УДК 681.3

РАЗРАБОТКА КОРПОРАТИВНОЙ МЕТОДИКИ АНАЛИЗА ИНФОРМАЦИОННЫХ РИСКОВ

Ю.С. НОСОВА, И.А. ЧУРКИН

Кубанский государственный технологический университет,
350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
электронная почта: bahes.in@gmail.com

При информатизации бизнеса, как правило, задействованы колоссальные бюджеты. В крупных компаниях масштабы проектной деятельности в области информационных технологий измеряются миллионами долларов. Большие бюджеты, в свою очередь, подразумевают больший уровень рисков, ответственности и компетенции тех людей, которые управляют информатизацией бизнеса. Естественно, что организацию и управление рисками необходимо осуществлять на основе известных существующих стандартов и методологий разработчиков программных продуктов и информационных технологий, лучших практик ИТ-корпораций, личного опыта менеджеров ИТ-проектов. Единственного правильного алгоритма управления рисками при информатизации бизнеса и реализации программных проектов просто не существует. Однако проектный характер разработки ПО, а также необходимость управления рисками в связи с высокой степенью уникальности и неопределенности программных проектов обусловили развитие специализированных методов управления рисками, которые описаны в данной статье.

Ключевые слова: анализ, риски, управление рисками, оценка рисков, корпоративные информационные системы, безопасность.

Анализ информационных рисков позволяет эффективно управлять информационной безопасностью предприятия. Для этого в начале работ по анализу рисков необходимо определить, что именно подлежит защите на предприятии и воздействию каких угроз оно подвержено, а затем выработать рекомендации по практике защиты. Обсудим теперь, как разработать свою собственную методику анализа и управления информационными рисками компании.

Такой анализ производится исходя из непосредственных целей и задач по защите конкретного вида информации конфиденциального характера. Одна из важнейших задач в рамках такой защиты информации – обеспечение ее целостности и доступности. Часто забывают, что нарушение целостности может произойти не только вследствие преднамеренных действий, но и по ряду других причин: сбоев оборудования, ведущих к потере или искажению информации; физических воздействий, в частности в результате стихийных

бедствий; ошибок в программном обеспечении (в том числе из-за недокументированных возможностей). Поэтому под термином «атака» будем понимать воздействия на информационные ресурсы не только человеческие, но и окружающей среды, в которой функционирует система обработки информации предприятия.

Анализ риска можно проводить согласно методике по сценарию, представленному на рисунке 1 [1].

Рисунок 1 – Сценарий анализа информационных рисков компании

Каждый из шести этапов анализа риска должен быть конкретизирован.

На первом и втором этапах выявляются сведения, составляющие для предприятия коммерческую тайну, которые предстоит защищать.

Понятно, что такие сведения хранятся в установленных местах и на конкретных носителях, передаются по каналам связи и обрабатываются в

соответствии с принятым регламентом. При этом основным фактором в технологии обращения с информацией является архитектура КИС, от которой во многом зависит защищенность информационных ресурсов предприятия.

В связи с этим необходимо еще раз подчеркнуть, что степень информационной безопасности определяется не только (а может быть и не столько) средствами и способами защиты, но и особенностями построения КИС. И когда говорят о КИС в защищенном исполнении, речь идет, прежде всего, о выборе такой архитектуры (топологии) системы обработки информации, расположения средств обработки конфиденциальной информации и способов ее хранения и передачи, которые существенно уменьшат число возможных точек доступа к информации.

Третий этап анализа риска – построение схем каналов доступа, утечки или воздействия на информационные ресурсы основных узлов КИС. Каждый канал доступа характеризуется множеством точек, с которых можно «снять» информацию. Именно они представляют собой уязвимости и требуют применения средств недопущения нежелательных воздействий на информацию.

Анализ способов защиты всех возможных точек атак соответствует целям защиты, и его результатом должна быть характеристика возможных брешей в обороне, в том числе за счет неблагоприятного стечения обстоятельств (четвертый этап).

На пятом этапе исходя из известных на данный момент способов и средств преодоления оборонительных рубежей находятся вероятности реализации угроз по каждой из возможных точек атак.

На заключительном этапе производится оценка ущерба организации в случае реализации каждой из атак. Эти данные вместе с оценками уязвимости позволяют получить ранжированный список угроз информационным ресурсам[2].

Результаты работы представляются в виде, удобном для их восприятия и выработки решений о коррекции существующей системы защиты информации. При этом важно, что каждый информационный ресурс может быть подвержен

воздействию нескольких потенциальных угроз. Принципиальное же значение имеет суммарная вероятность доступа к информационным ресурсам, которая складывается из элементарных вероятностей доступа к отдельным точкам прохождения информации.

Величина информационного риска по каждому ресурсу – это произведение вероятности нападения на ресурс, вероятности реализации угрозы и ущерба от информационного вторжения. В данном произведении могут быть использованы различные способы взвешивания составляющих.

Объединение рисков по всем ресурсам дает общую величину риска при принятой архитектуре КИС и внедренной в нее системы защиты информации[3].

Таким образом, варьируя варианты построения системы защиты информации и архитектуры КИС, можно (за счет изменения вероятности реализации угроз) представить и рассмотреть различные значения риска. Здесь весьма важным шагом является выбор одного из вариантов в соответствии с заданным критерием принятия решения. Таким критерием может быть допустимая величина риска или отношение затрат на обеспечение информационной безопасности к остаточному риску.

При построении систем обеспечения информационной безопасности также нужно определить стратегию управления рисками на предприятии.

На сегодня известно несколько подходов к управлению рисками. Один из наиболее распространенных – уменьшение риска путем принятия комплексной системы контрмер, включающей программно-технические и организационные меры защиты. Близким является подход, связанный с уклонением от риска. От некоторых классов рисков можно уклониться, например: вынесение веб-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны веб-клиентов.

Наконец, в ряде случаев допустимо принятие риска. В этой ситуации важно определиться со следующей дилеммой: что для предприятия выгоднее –

бороться с рисками или же с их последствиями. Здесь приходится решать оптимизационную задачу.

После того как стратегия управления рисками выбрана, проводится окончательная оценка мероприятий по обеспечению информационной безопасности с подготовкой экспертного заключения о защищенности информационных ресурсов. В экспертное заключение входят все материалы анализа рисков и рекомендации по их снижению.

Отметим, что выполнение анализа рисков и оценки потерь требует глубоких системных знаний и аналитического мышления во многих областях, смежных с проблемой защиты информации.

Методы оценки информационных рисков.

В настоящее время используются различные методы оценки информационных рисков отечественных компаний и управления ими. Оценка информационных рисков компании может быть выполнена в соответствии со следующим планом:

- идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса;

- оценивание возможных угроз;

- оценивание существующих уязвимостей;

- оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для бизнеса уязвимые информационные ресурсы компании подвергаются риску, если по отношению к ним существуют какие-либо угрозы. Другими словами, риски характеризуют опасность, которая может угрожать компонентам корпоративной информационной системы [4]. При этом информационные риски компании зависят от:

- показателей ценности информационных ресурсов;

- вероятности реализации угроз для ресурсов;

- эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. После оценки рисков можно выбрать средства, обеспечивающие желаемый уровень информационной безопасности компании. При оценивании рисков учитываются такие факторы, как ценность ресурсов, значимость угроз и уязвимостей, эффективность имеющихся и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть установлены как количественными методами (например, при нахождении стоимостных характеристик), так и качественными, скажем, с учетом штатных или чрезвычайно опасных нештатных воздействий внешней среды.

Возможность реализации угрозы для некоторого ресурса компании оценивается вероятностью ее реализации в течение заданного отрезка времени. При этом вероятность того, что угроза реализуется, определяется следующими основными факторами:

- привлекательностью ресурса (учитывается при рассмотрении угрозы от умышленного воздействия со стороны человека);

- возможностью использования ресурса для получения дохода (также в случае угрозы от умышленного воздействия со стороны человека);

- техническими возможностями реализации угрозы при умышленном воздействии со стороны человека;

- степенью легкости, с которой уязвимость может быть использована.

ЛИТЕРАТУРА

1. Расторгуев, С. П. Об обеспечении защиты АИС от недокументированных возможностей программного обеспечения // Конфидент. Защита информации №2. / С. П. Расторгуев – 2005. – с. 26-29.

2. Саати, Т. Принятие решений: метод анализа иерархий / Т. Саати – М.: Радио и связь, 1993. – с. 34-38.

3. Староверов, Д. Оценка угроз воздействия конкурента на ресурсы организации // Конфидент. Защита информации. №2. / Д. Староверов – 2005. – с. 58-62.

4. Трубачев, А. П. Оценка безопасности информационных технологий / А. П. Трубачев, М. Ю. Долинин, М. Т. Кобзарь, А. А. Сидак, В. И. Сороковиков / Под общ. ред. В. А. Галатенко. – М.: Издательство СИП РИА, 2008. – с.56-59.

REFERENCES

1. Rastorguyev, S. P. Ob obespechenii zashchity AIS ot nedokumentirovannykh vozmozhnostey programmnogo obespecheniya // Konfident. Zashchita informatsii №2. / S. P. Rastorguyev – 2005. – s. 26-29.

2. Saati, T. Prinyatiye resheniy: metod analiza iyerarkhiy / T. Saati – M.: Radio i svyaz', 1993. – s. 34-38.

3. Staroverov, D. Otsenka ugroz vozdeystviya konkurenta na resursy organizatsii // Konfident. Zashchita informatsii. №2. / D. Staroverov – 2005. – s. 58-62.

4. Trubachev, A. P. Otsenka bezopasnosti informatsionnykh tekhnologiy / A. P. Trubachev, M. YU. Dolinin, M. T. Kobzar', A. A. Sidak, V. I. Soroko-vikov / Pod obshch. red. V. A. Galatenko. – M.: Izdatel'stvo SIP RIA, 2008. – s.56-59.

DEVELOPMENT OF CORPORATE METHODOLOGY FOR ANALYZING INFORMATION RISKS

YU.S. NOSOVA, I. A. CHURKIN

Kuban State Technological University,
2, Moskovskaya st., Krasnodar, Russian Federation, 350072,
e-mail: bahes.in@gmail.com

At information business, involve huge budgets. Scales of design activity in the field of information technologies are measured in the large companies by millions of dollars. Big budgets, in turn, mean the bigger level of risks, responsibility and competence of those people who operate business information. Organization and risk management should be implemented based on known existing standards and methodologies developm-sors of software products and information technology, the best practices of IT corporations, personal experience of managers of IT projects. The only correct algorithm of risk management at business of information and implementation of program projects simply doesn't exist. However design nature of software development, and also need of risk management in connection with high degree of uniqueness and uncertainty of program projects caused development of specialized methods of management of risks which are described in this article.

Key words: analysis, risks, risk management, assessment of risks, corporate information systems, safety.