УДК 658.5.011

Дорохов В.

КЛАСИФІКАЦІЯ ПОРУШНИКІВ ЯК ЕТАП МЕНЕДЖМЕНТУ РЕПУТАЦІЙНИХ РИЗИКІВ УНАСЛІДОК ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Визначено поняття репутаційного ризику як складової інформаційної безпеки. Проаналізовано види взаємин, в рамках яких можливе виникнення інцидентів інформаційної безпеки: HR, PR, GR, IR. Звернуто увагу на зв'язок між репутаційними ризиками і прибутком компанії.

Ключові слова: *інформаційна безпека, репутаційні ризики, інцидент інформаційної безпеки.*

Информационная безопасность играет важную роль в деятельности организации. Утечка информации может спровоцировать множество негативных последствий, в конечном итоге влекущих за собой крупные финансовые потери.

Вместе с этим, немаловажным является контроль информационного поля вокруг организации, которое формирует ее имидж. Имидж, в свою очередь, оказывает прямое влияние на прибыль компании. Влияние на репутацию организации таких событий, как: разглашение критичной информации о процессах деятельности, опубликование в открытых источниках ложной информации и т. д. – формирует репутационные риски. Согласно проводимым ранее исследованиям [1]:

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.

Важность разработки методики для эффективного менеджмента репутационных рисков обуславливается критичностью репутационной составляющей для бизнеса, а также отсутствием регулирующего воздействия со стороны законодательства. В работе «Анализ инцидентов информационной безопасности, приводящих к потере репутации, как функция управления хозяйствующим субъектом» [2] был выявлен ряд инцидентов информационной безопасности в следующих основных видах взаимоотношений:

- ✓ взаимоотношения с работниками (HR);
- ✓ взаимоотношения с общественностью (PR);
- ✓ взаимоотношения с государственными органами власти (GR);
- ✓ взаимоотношения с инвесторами (IR).

В рамках данной работы проводится классификация нарушителей информационной безопасности, актуальной для бизнес-сектора. В качестве инцидентов, спровоцированных или совершенных нарушителем, предполагаются действия, приводящие к репутационным потерям для организации. Проводимая классификация базируется на основных видах взаимоотношений в компании в соответствии с инцидентами информационной безопасности.

Рассмотрим потенциальных нарушителей для каждого из видов взаимоотношений:

Взаимоотношения с работниками (HR).

Инцидент информационной безопасности в сфере взаимоотношений с сотрудниками в большинстве случаев происходит из-за низкого уровня осведомленности сотрудников в области информационной безопасности и принятой в организации политикой ИБ (если таковая существует). Составляя модель нарушителя в области HR, изначально предполагается то, что сотруднику, в соответствии с его рабочими обязанностями, становятся доступными сведения, критичные для организации. Нарушителей информационной безопасности, способных повлиять на репутацию хозяйствующего субъекта, с низким уровнем осведомленности целесообразно разделить на следующие классы:

HR1: сотрудник со слабыми профессиональными навыками и высокой лояльностью.

Наиболее «безопасный» класс нарушителя в области взаимоотношений с работниками. В соответствие с текущим уровнем профессионализма, к данному классу нарушителей целесообразно отнести так называемый «кадровый резерв» – будущих сотрудников, находящихся на этапе развития, не позволяющем принимать непосредственное участие в важных для организации аспектах ведения бизнеса. Опасность нарушитель данного класса может представлять лишь в связи с ошибочной трактовкой принципов построения процессов деятельности в организации вместе с низким уровнем осведомленности в принципах информационной безопасности (в т. ч., принятых в организации).

HR2: сотрудник с низким показателем лояльности и низким уровнем профессиональных навыков.

Данный класс сотрудников работает в компании, как правило, в течение испытательного срока, после чего его трудовые отношения с организацией прекращаются. Опасность нарушителя низкая, поскольку сравнительно с другими классами нарушителей HR данный класс знакомится с меньшим объемом критичной информации. Мотивом данного нарушителя может служить «несправедливое», по его мнению, увольнение из компании. Поскольку на момент публикации критичной информации либо ложных сведений нарушитель не является сотрудником компании, его действия нанесут незначительный ущерб организации. Отличительной особенностью нарушителей, относящихся к данному классу, является реализация инцидента информационной безопасностью путем распространения ложной информации о процессах деятельности организации.

HR3: высококвалифицированный сотрудник с высоким показателем лояльности.

В данном классе ущерб компании будет значительней, чем в случае нарушителя HR2, но менее вероятен в связи с высоким показателем лояльности. Реализация инцидента информационной безопасности, влекущего за собой репутационные потери для организации, в данном случае может быть спровоцирована исключительно неосведомленностью в политике информационной безопасности (в т. ч. ввиду ее отсутствия).

HR4: высококвалифицированный сотрудник с низким показателем лояльности, в т. ч. занимающий высокую должность в организации (вице-президент, заместитель генерального директора, главный бухгалтер).

В результате инцидентов информационной безопасности, спровоцированных сотрудниками данного класса, организация понесет наиболее ощутимые репутационные (а вследствие – и финансовые) потери. Опасность данного класса наиболее велика, поскольку сотрудники, занимающие упомянутые позиции в управлении компанией, непосредственно владеют большими объемами критичной для организации информации и имеют технологический доступ к ней. Более того, в соответствии с высоким уровнем профессионализма и пониманием всех слабых мест деятельности организации, данный класс нарушителей может спровоцировать инцидент информационной безопасности, влекущий за собой, в т. ч., полную остановку деятельности компании.

Стоит отметить следующие особенности при классификации нарушителя для данной группы:

- ✓ при необходимости определения класса нарушителя, принятого на работу, проходящего испытательный срок, данному сотруднику присваивается класс H2;
- ✓ показатель профессионализма сотрудника определяется экспертным мнением его непосредственного руководителя;
- ✓ показатель лояльности определяется удобной для компании методикой тестирования. Рекомендуется мероприятие по определению показателя лояльности для сотрудника проводить сразу после испытательного срока.

В соответствии с определенными в данной работе классами нарушителей информационной безопасности в сфере взаимоотношений с сотрудниками, необходимо сделать вывод, что для минимизации рисков потери репутации необходимо предпринимать следующие действия:

- ✓ регулярно контролировать степень лояльности сотрудников, в особенности занимающих высокие посты в организации. При обнаружении низкой степени лояльности, не допускать ознакомление со сведениями, составляющими критичную информацию для организации;
- ✓ разработка политики информационной безопасности, затрагивающей все аспекты эффективного менеджмента в области информационной безопасности;

- ✓ разработка полного перечня необходимой организационно-распорядительной документации в соответствии с принятой политикой информационной безопасности;
- ✓ регулярно проводить мероприятия по повышению уровня осведомленности персонала в вопросах информационной безопасности в целом и основным положениям политики безопасности, принятой в организации в частности.

Взаимоотношения с государственными органами (GR).

Во взаимоотношениях с государственными структурами инцидентом информационной безопасности, влекущим за собой репутационные потери, стоит считать факт нарушения требований нормативно-правовой документации в области обеспечения информационной безопасности. Кроме того, к инциденту информационной безопасности для данного вида взаимоотношений относится разглашение информации о деятельности организации, противоречащей законодательству. Для данного вида взаимоотношений представляется возможным определить следующие классы нарушителей:

GR1: сотрудники, ответственные за соответствие процессов деятельности компании законодательным требованиям (Compliance Manager).

При отсутствии данной позиции в компании ответственным является ее генеральный директор. В соответствии с должностными обязательствами сотрудник данного класса нарушителей обязан организовать выполнение всех организационно-правовых и технических мер по защите информации в соответствии с требованиями законодательных актов. По результатам проверок государственных регуляторов организация, как правило, получает предписание к устранению несоответствий законодательным требованиям (что влечет за собой финансовые убытки), а также обязана оплатить штрафы, предусмотренные за нарушение данных требований.

GR2: технические специалисты, отвечающие за обеспечение информационной безопасности в части настройки и администрирования средств защиты информации (СЗИ), не обладающие должной компетенцией либо не выполняющие предписание по настройке СЗИ в соответствии с требованиями, определенными в организации согласно положениям нормативно-правовых документов.

В большом количестве организаций к корректной настройке СЗИ относятся халатно. Администраторы информационной безопасности под давлением сотрудников, отвечающих за организацию и обслуживание информационных технологий, подстраиваются под текущую сетевую инфраструктуру, не производя в конфигурации средств вычислительной техники и активного сетевого оборудования настроек, изменяющих текущий порядок работы пользователей. Настройки безопасности существенно корректируются в соответствии с «желаниями» пользователей, а не в соответствии с требованиями, регламентированными законодательными актами. Из-за халатности сотрудников возрастает риск

утечки информации по техническим каналам, а также штрафов государственных регуляторов за несоответствие требованиям нормативной документации.

GR3: сотрудники, в соответствии с мероприятиями, инициированными с целью приведения процессов деятельности в соответствие с требованиями нормативных документов по информационной безопасности, назначенные ответственными за ведение организационно-распорядительной документации (например, журнал пользователей криптосредств и т. д.).

GR4: компании-конкуренты, в рамках проведения «конкурентной разведки» способные выявить различного рода нарушения законодательства. В соответствии с полученными сведениями нарушитель данного класса может спровоцировать внеплановую проверку со стороны государственных регуляторов.

На основании определенных в данной статье классов нарушителей информационной безопасности в сфере взаимоотношений с государственными органами можно сделать вывод, что для минимизации рисков потери репутации необходимо предпринимать следующие действия:

- ✓ привести все процессы обработки информации в соответствие с требованиями нормативных документов;
- ✓ однозначно и понятно разработать должностные инструкции для каждого сотрудника, участвующего в обработке информации, в соответствии с законодательством отнесенной к конфиденциальной (персональные данные, коммерческая тайна и др.);
- ✓ в политике информационной безопасности описать недопустимость отклонения от определенных законодательством методов защиты информации в части технической защиты информации, а также в соответствии с необходимыми к выполнению организационными мероприятиями;
- ✓ необходимо периодически проверять лояльность сотрудников к трудовым условиям работы в компании. Также регулярно следует проводить мероприятия по повышению уровня лояльности среди персонала.

Взаимоотношения с общественностью (PR).

Наибольшее влияние на репутацию компании оказывает общественное мнение. В то же время основными рычагами воздействия на общественное мнение являются СМИ. Опубликование компрометирующей информации в СМИ может вызвать негативную реакцию потребителей услуг, провоцируя финансовые убытки. В связи с этим целесообразно рассмотреть нарушителей информационной безопасности во взаимоотношениях с общественностью. Инцидент информационной безопасности во взаимоотношениях с общественностью может быть реализован как «специально», для влияния на репутацию организации, так и «случайно», вследствие низкого уровня осведомленности в политике информационной безопасности организации.

PR1: нарушитель, публикующий критическую для организации информацию с целью навредить организации.

К данному классу нарушителей можно отнести сотрудников организации с низким уровнем лояльности, в рамках своих служебных обязанностей ознакомленных с критичной для организации информацией.

Одновременно, к данному классу относятся и бывшие сотрудники организации, проработавшие в ней достаточное количество времени и уволенные в связи с конфликтом с руководством. Опасность данного нарушителя определяется в соответствии с тем, к какому классу HR он одновременно относится.

Вместе с тем к данной категории нарушителей стоит отнести и компании-конкуренты, которым в рамках конкурентной разведки удалось ознакомиться со сведениями, представляющими важность для организации и способными, посредством опубликования, повлиять на ее репутационную составляющую.

Также к данному классу нарушителей стоит отнести недовольных клиентов компании, неравнодушных общественных людей, либо сами СМИ, публикующие подобного рода статьи для расширения аудитории читателей. Методами, которыми пользуется нарушитель данного класса, могут также являться глобальные «пиар-компании».

PR2: нарушитель, публикующий в СМИ ложную информацию о процессах деятельности.

К данному классу нарушителей можно отнести бывших сотрудников, в т. ч. уволенных из организации после испытательного срока. Поскольку на протяжении испытательного срока сотрудник, как правило, не бывает ознакомлен с критической информацией для организации, увольнение, в связи с профнепригодностью провоцирует на ответные шаги со стороны сотрудника, с целью навредить не оценившему его руководству распространением ложной информации, которая может привести к репутационным потерям. Распространение ложной информации может происходить посредством как официальных СМИ, так и личных блогов и тематических форумов в интернете.

Одновременно ложную информацию с использованием СМИ могут распространять представители компаний-конкурентов по бизнесу, в рамках «черного пиара».

PR3: нарушитель, публикующий информацию в открытых источниках на законном основании.

К данному классу можно отнести представителей государственного регулятора, в рамках законных полномочий публикующих информацию о проблемах организации, связанных с невыполнением требований законодательных актов.

PR4: нарушитель, публикующий реальную критическую информацию без цели нанесения вреда организации.

К данному классу нарушителей относятся сотрудники, способные опубликовать критическую информацию в СМИ, а также личных блогах и тематических форумах, которые обладают низким уровнем осведомленности в области информационной безопасности в связи с отсутствием мероприятий по повышению осведомленности в ИБ либо отсутствием политики ИБ в организации

в целом. Ущерб от действий данного сотрудника зависит от уровня ознакомления его с критической для организации информацией.

В соответствии с определенными в данной статье классами нарушителей информационной безопасности в сфере взаимоотношений с общественностью можно сделать вывод, что для минимизации рисков потери репутации необходимо предпринимать следующие действия:

- ✓ проводить мероприятия по повышению уровня осведомленности сотрудников организации в области информационной безопасности;
- ✓ проводить проверочные мероприятия по наличию у сотрудников личных блогов или иных площадок размещения информации в интернете. Разработать инструкцию по работе сотрудников в сети интернет, максимально ограничивающую возможность разглашения критической информации о деятельности сотрудников;
- ✓ документально определить ответственность сотрудника за разглашение информации о деятельности организации, ставшей ему известной в соответствии с его служебными обязанностями. Ознакомить сотрудников под роспись с разработанными распорядительными документами в части обеспечения информационной безопасности;
- ✓ проводить мероприятия по противодействию конкурентной разведке со стороны компаний-конкурентов по бизнесу;
- ✓ выделять средства на рекламу основных видов деятельности компании, с целью снизить издержки от появления ложной информации.

Взаимоотношения с инвесторами (IR).

Для крупных компаний важным является не только сохранение репутации среди конечного потребителя, но и недопущение репутационных потерь в отношениях с инвесторами. Отказ инвестора по поводу вложений в процессы деятельности организации может привести к частичному или полному их прекращению. Также для компании важным аспектом является недопущение утечки информации о стратегических партнерах (инвесторах и партнерах по бизнесу), не желающих приобретать публичный статус. В соответствии с этим можно выделить следующие классы нарушителей в сфере взаимоотношений с инвесторами:

IR1: сотрудники компании, принимающие участие в процессах деятельности, связанных со стратегическим партнерством.

К данному классу целесообразно отнести сотрудников классов HR3 и HR4, в соответствии с уровнем осведомленности о стратегических партнерах организации. Инцидент, спровоцированный данным нарушителем, с большой вероятностью прервет сотрудничество либо приведет к основательному пересмотру условий сотрудничества.

IR2: сотрудники, ответственные за представление периодических отчетов инвесторам компании.

К данному классу относятся сотрудники, занимающие «высокие» посты в организации (класс HR4) – это главный бухгалтер, вице-президент, генераль-

ный директор и т. д. Возможное предоставление инвесторам ложной информации о деятельности организации нарушителями данного класса может повлечь за собой сокращение инвестиций.

К таким относятся сведения о:

- ✓ расходовании выделенных средств;
- ✓ способах управления объектом инвестирования;
- ✓ формировании денежного потока;
- ✓ фактической финансово-хозяйственной картине объекта инвестирования;
- ✓ финансовых, административных и иных рисках;
- ✓ рисках утраты активов и бизнеса в целом.

IR3: сотрудники, способные в силу низкого уровня осведомленности в области информационной безопасности распространять информацию о внутренних проблемах организации.

В данном виде взаимоотношений действия нарушителя данного класса могут спровоцировать понижение стоимости акций на бирже. Также возможен пересмотр политики инвестирования со стороны акционеров.

IR4: компании-конкуренты по бизнесу.

Данный класс нарушителей способен в рамках проведения конкурентной разведки стать обладателем информации о стратегических партнерах и инвесторах организации, по разным причинам не желающих быть публичными. Вследствие опубликования данной информации организация рискует прекращением выгодного партнерства либо понижением объемов инвестирования по ряду направлений, курируемых инвестором.

В соответствии с определенными в данной статье классами нарушителей информационной безопасности в сфере взаимоотношений с инвесторами можно сделать вывод, что для минимизации рисков потери репутации необходимо предпринимать следующие действия:

- ✓ разработать раздел политики информационной безопасности организации, описывающей информационное взаимодействие со стратегическими партнерами;
- ✓ периодически проводить организационные мероприятия, направленные на повышение уровня осведомленности сотрудников, рабочие обязанности которых предусматривают ознакомление с политикой стратегического взаимодействия с непубличными партнерами;
- ✓ проводить необходимые мероприятия по противодействию конкурентной разведке;
- ✓ проводить мероприятия по повышению лояльности сотрудников. Периодически проверять лояльность сотрудников, работающих по направлениям, связанным с взаимодействием со стратегическими партнерами организации.

В каждой компании состав мероприятий по минимизации репутационных рисков определяется индивидуально в соответствии с возможностями и рента-

бельностью их проведения. Проведенная классификация нарушителей информационной безопасности позволяет в достаточной мере представлять картину возможности появления репутационных рисков в компании. Также результаты исследования подчеркивают необходимость проведения ряда мероприятий по выявлению гипотетических классов нарушителей и вместе с тем определяют характер дальнейшей работы в компании, направленной на минимизацию возможных рисков. Стоит отметить, что классификация нарушителей информационной безопасности, которые могут спровоцировать инциденты, влияющие на репутацию, должна являться первым обязательным шагом для эффективного менеджмента в данной области.

Dorohov V. ***Classification of violators as a stage of reputation risks management in the light of information security incidents.*** *The article defines the concept of reputation risk as a component of information security. The types of relationships within which information security incidents may occur are analyzed: HR, PR, GR, IR. Attention is paid to the relationship between reputational risks and profits of the company.*

Key words: *information security, reputation risks, incident of information security.*

Дорохов В. Э. ***Классификация нарушителей как этап менеджмента репутационных рисков вследствие инцидентов информационной безопасности.*** *Определено понятие репутационного риска как составляющей информационной безопасности. Проанализированы виды взаимоотношений, в рамках которых возможно возникновения инцидентов информационной безопасности: HR, PR, GR, IR. Обращено внимание на связь между репутационными рисками и прибылью компании.*

Ключевые слова: *информационная безопасность, репутационные риски, инцидент информационной безопасности.*

Литература

1. *Дорохов В. Э.* О рисках потери репутации организации вследствие инцидентов информационной безопасности / В. Э. Дорохов // Безопасность информационных технологий. – 2014. – № 2. – С. 80–82.
2. *Дорохов В. Э.* Анализ инцидентов информационной безопасности, приводящих к потере репутации, как функция управления хозяйствующим субъектом / В. Э. Дорохов // Новые перспективы развития экономических наук: инновации и риски : сб. материалов XXII Международной науч.-практ. конф. для студ., аспир. и молодых ученых (Москва, 01. 02. 2014 г.). – Москва : Аналит. центр «Экономика и финансы», 2014. – С. 131–134.