ЗАЩИТА ИНФОРМАЦИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Т.В. Лебедева[1]

РИСКИ. ОЦЕНКА И УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ

В данной статье речь идет о рисках, методах их оценки и управления ими.

Ключевые слова: *риск, оценка рисков, информация, стоимость информации, оценка ущерба.*

T.V. Lebedeva

RISKS. RISK EVALUATION AND RISK MANAGEMENT

This article focuses on the risks, methods of their evaluation and management.

Keywords: *risk, opinion of risk, information, cost of information, opinion of damage.*

Бытует мнение, что управление рисками – удел топ-менеджеров либо сотрудников специализированных подразделений, риск-менеджеров, аналитиков. Однако на деле все обстоит по-иному. Регулирование, а тем более оценка рисков являются прикладными задачами. И сфера информационной безопасности (ИБ) – не исключение. Специалисты в области ИБ должны скрупулезно отслеживать возникающие угрозы, анализировать связанные с ними риски и представлять руководству уже готовый отчет-план, дающий представление о том, какими средствами нужно бороться за сохранность корпоративных данных.

Прежде чем заниматься рассмотрением вопроса управления рисками, необходимо дать определение и основное описание этого понятия.

Информационные риски – это опасность возникновения убытков или ущерба в результате использования компанией информационных технологий (*IT*). Иными словами, *IT*-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи.

***IT*-риски можно разделить на две категории**.

1. Риски, вызванные утечкой информации и использованием ее конкурентами или сотрудниками в целях, которые могут повредить бизнесу.

2. Риски технических сбоев работы аппаратного и программного обеспечения, каналов передачи информации, которые могут привести к убыткам.

Работа по минимизации *IT*-рисков заключается в предупреждении несанкционированного доступа к данным, а также аварий и сбоев оборудования и программного обеспечения.

Процесс минимизации *IT*-рисков следует рассматривать комплексно. Сначала выявляются возможные проблемы, а затем определяется, какими способами их можно решить.

1. Сможет ли компания в короткий срок интегрировать существующие технологии работы с информацией в системы предприятия, являющегося объектом слияния или приобретения? (Например, в компании установлена одна или несколько учетных систем, с помощью которых финансисты получают данные для составления консолидированной отчетности. При покупке нового предприятия выясняется, что у него установлена другая учетная система. Поэтому у компании должен быть четкий план трансформации такой отчетности в стандарты, принятые на головном предприятии. В противном случае она может потерять оперативный контроль над ситуацией.)

2. Позволяет ли организация документооборота компании в существующих системах продолжить ее деятельность в прежнем режиме в случае ухода ключевых сотрудников? (Эта проблема чрезвычайно актуальна для российских компаний, поскольку даже финансовая и бухгалтерская информация зачастую вводится и хранится в произвольном виде, не говоря уже о сведениях, касающихся клиентов и т.п. Это ведет к дополнительным затратам времени новых сотрудников на «вхождение» в курс дела и повышает вероятность возникновения ошибок.)

3. Обеспечена ли защита интеллектуальной собственности компании и ее клиентов?

4. Имеет ли компания четкий алгоритм дей-

---

[1] Аспирант НОУ ВПО «Российский новый университет».

ствий в критической ситуации, например в случае сбоев в работе компьютерных сетей или вирусной атаки?

5. Соответствует ли способ работы информационных систем общим задачам компании? (Если перед компанией стоит задача иметь общий центр управления денежными потоками, а учетные системы, установленные в разных филиалах, не связаны между собой, то поставленная задача не будет решена.)

Точно определить возможный ущерб от большинства *IT*-рисков довольно сложно, но примерно оценить их вполне возможно.

Виды рисков в информационных системах

Кроме критериев, учитывающих финансовые потери, коммерческие организации могут применять критерии, отражающие:

1) ущерб репутации организации;

2) неприятности, связанные с нарушением действующего законодательства;

3) ущерб для здоровья персонала;

4) ущерб, связанный с разглашением персональных данных отдельных лиц;

5) финансовые потери от разглашения информации;

6) финансовые потери, связанные с восстановлением ресурсов;

7) потери, связанные с невозможностью выполнения обязательств;

8) ущерб от дезорганизации деятельности.

Могут использоваться и другие критерии в зависимости от профиля организации. К примеру, в правительственных учреждениях прибегают к критериям, отражающим специфику национальной безопасности и международных отношений.

Этапы процесса управления рисками

Процесс управления рисками можно разделить на следующие этапы:

1) выбор анализируемых объектов и уровня детализации их рассмотрения;

2) выбор методологии оценки рисков;

3) идентификация активов;

4) анализ угроз и их последствий, выявление уязвимых мест в защите;

5) оценка рисков;

6) выбор ответных мер;

7) реализация и проверка выбранных мер;

8) оценка остаточного риска.

От последнего этапа в случае неприемлемости остаточного риска происходит возврат к началу.

Методики оценки рисков

Выбор методики оценки рисков является ключевым процессом управления рисками. Многие документы содержат рекомендации по выбору методики или просто вариант методики. В методиках в основном предлагаются различные способы сопоставления возможных последствий реализации угрозы с вероятностью ее реализации и получения соответствующих выводов.

В зависимости от «математизации» этой процедуры сопоставления и выводов методики иногда делят на *качественные*, *полуколичественные* и *количественные*. При этом можно встретить точку зрения, что количественные методики, в принципе, лучше качественных, и лишь недостаток точных данных (например, статистики инцидентов) не дает пока возможности полностью перейти на их использование, а если бы удалось еще сделать оценку последствий в денежных единицах, то проблема оценки рисков вообще перестала бы быть проблемой.

Обработка риска

После того как риск оценен, должно быть принято решение относительно его обработки – точнее, выбора и реализации мер и средств по минимизации риска. Помимо оцененного уровня риска при принятии решения могут быть учтены затраты на внедрение и сопровождение механизмов безопасности, политика руководства, простота реализации, мнение экспертов и др.

Предлагается одна из четырех мер обработки риска.

1. Уменьшение риска. Риск считается неприемлемым – и для его уменьшения выбираются и реализуются соответствующие меры и средства безопасности.

2. Передача риска. Риск считается неприемлемым – и на определенных условиях (например, в рамках страхования, поставки или аутсорсинга) переадресуется сторонней организации.

3. Принятие риска. Риск в конкретном случае считается осознанно допустимым – организация должна смириться с возможными последствиями. Обычно это означает, что стоимость контрмер значительно превосходит финансовые потери в случае реализации угрозы либо организация не может найти подходящие меры и средства безопасности.

4. Отказ от риска. Отказ от бизнес-процессов организации, являющихся причиной риска. Например, отказ от электронных платежей по Сети.

В результате обработки риска остается так называемый остаточный риск, относительно которого принимается решение о завершении этапа отработки риска.

В сфере ИБ постоянно возникают новые угрозы, соответственно в организациях все время должны совершенствоваться и меры защиты. Топ-менеджеры не могут сами отслеживать эти изменения. Если департамент ИБ не докладывает о на-

растающих внутренних угрозах, способных привести к ощутимым убыткам, откуда об этом узнает руководство? Таким образом, часть работы сотрудников ИБ состоит в том, чтобы отслеживать угрозы и докладывать о них начальству, которое принимает стратегические решения. Это несложно, тем более что проблемы безопасности широко освещаются в прессе, обсуждаются на конференциях и деловых встречах. Немало отчетов о разного рода инцидентах подготовили Секретная служба США, CERT, *Ponemon Institute, InfoWatch* и другие эксперты в области ИБ.

Еще одним аспектом работы над ИБ-проектом является выбор адекватного инструмента. Когда сотрудники подразделения ИБ выявляют угрозу, требуется сначала найти ее истинные причины. Изучить последствия недостаточно, нужно смотреть шире рамок конкретного инцидента. Комплексное решение зачастую поможет справиться не только с нынешними, но и с будущими угрозами. В то же время, в некоторых случаях большие траты неоправданны, стрелять из пушки по воробьям не нужно. Порой будет достаточно ограничить доступ конкретного сотрудника к конкретным конфиденциальным ресурсам, Интернету, закрыть *USB*-порты на компьютере и т.п. И тогда уже не будет нужды отслеживать его деятельность, работник уже не сможет скопировать секретные документы. Наблюдать надо за теми пользователями, которые имеют доступ к критическим данным.

Часто сотрудники, которые отвечают за ИБ, жалуются, что руководство их плохо финансирует. Однако на деле выясняется, что в большинстве таких случаев диалог сводится к простому обмену репликами: исполнитель просит столько-то денег, начальство отказывает. Оперируя цифрами, легко показать, сколько можно сэкономить и на чем выиграть от дополнительных инвестиций в безопасность. Если много говорить о проблемах и угрозах, не опираясь на факты, очень скоро на это перестанут обращать внимание. Многие сотрудники подразделений ИБ не готовы или просто не умеют подготовить экономическое обоснование затрат. Когда сотрудники ИБ и бизнес-управленцы смогут говорить на одном языке, сотрудничество получится более продуктивным. Если собрать свидетельства, подкрепить их отчетами аналитиков и представить четкий бизнес-план, как устранить угрозу, тогда будет легче убедить руководство в необходимости принять соответствующие меры.

Литература

1. Астахов, А. Искусство управления информационными рисками. – М. : ДМК Пресс, 2010. – 312 с

2. Велигура, А. О выборе методики оценки исков информационной безопасности // Информационная безопасность. – 2010. – 21 апреля.

3. Марков, А. Управление рисками – нормативный вакуум информационной безопасности. – http://www.osp.ru, от 09.11.2007

4. Ульянов, В. Анализ рисков в области информационной безопасности. – http://www.pcweek.ru, от 23.10.2007