УДК 338

МЕТОДЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ СЛУЖБЫ ВНУТРЕННЕГО КОНТРОЛЯ ОРГАНИЗАЦИИ ПРИ БОРЬБЕ С КИБЕРПРЕСТУПЛЕНИЯМИ И МОНИТОРИНГ СОВРЕМЕННОЙ СИТУАЦИИ

Инжеватова В.С.

Бакалавр

РЭУ им.Г. В. Плеханова

Москва, Россия

Аннотация. В современном обществе все большее количество организаций сталкиваются с экономическими преступлениями, а особенно – с киберпреступлениями, которые крайне негативно влияют на экономическую безопасность организаций. Для того чтобы предотвратить колоссальную потерю экономической безопасности не только в организациях, но и в стране в целом, необходимо оценить текущую ситуацию по экономическим киберпреступлениям в Российской Федерации, провести анализ тенденций, а также выявить методы борьбы с киберпреступлениями в организациях.

Ключевые слова. Киберпреступления, мошенничество, ответственность, меры противодействия.

METHODS OF INCREASE OF EFFICIENCY OF ACTIVITY OF SERVICE OF INTERNAL CONTROL OF THE ORGANIZATION IN THE FIGHT AGAINST CYBERCRIME

Inzhevatova V.S.

Bachelor

Plekhanov Russian University of Economics

Moscow, Russia

Abstract. In the global society, an increasing number of organizations are faced with economic crimes, in features – with cybercrimes which negatively affect the economic security of organizations. To prevent huge decline of economic security not only of organizations but the country in General, it is necessary to assess the current situation of economic cybercrime in the Russian Federation, to analyze trends, and to identify methods of combating cybercrime within organizations.
Keywords. Cybercrime, fraud, responsibility, countermeasures.

В настоящее время в условиях развития рыночных отношений каждая компания ставит перед собой основной задачей – получение прибыли.

Как только организация добивается успеха либо на местном, либо на мировом уровне, управленческому звену необходимо сразу же позаботиться о том, как сохранить денежные средства, товарно-материальные ценности организации от деяний мошенников.

Актуальность данной темы заключается в том, что организации ежегодно сталкиваются со всякими видами киберпреступлений, и, при этом, теряют значительную часть выручки.

Целью исследования является изучение основных методов киберпреступлений и способов борьбы с ними.

Однако, с развитием рыночных отношений, совершенствуются и методы, через которые мошенники совершают свои преступления. [5]

Самыми широко известными методами являются незаконные присвоения активов, мошенничество при закупках товаров, работ и услуг, взяточничество и коррупция (Рисунок 1).

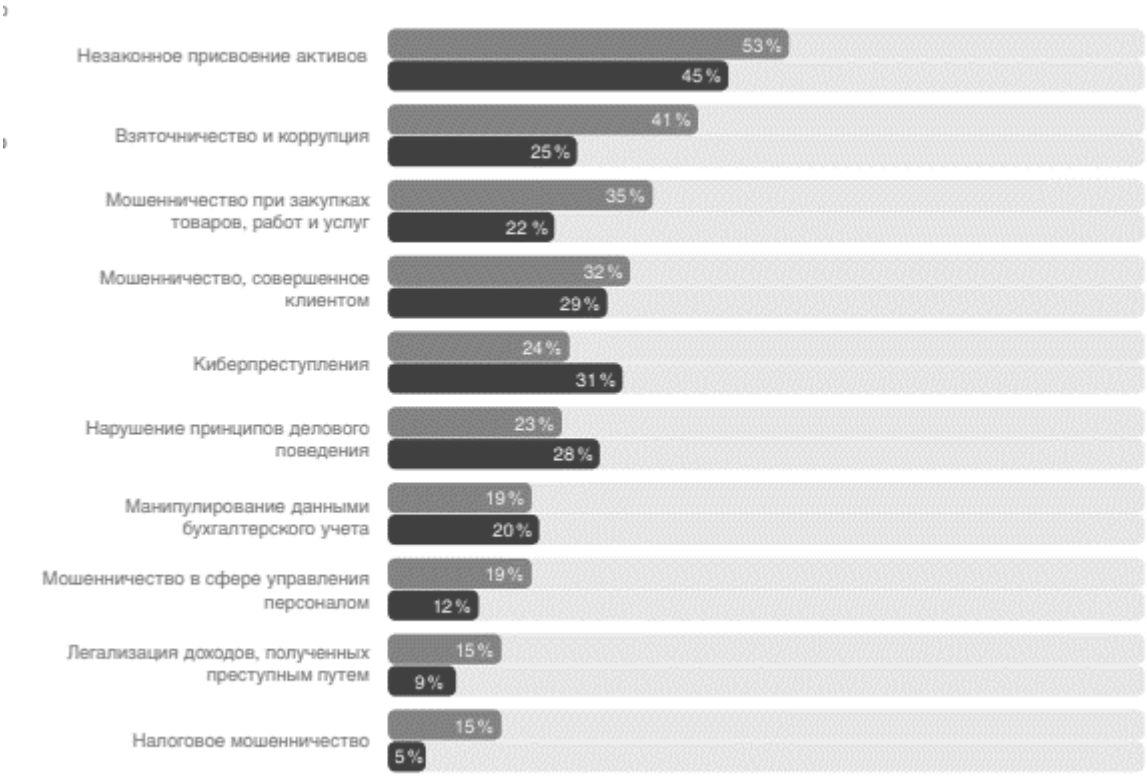

Рисунок 1 - Основные схемы мошенничества в Российской Федерации и мире в целом [1]

Рассмотрим схемы мошенничества по отраслевой специфике.

Приписки и пересортица. Приписки и пересортица очень распространены в сфере поставки сырья и материалов, используемых в производстве. При приемке, например, металлолома, сплавляющих материалов или семян подсолнечника пишется несуществующий объем, более высокое качество, большее содержание доли активного элемента, большая чистота сырья и т.п. При взвешивании масса «добирается» землей, отходами железобетона, некондиционной фракцией и т.п. На практике бывали случаи откровенного «беспредела»: после первого взвешивания машины даже не разгружались и отправлялись на второй круг. Поставщик оплачивает приписки приемщику или его руководителю, иногда прямо на месте. Метод может работать в совокупности со слабым входным контролем и бесконтрольным списанием затрат на производство.

Подобная схема работает и в отношении товарной продукции. Так, слитки дорогостоящих металлов списываются под видом более дешевых. Качественная книжно-журнальная продукция «бракуется» и реализуется как нестоящая по низким ценам (как правило, одной и той же организации), а затем продается на потребительском рынке по ценам, приближенным к рыночным.

Повторная закупка и списание. Мошенничества с дорогостоящими объектами, запчастями, оборудованием могут исполняться по данной схеме: закупка (реальная) - списание (часть — реально, часть — фиктивно) - закупка (фикция). В махинации задействованы поставщик, лицо, принимающее и хранящее товар, и лицо, которое несет ответственность за их установку, использование и списание. По методу повторной закупки и списания хорошо «проходят» запчасти, узлы для транспорта и оборудования, арматура и оснастка. Приключались и весьма нестандартные случаи. Так, комиссия из 4 человек два дня проводила инвентаризацию запчастей, узлов, материалов и конструкций по службе главного механика одного крупного производства. В итоге выявили, что шесть из восьми двадцати тонных контейнеров заполнены уже «списанными» ценностями. В данных условиях повторная закупка не предоставит сложности, особенно когда на предприятии два или более производств. Еще один вариант той же схемы: основное оборудование списывается как металлолом, экспортируется за границу и модернизируется, следом ввозится обратно под видом нового. «Заграница» в данной схеме — необязательный этап— модернизация может осуществляться внутри одной страны.

«Откаты» и другие махинации с ценами. «Откатные» схемы как способы манипуляций работников используются в самых разнообразных направлениях: покупки по завышенным ценам, предоставление товара подешевле по индивидуальным заказам, более высоких скидок. Во всяком случае организация-контрагент извлекает дополнительную денежную сумму,

откуда платит работнику, корректирующему цены. Аргументы сокрытия знакомы: значимость клиента, короткие сроки исполнения, хорошая репутация поставщика, неимение альтернативного варианта и т. п.

Другой вариант способов ценовых манипуляций: настоящие цены скрывают, а покупателю представляют товар по более высоким. В момент, когда покупатель просит «разрешить вопрос по вознаграждению», ему предлагаются цены из реального прайс-листа. Такая, безобидная на первый взгляд, «игра» в реальности влечет за собой значительные потери для фирмы: нарушение ценообразования и трудовой мотивации и, как вытекающее, падение доходности продаж. Все вышеперечисленные методы работают при отсутствии действующих регламентов ценообразования и анализа сложившегося состояния цен.

Некоторые виды мошенничеств не зависят от эффективности политики ценообразования. К примеру, сотрудник компании-продавца оформляет сделку по реализации (отделочных материалов) обычному заказчику (собственнику квартиры) на заказчика, имеющего более высокие скидки (дизайнер), и эту разницу в ценах оставляет себе.

Еще один вариант «обратного отката» встречается при сложных и ценных продажах: денежные средства, направленные на коммерческий подкуп закупщика, распределяются, и часть достается продавцу.

Киберпреступность же в нынешнем ее проявлении делится на два направления: преступления против личности и преступления против государства.

В обоих случаях можно выявить подразделы, например: преступления, направленные на личность, можно разделить на «экономические» и «моральные».

Преступления (экономические), направленные на имущество (мошенничество, кража личных данных, денег, информации и т. д.),

на сегодняшний день считаются наиболее популярными киберпреступлениями. Однако они уже давно находятся «под прицелом» правоохранительных и законодательных органов. Для них практически введен свой уголовный кодекс в большинстве стран мира, хотя, вероятно, он также может быть усовершенствован как с правовой точки зрения, так и со стороны защиты самих данных или иной собственности.

Преступления (моральные) против репутации личности (распространение через социальные сети ложной или порочащей честь человека информации). И хотя тут также есть прецеденты уголовного законодательства, проблемы в данном разделе значительно глубже, чем в первом случае. А особенно они свойственны демократическому обществу, к примеру, во время избирательных кампаний.

Статистика за 5 лет

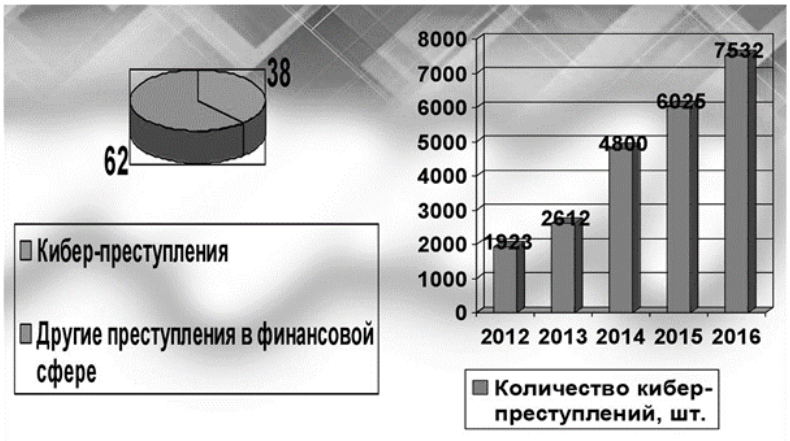

Рис. 3. Доля кибер-преступлений в общей численности преступлений в финансовой сфере

Рис. 4. Динамика численности кибер-преступлений

Однако, на начало 2018 года в мире с данным видом мошенничества столкнулись 31% организаций, по сравнению с 2016 показатель снизился на 1% (второе место среди экономических преступлений в мире), в Российской Федерации – 24 % (четвертое место среди экономических преступлений), в 2016 было 23%. Следует отметить, что данный показатель не является абсолютно точным в силу того, что:

- существует ограниченность при составлении выборки для проведения опроса с целью анализа данных;
- даже среди опрошенных организаций существует вероятность того, что респондент отвечал, что не пострадал от киберпреступлений, элементарно не подозревая об обратном.

Киберпреступления как отрасль мошенничества в нынешнее время широко распространены из-за столь динамичного развития информационных технологий.

Каждое новое открытие в информационных технологиях предоставляет все более новые преимущества для кибермошенников. Однако, проблема кибермошенничества – это не только проблема информационных технологий, это еще и одна из основных современных бизнес-проблем.

При этом, данный вид мошенничества является одним из самых сложных для борьбы со стороны службы внутреннего контроля организации.

За последнее время восприятие рисков киберпреступлений в организациях нашей страны динамично изменяется (Рисунок 2).

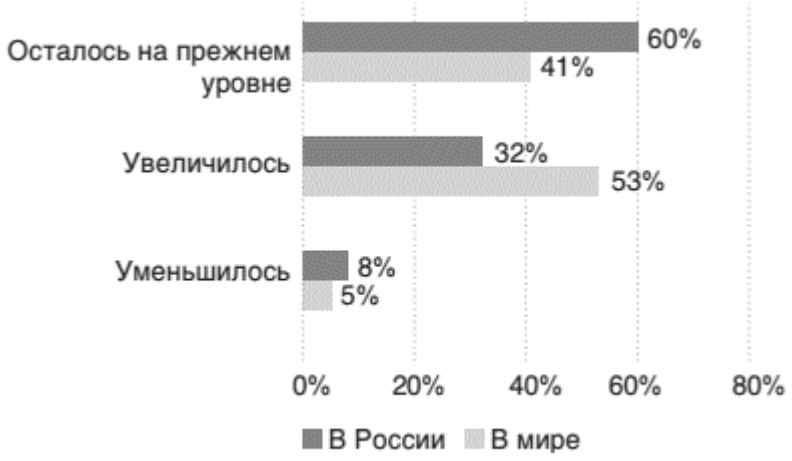

Рисунок 2 - Изменение восприятия рисков киберпреступлений [1]

Каждый год все большее количество организаций считают, что данный риск неуклонно растет.

Абсолютно в любой организации, которая сталкивается с киберпреступлениями, возникает колоссальный ущерб в той или иной форме (Рисунок 3):

- возникают финансовые потери;
- происходит потеря конфиденциальных данных;
- наносится огромный ущерб репутации организации;
- происходит нарушение нормального режима работы организации
- возникают дополнительные расходы, направленные на борьбу с последствиями после киберпреступлений.

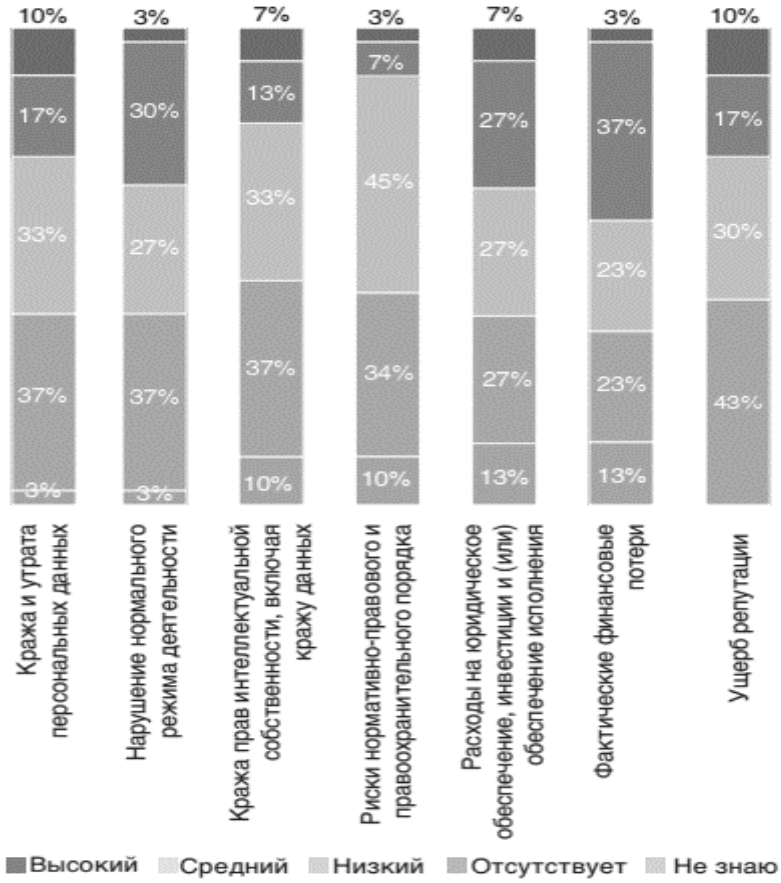

Рисунок 3 - Уровень влияния киберпреступлений на деятельность компании [1]

На сегодняшний день в нашей стране зафиксировано, что нанесение ущерба репутации и хищение персональных данных - одни из самых деструктивных последствий от киберпреступления в организации. Затем следуют хищение интеллектуальной собственности и расходы на юридическое обеспечение и принудительное исполнение.

Руководству любой компании вместе с отделом внутреннего контроля и специалистами по IT сследует обратить внимание на то, как противостоять и реагировать на киберпреступления, а также как совместно создавать план реагирования на типовые инциденты (Рисунок 4).

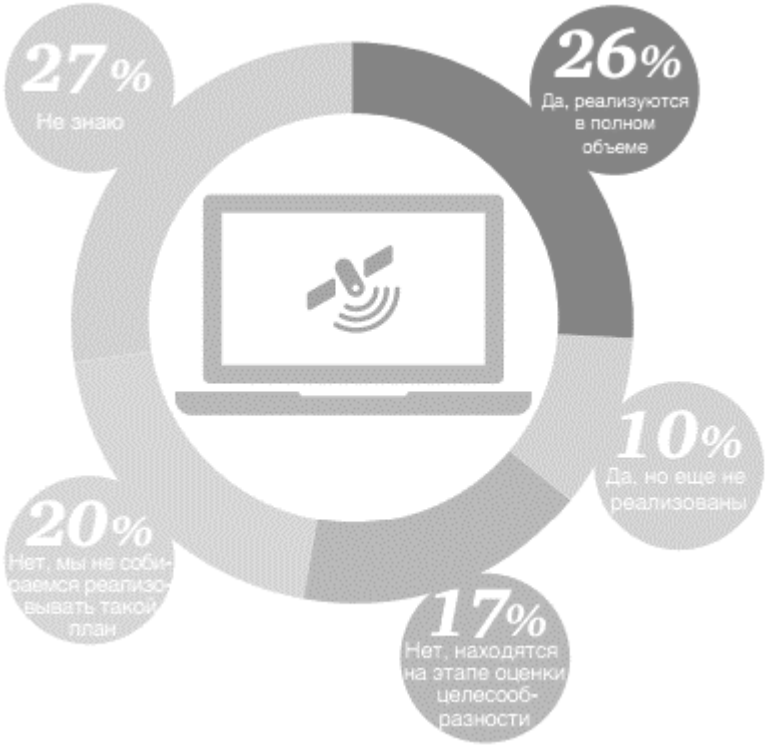

Рисунок 4 - Наличие в организациях планов реагирования на инциденты для решения проблем, связанных с кибератаками [1]

Идентификация угроз в области информационных технологий и их сокращение являются обязанностями всех подразделений компании.

Распределение обязанностей и координацию действий при киберпреступлениях берет на себя служба внутреннего контроля.

Минимизация рисков информационных технологий должна исходить от службы внутреннего контроля, при постоянном взаимодействии с другими подразделениями организации.

Внутренний контроль для борьбы с киберпреступлениями должен осуществляться через:

- уровень руководства;
- службу внутреннего контроля и аудита;
- юридическую службу;
- службу информационных технологий.

Внутренний контроль руководящего звена должен заключаться в:

- Разработке стратегии информационной безопасности
- Обеспечении получения и передачи качественной информации
- Внедрении программ осведомленности о безопасности
- Поддержке стратегии расходов на безопасность

Рисунок 5 - Взаимодействие служб системы внутреннего контроля организации [1]

Таким образом, система внутреннего контроля по вопросам борьбы с кибермошенничествами может работать эффективно лишь в том случае, если в нее будут входить специалисты различных областей, которые только вместе смогут разработать и внедрить в действие эффективную методику, основанную на синтезе следующих сфер:

- Анализ потенциальных рисков организации
- Юридическая поддержка
- Совершенствование информационных технологий
- Стратегия развития руководящего звена.

Библиографический список:

1. Алиев В.М. Современные тенденции в распространении экономической преступности // Безопасность бизнеса. 2014. N 3. С. 34 - 36.
2. Трунцевский Ю.В. Статья: Криминальные угрозы обеспечению корпоративной экономической безопасности в сфере промышленности и торговли: мировой опыт [Электронный ресурс]//Безопасность бизнеса, 2016, N 1. С. 6 - 13. – URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=CJI;n=95626#0(дата обращения 08.05.2018)
3. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 06.07.2016). [Электронный ресурс] / Консультант-плюс. – 1999-2016. – Электрон. дан. – Режим доступа: http://base.consultant.ru (дата обращения: 08.05.2018).
4. Федеральный закон «О противодействии коррупции» от 25.12.2008 N 273-ФЗ (действующая редакция, 2016). [Электронный ресурс] / Консультант-плюс. – 1999-2016. – Электрон. дан. – Режим доступа: http://base.consultant.ru (дата обращения: 08.05.2018).
5. PwC’s Global Economic Crime Survey 2016. A closer look at the Russian cut of the survey. [Электронный ресурс]//http://www.pwc.ru/ (дата обращения 08.05.2018)

Оригинальность 73%