В. Э. Дорохов

О РИСКАХ ПОТЕРИ РЕПУТАЦИИ ОРГАНИЗАЦИИ ВСЛЕДСТВИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационные технологии претерпевают стремительное развитие на протяжении последних десятилетий и предоставляют все больше возможностей, связанных с их использованием. Организации, как государственные, так и коммерческие, а также работники этих организаций имеют неограниченный доступ в сеть Интернет — если не из сети предприятия, то из дома или с личного портативного устройства. Соответственно, в сети Интернет обрабатывается колоссальное количество информации, которая попадает туда нередко вследствие нарушений информационной безопасности. В настоящее время организации уделяют недостаточно внимания учету рисков потери репутации вследствие инцидентов информационной безопасности.

Под термином «информационная безопасность» довольно часто понимается защита информации с использованием программных, аппаратных и программно-аппаратных решений. Но не менее важно учитывать вероятность возникновения событий иного характера, от которых трудно предотвратить, используя только технические средства защиты, такими событиями могут быть:

- публикация в интернет-блоге о внутренних проблемах организации;
- размещение на официальном сайте государственного органа информации о нарушениях организацией требований законодательства;
- заявление в СМИ работника крупного банка об убытках его организации.

Все подобные ситуации объединяет фактор влияния общественного мнения. Злоумышленники применяют ряд способов воздействия на репутацию организации, основным из которых являются несанкционированные операции с информационными активами организации, в том числе нарушение конфиденциальности, целостности и доступности защищаемой информации.

Зачастую в организации малого и среднего бизнеса отсутствуют регламентированные мероприятия по управлению основными видами взаимоотношений в части обеспечения информационной безопасности. Под основными видами взаимоотношений понимаются взаимоотношения с работниками (HR), с общественностью (PR), с государственными органами (GR), с инвесторами (IR). Виды взаимоотношений PR и IR характерны не для каждой организации, но HR и GR присутствуют всегда.

Взаимоотношения с работниками (HR) — это основной вид взаимоотношений, который присутствует в любой организации. Опасность наличия внутреннего нарушителя (инсайдера) крайне велика, поскольку полноценной защиты от его деятельности в настоящее время не

существует. Понимание работниками необходимости обеспечения информационной безопасности в большинстве случаев отсутствует, что приводит к неумышленным действиям сотрудника, допускающим утечку важной для организации информации. Невозможно запретить работнику действовать «не по инструкции», распространять противоречивые, ложные сведения о своей деятельности или деятельности организации, а также соответствующие действительности сведения о проблемах в организации среди знакомых, в сети Интернет и т. д. Потеря репутации организации из-за взаимоотношений с работниками может возникать в результате следующих инцидентов информационной безопасности:

- Разглашение работником важной информации организации внутри коллектива, например размера своей заработной платы (если это является коммерческой тайной). К этому может привести недостаточное понимание сотрудниками важности соблюдения правил информационной безопасности, пренебрежение политикой информационной безопасности организации. Рассматриваемый инцидент может спровоцировать ухудшение внутренних взаимоотношений в коллективе, разлад, уход ценных сотрудников (что влечет за собой издержки по нахождению новых квалифицированных кадров).
- Заявление работника в уполномоченные органы о нарушении компанией трудового или иного законодательства, что провоцирует проверки с их стороны. В результате организация теряет свой статус добросовестного работодателя, что отталкивает потенциальных кандидатов от вступления в трудовые правоотношения с компанией.
- Распространение работником информации о недостаточно хороших условиях труда в организации в своей профессиональной среде (как правило, среди бывших однокурсников и деловых партнеров). Инцидент приводит к потере репутации организации, которая считалась работодателем с приемлемыми условиями работы.

Взаимоотношения с государственными органами власти (GR) — это выстраивание и налаживание взаимоотношений с государственными органами власти, в том числе с правительством, региональными и местными органами власти.

Для поддержания хорошей репутации организации в государственном секторе, как правило, необходимо выстраивать свой бизнес в соответствии с множеством требований федеральных законов. В контексте информационной безопасности существует как перечень законодательных актов, положения которых необходимо учитывать любым организациям, вне зависимости от рода их деятельности, так и отдельные статьи отраслевых законов, регламентирующих различные аспекты информационной безопасности. Подробно нормативные правовые акты Российской Федерации в области обеспечения информационной безопасности (в том числе и требования отраслевого законодательства), а также мероприятия по защите информации ограниченного доступа были рассмотрены в работах [1] и [2].

Невыполнение требований по информационной безопасности, как правило, влечет санкции со стороны государственных структур, которые приводят к потере репутации организации, например:

- Приостановка, а также запрет на обработку некоторых видов информации (невыполнение требований № 152-ФЗ «О персональных данных» и его подзаконных актов, статьи 13.12, 19.20 КоАП РФ). Данная санкция в отношении организации свидетельствует о том, что обработка информации в организации ведется недолжным образом и допускает ее утечку, а также незаконное распространение. В итоге, организация подвергается явному риску потери репутации.
- Административная ответственность (статьи 5.27, 13.11, 13.12, 19.5, 19.20, 20.25 КоАП РФ). Эта санкция применяется, в частности, при осуществлении несанкционированного доступа к важной информации, в том числе законодательно отнесенной к какому-либо виду тайн. Получив данные о подобной санкции в отношении организации, партнеры и клиенты наверняка откажутся от дальнейшего сотрудничества ввиду снижения доверия к организации, восстановить которое будет крайне затруднительно.

- Уголовная ответственность (статьи 137 (нарушение неприкосновенности частной жизни), 140 (отказ в предоставлении гражданину информации о его персональных данных) УК РФ). Наличие уголовного дела в отношении высшего руководства организации предполагает максимальные финансовые убытки вследствие потери репутации организации, а для малого и среднего бизнеса наиболее вероятный исход — прекращение деятельности.

В каждом рассмотренном случае возникают разной степени негативные последствия, связанные с влиянием на репутацию организации. Вследствие этого предлагается ввести следующую формулировку для понятия «репутационный риск», определяемого в соответствии с проблемами обеспечения информационной безопасности:

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

В результате проведенного анализа можно сделать вывод о важности правильно выстроенных взаимоотношений с сотрудниками, поскольку ряд их действий, возможных вследствие недостаточности организационных мероприятий в области обеспечения информационной безопасности, влечет за собой потерю репутации организации и, как следствие, различного рода убытки. Также важны корректно выстроенные взаимоотношения с государственными органами, иными словами, надлежащее исполнение требований в рамках обеспечения информационной безопасности, так как, если организация приобретает статус недобросовестной по отношению к требованиям власти, это вызывает недоверие и потерю клиентов, деловых партнеров, акционеров и, следовательно, также приводит к убыткам. Таким образом, для снижения репутационных рисков, очевидно, возникает необходимость усовершенствования процессов управления указанными видами взаимоотношений, в частности, путем реализации мероприятий по предотвращению разглашения важной информации работниками организации (в том числе распространения ложной информации о деятельности организации), а также мероприятий, направленных на выполнение требований по защите информации, предъявляемых государственными органами власти.

СПИСОК ЛИТЕРАТУРЫ:

1. *Дорохов В. Э., Моисеев А. В.* Обзор нормативно-правовых актов Российской Федерации в области информационной безопасности // Безопасность информационных технологий. 2013. № 3. С. 106–110.
2. *Дорохов В. Э.* Мероприятия по защите информации ограниченного доступа на основе нормативно-правовых актов Российской Федерации с учетом их отраслевой направленности в информационной безопасности // Сборник тезисов докладов конференции «Обеспечение комплексной безопасности предприятий: проблемы и решения», 4–6 июня 2013 г. С. 82–83.

REFERENCES:

1. *V. E. Dorokhov, A. V. Moiseev.* Survey of Russian legislation in information security. *Security of Information Technologies*. 3 (2013). P. 106–110.
2. *V. E. Dorokhov.* Measures of protection classified information due to legal acts of the Russian Federation in accordance with its sectorial focus in information security, *Complex security of organizations: problems and solutions, 4–6 June 2013, Conference Proceedings*. P. 82–83.