Чумичева М. А.

УДК 005.53

Магистр 2 года обучения
факультета экономической информатики ХНЭУ им. С. Кузнеца

ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ КАК ОДИН ИЗ СПОСОБОВ МИНИМИЗАЦИИ БИЗНЕС-РИСКОВ

Аннотация. Исследованы бизнес-риски, их виды и методы борьбы с ними. Показана значимость повышения информационной безопасности предприятия в современных условиях.

Анотація. Досліджено бізнес-ризики, їх види і методи боротьби з ними. Показано значущість підвищення інформаційної безпеки підприємства в сучасних умовах.

Annotation. This article studies business risks, their types and methods of removing them. The increasing importance of information security in the modern world is shown.

Ключевые слова: бизнес, бизнес-риски, утечка информации, информационные активы, DLP-система.

Целью исследования является определение всех возможных методов борьбы с разными видами бизнес-рисков на основе определения бизнес-рисков.

В современных условиях хозяйствования бизнес-риски являются неотъемлемой частью развития и управления бизнесом, а также играют важную роль при оценке стоимости бизнеса. Бизнес-риск является одной из неоднозначных в определении характеристик. На сегодняшний день выделяют два подхода к определению понятия "бизнес-риск". Так, по мнению Стефана Ароса и Рондальфа Вестерфилда, эти подходы трактуются таким образом:

1. Бизнес-риск – это риск, определяющий чувствительность денежного потока фирмы в связи с колебанием агрегированного денежного потока экономики в целом [1].

Его основными факторами являются отраслевые особенности организации материально-технической (то есть ресурсной) базы и финансирования деятельности фирмы, неопределенность в объемах продаж, производственных и коммерческих расходах.

2. Бизнес-риск (в более узком смысле) – как синоним понятия "операционный риск" (или производственный риск) [2].

Приведенные понятия – довольно близкие по определению трактовки, согласно которой бизнес-риск – это риск, который несут акционеры фирмы в случае, если она финансируется лишь за счет собственного капитала (то есть без привлечения заемного капитала), в этом случае объединение бизнес-риска (то есть операционного риска) и финансового риска называют общим риском деятельности фирмы (TotalFirmRisk) [3].

Обобщая названные определения, можно констатировать, что бизнес-риски – это по большей степени абсолютно все риски, которые могут так или иначе поставить деятельность бизнеса под угрозу.

Рассматривая виды рисков, компания "Ernst&Young" провела исследование, в котором приняли участие 641 компания из 21 страны мира. В числе основных были выделены следующие бизнес-риски [4]:

1. Ценовое давление.
2. Рост издержек и падение рентабельности.
3. Рыночные риски.
4. Макроэкономические риски.
5. Недостаток квалифицированных специалистов.
6. Утечка информации и информационная безопасность.
7. Несовершенство законодательств.
8. Новые технологии.

Просмотрев данные по каждому из этих пунктов, хотелось бы остановиться на утечке информации и информационной безопасности, так как именно на этот риск может повлиять руководство. Например, если это утечка конфиденциальной информации, что может являться для всего бизнеса просто смертельным.

Существует по меньшей мере четыре программных решения, призванных противостоять утечкам конфиденциальной информации. Устойчивым названием для этого класса продуктов стал термин DLP (от англ. DataLossPrevention). При грамотном внедрении DLP-системы, подготовке процедурных документов эти решения позволяют существенно снизить вероятность несанкционированного перемещения конфиденциальных данных вовне.

Необходимо представить такую ситуацию: предприятию необходима концепция защиты от утечки информации и надо подобрать соответствующий программный продукт. Но внедрение DLP-решения

предполагает ведение достаточно длительных проектов, затрагивающих многие подразделения компании. Цена среднего внедрения такой системы в среднем составляет от 100 до 500 долларов в пересчете на одно рабочее

место. Разумеется, принять решение об инициации такого проекта можно только имея аргументированное обоснование.

А поскольку речь идет о снижении вредоносных последствий события, которое может наступить с некоторой вероятностью, бизнес-руководителю гораздо легче рассматривать ситуацию в рамках анализа рисков для бизнеса.

Логика проста:

следует представить оценку вероятности наступления события;

нужно оценить возможный ущерб;

следует сопоставить со стоимостью владения системой борьбы с утечкой информации.

Итак, бизнес готов общаться только в категориях управления рисками (Riskassessment) и оценки срока возврата инвестиций в обеспечение информационной безопасности (ROSI).

Без проведения оценки бизнес-рисков и обоснования серьезности потенциальных потерь проект по внедрению DLP-системы активной поддержки менеджмента не получит.

Существует три ситуации, когда риски очевидны и нет необходимости в их серьезном обосновании, а именно:

1. Требование закона.

В случае существования императивных требований законодательных актов о наличии систем борьбы с утечкой данных, ущерб оценить несложно. Как правило, в самом нормативном акте содержится перечень соответствующих санкций за его нарушение.

Кроме того, в случае невыполнения требований нормативного акта компания попросту может не получить нужного ей разрешения на доступ в платежную систему, к государственному конкурсу, на торговую площадку и т. д.

2. Базовые требования по безопасности (security baseline).

Зачастую требования по внедрению какой-либо системы информационной безопасности явно указываются в базовых требованиях обеспечения безопасности.

Совсем недавно ИТ-руководителям приходилось объяснять бизнесу необходимость и оправданность затрат на эти системы. Сейчас сложилось понимание необходимости наличия минимального набора технических средств, которые обеспечивают достаточный уровень информационной безопасности. Это понимание, многократно описанное во всевозможных Securityguide и Securitybaseline, принимается сейчас экспертным сообществом, крупнейшими производителями в области информационной безопасности и подавляющим большинством практикующих специалистов.

3. Аналитика и внешняя статистика.

Удобным и не требующим затрат средством демонстрации размера потенциального ущерба могут являться внешние данные. Это аналитические отчеты Gartner и IDC, данные опросов, предоставляемые вендорами, статистика по индустрии и собственные данные предприятия за предыдущие годы.

Так, по данным, которые приводятся в материалах компании McAfee, средняя стоимость мероприятий только по информированию клиентов о случившейся утечке финансовой информации составляет 268 тыс. долл. Websense в своих материалах ссылкой на PonemonInstitute SVB Alliant приводит среднюю оценку только прямых затрат на инцидент в размере 1,4 млн дол.

В целом идентификация рисков сводится к определению информации (assets), бесконтрольная утечка которой вовне может повлиять на бизнес, и оценке угроз (threats) – по сути, сценариев утечки.

Далее приведен перечень некоторых информационных активов, как правило, подлежащих защите:

финансовая и бухгалтерская информация;

документы стратегического развития;

прогнозы по развитию бизнеса;

внутренние документы конкурентного анализа;

аналитика по рынкам;

протоколы собраний и совещаний;

внутренние приказы и распоряжения;

персональные данные сотрудников;

должностные инструкции по отдельным подразделениям;

описание мотивационных схем персонала;

договоры с поставщиками.

Подготовка общего рубрикатора конфиденциальной информации является первым шагом, необходимым для определения информационных активов, подлежащих защите. На практике такой рубрикатор довольно сильно зависит от области деятельности компании.

Оценка угроз утечки предполагает описание возможных сценариев неконтролируемой утечки данных всеми доступными способами. Среди лидеров каналов утечки: сетевые коммуникации (email, web-mail, ICQ) и сохранение данных на переносные USB-накопители.

На практике эффективным методом снижения рисков утечки является разумное "закручивание гаек" в части получения доступа к защищаемой информации. Даже до проведения полноценного анализа рисков вполне реально выявить случаи избыточного доступа для отдельных групп сотрудников, запретить его и тем самым исключить часть угроз.

После того как создан рубрикатор данных, защищаемых от утечек, и выявлены реальные возможности несанкционированного перемещения данных угрозы, становится возможным проведение качественной оценки потенциальных потерь.

Общими негативными последствиями влияния на бизнес в результате утраты контроля над потенциальными бизнес-рисками являются:

снижение числа новых и отток существующих заказчиков;

потеря доверия поставщиков и партнеров;

ослабление позиций в конкурентной борьбе;

утрата технологических секретов;

снижение котировок акций и утрата доверия инвесторов;

снижение стоимости бренда;

влияние на рейтинги компании;

санкции контролирующих органов;

судебные разбирательства;

необходимость затрат на устранение последствий.

Главной задачей качественного анализа является расстановка приоритетов по списку выявленных рисков в зависимости от степени их влияния на бизнес.

На практике установленный приоритет может повлиять на очередность, с которой информационные ресурсы будут попадать в число защищаемых по мере внедрения системы борьбы с утечками.

В большинстве случаев руководству достаточно получить реестр рисков (основанный на рубрикаторе защищаемой информации) и результат качественного анализа рисков. Но в некоторых случаях требуется представить оценку ущерба, выраженную в числах.

Для иллюстрации количественной оценки возможных потерь для бизнеса (прямых затрат и неполученной прибыли) можно использовать следующую схему:

1) выделяется один из классов данных согласно разработанному рубрикатору конфиденциальной информации;

2) определяются все виды негативного влияния на бизнес вследствие утечки данных этого класса;

3) детализируется список затрат, необходимых для устранения последствий утечки.

Но полноценная оценка риска предполагает не только анализ масштабов ущерба, но и оценку вероятности наступления события. Существует несколько подходов, позволяющих получить такую оценку вероятности, а именно:

1. Внутренняя статистика инцидентов.

Практически неприменима в случае, когда компания только задумывается о развертывании системы противодействия утечкам. Даже если в компании сформировалась какая-то статистика по замеченным утечкам, нельзя оценить число оставшихся незамеченными.

2. Внешняя статистика.

Можно найти вероятностные оценки для отдельных типов событий. Но все, что касается инцидентов по утечкам, обычно надежно скрывается. Вероятностной оценки, основанной на собранной информации по рынку аналитики, для данной области не построить.

3. Экспертная оценка.

Неплохие результаты может дать проведение экспертной оценки возможности наступления угрозы. Эксперт должен будет выделить существующие каналы утечки конфиденциальной информации, описать реалистичные сценарии и вынести свою оценку возможности реализации для каждого из этих сценариев. Опираться в своей работе он может на опыт предыдущих проектов, руководства производителей DLP-систем и принцип "если могут – значит воруют". Результатом обычно является дискретная шкала оценки вероятности от "очень низкой" до "очень высокой".

4. Экспериментальная оценка.

Этот метод является наиболее эффективным методом оценки реалистичности угрозы. Именно экспериментальное развертывание системы слежения за перемещением конфиденциальной информации поможет дать ответ на вопрос о реалистичности угрозы для компании.

Эксперимент сводится к развертыванию в рабочей системе пилота DLP-системы. Существующие на рынке системы неплохо подходят для быстрых "пилотных" проектов. Это связано с возможностью быстрого обучения на образцах конфиденциальных документов. Реальный срок развертывания пилота в боевой системе даже крупной организации – около двух месяцев. Разумеется, существует ряд ограничений, которые необходимо соблюдать, чтобы эксперимент получился "чистый":

закрытость проекта;

реальные потоки информации;

проверка критичных данных.

В результате работы такого "пилотного" решения за срок порядка 30 – 45 дней скапливается достаточно оперативной информации, анализ которой позволяет сделать выводы о реалистичности угрозы неконтролируемой утечки данных и о том, какие могут быть использованы сценарии утечек в условиях данной среды.

Лучшим аргументом реалистичности угрозы является отчет DLP-системы о том, сколько всего переправили вовне сотрудники компании по ошибке, непониманию или злому умыслу.

И после этого бизнес-руководство принимает решение. В результате всей этой работы на рассмотрение руководства выносится отчет, содержащий, с одной стороны, картину рисков, с другой – структуру совокупной стоимости владения системой противодействия утечкам информации.

В свою очередь, совокупная стоимость владения DLP-системой должна включать цену лицензий на ПО, серверов, работ по внедрению продукта, затрат на обучение персонала, подготовку рубрикатора конфиденциальной информации, написанию процедур и политик и видения бизнеса.

Приведенный набор условий позволяет сделать вывод, что такие процедуры хоть и могут достигать весьма высоких ценовых порогов, но в то же время данные процедуры куда важней и "дешевле" чем покрытие убытков после той или иной утечки информации.

В целом бизнес-риски каждую минуту окружают работу того или иного бизнеса и только руководство вправе решать какой из этих рисков будет первый в списке по минимизации риска или его сведении до минимума.

Научн рук. Грачев В. И.

Литература: 1. Ross S. Corporate Finance / S. Ross, R. Westerfield, S. Jaffe. – 7th ed. – Irwin : McGraw-Hill, 2005. 2. Ross S. A. Fundamentals of Corporate Finance / S. A Ross, R. W. Westeijleld, B. D. Jordan. – Irwin, Inc., 1991. 3. VanHome. – Gitman. – P. 139. 4. Недосекин А. О. Комплексная оценка риска банкротства корпорации на основе нечетких описаний [Электронный ресурс] / А. О. Недосекин. – Режим доступа : ttp://sedok.narod.ru/sc_group.html.