V.E. Dorokhov

Information Security For Business: The Necessity Of Reputational Risk Management

Keywords: information security, information leakage, risk management, reputational risk

The article presents the analysis of actual information security problems in commercial segment. The main directions in regulations of the Russian Federation connected with information security assurance are defined. The results indicate the insufficiency of legal regulation in prevention of reputational losses due to information security incidents.

В.Э. Дорохов

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ ДЛЯ БИЗНЕСА: НЕОБХОДИМОСТЬ УПРАВЛЕНИЯ РЕПУТАЦИОННЫМИ РИСКАМИ

Подход к обеспечению информационной безопасности (далее – ИБ) в Российской Федерации, практикуемый как государственными, так и коммерческими организациями, можно сравнить с конструктором, поскольку известно, что в настоящее время не существует целостного подхода к обеспечению ИБ.

Для коммерческого сектора обеспечение ИБ можно сформулировать в виде трех основных направлений:

- развитие технологий по нейтрализации угроз ИБ при помощи технических средств защиты информации;
- усовершенствование контроля над процессами использования информации, т.е. предотвращение утечек информации путем разработки определенного перечня необходимых организационных мероприятий;
- контроль над информационным полем вокруг организации: направление наименее развитое, тесно перекликающееся с другими аспектами управления в компаниях, такими как взаимоотношения с сотрудниками (HR), взаимоотношения с государственными органами (GR), взаимоотношения с общественностью (PR), взаимоотношения с инвесторами (IR).

Рассмотрим каждое из представленных выше направлений.

Развитие технологий защиты информации непосредственно связано с развитием технологий обработки информации. Чем больше способов информационного взаимодействия с применением средств вычислительной техники и каналов передачи информации, тем больше уязвимостей, которыми может воспользоваться злоумышленник. Для принятия оптимального решения по составу программно-аппаратных средств защиты информации необходимо проанализировать следующие аспекты работы с информацией в организации.

- Использование средств вычислительной техники для работы с критически важной информацией; наличие технических средств с обязательной функцией обмена данными через сеть Интернет; технологии работы с информацией (виртуализация, системы управления базами данных (СУБД), программные средства и т.д.).
- Использование специализированного программного обеспечения при работе с критически важной информацией; учет особых требований на совместимость данного программного обеспечения; анализ порядка его разработки.
- Территориальное распределение важных сегментов организации, объединенных по принципу работы с одним и тем же составом критически важной информации.

- Модернизация сетевой инфраструктуры, в частности, возможность образования новых сегментов локальной вычислительной сети предприятия.

Для предотвращения инцидентов ИБ, реализованных путем разглашения сотрудниками информации ограниченного доступа, актуальным средством является повышение осведомленности сотрудников организации в вопросах обеспечения ИБ. Положения по работе со сведениями, составляющими важность для организации, должны быть задокументированы и однозначно понятны для всех сотрудников. Построение организационных мероприятий зиждется на следующих основных принципах:

- Определение перечня сведений, составляющих критически важную информацию для организации. Здесь необходимо учитывать возможное дополнение сведений, связанное с открытием новых направлений работы организации либо развитием старых, а также обусловленное этим увеличение количества работников компании.
- Определение направлений деятельности, связанных с обработкой критически важной информации. Также необходимо понимание, увеличится ли объем критичной информации, будут ли открываться новые направления деятельности с привлечением потенциальных стратегических компаньонов и др.
- Степень лояльности сотрудников, задействованных в обработке информации, и их количество. Важно учитывать, планируется ли сокращение штата сотрудников по направлениям, в которых осуществляется работа с критически важной информацией.
- Анализ условий работы сотрудников в организации на предмет соответствия конкурентным условиям на рынке труда. Также необходимо проанализировать, осуществляются ли мероприятия для работников по неразглашению ими условий труда.
- Анализ существующих организационных мероприятий на предмет соблюдения требований регуляторов в области ИБ. В том числе анализ актуальных законодательных актов в части обеспечения ИБ. Также необходимо учитывать, планируются ли изменения нормативных документов регуляторов, и в какие временные сроки.
- Анализ осведомленности персонала по вопросам ИБ посредством анкетирования либо тестирования.

Информационное поле вокруг организации, по сути, формирует ее имидж. Имидж, в свою очередь, оказывает прямое влияние на прибыль компании. В данном направлении необходимо проводить мероприятия по минимизации инцидентов ИБ влекущих за собой репутационные потери для организации. Согласно проводимым ранее исследованиям [1], понятие репутационного риска в контексте ИБ формулируется следующим образом:

Репутационный риск (информационная безопасность) – относительная величина, определяющая убытки организации, возникающие вследствие отсутствия подходящих организационных и технических мероприятий по нейтрализации угроз ИБ, приводящих к потере репутации организации для основных видов взаимоотношений организации.

С целью осуществления эффективного контроля над информационным полем вокруг организации, необходимыми для анализа являются:

- частота появления в СМИ сведений о направлениях деятельности организации, в рамках которых предполагается обработка критически важной инфор-

мации. Тенденция повышения интереса читателей к рубрикам, которые освещают подобные проблемы;

- наличие у сотрудников личных блогов в сети Интернет при отсутствии должного уровня осведомленности с Политикой ИБ (если данный документ утвержден в организации);
- наличие и тенденция обсуждения направлений в тематических формах (количество пользователей из числа работников, активность – количество сообщений). Данную информацию можно собрать анкетированием на этапе анализа проблемы;
- развитие смежных направлений в организации, имеющих повышенную конкуренцию, в том числе среди компаний, использующих «черный пиар» в качестве методов конкуренции.

Рассмотрим нормативные документы Российской Федерации, регламентирующие порядок обеспечения ИБ. Под термином «информационная безопасность» довольно часто понимается процесс защиты информации с использованием программных, аппаратных и программно-аппаратных решений с целью предотвращения утечки информации по техническим каналам. В этой области существует ряд нормативных документов Российской Федерации, регулирующих вопросы безопасности информации. Среди регуляторов стоит отметить ФСТЭК России, ФСБ России, Центральный банк Российской Федерации, Роскомнадзор.

Требования по ИБ изложены в следующих основных документах:

- Конституция Российской Федерации.
- Доктрина информационной безопасности Российской Федерации.
- Указ Президента РФ от 06.03.1997 №188 «Об утверждении Перечня сведений конфиденциального характера».
- Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 28.12.2013) «Об информации, информационных технологиях и о защите информации».
- Федеральный Закон от 27.07.2006 №152-ФЗ «О персональных данных», включая
  - Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
  - Постановление Правительства РФ от 15.09.2008 №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
  - Постановление Правительства РФ от 06.07.2008 № 512 (ред. От 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных вне информационных систем персональных данных».
  - Постановление Правительства РФ от 21.03.2012 №211 (ред. 20.07.2013) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
- Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи».
- Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 11.07.2011) «О коммерческой тайне».

- Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 23.07.2013) «О национальной платежной системе».
- Постановление Правительства РФ от 13.06.2012 №584 «Об утверждении Положения о защите информации в платежной системе».
- Нормативные документы государственных регуляторов (ФСТЭК России, ФСБ России, Роскомнадзор, Центральный Банк Российской Федерации).

Стоит отметить, что в основных законах и подзаконных актах, касающихся ИБ, не предъявляется в явном виде требование по физической защите информационных активов организации. Между тем риск физического воздействия при ненадлежащей охране весьма велик, и ущерб от физического воздействия, к примеру, на технические средства обработки и хранения информации, может оказаться гораздо больше, чем от хакерской атаки на них же. Также в основных законодательных актах Российской Федерации не нашел отражение вид утечки информации непосредственно через внутренних сотрудников организации, без использования технических каналов.

Помимо основных законов и подзаконных актов Российской Федерации, необходимо учитывать требования отраслевых нормативных актов в части ИБ. Стоит отметить, что в большинстве случаев обеспечение безопасности информации начинается с анализа основного закона отрасли, и следом, на основании проведенного анализа, строится работа по защите информации в организации. Для каждой отрасли необходимо учитывать специфические требования по обработке информации, определению конфиденциальности информации и др.

Исходя из анализа существующих нормативных актов, регламентирующих обеспечение ИБ, можно сделать вывод о необходимости проведения мероприятий по защите информации ограниченного доступа от утечки по техническим каналам. К таким мероприятиям относятся:

- Установка и настройка технических средств защиты информации на автоматизированные рабочие места сотрудников организации, на которых производится обработка информации ограниченного доступа.
- Использование защищенной среды передачи данных для исключения возможности утечки информации ограниченного доступа при обмене информацией во внутренней сети организации, а также при использовании внешних сетей.

Одновременно стоит отметить, что помимо утечки информации по техническим каналам для коммерческого сектора не менее важно учитывать вероятность возникновения событий иного характера, от которых трудно защититься только техническими средствами защиты, таких как:

- публикация в читаемом интернет-блоге о внутренних проблемах организации;
- размещение на официальном сайте государственного регулятора информации о нарушениях организацией требований законодательства;
- заявление в СМИ работника крупного банка об убытках его организации;
- разглашение работником важной информации внутри коллектива, например, сведений о заработной плате;
- заказная публикация от компаний-конкурентов в СМИ ложных сведений, дискредитирующих действия компании;
- появление в открытых источниках сведений об стратегических партнерах компании, желающих остаться инкогнито;
- и другие;

Все подобные ситуации объединяет фактор влияния общественного мнения. Злоумышленники применяют ряд способов воздействия на репутацию организации, ос-

новными из которых являются несанкционированные операции с информационными активами организации, в том числе нарушение конфиденциальности, целостности, доступности как основных свойств, и аутентичности, достоверности и др. как дополнительных свойств защищаемой информации. Как правило, исходами вследствие подобных инцидентов являются кадровые и финансовые потери. Другими словами, организация терпит крупные убытки, порой несопоставимые с возможностью продолжения дальнейшей деятельности. В связи с этим представители бизнес-сектора должны уделять внимание предотвращению утечки критически важной информации, так как негативные последствия этих инцидентов очевидны: прямые финансовые убытки, удар по репутации, потеря клиентов.

Наряду с анализом нормативно-правовой базы в области ИБ стоит отметить, что понятие «репутационный риск» или «риск потери деловой репутации» (анализируя документы, можно встретить оба варианта терминологии, несущие одинаковую смысловую нагрузку) в явном виде сформулировано лишь для банковской отрасли. В соответствии с Приложением к Письму Банка России «Об организации управления правовым риском и риском потери деловой репутации в кредитных организациях и банковских группах» от 30 июня 2005 г. № 92 – Т, репутационный риск означает риск возникновения у кредитной организации убытков вследствие влияния ряда факторов, приведенных в данном документе [2]. В формулировках данных факторов можно встретить ряд свойств, описывающих предпосылки к реализации инцидентов ИБ.

Исходя из вышеизложенного, можно сделать вывод о том, что для компаний – представителей коммерческого сектора – необходимо как выполнение требований нормативных актов Российской Федерации в области ИБ, так и проведение ряда дополнительных мероприятий. Нормативными документами Российской Федерации в области ИБ недостаточно регламентированы нетехнические меры по защите информации. В контексте проблематики, представленной в данной статье, стоит отметить отсутствие мероприятий по минимизации репутационных рисков, возникающих вследствие инцидентов ИБ. Мероприятия по обеспечению ИБ являются важнейшей составляющей управления бизнесом с целью предотвращения разного рода убытков, возникающих вследствие ухудшения репутации организации. Также стоит отметить, что потребности бизнеса в части обеспечения ИБ с точки зрения требований регуляторов учитываются не полностью, в связи с чем актуально проведение дополнительных исследований в данной области.

СПИСОК ЛИТЕРАТУРЫ:

1. В. Э. Дорохов. О рисках потери репутации организации вследствие инцидентов информационной безопасности // Безопасность Информационных Технологий, №2, 2014. – С. 80-82.
2. Письмо Банка России от 30.06.2005 № 92-Т «Об организации управления правовым риском и риском поери деловой репутации в кредитной организации и банковских группах». URL: http://base.garant.ru/585600. Дата обращения 25.06.2015.

REFERENCES:

1. Dorokhov V.E. O riskah poteri reputacii organizacii vsledstvie incidentov informacionnoj bezopasnosti // Bezopasnost' informacionnyh tehnologij, №2, 2014. – pp. 80-82.
2. Letter Bank of Russia 30.06.2005 № 92-T «Ob organizacii upravlenija pravovym riskom i riskom poteri delovoj reputacii v kreditnyh organizacijah i bankovskih gruppah». URL: http://base.garant.ru/585600