УДК 004.056.5

ТИПЫ УГРОЗ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

© 2015 Н.В. Никитина, А.В. Балановская, А.В. Волкодаева*

Ключевые слова: угроза, инцидент, информационная безопасность, атака, информация, преступление, защита, информационная система.

Рассматривается достижение состояния защищенности информационной среды с позиции трех проблем, представлена структура угроз информационной безопасности, инциденты информационной безопасности крупных российских компаний, приведена статистика внутренних угроз безопасности информации в корпоративных информационных системах. Акцентируется внимание на сведениях промышленных компаний, нуждающихся в защите, обозначены цели информационных атак на систему безопасности предприятия, приведена классификация информационных преступлений и статистика событий с подозрением на инцидент в системе информационной безопасности российских компаний, рассмотрены основные пути обеспечения информационной безопасности предприятия.

Обеспечение доступности, целостности и конфиденциальности информационных ресурсов является одной из ключевых задач для эффективного функционирования современной организации. К подобным ресурсам можно отнести информацию о новых проектах, бизнес-планах, сотрудниках, нематериальных активах, о текущей деятельности организации, информацию финансового и технического характера, данные бухгалтерского учета, контракты и договоры.

Вся подобного рода информация, в основном, хранится и обрабатывается при помощи автоматизированных информационных систем, а значит, результат деятельности предприятия во многом зависит от устойчивости и защищенности этих систем от действий злоумышленников, конкурентов.

Состояние защищенности информационной среды позволяет предприятию быть уверенным в эффективности системы информационной безопасности, которая реализуется путем использования различных мер технического, организационного и правового характера. Достижение состояния защищенности информационной среды важно рассматривать с позиции трех взаимоувязанных проблем: проблема защиты информации от влияния внутренних и внешних угроз в системе; проблема защиты информации от информационных угроз; проблема защиты внешней среды от угроз со стороны находящейся в системе информации.

Важно отметить, что проблема защиты от информационных угроз является более серьезной, нежели проблема защиты информации в целом, поскольку процесс выявления воздействия информационных угроз является более сложным.

Эффективная система информационной безопасности позволяет защитить информационную систему предприятия и предвидеть возникновение информационных угроз, приводящих к нарушению конфиденциальности информации, а также к неправомерному ее тиражированию. Существует множество угроз, подрывающих обеспечение информационной безопасности предприятия. Если некоторое время назад 82% угроз были внутренними (несовершенство системы защиты информации, низкая квалификация сотрудников, устаревшие программно-технические средства хранения и обработки данных, использование нелицензионного программного обеспечения, недостаточная техническая безопасность помещений и др.), 17% - вне-

* Никитина Наталья Владиславовна, кандидат экономических наук, доцент. E-mail: nikitina_nv@mail.ru; Балановская Анна Вячеславовна, кандидат экономических наук, доцент. E-mail: balanovskay@mail.ru. - Самарский государственный экономический университет; Волкодаева Арина Валерьевна, кандидат экономических наук, доцент Самарского института управления. E-mail: arina-21@mail.ru.

шними (шпионаж, шантаж, дезинформация; атаки на систему защиты с целью кражи, уничтожения, искажения информации, подрыва нормальной работы подразделений, отсутствие на рынке достаточного количества сертифицированных средств защиты информации, неполноценность существующей нормативно-правовой базы информационной безопасности и деятельность недобросовестных партнеров, клиентов) и 1% - случайными, то сейчас основными проблемами обеспечения информационной безопасности среди внешних названы недостаток специалистов по информационной безопасности (37%) и несовершенство нормативно-законодательной базы (26%)[1], среди внутренних - низкая квалификация сотрудников или вовсе наличие вакантных мест для специалистов по информационной безопасности, несовершенство системы защиты информации (36%), случайные угрозы остаются на том же уровне (1%) (рис. 1).

Невыявленные угрозы информационной безопасности становятся инцидентами, оказывающими негативное влияние на деятельность всей компании. Рассматривая подробнее инциденты в сфере информационной безопасности крупных российских компаний[2], можно говорить, что большинство из них связано с атаками из Интернета (рис. 2).

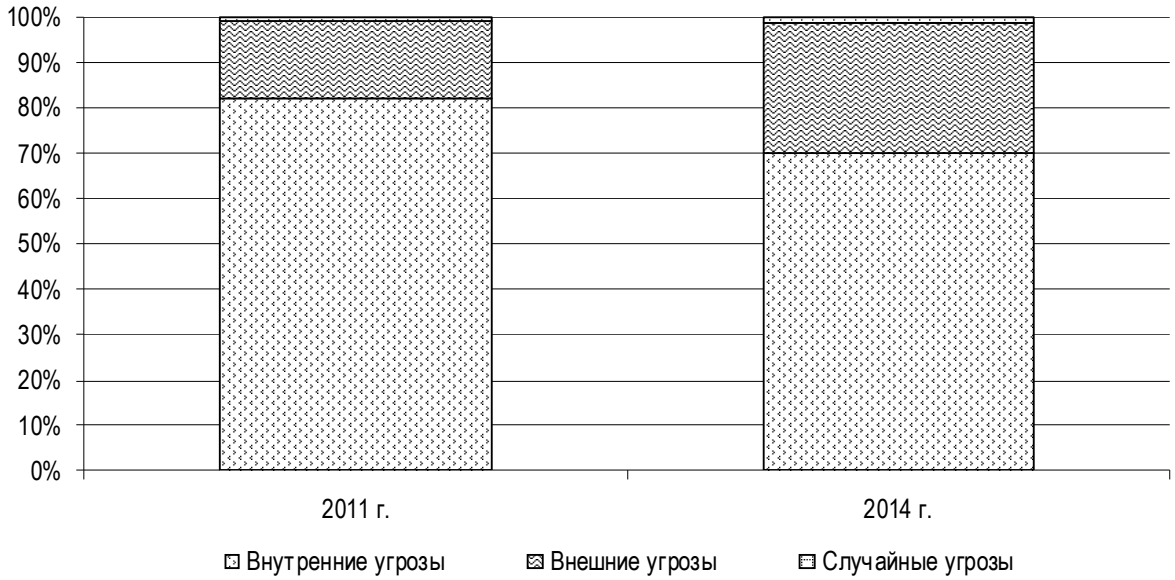

Рис. 1. **Структура угроз информационной безопасности предприятия**

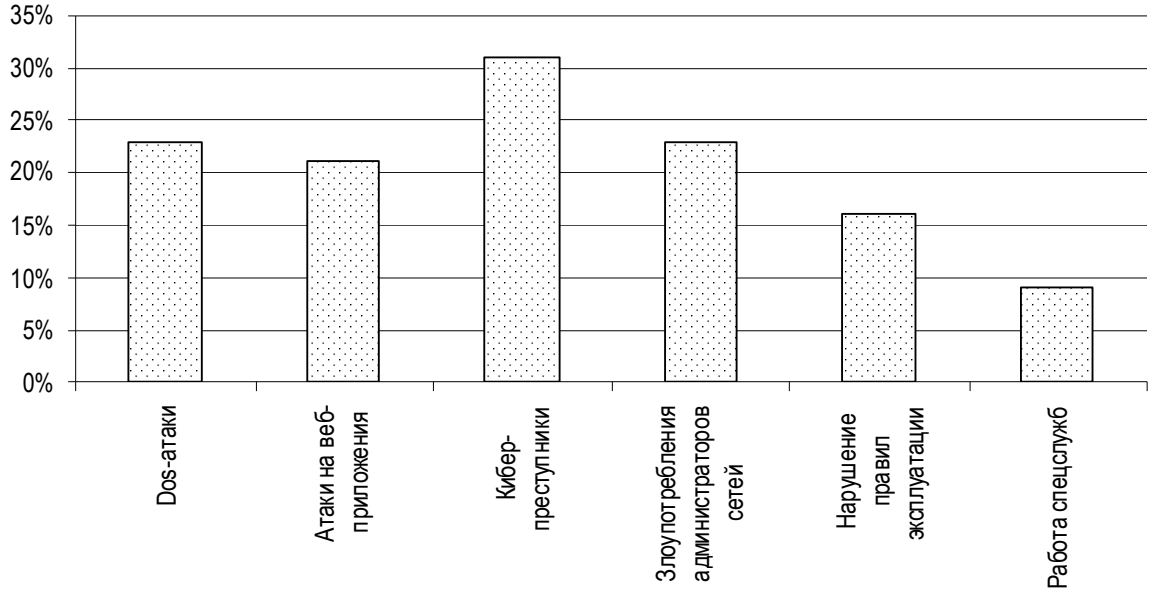

Рис. 2. **Инциденты информационной безопасности крупных российских компаний**

DOS-атаки (DOS - Denial-of-Service) представляют существенную угрозу для информационной безопасности предприятий непрерывного цикла работы (транспорт, связь, неотложная медицинская помощь и др.), поскольку в результате их влияния на длительное время теряется доступ к системе Интернет и, как следствие, возникает отказ в обслуживании в 90% случаев.

Как видно из рис. 2, большинство инцидентов связано либо с атаками из Интернета, либо со специализированным персоналом компаний. Данная ситуация вызвана тем, что сегодня информационная безопасность предприятия в большей степени зависит от качества технических систем и квалификации персонала. Успешное и эффективное их развитие возможно при соблюдении ряда условий, одно из которых подготовка персонала для работы в сфере информационного обеспечения инновационной деятельности в качестве разработчиков и пользователей[3].

Возникновение инцидентов приводит к существенным проблемам, таким как финансовые потери, ухудшение репутации компании, нарушение информационной инфраструктуры и пр. Обозначенных проблем можно избежать, если бы компании открыто признавали факты возникновения инцидентов или возможных угроз. Однако есть и другая сторона вопроса: признание компанией реальных и потенциальных проникновений в систему информационной безопасности предприятия указывает на существующие недостатки в ней и тем самым может привлечь внимание и других злоумышленников. Получается, что нераскрытие сведений об инцидентах и потенциальных угрозах конкретной компании и является одним и средств обеспечения информационной безопасности предприятия.

Существует статистика о внутренних угрозах безопасности информации в корпоративных информационных системах. Сотрудники Аналитического центра InfoWatch провели опрос специалистов и сотрудников ИТ-подразделений более 800 компаний о надежности защиты информации, уровне информационной безопасности, типах угроз, произошедших инцидентах и мероприятиях по решению возникающих проблем в системе информационной безопасности предприятия. Обобщая основные выводы исследования, можно заключить, что наибольшую угрозу представляют сотрудники с расширенными правами доступа к информации и инфраструктуре (администраторы сети, баз данных) и топ-менеджеры, поскольку именно в их сфере деятельности существует опасность злоупотребления доступом, утечки платежных данных и коммерческой тайны в финансовой сфере, а в промышленности - утечки ноу-хау. Так, например, в финансовой сфере значительная часть случаев нарушения информационной безопасности связана с утечкой платежных и персональных данных (более 85%)[4].

В промышленности, как правило, в защите нуждаются сведения, которые подпадают под категорию служебной или коммерческой тайны: научно-технологические сведения; конструкторская и технологическая документация; описание методов и способов производства изделий; уникальный программный продукт; финансовая документация; перспективные планы развития; направления модернизации производства; аналитические материалы об исследованиях контрагентов компании.

В дополнение можно отметить, что другими целями информационных атак на систему безопасности предприятия могут стать: офисные сети (угроза нарушения взаимодействия между исполнителями вследствие перехода от функционального к процессному управлению в организации и формирования единого информационного пространства[5]), продажи (утечка маркетинговых планов, системы ценообразования, базы данных клиентов), мобильные устройства (риски утечки информации при использовании сотрудниками компании собственных мобильных устройств для решения рабочих задач) и др.

Потенциальные угрозы и реальные инциденты в системе информационной безопасности предприятия рано или поздно становятся информационными преступлениями. Последние принято классифицировать следующим образом (В.А. Мещеряков): неправомерное завладение информацией или нарушение исключительного права ее использования; неправомерная модификация информации; разрушение информации; действие или бездействие по созданию информации с заданными свойствами; действия, направленные на создание препятствий пользования информацией законным пользователем[6].

В качестве примеров можно привести выявленные попытки распространения фальшивого документа на английском языке от имени ОАО «НК "Роснефть"», в котором некий гражданин Франции уполномочивается представлять интересы компании в качестве посредника при проведении переговоров. Документ исполнен с нарушением установленных в компании реквизитов, подписан несуществующим сотрудником и заверен фальшивой печатью. Еще одна угроза была зафиксирована в одном из дочерних обществ ОАО «НК "Роснефть"» - факт совершения неустановленным лицом действий, связанных с попыткой ввода в заблуждение руководства предприятия с целью получения денежных средств. Так, на телефон руководителя общества поступил звонок от лица, представившегося одним из вице-президентов компании и заявившего о необходимости выделения благотворительной финансовой помощи больному ребенку. При этом звонивший, ссылаясь на якобы имеющиеся устные указания Президента ОАО «НК "Роснефть"», предлагал перевести денежную сумму на банковскую карту[7].

Ситуация, связанная с недостаточностью защиты предприятия от потенциальных угроз, имеет множество объяснений. С одной стороны, руководители очень часто недооценивают возможные угрозы, с другой стороны, они убеждены, что инвестиции в IT-инфраструктуру и внедрение в практику защитных решений в любом случае превысят финансовый ущерб, который повлечет за собой инцидент информационной безопасности. Такой подход в высшей степени не оправдан. На сегодняшний день имеется множество исследований, которые доказали, что зачастую причиненный финансовый ущерб значительно превышает бюджеты многих предприятий, которые были ими выделены на организацию защиты и обеспечение информационной безопасности. Этот тезис подтверждается и результатами опросов, проводимых B2B International и Лабораторией "Касперского". Оценка затрагивала не только прямые финансовые потери, но и дополнительные расходы, которые предприятия были вынуждены понести после инцидента. Для повышения достоверности результата учитывались ответы и оценки только тех представителей предприятий, которые имели право указать конкретную сумму убытков и расходов. Полученные данные с учетом наличия информации о стоимости данной услуги на рынках различных стран позволили получить среднюю сумму финансового ущерба, который понесли предприятия в результате инцидента информационной безопасности.

Так, данные убытка включали в себя следующие элементы: расходы на внешние профессиональные сервисы (специалисты по IT-технологиям и информационной безопасности, адвокаты, PR-специалисты и т.д.); упущенные возможности (сорванные договоры, подпорченная репутация и т.д.); ущерб от простоя IT-инфраструктуры предприятия и остановки бизнес-процессов и т.д.

В итоге крупные предприятия от одного инцидента информационной безопасности теряют около 20 млн руб., средние - 780 тыс. руб.

Наибольший удельный вес финансовых потерь составляют дополнительные расходы, связанные с устранением последствий и предотвращением возможных инцидентов в перспективе. Дополнительные затраты складываются из расходов на привлечение и подбор персонала, приобретение специального ПО, аппаратных средств, обучающих тренингов и семинаров по информационной безопасности. Крупные предприятия на подобные цели, как правило, тратят порядка 2,2 млн руб.[8] Средние суммы затрат за 2014 г. представлены в таблице.

На вопросе дополнительных профессиональных услуг, которые потребовались в результате инцидента информационной безопасности практически 90% предприятий, следует остановиться более подробно. Рисунок 3 дает наглядное представление о перечне таких внешних специалистов и частоте обращения.

Треть пострадавших предприятий оценили понесенные дополнительные затраты на услуги таких узких специалистов как существенные

Ориентировочные суммы затрат предприятий на инцидент

Вид предприятий	Средний ущерб, тыс. руб.	Дополнительные расходы, тыс. руб.
Крупные предприятия	20 000	2200
Средние предприятия	780	324

(значительные). Практически в 70% случаев потребовалось привлечь консультанта по информационной безопасности. В 36% случаев прибегали к услугам юристов, адвокатов, которые чаще всего и назывались существенными (значительными). Тройку лидеров завершают специалисты по управлению рисками, услуги которых потребовались 30 % предприятий.

Не менее важным последствием инцидентов информационной безопасности становится и репутационный ущерб. На рис. 4 названы третьи стороны, которым предприятия раскрывали информацию об инциденте.

В общей сложности более половины всех предприятий, столкнувшихся с угрозой, в результате публично признавали и раскрывали информацию третьим сторонам. Больше трети предприятий были вынуждены уведомить клиентов, больше четверти - сообщали об инциденте партнерам и поставщикам. Круп-

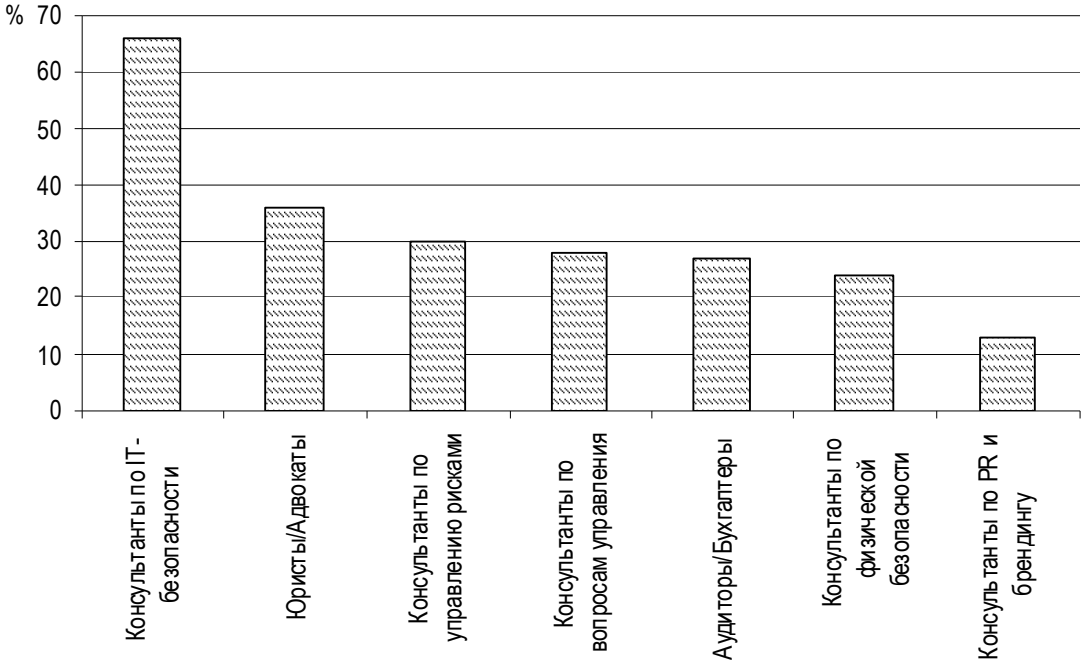

Рис. 3. **Оценка необходимости привлечения внешних специалистов в результате инцидентов информационной безопасности**

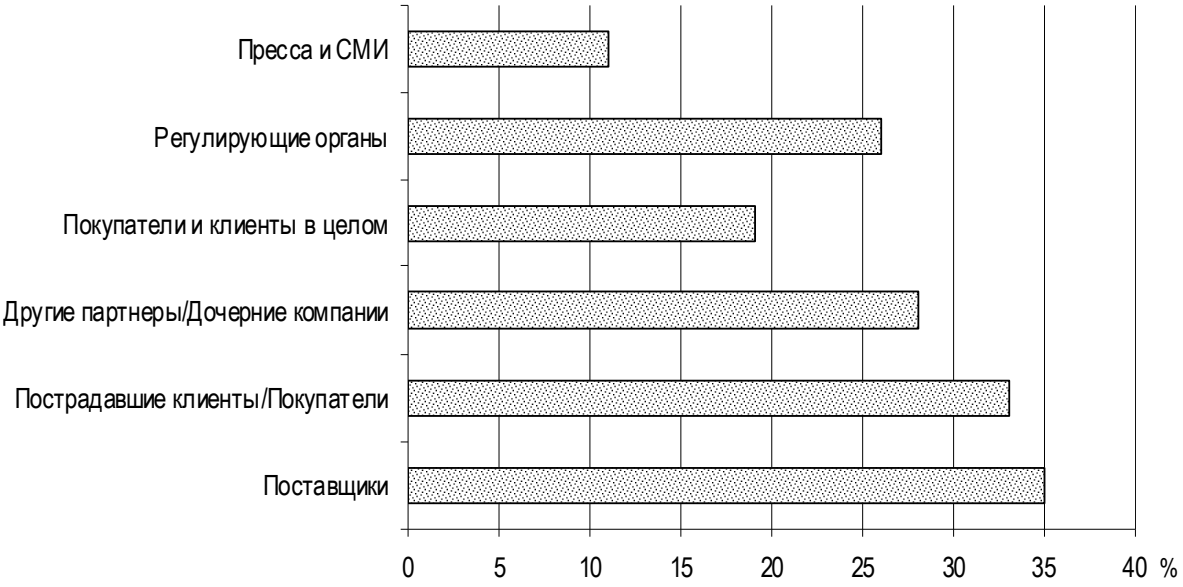

Рис. 4. **Доля компаний, раскрывших информацию об инциденте**

ные предприятия, как правило, обязаны информировать регулятора, СМИ и клиентов. А это, в свою очередь, наносит очень ощутимый удар по репутации предприятий. Для предотвращения инцидентов информационной безопасности в будущем предприятия предпринимают ряд мер, основные из которых представлены на рис. 5.

Так, более двух третей предприятий внедряют дополнительные программные и аппаратные решения для защиты IT-инфраструктуры. Более половины предприятий проводят обучение сотрудников, целью которого является научить последних безопасной работе с IT-технологиями и всей системой. Треть предприятий осуществляет подбор дополнительного персонала, в обязанности которого вменяется предотвращение возможных угроз, утечек и других инцидентов.

Ориентировочные суммы на подбор дополнительного персонала для крупных предприятий - 75 тыс. долл., обучение сотрудников - 34 тыс. долл., усовершенствование аппаратно-программных средств защиты - около 13 тыс. долл.[9]

Еще одним средством обеспечения дополнительной защиты предприятия является разработка и внедрение политик IT-безопасности. Оценка достаточности временных и финансовых затрат на политику информационной безопасности на предприятиях представлена на рис. 6.

Только 79% российских предприятий имеют разработанную и внедренную политику информационной безопасности, тогда как в целом в мире этот показатель достигает 86%. Треть респондентов указала, что на их предприятиях на разработку и внедрение политик выделяется достаточно времени и бюджетных средств. Велика доля предприятий, на которых данный вопрос даже не поднимался, она составляет 20%. Около половины всех предприятий деньги и время на разработку политик выделяют, однако недостаточно. На крупных предприятиях решение данного вопроса обстоит лучше всего. Почти половина респондентов удовлетворены выделяемыми ресурсами, как временными, так и финансовыми. Десятая часть опрошенных признались в полном отсутствии соответствующей статьи расходов. Причины, которые в основном приводят к невозможности построения эффективной системы обеспечения информационной безопаснос-

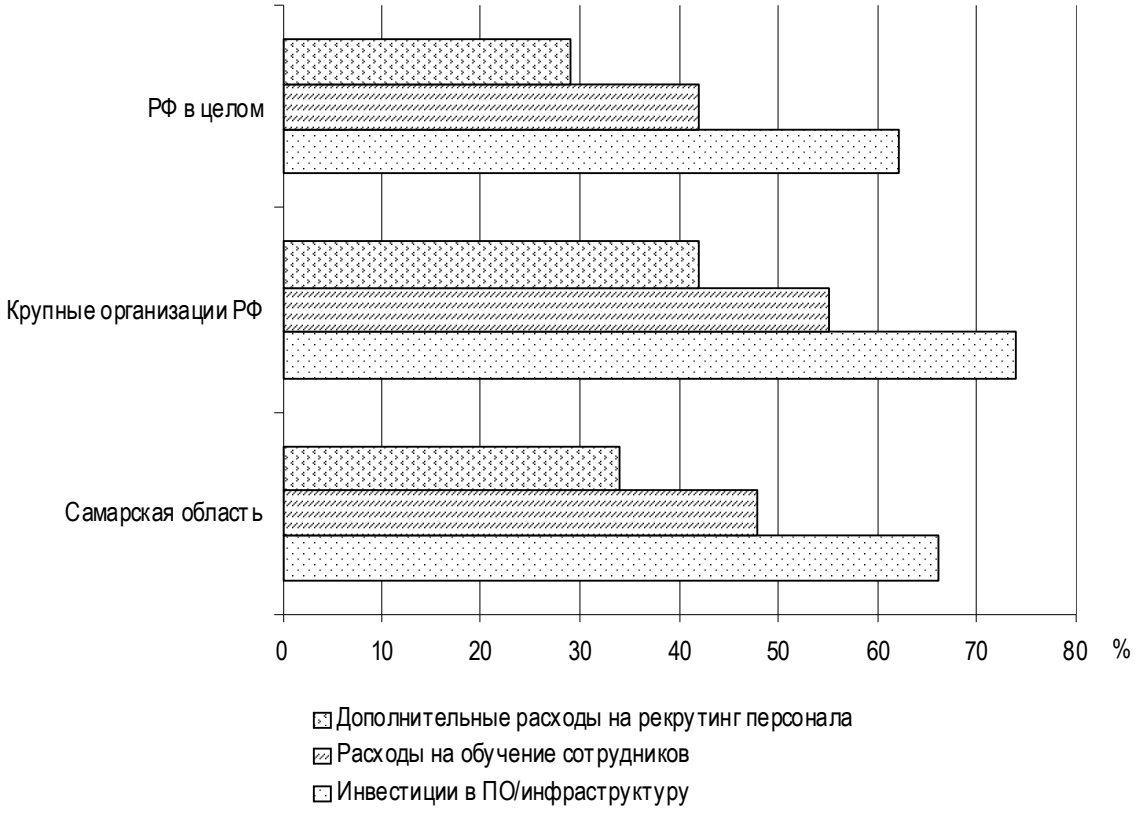

Рис. 5. **Меры по предотвращению инцидентов в будущем**

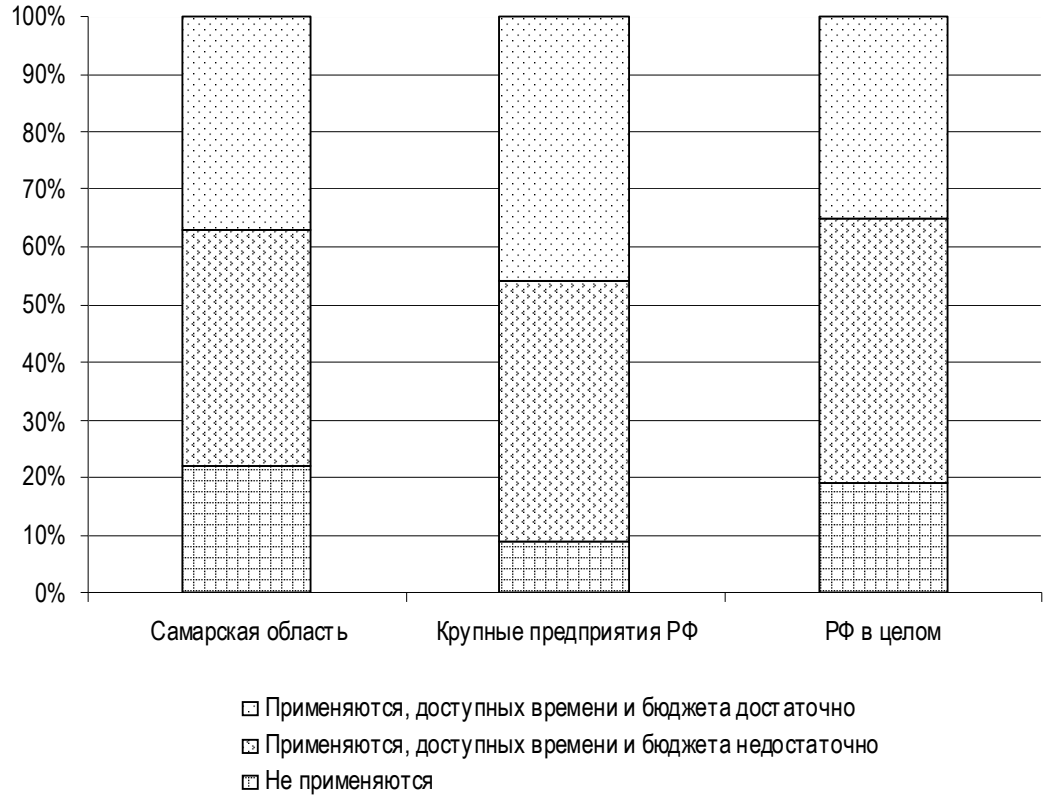

Рис. 6. **Оценка достаточности временных и финансовых затрат на политику информационной безопасности**

ти на предприятии, носят, как правило, исключительно внутриорганизационный характер. Основной проблемой продолжает оставаться проблема финансирования. Результаты оценки достаточности финансирования представлены на рис. 7.

Немногим менее чем на половине российских предприятий специалисты считают, что уровень финансирования IT-инфраструктуры достаточен для предотвращения инцидентов информационной безопасности. В Самарской области этот показатель достиг 40%. Среднемировой показатель составляет 59%. Однако хочется отметить и положительную динамику - снижение количества респондентов, которые оценивали уровень финансирования как недостаточный. Среднемировое значение улучшилось более чем на 10 п.п.

Абсолютное большинство также считают, что говорить об эффективной системе обеспечения информационной безопасности можно будет только в случае увеличения объемов инвестирования в эту сферу не меньше чем на 25% по сравнению с текущим моментом.

Следующие по важности причины, не позволяющие выстраивать эффективную защиту от угроз, представлены на рис. 8.

Около половины респондентов уверены, что у лиц, принимающих решение в сфере бюджетного распределения, отсутствует понимание данной проблемы как таковой. Проблему, рассмотренную ранее, касающуюся недостатка финансовых ресурсов, осознают и указывают 45% опрошенных. Третьей по важности проблемой называется отсутствие необходимого количества квалифицированного персонала, этот момент отметили 41% респондентов. 36 % специалистов утверждают, что высшее руководство не считает инциденты информационной безопасности существенным риском для хозяйственной и коммерческой деятельности. Однако присутствует и обратная проблема, выражающаяся в неспособности специалистов в сфере IT-технологий и информационной безопасности донести до руководства предприятий важность решения этой проблемы.

В сфере информационной безопасности количество преступлений изменяется с учетом типа угрозы. В последнее время все меньше преступлений связано с установкой и использованием нерегламентированного оборудования вследствие ужесточения контроля со стороны администрации и все больше угроз,

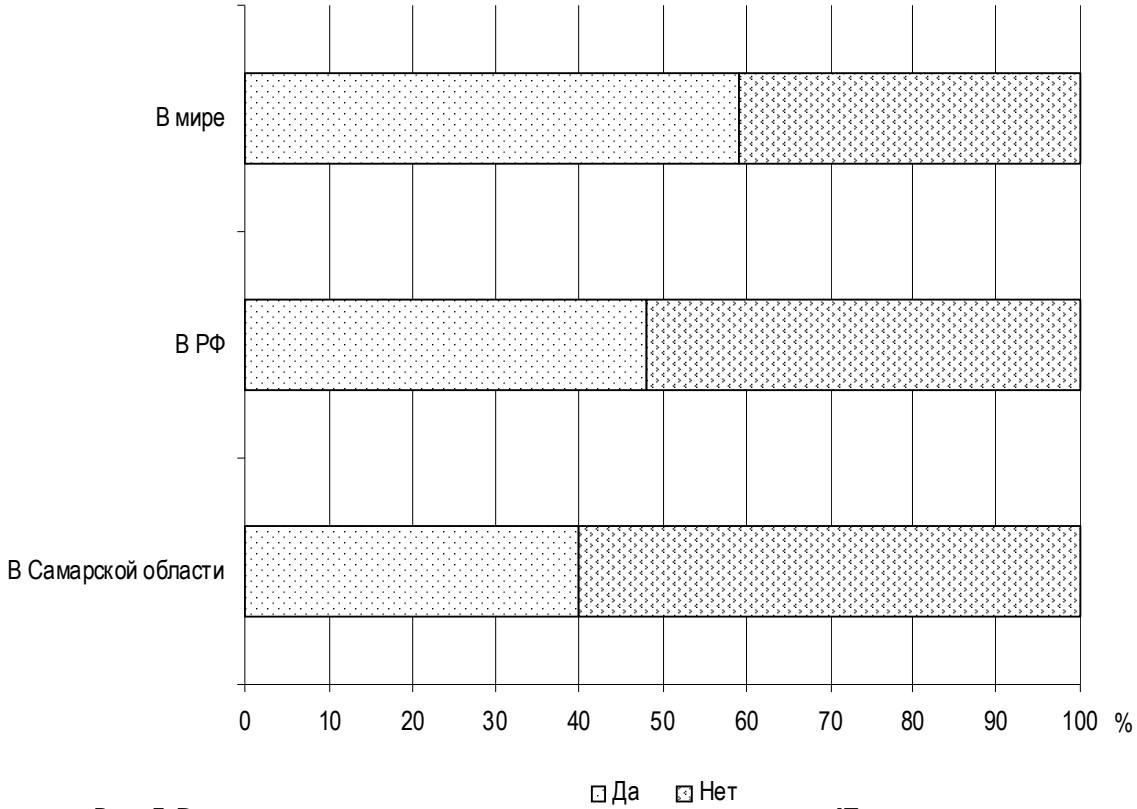

Рис. 7. **Результаты оценки достаточности финансирования IT-инфраструктуры**

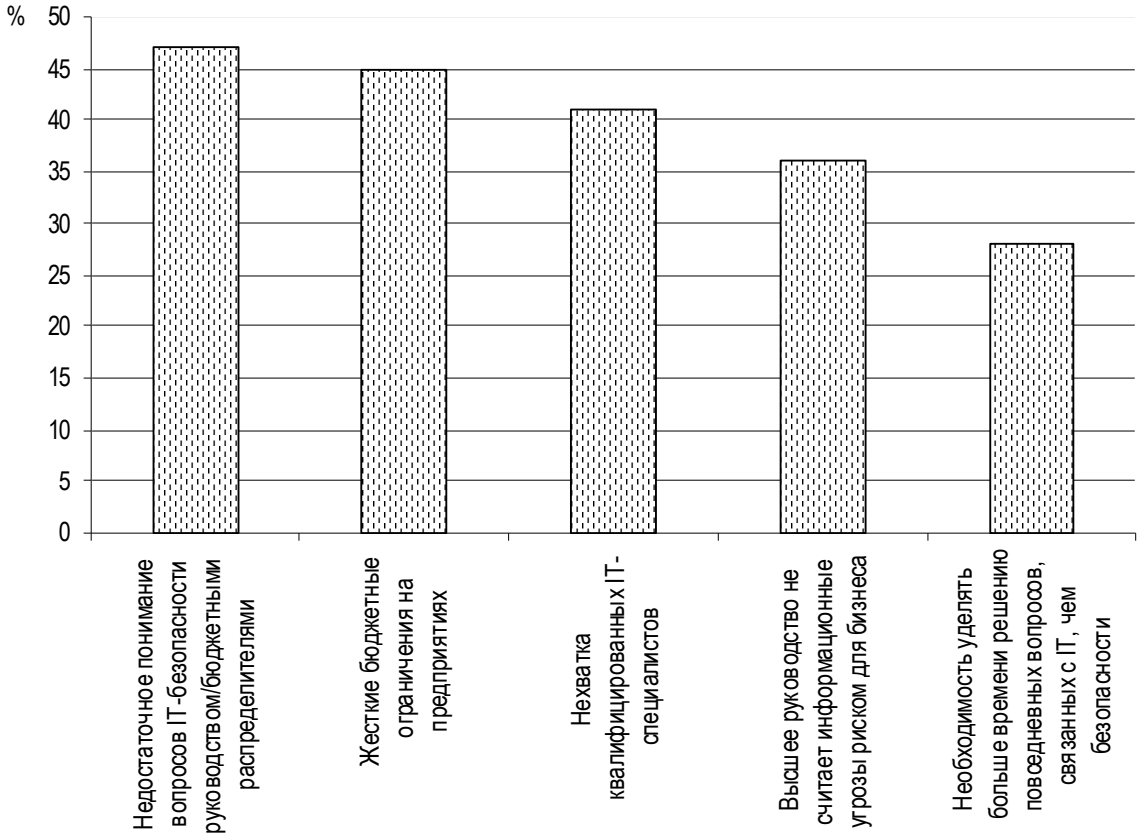

Рис. 8. **Причины, затрудняющие обеспечение эффективности функционирования системы обеспечения информационной безопасности**

связанных с интернет-атаками. Компанией "Инфосистемы Джет" с помощью первого в России коммерческого центра мониторинга и реагирования на инциденты информационной безопасности (JSOC) за первые три квартала 2014 г. зафиксировано 54 276 событий с подозрением на инцидент, а за первый квартал 2015 г. - 34 743 события с подозрением на инцидент. Причем, как отмечалось ранее, 41,2% всех внешних атак приходится на уровень веб-приложений, а наиболее часто совершаемой внутренней угрозой отмечена утечка информации (30,3%). Сводной статистикой по инцидентам за 2014 г. было зафиксировано 83 554 события с подозрением на инцидент, 29 278 из них приходится на четвертый квартал. При этом 64 % указанных событий было зафиксировано основными сервисами инфраструктуры и базовой безопасности (WAF, VPN, AD, антивирусы, прокси-серверы, IPS и пр.). Оставшиеся 36 % выявлены с помощью высокоинтеллектуальных средств защиты или анализа и имеют высокую степень критичности для информационной и экономической безопасности. Экспертами компаний отмечаются устойчивый рост процента атак, направленных на веб-сервисы, увеличение числа инцидентов в сфере утечек конфиденциальной информации[10]

Большинство инцидентов - целенаправленные атаки, совершаемые с целью получения управления и контроля над атакуемой системой и направленные либо на конкретный вид деятельности компании, либо на компанию в целом. Злоумышленникам результатом подобных атак видится нанесение ущерба компании или получение материальной выгоды. Целенаправленными являются в первую очередь кибератаки. Их выявление является трудоемким процессом и поэтому требует глубокой степени проработки. Трудности выявления кибератак обусловлены неявностью конечной цели, что затрудняет осуществление зависимости между промежуточными целями атак и итоговой, на правый взгляд не связанными друг с другом. Однако, какова бы ни была цель злоумышленника, факт угроз и атак на информационную систему предприятия должен предупреждаться и предотвращаться с помощью эффективной системы информационной безопасности.

Практика в области управления информационной безопасностью подтверждает, что основными задачами обеспечения информационной безопасности предприятия являются: защита от потерь, краж, искажения и уничтожения информации; предотвращение угроз информационной безопасности; создание стабильной и эффективной деятельности всех подразделений.

Таким образом, необходимо выделять и структурировать информацию, прогнозировать и своевременно выявлять угрозы информационной безопасности, а также создавать механизмы и условия эффективного реагирования системы информационной безопасности предприятия на информационные угрозы.

---

[1] Статистика уязвимостей корпоративных информационных систем 2014. URL: http://www.ptsecurity.ru/download/PT_Corporate_vulnerability_2015_rus.pdf. С. 6-7.

[2] Инциденты в информационной безопасности крупных российских компаний 2013. URL: http://www.ptsecurity.ru/download/PT_Security_Incidents_2014_rus.pdf. С. 4-5.

[3] *Бердников В.А., Булов В.Г.* Опыт постановки подходов к управлению информационным обеспечением инновационной деятельности на примере отечественных предприятий // Вестник Самарского государственного экономического университета. 2015. № 4 (126). С. 54.

[4] Безопасность информации в корпоративных информационных системах. Внутренние угрозы 2013. URL: http://www.infowatch.ru/sites default/files/report/analytics/russInfo Watch_Report_2013_ugroz.pdf. С. 10-15.

[5] *Корнеева Т.А., Степанов А.С.* Проблемные аспекты внедрения процессного подхода в управление промышленными предприятиями // Вестник Самарского государственного экономического университета. 2014. № 3 (113). С. 34.

[6] *Мещеряков В.А.* Криминалистическая классификация преступлений в сфере компьютерной информации // Конфидент. 1999. № 4. С 17.

[7] ОАО «НК "Роснефть"». Инвесторам и акционерам. Осторожно мошенники. URL: http://www.rosneft.ru/Investors/beware/fakedoc.

[8] Информационная безопасность бизнеса. Результаты исследования. Лаборатория "Касперского" - 2014. URL: http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf. С. 14.

[9] Информационная безопасность бизнеса. Результаты исследования. Лаборатория "Касперского" - 2013. URL: http://media.kaspersky.com/pdf/IT_risk_report_Russia_2013.pdf. С. 12.

[10] Компания Solar Security. Аналитика. Отчеты. URL: http://solarsecurity.ru/analytics/reports.

Поступила в редакцию 26.06.2015 г.