УДК 004.239.056

А.А. Пономарев

ОЦЕНКА И УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННЫХ СИСТЕМ

Обобщается опыт анализа рисков для информационных систем, излагаются существующие методики и приводятся новые методы анализа рисков для организаций.

Ключевые слова: анализ рисков, система защиты информации, преднамеренные и непреднамеренные угрозы, качественная оценка рисков, количественная оценка рисков, стоимость информационного ресурса, стратегия управления рисками.

Методология анализа рисков. На практике сложились два подхода к организации систем защиты информации (СЗИ) на предприятиях. Первый подход характерен для организаций, ведущих обработку государственной тайны, и заключается в выполнении нормативных требований с привлечением специального оборудования и специальных организаций. Другой подход относится к коммерческим организациям, обрабатывающим коммерческую и профессиональную (например, банковскую) тайны, и заключается в анализе рисков, в частности, в анализе существующей системы защиты информации.

При построении системы защиты информации и при совершенствовании существующей СЗИ сегодня рекомендуется применение методологии анализа рисков, что предполагает количественный или качественный анализ рисков.

Основой методологии анализа рисков на сегодняшний день является американский стандарт NIST [1], где приводится общая методология анализа рисков для организаций. В настоящее время существуют коммерческие программные продукты, которые оценивают риски для организаций и выдают некоторые рекомендации по усовершенствованию существующих систем. Обычно такие программные продукты строятся на основе вопросных листов, после ответа на вопросы программа решает, какие меры следует предпринять. Можно выделить три программных продукта: CRAMM, RiskWatch, ГРИФ. Но не следует думать, что данные программные продукты рассчитаны для неподготовленных людей, они ориентированы на пользователей, обладающих специальной подготовкой и высокой квалификацией. Так, входными данными программного продукта CRAMM должна стать следующая информация: ресурсы системы (оценка их стоимости), угрозы (идентифицируются и оцениваются) и уязвимости[2]. Оценка производится согласно выбранной шкале. Далее программа предлагает варианты мер противодействия выявленным рискам.

Методики анализа рисков. Можно выделить три сформировавшихся направления анализа рисков[3;5]:

- качественная оценка рисков;
- количественная оценка рисков;
- Именные методики (модель обобщенного стоимостного результата Миоры (англ. Miora Generalized Cost Consequence Model)) и коммерческие

программные продукты, в которых может быть реализована как количественная и качественная оценка рисков, так и оба подхода сразу.

Модель качественной оценки. Качественная оценка обычно сводится к введению некоторых качественных шкал оценки показателей для оценки важности информации (например, важная, критичная, жизненная) и оценки риска атаки (низкий, средний, высокий). Далее выбираются ресурсы с наибольшими показателями риска, они и подвергаются дополнительной защите. Ннапример, защищаются ресурсы с показателями важности информации (жизненная) и риском атаки (высоким).

Достоинства качественной оценки рисков:

• ускоряется и упрощается анализ рисков;

• нет необходимости оценивать в денежных единицах стоимость ресурса;

• нет необходимости вычислять вероятности проявления угрозы;

• нет необходимости вычислять соответствие применяемых мер угрозам.

Модель количественной оценки рисков. Количественная модель рисков оперирует такими понятиями, как[4]:

• годовая частота происшествия (англ. Annualized Rate of Occurrence – ARO);

• ожидаемый единичный ущерб (англ. Single Loss Expectancy – SLE);

• ожидаемый годовой ущерб (англ. Annualized Loss Expectancy – ALE), величина, равная произведению ARO на SLE.

ALE=ARO× SLE (1), где

ARO – частота появления события, приносящего ущерб в год. Данный показатель также можно назвать интенсивностью события.

SLE – показатель, который рассчитывается как произведение стоимости информации (Asset Value – AV) на фактор воздействия (англ.Exposure Factor – EF). Фактор воздействия – это размер ущерба или влияния на значение актива (от 0 до 1), то есть часть значения, которую актив потеряет в результате события.

SLE=AV× EF. (2)

Управление рисками считается эффективным, если расходы на безопасность в год не превышают ожидаемый годовой ущерб.

Пример. Имеется предприятие с внутренней инфраструктурой общей стоимостью 200 000 дол. Пожар может нанести ущерб с фактором воздействия 0,3. Пожар может случиться раз в 10 лет. Тогда:

SLE= 200000× 0,3=60000,

ALE= 60000× 0,1=6000.

Таким образом, если предприятие тратит до 6000 дол. в год, то управление рисками осуществляется верно.

Модель обобщенного стоимостного результата Миоры. Модель Миоры разработана как альтернатива количественной модели рисков для улучшения и облегчения расчетов и вычислений. Одним из основных недостатков которой является ее вероятностная составляющая.

Модель Миоры не учитывает вероятностей происшествия, она оперирует понятием ущерба от простоя как функцией времени после наступления события.

Для каждого информационного актива или группы сходных по ряду признаков активов, называемых категорией, определяется размер возможного ущерба, срок начала его влияния на организацию и распределённость по времени.

Развитие картины ущерба можно представить в виде графика, где категории – это функции по двум осям: «время в днях»; «ущерб в деньгах». В результирующем графике представляются две кривые: суммарный ущерб организации при отсутствии защитных мероприятий; суммарный ущерб при наличии защитных мероприятий.

На таком графике наглядно видны необходимость и эффективность применяемых мер для обеспечения защиты информации.

Отечественный опыт оценки рисков. После того как в коммерческой фирме выявлены все носители конфиденциальной информации (КИ), по каждому (группам однотипных) носителю должен быть произведен анализ рисков в целях выявления слабых мест существующей СЗИ и более правильного распределения выделенных на защиту материальных средств.

В работе [2] приводятся двухфакторный и трехфакторный анализы рисков, которые производятся по следующим формулам:

$$R = P_{происшествия} C_{потери}, \quad (3)$$

$$R = P_{угрозы} P_{уязвимости} C_{потери}, \quad (4)$$

где R -риск, $P_{происшествия}$ – вероятность происшествия, $P_{угрозы}$ – вероятность возникновения угрозы, $P_{уязвимости}$ – вероятность потери информации (потеря трактуется широко: уничтожение, разглашение, уничтожение, модификации), $C_{потери}$ – стоимость информации (цена потери). Данная методика является шагом назад по сравнению с приведенной выше методикой количественной оценки рисков, так как последняя позволяет рекомендовать, сколько средств нужно тратить на защиту информации. А методология, указанная в работе [2], лишь позволяет ранжировать риски.

При этом в обоих случаях количественная оценка рисков осложняется тем, что не приводится никаких методик по вычислениям вероятностей (или частоты появления события) и цены информации. Но не понятно, чем должны руководствоваться привлекаемые эксперты, поэтому методика нуждается в объяснении, желательно близком к математическому, каждого показателя вероятности и стоимости информации.

Отдельно рассмотрим формулу (4), в которой автор разложил $P_{происшествия}$ на $P_{угрозы}$ и $P_{уязвимости}$. Однако вероятности возникновения преднамеренных угроз в формуле (4) будут зависеть от вероятности уязвимости, поэтому данную формулу не всегда следует применять. $P_{угрозы}$ будет зависеть от $P_{уязвимости}$, поэтому следует более подробно подойти к анализу рисков, исходя из характера возникающих угроз. Таким образом, можно будет избежать ошибок, которые будут происходить по причине того, что вероятность происшествия и вероятность уязвимости будут не независимыми событиями. Например, одна организация применяет эффективную систему кон-

троля персонала, периодически проверяет наличие носителей конфиденциальных документов, в другой организации такого контроля не ведется. Однако, исходя из формулы (4), вероятность возникновения угрозы выноса материальных носителей, хранящих конфиденциальную информацию, будет одинаковой. Это неправильно, так как злоумышленник всегда оценивает свои силы и возможности перед совершением преступления, поэтому оценивать вероятность угрозы можно только для угроз, не зависящих от человека.

Предлагаемая методика оценки рисков. Для оценки вероятности возникновения угрозы сначала приведем удобную для дальнейшего рассмотрения классификацию угроз информации. Поскольку конечной целью оценки является (в идеальном случае) определение вероятности возникновения угрозы, выделим следующие источники угроз: естественные – это стихийные бедствия, аварии, сбои и отказы технических средств, другие события, вызванные объективными физическими явлениями, неподконтрольными человеку; искусственные – угрозы, вызванные деятельностью человека. Эти угрозы разделяются на непреднамеренные (неумышленные, случайные), вызванные ошибками в проектировании систем и элементов, ошибки в программном обеспечении, ошибки в действиях персонала и т.п., и преднамеренные (умышленные), связанные с сознательным причинением вреда.

При этом естественные и непреднамеренные искусственные угрозы будем считать случайными. Оценить вероятность возникновения (и частоты появления) случайных угроз возможно при накоплении достаточной статистики их возникновения. Случайные угрозы можно оценить, например, с помощью простого потока событий (Пуассона). На этом этапе можно полностью отбросить угрозы, вероятность возникновения которых пренебрежимо мала (падение метеорита), и воспользоваться приведенной выше методикой количественной оценки рисков.

Отдельно рассмотрим вопрос выхода из строя оборудования. Данный вопрос хорошо разработан в теории надежности, которая для анализа в данной области пользуется математическим аппаратом теории массового обслуживания.

Также отметим, что большинство случайно возникающих угроз это угрозы целостности и доступности информации.

Основные непреднамеренные угрозы:

•неумышленная порча оборудования, удаление и модификация файлов с важной информацией, порча носителей с информацией, другие действия, приводящие к отказу информационной системы;

•внесение изменений в настройки системы (без намерений ее испортить);

•отключение оборудования;

•установка и использование программ, не предусмотренных технологической необходимостью;

•некорректные действия с технологическими программами, способными повлиять на нормальное функционирование информационной системы»;

•заражение вирусами компонентов информационной системы;

•действия, приводящие к разглашению конфиденциальной информации;

•утрата, разглашение, предоставление в пользование неавторизованным субъектам паролей, ключей шифрования, средств идентификации; то есть действия, нарушающие разграничение доступа к ресурсам;

•пересылка данных на ошибочный адрес;
•игнорирование организационных ограничений;
•проектирование систем, разработка программ, технологий влияющих на работоспособность информационной системы и средства безопасности;
•ошибки при вводе данных;
•нарушение работы каналов связи;
•отключение средств обеспечения безопасности.

Анализ рисков для систем обработки информации на основе анализа рисков злоумышленника. Вероятность возникновения угрозы ($P_{угрозы}$) также тяжело оценивать в случае, когда идет речь о преднамеренных действиях людей (например, несанкционированный доступ), потому что действия будут зависеть от существующей СЗИ на предприятии. А давать оценку возникновения преднамеренной угрозы, не учитывая систему защиты информации, является неверным, так как злоумышленник будет оценивать свои силы, и если в плохо защищенной организации он попытается произвести действия, приводящие к потере информации, то в хорошо защищенной организации, осуществляющей пристальный контроль за действиями сотрудников фирмы, – не решится.

В большинстве случаев, если речь идет о преднамеренных действиях людей, имеет место их материальная заинтересованность. В этом случае проще перейти на позиции злоумышленника и оценивать риски с его позиции. Тогда заменим вероятность угрозы $P_{угрозы}$ на риск злоумышленника $R_{зл}$. В этом случае $R_{зл}$ можно записать следующим образом:

$$R_{зл} = \frac{C_{доход}}{C_{орг}} \mathrm{P}_{необн} \mathrm{P}_{получ} , \qquad (5)$$

где $C_{орг}$ – стоимость организации канала получения информации, $C_{доход}$ – доход, получаемый от добытой информации (не всегда равен стоимости информации для владельца), $\mathrm{P}_{необн}$ – вероятность необнаружения действий злоумышленника (зависит от частоты проверок действий собственных сотрудников, ошибок первого рода охранной сигнализации и др.), $\mathrm{P}_{получ}$ – вероятность получения информации (или какой то выгоды). При данном подходе можно объяснить действия злоумышленника, однако нельзя предсказать, сколько денег следует потратить на предотвращение (уменьшение) риска атаки, исходя из того, что злоумышленник будет осуществлять свои действия (атаки, НСД) на наименее защищенные объекты, которые и следует защищать.

Методика оценки рисков для преднамеренных угроз. Анализ рисков предлагается осуществлять по схеме, показанной на рис. 1.

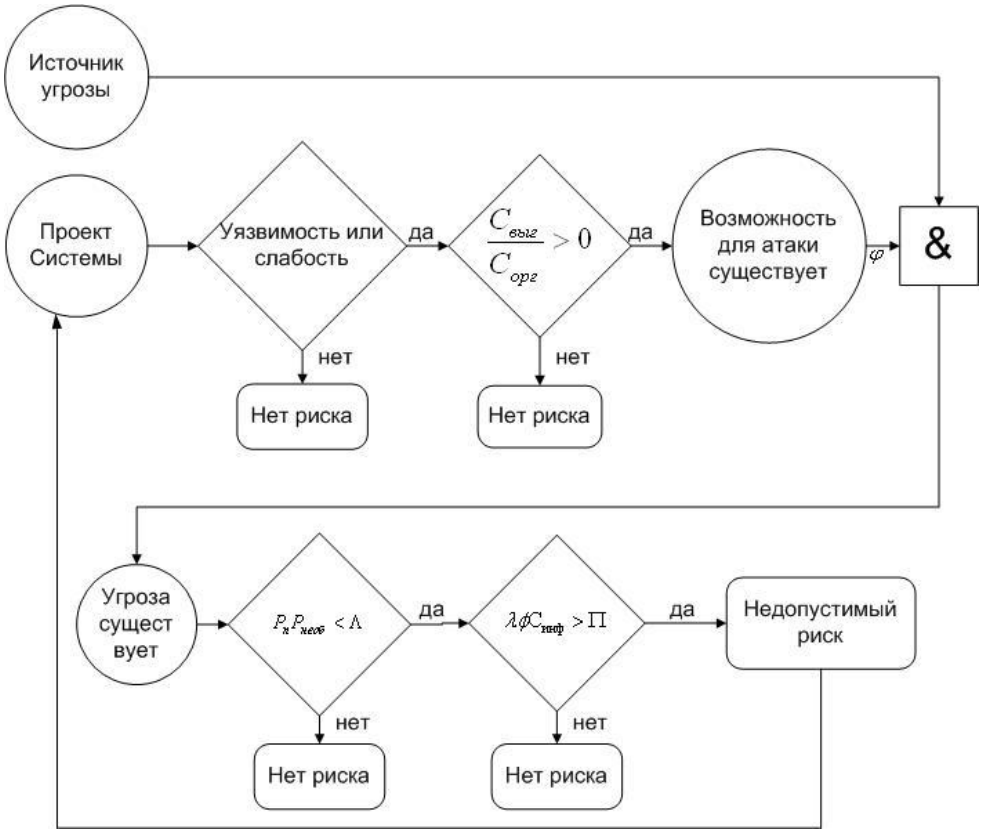

Рис. 1. Анализ рисков для преднамеренных угроз

На рис. 1 анализ рисков рассматривается для проекта системы защиты информации, та же методика применима и к существующей в организации системе защиты информации. В проекте (существующей системе) могут быть уязвимости и слабости реализации, которые должны быть найдены. Далее следует рассмотреть вопрос о том, могут ли найденные уязвимости эксплуатироваться злоумышленником, считается, что злоумышленник действует экономически целесообразно, а значит, отношение стоимости получаемой им выгоды к стоимости организации атаки будет больше единицы $\frac{C_{выг}}{C_{орг}} > 1$. Далее также следует рассмотреть, имеется ли у данной организации источник рассматриваемой угрозы. Если источник угрозы существует, то угроза существует и проявится, если произведение вероятности получения информации P_n и вероятности необнаружения действий злоумышленника $P_{необ}$ меньше какого-то порогового значения (страх злоумышленника перед наказанием) Λ: $P_n P_{необ} < \Lambda$. Далее, собственник информационных ресурсов применяет меры, если ежегодные потери больше порогового значения: $l f C_{инф} > \Pi$, где l – интенсивность происшествия в год, f – фактор утра-

ты, $С_{инф}$ – цена информационного ресурса (или процесса), $П$ – пороговое значение. Данное пороговое значение рассматривается применительно к конкретной угрозе, так как уменьшить некоторые угрозы – очень дорогое мероприятие, и собственнику следует перераспределить средства на защиту от других угроз. Исходить следует из того, что защита информации не должна быть дороже ежегодных потерь. Приведенная выше методика должна быть применена в отношении всех угроз безопасности информации, целью является минимизация общего риска для информационных ресурсов организации.

Основные преднамеренные угрозы:

•физическое разрушение информационной системы (взрыв, поджог, кража, порча носителей, вывод из строя персонала и др.);
•вывод из строя вспомогательных систем обеспечения нормальной работы информационной системы (вентиляции, кондиционирования, электропитания, линии связи и др.);
•нарушение организации работы системы (организация саботажа персоналом, внесение изменений в настройки, создание помех);
•внедрение своих подставных лиц в различные структуры предприятия, в т.ч. структуру безопасности и управления;
•подкуп или шантаж штатного персонала;
•применение средств несанкционированного слежения и съема информации;
•перехват данных в стандартных линиях связи;
•хищение носителей информации;
•неразрешенное копирование информации;
•незаконное получение паролей, других средств идентификации. Использование этих средств для маскировки под зарегистрированного пользователя;
•несанкционированная дешифровка данных;
•несанкционированная модификация передаваемых данных;
•ввод неверных данных в систему, навязывание пользователям ложных сообщений и прочей информации.

Оценка стоимости информационных ресурсов. Любая количественная оценка рисков требует оценки стоимости информационного ресурса (процесса). Для оценки стоимости информации следует воспользоваться теорией оценки, которая разработана достаточно хорошо. Различают следующие подходы к оценке: сравнительный (рыночный), затратный и доходный. Выбор конкретного подхода обосновывается в зависимости от той информации, которую следует оценить. Каждый подход позволяет подчеркнуть определенные характеристики информации. Так, при оценке с позиции доходного подхода во главу угла ставится доход как основной фактор, определяющий величину стоимости информации. Чем больше доход, приносимый информацией, тем больше его рыночная стоимость при прочих равных условиях. При этом имеют значение продолжительности периода получения возможного дохода, степень и вид рисков, сопровождающих данный процесс. Доходный подход – это определение текущей стоимости будущих доходов, которые возникнут в результате использования собственности будущих доходов, которые возникнут в результате использования информации и возможной дальнейшей её продажи.

Сравнительный подход эффективен в случае существования активного рынка сопоставимых информационных ресурсов. Точность оценки зависит от качества собранных данных, применяя этот подход, оценщик должен собрать достоверную информацию о недавних продажах сопоставимых объектов. Действенность такого подхода снижается, если сделок было мало и моменты их совершения и оценки разделяет продолжительный период, если рынок находится в аномальном состоянии, так как быстрые изменения на рынке приводят к искажению показателей. Сравнительный подход основан на применении принципа замещения. Для сравнения выбираются конкурирующие с оцениваемой информацией информационные ресурсы (продукты). Сравнительный подход основан на принципе замещения. Для сравнения выбираются конкурирующие с оцениваемой информацией информационные ресурсы других предприятий. Обычно существуют различия, поэтому следует провести корректировку данных. В основу приведения поправок положен принцип вклада.

Затратный подход применительно к оценке информации будем рассматривать как все затраты, которые понёс собственник информации на её получение. По сути, этот подход является самым простым для собственника информации, так как ему известны все составляющие затрат. Однако он может быть не объективным для работы с некоторой информацией, так как один человек может сделать больше десяти, которые получают ту же зарплату.

В целом все три подхода взаимосвязаны. Каждый из них предполагает использование различных видов информации. В общем случае самым действенным является затратный подход, поскольку он является самым простым с позиций собственника информации. Рассмотрим данный подход более подробно, используя работу [4].

При использовании затратного подхода при оценке нематериальных активов используются метод стоимости создания и метод выигрыша в себестоимости.

Метод стоимости создания

1. Определяется полная стоимость замещения или полная стоимость восстановления нематериального актива. Выявляются все фактические затраты, связанные с созданием, приобретением и введением его в действие. При приобретении и использовании нематериального актива необходимо учитывать следующие виды затрат:

• на приобретение имущественных прав;

• на освоение в производстве товаров с использованием нематериального актива;

• на маркетинг (исследование, анализ и отбор информации для определения аналогов предполагаемых объектов промышленной собственности).

При создании нематериального актива на самом предприятии необходимо учитывать следующие затраты:

• на поисковые работы и разработку темы;

• на создание экспериментальных образцов;

• на услуги сторонних организаций (например, на выявление ОИС, на выдачу охранных документов);

• на уплату патентных пошлин (поддержание патента в силе);

• на создание конструкторско-технической, технологической, проектной документации;

• на составление и утверждение отчета.

$$З_с = \sum \left[(З_{\text{рі}} + З_{\text{поі}}) \cdot \left(1 + \frac{\text{Р}}{100}\right) \cdot К_д \right], \quad (6)$$

где $З_с$ – сумма всех затрат, связанных с созданием и охраной нематериальных актива, ден. ед.;

$З_р$ – стоимость разработки нематериального актива, ден. ед.;

$З_{по}$ – затраты на правовую охрану объекта, ден. ед.;

$Р$ – рентабельность, %;

$К_д$ – коэффициент дисконтирования, с помощью которого разновременные затраты приводятся к единому моменту времени;

і – порядковый номер рассматриваемого года действия.

$$З_р = (З_{нир} + З_{ктд}), \quad (7)$$

где $З_{нир}$ – затраты на проведение НИР, ден. ед.;

$З_{ктд}$ – затраты на разработку конструкторско-технической, технологической и/или проектной документации, связанные с созданием объекта, ден. ед.

$$З_{нир} = З_п + З_{ти} + З_э + З_и + З_о + З_{др}, \quad (8)$$

где $З_п$ – затраты на поисковые работы, ден. ед.;

$З_{ти}$ – затраты на проведение теоретических исследований, ден. ед.;

$З_э$ – затраты на проведение экспериментов, ден. ед.;

$З_о$ – затраты на составление, рассмотрение и утверждение отчета, ден. ед.;

$З_и$ – затраты на проведение испытаний, ден. ед.;

$З_{др}$ – другие затраты, ден. ед.

$$З_{ктд} = З_{эп} + З_{тп} + З_{рп} + З_р + З_и + З_{ан} + З_д, \quad (9)$$

где $З_{эп}$ – затраты на выполнение эскизного проекта, ден. ед.;

$З_{тп}$ – затраты на выполнение технического проекта, ден. ед.;

$З_{рп}$ – затраты на выполнение рабочего проекта, ден. ед.;

$З_р$ – затраты на выполнение расчетов, ден. ед.;

$З_и$ – затраты на проведение испытаний, ден. ед.;

$З_{ан}$ – затраты на проведение авторского надзора, ден. ед.;

$З_д$ – затраты на дизайн, ден. ед.

2. Определяется величина коэффициента, учитывающего степень морального старения нематериального актива.

$$К_{мс} = 1 - \frac{Т_д}{Т_н}, \quad (10)$$

где $T_н$ – номинальный срок действия охранного документа;

$T_д$ – срок действия охранного документа по состоянию на расчетный год.

3. Рассчитывается остаточная стоимость нематериального актива с учетом коэффициента технико-экономической значимости, коэффициента морального старения.

$$C_о = З_с K_{мс} K_т K_и, \qquad (11)$$

где $C_о$ – стоимость объекта (нематериального актива)

$З_с$ – сумма всех затрат;

$K_{мс}$ – коэффициент морального старения;

$K_т$ – коэффициент технико-экономической значимости (определяется только для изобретений и полезных моделей);

$K_и$ – коэффициент, отражающий процессы в i-м году, учитывается на основании динамики цен.

Коэффициент технико-экономической значимости $K_т$ устанавливается по следующей шкале, предложенной специалистами Инженерной академии РФ:

1,0 – изобретения, относящиеся к одной простой детали, изменению одного параметра простого процесса, одной операции процесса, одного ингредиента рецептуры;

1,5 – изобретения, относящиеся к конструкции сложной детали неосновного узла, изменению нескольких параметров несложных операций, изменению нескольких неосновных ингредиентов в рецептуре;

2,0 – изобретения, относящиеся к одному основному или нескольким неосновным узлам, части неосновных процессов, части неосновной рецептуры;

2,5 – изобретения, относящиеся к конструкциям машин, приборов, станков, аппаратов, технологическим процессам, рецептурам;

3,0 – изобретения, относящиеся к конструкциям со сложной системой контроля, сложным комплексным технологическим процессам, рецептуре особой сложности;

4,0 – изобретения, относящиеся к конструкциям, техническим процессам, рецептуре особой сложности и главным образом к новым разделам науки и техники;

5,0 – изобретения, не имеющие прототипа, - пионерские изобретения.

Метод выигрыша в себестоимости. При оценке стоимости нематериального актива иногда используется такой метод затратного подхода, как метод выигрыша в себестоимости. Он содержит элементы как затратного, так и сравнительного подхода. Стоимость нематериального актива измеряется через определение экономии на затратах в результате его использования. Например, при применении ноу-хау.

Как можно заметить, теория оценки нематериальных активов различается с представлениями теории защиты информации, где обычно предлагается оценивать ущерб, наступающий после потери информации. Предлагается использовать некоторые из следующих критериев:

• ущерб репутации организации;
• нарушение действующего законодательства;
• ущерб для здоровья персонала;
• ущерб, связанный с разглашением персональных данных отдельных лиц;
• финансовые потери от разглашения информации;
• финансовые потери, связанные с восстановлением ресурсов;
• потери, связанные с невозможностью выполнения обязательств;
• дезорганизация деятельности.

Однако в пользу подхода, который используется для оценки нематериальных активов, говорит его большая практичность и разработанность. Не следует забывать, что объектами угроз могут являться:
•собственно информация;
•носители информации (компоненты и системы обработки и хранения);
•процессы обработки информации.

Приведенные выше подходы могут быть использованы к оценке любых объектов угроз. Методики же приводились именно для оценки стоимости информации.

Управление рисками. Этап управления рисками следует после того, как оценены частные риски, то есть риски по каждой угрозе. Управление должно заключаться в применении некоторой стратегии управления рисками в целях минимизации общего риска.

Минимизация общего риска. Общий риск для информационных ресурсов предприятия складывается из всех существующих угроз безопасности информации Управление общим риском должно заключать в себе меры, направленные на его снижение.

$$\mathrm{R}_{\mathrm{o}} = \sum_{1}^{\mathrm{n}} R_1, R_2, ..., R_n \rightarrow \min ,$$

где R_{o} – общий риск, $\sum_{1}^{\mathrm{n}} R_1, R_2, ..., R_n$ –сумма всех частных рисков (рисков по каждой угрозе). Иногда следует пренебречь некоторым частным риском, чтобы снизить другие частные риски.

Стратегии управления рисками. Управление рисками предполагает принятие мер, направленных на снижение частоты реализации угроз и снижение ущерба от них. В зависимости от полученных показателей рисков собственник информационных ресурсов должен выбрать стратегию управления рисками. Существуют следующие стратегии управления рисками: 1) принятие риска – собственник информационных ресурсов считает, что риск мал и не предпринимает никаких мер; 2) снижение (уменьшение) риска – собственник информации осуществляет меры по снижению показателя риска для информационных ресурсов; 3) Исключение риска – собственник информационного ресурса предпринимает меры, которые позволяют полностью исключить частный риск; 4) передача риска третьим лицам – меры, предпринимаемые

собственником в целях возмещения возможных последствий наступления риска (страхование).

Заключение. Оценка и управление рисками являются в настоящее время самой бурно развивающейся методологией, так как помогают организациям оптимизировать выделяемые на защиту информации материальные ресурсы и защитить объекты, которые находятся под самым большим риском. При этом объяснено, почему риски для естественных и искусственных угроз не могут рассматриваться вместе, оцениваться по одним и тем же формулам. Для искусственных угроз предложены две методики оценки рисков. Первая заключается в том, что, оценивая риски, мы встаём на позиции злоумышленника и оцениваем риски злоумышленника. Исходя из этих рисков, можно ранжировать риски для защищаемой организации. Вторая методика заключается в том, чтобы количественно оценить риски с системой ограничений, отражающей адекватность угроз для выбранной организации. Подробно рассмотрен вопрос об оценке стоимости информационных ресурсов, приведено несколько методик по оценке информационных ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. NIST Special Publication 800-30 Rev A. Risk management Guide for information Technology Systems, Gary Stoneburner, Alice Goguen, and Alexis Feringa.
2. Вопросы защиты информации / Научн.-практ. журн., 2003. №1. С. 25-33.
3. Методы и средства анализа рисков и управление ими в ИС //BYTE (Россия). 2005. №12. http://www.bytemag.ru/?ID=605155
4. Оценка бизнеса: Учебник / Под ред. А.Г. Грязновой, М.А. Федотовой, М.: Финансы и статистика, 2001.
5. Конев И.Р., Беляев А.В. Информационная безопасность предприятия. СПб.: БХВ-Петербург, 2003.

Поступила в редакцию 25.04.07

A.A. Ponomarev
Management of risks for systems of processing of the information

This article is about existing experience of risk management for information system. Also are stated new methods of risks analysis for information systems.

Пономарев А.А.
ГОУ ВПО «Удмуртский государственный университет»
426034, Россия, г. Ижевск,
ул. Университетская 1, (корп. 4)
Тел. 8-904-8325016