Б.И. Скородумов[1]

ИНФОРМАЦИОННЫЕ РИСКИ: ПРОБЛЕМЫ И ТЕНДЕНЦИИ

Статья посвящена проблематике информационных рисков, актуальной в нашей стране. В соответствии с законом Российской Федерации «О техническом регулировании» и положениями ряда стандартов предлагается математическая запись понятия «риск». Также предлагается через риск определять понятие «информационная безопасность». Рассматриваются вопросы управления информационными рисками.

Ключевые слова: *информационные риски, угрозы, количественная оценка рисков, управление информационными рисками, информационная безопасность.*

B.I. Skorodumov

INFORMATION RISKS: PROBLEMS AND TENDENCIES

The article considers some problems of information risks, which are relevant in our country. In accordance with the Law "On Technical Regulation" and the provisions of standards, mathematical notations of "risk" and "information security" notions are proposed . Questions of management are considered by information risks.

Keywords*: information risks, threats, quantitative assessment of risks, management of information risks, information security.*

Процесс информатизации общества привел к тому, что компьютерная информация превратилась в основной товар, обладающий значительной ценностью, в своеобразный стратегический ресурс. Генеральный секретарь ООН в своем заявлении по поводу провозглашения 17 мая Международным днем информационного общества отметил важность повышения доверия пользователей к ИТ. Он подчеркнул, что в современном мире, окутанном одной общей Сетью, у общества появилось много угроз и рисков, включая предумышленные атаки на важные информационные объекты, что ведет к ослаблению экономики и общества в целом. Для того чтобы повысить доверие к электронной торговле, электронным банковским системам, телемедицине, электронному правительству, необходима общая сплоченность в вопросах информационной безопасности на международном уровне. И поскольку это зависит от политики безопасности каждой страны, бизнеса и каждого гражданина, необходимо развить культуру инфобезопасности на международном уровне.

Предпринимательская деятельность тесно связана с понятием «риск». Для успешного существования в условиях рыночной экономики предпринимателю необходимо решаться на внедрение технических новшеств и на смелые, нетривиальные действия, что усиливает риск. Решая задачи обеспечения информационной безопасности бизнеса, необходимо помнить, что главной целью любого предпринимателя является прибыль, для получения которой он должен снижать издержки производства и реализации продукта. Весь бизнес-процесс сопровождается расчетами, построенными на базе измерений и учета. Слабым местом всего процесса расчетов является почти полное отсутствие количественных метрик информационной безопасности. «Настоящая наука начинается там, где начинаются измерения», – говорил Дмитрий Иванович Менделеев. Поэтому необходимо правильно оценивать степень риска и уметь управлять риском, чтобы добиваться более эффективных результатов на рынке, например за счет автоматизации. Стремительное развитие КИС сопровождается актуализацией проблемы информационной безопасности.

Риск-менеджмент представляет собой систему управления риском и экономическими отношениями, возникающими в процессе этого управления.

Основная задача риск-менеджмента – идентификация, оценка, анализ и управление рисками. Риск-менеджмент представляет собой постоянный и развивающийся процесс, который ана-

[1] Кандидат технических наук, доцент НОУ ВПО «Российский новый университет».

лизирует развитие организации и ее рисков в движении, а именно: прошлое, настоящее и будущее организации в целом.

Для эффективного управления информационными рисками современных автоматизированных систем предприятий разработаны специальные методики, например методики международных стандартов ISO 27000, ISO/I EC 27005 (BS7799), а также зарубежных национальных стандартов NIST 80030, SAC, COSO, SAS 55/78 и некоторые другие, аналогичные им.

Ранее, до наших дней, и сейчас в отечественных нормативно-методических материалах, созданных уполномоченными государственными организациями по информационной безопасности, широко упоминалось и применяется только понятие «угроза». В последнее время в отечественных стандартах, которые являются переводами международных документов, появилось родственное понятие «риск». Например, этот термин присутствует в стандарте ГОСТ Р ИСО/МЭК 15408 – 2002. Понятие «риск» является доминантным в стандарте ISO17799, который гармонизирован в нашей стране, и в отраслевом стандарте Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». Существенным недостатком банковского стандарта является приближенная качественная оценка информационных рисков.

Определение риска в многочисленной отечественной литературе излагается в разных трактовках. Мы возьмем за основу такое определение: «риск – вероятность причинения вреда…», изложенное в законе Российской Федерации «О техническом регулировании» в 2002 г. [1]. Исходя из идеологии понятия «риск», принятой в законе, можно сформулировать следующее его определение для конкретных технических применений: «риск – количественная (стоимостная) оценка вероятностного события, ведущего к ущербу». Следует отметить, что в той же литературе в основном приводится вербальная запись понятия «риск».

Целесообразно определение риска записать математически как набор упорядоченных пар неблагоприятных событий и вероятностей их реализации за период времени:

$$Risk(\tau) = \{(O_1, P_1(\tau)), \ldots, (O_n, P_n(\tau))\},$$

где *Oi, i=1,...,n* – неблагоприятные события, *Pi, i=1,...,n* – вероятности их реализации, τ – рассматриваемый период времени, $n \in \boldsymbol{N}$, $\boldsymbol{N}$ – множество натуральных чисел.

Уровень риска – математическое ожидание ущерба, вызываемого неблагоприятными событиями риска за период времени:

$$|\, Risk(\tau) \,| = \sum_{i=1}^{n} M[i(O_i)\, f(O_i, \tau)],$$

где *i(Oi)* – случайная величина ущерба, возникающего при единичном наступлении события *Oi*, *f* (*Oi,τ)* – случайная величина количества событий *Oi*, наступающих за период времени τ.

Тенденция развития управления информационным риском прослеживается в последнее время в негосударственном секторе России. В отечественной периодической печати появилась масса публикаций по рассматриваемой теме. Одновременно выходят монографии на данную тему, например [2–5]. При этом в зарубежной нормативной литературе и практике понятие риск применяется с давних времен, это объясняется тем, что категория «риск» присуща рыночной экономике. Следует отметить, что риск может использоваться как метрика информационной безопасности, что не характерно для применения термина «угроза».

В статье 2 Закона «О техническом регулировании» [1] вводятся новые понятия, главные и характерные для любого бизнеса. Например, «бе-зопасность – состояние, при котором отсутствует недопустимый риск, связанный с причинением вреда…» Применяя данные определения для термина «информационная безопасность», можно получить следующую, ориентированную на бизнес, дефиницию: «информационная безопасность – состояние информации при допустимом риске ее уничтожения, изменения или раскрытия, связанном с причинением вреда владельцу или пользователю информации» [7].

Достоинства нового определения

• Гармонизация положений новых стандартов (ГОСТ Р ИСО/МЭК 15408-1-2002, 27001, 17799) и прежнего научно-технического задела.

• Получение, через риск, количественных метрик информационной безопасности.

Данный тезис хорошо подкрепляется десятилетней практикой применения обобщенного критерия защищенности информации, используемого в методике французской банковской комиссии, построенной на базе количественного управления рисками [5].

Началом анализа рисков, связанных с эксплуатацией экономических автоматизированных

информационных систем (АИС), является оценка угроз (т.е. условий и факторов, которые могут стать причиной нарушения целостности системы, ее конфиденциальности, а также облегчить несанкционированный доступ к ней) и уязвимостей (слабых мест в защите, которые делают возможной реализацию угрозы), а также количественно обоснованное определение комплекса контрмер, обеспечивающего достаточный уровень защищенности АИС. При оценивании рисков учитываются многие факторы: ценность ресурсов, значимость угроз, уязвимостей, эффективность имеющихся и планируемых средств защиты и многое другое.

В настоящее время технологии управления информационными рисками в России развиты слабо. Основная причина такого положения состоит в том, что в российских государственных нормативных документах по информационной безопасности не рассматривается аспект рисков, их допустимый уровень и ответственность за принятие определенного уровня рисков. АИС, в зависимости от своего класса, должна обладать подсистемой безопасности с определенными формальными свойствами. Анализ рисков, как правило, выполняется формально, с использованием собственных методик неизвестного качества. В развитых зарубежных странах это не так. К примеру, в американском глоссарии по безопасности можно найти термин: Designated Approving Authority – лицо, уполномоченное принять решение о допустимости определенного уровня рисков. Вопросам анализа рисков уделяется серьезное внимание: десятилетиями собирается статистика нарушений, совершенствуются методики оценки рисков.

Однако и у нас в стране положение начинает меняться. Среди отечественных специалистов служб информационной безопасности коммерческих предприятий зреет понимание необходимости проведения такой работы. В первую очередь это относится к крупным коммерческим структурам [4; 5], то есть к тем, кто в первую очередь обязан серьезно заботиться о безопасности своих информационных ресурсов и экономически обоснованно определять затраты на обеспечение информационной безопасности (см. рис.1).

Каждая конкретная организация имеет свой спектр рисков и соответственно – возникающие задачи по их предотвращению или минимизации негативных последствий. В то же время, организации с позиций риск-менеджмента имеют и нечто общее – некий «каркас», вид риска, характеризуемый в трех измерениях: 1) ценность, находящаяся под угрозой; 2) источник, который может вызвать потерю этой ценности; 3) финансовые или иные последствия потери.

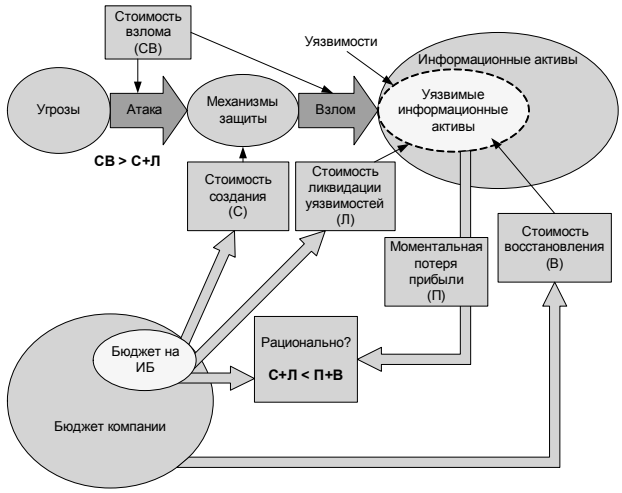

Рис. 1. Модель обоснования инвестиций в информационную безопасность

При выполнении полного анализа рисков приходится решать ряд сложных проблем. Процесс оценивания рисков содержит несколько этапов:

− идентификация ресурса и оценивание его количественных показателей или определение потенциального негативного воздействия на бизнес;

− оценивание угроз;

− оценивание уязвимостей;

− оценивание существующих и предполагаемых средств обеспечения информационной безопасности;

− оценивание рисков.

На основе оценивания рисков выбираются средства, обеспечивающие режим информационной безопасности. Информационные ресурсы, значимые для бизнеса и имеющие определенную стоимость и степень уязвимости, подвергаются риску, если по отношению к ним существует какая-либо угроза. При оценивании рисков учитываются возможное негативное воздействие от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей, а также угроз для них.

Ресурсы обычно подразделяются на несколько классов, например физические, программные и данные. Для каждого класса должна существовать своя методика оценки ценности элементов. Для оценки ценности ресурсов выбирается подходящая система критериев. Кроме критериев,

учитывающих финансовые потери, в организациях могут присутствовать критерии, отражающие:

− ущерб репутации организации;

− неприятности, связанные с нарушением действующего законодательства;

− ущерб для здоровья персонала;

− ущерб, связанный с разглашением персональных данных отдельных лиц;

− потери, связанные с невозможностью выполнения обязательств;

− ущерб от дезорганизации деятельности.

Могут использоваться и другие критерии в зависимости от профиля организации. К примеру, в правительственных учреждениях могут добавляться критерии, отражающие такие области, как национальная безопасность и международные отношения.

Кроме того, необходимо идентифицировать уязвимости – слабости в системе защиты, которые делают возможным реализацию угроз.

Для того чтобы конкретизировать вероятность реализации угрозы, рассматривается некоторый заданный отрезок времени, в течение которого предполагается защищать ресурс. Вероятность того, что угроза реализуется, определяется следующими факторами:

− привлекательностью ресурса (этот показатель учитывается при рассмотрении угрозы умышленного воздействия со стороны человека);

− возможностью использования ресурса для получения дохода (показатель учитывается при рассмотрении угрозы умышленного воздействия со стороны человека);

− простотой использования уязвимости при проведении атаки.

В настоящее время известно множество методов оценивания угроз и методик анализа рисков. Применение каких-либо инструментальных средств не является обязательным, однако позволяет уменьшить трудоемкость анализа рисков и выбора контрмер. Сейчас на рынке есть около двух десятков программных продуктов для анализа рисков: от простейших, ориентированных на базовый уровень безопасности, до сложных и дорогостоящих, позволяющих реализовать полный вариант анализа рисков и выбрать комплекс контрмер требуемой эффективности.

Примерами программных продуктов этого класса являются CRAMM (разработчик – компания Logica, Великобритания), MARION (разработчик CLUSIF, Франция), RiskWatch (США). Обязательным элементом этих продуктов является база данных, содержащая информацию по инцидентам в области информационной безопасности, позволяющая оценить риски и уязвимости, эффективность различных вариантов контрмер в определенной ситуации.

Один из возможных подходов к разработке подобных методик − накопление статистических данных о реальных происшествиях, анализ и классификация их причин, выявление факторов риска. На основе этой информации можно оценить угрозы и уязвимости в других отраслевых информационных системах. Практические сложности в реализации этого подхода следующие.

Во-первых, должен регулярно собираться весьма обширный материал о происшествиях в этой области.

Во-вторых, применение этого подхода оправданно далеко не всегда. Если информационная система достаточно крупная (содержит много элементов, расположена на обширной территории), имеет давнюю историю, то подобный подход, скорее всего, применим. Если система сравнительно невелика, использует только новейшие элементы технологии (для которых пока нет достаточной статистики), оценки рисков и уязвимостей могут оказаться недостоверными. Рассмотренная методология анализа рисков и управления ими полностью применима в российских условиях при соблюдении ряда условий. Особенно полезным представляется использование инструментальных средств типа метода CRAMM при проведении анализа рисков информационных систем с повышенными требованиями в области информационной безопасности. Это позволяет получать обоснованные оценки рисков, уязвимостей, эффективности защиты. Существенным достоинством таких методов является возможность проведения исследования в сжатые сроки с документированием результатов.

Итак, следует отметить, что для проведения высококачественного анализа и оценки рисков обязательна разработка собственных методик (с использованием существующих рекомендаций и методик), которые учитывают отраслевую специфику. Как правило, подобные методики закрыты и составляют ноу-хау компании, предоставляющей свои услуги в области информационной безопасности.

Большим сдерживающим фактором при проведении количественной оценки рисков являются трудности получения исходных величин вероятности событий безопасности и стоимости информационных ресурсов, которые являются раз-

нородными факторами (см. рис. 2), обеспечивающими требуемый уровень информационной безопасности [6].

Рис. 2. Система факторов, обеспечивающих требуемый уровень информационной безопасности

Указанные трудности объясняются отсутствием в нашей стране общепринятых отработанных методик определения исходных данныхдля количественной оценки рисков информационной безопасности. Первые шаги в направлении решения этой проблемы, как отмечалось, сделаны ЦБ РФ, который выпустил серию отраслевых стандартов информационной безопасности. Однако данные стандарты в своем большинстве носят характер концептуальных документов, в которых отсутствует конкретное решение базовой проблемы получения исходных величин вероятности событий безопасности и стоимости информационных ресурсов.

Выводы

1. Необходимо использовать дифференцированный подход в учебном процессе информационной безопасности, в зависимости от формы собственности АИС и обрабатываемой информации.

2. Получение количественных метрик информационной безопасности, например через риск, – актуальная задача бизнеса, которую следует учитывать в учебных программах.

3. Наступило время создания отечественных учебных курсов, учитывающих специфику обеспечения информационной безопасности коммерческих АИС с учетом информационных рисков.

Литература:

1. Закон Российской Федерации от 27.12.2002 № 184-ФЗ «О техническом регулировании».

2. Петренко, С.А., Симонов, С.В. Управление информационными рисками : экономически оправданная безопасность. – М. : Компания АйТи; ДМК Пресс, 2004.

3. Симонов, С. Технологии и инструментарий для управления рисками // Jet Info. – 2003. – № 2.

4. Оценка стоимости нематериальных активов и интеллектуальной собственности / А.Н. Козырев, В.Л. Макаров. – М. : Интерреклама, 2003.

5. Астахов, А.М. Исскуство управления информационными рисками. – М. : ДМК Пресс, 2010.

6. Цуканова, О.А., Смирнов, С.Б. Экономика защиты информации : учебное пособие. – СПб. : СПб ГУИТМО, 2007.

7. Скородумов, Б.И. О понятийно-терминологическом аппарате информационной безопасности // Безопасность информационных технологий. – 2008. – № 4. – С. 12–17.