (наиболее популярный метод, примитивный и простой захват бизнеса);
2. долговые. [6, с.45]

Долговой метод бывает трех разновидностей с использованием:

- залога (схему реализуют банки-кредиторы, обладающие правом на имущество, переданное под залог);
- кредиторской задолженности (на основе информации о финансовом состоянии компании, пределах ее финансовой устойчивости);
- долга перед бюджетом (механизм принуждения государства в частных интересах).

Чаще всего к захвату рейдеры привлекают (в основном за счет коррумпированных связей) следующие государственные структуры:

- правоохранительные органы – для осуществления давления на действующее руководство предприятия с целью понуждения его к заключению сделок в пользу захватчиков;
- судебные органы – для легализации результатов своей деятельности, привлечения к ответственности руководства предприятия;
- регистрационные органы – для закрепления своих прав предприятие и его на активы, а также прав на осуществление руководства захваченной организацией. [2, с.87]

Таким образом, рейдерские захваты в России имеют ярко выраженную специфику и не всегда захваты бывают дружественными.

Механизмы защиты от захватов и поглощений в современной России

Проблемы при борьбе с рейдерством заключаются не в нормативных пробелах, а в высокой степени коррупции.

Рассмотрим некоторые механизмы защиты от рейдерских захватов в России.

1. Структурирование бизнеса

Такая защита бизнеса от рейдерства как структурирование означает воплощение известного изречения о том, что не стоит держать активы компании в одном месте. Это сокращает риски за счет разделения направлений деятельности фирмы. Можно также:

разделить бизнес на несколько компаний, распределить между ними ценные активы;

сделать одни компании более закрытыми для внешнего вторжения;

перевести имущество на ИП, аффилированное с конечным бенефициаром бизнеса. [7, с.63]

2. Защита акций

Акции или доли в уставном капитале нуждаются в защите. Чтобы предупредить захват, необходим усиленный контроль над реестром акционеров. Размер и характер бизнеса, вид угрозы определяет способ контроля:

- крупным компаниям, рассчитывающим получать внешние инвестиции, лучше передать реестр крупному регистратору с безупречной репутацией и максимально формализованной работой;
- мелким фирмам лучше самостоятельно вести реестр.

3. Защита активов

Целью рейдеров является не фирма, а ее имущество. Поэтому защита от рейдерского захвата заключается в принятии первоочередных мер по созданию препятствий к отчуждению имущества. Оптимальные средства - залог, ипотека, с помощью которых компания получает дополнительные финансовые потоки. Главное, вовремя отдавать долг, чтобы банк не реализовал имущество. Рекомендуется обменять активы залогом в пользу подконтрольных фирм, лиц.

Что можно сделать предпринимателю в случаях преднамеренного захвата:

- Устранить недостатки в оформлении документов,
- Снижать привлекательность активов для рейдера,
- Передать реестр акций профессиональному реестродержателю,
- Правильно оформлять все сделки,
- Оптимизировать кредиторскую задолженность. [7,с.65]

Система реализации стратегии слияния и поглощения каждого предприятия индивидуальна. Ее эффективность зависит от имеющейся в государстве законодательной базы, достаточности материальных и финансовых ресурсов, знаний и практического опыта сотрудников службы безопасности.

Не только коммерческие компании могут быть жертвами рейдеров, но и муниципальная собственность.

Особенное развитие муниципальное рейдерство получило в Москве (а точнее в центре Москвы), поскольку цены на землю, а уж тем более арендные платежи за здания довольно высокие. Целью захвата является либо земля, либо здание, в котором расположено предприятие. в данном случае любые компании могут подвергаться рейдерским нападениям, если они расположены в престижном районе

Примерами данного вида рейдерства могут служить такие последние события, как захват Дома актёра в конце 2007 г., захват Дома скульптора в январе 2008 г., а также захват Планетария в конце марта 2008 г. Можно заметить, что схема захвата у всего перечисленного одна и та же.

Эффективное управление бизнесом на основе применения стратегии слияния/поглощения с последующим применением механизмов их реализации, позволяет оптимизировать интегральную стоимость конечного продукта.

На сегодняшний день ежегодно происходит успешных рейдерских захватов в России около 70 тыс. Чаще всего это происходит методом подделки документов, мошенничестве, а также из-за

коррумпированной структуры. [6, с.56]

Таким образом, оптимизация и совершенствования взаимодействия всех бизнес-структур при сохранении позиций компании в экономике, включая контроль над стратегически важными производственными процессами в сочетании с поддержкой предпринимательских инициатив, станет важным фактором развития цивилизованных рыночных отношений, укрепления отечественной экономики и политической стабильности российского общества.

Заключение

В рамках данной работы была рассмотрена актуальная проблема, касающаяся отечественной практики защиты бизнеса от рейдерских захватов.

Важным событием для развития рейдерства, послужил рынок акций.

Роль бизнеса в экономике страны увеличивается с каждым годом, становление поглощений и слияний в России – это скорее выход из кризиса некоторых компаний, которые стремятся хоть как-то выжить в непростых экономических условиях.

Выводы:

В качестве одной из основных задач российской экономики выступает ее структурная трансформация и реформирование.

Как показывает практика, все рейдерские захваты происходят на высоком уровне, малейшее отклонение от схемы может привести к негативным последствиям.

На сегодняшний день ежегодно происходит успешных рейдерских захватов в России около 70 тыс. Чаще всего это происходит методом подделки документов, мошенничестве, а также из-за коррумпированной структуры.

Не только коммерческие компании могут быть жертвами рейдеров, но и муниципальная собственность.

Бизнес играет огромную роль в экономике государства и очень чутко реагирует на все изменения, происходящие как на внутреннем рынке, так и на внешнем. Несмотря на то, что причины банкротства и несостоятельности бизнеса могут быть внешними и внутренними, необходимо вовремя принимать соответствующие меры для поддержания бизнеса.

От принятых мер со стороны государства и предотвращения банкротства предприятий зависит стабильность экономики страны. Предприниматели должны предельно ориентироваться на использование существующих механизмов, носящих объективный характер.

Список используемой литературы

1. Федеральный экономической закон от 05 августа 2001 г. №118-ФЗ «О внесении изменений и дополнений в главу 22 части второй Налогового кодекса Российской Федерации» // Собрание законодательства РФ от 07 августа 2000 г., №32, Ст. 3340.
2. Свиридов О.Ю. Финансовый менеджмент: учебное пособие / О.Ю. Свиридов, Е.В. Туманова. – М.: Март, 2016.
3. Саркисянц А. Слияния, банкротства и фондовый рынок // Рынок ценных бумаг. - 2010 - №3, с. 15-16.
4. Смирнов И. о некоторых аспектах рынка слияний и поглощений. // Управление компанией. -2012, № 3. с. 50-51
5. Тарасова Т.Ф. Управление затратами на предприятии: учебное пособие. – Белгород: Кооперативное образование, 2015. – 130 с.
6. Федорова Е.С. Оценка стоимости публичных компаний в процессе слияния на российском рынке // Финансовый менеджмент. 2006. № 6. С. 46 – 55.
7. Электронный ресурс: Российская Федерация. Законы. // Консультант Плюс. – URL: http:// www.consultant.ru // Основные методы экономического анализа.цц

САРАЧ ТАТЬЯНА СЕРГЕЕВНА
студентка факультета права
НИУ ВШЭ, г. Москва
E-mail: tssarach@edu.hse.ru

ОБЗОР ДОКУМЕНТОВ ООН О ПРОТИВОДЕЙСТВИИ КОРРУПЦИИ

SARACH TATYANA SERGEYEVNA
student, faculty of law
National Research University «Higher School of Economics», Moscow

UNITED NATIONS CONVENTION AGAINST CORRUPTION DOCUMENT REVIEW

Аннотация: В данной статье представлены представлен анализ документов ООН, направленные на борьбу с коррупцией, а именно Декларация Организации Объединённых Наций о борьбе с коррупцией и взяточничеством в международных коммерческих операциях, Конвенция Организации Объединённых Наций против транснациональной организованной преступности, Конвенция Организации Объединенных Наций против коррупции. Также рассмотрена имплементации норм этих документов в российское право.

Abstract: This article presents an analysis of UN documents aimed at combating corruption, namely the United Nations Declaration on the fight against corruption and bribery in international commercial operations, the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption. The implementation of the norms of these documents in Russian law is also considered

Ключевые слова: коррупция, документы ООН против коррупции, имплементация.

Keywords: corruption, UN documents against corruption, implementation.

Государственная власть осуществляет свои функции через специальные исполнительные, законодательные и судебные органы. Доверие граждан власти напрямую зависит от правомерного исполнения своих полномочий данными органами. Однако в современном мире всё чаще основной проблемой становится использование коррупции исполнительной и судебной власти, а также гражданами Российской Федерации.

Коррупция – это обыденное действие в российской реальности, и зачастую люди приумножают её, не задумываясь о том, что это незаконно. Например, когда благодарят врачей, или, когда ученики дарят подарки своим учителям. Для многих российских граждан в этом нет ничего противоправного, что распространяет влияние коррупции.

Однако данная проблема не является только российской. Коррупция существует и в других странах, что выносит её на межгосударственный уровень. Более того мировое сообщество осознало, что с этим надо бороться и вынесла это в ряд документов, обзор которых и будет представлен в данном эссе.

Прежде всего необходимо определиться с самим понятием коррупции. в ФЗ «О коррупции» даётся следующее его определение «коррупция – это злоупотребление служебным положением, дача взятки, получение взятки, злоупотребление полномочиями, коммерческий подкуп либо иное незаконное использование физическим лицом своего должностного положения вопреки законным интересам общества и государства в целях получения выгоды в виде денег, ценностей, иного имущества или услуг имущественного характера, иных имущественных прав для себя или третьих лиц либо незаконное предоставление такой выгоды указанному лицу другими физическими

лицами, а также совершение всех этих деяний от имени или в интересах юридического лица». Однако данное понятие является слишком громоздким и скорее отражает форму осуществления коррупции в реальности. По-видимому, в федеральном законе это было сделано для более ясного понимания гражданами смыла коррупции.

Если проанализировать научные труды учёных по данному вопросу, то можно заметить, что у понятия коррупция огромное количество определений, но все они имеют один смысл: коррупция – это противоправное явление, которое характеризуется использованием должностных полномочий лицами, замещающие государственные должности, в корыстных целях для удовлетворения личных интересов. Представляется, что данный термин наиболее точно охватывает понятие коррупции, и далее речь будет идти в рамках данной трактовки. Такое понятие также встречается в международных правовых документах. Например, в справочном документе ООН о международной борьбе с коррупцией, в рабочем определении междисциплинарной группы по коррупции Совета Европы, а также в Руководстве секретариата ООН. в них подчеркивается незаконное использование служебного положения для собственной личной выгоды.

Коррупция обладает рядом отличительных признаков. Во-первых, она является сложным социально-правовым явлением. Это означает, что некоторая совокупность одинаковых правонарушений не будет являться коррупцией, так как последняя является более широким понятием и охватывает больше общественных отношений. Во-вторых, явление коррупции – системное, то есть единичная дача взятки недостаточна для определения общего понятия коррупции. В-третьих, сущностью коррупции является получение госслужащими каких-либо незаконных вознаграждений от третьих лиц для удовлетворения их потребностей. Именно это является главным мотивом и двигателем коррупции, иначе у работников в государственной власти не было бы мотива нарушать закон. В-четвертых, госслужащие получают «вознаграждения» за действия, входящие в их компетенцию. Значит, коррупция связана именно со служебными обязанностями, которые они применяют в незаконных целях.

Коррупцию можно подразделить на несколько видов. в зависимости от функций органов власти делят на:

1. коррупцию в органах исполнительной власти;
2. коррупцию в органах законодательной власти;
3. коррупцию в органах судебной власти.

Также по критерию инициатора коррупционных отношений выделяют

1. коррупцию «снизу» - это коррупция, инициатором которой являются граждане.
2. коррупцию «сверху» - это коррупция, инициатором которой является государственная власть.

По национальному составу субъектов коррупционных отношений различают

1. транснациональную (международную) коррупцию, которая охватывает межгосударственный уровень.
2. внутригосударственную коррупцию, которая существует на территории определенного государства.

Из этого следует, что коррупция – международная проблема. Действительно, она выходит далеко за рамками одного государства, что еще больше приумножает её негативное влияние. Например, глава государства, пришедший к власти при помощи коррупции, может подорвать авторитет страны на международном уровне, а также своими действия поставить под угрозу ее безопасность. Соответственно, все мировое сообщество должно объединиться против коррупции. Только эффективное международное сотрудничество способно противостоять этому злу.

В рамках международной борьбы против коррупции государства создают организации или же поднимают этот вопрос в уже существующих организациях. Так, одной из самых важной и влиятельной организацией является созданная в 1945 году Организация Объединённых Наций, главной целью которой является поддержание и укрепление мира и безопасности. в данную организацию входят почти все страны мира, что подчеркивает её приоритетное значение и эффективность принятых организацией документов и мер. Страны-участники ООН активно борются

против коррупции, принимая соответствующие нормативные правовые акты.

Основными международными документами в борьбе против коррупции является принятая резолюцией 51/191 Генеральной Ассамблеи от 16 декабря 1996 года «Декларация Организации Объединённых Наций о борьбе с коррупцией и взяточничеством в международных коммерческих операциях», «Конвенция Организации Объединённых Наций против транснациональной организованной преступности», которая была принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года, а также резолюцией 58/4 Генеральной Ассамблеи от 31 октября 2003 года была принята «Конвенция Организации Объединенных Наций против коррупции». Проведём более подробный разбор каждого их них.

Первым по хронологии является «Декларация ООН о борьбе с коррупцией и взяточничеством в международных коммерческих операциях». Как мы видим, в ней содержится всего лишь 12 статей, характер которых является общий и основополагающий. Данные статьи отражают лишь общие признаки и направления в борьбе с коррупцией. Это подтверждают общие формулировки, такие как «принимать эффективные и конкретные меры по борьбе со всеми формами коррупции», «установить эффективными и скоординированным образом уголовную ответственность», «разработать или применять стандарты и методы учёта», «изучить возможность признания незаконного обогащения государственных должностных лиц или избранных представителей преступлением», «сотрудничать и оказывать друг другу максимально возможную помощь».

Стоит также отметить, что в документе даже нет определения коррупции, что ещё раз подтверждает абстрактность статей и общий характер документа. Кроме этого в нём нет определённых инструкций и заявление о том, как именно нужно бороться с коррупций, а лишь общие формулировка, очерчивающие вектор направления для дальнейшего развития. Однако «Декларация Организации Объединённых Наций о борьбе с коррупцией и взяточничеством в международных коммерческих операциях» имеет и свои положительные стороны, главная из которых то, что впервые была поднята проблема коррупции на межнациональный уровень, хотя и нет точного понятия этого явления. Из этого следует, что проблема приобрела всеобщий характер, и её увидели многие страны, а что ещё важнее, они стремятся её устранить.

Следующим документом ООН, касающийся борьбы с коррупцией является «Конвенция Организации Объединённых Наций против транснациональной организованной преступности». Здесь уже больше статей – 40, каждая из которых является сложной, то есть содержит в себе несколько пунктов. Также можно отметить, что нормы стали конкретнее. а самое главное – в «Конвенции Организации Объединённых Наций против транснациональной организованной преступности» появились основные термины, определённые в статье 2. Более того есть цель и сфера применения; вступление в силу и ратификация; взаимосвязь с протоколами и осуществление Конвенции, что подчёркивает конкретный характер данного документа.

Данная Конвенция раскрывает общие принципы, принятые ранее в Декларации. в статье 7 указаны конкретные меры по борьбе с отмыванием денег. Среди них установление всеобъемлющего режима регулирования банков, надзор за денежными операциями и организациями, поощрения стремления к противодействию коррупции. в 8-9 статье устанавливается правило для все государств-участников данной Конвенции о том, что они криминализируют коррупцию во внутригосударственном праве, а также все сопутствующие необходимые меры. Последующие статьи устанавливают нормы процессуального права в сфере противодействия коррупции.

В 2003 году была принята «Конвенция Организации Объединенных Наций против коррупции», документ наиболее полно регулирующий коррупцию на международном уровне. Он является единственным в своем роде международно-правовым инструментом по вопросам борьбы с коррупцией и уникальным, потому что является основой разработки комплексных решений сложной проблемы. Её подписали 140 участников из 173. Конвенция содержит 8 глав и преамбулу, что подчеркивает её важность и особое положение среди предыдущих документов.

Основной акцент данной Конвенции делается на предупреждение коррупции. Так, в ней предусмотрена система мер по предупреждению коррупции, которая вынесена в отдельную главу (Глава 2). в ней особое внимание уделяется профилактики коррупции, которые направлены и на публичный, и на частный сектор. Глава 2 определяет политику и органы предупреждения коррупп-

ции; прием на работу, прохождение и продвижение по службе, правила отбора кандидатов в публичной сфере. Она также в качестве предупреждения коррупции выделяет кодексы поведения публичных должностных лиц, создание системы государственных закупок на основе объективных критериев, а также неподкупность и честность судебной власти. в частном секторе предлагается устанавливать правила взаимодействия, кодексы поведения и аудит.

Глава 3 посвящена криминализации и правоохранительной деятельности. в ней криминализируются определенные деяния, такие как подкуп национальных публичных должностных лиц, хищение, неправомерное использование имущества публичным должностным лицом, злоупотребление служебным положением, незаконное обогащение и т.д. Кроме этого глава 3 устанавливает общие положения, касающиеся всех правонарушений (сроки, подсудность, ответственность, уголовное преследование, защита информации и свидетелей). Здесь примечательна статья 36, где говорится об органах по борьбе с коррупцией, что будет иметь очевидное влияние на уровень коррупции.

Глава 4 тоже является немаловажной, так как содержит в себе положения международного сотрудничества и выдачи граждан. Если каким-либо государством не допускается выдача собственных граждан, то это государство обязано принять меры по обеспечению уголовного преследования. Кроме этого в неё включены двусторонние соглашения о взаимной правовой помощи, требования о назначении контактного органа по вопросам взаимной правовой помощи.

В глава 5 говорится о мерах по возвращению активов, что является фундаментальным принципом Конвенции. Также в ней есть положения о предупреждении и выявлении переводов доходов от преступлений. Более того содержится положение об изъятии имущества посредством международного сотрудничества.

Анализируя данную Конвенцию, можно прийти к выводу о том, что она не содержит прямого определения коррупции. Проблема в определении коррупции в том, что она содержит в себя широкий спектр противоправных действий, поэтому международное сообщество согласилось выделить перечень коррупционных действий. При этом каждое государство оставляет за собой право расширить этот список. Как говорилось ранее, коррупция – это злоупотребление властью в личных целях. Виды коррупции, которые содержаться в Конвенции: подкуп должностных лиц, хищение, неправомерное использование имущества публичным должностным лицом, злоупотребление влиянием и служебным положением, незаконное обогащение.

Конвенция содержит ряд особенностей по сравнению с предыдущими документами. Прежде всего в ней делается акцент на предотвращении коррупции. Далее Конвенция содержит описание различных составов коррупционных преступлений и криминализирует незаконное обогащение, что способствует уголовному преследованию за коррупционные преступления. На мой взгляд, «Конвенция ООН против коррупции» служат прочной основой для разработки и реализации мер, обеспечивающих снижение коррупции.

Таким образом, можно сделать ряд важных выводов-тезисов. 1) Понятие коррупции трактуется по-разному многими учёными, однако сущность проблемы понимается ими и законодателями одинаково. 2) Коррупция- это международная проблема. 3) ООН как самая влиятельная организация приняла ряд важных документов против коррупции. 4) Основными такими документами являются: «Декларация Организации Объединённых Наций о борьбе с коррупцией и взяточничеством в международных коммерческих операциях», «Конвенция Организации Объединённых Наций против транснациональной организованной преступности», «Конвенция Организации Объединенных Наций против коррупции». 5) Данные документы расположены в хронологическом порядке, и каждый новый дополняет и конкретизирует предыдущий. 6) Однако ни в одном из них не представлено четкое определение понятию коррупции, даются лишь е виды. 7) Последняя Конвенция играет огромную роль и по сегодняшний день: она содержит ряд важных положения, выполнение которых обеспечит противодействие коррупции. 8) Большое значение имеет осознание мировым сообществом данного зла и стремление его устранить, хочется верить, что такая практика продолжится и в будущем.

Список литературы:

1. И.Д.Фиалковская Коррупция: понятие, признаки, виды // Вестник Нижегородского университета им. Н.И. Лобачевского. 2018. №1. С. 137-142.
2. Закон Российской Федерации «О противодействии коррупции» от 19 декабря 2008 № 273-ФЗ // Российская газета. 2008 г. № 4823.
3. Декларация Организации Объединенных Наций о борьбе с коррупцией и взяточничеством в международных коммерческих операциях // ООН URL: http://www.un.org/ru/documents/decl_conv/declarations/bribery.shtml (дата обращения: 18.11.2018).
4. Конвенция Организации Объединенных Наций против транснациональной организованной преступности // ООН URL: http://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml (дата обращения: 18.11.2018).
5. Конвенция Организации Объединенных Наций против коррупции // ООН URL: http://www.un.org/ru/documents/decl_conv/conventions/corruption.shtml (дата обращения: 18.11.2018).

СЕМЕНОВ НИКИТА СЕРГЕЕВИЧ
студент Факультета анализа рисков и экономической
безопасности имени профессора В.К.Сенчагова,
Финансовый университет при Правительстве Российской Федерации, г. Москва
E-mail: semyonnikita@yandex.ru;

КОРРУПЦИОННЫЕ РИСКИ «МУСОРНОЙ» РЕФОРМЫ (НА ПРИМЕРЕ СТОЛИЧНОГО МЕГАПОЛИСА)

SEMENOV NIKITA SERGEEVICH
student, Professor Senchagov Faculty of Risk Analysis and Economic Security
Financial University under the Government of the Russian Federation, Moscow

CORRUPTION RISKS OF "GARBAGE" REFORM (ON THE EXAMPLE OF THE CAPITAL'S MEGAPOLIS)

Аннотация: Сегодня в числе многочисленных вызовов и угроз России можно выделить загрязнение окружающей среды. в частности, остро стоит проблема утилизации бытовых отходов: действующие мусорные полигоны практически переполнены, а работа мусороперерабатывающей инфраструктуры ещё не налажена. Создание современной системы переработки мусора, эффективный общественный контроль и рекультивация мусорных свалок являются задачами национального проекта «Экология», реализуемого на основе «майского» Указа Президента 2018 года. с 2019 года в России начала реализовываться мусорная реформа, суть которой заключается в назначении единых региональных «операторов» по обращению с бытовыми отходами. Автором обозначены основные проблемы реализации «мусорной» реформы: рост тарифов для населения и непрозрачность деятельности региональных «операторов». Указаны подходы к определению коррупционных рисков В.В. Астанина, В.И. Авдийского и В.А. Дадалко, перечислены основные группы коррупционных рисков. Изучены госзакупки на право вывоза мусора в Москве, выявлены риски картельного сговора нескольких компаний и их аффилированность с представителями власти. Рассчитан ориентировочный ущерб от коррупционных действий компаний на торгах на основе исследуемой выборки. Предложены меры для снижения коррупционных рисков в ходе реализации «мусорной» реформы.

Abstract: Today, among the many challenges and threats to Russia, we can single out environmental pollution. In particular, the problem of recycling household waste is acute: existing landfills are almost full, and the work of the waste processing infrastructure has not yet been established. The creation of a modern waste management system, effective public control and reclamation of landfills are the tasks of the national project «Ecology», implemented on the basis of the «may» presidential Decree of 2018. Since 2019, Russia has started implementing a garbage reform, the essence of which is to appoint unified regional «operators» for handling household waste. The author identifies the main problems of implementing the «garbage» reform: the growth of tariffs for the population and the opacity of the activities of regional «operators». The approaches to determining corruption risks of V. V. Astanin, V. I. Avdiyskiy and V. A. Dadalko are indicated, and the main groups of corruption risks are listed. We studied public procurement for the right to remove garbage in Moscow, identified the risks of cartel collusion of several companies and their affiliation with the authorities. The estimated damage from corrupt actions of companies at auctions is calculated on the basis of the studied sample. Measures are proposed to reduce corruption risks during the implementation of the «garbage» reform.

Ключевые слова: «мусорная» реформа, коррупционные риски, государственные закупки, картельный сговор, конфликт интересов.

Keywords: «garbage» reform, corruption risks, public procurement, cartel, conflict of interest.

Введение

Перед российским государством и обществом сегодня стоит немало вызовов и угроз, связанных с неразрешенными социально-экономическими проблемами. Одной из главных угроз экономической безопасности России является загрязнение окружающей среды, следствием чего могут стать такие серьезные проблемы, как исчерпание ресурсного потенциала страны, ухудшение состояния здоровья людей, социально-политическая нестабильность в обществе.

Экологических проблем в стране сегодня довольно много: загрязнение водоемов, в том числе таких стратегически важных, как река Волга и озеро Байкал; вырубка и теневой экспорт леса; загрязнение воздуха. в рамках данного реферата автор ставит проблему назревшего «мусорного» кризиса и начатой в России «мусорной» реформы с позиции коррупционных рисков.

Актуальность проблемы заключается в острой фазе «мусорного» кризиса в Российской Федерации: исчерпании мощностей большинства действующих полигонов для захоронения мусора, отсутствии в достаточном количестве необходимой инфраструктуры для переработки отходов, а также наличии коррупциогенных факторов в деятельности мусоровывозящих компаний.

Цель реферата – изучить суть мусорной реформы и деятельность московских мусоровывозящих компаний и выявить коррупционные риски.

Для поставленной цели автор предлагает решить следующие задачи:

- изучение основных положений Федерального закона, регламентирующего порядок обращения с отходами, а также цели, поставленные Президентом РФ в рамках национального проекта «Экология»;
- мониторинг поведения компаний, занимающихся утилизацией мусора в Москве, на госзакупках, выявление коррупционных рисков в их деятельности;
- указание возможных негативных последствий реализации коррупционных рисков для мусоровывозящих компаний, государства и общества:
- предложение мер по снижению коррупционных рисков в деятельности мусоровывозящих компаний.

Обострение «мусорного» кризиса

Главная и основная проблема, касающаяся порядка обращения с бытовыми отходами, заключается в том, что потенциал подавляющего большинства действующих полигонов, куда свозили и складывали мусор, исчерпан. о проблеме заговорили на федеральном уровне в конце 2017 года, когда жители Балашихи стали жаловаться на неприятный запах, исходящий от гигантской свалки мусорного полигона «Кучино». Президент поручил закрыть эту свалку. а в 2018 году сильный общественный резонанс вызвали волнения жителей Волоколамского района Московской области, требовавших закрыть мусорный полигон «Ядрово», с которого также происходят вредоносные выбросы в атмосферу.

В сложившейся ситуации перед государством стоит дилемма: решать проблему экстенсивным путем, то есть продолжать открывать новые мусорные полигоны, или начать реализовывать инфраструктурные проекты по переработке отходов. в краткосрочной перспективе решить проблему в масштабах всей страны не представляется возможным, так как строительство мусороперерабатывающих заводов требует времени. По этой причине большинство мусорных полигонов продолжают функционировать, но их производственные мощности уже на исходе. Попытки открыть новые свалки закономерно оборачиваются протестами местного населения, что наглядно продемонстрировала недавняя попытка начать строительство полигона близ станции Шиес в Архангельской области.

В связи с назревшими проблемами государство стало принимать законодательные меры, направленные на выход из «мусорного» кризиса.

Законодательные меры, направленные на выход из «мусорного» кризиса

В первую очередь, необходимо отметить, что серьезность проблем осознается на высшем уровне. Согласно «майскому» указу Президента 2018 года, предметом одного из национальных проектов, порученных к исполнению Правительству РФ, является экология.

Ключевыми задачами нацпроекта «Экология» в части обращения с мусором являются:

- формирование комплексной системы обращения с отходами, включая рекультивацию территорий и ликвидацию свалок;
- создание и эффективное функционирование системы общественного контроля с целью выявления и ликвидации несанкционированных свалок;
- создание современной инфраструктуры для обращения с отходами и их вторичной переработки.

Приведены целевые показатели проекта до 2024 года. в частности, планируется повысить долю отходов, направленных на утилизацию, с 3% в 2018 году до 36% в 2024 году; долю отходов, направленных на переработку, с 7% в 2018 году до 60% в 2024 году.

Разумеется, для решения таких серьезных глобальных задач в течение шести лет необходимы ресурсы и структурные изменения в порядке обращения с мусором. Эти изменения начинают происходить уже сейчас и связаны с изменениями, внесенными Правительством в Федеральный закон «Об отходах производства и потребления», которые неофициально назвали «мусорной» реформой.

Суть основных изменений заключается в следующем:

- с 1 февраля 2019 года услуга «вывоз мусора» оплачивается по отдельному тарифу, который прописан в квитанции за жилищно-коммунальные услуги;
- с 2020 года все регионы, кроме городов федерального значения, переходят на систему «региональных операторов» – единственных подрядчиков в сфере обращения с отходами, которых вправе будут определять региональные власти; Москва, Санкт-Петербург и Севастополь начнут работать в таком режиме с 2022 года.

Две главные проблемы в рамках этих изменений: повышение тарифов и непрозрачность процедур выбора исполнителей контрактов на вывоз мусора.

По данным доклада Общероссийского народного фронта, в 36 регионах, несмотря на переход на новую систему оплаты вывоза мусора, жителям выставили двойной счет: по старым и по новым правилам. Кроме того, в том же докладе говорится о том, что многие из фирм, с которыми в недавнее время заключались контракты, имели признаки фирм-»прокладок» с уставным капиталом в 10000 рублей и 1-2 людьми в штате. Кроме того, в аудиторско-консалтинговой сети Finexpertiza, что региональный разброс тарифов на вывоз 1 куб. м мусора доходит до 27 раз, а ценообразование является непрозрачным.

В таких условиях у региональных органов власти и приближенных к ним лиц открываются широкие возможности для коррупционных действий с целью получения контрактов на обращение с отходами и установления административной диктатуры, позволяющей завышать тарифы, пользуясь монопольным положением на рынке.

Многие специалисты скептически относятся к проводимой «мусорной» реформе. Так, например, генеральный директор Центра экологических инициатив и член экспертного совета Госдумы по жилищной политике и ЖКХ Владимир Кузнецов утверждает следующее:

«Вы поймите, мусорный вопрос — чисто политический. При этом схема вывоза и утилизации мусора не меняется. Кто возил мусор, тот его и будет возить. Может быть, где-то компании поменяются на аффилированные с региональной властью, где-то поменяют руководителей. Но назвать это реформой язык не поворачивается» [Кузнецов, 2019].

Автор разделяет данную позицию и готов обосновать свою точку зрения на примере московского рынка вывоза мусора.

Сущность понятия «коррупционные риски» и его содержание в контексте рассматриваемой темы

В настоящее время в российском законодательстве нет единого понятия коррупционных рисков. Согласно нормативно-правовым документам МВД России, коррупционные риски – условия и обстоятельства, предоставляющие возможность для действий (бездействия) лиц, замещающих должности федеральной государственной службы и должности в государственных корпорациях (государственной компании), с целью незаконного извлечения выгоды при выполнении своих должностных полномочий.

На отсутствие единого подхода в своей работе указывает кандидат юридических наук, доцент Уральского государственного юридического университета А.Е. Помазуев. Он приводит разные подходы к трактовке данного понятия. Например, согласно позиции В.В. Астанина, под коррупционными рисками понимается вероятность возникновения коррупционного поведения, которое может быть вызвано с запретами и ограничениями, установленными для государственных служащих [Помазуев, 2016: 65].

В целом, согласно любому определению, коррупционные риски связаны со злоупотреблениями в ходе осуществления властных полномочий. в частности, специалисты кафедры «Анализ рисков и экономическая безопасность» В.И. Авдийский и В.А. Дадалко отмечают, что коррупции может быть подвержен любой человек, обладающий дискреционной властью, то есть властью по распределению не принадлежащих ему ресурсов по своему усмотрению [Авдийский, Дадалко, 2012: 67].

Определение исполнителей контрактов по вывозу мусора проводится в рамках проведения торгов в системе государственных закупок. Поэтому автор предлагает выделить следующие группы коррупционных рисков, реализация которых возможна в ходе закупочных процедур:

- законодательные риски: пробелы в законодательстве, возможность вольной трактовки положений, нехватка конкретики;
- ведомственные риски: отсутствие четких положений относительно требований к участникам торгов, искусственное ограничение конкуренции посредством завышенных или невыполнимых требований заказчика;
- организационные риски: недостаточная транспарентность проводимых закупок, неэффективный контроль за их проведением;
- кадровые риски: наличие дружественных или родственных связей между заказчиком и участником конкурса, что приводит к злоупотреблению служебным положением и конфликту интересов.

В ходе реализации коррупционных действий в сфере государственных закупок систематически нарушаются Федеральные законы №44-ФЗ и №223-ФЗ, регламентирующие закупочную деятельность, а также закон №135-ФЗ «О защите конкуренции».

Согласно ФЗ №135, признаются картелем и запрещаются действия, которые приводят к:

- поддержанию выгодных для сговорившихся субъектов цен на торгах;
- отказу от заключения договоров с определенными организациями;
- сокращению или прекращению производства товаров;
- разделу товарного рынка по объему или ассортименту продаж, по территориальному признаку.

Проанализируем, какие коррупционные риски реализуются в ходе проведения торгов на вывоз мусора в Москве.

Коррупционные риски на госзакупках с участием мусоровывозящих компаний в Москве

В целях проведения исследования автор изучил все закупки, проведенные конкурентными способами в течение 2016-2018 годов, победителем в которых стало ООО «Эколайн» – одна из ведущих мусоровывозящих компаний Москвы. в целях сбора информации использовался сайт

для проверки контрагентов rusprofile.ru и единый портал государственных закупок. Ключевая информация по закупкам собрана в таблице.

В ходе мониторинга закупок автор обратил внимание на поведение на торгах ООО «Эколайн» совместно с ООО «Хартия» и ООО «Спецтранс». в ходе торгов на аукционах с участием «Эколайна» и «Хартии» начальная максимальная цена контракта снижалась максимум на 2,5%, а с участием «Эколайна» и «Спецтранса» не ниже 5%. в это же время на торгах с участием ООО «Эколайн» и других компаний снижение варьировалось куда сильнее и доходило до 30%. Очень характерны показатели среднеквадратического отклонения от среднего снижения цен на торгах.

Таблица 1. Среднеквадратическое отклонение по снижению НМЦ. Источник: разработано автором на основе [17]

Конкурирующие компании	ООО «Эколайн» и ООО «Хартия»	ООО «Эколайн» и ООО «Спецтранс»	ООО «Эколайн» и другие участники
Среднеквадратическое отклонение по снижению НМЦ	0,48%	1,04%	8,04%

Поддержание цен на торгах – один из признаков картельного сговора на госзакупках, потому что в этом случае фирмы заранее договариваются о совместном участии на торгах и разделе рынка. в таких условиях конкуренция лишь имитируется, в результате чего цены снижаются меньше, чем при настоящей конкуренции.

Кроме того, по данным rusprofile.ru автором проведены проверка аффилированности ООО «Эколайн», ООО «Хартия» и ООО «Спецтранс» с другими организациями, а также поиск конечных бенефициаров.

ООО «Эколайн» учрежден организацией, учредителями которой являются бывшие работники ГУП «Мосгортранс», а головная фирма также аффилирована с топ-менеджерами ПАО «РЖД» Михаилом Акуловым и Александром Рязановым, а также их сыновьями. (Приложение 1).

ООО «Хартия» учреждена фирмами, бенефициарами которых является сын генерального прокурора Юрия Чайки Игорь и его партер Александр Пономарев. а ООО «Спецтранс» учреждена дочерними структурами государственной корпорации «Ростех». Примечательно, что фирмы, аффилированные с Пономаревым и «Ростехом», были учредителями ООО «Авант», первого генерального подрядчика «Газпром-арены» в Санкт-Петербурге. Контракт с этой фирмой был расторгнут, а большая часть денежных средств похищена. (Приложение 2).

Таким образом, в ходе мониторинга закупок удалось выявить как количественные, так и качественные признаки коррупционных рисков: поддержание цен на торгах тремя вышеуказанными фирмами и их аффилированность с лицами, имеющими возможность использовать родственные связи и административный ресурс в целях извлечения личной выгоды и ухода от ответственности. Например, Генеральный Прокурор Юрий Чайка может иметь личную заинтересованность в том, чтобы его сын Игорь не привлекался к ответственности за совершенные правонарушения.

Изучив московский рынок вывоза мусора, автор считает необходимым обозначить, какие негативные последствия могут возникать в результате реализации коррупционных рисков и какие меры необходимы для их минимизации.

Потери бюджета и мусоровывозящих компаний от коррупции на госзакупках

Как уже было заявлено выше, от картельных сговоров и поддержания высоких цен на торгах страдает государственный бюджет, так как в ходе конкуренции между независимыми фирмами экономия значительно выше, чем в ходе фиктивной конкуренции.

Автор предлагает ориентировочно оценить возможные потери бюджета от сговора между мусоровывозящими компаниями. Для этого посчитаем общее снижение начальных максимальных цен по всем изученным контрактам.

Таблица 2. Общее снижение НМЦ по контрактам. Источник: рассчитано автором по данным [17]

Конкурирующие фирмы / Показатель	Сумма начальных максимальных цен, руб.	Сумма контрактов, руб.	Экономия, %
ООО «Эколайн» и ООО «Хартия»	185 126 922,6	178 657 200,37	3,5
ООО «Эколайн» и ООО «Спецтранс»	25 153 584	23 942 704,8	4,8
ООО «Эколайн» и другие участники	78 636 159,57	49 125 609,79	37,5

По данным таблицы видно, что в случае с другими участниками цена на закупках снижалась значительнее примерно на 30%.

Таким образом, возможная коррупционная рента от взаимодействия ООО «Эколайн» с ООО «Хартия» и ООО «Спецтранс» составляет 0,3 * 25 153 584 + 0,3 * 185 126 922,6 = 63 084 151,98 рублей. Сумма в масштабах бюджета небольшая, однако в целом по экономике за 2018 год, по данным Минфина, российский бюджет потерял не менее 152 млрд. рублей, поэтому проблема носит системный характер.

Что касается мусоровывозящих компаний, то проблемы у них могут возникнуть в случае привлечения их к ответственности за нарушение законодательства о закупках и защите конкуренции. Причем эта ответственность может быть как административной, так и уголовной.

Уголовная ответственность предусмотрена статьей 178 УК РФ «Ограничение конкуренции». к ней могут быть привлечены физические лица – бенефициары компаний. Автор, в свою очередь, предлагает расчет потенциальных потерь изученных в рамках работы фирм в случае наложения на них административного штрафа.

Федеральная антимонопольная служба на базе Кодекса об административных нарушениях разрабатывает методические рекомендации по расчету величины штрафов. Если следовать данным указаниям ФАС, то максимальный штраф для ООО «Эколайн» может составить 4% от совокупной суммы выручки. Рассчитаем, сколько могла потерять фирма за 2016-2017 годы.

Таблица 3. Возможные максимальные суммы административных штрафов для ООО «Эколайн» за 2016-2017 годы Источник: разработано автором на основе [17]

Показатель / Год	2016	2017
Выручка, руб.	1 657 053 000	2 333 779 000
Возможный максимальный штраф, руб.	66 282 120	93 351 160

Таким образом, за 2 года фирма могла потерять 66 282 120 + 93 351 160 = 159 633 280 рублей, то есть более полутора миллиона.

В результате компании понесут потери в случае привлечения к ответственности за недобросовестное поведение на рынке. в противном случае, как уже было сказано, пострадает бюджет. а граждане России в результате монополизации рынка будут вынуждены переплачивать за вывоз мусора, что будет способствовать росту социальной напряженности, а это, в свою очередь, таит в себе серьезные угрозы национальной безопасности.

Исходя из проведенного анализа, автор переходит к предлагаемым мерам для минимизации и предупреждения коррупционных рисков в сфере обращения с отходами.

Предлагаемые меры снижения коррупционных рисков

Для того, чтобы «мусорная реформа» не обернулась провалом, а общественное недовольство не продолжало нарастать, автор может предложить следующие меры:

- Упрощение законодательства о государственных закупках с целью повышения уровня конкуренции. На данный момент Федеральный закон №44-ФЗ содержит в себе массу возможностей для заведомого ограничения конкуренции. в частности, данный закон содержит более 50 оснований для заключения контракта с единственным поставщиком, что изначально несет в себе риск коррупционных взаимодействий между государственными заказчиками и близкими к ним фирмами. Так, АНО «Трансперенси Интернешнл – Россия» провело исследование, в котором рассказало о коррупционных рисках контрактов с единственным поставщиком, заключенными на основании Указов Президента и Постановления Правительства. То же самое касается возможности определения «региональных операторов» по обращению с отходами вне конкурса.
- Устранение правовых коллизий. Например, ФАС имеет право запрашивать необходимую информацию по закону «О защите конкуренции», однако банки могут ее не предоставить по закону «О банках и банковской деятельности». Это сильно затрудняет работу ФАС, ведь чтобы доказать картельный сговор, необходимо знать о движении денежных средств по счетам компаний.
- Привлечение «региональных операторов» и победителей конкурсов на вывоз мусора к реализации инфраструктурных проектов по переработке и утилизации мусора. Такой подход выглядит вполне логичным, потому что в результате «мусорной» реформы возросла нагрузка на домохозяйства, производящие мусор, и собранные с них средства было бы логично вкладывать в новую инфраструктуру.
- Разработка и внедрение на ведомственном уровне автоматизированной системы проверки контрагентов на благонадежность. Подобный проект был успешно реализован государственной корпорацией «Росатом». Аналогичный программный продукт мог бы позволить Правительству вовремя отслеживать злоупотребления на местах.

Заключение

В начале работы автор изучил предпосылки и суть мусорной реформы, законодательные основы в сфере обращения с отходами. Далее были изучены теоретические основы коррупционных рисков и их практическая реализация на торгах для заключения контрактов на вывоз мусора. После этого обозначены негативные последствия от коррупционных проявлений как для государства, так и для бизнеса, посчитаны возможные убытки на основе изученных контрактов; предложены меры по снижению коррупционных рисков в отрасли.

Подводя итоги, необходимо отметить, что «мусорная» реформа является важным этапом и серьезным испытанием для российского общества. в сложившейся ситуации, когда быстрые перемены невозможны, реализация коррупционных рисков особенно опасна для всех участников процесса: государства, бизнеса и гражданского общества.

Для эффективного и безболезненного перехода на современную систему обращения с отходами необходима политическая воля государства к недопущению коррупционных злоупотреблений и одновременно готовность общества к переменам: экологичному образу жизни, раздельному сбору отходов и т.д. Только в случае готовности всех сторон к диалогу и ответственному поведению «мусорная» реформа будет направлена в правильное русло.

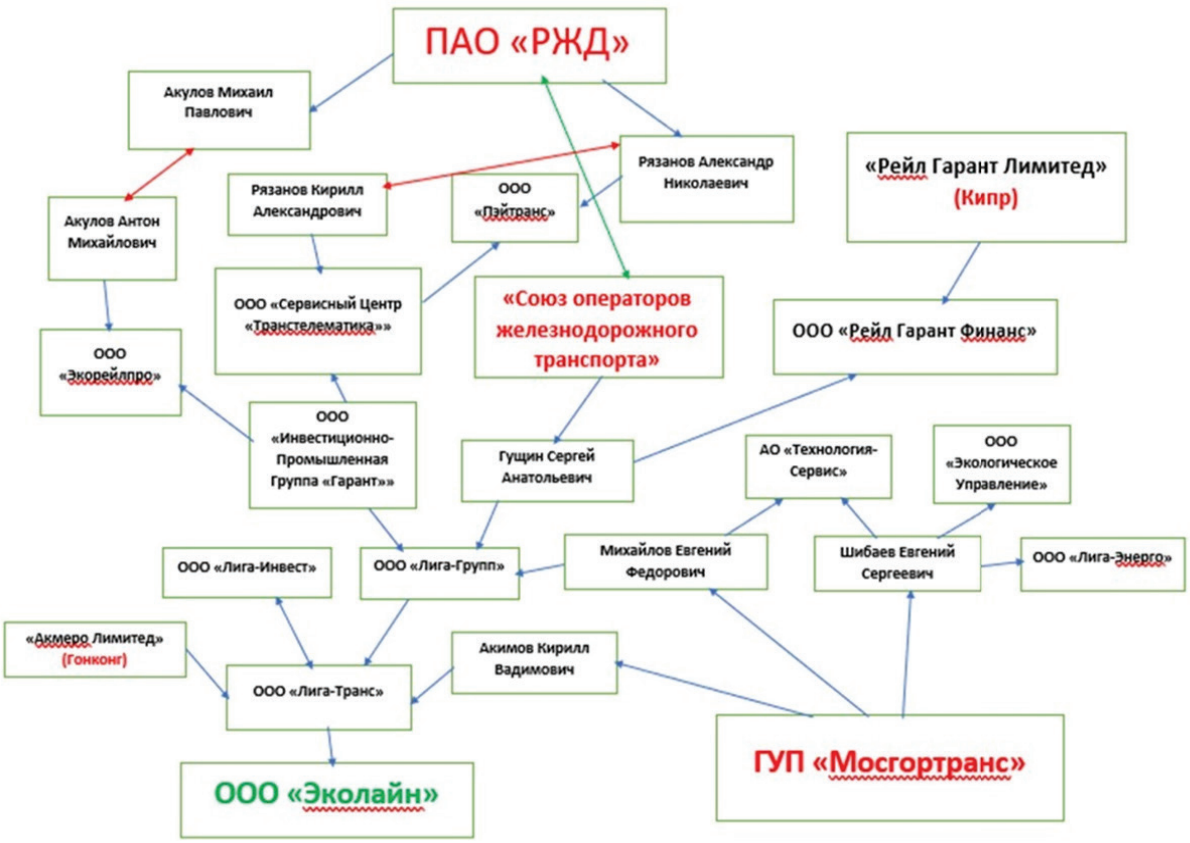
Источники

1. Авдийский В.И., Дадалко В.А. Теневая экономика и экономическая безопасность государства: учеб. пособие. – 2-е изд., доп. – М.: Альфа-М, ИНФРА-М, 2010. – 496 с. ;
2. Помазуев А.Е. Коррупционные риски: понятие и значение для механизма противодействия коррупции [Электронный ресурс]. URL: https://cyberleninka.ru/article/v/korruptsionnye-riski-ponyatie-i-znachenie-dlya-mehanizma-protivodeystviya-korruptsii ;
3. Федеральный закон от 31.12.2017 N 503-ФЗ «О внесении изменений в Федеральный закон «Об отходах производства и потребления» и отдельные законодательные акты Российской Федерации» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_286766/3d0cac60971a511280cbba229d9b6329c07731f7/ ;
4. Федеральный закон «О закупках товаров, работ, услуг отдельными видами юридических лиц» от 18.07.2011 N 223-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_116964/ ;
5. Федеральный закон «О защите конкуренции» от 26.07.2006 N 135-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61763/ ;
6. Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 N 44-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_144624/ ;
7. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/e8e8c98df722e05999230271e054b6a1f6f70f80/ ;
8. Указ Президента Российской Федерации «О национальных целях и стратегических задачах развития Российской Федерации до 2024 года» [Электронный ресурс]. URL: https://mvd.consultant.ru/files/1056500 ;
9. В Подмосковье продолжаются экологические протесты // Ведомости [Электронный ресурс]. URL: https://www.vedomosti.ru/politics/articles/2018/04/14/766717-mitingi-protiv-svalok ;
10. «Вы поймите, мусорный вопрос — чисто политический»: Почему «мусорная реформа» пошла не туда и вызывает недовольство граждан. Интервью // Знак [Электронный ресурс]. URL: https://www.znak.com/2019-02-01/pochemu_musornaya_reforma_poshla_ne_tuda_i_vyzyvaet_nedovolstvo_grazhdan_intervyu ;
11. Двойной отход: почему россияне выступают против «мусорной реформы» // Новая Газета [Электронный ресурс]. URL: https://www.novayagazeta.ru/articles/2019/03/05/79780-dvoynoy-othod ;
12. Единая информационная система в сфере государственных закупок [Электронный ресурс]. URL: http://zakupki.gov.ru/epz/main/public/home.html ;
13. Методические рекомендации по расчету величины штрафа, налагаемого на юридических лиц за совершение административных правонарушений, предусмотренных статьями 14.31 и 14.32 Кодекса Российской Федерации об административных правонарушениях [Электронный ресурс]. URL: http://arhangelsk.fas.gov.ru/page/7094 ;
14. Минфин подсчитал потери бюджета при проведении госзакупок // News.ru [Электронный ресурс]. URL: https://news.ru/den-gi/minfin-podschital-poteri-byudzheta-pri-provedenii-goszakupok/

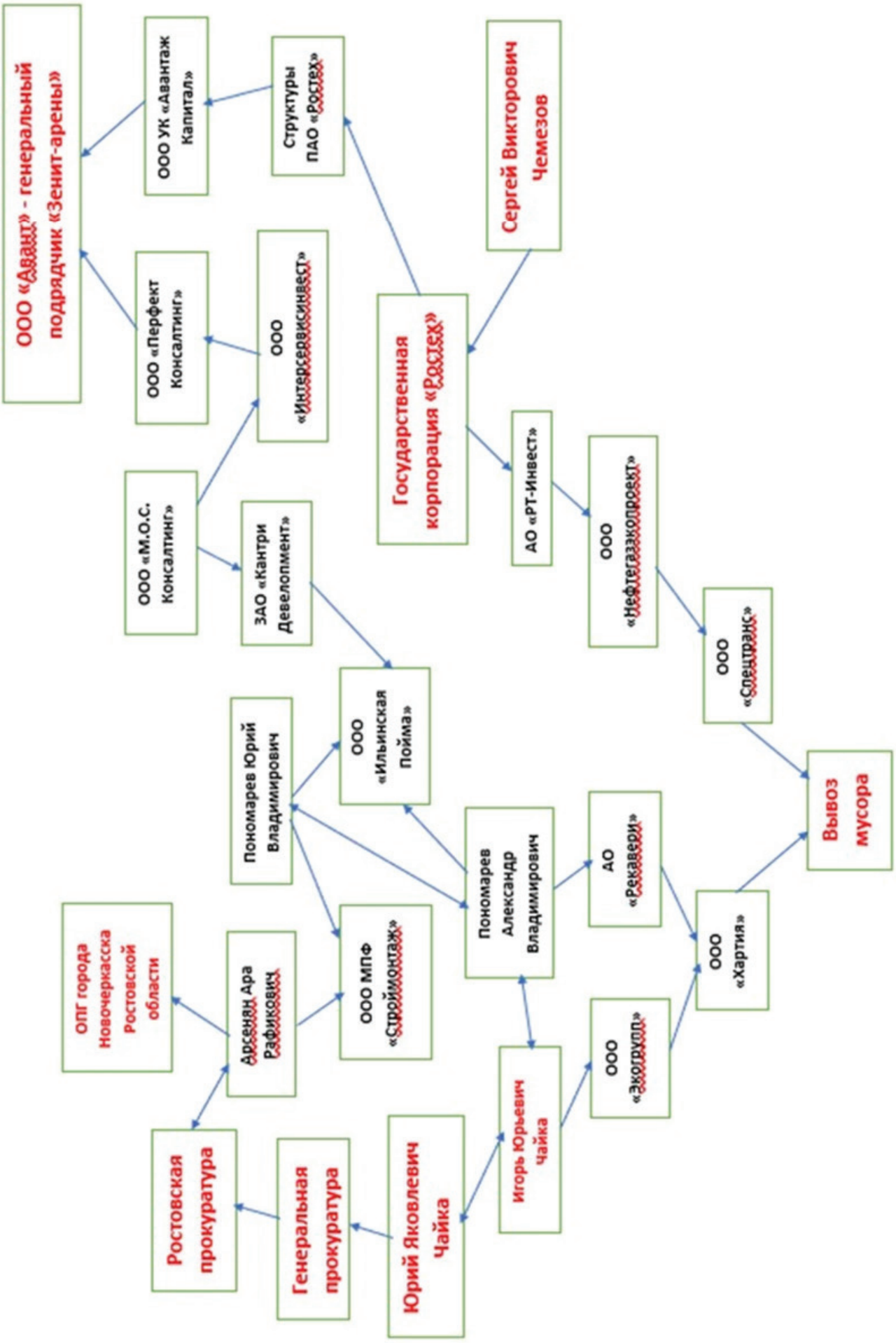
;
15. Национальный проект «Экология» [Электронный ресурс]. URL: https://strategy24.ru/rf/projects/project/view?slug=natsional-nyy-proyekt-ekologiya&category=ecology ;
16. Обещанного девять лет ждали: строительство, цены
17. и скандалы “Зенит-Арены” // ТАСС [Электронный ресурс]. URL: http://zenit-arena.tass.ru ;
18. Президент велел дорожать: Президент и правительство без конкурса отдают госконтракты компаниям Агаларова, Куснировича и Ротенберга [Электронный ресурс]. URL: https://zakupki.transparency.org.ru/2/ ;
19. Проверь любую организацию. Бесплатно. [Электронный ресурс]. URL: https://www.rusprofile.ru ;
20. Путин поручил закрыть свалку в Балашихе за месяц // РБК [Электронный ресурс]. URL: https://www.rbc.ru/politics/22/06/2017/594bc2609a7947fbe954ba15 ;
21. Путин удивился решению строить мусорный полигон в Архангельской области у поселков [Электронный ресурс]. URL: https://www.vedomosti.ru/politics/news/2019/05/16/801605-poselkov ;
22. Рекомендации по проведению оценки коррупционных рисков, возникающих при реализации функций // ГУ МВД России по г. Москве [Электронный ресурс]. URL: https://77.мвд.рф/гу-мвд/Protivodejstvie_korrupcii/Metodicheskie_materiali/Rekomendacii_po_provedeniju_ocenki_korru ;
23. Росатом создал базу недобросовестных поставщиков // ИА Regnum [Электронный ресурс]. URL: https://regnum.ru/news/2155021.html ;
24. Таблица торгов с участием ООО «Эколайн» [Электронный ресурс]. URL: https://docs.google.com/spreadsheets/d/1mJoNTC73mbzMNTEqEXdt1soZU5wGpuUZI3VpCzxmVW0/edit#gid=1553573769 .

Приложение

1. Схема аффилированности ООО «Эколайн» с другими физическими и юридическими лицами. Источник: составлено автором на основе [17]



2. Схема аффилированности ООО «Хартия» и ООО «Спецтранс» с другими физическими и юридическими лицами. Источник: составлено автором на основе [17]



СМИРНОВА КСЕНИЯ АНДРЕЕВНА
студентка факультета бизнеса и менеджмента
НИУ ВШЭ, г. Москва
E-mail: ks_smirnova@bk.ru

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

SMIRNOVA KSENIA ANDREEVNA
student, faculty of Business Management
National Research University «Higher School of Economics», Moscow

SOCIAL ENGINEERING AS AN INFORMATION SECURITY THREAT

Аннотация: В данной статье рассматривается такой вид угроз информационной безопасности как социальная инженерия, описываются некоторые виды атак социальных инженеров, анализируются причины повышенной опасности подобных атак для безопасности компании. Приводится ссылка на статистику, подтверждающую повышенную угрозу подобного вида нарушения информационной безопасности.

Annotation: This article discusses such type of information security threats as social engineering, describes some types of attacks that could be done by social engineers, analyzes the reasons for the increased danger of such attacks for company security. A link to a statistics report confirming the increased threat of this type of information security violation is provided.

Ключевые слова: информационная безопасность, социальная инженерия.

Key words: information security, social engineering.

В современном мире информация является наиболее ценным ресурсом, который может стать опасным оружием в руках мошенников или конкурентов по бизнесу. Несмотря на то, что рынок информационной безопасности совершенствуется с каждым годом, у злоумышленников появляются новые способы получения конфиденциальной информации. в данном эссе будет рассмотрен один из возможных способов получения информации – социальная инженерия, а также предложены методы противодействия данной угрозе.

Социальная инженерия – это способ получения необходимого доступа к информации, основанный на психологии людей. в основе этого метода лежит предположение, что, несмотря на стремительный научно-технологический прогресс, человеческая психология остается неизменной, поэтому для получения информации выгоднее и удобнее использовать уязвимости именно в ней, играя на чувствах и доверии других людей.

Действительно, компания может обеспечить себя наиболее передовыми системами физической защиты, установить современное программное обеспечение и антивирусные программы, провести обучение персонала, однако проблема человеческого фактора, непредсказуемости поведения людей, по-прежнему остается – и злоумышленник непременно воспользуется слабым местом.

Какие цели преследуют так называемые социальные инженеры? Некоторые из них стремятся к личной выгоде, например, представившись именем клиента и назвав его идентификационный номер либо другие конфиденциальные сведения, которые они узнали заранее, они получают скидку в интернет-магазине. Другие же занимаются этим профессионально и зарабатывают на добывании и продаже информации компаниям-конкурентам. Именно последний вариант, на

мой взгляд, может привести к критичным последствиям для организаций. Просто представьте, что компания-конкурент получила доступ к каким-либо материалам по разработке продукта и, прежде чем компания-жертва атаки успела понять, что произошла утечка данных, использовала полученные сведения для того, чтобы занять первое место на рынке.

При этом, как уже было сказано выше, одним из основных инструментов социальных инженеров является игра на доверии. Они не вынуждают выбранное атакуемое лицо сообщать конфиденциальную информацию под дулом пистолета. Чаще всего жертва даже не понимает, что подверглась атаке — социальные инженеры нередко прикидываются сотрудниками той же организации или клиентами, нуждающимися в помощи. Как можно отказать просьбе коллеги из филиала в другом городе, у которого сломался компьютер? Другим известным приемом социальных инженеров является так называемый «кви про кво» (лат. qui pro quo, что-то вместо чего-то, путаница, также услуга за услугу). При этом злоумышленник намеренно создает ситуацию, в которой жертве приходится обращаться к нему за помощью. в процессе оказания помощи социальный инженер может получить необходимую информацию или установить на компьютер жертвы вредоносное программное обеспечение. в некоторых случаях злоумышленники используют природное человеческое любопытство, оставляя на видном месте флеш-накопитель или направляя на электронную почту документ с интригующим названием, например «Списки на увольнение» или «Премии сотрудников 2019». Под видом интересной информации обычно скрывается программа-вирус.

На первый взгляд может показаться, что только очень недалекий человек может попасться на подобные уловки. в большинстве компаний сотрудники проходят базовое обучение основам информационной безопасности: их учат не открывать подозрительные файлы, не сообщать никому свои логины и пароли, не оставлять документы с конфиденциальной информацией на рабочем месте, где посторонние могут их увидеть. Однако социальные инженеры используют гораздо более хитрые и сложные методы получения информации, при этом манипулируя эмоциями. Например, это может быть страх подчиненных перед вышестоящим руководством или наоборот желание помочь и быть полезным, выслужиться. Опытный социальный инженер сможет надавить даже на человека, заметившего что-то подозрительное в просьбе собеседника, и в этом и заключается основная опасность подобной атаки. Даже если сотрудник компании действует строго по прописанному регламенту, нельзя гарантировать, что он продолжит следовать правилам, если ему пригрозят жалобой начальнику или сделают удачный комплимент.

Мне стало интересно, действительно ли социальная инженерия является эффективной, поэтому я нашла статистику, собранную в ходе тестирования на проникновение с помощью методов социальной инженерии (отправка сообщения с веб-ссылкой, файлом или формой для ввода пароля). Почти в 20% случаев сотрудники «атакуемой» компании своим поведением могли скомпрометировать конфиденциальную информацию. Наиболее уязвимыми оказались сотрудники служб, не связанных с IT: бухгалтеры, юристы и т.д. Некоторые сотрудники вступали в диалог с «атакующим», сообщали, что присланный документ не открывается, советовали направить письмо другому человеку. Это свидетельствует о крайне низком уровне осведомленности персонала о подобной угрозе.

Утечка информации является необратимым действием, способным привести к катастрофическим последствиям для бизнеса. в связи с этим, на мой взгляд, компании необходимо составить такой свод правил информационной безопасности, в котором найдется место противодействию социальной инженерии, а также регулярно проводить обучающие тренинги для сотрудников и включить в практику тестирование на проникновение с использованием методов социальной инженерии для обнаружения слабых мест и их устранения. Должны быть прописаны и соблюдены ключевые принципы информационной безопасности. Сотрудники компании должны осознавать, что не все люди, с которыми они общаются виртуально или по телефону на самом деле являются теми, за кого они себя выдают, даже если они звучат убедительно, владеют необходимой терминологией и какими-либо ключевыми для доступа данными. Помимо этого, сотрудники должны иметь возможность проверить, с кем они общаются на самом деле (например, найти в телефонном справочнике компании контакты человека и перезвонить ему самостоятельно). Каж-

дый из сотрудников должен осознавать, что он не подвергнется наказанию, если он не сообщит подозрительному лицу какую-либо информацию, напротив, именно утечка данных приведет к гораздо более разрушительным последствиям для компании.

Таким образом, можно прийти к выводу, что социальная инженерия является серьезной угрозой для информационной безопасности бизнеса. в работе с конфиденциальной информацией намного лучше проявить больше осмотрительности, чем допустить утечку. Без должного обучения персонал становится опасным уязвимым местом, которым не преминут воспользоваться злоумышленники. в связи с этим, в интересах компании повышать уровень осведомленности сотрудников, а также развивать службу безопасности, в которую персонал сможет обратиться в случае подозрительного запроса.

Список литературы

1. Митник К. Искусство вторжения / К. Митник, В.Л. Саймон – ДМК Пресс, 2004.
2. Отчет Positive Technologies – социальная инженерия открывает хакерам двери вашей компании (Электронный ресурс) / URL: https://www.securitylab.ru/news/492267.php Дата обращения к ресурсу – 01.12.2018
3. Should social engineering be a part of penetration testing? (Электронный ресурс) / URL: https://www.darknet.org.uk/2006/03/should-social-engineering-a-part-of-penetration-testing/ Дата обращения к ресурсу – 01.12.2018

СОРОКА ДАРЬЯ АНАТОЛЬЕВНА
студентка факультета бизнеса и менеджмента
НИУ ВШЭ, г. Москва
E-mail: dasoroka@edu.hse.ru

МЕТОДЫ ВОЗВРАТА ПРОСРОЧЕННОЙ ЗАДОЛЖЕННОСТИ

SOROKA DARIA ANATOLEVNA
student, faculty of business and management
National Research University «Higher School of Economics», Moscow

RETURN METHODS OF OVERDUE DEBTS

Аннотация: В статье рассматривается тема просроченной задолженности. в ходе подготовки её была использована учебная, научная и периодическая литература таких авторов, как Саблина М.Т., Тарташева В.А. и других, а также интернет-ресурсы. в статье описывается и анализируется задолженность как общественное явление, изучаются причины ее появления и, как результат, выявляются методы взыскания и порядок действий.

Abstract: The article discusses the topic of overdue debt. During its preparation, educational, scientific and periodical literature of such authors as Sablina M.T., Tartasheva V.A. and others was used, as well as online resources. The article describes and analyzes debt as a social phenomenon, studies the causes of its occurrence and, as a result, reveals methods of collection and the order of actions.

Ключевые слова: долг, задолженность, просроченная задолженность, debt.

Keywords: debt, arrears

Введение

В статье рассматривается тема просроченной задолженности, базовые термины для которой, - это сама «задолженность»/«долг». Существует несколько интерпретаций этих слов, рассмотрим основные. Итак, долг – это текущие обязательства по возврату денежных средств или иных материальных благ в установленный срок, который на текущий момент еще не наступил; задолженность – это обязательства, срок исполнения которых уже истек или, иными словами, это просроченный долг. Задолженность также можно описать как установленную договором или иным основанием обязанность одного лица (должника) совершить в пользу другого лица (кредитора) определенное действие, как-то передать имущество, выполнить работу, уплатить деньги и т.п. Таким образом, в данной статье исследуется именно просроченный долг, то есть задолженность – объект, а предметом станут методы ее возврата.

Актуальность работы обусловлена тем, что в любое время (в историческом аспекте) физические или юридические лица могут иметь те или иные задолженности, и «хозяин» того или иного имущества заинтересован в возврате долга. в современных условиях (кризисы, некоторый уровень нестабильности) проблема невозврата долга стоит весьма остро. Каждый кредитор (лица (юридические и физические), предоставившие свои временно свободные средства в распоряжение заемщика на определенный срок) надеется на своевременное погашение возникшей дебиторской задолженности.

История позволила выявить определенные требования, необходимые для законного и справедливого развития отношений между кредитором и дебитором. в наше время долговые отношения регулируются законодательством страны, которое устанавливает некоторые общие правила и защищает обе стороны от противоправных действий друг друга.

Практическая значимость данной статьи проистекает из вопросов ее актуальности, таким образом для нас важно донести до заинтересованных людей, до читателей методы, способы и процедуры возврата долгов основываясь на законодательстве и реальной практике.

Основная часть

Как было написано ранее, задолженность – это обязательства, срок исполнения которых уже истек, то есть это просроченный долг. в предпринимательской деятельности термин «задолженность» может быть применим к отношениям физических и/или юридических лиц между собой в рамках возникших между ними гражданско-правовых отношений.

Будем идти последовательно, начнем с «зарождения» задолженности, рассмотрим, как же попытаться ее предотвратить, разные ее стадии и, наконец, методы возврата теми или иными способами.

В предпринимательстве долги подстерегают «на каждом шагу», например, когда:

- поставщик поставил нам товар;
- при перевозке какого-либо товара;
- при оказании какой-либо услуги, когда еще предстоит выплатить деньги;
- при выплате заработной платы работникам, сотрудникам, персоналу компании;
- при оплате аренды помещения;
- при уплате налогов и др.;
- и другие.

Возникает вопрос: как же предотвратить появление задолженности? Конечно, это можно сделать, однако не всегда получается, как показывает практика. Необходимо осуществлять контроль за оплатой, возвратом имущества, денег на каждом этапе деятельности. На предприятии должна быть выработана определенная кредитная политика, некая система штрафов, пеней, либо наоборот поощрений в виде, например, скидок, также можно минимизировать или прекратить вовсе сотрудничество с недобросовестными контрагентами. Стоит создать качественную систему работы с клиентами и/или должниками. Таким образом, еще раз укажем на то, что необходим четкий контроль этой сферы.

Стадии задолженности. Рассмотрим на примере банка. Заемщик должен банку, он постепенно производит выплаты в соответствии с договором, это – текущая задолженность. в том случае, если заемщик в какой-то момент не произвел выплату и не предупредил об этом банк, это может именоваться «проблемной задолженностью». После этого он не произвел оплату еще несколько раз и просрочил выплаты согласно договору, это уже просроченная задолженность. И, если заемщик с тех пор скрывается, его не могут найти и принудить к выплате долга, то задолженность может быть в конечном счете списана.

В общем случае закон всегда защищает права кредитора. в случае невыплаты долга заимодавец имеет право обратиться с иском в суд, который учтет интересы кредитора и в принудительном порядке будет взыскать долги. Все правоотношения между сторонами договора регулируется законодательством и решаются в судебном или досудебном порядке, в зависимости от различных обстоятельств.

Возврат долга в досудебном порядке. Во-первых, бухгалтерия компании видит недостачу. в случае наличия задолженности должнику напоминают о ней; далее сообщается, что в если он в течение определенного времени не выплатит долг, заимодавец будет вынужден обратиться в суд, указываются негативные последствия судебного разбирательства.

Таким образом, все начинается с анализа ситуации, далее идет мягкое взыскание (soft collection) – состоит из способов возврата долга, включающих телефонные звонки, письма, уведомления, сообщения; потом жесткое (hard collection) – личные встречи с должником, то есть переговоры, убеждение, психологическое воздействие, юридическое (legal collection) – обращение в судебные органы.

Legal collection начинается после 60-90 дней после просрочки. Возникает этот этап, когда

никакие переговоры с должником не помогли, и остается только вариант – обратиться в суд. Этот этап состоит из стадий:

- судебное производство (взыскатель стремится получить защиту от государства);
- исполнительное производство (пристав исполняет решение суда).

Судебное разбирательство – вполне эффективный способ возврата долга при условии, что факт передачи имущества/денег документально подтверждён и доказан. в случае банковских кредитов с этим проблем не возникнет, так как на руках у кредиторов имеется оформленный по всем правилам договор.

Результатом успешного для кредитора судебного разбирательства выступает исполнительный лист или приказ о принудительном возврате средств. у должника есть законное право опротестовать судебное решение в установленный период.

Также возможен **внесудебный порядок взыскания**. Он дает возможность кредитору вернуть деньги без обращения в суд. Это ставит должника в неблагоприятное положение. Если в случае с судом заимодавцу необходимо было подготовить и подать иск, принять участие в нескольких судебных заседаниях, дождаться вступления решения суда в силу и только после этого он мог получить исполнительный лист, то теперь кредитор может сразу обратиться к приставам с исполнительной надписью на договоре.

Обратившись к приставам, кредитор может требовать совершения в отношении должника всех исполнительных действий, включая ограничение выезда за границу, арест счетов и имущества и др. Таким образом, внесудебный порядок обращения взыскания на имущество существенно облегчает жизнь кредитору и усложняет должнику.

В каждой конкретной ситуации необходим четкий анализ контрагента, так как нет никакой системы, каждый заемщик не похож ни на какого другого, следовательно, нужно выявить и выработать определенный план действий и стратегию взаимодействия.

Должники бывают разные, значит и воздействовать на них нужно по-разному. Например, со злостными неплательщиками нет смысла долго использовать Soft Collection, стоит сразу перейти к судебным процедурам.

Классифицировать должников можно по разным признакам, таким как:

- срок просрочки;
- тип должника (физическое, юридическое лицо, ИП);
- по основанию правоотношений (договор);
- по виду требований (денежные/неденежные, товар, услуга или деньги);
- по размеру долга;
- по причинам появления задолженности;
- по территориальному нахождению;
- по характеру отношений (разовый контрагент, долгосрочные отношения)
- другие.

Перейдем непосредственно к инструментам и методам возврата просроченной задолженности, в том числе и к практическим.

Для начала выделим этапы взыскания задолженности:

1. Сначала кредитор анализирует ситуацию выясняет, как и почему появилась задолженность. Вполне возможно, что должник не может расплатиться в определенный период в следствие форс-мажорных обстоятельств, болезни, увольнения.
2. Уведомление. Должник должен знать, что кредитор о нём не забыл и терпеливо ждёт возврата своих денег. Для этого сотрудники банка или частные лица всеми способами напоминают о наличии просрочке долга посредством звонков, сообщений, писем.
3. Официальная претензия. Подтверждает, что взыскание производилось по всем правилам. Она составляется в свободной форме, но в ней обязательно должны быть указаны данные должника, сумма задолженности, даты и сроки. Если дело дойдёт до суда, этот документ нужно будет приложить к исковому заявлению о взыскании долга.

4. Коллекторы. Если вышеперечисленные методы не помогли решить проблему, то кредитор имеет законное право обратиться к третьим лицам – коллекторам.
5. Уведомление о подготовке передачи дела в суд. Если кредитор понимает, что все все безрезультатно, у него остаётся только один выход – обратиться в суд. Сделать это вправе не только банки, но и частные лица, а также коллекторы или юристы по взысканию долгов, нанятые кредитором. Во-первых, должнику обязательно пришлют уведомление о том, что заимодатель исчерпал все методы и вынужден инициировать судебное разбирательство. у неплательщика есть последний шанс погасить задолженность. Если он этого не сделает, суда не избежать.
6. Подготовка документов неплательщика для передачи в юр. отдел.
7. Само судебное разбирательство.

Обращение к услугам коллекторов. Как показали различные социальные опросы, многие люди считают, что долги зачастую «выбиваются», как это происходило в 90-е годы, хотя современные коллекторы не имеют ничего общего с криминалом (по крайней мере не должны). Коллекторская деятельность должна быть совершенно законной, потому что ее цель – не наказать должника, а сделать все возможное, чтобы он вернул долг, то или иное имущество. Неплательщику следует знать, что эффективных методов возврата долга в досудебном порядке, не идущих в разрез с законодательством, - немного. Коллекторы пытаются создать максимально некомфортные условия для должника. Обычно они использует в работе четыре метода:

- назойливость.
- давление;
- убеждение;
- хитрость.

Рассмотрим подробно каждый из них:

1. Совершаются постоянные сообщения, звонки на домашний, сотовый и рабочий телефоны должника и его ближайшего окружения. Стоит упомянуть, что в новостях иногда показываются ситуации, когда коллекторы угрожают должникам расправой, что конечно же не является законным. Также практикуются визиты рано утром и поздно вечером. и не только к самому должнику домой, но также и к его родственникам. в большинстве случаев длительное воздействие на должника, его родственников в конечном счете помогало решить проблему.
2. Психологическое воздействие на должника. Вместе с предыдущим методом наиболее эффективен.
3. Если предыдущие способы (назойливость и давление) не дают желаемого эффекта, коллектор прибегает к убеждению. Должнику объясняется, почему он обязан вернуть долг, и что произойдет в случае неоплаты. Опытный коллектор сначала попытается заставить должника оплатить долг, приведет примеры отрицательных последствий и др., ответит на все вопросы.
4. Цель – любыми законными, пусть даже «скользкими» с точки зрения морали, способами склонить должника к возврату долга.

Заключение

Деятельность по взысканию долгов – это отлаженный механизм действий, от звонков, претензий, встреч до судебного разбирательства и коллекторской деятельности. Он требует умений и решительности.

Успех в этой деятельности обусловлен быстрым выявлением и реакцией на задолженность. Если в компании постоянно происходят такие «катаклизмы» в виде различных просрочек со стороны контрагентов, то стоит задаться определенными вопросами и отладить методы своей работы в данном направлении.

Стоит помнить, что все должники разные, и взаимодействовать с ними стоит по-разному, используя специальный подход.

Список литературы:

1. Саблин М.Т. Взыскание долгов: от профилактики до принуждения: практическое руководство по управлению дебиторской задолженностью. – «Wolters Kluwer», 2010г.
2. Тарташев В.А. Как избавиться от кредита. Реальные способы выхода из долгового тупика – «Питер», 2010г.

СОТНИКОВА МАРИЯ ИГОРЕВНА
стажер-исследователь Института институциональных исследований
НИУ ВШЭ, г. Москва
E-mail: sotnickova.maria787@yandex.ru

РОЛЬ МЕСТНОЙ ВЛАСТИ В РАЗВИТИИ МАЛОГО И СРЕДНЕГО ПРЕДПРИНИМАТЕЛЬСТВА

Sotnikova Maria Igorevna
Research assistant for Institutional Studies
National Research University «Higher School of Economics», Moscow

THE ROLE OF LOCAL AUTHORITIES IN THE DEVELOPMENT OF SMALL AND MEDIUM ENTERPRISES

Аннотация: В регионах России, ввиду институционального дефицита, произошла деформация системы власти на местном уровне, которая привела к непрозрачности, локальности и ситуативности правил взаимодействия между бизнесом и властью. Ключевую роль в процессе коммуникации местной власти и представителей малого и среднего предпринимательства регионов играют неформальные механизмы взаимодействия. Данное положение вещей негативным образом отражается на экономическом благосостоянии страны. Исследование базируется на социологическом анализе и структурно-функциональном подходе, основу которых составляют глубинные интервью и наблюдение (в том числе и включенйное наблюдение). в ходе экспедиций в 2 региона России было опрошено 11 представителей власти и 70 представителей малого и среднего бизнеса.

Abstract: Due to the institutional deficit, a deformation of the power system at the local level in the regions of Russia took place. That led to the opacity, locality and situationality of the rules of interaction between business and government. Informal mechanisms of interaction play a key role in the process of communication between local authorities and representatives of small and medium enterprises in the regions. This state of things negatively affects the economic well-being of the country. The study is based on a sociological analysis and a structural-functional approach, which are based on in-depth interviews and observation (including participant observation). 11 representatives of the authorities and 70 representatives of small and medium-sized businesses were interviewed during the expeditions to 2 regions of Russia.

Ключевые слова: малое и среднее предпринимательство; местная власть; G2B взаимодействие; развитие бизнеса.

Keywords: small and medium enterprises; local authorities; G2B interaction; business development.

В настоящее время в условиях динамично развивающихся процессов глобализации и цифровизации экономики, возрастания конкуренции и соперничества на различных рынках большое значение имеет поддержка и развитие малого и среднего предпринимательства. Малый и средний бизнес (МСБ) способен легче и быстрее адаптироваться к динамичным и непостоянным условиям конъюнктуры рынков благодаря тому, что является более маневренным по причине относительно небольшой капиталоемкости. Малому и среднему предпринимательству (МСП) отводится одна их главных ролей в экономике практически любой страны, поскольку МСП предоставляет возможности по устранению ряда проблем: создает конкуренцию, предоставляет новые рабочие места, тем самым решая вопрос занятости населения, стимулирует увеличение экспортного по-

тенциала страны посредством наполнения различными товарами и услугами внутреннего рынка. По этой причине малому и среднему предпринимательству оказывается особое внимание со стороны правительств многих стран, вне зависимости от уровня их социально-экономического благосостояния — государства развивают и всячески поддерживают деятельность МСБ, разрабатывая стратегии и программы, предоставляя льготы и субсидии начинающим бизнесменам. Однако многие программы поддержки, разрабатываемые государством, являются неэффективными на практике ввиду ряда причин. Поскольку формирование малого предпринимательства происходит на муниципальном уровне, особую роль в развитии МСП играет местная власть, которая далеко не всегда заинтересована в поддержании свободных рыночных отношений и «здоровой» (совершенной) конкуренции. Однако, как показывает практика, властные ресурсы далеко не всегда принадлежат чиновникам – представителям Администрации. Ввиду этого, в работе рассматриваются не только формальные механизмы взаимодействия местной власти и МСБ, но и неформальные, поскольку к местной власти относятся не только представители Администраций муниципальных образований, но и лица, входящие в «теневые руководящие сообщества». Состав сообществ определяют многочисленные факторы: например, историческое прошлое, экономико-географическое положение, наличие крупных предприятий в муниципальном образовании и количество конкурентов и др.

Цель данного исследования – выявить и проанализировать формальные и неформальные механизмы взаимодействия местной власти и представителей малого и среднего предпринимательства региона, а также разработать управленческие рекомендации по повышению эффективности взаимодействия власти и бизнеса.

Гипотеза исследовательской работы предполагает, что, ввиду институционального дефицита в сфере взаимодействия бизнеса и власти, произошла деформация системы власти на местном уровне, которая приводит к непрозрачности и ситуативности правил взаимодействия.

Изучение проблемы проходило в два этапа: кабинетный и полевой.

Методология исследования предполагает сравнительно-сопоставительный анализ на основе глубинных интервью (50 штук: из них 8 взято у представителей администрации, 42 – у представителей малого и среднего предпринимательства), собранных автором работы и коллегами-участниками экспедиции, и наблюдении (включенном наблюдении на правах коренного жителя города и наблюдении коллег-участников экспедиции). Изучению подлежали малые, средние и большие города, а также близлежащие станицы и поселки. Ввиду необходимости следования этическим нормам соблюдается строгая анонимность опрошенных респондентов.

Прежде всего, стоит отметить, что все исследуемые южные города роднят между собой некие общие черты: во всех муниципальных образованиях хорошо отлаженные тесные неформальные связи, что позволяет развиваться промыслам, гаражной, теневой экономике (как серой, так и черной) и реципрокному обмену. Населенные пункты относительно небольшие, ввиду чего все друг друга хорошо знают. в основном все населенные пункты живут за счет отдыхающих в период с конца весны и до поздней осени. Пик сезона приходится на июль-август. Ввиду этого, самое широкое распространение имеют гостиничный, ресторанный, туристический и развлекательный бизнесы. Как правило, на деньги, вырученные за сезон, живут весь год. Основными видами промыслов можно назвать виноградарство, рыболовство, пчеловодство, производство товаров народно-художественного творчества, выращивание и реализацию с-х. продукции, сезонное собирательство ягод и съедобных плодов, садоводство, травничество, ремонт техники и др. в разных районах промыслы имеют различную степень развития. Крупные сетевые ритейлерские магазины постепенно вытесняют мелких частных предпринимателей. Со стороны последних поступают жалобы относительно низкого спроса и невозможности конкуренции. При этом в межсезонье широко развиты отходничество и маятниковая миграция на предприятия в близлежащие более крупные и развитые населенные пункты. Кроме того, развиты проституция, браконьерство и наркотрафик.

Для лучшего понимания функционирования экономики были проанализированы формальные и неформальные механизмы взаимодействия местной власти и представителей малого и среднего предпринимательства региона. Прежде всего, необходимо отметить, что под местной

властью подразумевается не только формальная/официальная, но и фактическая (те, в чьих руках расположены властные ресурсы на практике). Были выявлены и проанализированы возможные варианты расстановки сил на территориях и зависимую (взаимозависимую) от этого структуру местной экономики. Таким образом, в ходе исследования были выявлены 4 типовые модели взаимодействия (описание конкретных локальных архитектур власти).

Модель 1. (Родовые общины — МСП)

От большинства среднерусских городов южные отличаются тем, что там присутствуют казаки и сильны национальные общины. На территории города-курорта таковыми являются армяне и греки. Они, вкупе с казаками, представляют собой силы, существенным образом влияющие на жизнь города. С общинами вынуждены считаться все, а их главы обладают серьёзным административным ресурсом. Многие крупные предприниматели являются греками или армянами. Национальные общины создают невозможность создания бизнеса обычных гражданам, не принадлежащим к «руководящему клану». Методами воздействия разнообразны: от запугивания, рейдерского захвата и «сбора дани» до применения «грубой силы». Несогласные и неугодные подлежат физической ликвидации. Администрация является промежуточным звеном и «марионеткой» местной национальной общины, с одной стороны, и высокопоставленного чиновника регионального уровня, с другой. в настоящее время казачье сообщество и национальная община состоят в конфронтации, что приводит к переделу собственности и стычкам. Чтобы контролировать муниципальные образования края, приобрести над ними власть и получать административную ренту, чиновник регионального уровня Краснодарского края способствовал возрождению казачества, тем самым нашел серьезную поддержку в их лице (как говорят в крае, создал «свою армию»). Таким образом, город и местные предприниматели либо принадлежат к одной из двух противоборствующих сил, либо подконтрольны им и вынуждены подчиняться и платить ренту, тем самым получая покровительство.

Модель 2. (Силовые структуры — МСП)

В другом районе края власть принадлежит представителям государства (МВД, таможенники, представители администрации, судья муниципалитета), распоряжающиеся административными и силовыми ресурсами в личных целях. Район поделен на зоны, где каждое «руководящее сообщество» отвечает за свой участок («крышует» и контролирует). Форма отношений представлена в виде «административной ренты». Стоит заметить, что район является очень криминализированным ввиду того, что там процветают нелегальные виды предпринимательской активности, такие как проституция, браконьерство, незаконная продажа алкогольной продукции и торговля наркотиками (возможно, причиной тому является наличие многочисленных портов). Однако при этом, район занимает 4-ое место по объёму доходов в консолидированный бюджет Краснодарского края (после крупных городов) - 10 млрд. рублей. Ввиду чего можно сделать вывод, что из рассматриваемых моделей, данный тип взаимодействия является наиболее эффективным и выгодным для края.

Модель 3. (ОПГ — МСП)

Данный район считался криминальным еще с 80-х годов. Первые деньги руководящей семье удалось «поднять» на инновациях: кооператив занимался производством молдингов — самоклеющихся резиновых накладок, новинку закупали по всей России. Кооператив выкупил небольшой участок земли, где был построен спортзал, в котором тренировались первые боевики. в 90-х стали происходить первые аферы с землей, запугивание коммерсантов и фермеров (несколько человек убито). Глава ОПГ заручился поддержкой у краснодарских и ростовских воров, наладил связи с главами администраций, юстиции, налоговой и МВД. Те, в свою очередь, получали адми-

нистративную ренту. Механизмы воздействия на предпринимателей: запугивание, применение грубой силы, рейдерский захват, сбор «дани».

Модель 4. (крупный предприниматель — МСП)

Бизнесмен самого крупного предприятия муниципального образования состоит в тесных неформальных связях с главой и другими представителями администрации. Они являются взаимозависимыми и пребывают в мирных взаимовыгодных отношениях, однако «правила игры» устанавливает бизнесмен, поскольку обладает большими властными и материальными ресурсами. Для жителей муниципального образования предприниматель предстает в образе благодетеля и социально-ответственного бизнесмена, финансово помогает главе решать проблемы, поскольку муниципального бюджета на них не хватает. в свою очередь, администрация создает административные барьеры конкурентам предприятия, не пускает новых игроков на рынок и не предоставляет возможности развиваться существующих. Все бюрократические вопросы владельца крупного предприятия решаются Администрацией без промедления, при этом на многие вещи и беззаконье чиновники «закрывают глаза».

Рекомендации

Таким образом, в ходе исследования было проанализировано, какие акторы могут выступать в качестве местной власти в широком смысле), влияние каждой из них на состояние и дизайн местной экономики. Широкое распространение нетиповых локальных рынков власти в общем-то и позволяет сделать вывод о том, что централизованные институты и их внедрение государством не состоялись, то есть, подтвердить гипотезу работы).

Проанализированная ситуация говорит о том, что дисфункции возникают в силу непрозрачности и чрезмерной сложности устанавливаемых государством правил игры для субъектов МСБ, а также чрезмерного человеческого фактора. Следовательно, нужно упростить правила игры и максимально исключить роль отдельных персоналий. Этому может поспособствовать внедрение современных информационных технологий. Так, профильные исследования подтверждают, что сборы ренты с бизнеса несколько снизились после внедрения Федеральной налоговой службой личных кабинетов физических и юридических лиц – люди стали видеть свои задолженности и прочие сведения в онлайн режиме в централизованной системе, это снизило асимметрию информации и элиминировало некоторые каналы давления со стороны сотрудников контрольных и силовых органов.

Для решения проблем, выявленных при исследовании вопроса, и перехода к цивилизованным механизмам взаимодействия бизнеса и власти необходимо принять радикальные меры. Прежде всего, необходимо желание властей изменить принцип функционирования устоявшейся системы. Частично и в долгосрочном периоде проблему теневой экономики возможно решить посредством перехода на цифровую экономику, которая потенциально может предоставить огромные возможности для развития МСП. Подобная трансформация способна стать ключом к решению ряда основных проблем, а именно она позволит:

1. преодолеть административные барьеры и повысить заинтересованность в участии в муниципальном заказе;
2. устранить проблему асимметрии информации;
3. вывести «из тени» большую часть представителей МСП;
4. «канализировать», сделать формальными и прозрачными механизмы взаимодействия МСБ и государства и тем самым минимизировать уровень коррупции.

Производить трансформацию необходимо поэтапно и продуманно. Однако, прежде чем осуществлять переход на цифровую экономику, необходимо: 1. Упростить и довести до бизнеса «правила игры» 2. Произвести фактическое внедрение электронного правительства. 3. Преодолеть вызовы, стоящие перед государством в связи с имплементацией цифровых изменений.

При этом рекомендации по переходу к цифровой экономике будут приемлемы лишь для 2 и 4 моделей, в которых отсутствуют ОПГ и родовые общины, применяющие грубую силу для решения проблем. Бороться с ними необходимо иными (силовыми) методами (лишить властного ресурса и осуществить правосудие). Безусловно, проблемы государственного управления, существующие в стране веками, и устоявшихся механизмов взаимодействия цифровой экономикой не решить. Ввиду этого, необходимо разработать новую модель G2B (модель сотрудничества МСП и власти), где цифровые технологии будут играть одну из первостепенных ролей, поскольку позволят сделать механизмы взаимодействия открытыми и прозрачными.

Список используемой литературы

1. Барсукова С. Ю. Эссе о неформальной экономике, или 16 оттенков серого. (М.: ВШЭ, 2015)
2. Барсукова С. Ю., Радаев В. В. Неформальная экономика в России: краткий обзор // Экономическая социология. 2012. Т. 13. No 2. С. 99-111.
3. Волков В.В. Силовое предпринимательство: экономико-социологический анализ. М.: Изд. дом ГУ ВШЭ, 2005.
4. Ладыгин В.В. Поддержка малого бизнеса на муниципальном уровне в России: основные этапы и тенденции // Вопросы государственного и муниципального управления. 2010. No4. С. 32-49.
5. Плюснин Ю. М., Слободской-Плюснин Я. Ю. Короткий список претензий: неотложные вопросы малого бизнеса к власти // в кн.: Дезурбанизация и природный капитал: миграционные тренды, инфокоммуникация и новые сельские поселения / Под общ. ред.: Н. Е. Покровский, Т. Г. Нефедова. М.: [б.и.], 2013. Гл. 7. С. 159-179.
6. Сухова А. С., Гладникова Е. В., Нагерняк М., Рощина Я. М. Неформальная эко- номика в российских домохозяйствах в первой половине 2000-х: домашний труд, агропроизводство и межсемейные трансферты / Рук.: Я. М. Рощина; отв. ред.: Н. В. Андрианова; под общ. ред.: В. В. Радаев; науч. ред.: В. В. Радаев. Вып. 12. М.: Издательский дом НИУ ВШЭ, 2013.
7. Чепуренко А. Ю. Совмещая универсальные концепции с национальной спецификой: Поддержка малого и среднего предпринимательства // Вопросы государственного и муниципального управления. 2017. No 1. С. 7-30.
8. Чепуренко А. Ю. Возможности и перспективы развития предпринимательства в России (перечитывая современных классиков теории предпринимательства) // в кн.: Современные классики теории предпринимательства / (под ред.: А. Ю. Чепуренко). М.: Издательский дом НИУ ВШЭ, 2013. Гл. 17. С. 497-526.

ЧЕРНОБАЙ МАРИНА СЕРГЕЕВНА
студентка факультета социальных наук
НИУ ВШЭ, г. Москва
E-mail: mschernobay@edu.hse.ru

ОТЕЧЕСТВЕННАЯ ПРАКТИКА ЗАЩИТЫ БИЗНЕСА ОТ РЕЙДЕРСКИХ ЗАХВАТОВ

CHERNOBAI MARINA SERGEEVNA
student, faculty of social sciences
National Research University «Higher School of Economics», Moscow

RAIDER SEIZURES PROTECTION FOR BUSINESS IN RUSSIA.

Аннотация: В работе анализируется проблема защиты бизнеса от рейдерства (недружественных поглощений). Упор делается на рассмотрение и выявление определенные особенности отечественных недружественных поглощений и систем безопасности от данного рода захватов. Данные, представленные в статье, построены на следующих эмпирических методах исследования: изучение и анализ литературы, информации из СМИ, статистических данных и исследований других авторов. На основе анализа делается вывод о том, что проблема рейдерства в России стоит весьма остро. При возрождении в России предпринимательства, появились и предпосылки для феномена таких захватов, парадигма которого стала уже императивом для российского бизнеса. Борьбу с рейдерством в России нельзя назвать успешной ввиду халатного отношения предпринимательства и правовых структур к данной проблеме. Бороться с проблемой поможет изменение этого отношения и разумное использования комплексных мер.

Abstract: The paper analyzes the problem of protecting a business from raiding (hostile takeovers). The emphasis is on the consideration and identification of certain features of hostile takeovers in Russia and security systems from this type of seizure. The data presented in the article is based on the empirical research methods: study and analysis of literature, information from the media, statistical data and studies of other authors. Based on the analysis, it is concluded that the problem of raiding in Russia is very acute. Prerequisites for takeovers appeared after the beginning of entrepreneurship revival in Russia. Paradigm of such phenomenon has already become imperative for Russian business. The fight against raiding in Russia cannot be called successful due to the negligent attitude of entrepreneurship and legal structures to this problem. A change in this attitude and the wise use of integrated measures will help to combat the problem.

Ключевые слова: рейдерство, защита бизнеса, российское предпринимательство.

Key words: raiding, business protection, Russian entrepreneurship.

Введение

На сегодняшний день в современной России проблема защиты от рейдерства (недружественных поглощений) бизнеса становится все более актуальной. в разрешении данной проблемы заинтересованы не только экономисты, но и даже руководство страны.

В нынешних экономических условиях каждый предприниматель не должен забывать, что в любой момент может наступить такая ситуация, когда риск потерять свой бизнес оказывается очень велик, поскольку с каждым годом схемы рейдерского захвата изменяются и совершенствуются, подстраиваются под изменчивые экономические условия. Они все сильнее становятся завуалированными, что усложняет процесс признания этих действий незаконными, а следовательно

наказание становится практически невозможно. Тем не менее, рациональное применение технологий по противодействию рейдерству способно предотвратить нападение. Также следует всегда помнить, что предотвратить угрозу намного проще, чем бороться с ней, однако, несмотря на это, в России система превентивной безопасности остается недооцененной, что также влечет за собой ряд дополнительных проблем. Особенно остро эта угроза стоит для малого и среднего бизнеса.

В Интернете имеется множество статей и новостных обзоров по поводу случаев недружественных слияний. и таких случаев в России описано большое количество. Актуальность проблемы также подтверждает большое количество научных работ отечественных исследователей. в работе Ельмеевой (2013) подробно разбираются виды рейдерских захватов, методы захватчиков и методы защиты от них. Приводится статистика и динамика рейдерских захватов в России, которая с каждым годом все растет. Сажнев (2010) и Кисилев (2013) больший упор делают на методы защиты, в частности превентивные [Кисилев, 2013]. в работе Староверова (2010) приводится опрос предприятий АПК касаемо явления рейдерских захватов (оценка возможностей для борьбы, благоприятные факторы для рейдерства, системы защиты). Результаты вышеописанных исследований легли в основу данной работы. Для более полного раскрытия темы использовались данные из учебной литературы (Шульц, 2018) и данные о конкретных случаях недружественных захватов.

В данной работе объектом является рейдерский захват, предметом - отечественная практика защиты бизнеса от рейдерских захватов.

Цель работы: выявить определенные особенности отечественных недружественных поглощений и систем безопасности от данного рода захватов. Для этого выполняются следующие задачи:

1. Объяснить, что представляет собой рейдерский захват в общем понимании.
2. Изучить риски и методы защиты при рейдерских захватах.
3. Проанализировать случаи рейдерских захватов в России.

1. Сущность рейдерского захвата.

Рейдерский захват представляет собой «процесс поглощения предприятия обманным методом, против воли его собственника, в результате чего захватчики приобретают контроль над активами предприятия и продают их». [Ельмеева, 2013] Обычно рейдерство подразделяют на три вида: «белое», «серое» и «черное».

«Белое» рейдерство происходит в рамках закона и в основном сводится к корпоративному шантажу. При «белом» рейдерстве используются квазизаконные методы такие, как организация забастовок, проверки контролирующими органами, использование пробелов в законодательстве. с таким видом рейдерства обычно сталкиваются компании с проблемами финансового характера или слабым корпоративным управлением. За защитой от такого вида рейдерства можно обратиться в судебные и административные органы.

«Серое» рейдерство совмещает применение квази-законных и незаконных методов, которые влекут за собой нарушение гражданско-правовых норм. Среди таких методов можно выделить следующие: подкуп судей и других должностных лиц, подделывание документов, шантаж контрагентов для создания ситуации невозможности продолжения деятельности. Такие схемы применимы для любого вида бизнеса, а защита от «серого» рейдерства очень сложна, поскольку действия данного характера производятся под прикрытием несовершенства законодательства и признать их противоправными становится трудно.

«Черное» рейдерство подразумевает явное использование незаконных способов: подкуп, шантаж, силовой вход на предприятие, подделка реестра акционеров и судебных решений и т. д. Также применим к любой компании, особенно непубличной. Защита от такого рейдерства реализовывается всеми допустимыми способами, в первую очередь в правоохранительных и судебных службах. [Ельмеева, 2013], [Шульц,2018]

Среди методов и признаков рейдерского захвата можно выделить: силовые акции, смена ох-

раны, взлом замков, психологическое давление («гринмейл»), банкротство, привлечение местных или федеральных властей, операции с акционерным капиталом, наемное руководство, оспаривание приватизации и прочее. [Ельмеева, 2013]

2. Риски и методы защиты от рейдерских захватов.

В России практика рейдерства весьма распространена и связана с определенными угрозами безопасности: повышение уровня безработицы, усиление коррупции государственных служащих и судей, уклонение от уплаты налогов, монополизация ряда сегментов рынка, потеря конкурентоспособности, спад производства, падение авторитета власти и правовой идеологии, правоохранительных органов и судов, ухудшение инвестиционного климата, активизация процессов отмывания денег, полученных преступным путем. Из целого ряда разнообразных негативных последствий рейдерство следует вывод, что противоборство рейдерству имеет как экономическое, так и правовое и политическое значение для государства. [Кисилев, 2013]

Более того, около 90% отечественных случаев рейдерства обременено множеством правонарушений: угроза убийством или причинением тяжкого вреда здоровью, похищение человека, мошенничество, вымогательство, злоупотребление полномочиями, нарушение тайны переписки и многими другими. [Староверов, 2010]

Так как любой бизнес в России имеет высокую вероятность рано или поздно столкнуться с угрозой недружественного поглощения, необходимо выстраивать правильную тактику и систему защиты в таких ситуациях. Классическая структура защиты от рейдерства представлена на рисунке 1:

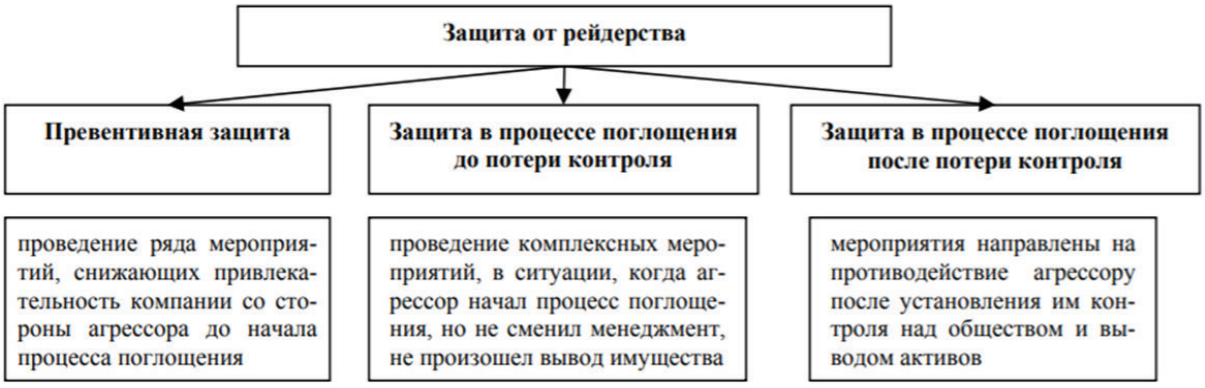


Рисунок1. Структура видов защиты от рейдерства предпринимательских структур. Источник: Схема А.Н. Сажнева на основе исследования Биджакова Э.В.: Биджаков Э. В. Место и роль недружественных поглощений в процессе совершенствования экономической политики государства // Социально-экономические явления и процессы. 2008. №4.

Сама по себе защита от рейдерства представляет собой систему правовых, административных, социальных и других механизмов, усложняющих переход контроля над предприятием рейдером.

В том случае, когда процесс поглощения уже начался, специалисты охранных служб используют следующие методы для оказания противодействия рейдерам: реструктуризация активов и препятствование массовой скупке акций, защита реестра акционеров и коммерческой тайны, ответное использование методов рейдера в рамках закона против него самого, организация физической защиты объекта, руководства и его семей.

Очевидно, что лучше до таких моментов не дотягивать, а предотвращать проблему еще в ее корне, используя превентивные меры, так как эти методы считаются наиболее эффективными. Превентивные меры направлены на минимизацию риска захвата и совершенствование корпоративной защиты. к таким мерам можно отнести систематический информационный мониторинг для отслеживания заинтересованности компаний-агрессоров, проведение реструктуризации бизнеса (преобразование обособленных подразделений компании в независимые юрлица, фор-

мальное изменение собственников активов или их диверсификация, применение механизмов перекрестного владения), изменение учредительных и других документов бизнеса, защиту инсайдерской информации, мониторинг и управление кредиторской задолженностью, мотивационная политика для наемных сотрудников для развития производственной деятельности и, наконец, защита владельцев от утраты или хищения акций. [Сажнев, 2010]

К сожалению, российские предприниматели зачастую пренебрегают этими мерами, ввиду их высокой стоимости и своего халатного отношения к угрозам безопасности предпринимательской структуры. Более того, статистика за 2010 год, представленная в таблице 1, касаемо защиты от рейдерских захватов, выглядит весьма печально:

Таблица 1. Наличие на предприятии системы защиты от рейдерских захватов, в %. Источник: Данные опроса ассоциации менеджеров и данные опроса предпринимателей АПК при участии Староверова В.В.

Представляют бизнес	Имеется	Нет	Есть ее элементы
Крупный *	21,8	76,4	1,8
Средний	11,5	87,9	0,6
Малый	---	100,0	---
Семейный	---	100,0	---

Источник: *Данные опроса Ассоциации менеджеров; данные опроса предпринимателей АПК.

Согласно представленным данным, можно понять, что ни один семейный или малый бизнес не имеет систем защиты против рейдерских захватов, а ситуация в крупном и среднем бизнесе оставляет желать лучшего – только 21,8% и 11,5% предприятий соответственно имеют систему защиты, а 1,8% и 0,6% только ее элементы, тогда как огромная доля предприятий функционирует вообще без подобных систем безопасности. Положение государственных и кооперативных предприятий можно приравнять к положению семейного и малого бизнеса, поскольку первые возлагают слишком большую надежду на защиту их предприятий официальными институтами. [Староверов, 2010]

Государство, со своей стороны, пытается бороться с рейдерскими захватами правовым методом, внося поправки в Уголовный Кодекс. Как результат, поправки дали возможность сотрудникам правоохранительных органов устранять рейдерские атаки на первых этапах. Более того, интерес рейдеров переместился на предприятия малого бизнеса, а суммы ущерба уменьшились. [Кисилев, 2013]

Несмотря на внесение поправок в УК РФ с целью конкретизации составов преступлений, по которым можно привлекать рейдеров к ответственности, на практике количество рейдерских атак остаётся высоким. [Кисилев, 2013] Стоит еще отметить тот факт, что, захватывая предприятие, рейдеры никогда не проигрывают, поскольку многочисленные судебные разбирательства занимают крайне много времени, за которое рейдеры успевают извлечь из захваченного ими объекта максимум прибыли. [Липов, 2013]

Случаи рейдерских захватов в России

По сей день можно слышать о рейдерских захватах различного характера и исхода в России. По данным Национального антикоррупционного комитета, ежегодно в России происходит около 700 тысяч рейдерских захватов с успешным исходом для рейдеров. Только 10% захвата повлекли за собой возбуждение уголовных дел, а процент дел, по которым ведутся судебные разбирательства еще меньше.

В СМИ можно найти огромное количество примеров рейдерских захватов. По рассказам главного бухгалтера салонов красоты «Сефар» в бухгалтерию стали поступать звонки от якобы представителей департамента поддержки и развития малого предпринимательства, которые хотели выяснить, какова выручка компании, размер налоговых платежей, структура собственников. Логичными действиями в данном случае стали отказ предоставлять подобного рода информацию и игнорирование звонков.

Однако не всегда рейдеры действуют такими мягкими методами, которые можно предотвратить без особых усилий. Захваты часто происходят и в крупном бизнесе с более плачевными последствиями. Так, летом 2003 года столичная компания по производству женской обуви «Аста» стала жертвой силового рейдерского захвата. в здание ворвались вооруженные люди, выгнали всех сотрудников на улицу и объявили им о том, что у компании теперь новый директор.

Выяснилось, что 80% акций миноритариев было продано компании «Росбилдинг» за полгода до инцидента. Более того, «Росбилдинг» уже появлялся в рейдерских сводках, а ее директор считался одним из первопроходцев отечественного рейдерства. в результате мажоритарии попытались спасти ситуацию. Они смогли размыть долю захватчиков до 3% путем допэмиссии. Судебные разбирательства по данному делу длились год, и, в итоге, компания была возвращена владельцам.

Среди громких историй рейдерских захватов стоит также упомянуть дело об аэропорте «Домодедово», захват НИИЭМИ, захват колхозов в Рузском районе и другие. и не все из них имели счастливый конец, поскольку каждая ситуация уникальна и для каждой ситуации необходима своя стратегия и система безопасности.

Заключение

Исходя из проведенного анализа, можно сделать вывод о том, что проблема рейдерства в России стоит весьма остро. При возрождении в России предпринимательства, появились и предпосылки для феномена таких захватов, парадигма которого стала уже императивом для российского бизнеса. Такие процессы выводят российское предпринимательство за рамки цивилизованного мирового рынка, а также влекут за собой широкий ряд негативных последствий для всех сфер жизни общества.

Борьба с рейдерством в России протекает с трудом, что также усугубляется тем фактом, что универсальной защиты от рейдерских атак не существует. Приведенные в данной работе превентивные меры лишь снижают шансы захватов на успех. Однако, если эти меры не применять своевременно, либо осуществлять их непрофессионально, то при атаке, возлагать большие надежды на другие защитные меры уже не стоит. Отсюда следует вывод, что только своевременное и умелое применение определенных мер может спасти бизнес от поглощения, но, исходя из российских особенностей, необходимо менять и само отношение предпринимательства и правовых структур к данной проблеме.

Список литературы

1. Ельмеева И. Г. Практика рейдерских захватов в России // Проблемы и перспективы экономики и управления: материалы II Междунар. науч. конф. (г. Санкт-Петербург, июнь 2013 г.). СПб.: Реноме, 2013. С. 10-12.
2. Киселев Н. С. Превентивная защита от рейдерских атак // Национальная безопасность. 2013. № 1 (24). С. 171—178
3. Липов А. Н. Рейдерство как социально-экономический феномен (к теории и практике российских захватов) // Экономическая и философская газета. 2013 № 27 (969). С. 3

4. Методы защиты от рейдеров // URL: https://fd.ru/articles/38296-metody-zashchity-ot-reyderov (дата обращения: 19.04.2019).
5. Профессиональная защита от рейдерского захвата: современные методы и способы, применяемые ЧОП // URL: https://www.legis-s.ru/clients/articles/professionalnaya-zashchita-ot-reyderskogo-zakhvata-sovremennye-metody-i-sposoby-primenyaemye-chop/ (дата обращения: 19.04.2019).
6. Рейдерские захваты организаций, компаний, предприятий // URL: https://m16-consulting.ru/articles/reyderskie-zakhvaty-organizaciy / (дата обращения: 19.04.2019).
7. Сажнев А. Н. Возможности противодействия рейдерству: комплекс экономических мер и мероприятий предпринимательских структур // Социально-экономические явления и процессы. 2010. №4.
8. Староверов В. В. Рейдерство. Недружественный захват предприятий // Мониторинг. 2010. №1 (95).
9. Шульц, В. Л. Безопасность предпринимательской деятельности в 2 ч. Часть 1: учебник для академического бакалавриата / В. Л. Шульц, А. В. Юрченко, А. Д. Рудченко; под ред. В. Л. Шульца. Москва: Издательство Юрайт, 2018. 288 с.

ШАСТИНА ЕКАТЕРИНА СЕРГЕЕВНА
студентка факультета экономики
НИУ ВШЭ, г. Москва
E-mail: eshastina@edu.hse.ru

СОВРЕМЕННЫЕ ОФФШОРНЫЕ ЗОНЫ В ВЕЛИКОБРИТАНИИ

SHASTINA EKATERINA SERGEEVNA
student, faculty of economics
National Research University Higher School of Economics, Moscow

THE MODERN OFFSHORE ZONES IN THE UK

Аннотация: Великобритания – это страна с интересной и довольно богатой историей. Государство занимает пятое место по темпам развития экономики. Также Великобритания состоит во многих международных организациях. Великобританию действительно можно назвать «родиной оффшорного бизнеса». Именно там берут начало все существующие на сегодняшний день системы оффшоров. Да и само понятие оффшор также родом из Великобритании. Что же такое оффшор? Оффшор – это территория с определенными, можно сказать особенными, условиями ведения бизнеса для иностранных компаний. Особенность заключается в том, что для этих компаний присущи низкие или вовсе нулевые налоги, более простая финансовая отчетность, а также можно скрыть настоящего владельца той или иной организации. Иными словами, регистрируя оффшорные компании, можно минимизировать налоги на деятельность компании.

Abstract: Great Britain is a country with an interesting and quite rich history. The state takes fifth place in terms of economic development. Also, the UK is a member of many international organizations. The Great Britain actually can be called the “motherland of the offshore business”. The existed systems of offshore begin take the beginning exactly there. The definition of offshore also is from Great Britain. What is offshore? Offshore is a territory with certain and perhaps special conditions of managing business for foreign companies. The feature is consisted in low or zero taxes for these companies. Moreover, the specificity is in simple financial statements and hidden real owner of this or that organization. In other words, you can minimize taxes on the activities of the company by registering offshore companies.

Ключевые слова: Оффшорные зоны, бизнес, LTD, LLP, низкие налоги, репутация.

Key words: offshore zones, business, LTD, LLP, low taxes, reputation.

Введение

Привлекательность Великобритании в том, что это страна с высокой репутацией и она хорошо принимается в качестве партнера для ведения бизнеса во всем мире. Британия подписывает довольно большое количество договоров с другими странами, в том числе и с Россией, об избежании двойного налогообложения.

По данным аналитиков, экономика Великобритании является одной из самых устойчивых, а среди клиентов банков этой страны есть самые богатые люди нашей планеты. Несмотря на все то, что происходит сейчас в мире, регистрация компаний в оффшорных зонах Великобритании всегда выгодна и на ее территории вести свой бизнес более безопасно. Если зарегистрировать компанию на территории этой страны, то сразу можно получить статус чистой перед законом фирмы, с которой выгодно сотрудничать.

Основная часть

Англия является довольно перспективной зоной для того, чтобы вести бизнес. Можно выделить три основные причины. Во-первых, экономическая и политическая ситуация настолько стабильны, что с ней не сравнятся другие оффшорные зоны. Доверие, которое идет со стороны финансово кредитных организаций, позволяет выходить фирмам на более высокий уровень развития. Во – вторых, зарегистрировать компанию можно довольно быстро и относительно легко, обычно это происходит в течение суток, в режиме онлайн. в интернете можно ознакомиться с законодательными актами и прочитать объяснения к ним. в – третьих, система налогообложения считается одной из самых простых и понятных. На законных основаниях можно уменьшить величину налога. Если прибыль компании меньше, чем 10 000 фунтов стерлингов, то налог и вовсе не уплачивается. а если прибыль больше, чем 10 000 фунтов стерлингов, то ставка налога возрастает до 30%.

Среди преимуществ оффшорных зон Великобритании можно выделить и недостатки. Во – первых, это необходимость в предоставлении финансовой отчетности, которая заверена аудитором. Даже если компания маленькая, финансовая отчетность все равно необходима, но вот аудит можно не проводить. Также всю информацию необходимо предоставлять в строго оговоренные сроки, иначе это влечет за собой штрафные санкции. Во – вторых, банки Великобритании не любят работать с формально зарегистрированными компаниями, которые ведут свою деятельность в других странах.

Но на фоне всех преимуществ, недостатки считаются незначительными. Регистрация компании в оффшорных зонах Британии – это идеальная деловая репутация, престиж компании, большие возможности, надежное вложение денежных средств, а также уверенность в завтрашнем дне.

По рейтингу, составленным Мировым банком, Великобритания занимает седьмое место по простоте ведения бизнеса, Главное преимущество – доступность кредитования, достаточно высокий уровень защищенности прав всех инвесторов, простота ведения торговли между странами, а также легкость процедуры регистрации компаний.

В Великобритании есть возможность зарегистрировать два вида оффшоров: LTD (Private Limited Company) и LLP (Limited Liability Partnership). LTD – резидентная компания Великобритании. Компания такого типа может получить номер плательщика НДС. Организация должна обязательно платить налог 20 – 25%, в зависимости от прибыли. LLP – оффшор в Великобритании. Этот тип является нерезидентным. Не платит налоги в Великобритании, нет требований для уставного капитала. Аудиторская проверка необходимо только для крупных фирм. Информация находится в открытом доступе.

По некоторым источникам, Великобритания не является оффшорной зоной, в ней просто налогообложение лояльно по отношению к фирме. По показателю простоты системы налогообложения Великобритания уступает только некоторым странам: Мальдивы, Катар, Гонконг, Бахрейн и Люксембург. Организации, создаваемые в Великобритании, могут на протяжении длительного периода времени подавать нулевые отчеты. То есть, может иметь нулевую деятельность и вовсе не вести торговую деятельность на территории Британии. Но несмотря на нулевой статус, ликвидировать компанию контролирующие органы не могут. Если же компания ведет какую – либо деятельность, то на уплату налогов у нее в распоряжении есть девять месяцев. Основным видом налога для Великобритании считается корпоративный налог. Это тот налог, когда ставка зависит от размера прибыли. в последнее время ставка корпоративного налога значительно уменьшилась, что сделало налоговую политику Великобритании привлекательнее. Этим правительство страны показывает заинтересованность в развитии бизнеса в Великобритании.

Правительства некоторых стран создают офшоры, так как они приносят дополнительный доход в бюджет государства. Есть несколько видов офшорных зон.

По налогообложению. Главная причина, по который предприниматели оформляют свой бизнес в оффшорах – это низкий уровень налогов. в некоторых зонах можно и вовсе не платить налоги. Следовательно, предприниматель получит более высокую прибыль. Основываясь на закон о компаниях 1985 года и закон о компаниях 2006 года, для юридических лиц существует три

типа организационно – правовых форм. Первый – это компания открытого топа. Преимущество такой компании в том, что акции могут обращаться на биржах и могут быть предложены к продаже большому количеству инвесторов. Второй тип – компания с неограниченной ответственностью. Ну и третья, наиболее часто используемая – компания с ограниченной ответственностью. Требования ограничены лишь взносами владельцев, нет определенных требований к уставному капиталу. Это компания может развивать свою деятельность в любом направлении.

По законодательной среде. Если предприниматель регистрирует свой бизнес на территории другого государства, то он соглашается с условиями, которые прописаны в законодательстве этой страны. Данная среда разделяет зоны на три крупные классификации. Во – первых, по порядку регистрации бизнеса свободные (необходимы только заявлении и копии учредительных документов) и формальные (требуется ряд дополнительных бумаг). Во – вторых, по характеру проверки отчетности. и в – третьих, по степени конфиденциальности (зоны с открытым, умеренным и закрытым реестрами).

По лояльности к субъектам. Когда предприниматель выбирает офшор для того, чтобы разместить там головной офис, он выбирает не только выгодные условие, но и хорошую репутацию страны. Для того, чтобы получить место в довольно престижной стране, иногда приходится идти на некоторые уступки. По степени лояльность офшоры делятся на: классические, престижные и оншорные зоны. Классические территории офшора – они часто могут стать убежищем нелегальных финансовых сделок и операций, даже несмотря на их высокую привлекательность. Престижные офшорные зоны – высоко ценятся иностранными бизнесменами, необходима финансовая отчетность. Оншорные зоны – не являются офшорами, но имеют право предоставить иностранным предпринимателям некоторые льготы, более простой способ регистрации и конфиденциальность.

Рейтинг популярности. Предпринимателям, которые регистрируют свою фирмы впервые, стоит ознакомиться с рейтингом популярность данной оффшорной зоны.

Заключение

Таким образом, оффшорные зоны в Великобритании – это отличная возможность не уплачивать крупные налоговые отчисления, а также предостеречь свой бизнес от частых проверок государственных органов. в большинстве случаев, офшоры подходят для бизнеса среднего размера, который с одной стороны работает как юридическое лицо и должен платить налоги, а с другой стороны он имеет ограниченный бюджет.

По мнению многих людей, офшор – это зона, освобождающая от налогов. Правды в этом немного, так как существуют различные зоны торговли. Есть те, которые считаются более престижными. а есть другие, в которых просто создаются благоприятные схемы налогообложения для иностранных инвесторов. Участие компании в различных налоговых схемах может помочь сократить ставки налога.

Список литературы:

1. Авдокунин Е.Ф. Международные экономические отношения. -М: Юристъ, 2005.
2. Е.В. Локатарева, «Международное налогообложение и оффшорные центры», Москва, 2008 г.
3. 3. Корнеева Е.И. Оффшорный мир. Взгляд изнутри. /М.: Экономика, 2007
4. Троценко А., Дьякова Н. Энциклопедия Оффшорного бизнеса М-2006
5. Троценко А., Карманова Е. Оффшорные компании: обзоры, комментарии, рекомендации М-2007
6. Статья «Великобритания как оффшор: кому в Британии жить хорошо» от 23 октября 2012 года https://delo.ua/businessman/velikobritanija-kak-offshor-kakie-vygody-nashli-tam-ukraincy-187852/
7. Статья «Обзор оффшорной зоны Великобритании» http://taxzilla.info/offshore-great-britain/
8. Статья «Оффшорные зоны» http://ipopen.ru/registracija/offshory/offshornye-zony/

ШУЛЬГИНА ГАЛИНА ИГОРЕВНА
студентка факультета социальных наук
НИУ ВШЭ, г. Москва
E-mail: gshulgina@hse.ru

ОБЗОР ПРОГРАММ ЗАРУБЕЖНЫХ УНИВЕРСИТЕТОВ, ЗАНИМАЮЩИХСЯ ПОДГОТОВКОЙ МАГИСТРОВ ПО ПРОФИЛЮ «ДЕЛОВАЯ (КОНКУРЕНТНАЯ) РАЗВЕДКА»

SHULGINA GALINA IGOREVNA
student, faculty of social sciences
National Research University Higher School of Economics, Moscow

OVERVIEW OF FOREIGN UNIVERSITIES' MASTER PROGRAMS IN THE FIELD OF COMPETITIVE INTELLIGENCE

Аннотация: В рамках данной работы был проведен обзор рынка образовательных услуг в сфере подготовки магистров по направлению «Аналитик конкурентной (деловой) разведки» как пример реализации функции конкурентной разведки. Методология исследования – сбор и сравнительный анализ информации в сети Интернет. В результате исследования был проведен сравнительный анализ содержания двух магистерских программ зарубежных университетов и магистерской программы НИУ ВШЭ в области деловой разведки, выделена их специфика, плюсы и минусы. В качестве критериев для сравнения были выбраны сложность и длительность программы, фокус и цель программы, учебный план, преподавательский состав, профиль студентов и их карьерные перспективы. Практической значимостью данной работы является ее применение сотрудниками Института проблем безопасности НИУ ВШЭ для анализа зарубежных образовательных продуктов, ориентированных примерно на ту же сферу, что и магистерская программа Института.

Abstract: The paper examines the significance of competitive intelligence function in educational services market. In the first section the author describes the theoretical basis, namely the definition, basic principles and approaches of competitive intelligence. Then, in the second chapter, the two chosen foreign universities' master programs are briefly considered, and then a comparative analysis of Russian and foreign educational products is carried out regarding approaches to teaching business intelligence. The research methodology is the collection and comparative analysis of information from the official websites of universities. As a result of the study, a comparative analysis of the contents of two master's programs of foreign universities and the master's program of the HSE in competitive intelligence was carried out, their specifics, pluses and minuses were highlighted. The complexity and duration of the program, the focus and purpose of the program, the curriculum, the teaching staff, the profile of students and their career prospects were chosen as criteria for comparison.

Ключевые слова: деловая разведка, конкурентная разведка, высшее образование

Keywords: competitive intelligence, higher education, master program.

Введение

Рынок образовательных услуг в значительной мере зависит от силы и привлекательности бренда образовательной организации в сети Интернет, поскольку именно этот источник информации, как правило, используют потенциальные студенты для того, чтобы сделать свой выбор. В связи с этим крупные университеты и институты вкладывают значительные средства не только в создание и поддержание удобных и привлекательных информационных ресурсов о себе, но и в

проведение деловой разведки с целью мониторинга высококонкурентной среды.

Магистерская программа «Аналитик деловой разведки» появилась в НИУ ВШЭ в 2018-2019 учебном году. В России не существует аналогичного образовательного продукта, нацеленного на трансфер знаний и выработку компетенций именно в сфере деловой разведки, однако аналогичные продукты есть за рубежом.

В связи с этим автор ставит перед собой следующий исследовательский вопрос: какими характеристиками обладают магистерские программы в сфере конкурентной разведки, реализуемые в зарубежных университетах, и как они соотносятся с магистерской программой НИУ ВШЭ в данной области?

Цель исследования: сравнительный анализ отечественного и зарубежного образовательных продуктов по подготовке магистров в области конкурентной (деловой) разведки в рамках реализации функции деловой разведки.

Задачи исследования:

1. Обзор теоретико-методологических основ деловой разведки, её методов и ограничений;
2. Поиск и отбор терминов, эквивалентных понятию «конкурентная разведка» в английском языке для дальнейшего поиска информации;
3. Поиск и отбор магистерских программ в области конкурентной (деловой) разведки;
4. Поиск и анализ информации о характеристиках отобранных магистерских программ;
5. Сравнение содержания описанных зарубежных образовательных продуктов с отечественной магистерской программой НИУ ВШЭ в данной области, выделение их специфики, плюсов и минусов;

Методология исследования - сбор и сравнительный анализ информации с официальных сайтов университетов, реализующих отобранные магистерские программы, в сети Интернет. В качестве критериев для сравнения были выбраны сложность и длительность программы, фокус и цель программы, учебный план, преподавательский состав, профиль студентов и их карьерные перспективы.

Теоретическая часть

Прежде чем переходить к сбору и анализу информации, необходимо определить понятие конкурентной разведки, а также особенности и ограничения данного процесса.

Так, члены международного Общества профессионалов конкурентной разведки (SCIP) определяют данное понятие как «законный и этический сбор и анализ информации о возможностях, уязвимостях и намерениях конкурентов» [8]. По сути, основной целью проведения конкурентной разведки является повышение конкурентоспособности бизнеса на рынке посредством более глубокого, но однозначно этического понимания конкурентов фирмы и конкурентной среды.

Российское Сообщество практиков конкурентной разведки определяет данное понятие как «комплекс адаптированных к гражданскому обороту методов и приемов работы государственной разведки, направленных на сбор и обработку данных из различных источников, с целью информационной поддержки выработки управленческих решений, проводимых в рамках закона и с соблюдением этических норм (в отличие от промышленного шпионажа); а также результаты деятельности структурного подразделения предприятия, выполняющего эти функции» [8].

Оба приведенных определения ставят акцент на соблюдение этических норм при реализации такого вида деятельности, как конкурентная разведка. Именно соблюдение этических норм является основным отличием конкурентной разведки от такого вида нелегальной деятельности, как промышленный шпионаж, под которым понимают «деятельность по получению сведений, составляющих коммерческую тайну, нечестным путем, например, путем подслушивания телефонных переговоров» [9]. Промышленный шпионаж, как правило, применяется как на уровне государств для обеспечения национальной безопасности, так и на уровне крупных транснациональных корпораций, имеющие достаточные ресурсы для его сокрытия. Конкурентная разведка

является инструментом более мелких организаций (малый, средний и крупный бизнес), а также небольших государств, не имеющих достаточное количество ресурсов. В рамках данной работы будут рассматриваться только деловая (конкурентная) разведка.

Еще одной ключевой характеристикой эффективной деловой разведки является ее непрерывность. В связи с чрезвычайно быстрым устареванием информации и высоким уровнем изменчивости окружающей среды компании (как внутренней, так и внешней) реализация функции конкурентной разведки должна происходить на постоянной основе для поддержки процессов принятия решений.

Также важно еще раз отметить, что все данные, собираемые и анализируемые в рамках деловой разведки, должны быть публичными, т. е. полученными из открытых источников. Данный признак деловой разведки выделяется в зарубежных научных работах [McGonagle& Vella, 2012].

Поскольку автором работы в практической части будет рассмотрена программа зарубежного университета, занимающегося подготовкой магистров по профилю «Деловая (конкурентная) разведка», необходимо найти англоязычные эквиваленты, являющиеся максимально близкими синонимами к понятию «деловая (конкурентная) разведка».

В зарубежной литературе существует множество терминов, так или иначе обозначающих конкурентную разведку: «competitive intelligence, competitor intelligence, business intelligence, strategic intelligence, marketing intelligence, competitive technical intelligence, technology intelligence, and technical intelligence» [McGonagle& Vella, 2012]. Основные различия между ними будут представлены в таблице ниже.

Название термина	**Определение**
Strategic Intelligence	Деловая разведка, поддерживающая принятие стратегических решений. Её результаты используются топ-менеджментом и собственниками организации для создания и реализации стратегии компании.
Competitor Intelligence	Разведка информации о конкурентах. Фокусируется на конкурентах, их возможностях, текущей деятельности, планах и намерениях. Чаще всего используется менеджерами по стратегическому планированию, а также операционными менеджерами в рамках бизнес-единиц.
Market Intelligence	Рыночная разведка фокусируется на текущих действиях на рынке. Обычно используется сотрудниками отделов маркетинга и продаж.
Technical Intelligence	Техническая разведка нацелена на выявление рисков и использование возможностей, связанных с развитием науки и технологий в рамках рынка.
Источник: *John J. McGonagle, Carolyn M. Vella. Proactive Intelligence. Chapter 2. What is Competitive Intelligence and Why Should You Care About it? Режим доступа: https://www.springer.com/cda/content/document/cda_downloaddocument/9781447127413-c2.pdf?SGWID=0-0-45-1299240-p174282177 (дата обращения: 10.03.2019)*	

Также в связи с обилием в разных публикациях понятий, относящихся к деловой разведке, необходимо также отделить те из них, что не относятся к рассматриваемому в рамках данной работы виду деятельности, но также основанных на знаниях.

Согласно статье J. J. McGonagle & C. M. Vella, не относящимся к конкурентной разведке понятиям относятся следующие:

Понятие	***Определение***
Environmental Scanning	Сканирование окружающей среды. Данный термин относится к будущему и подразумевает сбор данных для создания системы раннего предупреждения, а не их анализ для поддержки процесса принятия решений.
Business Intelligence	Бизнес-аналитика. В настоящее время термин используется для обозначения инструментов управления и хранения данных. Данный процесс обеспечивается с помощью программного обеспечения для хранения и работы с данными и инструментами их интеллектуального анализа
Knowledge Management	Управление знаниями. Системы управления знаниями в основном имеют количественную направленность и нацелены на обработку данных с целью узнать что-то о прошлом. Деловая разведка также имеет доступ к людям, что позволяет ориентироваться на будущее. Также обычно данные системы не собирают данные, которые не касаются непосредственно фирмы, и не регистрируют историю принятия решений.
Market Research and Quantitative Research	Исследования рынка фокусируются на конкурентах и собственном взаимодействии фирмы со своими клиентами на исторической основе и в режиме реального времени. Деловая разведка включает более широкий горизонт, например, потенциальных конкурентов, цепочки поставок и распределения, а также исследования и разработки. Также деловая разведка в большей степени использует качественные данные.
Источник: *John J. McGonagle, Carolyn M. Vella. Proactive Intelligence. Chapter 2. What is Competitive Intelligence and Why Should You Care About it? Режим доступа: https://www.springer.com/cda/content/document/cda_downloaddocument/9781447127413-c2.pdf?SGWID=0-0-45-1299240-p174282177 (дата обращения: 10.03.2019)*	

Таким образом, для поиска информации об интересующих программах магистратуры по направлению «Деловая (конкурентная) разведка» мною будет применяться термин «competitive intelligence» как наиболее соответствующих рассматриваемому виду деятельности.

Также необходимо перечислить основные кабинетные и полевые методы конкурентной разведки, на некоторых из которых будет строиться практическая часть данной работы (см. таблицу ниже).

Кабинетные методы работы конкурентной разведки	***Полевые методы работы конкурентной разведки***
1. Интернет (поисковые машины, социальные сети, блогосфера, интернет-форумы, сервисы коммуникаций, изучение сайтов и файлов); 2. СМИ; 3. Официальные отчеты компаний	1. Выставки и конференции; 2. Беседы с людьми; 3. Установление долговременных отношений и привлечение людей к сотрудничеству.
Источник: на основе [1]	

Наконец, необходимо кратко обозначить основные этические принципы, которых аналитики деловой разведки придерживаются в своей работе. Так, согласно этическому кодексу Общества профессионалов конкурентной разведки (SCIP), необходимо:

- «соблюдать все локальные и международные законы;
- избегать конфликта интересов при выполнении непосредственных обязанностей;
- предоставлять честные и отражающие действительность выводы и рекомендации по резуль-

татам работы;
- постоянно стремиться повысить престиж профессии и уважение к ней;
- точно раскрывать всю необходимую информацию как о физ. лицах, так и об организациях;
- продвигать цели и ценности данного Кодекса в компаниях, где трудоустроены аналитики, а также добросовестно соблюдать цели, ценности и принципы Общества» [8].

Таким образом, после определения понятия «деловой разведки», а также ключевых характеристик, методов и этических норм данного процесса в следующем разделе будет описано практическое применение указанных принципов при решении задачи конкурентной разведки в сфере образования на примере анализа образовательной программы зарубежного университета, занимающегося подготовкой магистров по профилю «Деловая (конкурентная) разведка».

Практическая часть

В рамках практической части работы мной будет проведен анализ двух образовательных программ зарубежных университетов, занимающихся подготовкой магистров по профилю «Деловая (конкурентная) разведка».

Название программы		***Кол-во кредитов***	***Описание***
Master of Professional Studies in Applied Intelligence, Georgetown University [3]	Магистр профессиональных исследований в области прикладной разведки	33	Длительность – 2-5 лет; Формат – очно или онлайн; Расписание – полный или неполный день
Master of Science, Applied Intelligence (Erie, Pa), Mercyhurst University [4]	Магистр наук в области прикладной разведки	34	Длительность – 2 года; Формат – очно; Расписание – неизвестно

Джорджтаунский университет демонстрирует лучшее качество образования, поскольку занимает в рейтинге лучших университетов мира (THE Rating) в 2019 г. 30 место в США и 109 место в мире [5]. Для сравнения Университет Мерсихерст занимает 501-600 место по США [6]. Однако ввиду значительных различий в специфике преподаваемых магистерских программ, представляется необходимым изучить оба образовательных продукта.

Обзор будет произведен с помощью кабинетных методов, а именно: анализа информации на официальном сайте университета в целом и магистерской программы в частности.

Образовательная программа Университета Джорджстаун

Общая информация о программе

Согласно официальному сайту, данная магистерская образовательная программа была запущена осенью 2017 г. и готовит слушателей к ориентации в современном высоко изменчивом информационном мире.

Рассматриваемая магистерская образовательная программа фокусируется на следующих четырех направления:

1. **Национальная безопасность;**
   В рамках данного направления студенты приобретут знания о том, как сформировать оценку ситуации на базе деловой разведки и оценить риски национальной безопасности, а также узнают, какова роль технологий в процессе сбора, анализа и обмена разведданными.
2. **Кибер-разведка;**

Студенты получат и усовершенствуют профессиональные навыки по созданию кибер-угроз и их предотвращению, а также научатся управлять операциями с использованием кибер-наблюдения.

3. **Правоохранительная деятельность;**
   Данный блок позволит студентам понять, как разрабатывать и применять основы разведывательных операций для контроля и пресечения организационной преступности и террористической деятельности, получая при этом более глубокое понимание современных проблем правоохранительной деятельности и использования технологий для предотвращения преступной деятельности.
4. **Конкурентная деловая разведка;**
   Студенты узнают о том, как с максимальной эффективностью и результативностью использовать инструменты бизнес-аналитики и деловую разведку для поддержки процессов принятия решений и повышения конкурентоспособности организации.

Интересной особенностью программы является ее гибкость, поскольку предусмотрено как очное обучение в стенах университета, так и изучение онлайн-курсов, что позволяет студентам успешно сочетать профессиональную деятельность и обучение. Продолжительность обучения составляет от 2 до 5 лет в зависимость от степени интенсивности, программа рассчитана на 33 кредита. Преподавание в рамках программы осуществляют ведущие исследователи и практики в данной области, что позволяет студентам ознакомиться с наиболее современными технологиями и подходами деловой разведки.

Учебный план

Для того чтобы получить степень магистра профессиональных исследований в области прикладной разведки, студентам необходимо освоить 11 курсов, составляющих в сумме 30 кредитов. Структура предлагаемых курсов следующая [3]:

1. **2 основных курса** (в сумме на 6 кредитов) – Этика и Базовый интегративный курс/ Проектная работа (capstone;
2. **4 базовых курса** (в сумме на 12 кредитов)
   1) Введение в прикладную разведку;
   2) Психология прикладной разведки;
   3) Прикладные коммуникации в разведке;
   4) Понимание сбора разведывательной информации.
3. **5 курсов по выбору** (в сумме на 15 кредитов) [3].
   a. *Прикладные коммуникации в рамках деловой разведки;*
      Курс направлен на выработку необходимых навыков письменного и устного общения, а также доведения информации до лиц, принимающих решения в области обеспечения правопорядка, *национальной безопасности и конкурентной разведки.*
   2. *Анализ посредством конкурентной разведки;*
      Студенты осваивают сбор организационных данных, их интерпретацию, а также оценку и формирование рекомендаций для совершенствования организационной стратегии на основе собственных исследований. Фокус курса – развитие и применение навыков анализа данных и презентаций.
   3. *Анализ кибер-защиты;*
      Курс нацелен на сбор данных с помощью различных инструментов защиты информационных систем с целью анализа событий, выявления вредоносных действий и рекомендации контрмер. Курс формирует навыки анализа данных об инцидентах, связанных с вторжением, оценки целостности системы и интерпретации собранной информации для установления мер по защите и смягчению последствий инцидента.
   4. *Разведывательный анализ с помощью электронных средств;*
      Курс нацелен на поиск и анализ необходимых данных из электронных источников, вклю-

чая метаданные с телефонов и сигналы от радио и спутниковых источников.

5. *Глобальная деловая разведка;*
   Предмет курса – конкурентная разведка как сбор и анализ информации для прогнозирования конкурентной активности и для беспристрастной интерпретации событий в глобальной перспективе. Дисциплина включает в себя разработку методов анализа данных с учетом этических принципов и использования открытых и закрытых источников информации.
6. *Информационная безопасность;*
   Курс рассматривает теоретические и прикладные основы информационной безопасности и её обеспечения.
7. *Разведывательный анализ организованной преступности;*
   Курс нацелен на анализ уникальных проблем, возникающих при расследовании деятельности организованной преступности местными и международными правоохранительными органами.
8. *Понимание процессов сбора разведывательных данных.*
   Цели курса – демонстрация различных методов для реализации проектов в сфере разведки: разведка с помощью открытых источников, разведка с помощью непосредственного общения с людьми, разведка на базе сбора и анализа изображений. Студенты развивают фундаментальные навыки и умения, связанные с оценкой точности и актуальности собранных данных. К концу курса студенты смогут определить и использовать различные средства сбора информации для решения различных задач.

Цели программы и преподавательский состав

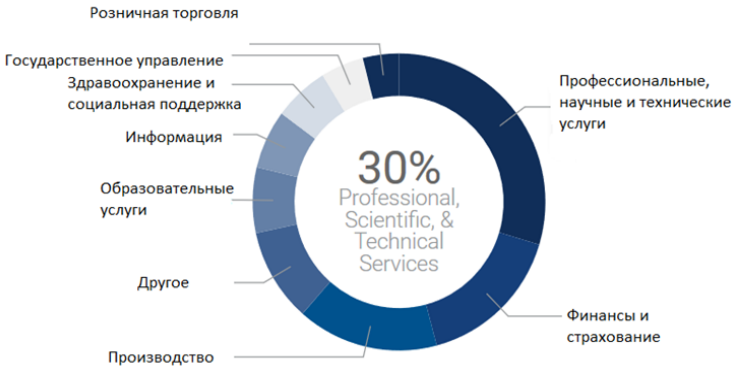
Рассматриваемая магистерская программа в сфере прикладной разведки, по словам Директора факультета, предлагает уникальное сочетание концептуальных и практических знаний, которые необходимы аналитикам для понимания сложности обеспечения безопасности в XXI веке.

Отдельно необходимо отметить преподавательский состав рассматриваемой магистерской программы, в который входят:

- видные ученые в области глобальных угроз и обеспечения национальной безопасности, философии, социологии терроризма;
- бывшие и действующие сотрудники специализированных ведомств США в сфере обеспечения безопасности, например, Министерства обороны США (DoD), Агентства по снижению угроз безопасности (DTRA); Федерального бюро расследований США; Министерства национальной безопасности США; Национальной разведывательной службы;
- бывшие сотрудники правоохранительных органов с опытом службы в горячих точках; бывшие сотрудники военной разведки США, аналитики в сфере терроризма Армии США.

Ожидаемые карьерные перспективы студентов

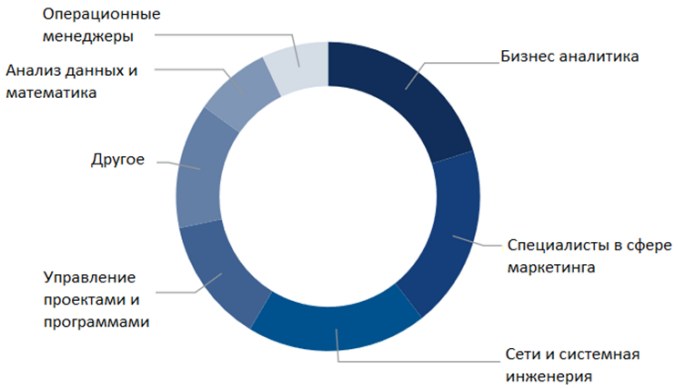
На данной магистерской программе обучаются студенты с разнообразными академическими специализациями, которые они приобрели после обучения в бакалавриате. К сферам профессиональных знаний, которыми обладают студенты, относятся безопасность, правоохранительная деятельность, технологии, исследования, аналитика, а также военная и оборонная деятельность.



Индустрии

На графике слева – индустрии, в которых трудоустраиваются после обучения выпускники [3].

На графике справа – должности, которые занимают выпускники магистерской программы после завершения обучения.



КАРЬЕРА

Наиболее часто встречающиеся должности, которые занимают выпускники - Аналитик в сфере разведки, Специалист по разведке, Ведущий аналитик по киберугрозам, Аналитик в сфере информационной безопасности и Менеджер деловой разведки.

Образовательная программа Университета Мерсихерст

Данная магистерская программа предоставляет студентам образовательную базу, необходимую для успеха в качестве аналитиков в сфере разведки как в федеральных агентствах национальной безопасности и правоохранительных органах, так и в частных и некоммерческих организациях [4]. Образовательная программа рассчитана на 34 кредита.

В качестве ожидаемых от обучения на данной образовательной программе выделяют следующие умения:

Толкование теории и истории разведки	Применение навыков критического мышления к реальным проблемам
Оценка данных с помощью различных аналитических инструментов и методологии	Подготовка аналитических продуктов в письменном, устном и/или аудиовизуальном форматах
Управление инструментами и практиками разведки, их оптимизация	Разработка методов исследования на основании информации из открытых источников и управление сбором информации

Проведение исследований в области разведки

Структура дисциплин, преподаваемых в рамках рассматриваемой программы, выглядит следующим образом:

1. 7 обязательных базовых курсов (в сумме на 21 кредит)
   a. Методы исследования в разведке;
   b. Теория разведки и ее применение;
   c. Деловая (конкурентная) разведка;
   d. Разведка в рамках правоохранительной деятельности;
   e. Коммуникации в рамках разведки;
   f. Современное лидерство в рамках разведки;
   g. Управление стратегической разведкой.
2. Курсы по выбору (необходимо выбрать любые 3);

Анализ киберугроз	Продвинутые аналитические методы
Сравнительная история разведки	Разведывательная поддержка при таргетинге
Геопространственная разведка	Анализ данных финансовой разведки
Разведка и стратегия бизнеса	Аналитика данных для частного сектора
Семинар для выпускников: национальная безопасность	Великая стратегия: стратегическое планирование и разведка
Исследования терроризма	Контршпионаж: политика и практика
Производственная практика	Предметы обсуждения в рамках разведки
Разведка, вооруженные силы и приемы ведения войны	

3. Обязательные научно-исследовательские и практические курсы.
   a. Семинар по написанию курсовой работы по теме разведки;
   b. Диссертация в области прикладной разведки.

Прохождение практики необязательно, но рекомендуется. Студент должен пройти производственную практику (минимум 200 часов) в качестве аналитика в области разведки в правительстве или международном агентстве или корпорации.

Выпускники образовательной программы впоследствии занимают следующие должности: аналитик разведки, офицер разведки, специальный агент, аналитик социальных сетей, аналитик по борьбе с отмыванием денег / аналитик в сфере «знаний своего контрагента», аналитик по исследованию рынка, полицейские, консультанты по управлению, аналитики угроз в сфере кибербезопасности и т.д.

Выпускники программы получили работу в различных федеральных агентствах, глобальных корпорациях и международных НКО, например, в Центральном разведывательном управлении, Федеральном бюро расследований, Агентстве военной разведки, Агентстве национальной безопасности, компаниях JP Morgan Chase, Johnson & Johnson, Nike, Disney, Wells Fargo, Procter & Gamble, Pricewaterhouse Coopers, а также Армии США, военно-воздушных силах и морской пехоте США.

Полная стоимость образовательной программы составляет около $ 31 600. Также возможно получение стипендии или финансовой помощи.

Магистерская программа «Аналитик деловой разведки», реализуемая Институтом проблем безопасности НИУ ВШЭ

Для полноты анализа необходимо также кратко рассмотреть особенности отечественного образовательного продукта в сфере подготовки аналитиков деловой разведки.

Данная магистерская программа была открыта осенью 2018 г., когда начал обучение её первый набор. Согласно официальной странице программы на сайте НИУ ВШЭ, её основная задача – «подготовка специалистов информационно-аналитического обеспечения комплексной безопасности бизнеса» [2].

Данная магистерская программа рассчитана на 2 года, в рамках которой студенту необходимо изучить ряд дисциплин в объеме 120 кредитов.

К основным преимуществам программы относятся применение междисциплинарного и риск-ориентированного подходов, а также инновационных методов обучения, ярко выраженная практическая направленность, а также высокий уровень мастерства профессорско-преподавательского состава [2]. Также в рамках образовательной деятельности часто проводятся мастер-классы, где приглашенные практики делятся накопленным опытом и наиболее современными инструментами и методами. Отдельно необходимо отметить значительную долю проектной и научно-исследовательской работы в рамках рассматриваемой программы.

Структура учебных курсов, преподаваемых в рамках дисциплины, выглядит следующим образом:

1. Адаптационные дисциплины – Теория организации о организационное поведение; Правовая среда бизнеса; Основы бухгалтерского учета, налогообложения и аудита.
2. Цикл общих дисциплин направления – Методология научных исследований в менеджменте; Стратегии в менеджменте; Экономика.
3. Цикл дисциплин программы. Базовая часть.
    1. Безопасность предпринимательской деятельности;
    2. Цикл деловой разведки;
    3. Принятие решений в условиях неопределенности и риска;
    4. Риск-менеджмент.
4. Дисциплины по выбору (необходимо изучить 5);

Комплексный анализ предприятия	Анализ финансовой отчетности
Введение в технологию маркетинговых исследований	Дисциплина из общеуниверситетского пула МАГОЛЕГО
Анализ отраслевых рынков	Анализ финансовых рынков
Стратегических организационный дизайн	Онлайн дисциплины по выбору из рекомендованного списка (MOOCs)

5. Научно-исследовательский семинар (НИС).
   Реализуется на протяжении всего периода обучения и включает в себя работу с научными источниками, самостоятельное проведение исследований и обсуждение полученных результатов. В рамках данного курса предусмотрено проведение упомянутых выше мастер-классов практиков из сферы бизнеса.
6. Проектный семинар.
7. Практика.

Таким образом, данная программа фокусируется на деловой разведке как составной части менеджмента организации. Более широкий охват базовой дисциплины «Безопасность предпринимательской деятельности» роднит её с зарубежными образовательными продуктами, поскольку она включает в себя рассмотрение проблем национальной безопасности, правоохранительной

деятельности, борьбы с терроризмом.

Заключение

В рамках реализации функции деловой разведки был проведен обзор рынка образовательных услуг в сфере подготовки магистров по направлению «Аналитик конкурентной (деловой) разведки».

В первой части данной работы были проанализированы разные определения понятия «деловая разведка» и его аналогов в английском языке. После выявления методов, а также этических ограничений при проведении деловой разведки была проведена практическая часть по точечной реализации данной функции. Автором были проанализированы две зарубежные образовательные программы, нацеленные на подготовку магистров в сфере деловой разведки.

В Университете Джорджстауна магистерская программа носит широкий характер, что объясняется её фокусом на взаимодействие с государственными органами США в сфере обеспечения безопасности. Программа гибкая, поскольку предполагает онлайн-формат обучения, и компактная. Её преимуществом является большое количество практиков преимущественно из сферы обеспечения государственной безопасности и правоохранительной деятельности, что способствует повышению качества и актуальности предоставляемых знаний, а также частично обуславливает акцент на национальной безопасности в ее рамках.

Магистерская программа Университета Мерсихерст также компактная (34 кредита), однако сфокусирована на деловой разведке (несмотря на наличие курсов по выбору в сфере национальной безопасности, противодействию терроризму). Частично по преподаваемым дисциплинам она схожа с отечественной образовательной программой НИУ ВШЭ, поскольку представители Университета Мерсихерст пытаются обеспечить наиболее комплексный взгляд на функцию деловой разведке. Еще одним плюсом является акцент на научно-исследовательской работе. Минусом данной программы является отсутствие информации и профессиональном прошлом преподавателей. Также данная программа лишена фокуса на менеджменте организации при рассмотрении деловой разведки. Данная деятельность рассматривается с широких позиций обеспечения национальной безопасности, правоохранительной деятельности и деятельности бизнеса.

Магистерская программа НИУ ВШЭ является наиболее полной и комплексной (120 кредитов), а также максимально ориентированной именно на конкурентную разведку в составе менеджмента организации. Плюсами программы является уникальный инновационный, практико-ориентированный образовательных подход, а также высокое мастерство профессорско-преподавательского состава, обладающего значительным опытом в преподаваемой области.

Таким образом, в рамках данной работы были выявлены различные подходы членов научного сообщества к построению и реализации образовательных программ, нацеленных на подготовку магистров в сфере деловой разведки.

Практической значимостью данной работы является ее применение сотрудниками Института проблем безопасности НИУ ВШЭ для обзора и анализа зарубежных образовательных продуктов, ориентированных примерно на ту же сферу, что и магистерская программа Института. Возможно, данный обзор вдохновит профессорско-преподавательский состав на создание каких-то новых образовательных курсов в рамках магистерской программы или же просто может стать информацией к размышлению.

Список использованной литературы

1. Конкурентная разведка. Под редакцией Е. Л. Ющука, А. А. Мальцева. М-во образования и науки Рос. Федерации, Урал. гос. экон. ун-т. – Екатеринбург: [Изд-во Урал. гос. экон. ун-та], 2015. – Ч. 1. – 210 с. Режим доступа: http://ci-razvedka.ru/Docs/Uchebmik-Konkurentnaya-Razvedka-UrGEU-Part1.pdf (дата обращения: 10.03.2019)
2. Магистерская программа «Аналитик деловой разведки» НИУ ВШЭ. Официальная страница. Режим доступа: https://www.hse.ru/ma/intelligence/ (дата обращения: 10.03.2019)

3. Официальный сайт магистерской программы Master of Professional Studies in Applied Intelligence. Режим доступа: https://scs.georgetown.edu/programs/423/master-of-professional-studies-in-applied-intelligence/ (дата обращения: 10.03.2019)
4. Официальный сайт магистерской программы Master of Science, Applied Intelligence (Erie, Pa), Mercyhurst University. Режим доступа: https://www.mercyhurst.edu/academics/graduate-programs/graduate-degrees-and-certificates-intelligence-studies/applied-0 (дата обращения: 10.03.2019)
5. Официальный сайт рейтинга лучших университетов мира (THE Rating). Джорджтаунский Университет. Режим доступа: https://www.timeshighereducation.com/world-university-rankings/georgetown-university#survey-answer (дата обращения: 10.03.2019)
6. Официальный сайт рейтинга лучших университетов мира (THE Rating). Университет Мерсихерст. Режим доступа: https://www.timeshighereducation.com/world-university-rankings/mercyhurst-university (дата обращения: 10.03.2019)
7. Официальный сайт Общества профессионалов конкурентной разведки. Режим доступа: https://www.scip.org/page/AboutSCIP (дата обращения: 10.03.2019)
8. Официальный сайт Общества профессионалов конкурентной разведки. Этический кодекс. Режим доступа: https://www.scip.org/page/CodeofEthics (дата обращения: 10.03.2019)
9. Collins Dictionary. Industrial espionage. Режим доступа: https://www.collinsdictionary.com/dictionary/english/industrial-espionage (дата обращения: 10.03.2019)
10. John J. McGonagle, Carolyn M. Vella. Proactive Intelligence. Chapter 2. What is Competitive Intelligence and Why Should You Care About it? Режим доступа: https://www.springer.com/cda/content/document/cda_downloaddocument/9781447127413-c2.pdf?SGWID=0-0-45-1299240-p174282177 (дата обращения: 10.03.2019)

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНСТИТУТ ПРОБЛЕМ ПРОБЛЕМ БЕЗОПАСНОСТИ

МОСКВА, 2020