Федеральное государственное образовательное бюджетное учреждение высшего образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Россия: от кризиса к устойчивому развитию. Ресурсы. Ограничения. Риски.

Сборник тезисов научных работ участников VIII Международного научного студенческого конгресса 9 марта – 17 апреля 2017 года

ТОМ № I
Факультет анализа рисков и экономической безопасности им. профессора В.К. Сенчагова

Москва 2017

«Россия: от кризиса к устойчивому развитию. Ресурсы. Ограничения. Риски»: Сборник статей участников VIII Международного научного студенческого конгресса «Россия: от кризиса к устойчивому развитию. Ресурсы. Ограничения. Риски» в 15 томах, 9 марта - 17 апреля 2017 года.

Под ред. Биткиной И.В. / ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации» — М.: Финуниверситет, 2017. - Том. I Факультет анализа рисков и экономической безопасности им. профессора В.К. Сенчагова. Электронный ресурс.

Материалы публикуются в авторской редакции

ИСПОЛЬЗОВАНИЕ «БОЛЬШИХ ДАННЫХ» В ОБЛАСТИ МИНИМИЗАЦИИ УГРОЗ И РИСКОВ В БАНКОВСКОЙ ОТРАСЛИ

Акопов М.В.
Научный руководитель: д.т.н., профессор Дворянкин С. В.
Финансовый университет при Правительстве Российской Федерации

1. Категориальный аппарат

Большие данные - серия подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объёмов и значительного многообразия для получения воспринимаемых человеком результатов, эффективных в условиях непрерывного прироста, распределения по многочисленным узлам вычислительной сети, альтернативных традиционным системам управления базами данных и решениям класса Business Intelligence[1].

Таблица 1 – Три основные характеристики больших данных

В основном большие данные определяются тремя основными характеристиками:	
1)	объем
2)	скорость
3)	разнообразие данных

2. Актуальность исследования

Банки концентрируют колоссальные объёмы данных. Согласно данным Frank Research Group банки обрабатывают:

1. Клиентские данные:
a) 10 млрд. – транзакций картами в год
b) 800 млрд. – документов в бюро кредитных историй
c) 3,8 Пбайт – средний объём хранилища в банках
2. Операционные данные:
a) 40 млн. кредитных заявок в год
3. Данные о внешней среде
a) 50 млн. показателей публичной финансовой отчётности в год [4]

Согласно данным Frank Research Group 80% экономически активных россиян охвачено банковскими услугами. По результатам опроса McKinsey & Company 76% банков заявляют, что Big Data позволяют привлекать новых клиентов, лучше взаимодействовать с ними и поддерживать их лояльность. По оценкам Gartner 34% банков инвестировали в развитие технологий Больших данных. По данным McKinsey & Company 25% всей индустрии Big Data владеет финансовая индустрия [5].

3. Задачи исследования

Таблица 2 – Основные задачи для исследования

Исходя из целей, основными задачами для исследования, являются:	
1.	использование социальных сетей
2.	противодействие мошенничеству
3.	повышение физической безопасности

4.Технология обработки информации с помощью технологии Big Data и экономическое обоснование хранения большого количества данных

Технологии Big Data могут обеспечить экономическое обоснование хранения информации, которое состоит в том, что весь огромный массив будет организован и структурирован. Ведь без Big Data извлечь ценность из накопленного богатства информации невозможно.

Рис 1 - Способ обработки данных с помощью Big Data[2]

5. Противодействие мошенничеству

Нынешние (уже внедрённые в банковскую систему) технологии вполне позволяют обрабатывать накопленные массивы информации. Однако проблема в том, что делают они это не очень быстро [3]. Данный изъян не позволяет эффективно противодействовать мошенничеству.

6. Использование социальных сетей

Социальные сети являются еще одним прекрасным источником данных. Они могут сказать о человеке больше, чем он сам готов транслировать миру. Крайне полезным инструментом являются анализаторы сообщений пользовательских сообщений в социальных сетях. В пример можно привести программный продукт Hedonometer, который анализирует твиты пользователей и позволяет оценить их настроения.

7. Повышение физической безопасности

Колоссальные перспективы в сфере обеспечение безопасности раскрывает сочетание Big Data и геоаналитики. В частности, проект организации «Senseable City Lab», который позволяет прокладывать маршруты следования и подробно отслеживать передвижения объектов в режиме реального времени. Программное обеспечение было разработано и использовалось в США. Также данное ПО было приобретено Южной Кореей.

8. Основные проблемы при внедрении проектов больших данных

По результатам исследования компании Accenture наибольшими трудностями при внедрении технологии Больших данных являются:

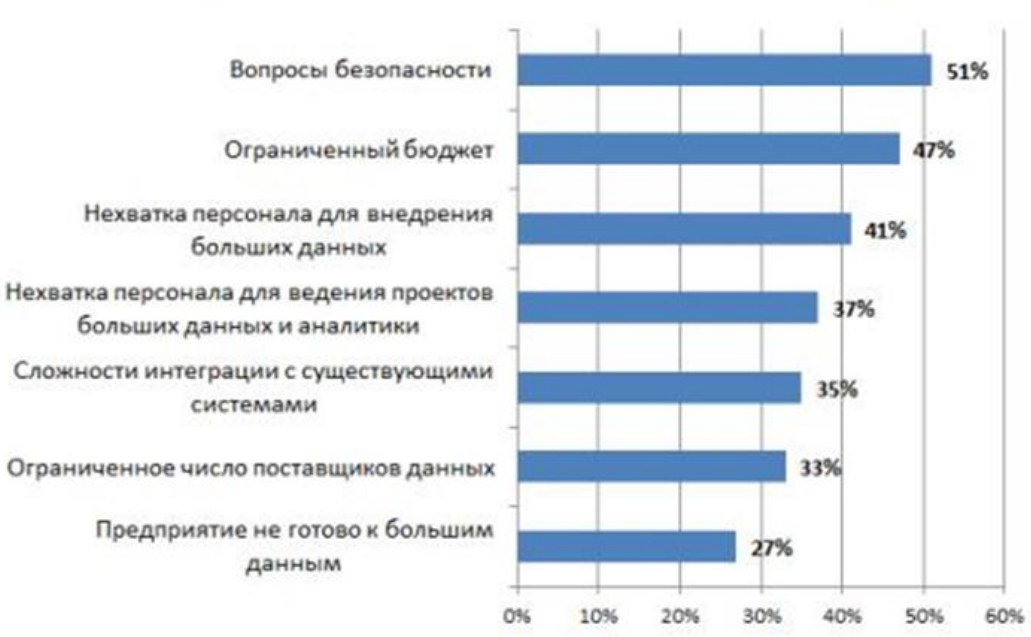

Рис 2 - Основные проблемы при внедрении проектов больших данных[66]

9. Выводы

Таким образом результат исследования темы “Инновационные технологии применения Big Data в банковской сфере” позволяет сделать следующие выводы:

1. Использование социальных сетей является эффективным способом добывания важной информации о клиентах. В направлении использования социальных сетей для добычи полезной информации уже ведутся активные разработки (в частности, проект Hedonometer);
2. Технология «Больших данных» даёт экономическое обоснование использования огромных массивов различной информации в банках;
3. В области повышения физической безопасности банков весомые перспективы открывает решение лаборатории Senseable City Lab, которое сочетает в себе технологии Big Data и геоаналитики;
4. Нынешние технологии, внедрённые в банках, не позволяет эффективно противодействовать мошенничеству. Технология больших данных призвана не только увеличить эффективность, но и ускорить процесс обработки огромных потоков информации.

Список использованных источников

1. Big Data от А до Я. Часть 1: Принципы работы с большими данными, парадигма MapReduce [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/dca/blog/267361/
2. Oracle Big Data [Электронный ресурс]. – Режим доступа: https://www.oracle.com/webfolder/s/delivery_production/docs/FY15h1/doc6/big-data-enterprise.pdf
3. Когда данных слишком много: Банки на передовой Big Data [Электронный ресурс]. – Режим доступа: https://republic.ru/specials/data-economics/articles/bankiri/
4. Сергей Кашпоров — Frank Research Group — ICBDA 2015. Как с помощью данных и аналитики повысить эффективность продаж в банке [Электронный ресурс]. – Режим доступа: http://rb.ru/news/big-data-for-banks-and-insurance/
5. Big data для банкиров и страховщиков [Электронный ресурс]. – Режим доступа: https://www.frankrg.com/index.php?new_div_id=505
6. Аналитический обзор рынка Big Data [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/company/moex/blog/256747/

ИНТЕРНЕТ ВЕЩЕЙ: ИННОВАЦИОННАЯ ОПАСНОСТЬ ФИНАНСОВОГО СЕКТОРА ЭКОНОМИКИ РФ

Воеводин А.Ю., Хатырева А.С.
Научный руководитель: д.т.н., профессор Дворянкин С. В.
Финансовый университет при Правительстве Российской Федерации

Несмотря на то, что первое упоминание термина «Интернет вещей встречается в 1999 году, единая терминологическая база до сих пор не окончательно сформирована. В рамках данной статьи под Интернетом вещей будем понимать расширение возможностей подключения к сети и вычислительных способностей для объектов, устройств, датчиков и других предметов, обычно не считающихся компьютерами.

Ряд компаний и научно-исследовательских организаций делают многочисленные прогнозы относительно потенциального воздействия IoT мировую экономику в течение ближайших пяти или десяти лет. Например, согласно исследованиям McKinsey Global Institute, финансовое влияние IoT может достигнуть от 3,9 до 11,1 млрд. долларов к 2025 году. Очевидно, что для Российской Федерации важно находиться в числе лидеров по внедрению и развитию таких технологий.

Вопросы безопасности IoT

При постоянном увеличении числа устройств, подключенных к Интернету, неизбежно возникновение новых потенциально уязвимых мест. Если устройство недостаточно защищено, оно может служить точкой доступа для кибератаки. [1]

Оценка рисков и возможных последствий включает в себя целый ряд факторов: наличие четкого понимания существующих рисков безопасности и потенциальных рисков в будущем; приблизительные экономические и другие последствия в случае осуществления рисков; приблизительную стоимость устранения их последствий.

Необходимо заметить, что устройства IoT имеют ряд уникальных проблем безопасности. Например, многие из этих устройств смогут самостоятельно устанавливать связь друг с другом непредсказуемым и динамическим способом. В результате потенциальное число взаимных подключений между этими устройствами является беспрецедентным.

Многие системы IoT будут состоять из групп идентичных или почти идентичных устройств. Такая однородность усиливает потенциальное воздействие каждой уязвимости, умножая его на количество устройств, имеющих те же характеристики.

Многие устройства IoT изначально не предполагают возможности обновления либо эта процедура слишком неудобна и непрактична. В качестве примера можно взять отзыв 1,4 млн автомобилей Fiat Chrysler в 2015 году [2] для устранения уязвимости, благодаря которой злоумышленник смог взломать автомобиль с помощью беспроводной сети.

Многие устройства IoT работают таким образом, что пользователь не имеет или почти не имеет представления о внутреннем функционировании устройства или создаваемых им потоках данных. Это создает уязвимость в области безопасности, когда пользователь считает, что устройство IoT выполняет определенные функции, в то время как на самом деле оно может выполнять нежелательные действия или собирать данные, которые пользователь не намерен предоставлять.

IoT в банкинге

Преимущества IoT в банковском маркетинге и финансовых сервисах:

- Сбор данных постоянно и в режиме реального времени

Например, страховщик может оценить реальные модели использования застрахованного автомобиля. Он так же может установить правила, по которым можно будет дистанционно заблокировать модели поведения автомобиля (превышение скорости и т.д.).

- Действия клиента могут вызывать ответные маркетинговые действия

Например, установленный в дверь магазина маяк может распознавать телефон или RFID и предлагать индивидуальный кэшбэк.

- Мгновенный обмен данными между устройствами

Например, использовать в магазинах сканеры для идентификации продуктов в корзине и мобильного бумажника клиента, сам же покупатель будет использовать для оплаты RFID. [3]

Основные барьеры для развития IoT в сфере финансовых услуг и банковского маркетинга:

- Конфиденциальность и вопросы безопасности;
- Соблюдение установленных норм;
- Отсутствие общих стандартов.

В августе 2015 года IDC (International Data Corporation – ведущий поставщик информации, консультационных услуг и организатор мероприятий на рынках информационных технологий, телекоммуникаций и потребительской техники.) был проведен опрос. Согласно этому исследованию 58,4% тех, кто принимает решения в финансово-промышленной сфере, рассматривают IoT как «стратегические» инициативы; 20% полагают, что это лишь «трансформационные» инициативы и лишь 5,6% респондентов сказали, что влияние IoT не играет роли [4].

Нет никаких сомнений в том, что развитие IoT в банковской и финансовой сферах услуг будет поддерживаться следующими факторами:

1. Технический прогресс делает IoT более доступным и стандартизованным;
2. Массовое принятие технологий IoT;
3. Конкуренция в финансово-техническом секторе (мобильные платежи и т.д.)

Рост может быть замедлен несоответствием нормативным требованиям, особенно в конфиденциальности данных, но в целом неизбежен. Ниже приведены примеры использования IoT в банкинге, которые четко показывают конкурентное преимущество данной технологии.

Примеры IoT в сфере банковских и финансовых услуг

- Visa Mobile Location Confirmation

Компания Visa запускает сервис под названием Mobile Location Confirmation, который позволит отслеживать местонахождение держателя карты автоматически. Он будет сопоставлять эту информацию с информацией о месте расходования средств, помечая транзакцию как надёжную, если они совпадают. Данная мера обещает стать эффективным инструментом в борьбе с мошенничеством [5].

- Sense by Alfa-Bank

На конференции Finovate представители «Альфа-Банка» представили персонального финансового ассистента Sense. Это приложение может давать подсказки пользователю на основе его трат.

Sense использует машинное обучение и подсказывает, что может понадобиться клиенту. Приложение получает информацию о привычках пользователя, исходя из его трат, а также данных от других сервисов, которые подключаются к Sense [6].

- Groceries by MasterCard

MasterCard и Samsung представили на выставке CES встроенное в смарт-холодильник решение, с которым покупка продуктов для всей семьи станет еще проще, быстрее и удобнее. Приложение Groceries by MasterCard позволяет выбирать и оплачивать продукты прямо на дисплее нового смарт-холодильника Samsung Family Hub.

Также приложение позволяет контролировать семейные расходы: финальный список утверждается введением 4-х значного пин-кода [7].

Принципы защиты IoT

Первый важный шаг в обеспечении безопасности устройства заключается в том, чтобы гарантировать, что пользователь действительно является тем, за кого себя выдаёт, и действительно имеет право для доступа к этому устройству. Процедура аутентификация является важным аспектом при работе с подключенными устройствами. Например, когда мы открываем свой умный автомобиль с помощью мобильного телефона, мы хотим быть уверены, что никто кроме нас не сможет этого сделать.

Поставщики оборудования также должны быть авторизованы для доступа к удалённому устройству. Производитель электромобиля Tesla оповещает водителей о доступности обновления прошивки и о том, когда это обновление будет загружено. Таким образом, водитель понимает, что обновление было получено непосредственно от Tesla, и что это не попытка злоумышленника проникнуть в систему. Для более надежной аутентификации всё чаще используются биометрические данные, например, отпечатки пальцев или сканирование сетчатки, которые позволяют достоверно подтвердить, что мы являемся именно теми, за кого себя выдаём.

Анализ ситуации показывает необходимость использования комплексного и научно-обоснованного подхода к обеспечению безопасности Интернета вещей:

Оценка рисков – для разработчика важно понимать все потенциальные уязвимости. Методология оценки должна охватывать вопросы обеспечения конфиденциальности, безопасности, предотвращения мошеннических действий, кибератак и кражи интеллектуальной собственности.

Обеспечение безопасности на этапе проектирования – ключевой момент заключается в том, что безопасность устройства должна учитываться на этапе проектирования.

Обеспечение безопасности данных – строгая аутентификация, шифрование и безопасное управление ключами шифрования должны использоваться для защиты информации, как хранящейся на устройстве, так и в момент её передачи.

Управление жизненным циклом – обеспечение безопасности не следует рассматривать как обособленный процесс, который достаточно выполнить один раз и забыть о нём. Крайне важно, чтобы устройства, использующиеся в экосистеме Интернета вещей, были защищены на протяжении всего их жизненного цикла.

Таким образом, подводя итог вышеизложенному, отметим, что в соответствии с Доктриной информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) в качестве одной из угроз выделена преступность в кредитно-финансовой сфере. Учитывая повышенный интерес, популярность и распространенность концепции Интернета вещей, следует особое внимание уделить IoT как к инновационному методу совершения таких преступлений.

Список использованных источников

1. Совместная безопасность: подход к решению проблем Интернет- безопасности. Internet Society, апрель 2015 г., https://www.internetsociety.org/ collaborativesecurity

2. Fiat Chrysler отзывает 1,4 млн машин в США из-за риска взлома хакерами, июль 2015 г., https://ria.ru/world/20150724/1146131999.html

3. IoT in Financial Services and Banking – Definition and Examples, June 2016, https://www.k-message.com/iot-financial-services-bank-marketing-definition-examples/

4. Internet of Things: The Complete Reimaginative Force TCS Global Trend Study, July 2015, https://www.tcs.com/SiteCollectionDocuments/White%20Papers/Internet-of-Things-The-Complete-Reimaginative-Force.pdf

5. Пол Маккри (Visa): «Люди не хотят платить, они хотят покупать», август 2016 г., https://bankir.ru/publikacii/20160815/pol-makkri-visa-lyudi-ne-khotyat-platit-oni-khotyat-pokupat-10007916/

6. «Альфа-Банк» анонсировал приложение-помощника для финансовых консультаций Sense, сентябрь 2015 г., https://vc.ru/n/alfa-sense

7. MasterCard представила решения для платежей через холодильник и фитнес-браслеты, январь 2016 г., https://www.banki.ru/news/lenta/?id=8603837

АНТИКОРРУПЦИОННЫЙ КОМПЛАЕНС КАК ИНСТРУМЕНТ УПРАВЛЕНИЯ ПРОЦЕССОМ ИНВЕСТИРОВАНИЯ

Кабанов В.С.
Научный руководитель: к.э.н. Петухов В. А.
Финансовый университет при Правительстве Российской Федерации

Инвестиции являются неотъемлемой частью современной экономики. Под инвестициями понимается вложения главной целью которых является получение прибыли. Инвестиции могут выступать в различных формах и видах. По форме собственности на инвестиции они разделяются на:

- частные;
- государственные;
- иностранные;
- смешанные.

Деятельность, связанная с инвестициями различных форм и уровней, называется инвестиционным процессом. Его понимание необходимо для оценки рисков и угроз, возникающих в данной деятельности. Инвестиционный процесс состоит из трёх этапов.

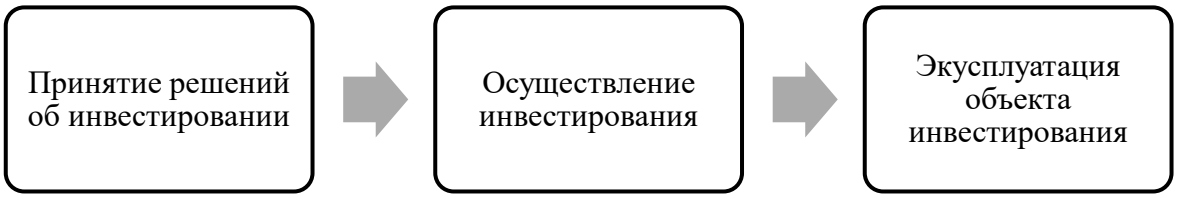

Рисунок 1. Этапы инвестиционной деятельности. (составлено автором)

Первый этап заключается в идее инвестирования и состоит также из трёх фаз. Первой фазой выступает цель инвестиций. В большинстве случаев целью инвестиций является сохранение и преумножение капитала, т.е. инвестор должен не потерять что имеет и сверху получить прибыль. Ещё одной из целей может являться минимизация срока возвращения, ведь, чем раньше к инвестору вернуться деньги, тем менее рискованно, а соответственно более привлекательно для него вложение.

Второй фазой первого этапа является выбор направления инвестирования. Обычно от выбора направления зависит выгодность и надёжность инвестиций, а также риски, которые являются одними из важнейших параметров. В качестве направлений могут выступать:

- драгоценные металлы
- ценные бумаги
- бизнес
- недвижимость
- вклады
- альтернативные виды

Перед третьей фазой происходит выбор как будет осуществляться инвестирование, напрямую или через инвестиционные институты. К институтам инвестиционного процесса могут относится коммерческие банки (универсальные и специализированные), небанковские кредитно-финансовые организации и различные фонды, компании, биржи.

Третья фаза заключается в выборе объекта инвестирования по выбранному направления. Также подготовка и заключение инвестиционного договора, определение прав и обязанностей сторон и остальные параметры, связанные со взаимодействием сторон.

Осуществление инвестиций во втором этапе, является практическим применением договоров в отношении объектов инвестирования, заключенных на предыдущем этап. Это

может быть передача каких-либо материальных и нематериальных средств, для выполнения инвестиционного проекта. Важно отметить, что данный этап завершается после создания проекта.

Третий этап связан с получением прибыли и возвращением капитала инвестору. Данный этап обычно является сроком окупаемости проекта. В его рамках запускается производство товаров, работы или услуг, выручка от которых и идёт на покрытие инвестиций.

Под инструментами управления инвестиционными процессами в работе понимаются правовое, административное, экономическое и организационно-управленческое регулирование. Но помимо названных инструментов, оказывающих воздействие на качество управления инвестициями, существует такое понятие как инвестиционные климат, которое отражает уровень доходности и риски инвестирования.

Если рассматривать инвестиционный климат России, то он является неудовлетворительным. Данная оценка связана с таким параметром, как уровень коррупции в стране. С каждым годом растёт количество преступлений коррупционной направленности (рис. 2). [1] Это вызывает недоверие у инвесторов, которые связывают коррупцию с большим риском потери средств, которые они могут вложить.

Таблица 1. Количество преступлений коррупционной направленности (составлено автором).

2016	2015	2014
32924	32455	32060

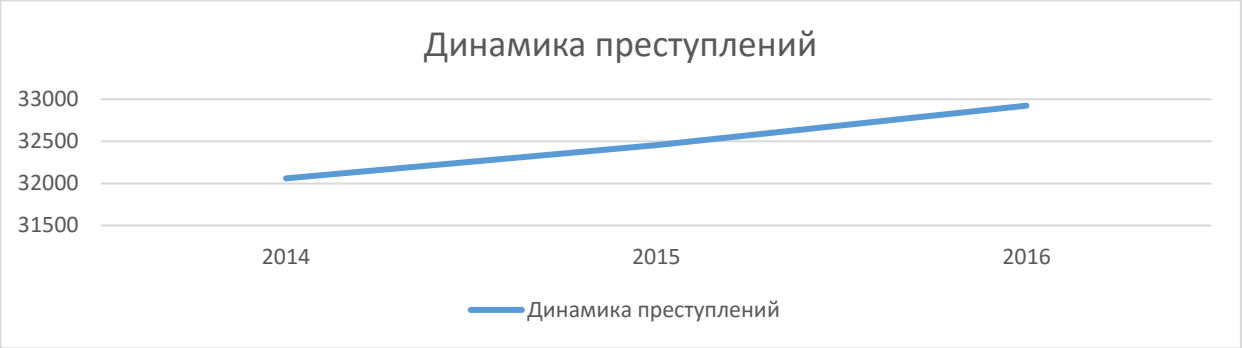

Рисунок 2. Динамика преступлений коррупционной направленности (составлено автором).

Получается, если государственного регулирования оказывается недостаточно, и в России сохраняется высокий уровень коррупции с положительной динамикой, организациям необходимо создавать условия, которые позволят существенно снизить уровень коррупции в организациях.

Комплаенс контроль является эффективной системой, которая включает в себя все инструменты управления инвестиционными процессами и позволяет комплексно осуществлять регулирование инвестиционной деятельности. Он представляет собой внутренний контроль, который отвечает за соответствие правовым нормам деятельности компании и работает как система. Но как это поможет в управлении инвестиционной деятельности организации?

Политика «Китайской стены» служит для закрытия информации. Поскольку работники организации, могут быть аффилированы, и продавать информацию об инвестиционных проектах организации с целью получения прибыли. Ведь из-за разглашения данной информации компания может понести большие убытки.

Сотрудники финансового или инвестиционного отделов так же могут быть вовлечены в коррупционные схемы. Путём дачи взяток и подкупов, они могут как сами создавать якобы выгодный инвестиционные проект, через который могут вывести деньги себе, а проект окажется провальным, либо через уже имеющийся.

Помимо этого, крупный государственные чиновники также могут участвовать в сделках, получая свой барыш, за реализацию инвестиционных сделок для компаний. Таким примером может являться недавно произошедший случай с министром экономического развития А.В.Улюкаевым. [2]

Также за счёт остальных своих функций комплаенс контроль должен создать систему, которая как прямо, так и косвенно будет влиять на повышение защищённости и снижение рисков в процессе инвестирования.

Система состоит из контрольной среды, которая включает в себя такие аспекты как разработка внутренней документации (кодекс корпоративной этики и т.д.), установление зон ответственности, для избегания утечки информации, ведь не имея полной информации тяжело делать какие-то выводы о деятельности организации. Также установление ответственности за нарушения внутренних и регламентов.

В качестве средств контроля необходимо проводить мониторинг счетов контроля сотрудников и согласование различных сделок и транзакций, как внутри инвестиционного проекта, так и в деятельности организации.

Такие параметры как создание горячей линии, и обучение и аттестация персонала можно отнести к информационно-коммуникационному аспекту комплаенс контроля, который является крайне важным для стабильной работы организации.

Мониторинг за адекватностью процедур уровню риска в инвестиционной деятельности можно выделить как одни из основных аспектов деятельности комплаенс контроля в инвестиционной деятельности.

Выше описанные меры помогут повысить эффективность работы организации. Помимо этого, будет вестись борьба с коррупцией, что выведет уровень инвестиционной привлекательности и деловой активности на новый уровень.

Список использованных источников

1. Портал правовой статистики URL: http://crimestat.ru/ (Дата обращения: 08.03.2017).

2. Министр Улюкаев пойман при получении взятки в два миллиона долларов // Газета Lenta.ru. URL: https://lenta.ru/articles/2016/11/15/ulyukaevcorruption/ (дата обращения: 05.03.2017).

3. Марковецкий М.Ю Использование финансовых инструментов рынка ценных бумаг в инвестиционном процессе // Финансы и кредит. - 2005. - №33. - С. 53-63.

ПОВЫШЕНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ МЕТАЛЛУРГИЧЕСКИХ ПРЕДПРИЯТИЙ ПУТЕМ ВНЕДРЕНИЯ ЭКОЛОГО-ЭКОНОМИЧЕСКОГО ЭЛЕМЕНТА СИСТЕМЫ БЕЗОПАСНОСТИ

Комиссарова Д.А.
Научный руководитель: к.э.н., Лебедев И.А.
Финансовый университет при Правительстве Российской Федерации

В последние годы все актуальнее становится вопрос снижения негативного воздействия промышленных предприятий на окружающую среду. Негативные тенденции изменения окружающей среды во многом определяются промышленным производством. Так, например, по данным Министерства природных ресурсов и экологии РФ, наибольшие объемы выбросов загрязняющих веществ в атмосферный воздух от стационарных источников в 2015 году приходились на такие виды экономической деятельности как «обрабатывающие производства» (34,5% от всех выбросов от стационарных источников) и «добыча полезных ископаемых» - 27,5%). [1] При этом произошло снижение инвестиционной активности предприятий металлургической отрасли с 133 миллиардов рублей в 2014 году до 110 миллиардов рублей в 2015 году. [2] Поэтому в условиях современной экологической ситуации проблема поиска инструментов и механизмов, обеспечивающих эффективное экономическое функционирование металлургических предприятий при одновременном обеспечении их экологической безопасности, является весьма актуальной.

Рассмотрим взаимосвязь финансово-хозяйственного состояния предприятия и мер экологической безопасности на примере ОАО «Магнитогорский металлургический комбинат», который является крупнейшим в России металлургическим комбинатом.

По данным Росстата в 2015 году выбросы от деятельности «ММК» составили 89,9 %, от общего количества загрязняющих выбросов в городе, где находится комбинат, но в то же время затраты на реализацию мер экологической безопасности составили 2788,9 миллионов. Это говорит о том руководство компании, уделяет особое внимание вопросам экологической безопасности и выделяет достаточно средств на минимизацию воздействия на окружающую среду и выполнение требований природоохранного законодательства.

Также стоит отметить, что, начиная с 2014 года объемы вредных выбросов ежегодно уменьшаются. Прежде всего это связано с кризисом в металлургической отрасли, который привел к сокращению производства, а значит и к снижению вредоносных выбросов: мощности в общей сложности в 2015 году были загружены на 84 %, а общее производство по итогам года сократилось на 6,1 %. Но снижение воздействия на экологию в данном случае имеет негативные тенденции для самого предприятия, так как оно недополучает прибыль в том объеме в каком могло бы получить при 100% загруженности мощностей.

Также влияние на снижение воздействия на окружающую среду имело внедрение и реализация грамотной экологической политики компании. Согласно данной политики ОАО «ММК» осуществляет установку новейших очистительных систем в наиболее грязных производствах, модернизацию устаревших производств и внедрение новых технологий, обучение, повышение компетентности и распределение ответственности персонала в области обеспечения экологической безопасности. Например, в 2016 году, согласно графику осуществления, природоохранных мероприятий, была завершена установка электрофильтра с системой удаления золы котла № 6. [3] Данное техническое перевооружение привело к сокращению выбросов пыли на 680 т/год, а также к прекращению размещения 15 тыс. тонн/год золы (являются отходами 5 класса опасности).

Благодаря реализации этих задач, комбинат получил международный сертификат ISO 14001.

Сертификат ISO 14001 «Системы экологического менеджмента. Спецификация и руководство по использованию» – стандарт серии ISO 14000, устанавливающий требования к

системам экологического менеджмента с тем, чтобы дать организациям инструмент для разработки политики и определения задач сокращения воздействия на окружающую среду.

Получение данного сертификата повлияло и на финансово-хозяйственную деятельность ОАО «ММК»:

1. Увеличение инвестиций и соответственно повышение инвестиционной привлекательности компании. Так в первом полугодии 2015 года инвестиции составили 5,1 миллиардов рублей. Большая часть средств пошла на техническое перевооружение доменных печей и строительство закрытого цикла переработки химических продуктов. Ввод в строй данного комплекса обеспечит значительное ежегодное сокращение выбросов загрязняющих веществ.

2. Упрощение выхода продукции «ММК» на внешний рынок. Наличие документа об экологической сертификации производства устраняет ряд барьеров в торговле на международном уровне. Так, например, некоторые страны взимают «экологический налог» за продукцию несоответствующую международным стандартам.

3. Формирование положительного общественного мнения о комбинате. Сейчас все больше людей обеспокоены состоянием окружающей среды и компания, чьи приоритеты направлены на экологически ориентированное производство, вызывает доверие и желание приобретать у нее продукцию.

4. Повышение эффективности производства и приведение деятельности к международным стандартам. Это увеличит конкурентоспособность предприятия на мировом и внутреннем рынках, так как потребители в процессе удовлетворения своих потребностей стремятся не только к изобилию товаров и услуг, но и к сохранению и улучшению среды обитания. Таким образом экологическое качество производства и продукции становится фактором привлечения потребителя, который трансформируется в спрос и, как следствие, в повышение конкурентоспособности.

5. Отсутствие штрафов и снижение коэффициента при расчете платы за негативное воздействие на окружающую среду за соответствие требованиям природоохранному законодательству. Например, в 2013 году в результате проверки Федеральной службой Росприроднадзора были выявлены некоторые нарушения обязательных требований в области охраны атмосферного воздуха. За нарушения природоохранного законодательства должностные лица «ММК» были привлечены к административной ответственности по: ст. 8.1. «Несоблюдение экологических требований при осуществлении градостроительной деятельности и эксплуатации предприятий, сооружений или иных объектов»; ч. 2 и ч.3 ст. 8.21. «Нарушение правил охраны атмосферного воздуха». Это привело к тому, что комбинату пришлось выплатить штраф в размере 215 000 рублей, а это хоть и небольшой, но все-таки ущерб для прибыли предприятия.

В последующие годы по результатам проведенных проверок нарушений выявлено не было. Это говорит о том, что ОАО «ММК» дорожит своей репутацией и делает все для того, чтобы свести риски применения санкций в результате нарушения норм природоохранного законодательства к минимуму.

Таким образом, учитывая все вышесказанное, можно сказать, что существует зависимость между экологическим воздействием предприятия на окружающую среду и ее финансово-хозяйственной деятельностью. Соблюдение баланса между двумя этими факторам обеспечит стабильное функционирование и экономический рост предприятия.

Для обеспечения этого баланса необходимо внести изменения в экологическую политику комбината, где в качестве одной из цели обозначить введение эколого-экономической безопасности предприятия.

Для того чтобы дать определение эколого-экономической безопасности, рассмотрим понятия экологической и экономической безопасности:

- Экологическая безопасность – это состояние защищенности природной среды и жизненно важных интересов человека от возможного негативного воздействия хозяйственной

и иной деятельности, чрезвычайных ситуаций природного и техногенного характера, их последствий. [4]

- Экономическая безопасность – это состояние защищенности его жизненно важных и законных интересов от внешних и внутренних негативных активностей, проявляемых в формах конкурентной борьбы, обеспечивающее нормальные условия его функционирования и возможность стабильного развития в будущем. [5]

Исходя из этих определений, можно сказать, что эколого-экономическая безопасность представляет собой сочетание экономических, социальных и экологических условий и факторов, обеспечивающих устойчивое и эффективное развитие предприятия, направленное на повышение его экономической деятельности, инвестиционной привлекательности, конкурентоспособности, а также состояния окружающей природной среды.

Особенностью данной безопасности является то, что она должна учитывать интересы собственников в получении прибыли; интересы работников – в безопасных условиях труда; интересы потребителей – в получении продукции соответствующей экологическим стандартам; интересы населения, не имеющего отношения к данному предприятию, но проживающему на данной территории в качестве окружающей среды. В общем соблюдение баланса, как и экономических, так и экологических интересов предприятия.

Резюмируя все вышесказанное, можно сказать, что благодаря осуществлению экологическим фактором значительного влияния на показатели и эффективность финансово-хозяйственной деятельности предприятий, механизмы эколого-ориентированного развития являются одними из важнейших инструментов перехода современных предприятий на инновационный путь развития. Следовательно, необходимым условием конкурентоспособного, финансово устойчивого и инвестиционно-привлекательного предприятия в долгосрочной перспективе является согласование задач финансовой и экономической эффективности его деятельности с экологическими условиями и требованиями, которые диктуются рыночной средой.

Список использованных источников

1. Государственный доклад «О состоянии и об охране окружающей среды российской федерации в 2015 году» // Официальный сайт Министерства природных ресурсов и экологии РФ [Электронный ресурс]. URL: http://www.mnr.gov.ru/upload/iblock/b27/gosdoklad_2015.pdf. – Заглавие с экрана. – (Дата обращения: 21.03.2017).

2. Государственный доклад «О состоянии и об охране окружающей среды российской федерации в 2015 году» // Официальный сайт Министерства природных ресурсов и экологии РФ [Электронный ресурс]. URL: http://www.mnr.gov.ru/upload/iblock/b27/gosdoklad_2015.pdf. – Заглавие с экрана. – (Дата обращения: 23.03.2017).

3. Наиболее значимые природоохранные мероприятия Экологической программы Группы ОАО «ММК» реализованные в 2015 году // http://www.mmk.ru (дата обращения: 19.03.2017).

4. ФЗ № 7 от 10.01.2002 «Об охране окружающей среды» [Электронный ресурс]. – Режим доступа: система Гарант. (Дата обращения:21.03.2017)

5. Экономическая безопасность России. Общий курс. [Электронный ресурс]: учебник/ под ред. В.К. Сенчагова. – 4-е изд. – Режим доступа: электронно-библиотечная система Znanium.com. (Дата обращения:21.03.2017)

УЧЕТ ИНДИВИДУАЛЬНЫХ ОСОБЕННОСТЕЙ РАЗВИТИЯ ХОЗЯЙСТВУЩЕГО СУБЪЕКТА ПРИ УСТАНОВЛЕНИИ ПОРОГОВЫХ ЗНАЧЕНИЙ ИНДИКАТОРОВ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ АО «АЛЬФА-БАНК»

Максимова В.В.
Научный руководитель: д.т.н., профессор Родионов А.С.
Финансовый университет при Правительстве Российской Федерации

На сегодняшний день большинство хозяйствующих субъектов при формировании реестра индикаторов экономической безопасности устанавливают их пороговые значения на принятом в отрасли уровне без учета индивидуальных факторов развития, что нередко приводит к несвоевременному выявлению угроз экономической безопасности ХС.

Индикаторы экономической безопасности ХС – это количественные показатели уровня экономической безопасности в ХС, имеющие пороговые значения, выход за пределы, которых, как правило, сопровождается снижением темпов развития ХС и свидетельствует о возникновении угроз экономической безопасности ХС. Реестр индикаторов занимает важную роль в системе обеспечения экономической безопасности, так как он позволяет выявить угрозы на ранней стадии, когда их проще устранить, а ущерб от их воздействия минимальный.

В банковской отросли реестр индикаторов экономической безопасности (Таблица1), состоит из показателей и их пороговых значений, установленных инструкцией Банка России от 3 декабря 2012 г. N 139-И "Об обязательных нормативах банков".

Таблица 1. Обязательные нормативы банка

Индикатор	Пороговые значения
Норматив достаточности собственных средств (капитала) (Н1)	>10%
Норматив мгновенной ликвидности (Н2)	>15%
Норматив текущей ликвидности (Н3)	>50%
Норматив долгосрочной ликвидности (Н4)	<120%
Норматив максимального размера риска на одного заемщика или группу связанных заемщиков (Н6)	<25%
Норматив максимального размера крупных кредитных рисков (Н7)	<800%
Норматив максимального размера кредитов, банковских гарантий и поручительств, предоставленных банком своим участникам (акционерам) (Н9.1)	<50%
Норматив совокупной величины риска по инсайдерам банка (Н10.1)	<3%
Норматив использования собственных средств (капитала) банка для приобретения акций (долей) других юридических лиц (Н12)	<25%

Источник: составлено автором.

В таблице 2 представлен реестр индикаторов АО «Альфа-Банк» за последние 5 лет, составленный на основе вышеупомянутой инструкции ЦБ.

Таблица 2. Реестр индикаторов экономической безопасности АО «Альфа-Банк

год	Н1	Н2	Н3	Н4	Н6	Н7	Н9.1	Н10.1	Н12
2011	11,3	34,4	65,1	85,2	19,5	424,4	0	0,1	11,3
2012	11,5	40,7	65,6	76,9	19	318,6	0	0,2	10,4
2013	12,2	43,1	65,9	70	18	208,3	0	0,1	4,8
2014	11,1	61,5	93,4	99,2	24,4	323,3	0	0,1	3,9
2015	15,3	131,5	160	54,7	22,1	232,9	0	0	4

Источник: составлено автором.

Сопоставив Таблицу 2 с Таблицей 1, можно заметить, что за последние 5 лет ни один индикатор не вышел за свои пороговые значения. На основе этого можно сделать вывод о том, что не существует угроз экономической безопасности банка, которые смогли бы серьёзно повлиять на его развитие.

Тем не менее, как можно видеть на Рисунке1, начиная с 2013 года темпы роста прибыли банка сократились практически в 2 раза, а в 2015 году наблюдался отрицательный темп роста.

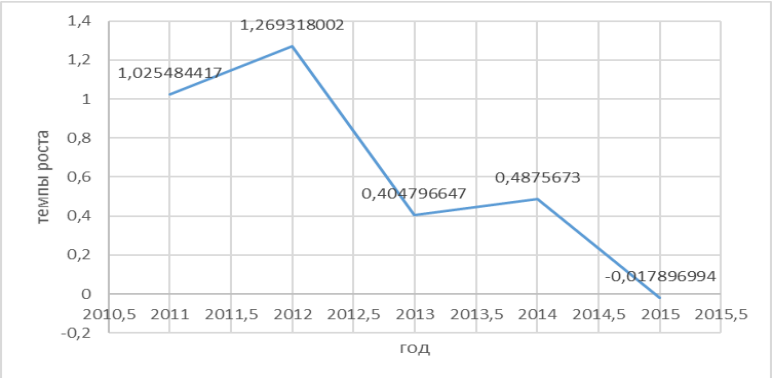

Рисунок 1 – Темпы роста прибыли АО «Альфа-банк» 2011-2015 года
Источник: составлено автором.

Замедление темпов роста, а затем и отрицательное значение этого показателя свидетельствует о наличии не выявленных угроз экономической безопасности. Основываясь на темпах роста банка за последние 5 лет и значениях показателей индикаторов экономической безопасности, необходимо пересмотреть пороговые значения данных индикаторов, не нарушая при этом Инструкцию, установленную ЦБ.

Сопоставив в рассматриваемом периоде (2011-2015 гг.) темпы роста прибыли за год со значениями индикаторов, можно прийти к следующим выводам:

1. Превышение показателя Н1 12% совпадает со снижением темпа роста прибыли (2013 и 2015 года). Увеличение значений данного показателя связано со снижение доли рисковых активов в структуре активов банков, которые в свою очередь являются более доходными, что, могло стать одной из причин снижения темпов роста прибыли. Поэтому, необходимо установить верхнее пороговое значение данного индикатора на уровне 12%.
2. Превышение показателя Н2 43% также совпадает со снижением темпа роста прибыли, начиная с 2013 года, следовательно, необходимо установить верхнее пороговое значение на данном уровне.
3. Достижение индикатора Н3 160% совпадает с отрицательным темпом роста прибыли в 2015 году, следовательно, должно быть установлено верхнее пороговое значение данного индикатора на уровне 160%.

Увеличение значений показателей Н2 и Н3 связано с ростом обязательств до востребования и увеличением их удельного веса в структуре пассивов (так в 2015 году доля удельного веса обязательств до востребования в структуре пассивов Альфа-Банка увеличилась на 1,1%). Увеличение обязательств до востребования негативно влияют на развитие банка, так как клиент может изъять их в любой момент.

4. Н4 в 2015 году снизился до 54%, что говорит о необходимости установления на этом уровне нижней границы индикатора, так как слишком низкое значение данного показателя вызвано снижением количества межбанковских кредитов (на 16%), которые также оказывают негативное влияние на рост прибыли банка.
5. Темпы роста прибыли, превышающие 100%, в 2011-2012 год, соответствовали значению показателя Н6 около 19%, следовательно, значение данного показателя совпадает с оптимальной совокупностью кредитов одного заемщика или связанных заемщиков. И отклонение от этого оптимального значения как в большую сторону (2014-2015 гг.), так и в

меньшую сторону (2013г.) может являться причиной снижения темпов роста прибыли. Необходимо установить нижнюю пороговую границу на уровне 18%, а верхнюю пороговую границу на уровне 22%.

6. Снижение значения индикатора Н7 до 300%, совпадает с резким сокращением темпов роста прибыли в 2013 году и с отрицательными темпами роста прибыли в 2015 году, следовательно, необходимо установить нижнее пороговое значение на уровне 300%. Снижение значения данного индикатора связано со снижением совокупности крупных обязательств всех его клиентов, от которых доход банка выше. Следовательно, необходимо установить нижнюю границу данного индикатора.

7. Резкое сокращение темпов роста прибыли в 2013 году и отрицательные темпы роста в 2015 году совпали со значением индикатора Н12 4,8 и 4,2 соответственно, это говорит о необходимости установить нижнюю границу данного индикатора на уровне 5%. Вложение банка в акции других юридических лиц является одним из источников дохода и их снижение также могло отрицательно сказаться на темпе роста прибыли.

С учетом вышесказанного реестр индикаторов «Альфа-Банка» выглядит следующим образом:

Таблица 2. Реестр индикаторов экономической безопасности АО «Альфа-Банка»

Индикатор	Пороговые значения	Индикатор	Пороговые значения
Н1	10-12	Н7	300-800
Н2	15-43	Н9.1	50
Н3	50-160	Н10.1	3.0
Н4	54-120	Н.12	5-25
Н6	18-22		

Источник: разработано автором.

Таким образом, данный реестр поможет своевременно выявить угрозу экономической безопасности, последствием которой стало падение темпов роста прибыли, а факторный анализ индикатора, чьи значения выходят за рамки нормативных, поможет выявить источник угрозы. Так как был исследован небольшой временной период, то при дальнейшем использовании данного реестра некоторые пороговые значения могут быть уточнены.

Список использованных источников

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. Инструкция Банка России от 3 декабря 2012 г. N 139-И "Об обязательных нормативах банков" [Электронный ресурс]. – Режим доступа: СПС Консультант Плюс. (Дата обращения: 26.12.16).

3. Официальный сайт АО «Альфа-Банк» URL: https://alfabank.ru.(дата обращения: 21.03.2017).

ИННОВАЦИОННЫЙ ПОТЕНЦИАЛ ОБОРОННО-ПРОМЫШЛЕННОГО КОМПЛЕКСА КАК СТИМУЛ РОСТА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ

Попова В.В.
Научный руководитель: к.э.н., доцент Бакулина А.А.
Финансовый университет при Правительстве Российской Федерации

Инновационная безопасность является составной часть экономической безопасности, обеспечивающей защищённость экономики путем обеспечения конкурентоспособности как выпускаемой продукции, так и научно-технических результатов, и использующей практические решения по защите от угроз и рисков в экономической сфере. Разработка и реализация инновационных проектов способствует экономическому росту и экономической устойчивости.

Согласно The Global Innovation Index, Россия поднялась на 5 позиций: с 48 места на 43 из 128 стран.[1] Несмотря на хороший результат, Россия продолжает оставаться на уровне ниже развитых стран и ниже среднего по инновационному развитию (38,5 баллов из 100).

В современных экономических и политических условиях именно оборонно-промышленный комплекс (ОПК) оснащает армию и другие специальные службы нашей страны современным и высокотехнологичным оружием, а гражданский сектор национальной экономики – инновационной продукцией. Выделять ОПК как высокотехнологичный и наукоемкий сектор позволяют следующие показатели: на долю ОПК приходится более 70% всей научной продукции России; уровень занятости научных сотрудников в ОПК составляет более 50%; ОПК обеспечивает производство 70% средств связи, 60% сложной медицинской техники. [2] В 2016 г. ОПК начал производство 32-разрядных микроконтроллеров для современных отечественных автомобилей, кораблей, электрического транспорта и робототехники – разработка высокого зарубежного уровня. Также планируется сделать упор на инновации на рынке медицинской продукции: к 2025 г. 60% отечественных производителей смогут занимать место на медицинском рынке. [3]

Последние годы ОПК активно развивается: улучшилось качество и интенсивность боевой учебы, улучшилось материально-техническое обеспечение, уровень современных образцов техники и вооружений достиг 47,2%. [4] Важно, что модернизация ОПК должна затрагивать и смежные производства, чтобы происходила и модернизация в гражданском секторе. На сегодняшний день ОПК – достоинство России, потому что производственные мощности ОПК развиваются даже в непростых макроэкономических условиях.

Однако существуют проблемы при создании научно-технических разработок, выражающиеся в нехватке финансирования НИОКР и мошеннических действиях при их выполнении. Мошенничество выражается в дублировании научно-исследовательских работ в ОПК – около 20%, а в части электронных средств – 30%. [5] Это в итоге ведет к распылению средств, и мероприятия по модернизации не достигают цели. Решить проблему, связанную с недостатком финансирования НИОКР, возможно за счет размещения научно-технических результатов в гражданском секторе, потому что изначально они обладают потенциалом двойного применения. Это позволит получать дополнительные налоги от реализации гражданской продукции, а также увеличит рентабельность оборонного производства.

Таблица 1. Доля расходов на НИОКР, 2015 %

Страна	Доля в мировых расходах на НИОКР	Доля расходов на НИОКР в ВВП страны
США	26,4	2,76
Китай	19,8	1,98
Япония	8,7	3,39
Германия	5,7	2,92

Продолжение таблицы 1

Южная Корея	4,0	4,04
Индия	3,5	0,85
Франция	3,1	2,26
РФ	2,7	1,50
Великобритания	2,4	1,78
Бразилия	2,0	1,21
Канада	1,5	1,79
Весь мир	100,0	1,75

Источник: Приоритеты зарубежных НИОКР двойного назначения / Отв. Ред.: Л.В. Панкова, С.Ю. Казеннов. – М.: ИМЭМО РАН, 2016. – 236с.

По объемам финансирования вопрос остается открытым. Уровень выполнения гособоронзаказа (ГОЗ) растет в последние годы: 2013 г. – 93%; 2014 г. – 96,7%; 2015 г. – 97,6%; 2016 г. – 98,8%, [6] что свидетельствует об эффективности направляемых бюджетных средств, но, с другой стороны, объем федеральных средств может снизиться. Именно государственный спрос на инновационную продукцию ОПК – ключевой фактор развития и распространения технологий, оказавший влияние на появление новых отраслей экономики. Развитие инновационного потенциала России невозможно без построения новой модели взаимоотношений государства. Приоритетным направлением должно быть создание контрактной системы в сфере закупок для обеспечения государственных и муниципальных нужд, выступающей основой для развития нового контрактного института в России, поскольку выполнение ГОЗ позволяет эффективнее использовать ресурсы и создает новые технологии в промышленном и непромышленном секторах экономики, повышает эффективность деятельности государства как субъекта контрактных отношений и позволяет государственному управлению переориентироваться на более гибкие контрактные механизмы.

Зарубежные санкции в отношении России оказали негативное воздействие, прежде всего, отражающееся на международном сотрудничестве. Государством должен быть проведен комплекс мер по расширению взаимовыгодного научно-технического сотрудничества внутри интеграционных объединений таких, как: Таможенный Союз, Организация договора о коллективной безопасности и другие. Необходимость в сотрудничестве связано с тем, что совместное производство позволит распределить компетенции, тем самым, разделить риски с участниками проекта и минимизировать финансовые расходы, а также получить доступ на мировые платежеспособные рынки. Более того, совместное производство создаст емкий рынок, наполненный высокотехнологичной продукцией как оборонного назначения, так и гражданского. Однако при возникновении международных конфликтов и обострении неблагоприятной международной обстановки система кооперации может давать сбои. Поэтому Россия должна развивать собственную высокотехнологичную базу, создавать новые научные разработки, но при этом не стоит закрываться от иностранных партнеров, поскольку полностью заменить кооперативную базу на отечественную невозможно.

В целях совершенствования научно-технического потенциала ОПК следует:

1. Разработать меры по стимулированию разработчиков и производителей высокотехнологичной продукции, а также разработать проект по целевой контрактной подготовке кадров для ОПК.

2. Ввести налоговые льготы для инновационных проектов, благодаря которым предприятия смогут направить сэкономленные средств на модернизацию, поскольку существующие налоговые льготы являются общими и не отражают специфику функционирования различных отраслей. Предлагается классифицировать налоговые льготы с учетом особенностей инновационной деятельности предприятий: тип инноваций, фаза жизненного цикла, стадии процесса. Действенной мерой является освобождение на определенный срок предприятия ОПК от некоторых видов налогов: на прибыль, имущество и

землю для инвестиционных проектов; от налога на дивиденды освободить средства для инвестиционных проектов.

3. Создать международный центр, концентрирующий международный опыт в сфере инновационных разработок и применений технологий.

Таким образом, в условиях технологического отставания России от развитых стран стимулирование инновационного развития ОПК является важной задачей российской экономики, поскольку он определяет эффективность функционирования высокотехнологичных и наукоемких отраслей экономики. Обеспечение экономической безопасности России в значительной степени зависит от преобразования ОПК, где и сосредоточен основной инновационный и научно-технический потенциал страны.

Список использованных источников

1. The Global Innovation Index // URL: https://www.globalinnovationindex.org/gii-2016-report (дата обращения: 17.03.2017).

2. Ростех: Объединенная приборостроительная корпорация поддержит российских производителей медтехники // URL: http://rostec.ru/news/4516394 (11.09.2016).

3. Николаев Алексей Евгеньевич Государственно-частное партнерство в научно-технологической сфере оборонной промышленности: российские реалии и Международный опыт // Экономические и социальные перемены: факты, тенденции, прогноз. 2012. №2. Режим доступа: http://cyberleninka.ru/article/n/gosudarstvenno-chastnoe-partnerstvo-v-nauchno-tehnologicheskoy-sfere-oboronnoy-promyshlennosti-rossiyskie-realii-i-mezhdunarodnyy (дата обращения: 21.03.2017).

4. Цветков В.А. Оборонно-промышленный комплекс России: проблемы и перспективы развития. Режим доступа: http://www.ipr-ras.ru/appearances/tsvetkov-opcconf-2016.pdf (дата обращения: 20.11.2016)

5. Путин: Госборонзаказ по итогам 2016 года выполнен на 98,8%. Режим доступа: http://dfnc.ru/c106-technika/putin-goboronzakaz-po-itogam-2016-goda-vypolnen-na-98-8/ (дата орбащения: 20.11.2016).

6. Президент РФ назвал приемлемыми темпы оснащения армии современной техникой. Режим доступа: http://xn--b1aecn3adibka9mra.xn--p1ai/blog/43544958101/Prezident-RF-nazval-priemlemyimi-tempyi-osnascheniya-armii-sovre (дата обращения: 21.03.2017).

ВЛИЯНИЕ ВНУТРЕННИХ КОНФЛИКТОВ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ АГЕНТСТВА НЕДВИЖИМОСТИ

Потехина В.В.
Научный руководитель: к.э.н., Кабанова Н.А.
Финансовый университет при Правительстве Российской Федерации

Основой любой организации являются люди, и представить функционирование агентства недвижимости без осуществления их деятельности невозможно. Взаимодействие трудового коллектива, возникающие потребности, их удовлетворение являются сложными процессами. Именно поэтому, ежедневно в коллективах возникают партнерские отношения, в ходе осуществления которых между сотрудниками прослеживаются противоречия по широкому кругу вопросов. Очевидно, что сами по себе данные внутренние конфликтные разногласия и противоречия могут принимать более острую форму, в результате которой ставится под вопрос экономическая безопасность хозяйствующего субъекта. Поэтому, для поддержания эффективной и устойчивой хозяйственной деятельности агентства недвижимости, важно уметь правильно установить конфликт и применить необходимые меры для минимизации рисков.

Любой хозяйствующий субъект, независимо от своего размера и специфики деятельности, представляет собой совокупность групп и людей. И там, где начинается взаимодействия людей, часто возникают конфликты. С одной стороны, в то время пока все усилия направлены на общий результат, конфликты, которые возникают в организации, скорее действуют как «целительная» сила, нежели как разрушающая. Они повышают результат работы и укрепляют отношения между сотрудниками. С помощью конфликтов появляется возможность обнаружения важной и актуальной информации, которая направлена на учет и устранение противоположных интересов до появления креативных решений, поиск новых способов развития. [1]

Однако с другой стороны, конфликты могут носить разрушающий характер в отношении хозяйствующего субъекта. Сложности в такой ситуации особенно испытывают малые предприятия. Действительно, хозяйствующий субъект - социальная система. Она представляет собой совокупность объектов и процессов, называемых компонентами, взаимосвязанных и взаимодействующих между собой. В свою очередь, компоненты образуют единое целое и обладают свойствами, не присущими составляющим компонентам, взятым в отдельности.

Из этого следует, что целостность системы и ее экономическая безопасность зависит от налаженного внутреннего механизма взаимодействия всех субъектов, ключевыми из которых являются кадры. Очевидно, что для агентства недвижимости, трудно осуществлять свою деятельность в условиях постоянно разгорающихся конфликтных ситуаций. Поэтому, необходимо жизнедеятельность, рассматриваемой социальной системы, контролировать через важнейшие функции – функцию развития и функцию безопасности.

Функция развития представляет собой конкретные действия, которые непосредственно связанны с реализацией интересов хозяйствующего субъекта и направленные на закономерное изменение конкретных материальных объектов, приводящие к возникновению качественно новых состояний.

Говоря о внутренних конфликтах, как об основных источниках возможных угроз интересам риэлторских организаций, наиболее важным является поддержание функции безопасности хозяйствующего субъекта. Целью данной функции является поддержание устойчивого функционирования организации и защита функции развития от наступления возможных внутренних угроз.

Функция безопасности имеет сложную структуру, включающую две взаимосвязанные части: родовую, которая выступает как основная, и видовую, рассматриваемую как вспомогательную.

В подтверждение того факта, что кадры являются ключевым субъектом стабильности агентства недвижимости, стоит отметить их важную роль в поддержании экономической безопасности. Следовательно, все результаты хозяйственной деятельности, так или иначе связанны с сотрудниками агентства недвижимости, цель которых достижение поставленных задач. Именно поэтому кадры – основа родовой части функции безопасности.

К видовой части функции безопасности, обусловленной условиями и факторами, ответственными за ее реализацию, следует относить как раз те самые действия, направленные на реализацию контроля и устранения возможных негативных ситуаций. Важно отметить, что невыполнение определенных действий, направленных на устранение внутренних конфликтов, может привести к гибели всей социальной системы.

Для лучшего понимания и выбора мер противодействия наступлению внутренних конфликтов, возникающих в коллективе, важно понять природу и особенности конфликта.

Итак, конфликт представляет собой столкновение противоположных точек зрения, несовместимых друг с другом тенденций в сознании отдельно взятого индивида, или группы людей, которые связаны с острыми отрицательными эмоциональными переживаниями. [2]

Всевозможные организационные изменения, возникающие противоречивые ситуации, деловые и личностные отношения между людьми нередко порождают конфликтные ситуации, которые субъективно сопровождаются серьезными психологическими переживаниями. Чаще всего именно такие переживания побуждают человека совершать резкие и не всегда хорошо обдуманные действия, наносящие ущерб эконмической и кадровой безопасности малого бизнеса.

Наиболее распространенными видами внутренних конфликтов, которые возникают в агентстве недвижимости являются следующие группы:

Конфликты по направленности действия, а именно «горизонтальные», «вертикальные», а также «смешанные». Так горизонтальные конфликтные ситуации возникаю между сотрудниками, которые находятся в подчинении друг у друга. Вертикальные конфликты возникают между сотрудниками, один из которых находится в подчинении у дугового. В смешанных конфликтах представлены и вертикальные, и горизонтальные составляющие. Исследование показывает, что в данной группе наиболее распространенным видом возможных конфликтов являются вертикальные внутренние конфликты.

Конфликты по значению для сотрудников и организации, а именно конструктивные и деструктивные. Очевидно, что первые выступают как поддерживающий фактор деятельности хозяйствующего субъекта, а вторые наоборот. Важно понимать, что исключение конструктивных внутренних конфликтов, может привести к приостановлению развития деятельности предприятия. Меры по снижению конфликтных ситуаций должны быть направлены на минимизацию деструктивных внутренних конфликтов. [3]

Характерным видом внутренних конфликтов риэлтерского бизнеса выступают ситуации, имеющие социально-психологический эффект. Данная классификация подразделяется на развивающие, утверждающие, активизирующие каждую из конфликтующих сторон в целом. Второй подвид заключается в самоутверждении одного из конфликтующих субъектов и подавлению оппонента или коллектива в целом.

Таким образом, для обеспечения экономической безопасности малого бизнеса важную роль играет снижение вероятности наступления возможных внутренних конфликтов, возникающих между сотрудниками. Действительно, кадры – ценность организации. Обеспечение всевозможных условий для поддержания рабочей и непротиворечивой атмосферы является залогом успеха деятельности хозяйствующего субъекта.

Однако, изучив часто встречаемые внутренние конфликты, можно сказать, что все они тесно связаны между собой. Чаще всего одна форма конфликта, может перейти в другую. Для разрешения конфликтных ситуаций важно уметь разграничивать, к какому виду относятся то или иное событие.

Тем не менее, внутренние конфликты могут проявляться в форме положительного воздействия, что повышает эффективность хозяйственной деятельности агентства недвижимости.

Список использованных источников

1. Управление без страха и упрека: конфликты в организации // URL: https://www.b17.ru/article/upravlenie__bez__straha__i__upreka/ (Дата обращения: 21.03.17).

2. Классификация конфликтов в организации // URL: http://society.polbu.ru/frolov_esociology/ch35_all.html (Дата обращения: 21.03.17).

3. Управление кадровыми рисками // URL: http://psyfactor.org/personal/personal10-12.htm (Дата обращения: 21.03.17).

РАЗРАБОТКА МЕТОДОВ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ В СФЕРЕ НЕЗАКОННОГО ПРИСВОЕНИЯ АКТИВОВ НА ПРИМЕРЕ КОМПАНИИ ООО «ПАНОРАМА»

Сургутанова К. Н.
Научный руководитель: к.ю.н., Буянский С.Г.
Финансовый университет при Правительстве Российской Федерации

На сегодняшний день, мошенничество считается серьезной потенциальной угрозой для компании любого размера. Как минимум 41% респондентов считают, что их компании, вероятно, столкнутся с экономическими преступлениями в ближайшие два года. [2]

Если обратиться к УК РФ, то можно определить мошенничество как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. [3] Также, стоит ввести такое понятие, как фрод. Фрод – это умышленное действие или бездействие физических и/или юридических лиц с целью получения выгоды за счет компании и/или причинить ей материальный и/или нематериальный ущерб. [4]

Главное отличие мошенничества от фрод заключается более широком подходе, который основывается на Международном стандарте аудита ISA 240. Но, в РФ данное понятие также используется при необращении компании в правоохранительные органы, то есть при недоведении дела до суда.

Что касается экономических противоправных действий в РФ, то их классификация остается неизменной уже на протяжении долгих лет.

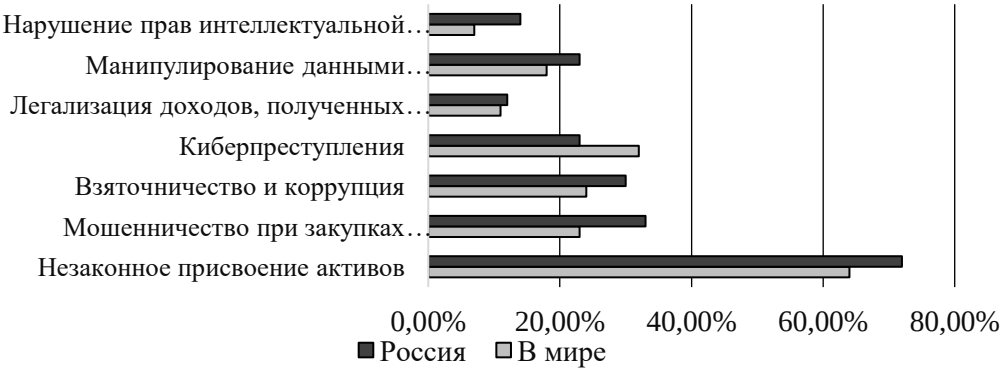

Рисунок 1. Основные виды экономических преступлений в России по сравнению с мировыми тенденциями за 2016 г.
Источник: составлено автором на основе материала «Российский обзор экономических преступлений за 2016 год». URL: http://www.pwc.ru/ru/forensic-services.

Итак, согласно рисунку 1 наиболее распространенный вид мошенничества в РФ – это незаконное присвоение активов (72%), на втором месте - мошенничество в сфере закупок товаров и услуг (33%), а уже далее - взяточничество и коррупция (30%).

Для исследования более интересен вид мошенничества - незаконное присвоение активов, так как кассовое мошенничество является его составной частью, а ООО «Панорама» - это небольшая компания в сфере розничной торговли обувными изделиями, одеждой и аксессуарами для женской половины населения.

Итак, незаконное присвоение активов – это махинации с наличными средствами, чековыми расчетами организации, получение «навара» с продажи «неучтенного товара», а также незаконное списание, неприкрытое изъятие и т.д.

Наиболее распространенными мошенническими действиями в сфере незаконного присвоения активов в компании ООО «Панорама» является кассовое мошенничество, которое и будет проанализирована в дальнейшем.

Для начала необходимо понять, что же такое кассовое оборудование. Кассовое оборудование для розничной торговли - это высокотехнологичный набор оборудования, обеспечивающий правильную работоспособность торговой точки и ускорения процесса. В состав кассового оборудования для розничных магазинов входят: POS – компьютеры, POS – мониторы, POS – клавиатура, банковский терминал, контрольно-кассовое оборудование, денежные ящики. [5]

Наконец, проанализируем наиболее распространённые виды кассового мошенничества и фрод в компании ООО «Панорама» за 2013-2016 гг.

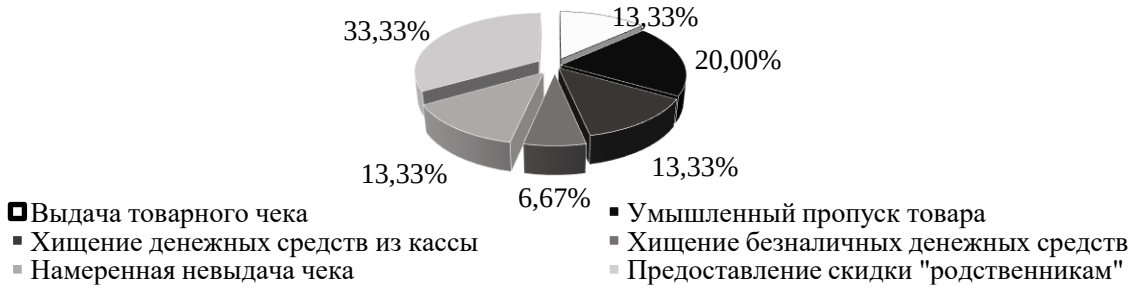

Рисунок 2. Статистика мошенничества и фрод с помощью кассового оборудования в компании ООО «Панорама» за 2013-2016 гг.
Источник: разработано автором.

На рисунке 2 можно видеть, что наиболее распространенным видом мошенничества является «Предоставление скидки «родственникам». Главное в данном виде мошенничества – это сумма ущерба, так как она является небольшой для деятельности компании и составляет примерно 58’000 руб. или 2,56% от средней месячной выручки в 2016 г.

Что касается наиболее значительного преступления в компании - хищения безналичных денежных средств, то можно увидеть, что данный вид правонарушения составляет наименьший процент, так как компания столкнулась с ним только однажды.

Как уже было сказано, ущерб от донного преступления был наиболее весомым для ООО «Панорама» и составил 300’000 руб. или 13,22% от средней месячной выручки в 2016 г. Вследствие всех совершенных правонарушений, компания потеряла за 4 года примерно 630’920 руб. Возможно, это может показаться не настолько крупной суммой для осуществления регулирования, но кризисная ситуация заставила понять, что это не так. Для компании любые денежные средства на сегодняшний день являются значительными, поэтому необходимо разработать определенные меры по минимизации данного ущерба в будущем.

В качестве мер по противодействию мошенничества с кассовым оборудованием был разработан документ «Отчет по анализу квалифицирующих признаков кассового мошенничества и системе по их противодействию ООО «Панорама», в котором четко разобраны причины совершения противоправных действий, классификация видов кассового мошенничества и рассчитан ущерб от их реализации, создан портрет потенциального мошенника, а также приведен ряд мер по противодействию кассового мошенничества с помощью технической и кадрово-психологической составляющих.

Для начала разберем портрет потенциального мошенника, с которым может столкнуться компания. Данный анализ основывался на уже произошедших мошеннических действий.

Таблица 1. Портрет потенциального мошенника

Фактор	Проблемные зоны
Возраст	19-22 г.
Стаж работы в компании	Превышает 1 год
Образование	Среднее
Уровень жизни	Ниже среднего (за счет родителей)
Проблемы в семье	✓

Продолжение таблицы 1

Семейное положение	В браке (гражданский или официальный)
Отношение с коллегами	Плохое (нечестное, неэтичное)
Финансовое положение	1. Наличие больших долгов 2. Финансовые запросы, превышающие возможности
Вредные привычки	✓ Наркомания, ✓ Пьянство, ✓ Игромания
Вредные привычки у молодого человека (мужа)	
Вредные привычки у родственников	

Источник: разработано автором.

С помощью данного портрета руководство компании сможет выявить потенциальных мошенников и предотвратить риски, связанные с нанесение ущерба активам организации. Также необходимо рассмотреть меры, которые компания сможет применить для минимизации ущерба от кассового мошенничества.

Таблица 2. Меры противодействия мошенничеству с технической точки зрения

Название вида кассового мошенничества	Метод противодействия	Стоимость (2 магазина)
Выдача товарного чека	1. Усиление наблюдения за сотрудниками с помощью видеокамер и дополнительного наблюдающего 2. Ежемесячное проведение инвентаризации 3. Синхронизация видеозаписи с информацией о кассовых операциях	1. 7’000 руб. (мес.) 2. 4’000 руб. (мес.) 3. 20’000 руб.
Умышленный пропуск товара		
Хищение денежных средств из кассы	Увеличение количество видеокамер в области кассы для устранения слепых зон (+ 3)	9’600 руб.
Хищение безналичных денежных средств	1. Ежемесячная проверка банковских операций через POS-терминал (запрос в банке, либо выписка с POS-терминала) 2. Ежемесячная ревизия кассового оборудования	1. 3’000 руб. (мес.) 2. -
Предоставление скидки "родственникам"	Создание отчета по предоставлению 20% скидок	300 руб. мес. каждому продавцу Итого: 3’000 руб.
Единоразовый платеж:		29’600 руб.
Платежи (год):		204’000 руб.
Общий итог за год:		233’600 руб.

Источник: разработано автором.

Из таблицы 2 можно видеть, что технические меры по предотвращению кассового мошенничества являются достаточно затратными, поэтому компания для себя может выбрать лишь несколько, основываясь на необходимости защиты от определенного вида противоправного действия.

Таблица 3. Меры противодействия мошенничеству с кадровой точки зрения

Метод противодействия	Стоимость

	(2 магазина)

Продолжение таблицы 3

Ежемесячная правовая работа с сотрудниками директора магазина	3000 руб.
Анализ потенциального сотрудника по портрету мошенника при приеме на работу и в течение всего рабочего периода	-
Тайный покупатель (1 раз в квартал)	2’000 руб.
Сокращение удельного веса работников магазинов с заработной платой ниже рыночной (индексирование з.п. на 3% ежегодно)	3’000 руб. (мес.)
Платежи за месяц:	6’500 руб.
Общий итог:	80’000 руб.

Источник: разработано автором.

Наконец, компания может использовать и кадрово-психологические меры противодействия мошенничеству, так как они являются е менее эффективными, а затраты на них существенно меньше (Таблица 3).

В качестве заключения, хотелось бы отметить, что каждая компания, ориентированная на женскую часть населения может использовать составленный портрет потенциального мошенника (Таблица 1). Более того, использование технических и кадрово-психологических методов противодействия кассовому мошенничеству актуально для любой компании, так как данные составляющие являются наиболее важными в экономической безопасности на сегодняшний день.

Список использованных источников

1. Уголовный кодекс Российской Федерации: текст с изменениями и дополнениями на 1 апреля 2016 г. – Москва: Эксмо, 2016. – 256 с.

2. Аудиторская компания PwC [Электронный ресурс] URL: http://www.pwc.ru/ru/forensic-services // Российский обзор экономических преступлений за 2016 год. – 2016 г. - С. 34. (Дата обращения 23.03.2017)

3. Безопасность бизнеса [Электронный ресурс]. URL: http://www.ekb-security.ru/publications/9455-kak-voruyut-kassiry-skhemy-moshennichestva-v-magazine.html // «Как воруют кассиры: схемы мошенничества в магазине». – (Дата обращения 23.03.2017)

4. Первое профессиональное агентство по выявлению лжи URL: http://alibinet.ru/pages/vorovstvo_torgovlya.html // «Кражи, мошенничество и воровство в сфере торговли». – (Дата обращения 23.03.2017)

5. ETIM [Электронный ресурс] URL: https://www.etim.ru/one-articles/65 // Кассовое оборудование - залог легальной и эффективной работы розничного магазина. - (Дата обращения 23.03.2017)

БЕЗОПАСНОСТЬ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ КОМПАНИИ

Третьякова Ю. Д.
Научный руководитель: к.э.н, Кабанова Н.А.
Финансовый Университет при Правительстве Российской Федерации

Информация обладает первостепенным значением в современном обществе. Собственные технологии и ноу-хау - важное конкурентное преимущество на рынке для каждого предприятия в отдельности и для России в целом. Во времена кризисов конкуренция особенно часто приобретает незаконный характер. К ней можно отнести использование информации, составляющей чужую коммерческую тайну.

Особо остро стоит вопрос об обеспечении безопасности коммерческой тайны, а также конфиденциальной информации на предприятиях.

Коммерческая тайна - это любая информация, которая имеет действительную или же потенциальную коммерческую ценность в силу того, что она неизвестна третьим лицам, также к данной информации нет доступа на законном основании и обладатель данной информации, который принимает меры по защите её конфиденциальности. [2]

Большинство предприятий не отличается существованием единой политики в области защиты интеллектуальной собственности и продвижении собственных интеллектуальных ресурсов на рынок.

Перед каждым руководителем должна стоять цель – создание комплексной системы обеспечения безопасности предприятия.

Согласно статистике, Компания Zecurion 70 % работников выносят информацию, составляющую коммерческую тайну, за пределы офисов. 30 % признались, что умышленно крадут информацию для дополнительного заработка, надеясь предложить сведения конкурентам, оставить для самостоятельных разработок или унести в другую компанию, сменив место работы. Однако 37% инцидентов с потерей конфиденциальных данных происходит исключительно по вине либо недостаточно подготовленного персонала, либо попросту игнорирования элементарных правила безопасности. Из-за низкой мотивации сотрудники умышленно скрывают ценную для компании информацию и не видят смысла в разработке новых идей. [1]

Сотрудники предприятия должны предупреждаться о том, что на предприятии существует режим коммерческой тайны. Обязательно должны быть разработаны приказы об организации рабочего процесса в соответствии с защитой коммерческой тайны, о компьютерной безопасности, также обязательство по неразглашению коммерческой тайны и конфиденциальной информации, перечень сведений, которые относятся к коммерческой тайне организации и инструкции по работе с документами и другими видами носителей информации, которая составляет коммерческую тайну предприятия. Затем данные документы необходимо утвердить и довести до всех сотрудников предприятия, желательно под роспись.

В целях защиты интеллектуальной собственности нужно применять организационно-профилактические и режимные меры, которые заключаются в создании перечня коммерческой тайны и конфиденциальной информации, организации системы разграничения для сотрудников доступа к информации, включённой в перечень, в контроле над доступом, хранением и передачей носителей информации, которая относится к перечню с коммерческой тайной или же конфиденциальной информацией.

На собраниях и при приёме на работу разъясняются требования юридических документов и ответственность, которая может наступить при их нарушении.

Ответственность, наступающую впоследствии разглашения коммерческой тайны, стоит прописывать отдельно в трудовом договоре, в целях профилактической и юридической защиты.

Руководством предприятия или работниками всем режимных мер необходимо вести постоянный гласный, а также негласный контроль.

На больших предприятиях рекомендуется отдельно назначать в каждое подразделение предприятия лиц, которые будут ответственны за соблюдение режима охраны коммерческой тайны в организации. В бюджет организации может быть включена расходная статья на проведение дополнительного обучения этих людей, помимо зарплаты должна быть денежное вознаграждение.

В момент увольнения сотрудника из организации ему предлагают написание расписки о неразглашении сведений, которые составляют коммерческую тайну.

В расписке должно быть указано, что бывший работник обязуется в будущем не разглашать коммерческую тайну предприятия в соответствии с действующим законодательством и не проводить в отношении указанной организации нелегальной подрывной деятельности в будущем.

Профилактическая беседа проводится специальными сотрудниками с бывшим работником на предмет неразглашения им конфиденциальной информации на ближайшие 5 лет. Продуманная и слаженная система увольнения сотрудников позволяет весомо сократить риск разглашения секретной информации.

Специалисты информационной безопасности считают, что даже самые современные системы безопасности не могут гарантировать 100%-ой защиты конфиденциальной информации, но их использование предприятиями способно уменьшить риски утечки информации. Такие системы безопасности, как DLP (Data Loss Prevention), что в переводе означает контроль утечки информации, мониторят и блокируют попытки выноса сотрудниками конфиденциальной информации за пределы предприятия почти по всем каналам. К таким каналам относится запись на флешки, печать на принтере, отправка по электронной почте и многие другие. Удобство данных систем заключается в том, что информация, которая не относится к перечню конфиденциальной информации и коммерческой тайны, может свободно передаваться сотрудниками по всем доступным электронным каналам. Уже на данный момент 40% компаний в России внедрили или находятся на стадии внедрения системы DLP, после учащения серьёзных инцидентов с утечкой информации.

Не секрет, что главный мотиватор для сотрудников – материальные блага, но существуют и другие решения.

В некоторых случаях сотрудникам даётся 15% от рабочего времени на деятельность по своему усмотрению, ориентированную на разработку новшеств, которые впоследствии могут быть отнесены к перечню с коммерческой тайной. Цель также может быть поставлена руководителем, но каким образом ее достичь работники решат сами.

Может предоставляться такая возможность, при которой сотрудники будут сами разрабатывать персональные проекты. При условии, что сотрудники для начала будут согласовывать порядок реализации проекта и ключевые его части с руководством. Может применяться и более формализованная система. Например, фиксированный процент от бюджета НИОКР организация будет выделять на проекты с высокой степенью риска, при этом любому исследователю возможно воспользоваться данным процентом бюджета.

Ежегодно в мире количество утечек информации на предприятиях возрастает в 1,5 раза. В 2017 году по исследованиям Symantec можно ожидать ещё более значительный скачок, особенно увеличатся кражи в банковской сфере, так как такая информация позволит злоумышленникам быстро монетизировать полученные сведения. Вопросы обеспечения безопасности коммерческой тайны, как важнейшей составляющей интеллектуальной собственности, влияют на уровень экономической безопасности предприятия и требуют комплексной и системной разработки.

Список использованных источников

1. Официальный сайт Zecurion URL: http://www.zecurion.ru (дата обращения: 12.05.2016)

2. Федеральный закон РФ "О коммерческой тайне" от 29.07.2004 № 98-ФЗ // Собрание законодательства Российской Федерации. с изм. и допол. в ред. от 12.03.2014

АНАЛИЗ КАНАЛОВ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В СОВРЕМЕННЫХ ОРГАНИЗАЦИЯХ

Тухбатулина М.А.
Научный руководитель: к.э.н., доцент Боташева Л.Х.
Финансовый университет при Правительстве Российской Федерации

В современных условиях информация играет важную роль в функционировании деятельности предприятия. Множество информационных данных носят конфиденциальный характер, которые нуждаются в защищенности, а в случае реализации утечки, появляется высокий риск крупномасштабных, как материальных, так и нематериальных потерь.

Обеспечение информационной безопасности на предприятии становятся с каждым днем все более сложным для защиты по причине перехода на автоматизированную безбумажную отчетность, а также совершенствуются способы и методы взлома серверов, содержащих конфиденциальную информацию хозяйствующего субъекта.

Проблема многих предприятий заключается в нежелании затрачивать дополнительные денежные средства на защиту информации, надеясь о том, что она не выйдет за пределы организации и прибегают к осуществлению защиты только после утечки информации, которая негативно сказалась на деятельности компании.

Для осуществления защиты информации необходимо провести анализ статистических данных по ее утечке.

Одним из важных аспектов защиты информации являются надежные носители, данные на которых будут менее доступны для злоумышленников. Согласно статистическим данным, такими носителями являются мобильные устройства и IM средства, доля утечки информации с данных носителей составляет всего около 1%. Также наиболее безопасными являются съемные носители, хищение информации с данных каналов находится в размере 3%. А наиболее распространённым каналом утечки информации являются бумажная документация, именно по этой причине важную информацию стоит лучше переводит на автоматизированную электронную систему (рисунок 1). [1]

Рисунок 1. Распределение утечек по каналам, 2014 г.

Также при покидании пределов организации конфиденциальной информацией высокое значение имеет отрасль, в которой находится предприятие, так как в определённых отраслях злоумышленники наиболее заинтересованы в добыче конфиденциальной информации. По подсчетам самой распространенной отраслью по утечки информации является сфера ритейла, на ее долю приходится больше половины от количества всех утечек информации, которая не

должна покидать пределы организации. Самый низкий процент утечки информации приходится на долю здравоохранения, всего около 3%. [2]

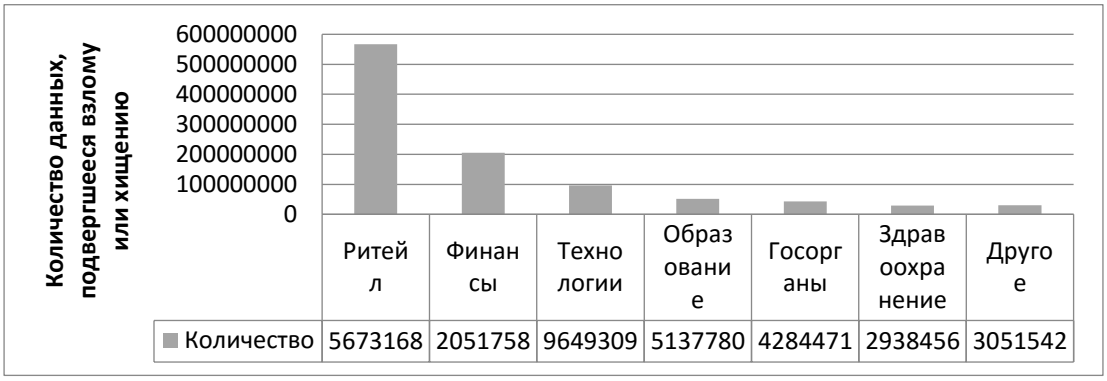

Рисунок 2. Доля утечек данных по отраслям, 2014 г.

Для владельцев организаций важно защищать все типы информации, но необходимо сосредоточить свое внимание на наиболее важных и значимых типах информации, в том числе на информации, которая наиболее часто является объектом взлома или хищения. Согласно аналитическим данным, которые были приведены компанией SafefNet наибольший уровень безопасности необходимо обеспечить для информации, содержащей идентификационные данные, содержащие финансовую отчетность. При исследовании 1541 инцидента из них 827 инцидентов были связаны с идентификационными данными, 261 - с финансовой информацией, 162 – с доступом к учетным записям, 157 – со случаями хулиганства и 8% инцидентов было связано со стратегически важными данными. [3]

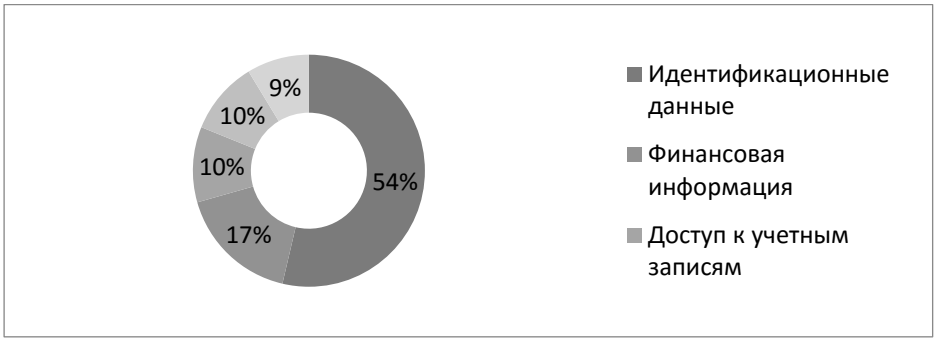

Рисунок 3. Количество инцидентов, связанных с утечкой информации по типам

Важно так же знать, что утечка конфиденциальной информации возможна со стороны внутренних источников, при чем на долю действующих сотрудников доля инцидентов самая высокая, далее по уровню опасности среди внутренних источников утечки информации находятся бывшие сотрудники предприятий, во многих инцидентах утечки информации были задействованы действующие и бывшие поставщики, консультанты, подрядчики, поставщики, контрагенты и клиенты организаций (рисунок 4). [4]

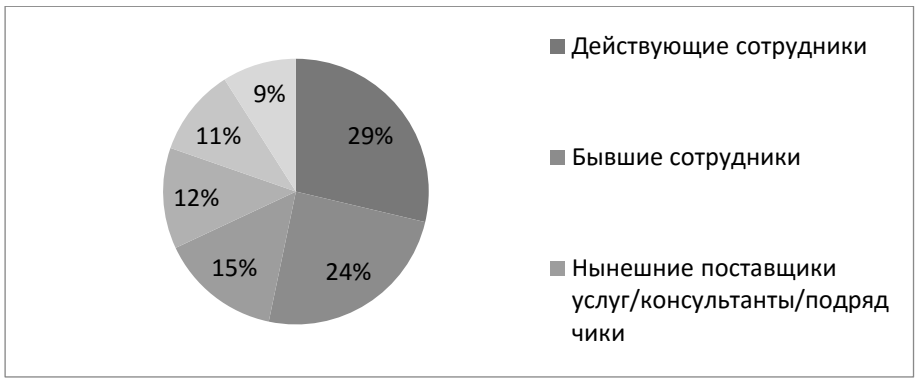

Рисунок 4. Виновники инцидентов информационной безопасности, 2014г.

Существует множество способов и мер по обеспечению информационной безопасности на предприятии, которой пренебрегает руководство многих предприятий.

Перед тем, как устанавливать то или иное обеспечение защиты необходимо провести мониторинг действий сотрудников:

- статистика по запуску сотрудниками приложений и программ;
- количество подключений и используемые съемные устройства;
- теневые копии файлов, копируемые на внешние носители;
- использование wi-fi сетей;
- копирование данных в облачные хранилища и т.д.

Данные действия позволят вести аудит запускаемых приложений и формировать картину работы персонала.

Также руководство многих организаций не использует контроля над использованием внешних устройств и не разграничивает права на доступ к информации. В то время как для надежной защиты необходимо обеспечение контроля доступа к устройствам, портам, сетевым интерфейсам, сетевым каталогом и облачным хранилищам.

Так, компанией InfoWatch был создан продукт, который позволяет контролировать более 24 видов различных устройств.

Данная программа позволяет управлять следующими правами доступа:

- управление по списку разрешённых классов носителей;
- по разрешенным моделям устройств (разрешается доступ лишь к тем моделям устройств, которые находятся в разрешенном списке, доступ к остальным запрещен);
- управление по серийному номеру устройства (разрешается доступ к устройствам с определенным серийным номером независимо от прав пользователя);
- управление по списку разрешенных беспроводных сетей (можно запретить доступ к wi-fi сетям, не входящим в список разрешенных);
- по типам файлов и размеру файлов. [5]

Большое внимание для осуществления безопасности информации необходимо уделять управлению безопасности мобильных устройств, так как за последнее время данные девайсы очень часто используются для передачи информации. Анализируя каналы утечки с данных устройств, необходимо провести контроль запуска различных мобильных приложений (формирование «черных и белых списков»), необходимо создавать возможность для дистанционного удаления файлов с мобильного устройства при его краже или потери, осуществлять контроль местоположения персонала в рабочее время и иные меры, которые разрабатываются аутсорсинговыми информационными компаниями. [6]

Также необходимо в рабочем процессе осуществлять безвозвратное уничтожение файлов на персональных компьютерах работников, которое позволит оперативно и гарантировано удалять данные по заранее заданному расписанию или по мере необходимости.

Таким образом, основными мероприятиями по предотвращению утечек конфиденциальной информации являются:

1. Политика программного обеспечения. Данный способ по обеспечению информации должен быть специально приобретен в лицензионной версии и установлен высококлассными специалистами.

2. Политика антивирусной защиты. Обязательно на предприятии должны быть установлены антивирусные программы и их регулярное обновление на персональных компьютерах сотрудников организаций, должен обеспечиваться регулярный контроль персональных компьютеров на отсутствие вредоносных файлов.

3. Политика ограниченного доступа к информационным ресурсам. На предприятии должен соблюдаться ограниченный доступ к налоговой, финансовой, бухгалтерской и иным видам отчетов, так же должна держаться в закрытом доступе информация о производстве, если такое имеется на предприятии, должен соблюдаться ограниченный доступ к персональным компьютерам, входу в систему и ограниченный доступ к электронным и бумажным папкам, содержащим конфиденциальную информацию.

4. Политика использования кодов и паролей. На предприятиях, как с большим, так и с малым количеством сотрудников, важно иметь персональные пароли для каждого персонального компьютера и папки, содержащие конфиденциальную информацию, должны быть оснащены дополнительными паролями при входе.

5. Политика контроля ограниченного доступа к конфиденциальной информации. Сотрудниками организации должны совершаться регулярные проверки на ошибки входа в систему, проверки на попытки несанкционированного входа в систему, а также пароли должны регулярно меняться для снижения риска перехвата старых данных и использования их.

6. Политика чистого стола и чистого экрана. На рабочем столе персональных компьютеров сотрудников персонала должны отсутствовать папки или ярлыки с информацией предприятия.

7. Обеспечение системы мотивации на предприятии. В организации должна создаваться и обеспечиваться система мотивации для сотрудников предприятия, чтобы у персонала предприятия было меньше мотивов для разглашения информации.

Список использованных источников

1. О новых технологиях и их влиянии на жизнь «компьютера» URL: http://www.computerra.ru/lenta/?id=117489 (Дата обращения: 15.02.2017).

2. Security to be free «Gemalto» URL: http://www.gemalto.com/ (Дата обращения: 15.02.2017)

3. Защита ценных информационных активов «SafeNet» URL: http://ru.safenet-inc.com/resource/resources7.aspx (Дата обращения: 18.02.2017)

4. Компания InfoWatch, «Типы информации, подверженные утечке» URL: https://www.infowatch.ru/analytics/panels (Дата обращения: 18.02.2017)

5. Компания InfoWatch, «Разграничение доступа сотрудников к важной информации» URL: https://www.infowatch.ru/products/endpoint_security/features (Дата обращения: 18.02.2017)

6. Проект ИТ-защита «Проблемы безопасности мобильных устройств, систем, приложений» URL: http://itzashita.ru/mobilnyie-ustroystva/problemyi-bezopasnosti-mobilnyih-ustroystv-sistem-i-prilozheniy-chast-2.html (Дата обращения: 18.02.2017)

ОПРЕДЕЛЕНИЕ НЕДОСТАТОЧНО РАЗВИТЫХ КОМПОНЕНТОВ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА И РАЗРАБОТКА МЕТОДОВ ИХ РЕГУЛИРОВАНИЯ НА ПРИМЕРЕ КОМПАНИИ ООО «ПОСТУПЬ»

Чупилина Т.С.
Научный руководитель: к.э.н, доцент Кабанова Н.А.
Финансовый Университет при Правительстве Российской Федерации

Для анализа характеристики и тенденций развития малого бизнеса в России в первую очередь необходимо выявить критерии отнесения компаний к данной форме предпринимательской деятельности. В России в соответствии с Федеральным Законом "О развитии малого и среднего предпринимательства" средняя численность работников за календарный период не должна превышать предельного значения - ста человек включительно для малых предприятий. [1] Предельные значения выручки от реализации товаров (работ, услуг) за предшествующий календарный год без учета налога на добавленную стоимость установлены для каждой категории субъектов предпринимательства в соответствии с Постановлением Правительства РФ от 13.07.15 N 702. Микропредприятия могут получать до 120 млн. рублей, а малые - до 800 млн. [2]

В 2015 году большая часть компаний малого бизнеса занимались следующими видам экономической деятельности 38,8% - оптовой и розничной торговлей, 20,4% - операциями с недвижимым имуществом, 11,9% - строительством. [3]

ООО «Поступь» - ортопедический салон в г. Мытищи. Основной вид деятельности: розничная торговля обувью, фармацевтическими товарами и ортопедическими изделиями. В компании представлена продукция более 50 торговых марок и огромный ассортимент ортопедической обуви для взрослых и детей.

Объем товарооборота в 2015 году составил 24897, а чистая прибыль компании 6663000 руб., что ниже значений прошлого года. [4] Это связано в первую очередь с появлением в 2015 году на рынке г. Мытищи крупного сетевого салона Ортека. Деятельность компании активно развивается, приобретается и реализуется современная продукция, сотрудники салона следят за изменениями на рынке ортопедической продукции и регулярно внедряют дополнения к предоставляемым товарам и услугам.

В компании работает 12 человек: генеральный директор; заместитель директора, ответственный за экономическую безопасность; бухгалтер; маркетолог; менеджер по продажам; ортопед-остеопат; врач семейной практики, ортопед; 5 техников-ортопедов. [5] В качестве наиболее подходящей формы организационной структуры была выбрана линейная структура управления персоналом

В современном мире для любой компании особую роль играют экономическая безопасность и устойчивое, стабильное развитие. Переход страны к рыночной экономике привел к формированию широкого спектра потенциальных рисков и угроз, поэтому компаниям приходится уделять больше внимание вопросам обеспечения своей безопасности.

Для определения уровня экономической безопасности ООО «Поступь» в первую очередь необходимо выделить её основные составляющие, оценка которых будет рассчитана по 100 бальной шкале в зависимости от числа мер, принятых по регулированию компонента. Также необходимо определить степень, в которой каждый из компонентов способен повлиять на общий уровень показателя. Для этого в оценочной модели будет присутствовать весовой коэффициент k, а сумма всех коэффициентов должна быть равна 1.

Таким образом, математическая модель экономической безопасности будет выглядеть следующим образом:

$$ES = TS * k_{TS} + FS * k_{FS} + SS * k_{SS} + LS * k_{LS} + IS * k_{IS} + PS * k_{PS}$$

Технико-технологическая безопасность (TS) определяется наличием и использованием компанией современных технических средств для выполнения рабочих обязанностей

сотрудников, конкурентоспособностью технического потенциала фирмы, её инновационность.

Финансовая безопасность (FS) определяется уровнем финансовой эффективности, стойкости и независимости компании.

Кадровая безопасность (SS) зависит от квалификации сотрудников, качества выполнения ими должностных обязательств и интеллектуального потенциала.

Показатель политико-правовой (LS) безопасности выявляется в зависимости от степени соответствия деятельности фирмы законодательству страны, правильности ведения всей бухгалтерской отчетности, соблюдения требований к составляемым договорам и тд.

Информационная безопасность (IS) заключается в уровне обеспечения защиты всех информационных источников компании, степени сохранности и определенности конфиденциальных данных, проводимых мер по сохранению недоступности к носителям информации посторонних лиц.

Силовая безопасность (PS) – это обеспечение физической безопасности персонала фирмы, её капитала и имущества.

Если в фирме не принимается никаких действий по регулированию компонента, то он равен 0. Когда руководство начинает внедрять мероприятия для изменения элемента, но польза от них невелика из-за необходимости принятия дополнительных решений, либо они не работают, значение варьируется от 10 до 30. В том случае, если принятые меры обеспечивают регулярный контроль, но по каким-то причинам не охватывают направления полностью – 40-50. Коэффициент равен 60-80 в зависимости от эффективности принимаемых действий, в данную категорию входят элементы, по отношению к которым принимается комплексный подход по обеспечению безопасности, регулярно вводятся изменения, но в связи с изменением внутреннего и внешнего состояния состояние не всегда стабильно. 90-100-идеальное состояние безопасности, не зависящее ни от каких обстоятельств.

В связи со спецификой деятельности ООО «Поступь» и присутствием на рынке города Мытищи сильных оптовых конкурентов особую важность для компании имеет её информационная безопасность. Фирма изготавливает уникальные ортопедические стельки по технологии, доступной только её сотрудникам, они являются основным конкурентным преимуществом салона. По этой же причине не менее важным аспектом является технико-технологическая составляющая, способная обеспечивать спрос со стороны целевой аудитории. Эти части экономической безопасности обеспечивают регулярный приток новых клиентов, поэтому значение $k_{IS}=k_{TS}\approx 0{,}195$. $K_{SS}\approx 0{,}25$, поскольку именно сотрудники салона являются основным источником угроз его безопасности, а значит, влияние данного коэффициента особенно велико. Остальные компоненты, несомненно, также важны, их значение≈0,12.

Таблица 2

Компонент ЭБ	Оценка регулирования аспекта	Коэффициент
Информационная безопасность (IS)	50	0,195
Финансовая безопасность (FS)	60	0,12
Технико-технологическая безопасность (TS)	70	0,195
Политико-правовая безопасность (LS)	80	0,12
Кадровая безопасность (SS)	90	0,25
Силовая безопасность (PS)	90	0,12

В ООО «Поступь» уровень экономической безопасности принимает следующее значение:

$$ES = 70 * 0{,}195 + 60 * 0{,}12 + 90 * 0{,}25 + 80 * 0{,}12 + 50 * 0{,}195 + 90 * 0{,}12$$
$$= 13{,}65 + 7{,}2 + 22{,}5 + 9{,}6 + 9{,}75 + 10{,}8 = 73{,}5\ (\%)$$

Уровень экономической безопасности салона достаточно высок, однако существуют важные её аспекты, нуждающиеся в установлении дополнительных мер регулирования. В

первую очередь, генеральному директору необходимо обратить внимание на информационную безопасность, поскольку именно это направление отвечает за сохранение конфиденциальных данных об ортопедическом салоне, а отсутствие регулирования данного компонента на высоком уровне может привести к потере конкурентных преимуществ. В связи с этим необходимо провести ряд дополнительных мероприятий и оценить число затрат на них.

1. Закупка официальных антивирусных программ на все компьютеры - 4 шт по 900-1000 рублей

2. Видеокамеры в кабинет менеджера по продажам, бухгалтера и маркетолога, на склад, дополнительную камеру в торговый зал (над кассовым аппаратом)-3 шт по 3000-4000 рублей

3. Сетевая камера D-Link DCS-5030L в кабинет генерального директора за 12400-15200 рублей

4. Закупка стеллажа для хранения документации с грифом «коммерческая тайна» (КТ), 2500-3000 рублей

5. Покупка журнала для записи пользователей информации за 500-1000 рублей

6. Более того, необходимо доработать нормативно-правовое регулирование информационной безопасности:

- Добавление в концепцию ИБ пункта о том, что всем сотрудникам необходимо изменять пароли для доступа в систему каждый месяц.
- Разработка положения о коммерческой тайне, включающая в себя документы из приложения №2, меры по их охране, определение прав доступа, потенциальные риски и способы противодействия им и др.

Таким образом, общее число затрат составит 28000-35200 рублей.

Эффективность всех мер, предлагаемых в разделе 3.1 можно посчитать, разделяя на 3 группы все издержки на покрытие ущербов, которые компания понесла от инцидентов, связанных с информационной безопасностью:

Первая группа событий приводит к незначительным финансовым потерям-до 20000 рублей. Такие ситуации случаются в компании примерно 5 раз в год, а, значит, сумма ущерба составляет 20000*5=100000.

$$R = \frac{\text{Предполагаемый ущерб}}{\text{Сумма затрат на реализуемые меры}} = \frac{100000}{31600} = 3,16\%$$

События, приводящие к среднему ущербу (20 тыс. руб. – 50 тыс. руб.), случаются несколько реже - около 3 раз в год. Общий ущерб в данной группе составляет 150000, тогда рентабельность реализуемых мер:

$$R = \frac{\text{Предполагаемый ущерб}}{\text{Сумма затрат на реализуемые меры}} = \frac{150000}{31600} = 11,03\%$$

События из группы крупного ущерба (>50000) происходит в компании максимум 1 раз в год, следовательно:

$$R = \frac{\text{Предполагаемый ущерб}}{\text{Сумма затрат на реализуемые меры}} = \frac{50000}{31600} = 1,59\%$$

Таким образом, предлагаемые меры будут актуальны для всех групп угроз, причем наибольшую эффективность они покажут для событий, приводящих к среднему ущербу. При внедрении данных действий, IS≈90, а уровень экономической безопасности в целом при этом возрастет на 7,8% по сравнению с текущим значением:

$$ES = 70 * 0,195 + 60 * 0,12 + 90 * 0,25 + 80 * 0,12 + 90 * 0,195 + 90 * 0,12$$
$$= 13,65 + 7,2 + 22,5 + 9,6 + 17,55 + 10,8 = 81,3\ (\%)$$

Список использованных источников

1. Федеральный Закон РФ "О развитии малого и среднего предпринимательства в Российской Федерации" от 24.07.2007 № 209-ФЗ // Российская газета.

2. Постановление Правительства РФ "О предельных значениях выручки от реализации товаров (работ, услуг) для каждой категории субъектов малого и среднего предпринимательства" от 13.07.2015 № 702

3. Статистический сборник «Малое и среднее предпринимательство в России. - М.: Росстат, 2015. - 96 с.

4. СПАРК-Проверка контрагентов URL: http://www.spark-interfax.ru/ (дата обращения: 18.03.2017)

5. Сайт компании ООО «Поступь» URL: http://www.stopa03.ru/ (дата обращения: 18.03.2017).