Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 2 (117)/2003

Технологии и инструментарий для управления рисками

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Технологии и инструментарий для управления рисками

Сергей Симонов

СОДЕРЖАНИЕ

Введение

На этапе анализа рисков определяется возможность понести убытки из-за нарушения режима информационной безопасности организации, детализируются характеристики (или составляющие) рисков для информационных ресурсов и технологий. Результаты анализа используются при выборе средств защиты, оценке эффективности существующих и проектируемых подсистем информационной безопасности.

Под управлением рисками понимается процесс идентификации и уменьшения рисков, которые могут воздействовать на информационную систему.

Концепции анализа рисков, управления рисками на всех стадиях жизненного цикла информационной технологии были предложены многими крупными организациями, занимающимися проблемами информационной безопасности. Отечественные аналитики начали использовать различные методики на практике. Несколькими российскими организациями были разработаны собственные методики анализа и управления рисками, разработано собственное ПО, которое, наряду с зарубежным, имеется на отечественном рынке.

Таким образом, различные технологии анализа рисков начали реально применяться в России. Появилась возможность обобщить этот опыт, более четко очертить границы применимости различных методов в отечественных условиях.

В статье рассматривается следующий круг вопросов:

- Различные определения и постановки задач анализа рисков.
- Современные концепции управления рисками.
- Реализация методик в соответствии с этими концепциями.
- Обзор специализированного ПО анализа и управления рисков.

1. Анализ рисков: различные определения и постановки задач

Комплекс вопросов, связанных с анализом рисков, был рассмотрен в [1.2.3]. Там же приведен один из вариантов определений основных понятий (риск, угроза, уязвимость). В многочисленных публикациях на эту тему предлагаются и другие постановки задач и определения основных понятий, некоторые из них приводятся в приложении.

Постановка задачи обеспечения информационной безопасности может варьироваться в широких пределах. Соответственно варьируются и постановки задач анализа рисков.

Основным фактором, определяющим отношение организации к вопросам информационной безопасности, является степень ее зрелости.

В соответствии с одной из моделей организации с позиции их зрелости, предлагаемой Carnegie Mellon University [4], выделяется 5 уровней зрелости, которым, как правило, соответствует различное понимание проблем информационной безопасности организации. (Схема 1).

Проблема обеспечения режима информационной безопасности будет ставиться (хотя бы в неявном виде) и решаться для организаций, находящихся на разных уровнях развития, по-разному.

На первом уровне она, как правило, руководством формально не ставится. Но это не значит, что она не решается сотрудниками по собственной инициативе, и возможно эффективно.
В качестве положительного примера можно привести один случай, имевший место в действительности. Сравнительно небольшая организация (порядка 80 компьютеров, 3 файл-сервера), занимающаяся рекламным бизнесом, в результате пожара в арендуемом ей здании, потеряла всю вычислительную технику и данные.
Однако уже через неделю она полностью смогла восстановить свою работу. Некоторые сотрудники по своей инициативе делали копии наиболее важной информации на CD, что-то хранилось на домашних компьютерах сотрудников, что-то отправлялось по электронной почте различным адресатам и было затребовано обратно.
В результате большая часть наиболее ценных информационных ресурсов была быстро восстановлена (а техника быстро закуплена), что позволило фирме успешно продолжить работу.
При этом вопросы информационной безопасности руководством никогда не ставились и по-видимому ставиться не будут.

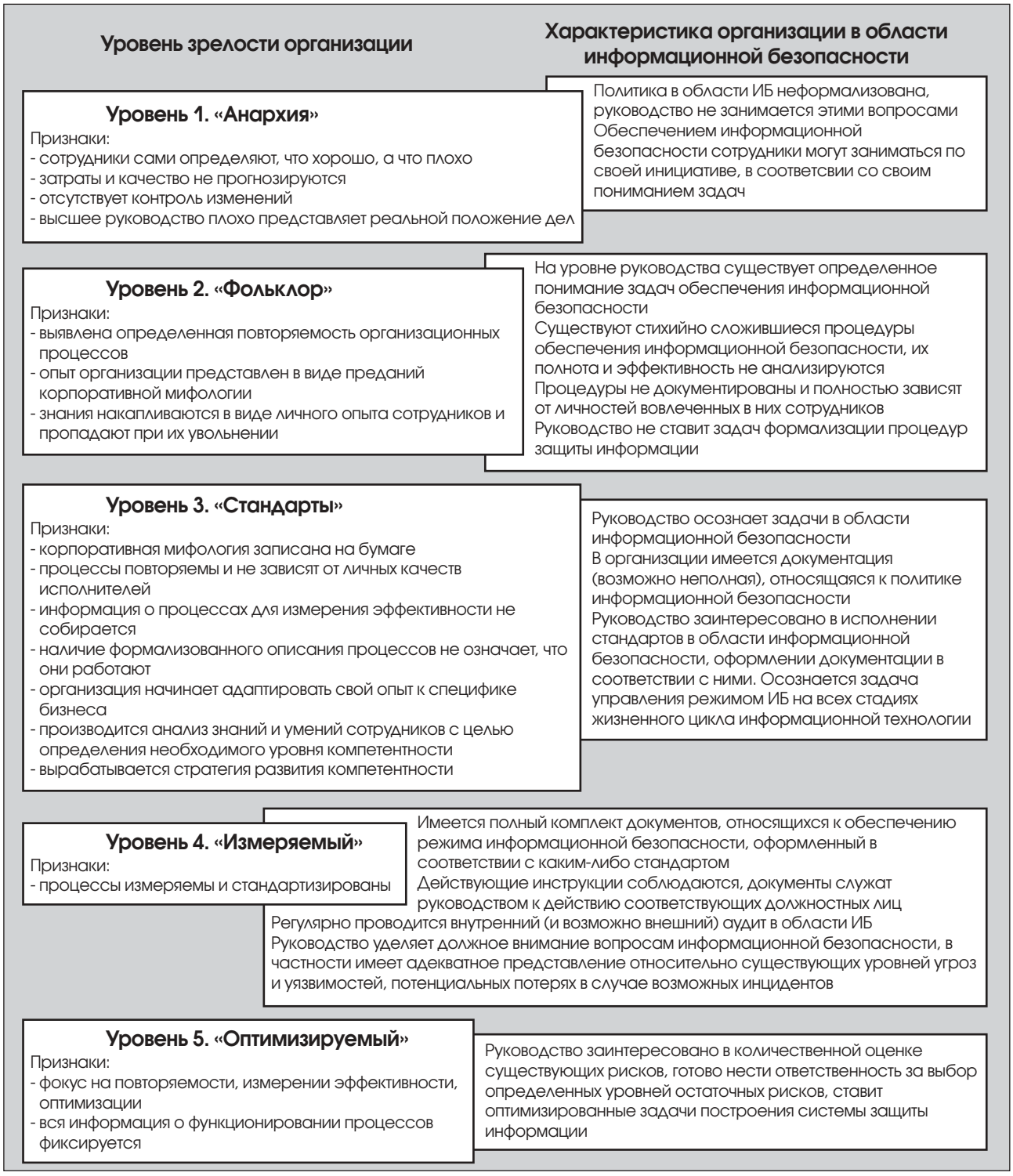

Схема 1. Соответствие уровня зрелости организации и ее потребностей в области информационной безопасности.

Наряду со случаями, когда все окончилось благополучно, можно привести и много иных примеров, когда пренебрежение вопросами информационной безопасности имело чрезвычайно серьезные последствия.

Тем не менее, с точки зрения руководства организации, находящейся на первом уровне зрелости, задачи обеспечения режима информационной безопасности, как правило, неактуальны. Несмотря на это, организации могут быть вполне жизнеспособными.

На втором уровне проблема обеспечения информационной безопасности решается неформально, на основе постепенно сложившейся практики. Комплекс мер (организационных и программно-технических) позволяет защититься от наиболее вероятных угроз, как потенциально возможных, так и имевших место ранее. Вопрос относительно

эффективности защиты не ставится. Таким образом, постепенно складывается неформальный список актуальных для организации классов рисков, который постепенно пополняется.

Если серьезных инцидентов не происходило, руководство организации, как правило, считает вопросы информационной безопасности не приоритетными.

В случае серьезного инцидента сложившаяся система обеспечения безопасности корректируется, а проблема поиска других возможных брешей в защите может быть осознана руководством.

Один из вариантов определения риска в этом случае: ситуация, когда известны уязвимости, потенциальные нарушители и их мотивация (модель нарушителя), сценарии развития событий, связанные с выявленными уязвимостями [IATF].

Для данного уровня зрелости организации типичными являются локальные (не связанные с другими этапами жизненного цикла технологии) постановки задачи анализа рисков, когда считается достаточным перечислить актуальные для данной информационной системы классы рисков и возможно описать модель нарушителя, а задача анализа вариантов контрмер, их эффективность, управление рисками, как правило, не считается актуальной.

На третьем уровне в организации считается целесообразным следовать в той или иной мере (возможно частично) стандартам и рекомендациям, обеспечивающим базовый уровень информационной безопасности (например, ISO 17799), вопросам документирования уделяется должное внимание.

Задача анализа рисков считается руководством актуальной. Анализ рисков рассматривается как один из элементов технологии управления режимом информационной безопасности на всех стадиях жизненного цикла. Понятие риска включает несколько аспектов: вероятность, угроза, уязвимость, иногда стоимость.

Один из вариантов определения риска (определенного класса) в этом случае: вероятность возникновения инцидента в результате того, что имеющаяся уязвимость (определенного класса) будет способствовать реализации угрозы (определенного класса).

Технология управления режимом информационной безопасности в полном варианте включает следующие элементы:

- Документирование информационной системы организации с позиции информационной безопасности.
- Категорирование информационных ресурсов с позиции руководства организации.
- Определение возможного воздействия различного рода происшествий в области безопасности на информационную технологию.
- Анализ рисков.
- Технология управление рисками на всех этапах жизненного цикла.
- Аудит в области информационной безопасности.

На данном уровне зрелости организации анализ рисков связан с другими компонентами технологии управления режимом информационной безопасности, подробнее эти вопросы рассматриваются в разделе «Современные концепции управления рисками».

На четвертом уровне для руководства организации актуальны вопросы измерения параметров, характеризующих режим информационной безопасности. На этом уровне руководство осознанно принимает на себя ответственность за выбор определенных величин остаточных рисков (которые остаются всегда). Риски, как правило, оцениваются по нескольким критериям (не только стоимостным).

Технология управления режимом информационной безопасности остается прежней, но на этапе анализа рисков применяются количественные методы, позволяющие оценить параметры остаточных рисков, эффективность различных вариантов контрмер при управлении рисками.

На пятом уровне ставятся и решаются различные варианты оптимизационных задач в области обеспечения режима информационной безопасности. Примеры постановок задач:

- Выбрать вариант подсистемы информационной безопасности, оптимизированной по критерию стоимость/эффективность при заданном уровне остаточных рисков.
- Выбрать вариант подсистемы информационной безопасности, при котором минимизируются остаточные риски при фиксированной стоимости подсистемы безопасности.
- Выбрать архитектуру подсистемы информационной безопасности с минимальной стоимостью владения на протяжении жизненного цикла при определенном уровне остаточных рисков.

Распределение организаций по их подходам к вопросам информационной безопасности иллюстрируют диаграммы (Рис. 1 и 2), относящиеся к развитым зарубежным странам (заимствованы из обзора компании Эрнст энд Янг).

В Табл. 1 показано, какие критерии используются организациями для оценки системы информационной безопасности (если они используются).

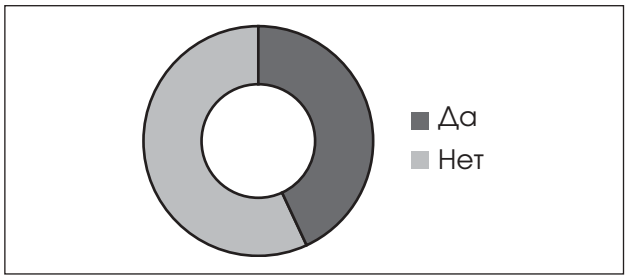

Рис. 1. Контролируют ли в Вашей организации инциденты в области информационной безопасности?

Рис. 2. Используете ли Вы формальные критерии для оценки системы информационной безопасности?

Корпоративные стандарты (собственная разработка)	43
Замечания аудиторов	40
Стандарты лучшей мировой практики (например, BS7799/ISO17799)	29
Число инцидентов в области безопасности	22
Финансовые потери в результате инцидентов	22
Расходы на ИБ	16
Эффективность в достижении поставленных целей	14

Табл. 1. Критерии оценки защищенности информационных систем.

Таким образом, более половины организаций относятся к первому или второму уровню зрелости и не заинтересованы в проведении анализа рисков в любой постановке.

Организации третьего уровня зрелости (около 40% общего числа), использующие (или планирующие использовать) какие-либо подходы к оценке системы информационной безопасности, применяют стандартные рекомендации и руководства класса «good practice», относящиеся к базовому уровню информационной безопасности. Эти организации используют или планируют использовать систему управления рисками базового уровня (или ее элементы) на всех стадиях жизненного цикла информационной технологии.

Организации, относящиеся к четвертому и пятому уровням зрелости, составляющие в настоящее время не более 7% от общего числа, используют разнообразные «углубленные» методики анализа рисков, обладающие дополнительными возможностями по сравнению с методиками базового уровня. Такого рода дополнения, обеспечивающие возможность количественного анализа и оптимизации подсистемы информационной безопасности в различной постановке, в официальных руководствах не регламентируются.

В России доля организаций, относящихся к третьему, четвертому и пятому уровням зрелости, еще меньше. Соответственно наиболее востребованными в настоящее время являются простейшие методики анализа рисков, являющиеся частью методик управления рисками базового уровня.

Потребителями количественных методик анализа рисков в России являются в основном компании финансового профиля, для которых информационные ресурсы представляют большую ценность. Их немного, но они готовы вкладывать существенные ресурсы в разработку собственных (приемлемых для них) количественных методик.

2. Современные концепции управления рисками

Наличие системы управления рисками (Risk Management) является обязательным компонентом общей системы обеспечения информационной безопасности на всех этапах жизненного цикла. Организации, начиная с третьего уровня зрелости, применяют какой-либо вариант системы управления рисками. Многие зарубежные национальные институты стандартов, организации, специализирующиеся в решении комплексных проблем информационной безопасности предложили схожие концепции управления информационными рисками. В [1] были рассмотрены концепции Британского стандарта BS 7799 и Германского BSI. Рассмотрим концепции, опубликованные национальным институтом стандартов США (NIST) [5] и организацией MITRE [6].

2.1. Управление рисками в соответствии со стандартом NIST 800-30

Система управления (информационными) рисками организации должна минимизировать возможные

Фаза жизненного цикла информационной технологии	Соответствие фазе управления рисками
1. Предпроектная стадия ИС (концепция данной ИС: определение целей и задач и их документирование)	Выявление основных классов рисков для данной ИС, вытекающих из целей и задач, концепция обеспечения ИБ
2. Проектирование ИС	Выявление рисков, специфичных для данной ИС (вытекающих из особенностей архитектуры ИС)
3. Создание ИС: поставка элементов, монтаж, настройка и конфигурирование	До начала функционирования ИС должны быть идентифицированы и приняты во внимания все классы рисков
4. Функционирование ИС	Периодическая переоценка рисков, связанная с изменениями внешних условий и в конфигурации ИС
5. Прекращение функционирования ИС (информационные и вычислительные ресурсы более не используются по назначению и утилизируются)	Соблюдение требований информационной безопасности по отношению к выводимым информационным ресурсам

Табл. 2. Управление рисками на различных стадиях жизненного цикла информационной технологии

негативные последствия, связанные с использованием информационных технологий и обеспечить возможность выполнения основных бизнес-целей предприятия.

Система управления рисками должна быть интегрирована в систему управления жизненным циклом информационной технологии (Табл. 2).

В соответствии с [5] технология управления рисками должна включать следующие основные стадии (рис. 3).

2.2. Концепция управления рисками MITRE

Организацией MITRE [6] была предложена концепция управления рисками при построении различных систем (не только информационных). В целом эта концепция близка к рассмотренной выше. MITRE бесплатно распространяет простейший инструментарий на базе электронной таблицы, предназначенный для использования на этапе идентификации и оценки рисков, выбора возможных контрмер в соответствии с этой концепцией — «Risk Matrix» [7].

В данной концепции риск не разделяется на составляющие части (угрозы и уязвимости), что в некоторых случаях может оказаться более удобным с точки зрения владельцев информационных ресурсов. Например, в России в настоящее время на этапе анализа рисков (если он вообще выполняется) весьма распространено построение модели нарушителя с прямой экспертной оценкой рисков. По этой причине простейшие методики и инструменты типа «Risk Matrix» наиболее востребованы в настоящее время на Российском рынке.

3. Реализация концепции управления рисками на практике

Опубликованные документы различных организаций, касающиеся управления рисками, не содержат ряда важных деталей, которые обязательно надо конкретизировать при разработке применимых на практике методик. Конкретизация этих деталей зависит от уровня зрелости организации, специфики ее деятельности и некоторых других факторов. Таким образом, невозможно предложить единую, приемлемую для всех, универсальную методику, соответствующую некоторой концепции управления рисками.

Рассмотрим типичные вопросы, возникающие при реализации концепции управления рисками и возможные подходы к их решению.

3.1 Идентификация рисков

В любой методике необходимо идентифицировать риски, как вариант — их составляющие (угрозы и уязвимости). Естественным требованием к списку является его полнота.

Сложность задачи составления списка и доказательство его полноты зависит от того, какие требования предъявляются к детализации списка.

На базовом уровне безопасности (третий уровень зрелости организации) специальных требований к детализации классов, как правило, не предъявляется и достаточно использовать какой-либо подходящий в данном случае стандартный список классов рисков.

Примером является Германский стандарт BSI, в котором имеется каталог угроз применительно к различным элементам информационной технологии.

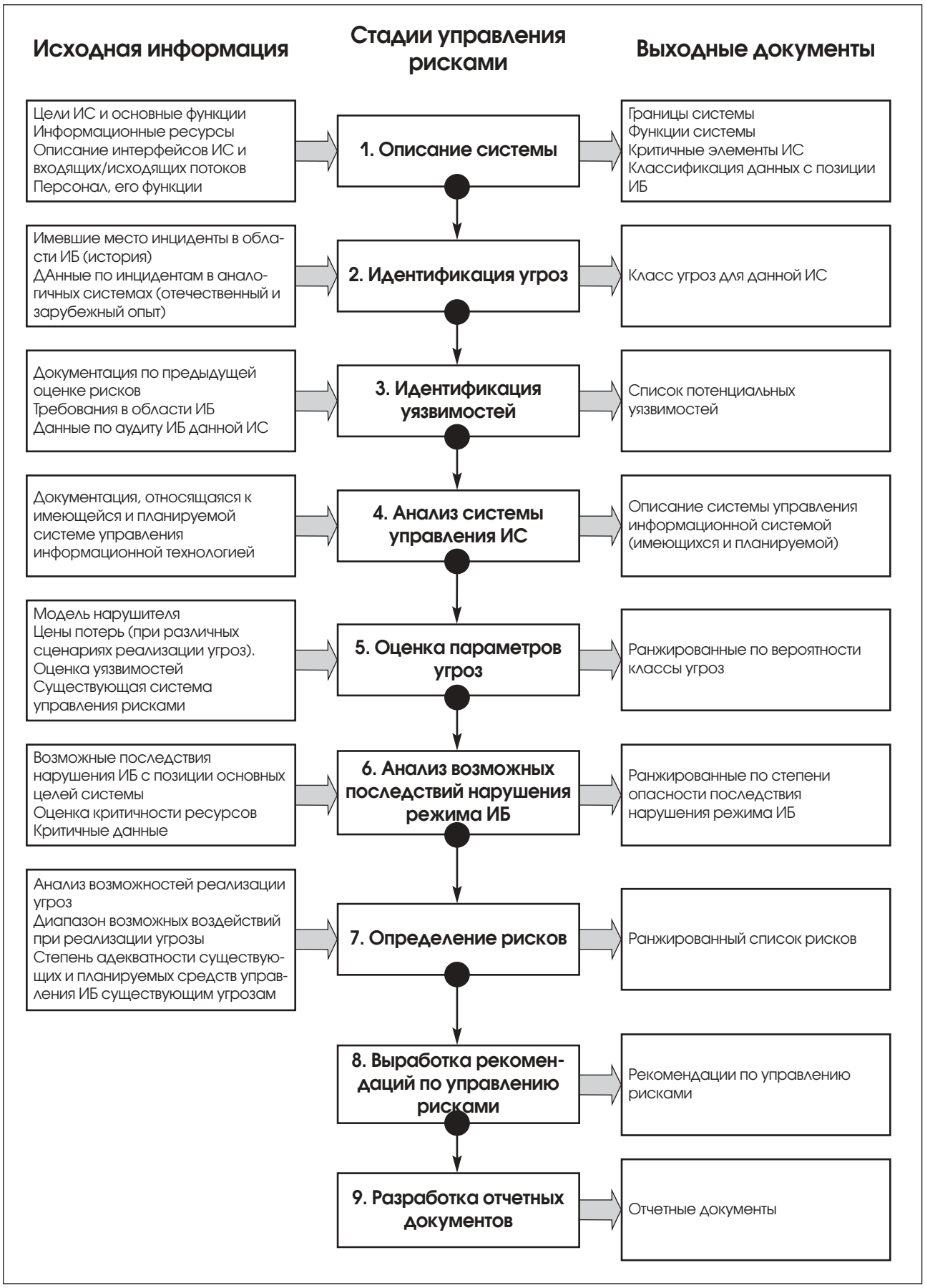

Рис. 3. Концепция управления рисками NIST 800-30

Оценка величины рисков не рассматривается, что приемлемо для некоторых разновидностей методик базового уровня.

Списки классов рисков содержатся в некоторых руководствах, в специализированном ПО анализа рисков. Классификация рисков, используемая в методе CRAMM, была рассмотрена в [1], в [8] даны другие примеры классификаций.

Достоинством подобных списков является их полнота: классов, как правило, немного (десятки), они достаточно широкие и заведомо покрывают всё существующее множество рисков.

Недостаток — сложность оценки уровня риска и эффективности контрмер для широкого класса, поскольку подобные расчеты удобнее проводить по более узким (конкретным) классам рисков. К примеру, класс рисков «неисправность маршрутизатора» может быть разбит на множество подклассов, включающих возможные виды неисправности (уязвимости) ПО конкретного маршрутизатора и неисправности оборудования.

3.2. Оценивание рисков

Рассмотрим следующие аспекты:

- Шкалы и критерии, по которым можно измерять риски.
- Оценку вероятностей событий.
- Технологии измерения рисков.

3.2.1. Шкалы и критерии, по которым измеряются риски

Для измерения какого-либо свойства необходимо выбрать шкалу. Шкалы могут быть прямыми (естественными) или косвенными (производными). Примерами прямых шкал являются шкалы для измерения физических величин, например, литры для измерения объемов, метры для измерения длины.

В ряде случаев прямых шкал не существует, приходится использовать либо прямые шкалы других свойств, связанных с интересующими нас, либо определять новые шкалы. Примером является шкала для измерения субъективного свойства «ценность информационного ресурса». Она может измеряться в производных шкалах, таких как стоимость восстановления ресурса, время восстановления ресурса и других. Другой вариант — определить шкалу для получения экспертной оценки, например, имеющую три значения:

- Малоценный информационный ресурс: от него не зависят критически важные задачи и он может быть восстановлен с небольшими затратами времени и денег.
- Ресурс средней ценности: от него зависит ряд важных задач, но в случае его утраты он может быть восстановлен за время менее, чем критически допустимое, стоимость восстановления высокая.
- Ценный ресурс: от него зависят критически важные задачи, в случае утраты время восстановления превышает критически допустимое, либо стоимость чрезвычайно высока.

Для измерения рисков не существует естественной шкалы.

Риски можно оценивать по объективным либо субъективным критериям.

Примером объективного критерия является вероятность выхода из строя какого-либо оборудования, например, ПК за определенный промежуток времени.

Примером субъективного критерия является оценка владельцем информационного ресурса риска выхода из строя ПК. Для этого обычно разрабатывается качественная шкала с несколькими градациями, например: низкий, средний, высокий уровени.

В методиках анализа рисков, как правило, используются субъективные критерии, измеряемые в качественных шкалах, поскольку:

- Оценка должна отражать субъективную точку зрения владельца информационных ресурсов.
- Должны быть учтены различные аспекты, не только технические, но и организационные, психологические, и т.д.

Для получения субъективной оценки в рассматриваемом примере с оценкой риска выхода из строя ПК, можно использовать либо прямую экспертную оценку, либо определить функцию, отображающую объективные данные (вероятность) в субъективную шкалу рисков.

Субъективные шкалы могут быть количественными и качественными, но на практике, как правило, используются качественные шкалы с 3-7 градациями. С одной стороны, это просто и удобно, с другой — требует грамотного подхода к обработке данных.

3.2.2 Объективные и субъективные вероятности

Термин «вероятность» имеет несколько различных значений. Наиболее часто встречаются два толкования этого слова, которые обозначаются сочетанием «объективная вероятность» и «субъективная вероятность». Под объективной (иногда называемой физической) вероятностью понимается относительная частота появления какого-либо события в общем объеме наблюдений или отношение числа благоприятных исходов к общему их количеству. Объективная вероятность возникает при анализе резуль-

татов большого числа наблюдений, имевших место в прошлом, а также как следствия из моделей, описывающих некоторые процессы.

Под субъективной вероятностью понимается мера уверенности некоторого человека или группы людей в том, что данное событие в действительности будет иметь место.

Как мера уверенности человека в возможности наступления события субъективная вероятность может быть формально представлена различными способами: вероятностным распределением на множестве событий, бинарным отношением на множестве событий, неполностью заданным вероятностным распределением или бинарным отношением и другими способами. Наиболее часто субъективная вероятность представляет собой вероятностную меру, полученную экспертным путем.

Именно в этом смысле мы и будем понимать субъективную вероятность в дальнейшем.

Субъективная вероятность в современных работах в области системного анализа не просто представляет меру уверенности на множестве событий, а увязывается с системой предпочтений лица, принимающего решения (ЛПР), и в конечном итоге с функцией полезности, отражающей его предпочтения на множестве альтернатив.

Тесная связь между субъективной вероятностью и полезностью используется при построении некоторых методов получения субъективной вероятности.

3.2.3. Получение оценок субъективной вероятности

Процесс получения субъективной вероятности принято разделять на три этапа:

- Подготовительный этап.
- Получение оценок.
- Этап анализа полученных оценок.

Первый этап. Во время этого этапа формируется объект исследования — множество событий, проводится предварительный анализ свойств этого множества (устанавливается зависимость или независимость событий, дискретность или непрерывность случайной величины, порождающей данное множество событий). На основе такого анализа выбирается один из подходящих методов (подробно рассматриваются в [8]) получения субъективной вероятности.

На этом же этапе производится подготовка эксперта или группы экспертов, ознакомление их с методом и проверка понимания поставленной задачи экспертами.

Второй этап состоит в применении метода, выбранного на первом этапе. Результатом этого этапа является набор чисел, который отражает субъективный взгляд эксперта или группы экспертов на вероятность того или иного события, однако далеко не всегда может считаться окончательно полученным распределением, поскольку может быть противоречивым.

Третий этап состоит в исследовании результатов опроса. Если вероятности, полученные от экспертов, не согласуются с аксиомами вероятности, то на это обращается внимание экспертов и производится уточнение ответов с целью их соответствия аксиомам.

Для некоторых методов получения субъективной вероятности третий этап не проводится, поскольку сам метод состоит в выборе вероятного распределения, подчиняющегося аксиомам вероятности, которое в том или другом смысле наиболее близко к оценкам экспертов.

Особую важность третий этап приобретает при агрегировании оценок, полученных от группы экспертов. Более подробно технология агрегирования групповых оценок применительно к факторам риска рассмотрена в [8].

3.2.4. Измерение рисков

Существует ряд подходов к измерению рисков. Рассмотрим наиболее распространенные:

- Оценка по двум факторам;
- Оценка по трем факторам.

3.2.4.1 Оценка рисков по двум факторам

В простейшем случае используется оценка двух факторов: вероятность происшествия и тяжесть возможных последствий. Обычно считается, что риск тем больше, чем больше вероятность происшествия и тяжесть последствий. Общая идея может быть выражена формулой:

$$\text{РИСК} = \text{Р}_{\text{происшествия}} * \text{ЦЕНА ПОТЕРИ}$$

Если переменные являются количественными величинами — риск это оценка математического ожидания потерь.

Если переменные являются качественными величинами, то метрическая операция умножения не определена. Таким образом, в явном виде эта формула использоваться не должна. Рассмотрим вариант использования качественных величин (наиболее часто встречающаяся ситуация).

Вначале должны быть определены шкалы.

Определяется субъективная шкала вероятностей событий, пример такой шкалы [5]:

A — Событие практически никогда не происходит.

B — Событие случается редко.

	Negligible	Minor	Moderate	Serious	Critical
A	Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
B	Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
C	Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
D	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
E	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

Табл. 3. Определение риска в зависимости от двух факторов.

C — Вероятность события за рассматриваемый промежуток времени — около 0.5.
D — Скорее всего событие произойдет.
E — Событие почти обязательно произойдет.

Кроме того, определяется субъективная шкала серьезности происшествий, например, в соответствии с [5]:

N (Negligible) — Воздействием можно пренебречь.
Mi (Minor) — Незначительное происшествие: последствия легко устранимы, затраты на ликвидацию последствий не велики, воздействие на информационную технологию -незначительно.
Mo (Moderate) — Происшествие с умеренными результатами: ликвидация последствий не связана с крупными затратами, воздействие на информационную технологию не велико и не затрагивает критически важные задачи.
S (Serious) — Происшествие с серьезными последствиями: ликвидация последствий связана со значительными затратами, воздействие на информационные технологии ощутимо, воздействует на выполнение критически важных задач.
C (Critical) — Происшествие приводит к невозможности решения критически важных задач.

Для оценки рисков определяется шкала из трех значений:

- Низкий риск.
- Средний риск.
- Высокий риск.

Риск, связанный с определенным событием, зависит от двух факторов и может быть определен так [5] — Табл. 3.

Шкалы факторов риска и сама таблица могут быть определены иначе, иметь другое число градаций.

Подобный подход к оценке рисков достаточно распространен.

При разработке (использовании) методик оценки рисков необходимо учитывать следующие особенности:

- Значения шкал должны быть четко определены (словесное описание) и пониматься одинаково всеми участниками процедуры экспертной оценки.
- Требуются обоснования выбранной таблицы. Необходимо убедиться, что разные инциденты, характеризующиеся одинаковыми сочетаниями факторов риска, имеют с точки зрения экспертов одинаковый уровень рисков. Для этого существуют специальные процедуры проверки, подробности можно посмотреть в [8].

Подобные методики широко применяются при проведении анализа рисков базового уровня.

3.2.4.2 Оценка рисков по трем факторам.

В зарубежных методиках, рассчитанных на более высокие требования, чем базовый уровень, используется модель оценки риска с тремя факторами: угроза, уязвимость, цена потери. Угроза и уязвимость определяются следующим образом:

Угроза — совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.
Уязвимость — слабость в системе защиты, которая делает возможным реализацию угрозы.

Вероятность происшествия, которая в данном подходе может быть объективной либо субъективной величиной, зависит от уровней (вероятностей) угроз и уязвимостей:

$$P_{\text{происшествия}} = P_{\text{угрозы}} * P_{\text{уязвимости}}$$

Соответственно риск определяется следующим образом:

$$\text{РИСК} = P_{\text{угрозы}} * P_{\text{уязвимости}} * \text{ЦЕНА ПОТЕРИ}$$

Данное выражение можно рассматривать как математическую формулу, если используются количественные шкалы, либо как формулировку общей идеи, если хотя бы одна из шкал — качественная. В последнем случае используются различного рода табличные методы для определения риска в зависимости от трех факторов.

Степень серьезности происшествия (цена потери)	Уровень угрозы: Низкий, Уровни уязвимостей			Средний, Уровни уязвимостей			Высокий, Уровни уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
Negligible	0	1	2	1	2	3	2	3	4
Minor	1	2	3	2	3	4	3	4	5
Moderate	2	3	4	3	4	5	4	5	6
Serious	3	4	5	4	5	6	5	6	7
Critical	4	5	6	5	6	7	6	7	8

Табл. 4. Определение риска в зависимости от трех факторов

Например, показатель риска измеряется в шкале от 0 до 8 со следующими определениями уровней риска:

1 риск практически отсутствует. Теоретически возможны ситуации, при которых событие наступает, но на практике это случается редко, а потенциальный ущерб сравнительно невелик.

2 риск очень мал. События подобного рода случались достаточно редко, кроме того, негативные последствия сравнительно невелики.

...

8 риск очень велик. Событие скорее всего наступит, и последствия будут чрезвычайно тяжелыми.

Матрица может быть определена следующим образом — Табл. 4. В данной таблице уровни уязвимости Н, С, В означают соответственно: низкий, средний, высокий уровни. Некоторые другие варианты таблиц рассмотрены в [2].

Подобные таблицы используются как в «бумажных» вариантах методик оценки рисков, так и в различного рода инструментальных средствах — ПО анализа рисков.

В последнем случае матрица задается разработчиками ПО и, как правило, не подлежит корректировке. Это один из факторов, ограничивающих точность подобного рода инструментария.

3.2.5 Технология оценки угроз и уязвимостей

Для оценки угроз и уязвимостей используются различные методы, в основе которых могут лежать:

- Экспертные оценки.
- Статистические данные.
- Учет факторов, влияющих на уровни угроз и уязвимостей.

Один из возможных подходов к разработке подобных методик — накопление статистических данных о реально случившихся происшествиях, анализ и классификация их причин, выявление факторов, от которых они зависят. На основе этой информации можно оценить угрозы и уязвимости в других информационных системах.

Практические сложности в реализации этого подхода следующие:

Во-первых, должен быть собран весьма обширный материал о происшествиях в этой области.

Во-вторых, применение этого подхода оправдано 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 новейшие элементы технологии (для которых пока нет достоверной статистики), оценки угроз и уязвимостей могут оказаться недостоверными.

Наиболее распространенным в настоящее время является подход, основанный на учете различных факторов, влияющих на уровни угроз и уязвимостей. Такой подход позволяет абстрагироваться от малосущественных технических деталей, учесть не только программно-технические, но и иные аспекты.

Рассмотрим пример реализации подобного подхода, используемого в методе CRAMM 4.0 для одного из классов рисков: **«Использование чужого идентификатора сотрудниками организации («маскарад»)».**

Для оценки угроз выбраны следующие косвенные факторы:

- Статистика по зарегистрированным инцидентам.
- Тенденции в статистке по подобным нарушениям.
- Наличие в системе информации, представляющей интерес для потенциальных внутренних или внешних нарушителей.
- Моральные качества персонала.
- Возможность извлечь выгоду из изменения обрабатываемой в системе информации.
- Наличие альтернативных способов доступа к информации.
- Статистика по подобным нарушениям в других информационных системах организации.

Для оценки уязвимостей выбраны следующие косвенные факторы:

- Количество рабочих мест (пользователей) в системе.
- Размер рабочих групп.
- Осведомленность руководства о действиях сотрудников (разные аспекты).
- Характер используемого на рабочих местах оборудования и ПО.
- Полномочия пользователей.

По косвенным факторам предложены вопросы и несколько фиксированных вариантов ответов, которые «стоят» определенное количество баллов. Итоговая оценка угрозы и уязвимости данного класса определяется путем суммирования баллов.

Оценка угрозы

Ответьте на вопросы

1. Сколько раз за последние 3 года сотрудники организации пытались получить несанкционированный доступ к хранящейся в информационной системе информации с использованием прав других пользователей?

Варианты ответов

a	Ни разу	0
b	Один или два раза	10
c	В среднем раз в год	20
d	В среднем чаще одного раза в год	30
e	Неизвестно	10

2. Какова тенденция в статистике такого рода попыток несанкционированного проникновения в информационную систему?

Варианты ответов

a	К возрастанию	10
b	Оставаться постоянной	0
c	К снижению	-10

3. Хранится ли в информационной системе информация (например, личные дела), которая может представлять интерес для сотрудников организации и побуждать их к попыткам несанкционированного доступа к ней?

Варианты ответов

a	Да	5
b	Нет	0

4. Известны ли случаи нападения, угроз, шантажа, давления на сотрудников со стороны посторонних лиц?

Варианты ответов

a	Да	10
b	Нет	0

5. Существуют ли среди персонала группы лиц или отдельные лица с недостаточно высокими моральными качествами?

Варианты ответов

a	Нет, все сотрудники отличаются высокой честностью и порядочностью	0
b	Существуют группы лиц и отдельные личности с недостаточно высокими моральными качествами, но это вряд ли может спровоцировать их на несанкционированное использование системы	5
c	Существуют группы лиц и отдельные личности с настолько низкими моральными качествами, что это повышает вероятность несанкционированного использования системы сотрудниками	10

6. Хранится ли в информационной системе информация, несанкционированное изменение которой может принести прямую выгоду сотрудникам?

Варианты ответов

a	Да	5
b	Нет	0

7. Предусмотрена ли в информационной системе поддержка пользователей, обладающих техническими возможностями совершить подобные действия?

Варианты ответов

a	Нет	0
b	Да	5

8. Существуют ли другие способы просмотра информации, позволяющие злоумышленнику добраться до нее более простыми методами, чем с использованием «маскарада»?

Варианты ответов

a	Да	-10
b	Нет	0

9. Существуют ли другие способы несанкционированного изменения информации, позволяющие злоумышленнику достичь желаемого результата более простыми методами, чем с использованием «маскарада»?

Варианты ответов

a	Да	-10
b	Нет	0

10. Сколько раз за последние 3 года сотрудники пытались получить несанкционированный доступ к информации, хранящейся в других подобных системах в вашей организации?

Варианты ответов

a	Ни разу	0
b	Один или два раза	5
c	В среднем раз в год	10
d	В среднем чаще одного раза в год	15
e	Неизвестно	10

Степень угрозы при количестве баллов:

До 9	Очень низкая
От 10 до 19	Низкая
От 20 до 29	Средняя
От 30 до 39	Высокая
40 и более	Очень высокая

Оценка уязвимости

Ответьте на вопросы:

1. Сколько людей имеют право пользоваться информационной системой?

Варианты ответов

a	От 1 до 10	0
b	От 11 до 50	4
c	От 51 до 200	10
d	От 200 до 1000	14
e	Свыше 1000	20

2. Будет ли руководство осведомлено о том, что люди, работающие под их началом, ведут себя необычным образом?

Варианты ответов

a	Да	0
b	Нет	10

3. Какие устройства и программы доступны пользователям?

Варианты ответов

a	Только терминалы или сетевые контроллеры, ответственные за предоставление и маршрутизацию информации, но не за передачу данных	-5
b	Только стандартные офисные устройства и программы и управляемые с помощью меню подчиненные прикладные программы	0
c	Пользователи могут получить доступ к операционной системе, но не к компиляторам	5
d	Пользователи могут получить доступ к компиляторам	10

4. Возможны ли ситуации, когда сотрудникам, предупрежденным о предстоящем сокращении или увольнении, разрешается логический доступ к информационной системе?

Варианты ответов

a	Да	10
b	Нет	0

5. Каковы в среднем размеры рабочих групп сотрудников пользовательских подразделений, имеющих доступ к информационной системе?

Варианты ответов

a	Менее 10 человек	0
b	От 11 до 20 человек	5
c	Свыше 20 человек	10

6. Станет ли факт изменения хранящихся в информационной системе данных очевидным сразу для нескольких человек (в результате чего его будет очень трудно скрыть)?

Варианты ответов

a	Да	0
b	Нет	10

7. Насколько велики официально предоставленные пользователям возможности по просмотру всех хранящихся в системе данных?

Варианты ответов

a	Официальное право предоставлено всем пользователям	-2
b	Официальное право предоставлено только некоторым пользователям	0

8. Насколько необходимо пользователям знать всю информацию, хранящуюся в системе?

Варианты ответов

a	Всем пользователям необходимо знать всю информацию	-4
b	Отдельным пользователям необходимо знать лишь относящуюся к ним информацию	0

Степень уязвимости при количестве баллов:

До 9	Низкая
От 10 до 19	Средняя
20 и более	Высокая

Возможности данного подхода и границы его применимости.

Несомненным достоинством данного подхода является возможность учета множества косвенных факторов (не только технических). Методика проста и дает владельцу информационных ресурсов ясное представление, каким образом получается итоговая оценка и что надо изменить, чтобы улучшить оценки.

Недостатки: Косвенные факторы зависят от сферы деятельности организации, а также от ряда иных обстоятельств. Таким образом, методика всегда требует подстройки под конкретный объект. При

этом доказательство полноты выбранных косвенных факторов и правильности их весовых коэффициентов (задача малоформализованная и сложная) на практике решается экспертными методами (проверка соответствия полученных по методике результатов ожидаемым для тестовых ситуаций).

Подобные методики, как правило, разрабатываются для организаций определенного профиля (ведомств), апробируются и затем используются в качестве ведомственного стандарта. По такому пути пошли и разработчики CRAMM, создав около десятка версий метода для разных ведомств (министерство иностранных дел, вооруженные силы и т.д.).

Оценки рисков и уязвимостей в рассмотренном примере являются качественными величинами. Однако подобными методами могут быть получены и количественные оценки, необходимые при расчете остаточных рисков, решении оптимизационных задач. Для этого применяется ряд методов, позволяющих установить на упорядоченном множестве оценок систему расстояний, обзор приводится в [8].

Получение объективных количественных оценок рисков должно быть актуально для страховых агентств, занимающихся страхованием информационных рисков.

На практике страховые агентства пользуются в большинстве случаев качественными оценками. Простые методики без длительного и дорогостоящего обследования позволяют отнести информационную систему к той или иной группе риска (по классификации страховой компании) на основе интервью с рядом должностных лиц. В таких методиках также фиксируются и анализируются косвенные факторы.

3.3 Выбор допустимого уровня риска

Выбор допустимого уровня риска связан с затратами на реализацию подсистемы информационной безопасности. Существует два подхода к выбору допустимого уровня рисков.

Первый подход типичен для базового уровня безопасности. Уровень остаточных рисков не принимается во внимание. Затраты на программно-технические средства защиты и организационные мероприятия, необходимые для соответствия информационной системы спецификациям базового уровня (антивирусное ПО, МЭ, криптографическая защита, системы резервного копирования, системы контроля доступа) являются обязательными, целесообразность их использования не обсуждается. Дополнительные затраты (если такой вопрос будет поставлен по результатам проведения аудита ИБ либо по инициативе службы безопасности) должны находиться в разумных пределах и не превышать 5-15% средств, которые тратятся на поддержание работы информационной системы.

Второй подход применяется при обеспечении повышенного уровня безопасности. Собственник информационных ресурсов должен сам выбирать допустимый уровень остаточных рисков и нести ответственность за свой выбор.

В зависимости от уровня зрелости организации, характера основной деятельности обоснование выбора допустимого уровня риска может проводиться разными способами.

Наиболее распространенным является анализ стоимость/эффективность различных вариантов защиты, примеры постановок задач:

- Стоимость подсистемы безопасности должна составлять не более 20% от стоимости информационной системы. Найти вариант контрмер, максимально снижающих уровень интегральный рисков.
- Уровень рисков по всем классам не должен превышать «очень низкий уровень». Найти вариант контрмер с минимальной стоимостью.

В случае постановок оптимизационных задач важно правильно выбрать комплекс контрмер (перечислить возможные варианты) и оценить его эффективность.

3.4 Выбор контрмер и оценка их эффективности

Система защиты строится комплексно, включает контрмеры разных уровней (административные, организационные, программно-технические).

Для облегчения выбора комплекса контрмер в различных методиках используются таблицы, в которых классам угроз ставятся в соответствие возможные контрмеры. Ниже приводится пример классификатора контрмер CRAMM 4:

Классы контрмеры, соответствующие классам угроз в методе CRAMM 4 (фрагмент)

Masquerading of User Identity by Insiders

Identification and Authentication
Logical Access Control
Accounting
Audit
Object Re-use
Security Testing
Software Integrity
Mobile Computing and Teleworking
Software Distribution
System Input/Output Controls
Network Access Controls

System Administration Controls
Application Input/Output Controls
Back-up of Data
Personnel
Security Education and Training
Security Policy
Security Infrastructure
Data Protection Legalisation
Incident Handling
Compliance Checks

Masquerading of User Identity by Contracted Service Providers

Identification and Authentication
Logical Access Control
Accounting
Audit
Object Re-use
Security Testing
Software Integrity
Mobile Computing and Teleworking
Software Distribution
System Input/Output Controls
Network Access Controls
System Administration Controls
Application Input/Output Controls
Back-up of Data
Personnel
Security Education and Training
Security Policy
Security Infrastructure
Outsourcing
Data Protection Legalisation
Incident Handling
Compliance Checks

Masquerading of User Identity by Outsiders

Identification and Authentication
Logical Access Control
Accounting
Audit
Object Re-use
Security Testing
Software Integrity
Mobile Computing and Teleworking
Software Distribution
System Input/Output Controls
Network Security Management
Network Access Controls
System Administration Controls
Application Input/Output Controls
Back-up of Data
Security Education and Training
Security Policy
Security Infrastructure
Data Protection Legalisation
Incident Handling
Compliance Checks

Подобные классификаторы позволяют автоматически выбирать и предлагать конкретные варианты контрмер, возможных для рассматриваемой информационной системы. Владелец информационных ресурсов может отбирать из них приемлемые. Следующий шаг — оценка эффективности контрмер.

Задача оценки эффективности контрмер является не менее сложной, чем оценка рисков.

Причина в том, что оценка эффективности комплексной подсистемы безопасности, включающей контрмеры разных уровней (административные, организационные, программно-технические) в конкретной информационной системе — методологически чрезвычайно сложная задача. По этой причине обычно используются упрощенные, качественные оценки эффективности контрмер.

Примером является таблица типичных значений эффективности контрмер, используемых в методе анализа рисков RiskWatch, рассматриваемом в следующем разделе.

Указанные в Табл. 5 значения являются ориентировочными оценками эффективности вложений в различные классы мероприятий в области защиты информации.

Табл. 5. Ориентировочная эффективность мероприятий в области защиты информации по критерию ROI (Return of Investment — возврат вложений)

В ряде случаев используются более сложные таблицы, в которых эффективность зависит от ряда факторов (аналогично примеру оценки угроз и уязвимостей в 3.2.5).

На основе подобных таблиц делаются качественные оценки эффективности контрмер.

4. Инструментарий для анализа и управления рисками

Инструментальные средства анализа рисков позволяют автоматизировать работу специалистов в области защиты информации, осуществляющих оценку информационных рисков предприятия.

В России в настоящее время чаще всего используются разнообразные «бумажные» методики, достоинствами которых является гибкость и адаптивность. Как правило, разработкой данных методик занимаются компании — системные и специализированные интеграторы в области защиты информации. По понятным причинам методики обычно не публикуются, поскольку относятся к «Know how» компании. В силу закрытости данных методик судить об их качестве, объективности и возможностях достаточно сложно.

Специализированное ПО, реализующее методики анализа рисков, может относиться к категории программных продуктов (продается на рынке) либо являться собственностью ведомства или организации и не продаваться. Если ПО разрабатывается как программный продукт, оно должно быть в достаточной степени универсальным. Ведомственные варианты ПО адаптированы под особенности постановок задач анализа и управления рисками, и позволяют учесть специфику информационных технологий организации.

Предлагаемое на рынке ПО ориентировано в основном на уровень информационной безопасности, несколько превышающий базовый уровень защищенности. Таким образом, инструментарий рассчитан в основном на потребности организаций 3-4 степени зрелости.

ПО анализа рисков, присутствующее на рынке по состоянию на 1998 год было рассмотрено в [1]. Рассмотрим современное состояние этого рынка и основные тенденции его развития.

В 2000 году был принят международный стандарт ISO 17799, за основу которого был взят Британский стандарт BS 7799, рассмотрений в [1,2]. В результате большинство инструментальных средств (ПО анализа и управления рисками) было в последнее время модифицировано таким образом, чтобы обеспечить соответствие требованиям этого стандарта.

В обзоре ПО условно разделено на 2 группы:

- ПО базового уровня;
- ПО полного анализа рисков.

Надо учитывать, что это разделение весьма условно, поскольку инструментарий базового уровня зачастую содержит дополнительные возможности, относящиеся к полному анализу рисков.

4.1 Инструментарий базового уровня

Вначале рассмотрим инструментарий, соответствующий ISO17799:

- Справочные и методические материалы.
- ПО анализа рисков и аудита «Cobra».
- ПО анализа рисков и аудита «Software Tool».

4.1.1 Справочные и методические материалы

Ряд Британских фирм [9] предлагает следующие продукты:

- Information Security Police
- SOS — INTERACTIVE 'ONLINE' SECURITY POLICIES AND SUPPORT
- Security Professionals Guide

Эти продукты представляют собой справочники, посвященные практическим аспектам реализации политики безопасности в соответствии с ISO17799, вид справочника приводится на рис. 4.1. Демонстрационные версии (Evaluation version) можно загрузить с сайта [11].

Эти методические материалы детализируют требования ISO17799 и выполнены в стиле этого стандарта. Достоинством является гипертекстовая структура, удобная навигация.

Еще один продукт подобного рода — «THE ISO17799 TOOLKIT» — текст стандарта ISO17799 с комплектом методических материалов и презентацией [11].

4.1.2 COBRA

ПО COBRA [9], производитель — C & A Systems Security Ltd., позволяет формализовать и ускорить процесс проверки на соответствие режима информационной безопасности требованиям Британского стандарта BS 7799 (ISO 17799) и провести анализ

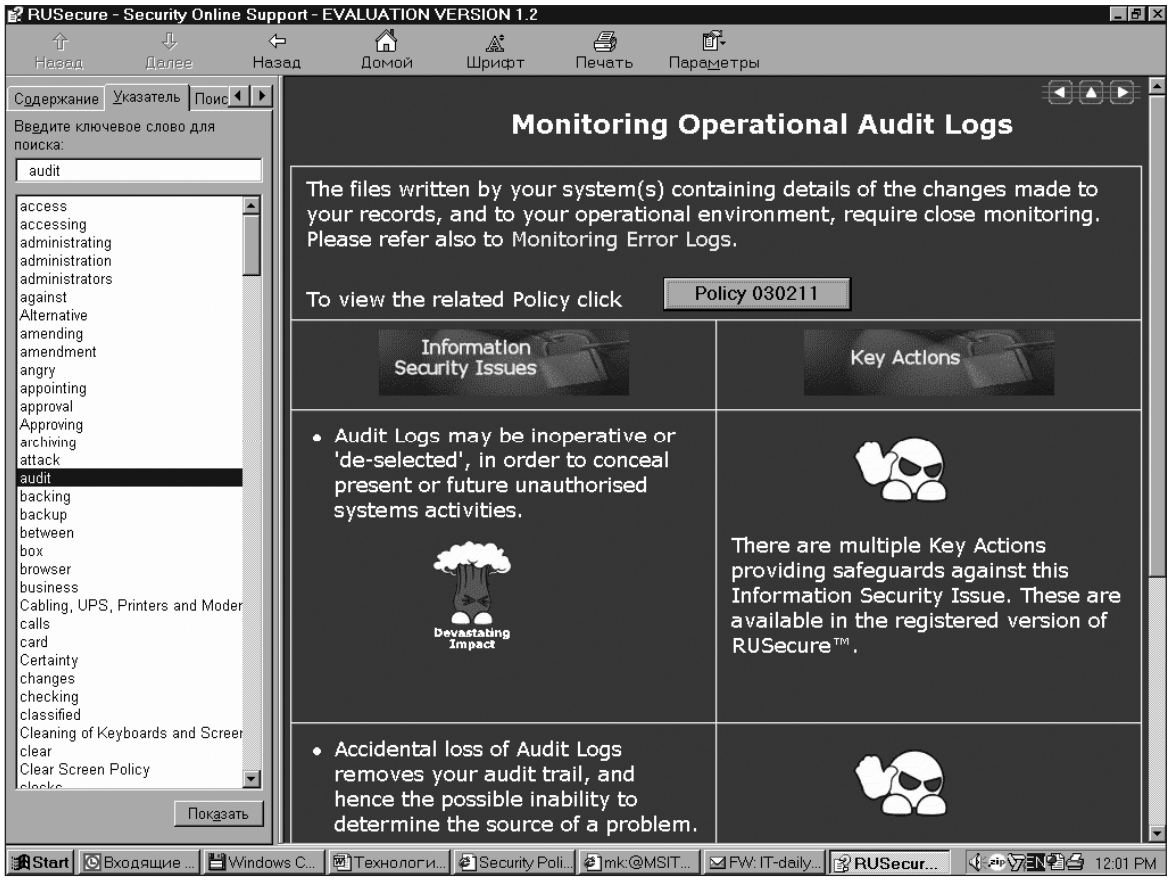

Рис 4.1. Справочник 'ONLINE' SECURITY POLICIES AND SUPPORT

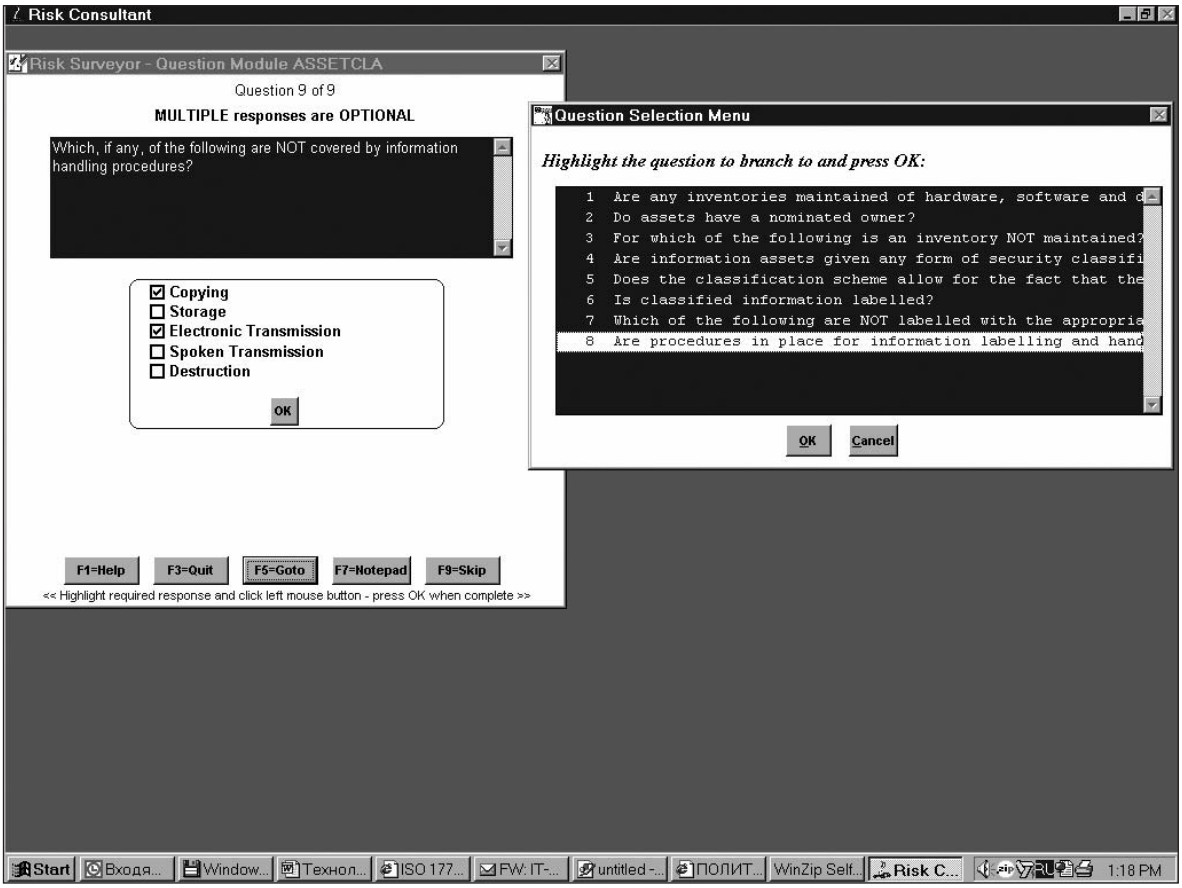

Рис 4.2. Анализ рисков с использованием ПО "Cobra"

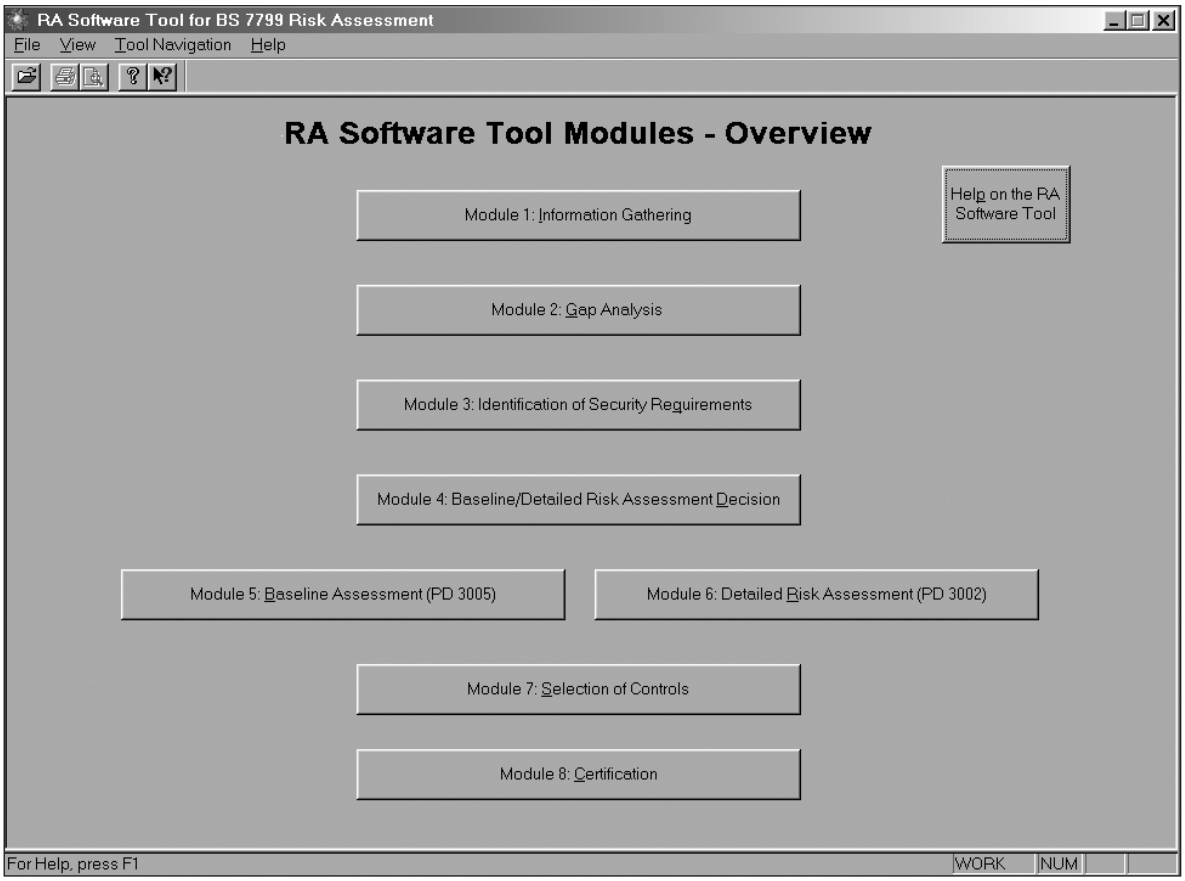

Рис 4.3. Основные модули RA Software Tool

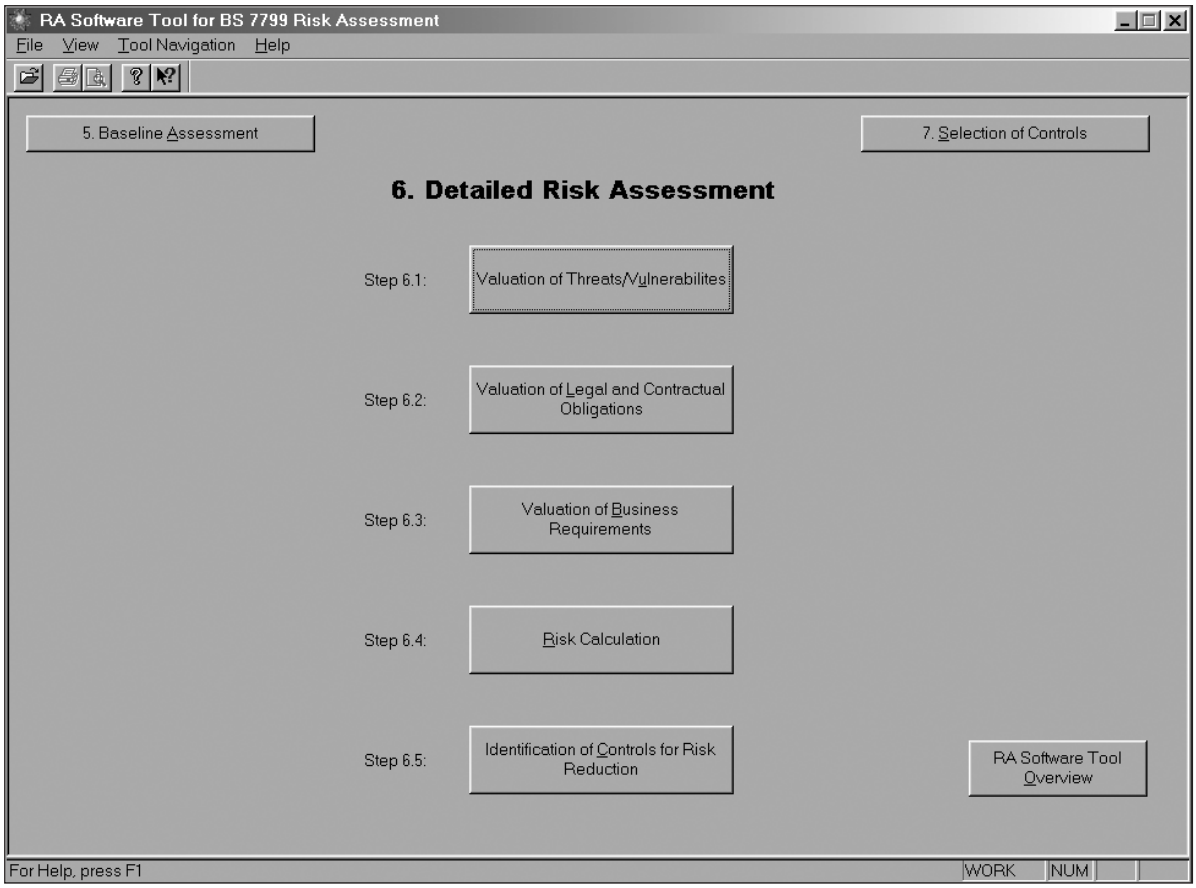

Рис 4.4. Детальная оценка рисков в RA Software Tool, основные шаги

рисков. Имеется несколько баз знаний: общие требования BS 7799 (ISO 17799) и специализированные базы, ориентированные на различные области применения. Доступна Evaluation version этого ПО.

COBRA позволяет представить требования стандарта в виде тематических «вопросников» по отдельным аспектам деятельности организации, пример приводится на рис 4.2.

Анализ рисков, выполняемый данным методом, соответствует базовому уровню безопасности, т.е. уровни рисков не определяются. Достоинством методики является простота. Необходимо ответить на несколько десятков вопросов, затем автоматически формируется отчет.

Этот программный продукт может использоваться при проведении аудита ИБ или для работы специалистов служб, отвечающих за обеспечение информационной безопасности.

Простота, соответствие международному стандарту, сравнительно небольшое число вопросов, позволяют легко адаптировать этот метод для работы в отечественных условиях.

4.1.3 RA Software Tool

Еще один метод, условно относящийся к базовому уровню — RA Software Tool [13], базируется на британском стандарте BS 7799 часть 1 и 2, методических материалах британского института стандартов (BSI) PD 3002 (Руководство по оценке и управлению рисками), PD 3003 (Оценка готовности компании к аудиту в соответствии с BS 7799) , PD 3005 (Руководство по выбору системы защиты), а также стандарт ISO 13335 часть 3 и 4 (Руководство по управлению режимом информационной безопасности, технологии управления безопасностью и выбор средств защиты). Основные модули этого метода показаны на рис 4.3.

Этот инструментарий позволяет выполнять оценку рисков (модули 4 и 5) как в соответствии с требованиями базового уровня, так и в соответствии с более детальными спецификациями PD 3002 Британского института стандартов. Каждый из модулей разбивается, в свою очередь, на ряд шагов (рис 4.4).

Демонстрационная версия данного метода, доступная на сайте [13], отличается от полной версии небольшими купюрами, и может быть полезна при разработке собственных методик и инструментария для анализа и управления рисками.

4.2 Инструментарий для обеспечения повышенного уровня безопасности

Рассмотрим несколько методов, которые можно отнести к инструментарию для нужд организаций четвертого и пятого уровней зрелости.

Как уже отмечалось, четко провести границу между методами базового и полного анализа рисков сложно, примером является рассмотренный выше RA Software Tool, имеющий ряд простейших средств, которые позволяют формально отнести его к средствам полного анализа рисков. Ниже рассматривается инструментарий с более развитыми средствами анализа и управления рисками.

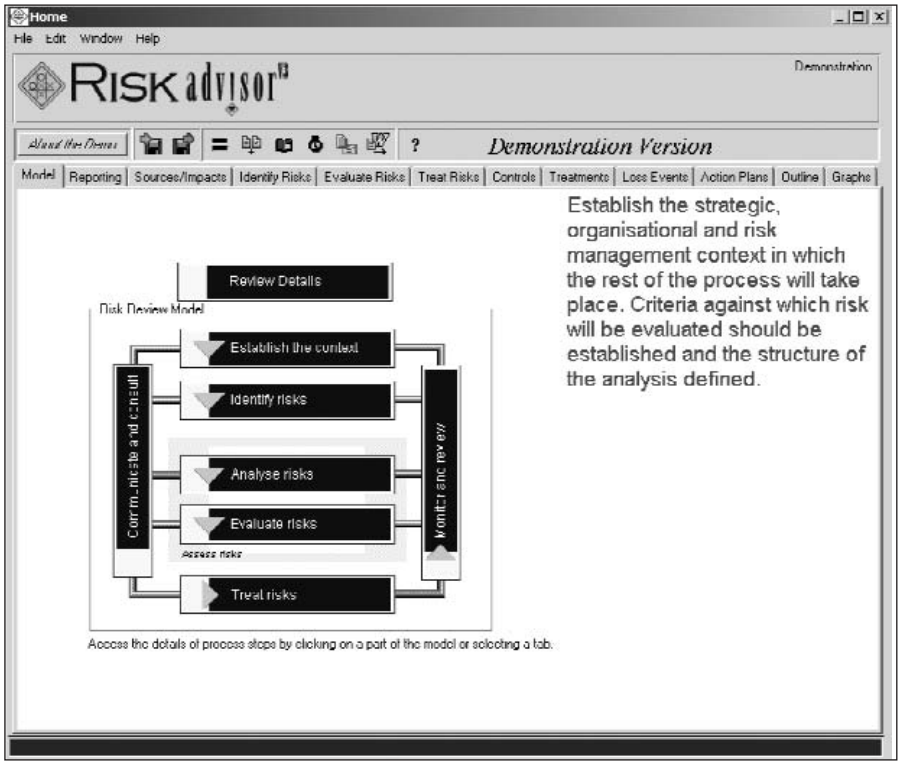

Рис 4.5. Основные этапы в методе Risk Advisor

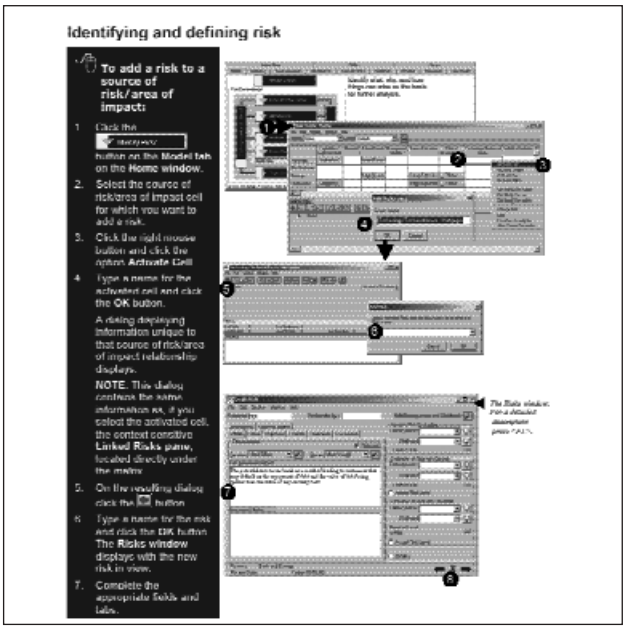

Рис. 4.6. Идентификация и определение рисков в Risk Advisor

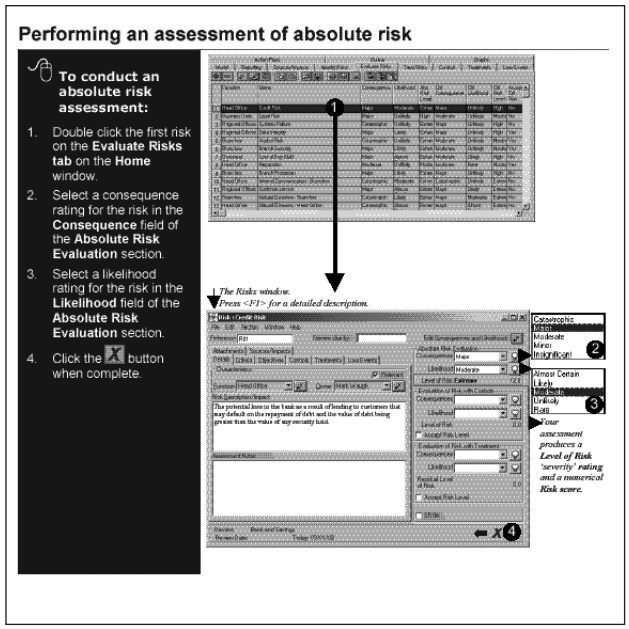

Рис. 4.7. Разделение рисков на приемлемые и неприемлемые в Risk Advisor.

4.2.1 ПО компании MethodWare

Компания MethodWare [10] выпускает ряд продуктов, которые могут использоваться аналитиками в области информационной безопасности при проведении анализа рисков, управлении рисками, аудите информационной безопасности. Это:

- ПО анализа и управления рисками Operational Risk Builder и Risk Advisor. Методология соответствует австралийскому стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999). Имеется и версия, соответствующая ISO17799.
- ПО управления жизненным циклом информационной технологии: CobiT Advisor 3rd Edition (Audit) и CobiT 3rd Edition Management Advisor. В руководствах CobiT существенное место уделяется анализу и управлению рисками.
- ПО для автоматизации построения разнообразных опросных листов Questionnaire Builder

Демо-версии этого ПО можно загрузить с сайта компании MethodWare [10].

Risk Advisor

Это ПО позиционируется как инструментарий аналитика или менеджера в области информационной безопасности. Реализована методика, позволяющая задать модель информационной системы с позиции информационной безопасности, идентифицировать риски, угрозы, потери в результате инцидентов.

Основные этапы работы:

- Описание контекста
- Риски
- Угрозы
- Потери
- Управляющие воздействия
- Контрмеры и план действий

Описание контекста

На этапе описания контекста описывается модель взаимодействия организации с внешним миром в нескольких аспектах: стратегическом, организационном, бизнес-цели, управление рисками, критерии.

Стратегический аспект описывает сильные и слабые стороны организации с внешних позиций, варианты развития, классы угроз и отношения с партнерами.

Организационный контекст описывает отношения внутри организации: стратегию, цели на организационном уровне, внутреннюю политику.

Контекст управления рисками описывает концепцию информационной безопасности.

Контекст бизнес-целей — основные бизнес-цели.

Критерии оценки — критерии оценки, используемые при управлении рисками.

Описание рисков

Задается матрица рисков (рис 4.6), в результате риски будут описаны в соответствии с определенным шаблоном и заданы связи этих рисков с другими элементами модели.

Риски оцениваются по качественной шкале и разделяются на приемлемые и неприемлемые (рис. 4.7) на основе простейшей модели.

Затем выбираются управляющие воздействия (контрмеры) с учетом зафиксированной ранее системы критериев, эффективности контрмер и их

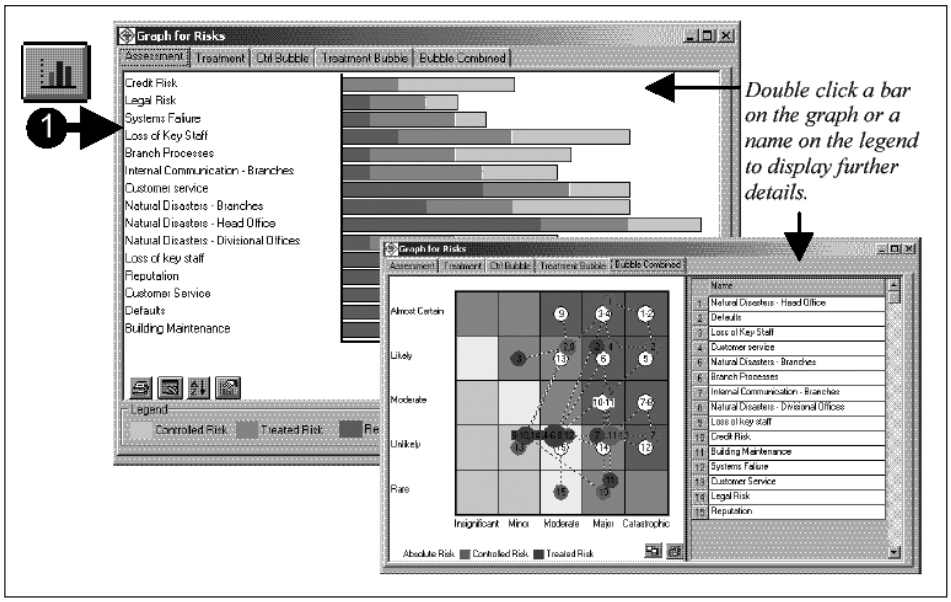

Рис. 4.8. Анализ результатов в Risk Advisor

стоимости. Стоимость и эффективность также оцениваются в качественных шкалах.

Описание угроз
В начале формируется список угроз. Угрозы определенным образом классифицируются, затем описывается связь между рисками и угрозами. Описание также делается на качественном уровне и позволяет зафиксировать их взаимосвязи.

Описание потерь
Описываются события (последствия), связанные с нарушением режима информационной безопасности. Потери оцениваются в выбранной системе критериев.

Анализ результатов
В результате построения модели можно сформировать подробный отчет (около100 разделов), посмотреть на экране агрегированные описания в виде графа рисков (рис. 4.8).

Оценка возможностей метода Risk Advisor
Данный инструмент позволяет документировать всевозможные аспекты, связанные с управлением риском, на верхних уровнях — административном и организационном. Программно-технические аспекты описывать в данной модели не очень удобно. Оценки даются в качественных шкалах, подробного анализа факторов рисков не предусмотрено.

Сильной стороной данного метода является возможность описания разноплановых взаимосвязей, адекватного учета многих факторов риска.

4.2.2 АванГард

В настоящее время на российском рынке продается отечественное ПО «АванГард», разработка института системного анализа РАН, подробное описание в [15].

«АванГард» позиционируется как экспертная система управления информационной безопасностью. Предлагаются две версии метода: «АванГард-Анализ» — для проведения анализа рисков, «АванГард-Контроль» — управление рисками. Структура и функции комплекса приводятся на рис. 4.9.

Данный программный комплекс обладает развитыми средствами для построения моделей информационных систем с позиции информационной безопасности. В нем, в отличие от описанного выше Risk Advisor, можно строить модели разных уровней (административного, организационного, программно-технического, физического) и разной степени абстракции.

Авторы метода постарались не вносить «внутрь» конкретные методики расчета составляющих элементов рисков. Риск (в терминах авторов размер риска) определяется как произведение ущерба (в терминах авторов цена риска) на вероятность риска. Исходные данные — ущерб и вероятность должны быть введены в модель. Существует справочная база данных, помогающая ЛПР в выборе этих значений, но процедура намеренно не формализована. Такой подход имеет свои достоинства и недостатки. Недостатком является то, что методологически сложный этап — выбор значений, которые к тому же должны быть измерены в количественных шкалах, полностью перекладывается на аналитика (пользователя). Какой-либо верификации значений не предполагается.

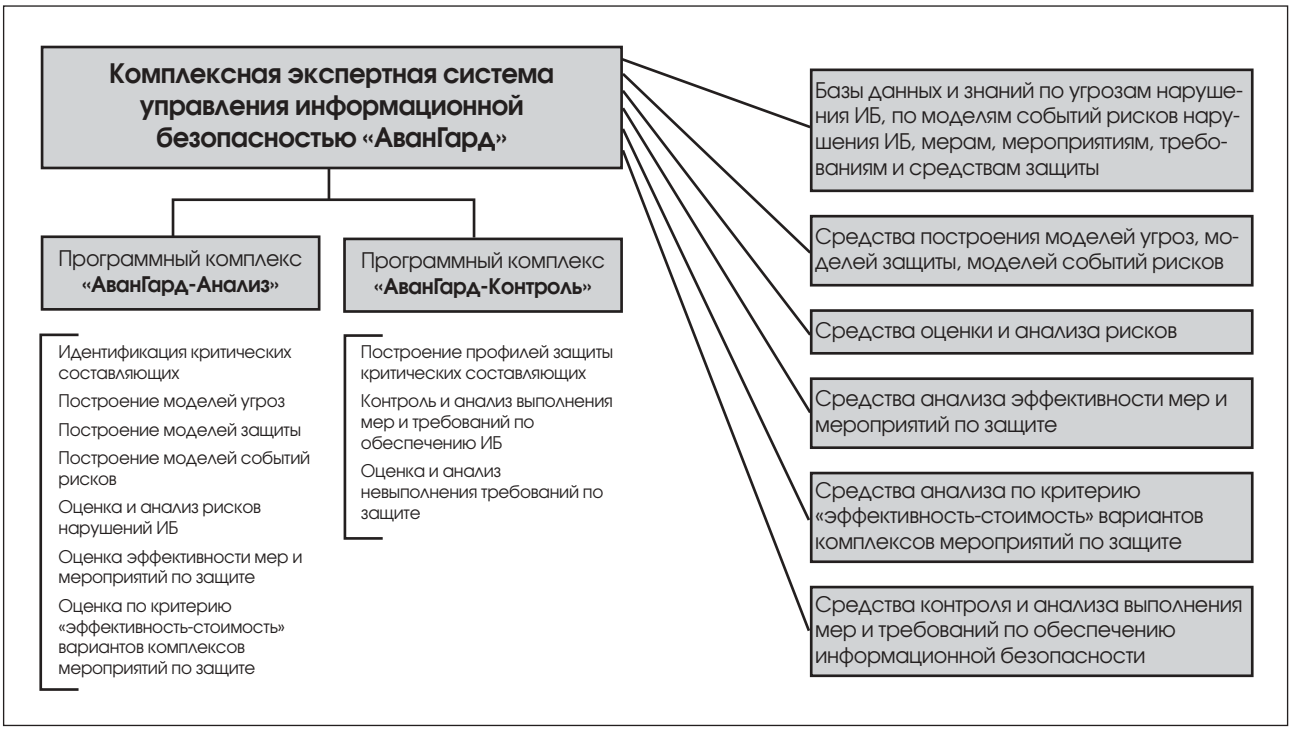

Рис. 4.9. Структура и функции «АванГард»

Другая особенность — базы данных заполняются информацией под конкретный заказ. Универсальной версии, рассчитанной на «среднего» потребителя не поставляется.

Таким образом, «АванГард» подходит для построения ведомственных методик анализа и управления рисками, но вряд ли его можно рассматривать как универсальный инструментарий аналитика.

4.2.3 RiskWatch

Компания RiskWatch [12] предлагает два продукта: один в области информационной безопасности, второй в области физической безопасности. ПО предназначено для идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в сфере компьютерной и «физической» безопасности предприятия.

В продукте, предназначенном для управления рисками в информационных системах, учитываются требования стандартов США (можно выбирать требуемый уровень защищенности). Кроме того, выпущена версия продукта RiskWatch RW17799®, соответствующая стандарту ISO 17799.

RiskWatch помогает провести анализ рисков и сделать обоснованный выбор мер и средств защиты. Используемая в программе методика включает в себя 4 фазы.

1) Первая фаза — определение предмета исследования. На данном этапе описываются параметры организации — тип организации, состав исследуемой системы, базовые требования в области безопасности (рис. 4.10). Описание формализуется в ряде подпунктов, которые можно выбрать для более подробного описания (рис. 4.11) или пропустить.
   Далее каждый из выбранных пунктов описывается подробно.
   Для облегчения работы аналитика в шаблонах даются списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно выбрать те, что реально присутствуют в организации.
   На рис. 4.11 приводится пример описания различных категорий ресурсов.
   Допускается модификация названий, описаний, а также добавление новых категорий. Это позволяет достаточно просто русифицировать данный метод.
2) Вторая фаза — ввод данных, описывающих конкретные характеристики системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей.
   На этом этапе:
   - Подробно описываются ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов;
   - Для выявления возможных уязвимостей используется опросник, база которого содержит более 600 вопросов. Вопросы связаны с категориями ресурсов. Допускается корректировка вопросов, исключение или добавление новых.

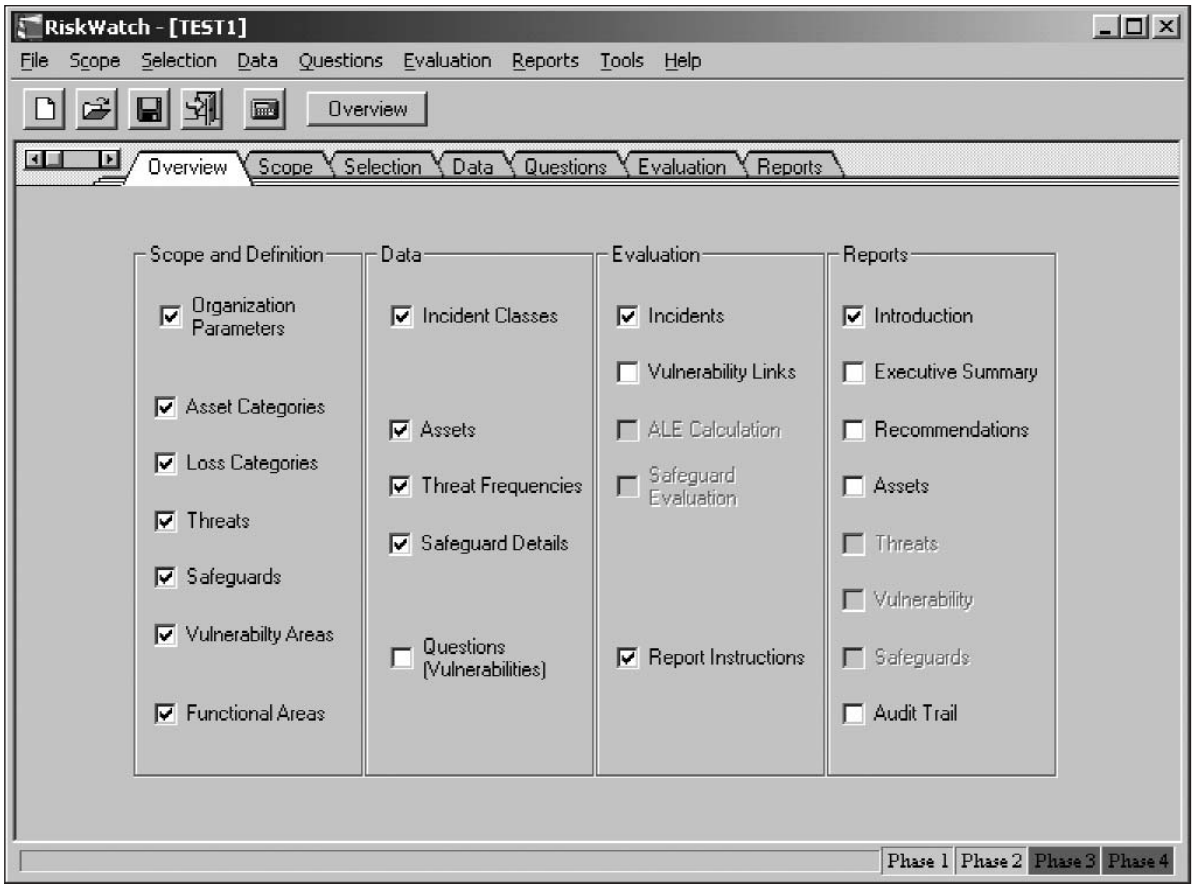

Рис. 4.10. Описание информационной системы с позиции безопасности в RiskWatch

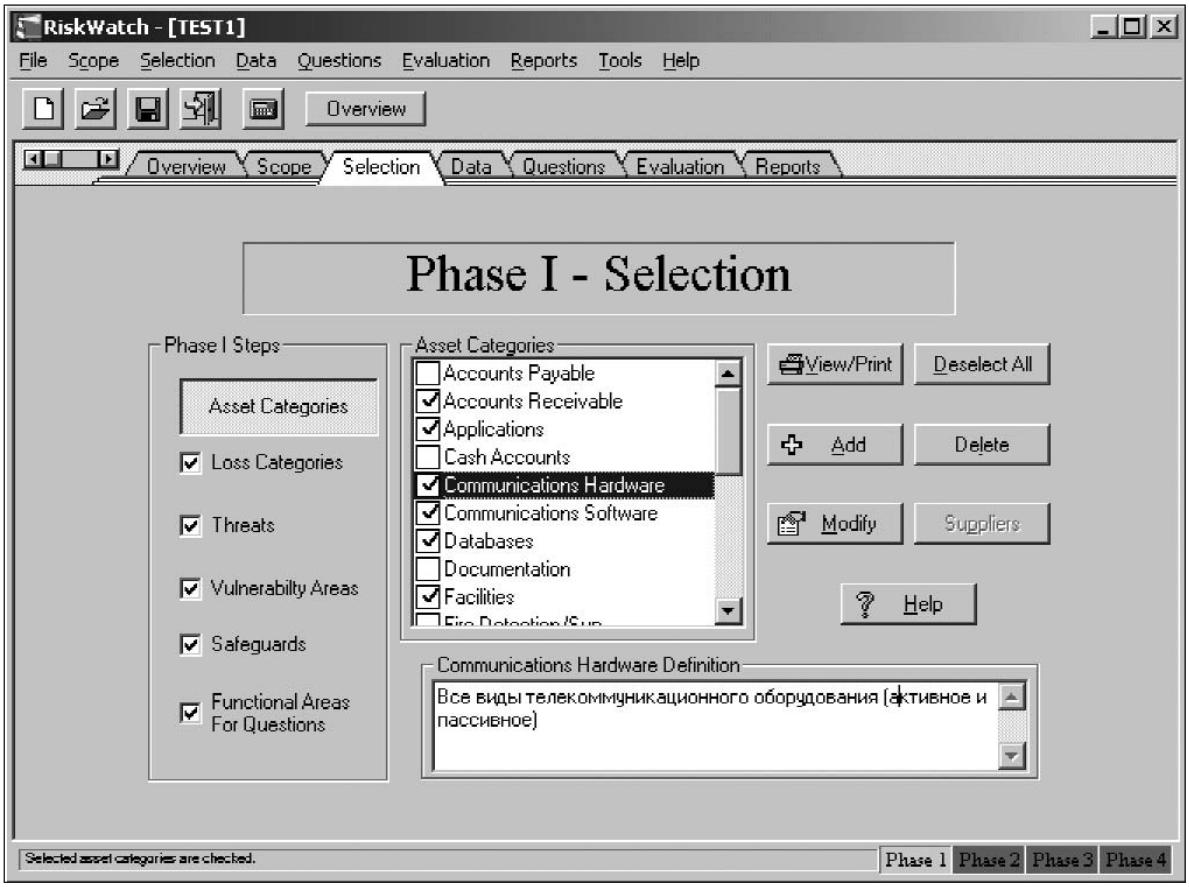

Рис. 4.11. Описание ресурсов информационной системы

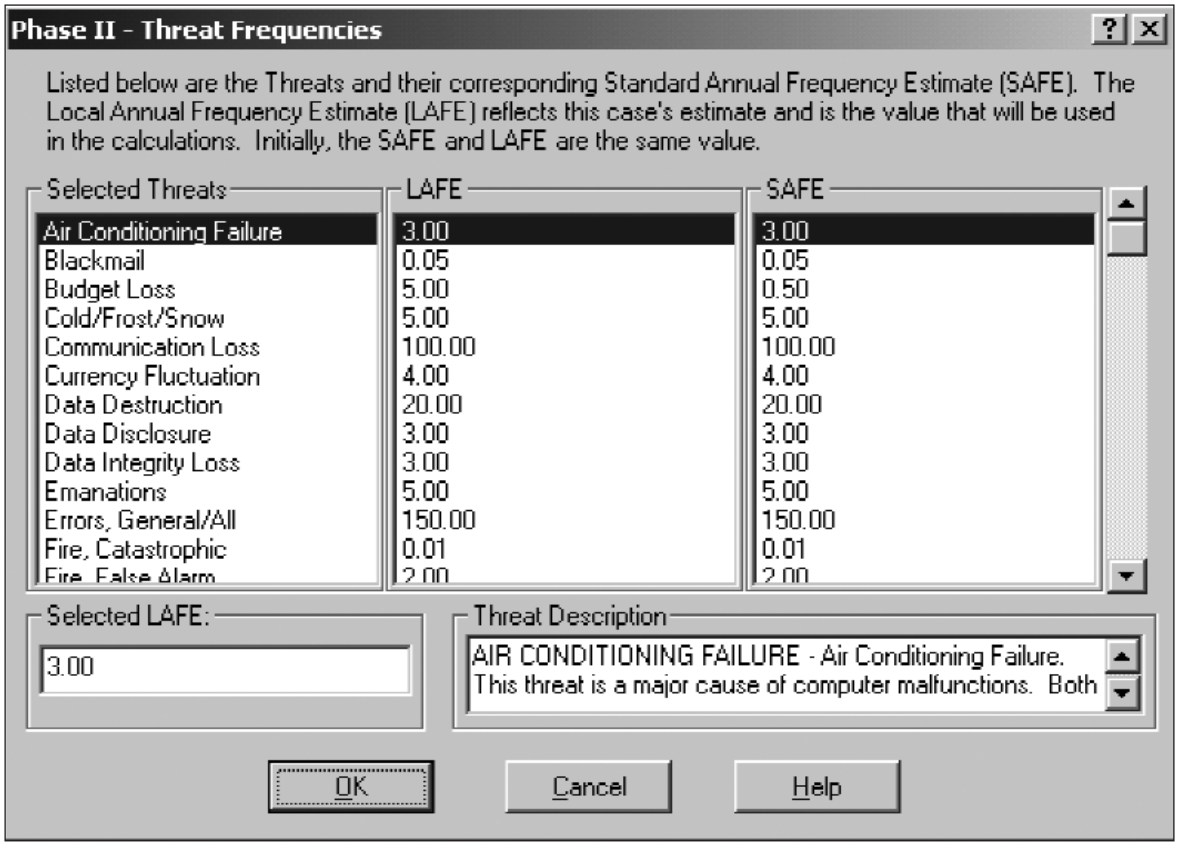

Рис 4.12. Оценка параметров угроз с использованием статистических данных

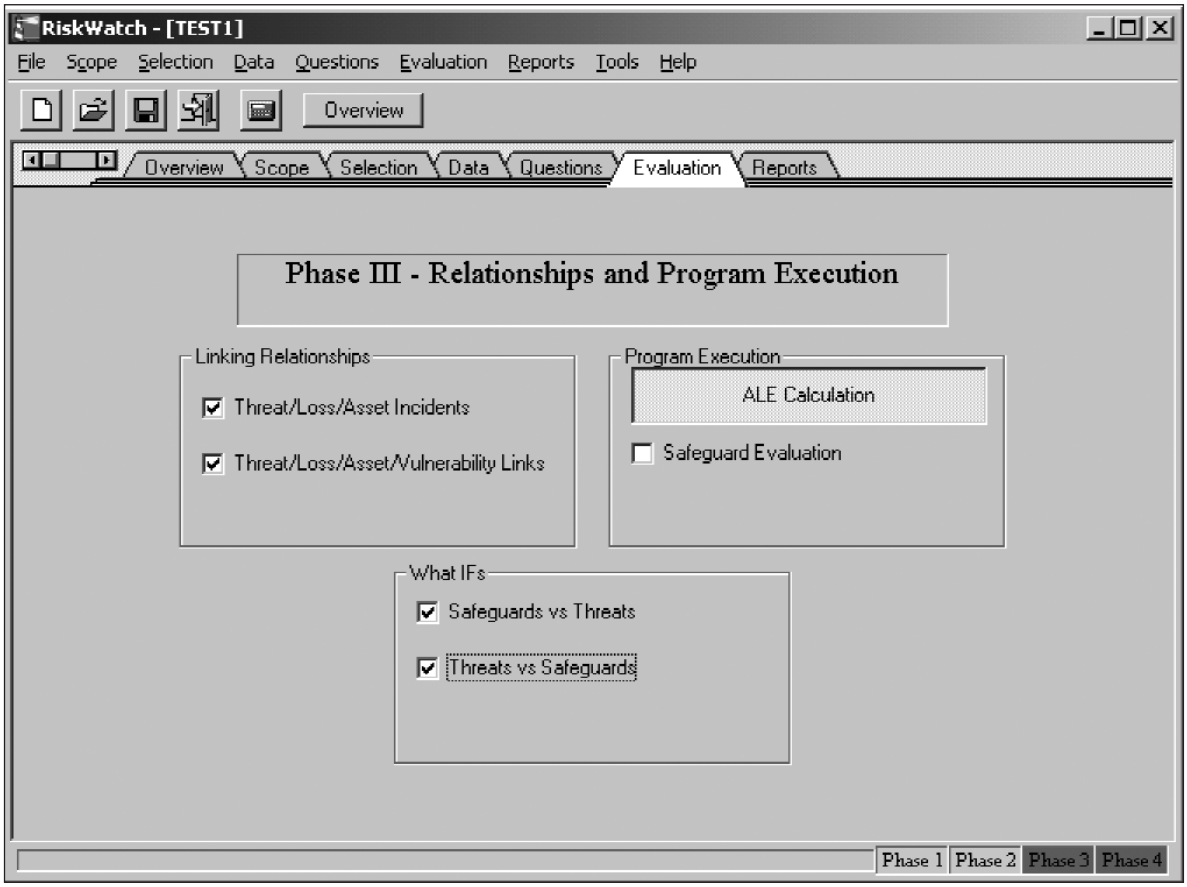

Рис. 4.13. Содержание третьей стадии в RiskWatch

Theft - Company Property - AFE: 2.00
The various incident classes associated with this threat are shown in the following table:

Incident Class	SLE	ALE	% of total ALE
Delays/Denials, Communications Equipment	$26,401.	$52,801.	68.0%
Delays/Denials, Data/Information	$4,400.	$8,800.	11.3%
Delays/Denials, Physical Inventory/Product	$2,750.	$5,500.	7.1%
Direct Loss, Cash	$2,200.	$4,400.	5.7%
Delays/Denials, Production Resources	$1,100.	$2,200.	2.8%
Direct Loss, Physical Inventory/Product	$1,100.	$2,200.	2.8%
Direct Loss, Data/Information	$550.	$1,100.	1.4%
Direct Loss, Production Resources	$275.	$550.	0.7%
Direct Loss, Communications Equipment	$39.	$77.	0.1%

Табл 6. Фрагмент отчета

- Задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Все это используется в дальнейшем для расчета эффективности внедрения средств защиты.

3) Третья фаза — оценка рисков. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих этапах.
   Для рисков рассчитываются математические ожидания потерь за год по формуле:

$$m = p * v$$

   где p — частота возникновения угрозы в течении года, v — стоимость ресурса, который подвергается угрозе.
   Например, если стоимость сервера $150000, а вероятность того, что он будет уничтожен пожаром в течение года равна 0.01, то ожидаемые потери составят $1500.
   Дополнительно рассматриваются сценарии «что если...», которые позволяют описать аналогичные ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при условии внедрения защитных мер и без них можно оценить эффект от таких мероприятий.
4) Четвертая фаза — генерация отчетов (Табл. 6). Типы отчетов:
   - Краткие итоги.
   - Полные и краткие отчеты об элементах, описанных на стадиях 1 и 2.
   - Отчет о стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз.
   - Отчет об угрозах и мерах противодействия.
   - Отчет о результатах аудита безопасности.

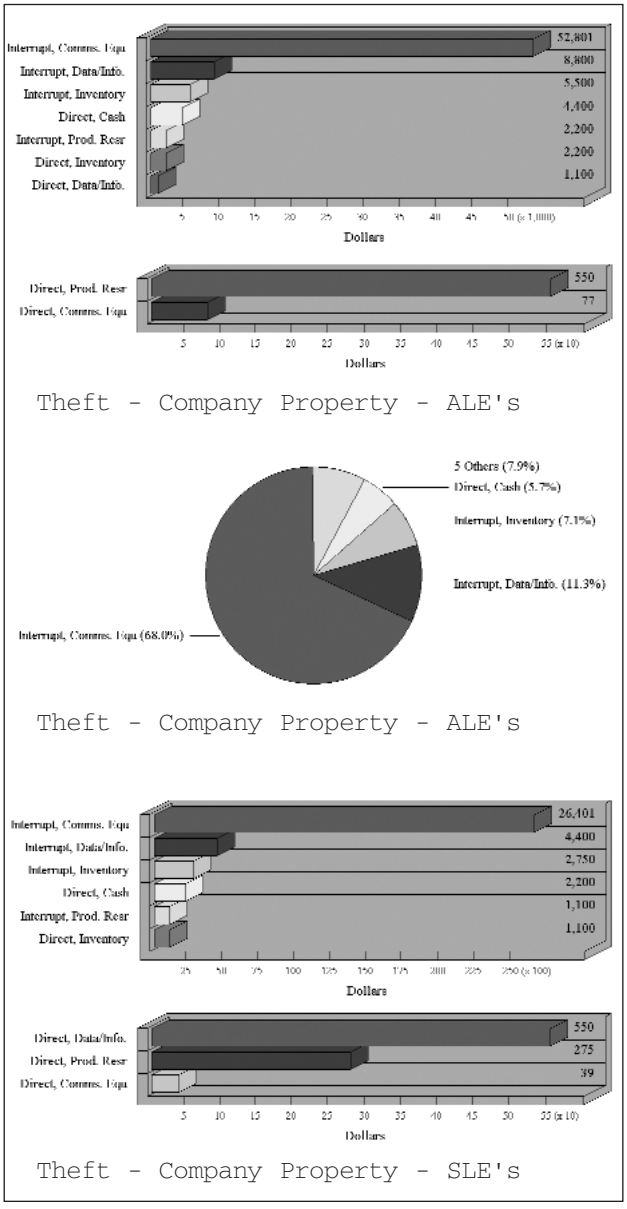

Рис. 4.14 Результирующие оценки по одной из угроз (кражи)

Возможности RiskWatch

В RiskWatch используется упрощенный подход, как к описанию модели информационной системы, так и оценке рисков.

Трудоемкость работ по анализу рисков с использованием этого метода сравнительно невелика. Такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов. Однако надо учитывать, что полученные оценки рисков (математическое ожидание

потерь) далеко не исчерпывает понимание риска с системных позиций.

Существенным достоинством RiskWatch с точки зрения отечественного потребителя является сравнительная простота, малая трудоемкость русификации и большая гибкость метода, обеспечиваемая возможностью введения новых категорий, описаний, вопросов и т.д. На основе этого метода отечественные разработчики могут создавать свои профили, учитывающие отечественные требования в области безопасности, разработать ведомственные методики анализа и управления рисками.

4.2.4 CRAMM

Метод анализа и управления рисками CRAMM, разработанный Британской правительственной организацией ССТА, в России в настоящее время используется несколькими компаниями — системными интеграторами.

Возможности версии CRAMM 3.2 были рассмотрены в [1]. Отличительными особенностями новой версии CRAMM 4.0 являются:

- Соответствие стандарту BS 7799 (ISO 17799).
- Увеличено количество возможных отчетов, добавлены возможности управления их содержанием.
- Добавлены новые классы информационных ресурсов.
- Существенно расширена база данных по контрмерам.

В области обеспечения соответствия стандарту BS 7799, наиболее важным нововведением является возможность генерации отчетов:

- Политика информационной безопасности.
- Система управления информационной безопасностью.
- План обеспечения бесперебойной работы.
- Ведомость соответствия.

Эти отчеты необходимы при проведении аудита информационной безопасности в соответствии с BS 7799. Метод CRAMM в настоящее время является наиболее часто используемым ПО, если требуется провести аудит в соответствии с требованиями Британского стандарта BS 7799.

Добавлено много новых средств, повышающих гибкость метода. В частности, добавлен ряд настроек, позволяющих лучше адаптировать его к решению конкретной задачи (рис. 4.15).

Его достоинствами являются использование технологии оценки угроз и уязвимостей по косвенным факторам с возможностью верификации результатов, удобная система моделирования информационной системы с позиции безопасности, обширная база данных по контрмерам. Данный метод является самым «мощным» и самым трудоемким из рассмотренных в данном обзоре, он позволяет весьма детально оценить риски и различные варианты контрмер.

Недостаток с позиции отечественного потребителя — сложность русификации и большой объем выходных документов (сотни страниц). Аналитик обычно вынужден на основе полученных документов сам писать отчет для заказчика.

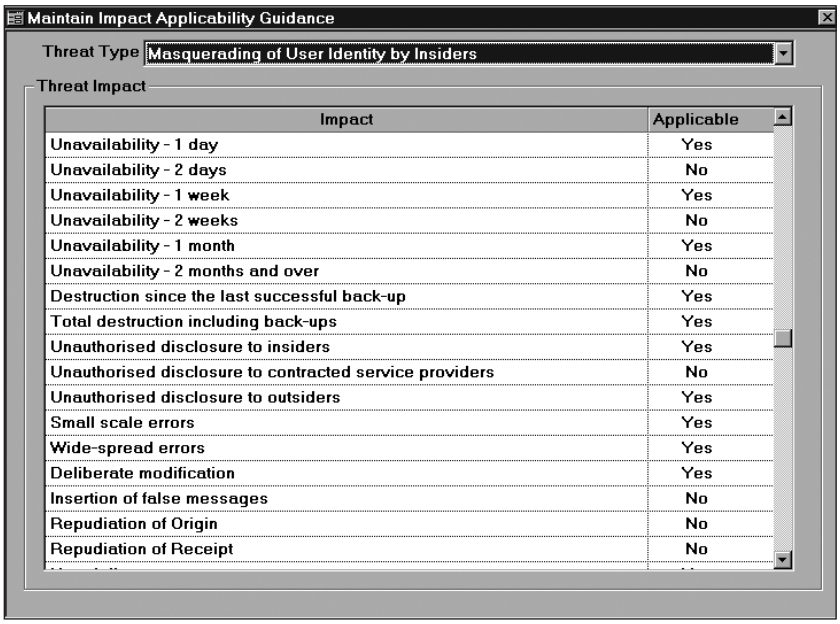

Рис 4.15. Дополнительные настройки в CRAMM 4.0: определение возможных последствий по типам угроз

Заключение

В организациях, достигнувших определенной степени зрелости, проведение анализа рисков и управление рисками на всех стадиях жизненного цикла информационной технологии являются обязательными элементами в системе мероприятий по обеспечению режима информационной безопасности. Требования к проведению этих этапов, предъявляемые разными организациями, различаются и находятся в широких пределах. Соответственно используются различные технологии анализа рисков.

Разработка методик анализа рисков связана с рядом методологических сложностей. Наибольшую сложность представляют:

- Разработка корректных процедур измерения рисков.
- Построение модели информационной технологии с системных позиций, учитывающей разноплановые факторы, относящиеся к организационному, процедурному, программно-техническому уровням, а также их взаимосвязи.

В настоящее время на рынке имеется ПО, реализующее различные методики анализа рисков. Это ПО можно использовать в качестве инструментария аналитика. Однако одного «лучшего» универсального метода не существует, в каждом случае требуется выбирать подходящее ПО и настраивать его в соответствии со спецификой объекта исследования. По этой причине «бумажные» методики весьма распространены.

В России технологии анализа рисков и управления рисками начали применяться на практике. Многие фирмы, специализирующиеся в вопросах информационной безопасности, предлагают услуги в этой области. Однако объективно оценить качество используемых методик, качество проведенных исследований сложно, поскольку отечественных стандартов (типа BS 7799) в этой области не существует.

Приложение

Определения основных терминов, относящиеся к тематике анализа рисков, управления рисками

Ниже приводятся определения основных терминов по тематике анализа рисков, используемые различными авторами и организациями.

Терминология и определения в публикациях на русском языке.

Базовый (Baseline) анализ рисков [1] — анализ рисков, проводимый в соответствии с требованиями базового уровня защищенности. Прикладные методы анализа рисков, ориентированные на данный уровень, обычно не рассматривают ценность ресурсов и не оценивают эффективность контрмер. Методы данного класса применяются в случаях, когда к информационной системе не предъявляется повышенных требований в области информационной безопасности.

Полный (Full) анализ рисков [1] — анализ рисков для информационных систем, предъявляющих повышенные требования в области ИБ (более высокие, чем базовый уровень защищенности). Это предполагает:

- определение ценности ресурсов;
- оценку угроз и уязвимостей;
- выбор адекватных контрмер, оценку их эффективности.

Угроза (Threat) [1] — совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности.

Угроза ИБ [Threat] [14] — возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и/или потери информации.

Источник угрозы [14] — это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Последствия (атака) [14] — это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).
Как видно из определения, атака — это всегда пара «источник — фактор», реализующая угрозу и приводящая к ущербу.

Уязвимость (Vulnerability) [1] — слабость в системе защиты, которая делает возможной реализацию угрозы.

Уязвимость (фактор) [Vulnerability] [14] Присущие *объекту* причины, приводящие к нарушению безопасности информации и обусловленные недостатками процесса функционирования *объекта*, свойствами архитектуры АС, протоколами обмена и интерфейсами, применяемыми ПО и аппаратной платформой, условиями эксплуатации.

Анализ рисков[1] — процесс определения угроз, уязвимостей, возможного ущерба, а также контрмер.

Терминология и определения на английском языке. Определения взяты из глоссария [16] и даются в переводе.

Риск (risk)

- Ожидаемые потери или возможный результат реализации угрозы при наличии уязвимости и определенных обстоятельств или событий, приводящих к реализации угрозы. [FCv1], [AJP].
- Возможность того, что определенная угроза реализуется вследствие наличия определенной уязвимости системы. [AJP].
- Вероятность потерь вследствие того, что определенная угроза при наличии определенной уязвимости реализуется и приведет к негативным последствиям. [RFC2828].
- Возможность потери из-за одной или более угроз для информационных ресурсов (не путать с финансовым или деловым риском) [RFC2828].
- Ситуация, в которой существует уязвимость и потенциальный нарушитель имеет возможность и желание воспользоваться ею. [IATF] .
- Возможность того, что специфическая уязвимость будет использована. [AFSEC].
- Потенциал, который данная угроза имеет вследствие наличия уязвимости информационных ресурсов. В результате реализации этого потенциала организации может быть причинен вред. [ISO/IEC PDTR 13335-1 (11/2001)] [SC27].
- Вероятность того, что специфическая угроза реализуется вследствие наличия специфической уязвимости системы. [NCSC/TG004].

Анализ риска (risk analysis)

- Процесс идентификации рисков, определение их величины и выделение областей, требующих защиты. Анализ риска — часть управления рисками. [AJP] [NCSC/TG004].
- Систематический процесс оценки величины рисков. [ISO/IEC PDTR 13335-1 (11/2001)] [SC27].

Оценка риска (risk assessment)

- Процесс идентификации информационных ресурсов системы и угроз этим ресурсам, возможных потерь (то есть потенциал потери) основанный на оценке частоты возникновения событий и размере ущерба. Рекомендуется перед введением новых информационных ресурсов выбрать контрмеры, позволяющие минимизировать возможные потери. [RFC2828].
- (C) Составление списка рисков, ранжированных по цене и критичности. Список позволяет определить, где контрмеры должны применяться в первую очередь. Обычно невозможно предложить контрмеры, снижающие все аспекты рисков до нуля, и некоторые остаточные риски останутся даже после того, как все доступные (по цене) контрмеры были применены. [FP031, R2196] [RFC2828].
- Изучение уязвимостей, угроз, вероятности, возможных потерь и теоретической эффективности контрмер. Чтобы определить ожидаемые потери и установить степень их приемлемости, процесс оценки угроз и уязвимости описывается в общедоступной методике, ставшей стандартом де-факто. [NSAINT].
- Процесс, в который входят: идентификация риска, анализ риска, оценка риска. [ISO/IEC PDTR 13335-1 (11/2001)].
- Оценка угроз, воздействия на уязвимости информационных ресурсов и информационных процессов а также вероятности их возникновения ISO/IEC 17799: 2000] [SC27].

Идентификация риска — процесс идентификации рисков, при котором рассматриваются бизнес-цели, угрозы и уязвимость, как основа для дальнейшего анализа. [ISO/IEC PDTR 13335-1 (11/2001)] [SC27].

Управление рисками (risk management)

- Процесс идентификации, управления, устранения или уменьшения вероятности событий, которые могут негативно воздействовать на системные ресурсы системы. [RFC2828] .
- Процесс, включающий идентификацию, управление и устранение или уменьшение вероятности событий, которые могут затрагивать информационные ресурсы системы. [ISO/IEC PDTR 13335-1 (11/2001)].
- Процесс идентификации, управления и уменьшения рисков безопасности, которые могут воздействовать на информационную систему при условии приемлемой стоимости комплекса. [ISO/IEC 17799: 2000] [SC27] .

- Процесс идентификации, управления, устранения или уменьшения вероятности событий, которые могут негативно воздействовать на системные ресурсы системы. Этот процесс включает анализ риска, анализ стоимость/эффективность, выбор, построение и испытание подсистемы безопасности и исследование всех аспектов безопасности. [AJP] [NCSC/TG004].
- Процесс идентификации, управления, устранения или уменьшения потенциального воздействия возможных происшествий. Цель процедуры управления риском состоит в том, чтобы уменьшить риски до уровней, одобренных DAA (Designated Approving Authority — лицо, уполномоченное выбрать уровни рисков). [NSAINT] [AFSEC].

Учет рисков (risk treatment) процесс планирования системы управления рисками, основанный на оценке рисков. [ISO/IEC PDTR 13335-1 (11/2001)] [SC27] .

Уязвимость (vulnerability)

- Слабость в защите, которая может быть объектом воздействия (например, из-за неверно проведенного анализа, планирования или реализации системы защиты).
- Слабость в информационной системе или ее компонентах (например, системные процедуры защиты, аппаратная реализация или внутренние средства управления), которые могут способствовать реализации негативных событий, связанных с информацией.
- Слабость в процедурах защиты, проектировании информационной системы, реализации системы, внутренней системе управления и так далее, которая может способствовать нарушению политики информационной безопасности. [AJP].
- Недостатки или бреши на этапе проектирования информационной системы, реализации или управления, которые могли стать причиной нарушения политики информационной безопасности. [RFC2828].
- (C) Большинство систем имеют уязвимости в программном обеспечении, но из этого не следует, что информационные системы нельзя использовать по причине их возможных брешей. Не каждая угроза в случае ее реализации или атака приведет к успеху. Успех зависит от степени уязвимости, потенциала угрозы (атаки) и эффективности используемых контрмер. Если для реализации угрозы необходимо наличие уязвимости, которая практически не возникает, тогда с существованием уязвимости можно примириться. Если потенциальная выгода от осуществления атаки невелика, тогда может быть терпима даже уязвимость, которую можно легко использовать. Но если некоторый тип атаки хорошо известен и потенциально легко осуществим для большого числа пользователей, тогда, вероятно, найдется желающий осуществить нападение. [RFC2828].
- Слабость защиты в объекте потенциальной атаки (например, из-за недоработок на стадиях анализа, проектирования, построения системы или эксплуатации). [ITSEC].
- Уязвимость — существование слабости, ошибок проектирования или построения системы, которые могут вести к неожиданному, нежелательному событию, компрометирующему систему информационной безопасности, сети, приложения или протоколы. [RFC2504].
- Слабость в информационной системе или компонентах (например, процедуры обеспечения безопасности на системном уровне, проектные решения на аппаратном уровне, система управления), которые могут быть использованы, чтобы реализовать угрозу, связанную с информационными ресурсами. [FCv1].
- Слабость в процедурах обеспечения безопасности, системном проекте, реализации, системе управления и т.д, которая может случайно или преднамеренно привести к нарушению политики информационной безопасности. Условие или слабость в процедурах обеспечения информационной безопасности, системе управления техническими средствами, физической защите, которые способствуют реализации угрозы. [SRV-BOOKS].
- Слабость в процедурах обеспечения безопасности, системном проекте, реализации, системе управления и т.д., которая может способствовать нарушению политики безопасности. [NCSC/TG004].
- Слабость ресурса или группы ресурсов информационной системы, которая может способствовать реализации угрозы. [SC27] [ISO/IEC PDTR 13335-1 (11/2001)].
- Аппаратные средства, программное обеспечение и потоки данных составляют систему обработки информации. Слабости в автоматизированных системах обеспечения информационной безопасности на программно-техническом уровне, системе административного управления, размещении оборудования и т.д, которые могут приводить к реализации угроз несанкционированного доступа к информации или привести к нарушениям в критически важном про-

цессе обработки информации. [AFSEC] [NSAINT].

Анализ уязвимости (vulnerability analysis)

- Систематически проводимая экспертиза информационной системы, позволяющая определить адекватность мер защиты, идентифицировать погрешности в построении защиты, собрать исходные данные, чтобы оценить эффективность предложенных мер защиты и подтверждать адекватность таких мер после их реализации. [NSAINT] [AFSEC].
- Систематически проводимая экспертиза информационной системы, позволяющая определить адекватность мер защиты, идентифицировать погрешности в построении защиты, собрать исходные данные, чтобы оценить эффективность предложенных мер защиты. [SRVBOOKS. [AJP] [NCSC/TG004].

Объект оценки (Target of Evaluation (TOE))

- Отдельные элементы информационной системы, результаты ее работы или вся система в целом, включая администратора, пользовательскую документацию и руководства, которая является объектом оценки. [CC2] [CC21] [IATF] [ISO/IEC 15408-1: 1999] [SC27].
- Отдельные элементы информационной системы, результаты ее работы или вся система в целом, которая рассматривается на предмет оценки защищенности. [AJP] [CC1] [ITSEC].

Оценка уязвимости (vulnerability assessment)

- Аспект оценки эффективности защиты объекта оценки (TOE), а именно: могла ли определенная уязвимость в объекте оценки на практике компрометировать (поставить под угрозу) его защиту. [ITSEC].
- Измерение уязвимости, которая включает восприимчивость исследуемой системы к определенному виду атаки и возможность агента угрозы осуществить нападение. [AJP] [SRVBOOKS] [NCSC/TG004].

Угроза (threat)

- Действие или событие, которое может нанести ущерб безопасности.
- Последовательность обстоятельств и событий, которые позволяют человеку или другому агенту воспользоваться уязвимостью информационной системы и причинять ущерб информационным ресурсам. [AJP] [FCv1].
- Любое обстоятельство или события, которые потенциально могут причинить вред информационной системе в форме разрушения, раскрытия, модификации данных или отказа в обслуживании (DoS). [AJP].
- (I) потенциал для нарушения режима безопасности, который существует, когда складываются обстоятельства, производятся определенные действия или происходят события, которые могут нарушать режим безопасности и причинять вред.
- (C) возможная опасность, которая может иметь место в случае использования уязвимости. Угроза может быть либо 'умышленной' (т.е. задумана и спланирована, например, хакером или преступной организацией) или 'случайной' (например, результат сбоев компьютера или возможности 'стихийного бедствия' типа землетрясения, пожара, торнадо).
- В некоторых контекстах, типа следующего, термин «Угроза» используется узко и относится только к умышленным угрозам:
  - (N) В американских (U.S.) правительственных документах: способность враждебного юридического лица обнаруживать, эксплуатировать или выводить из строя дружественные информационные системы и намерение данного юридического лица (демонстрируемое или предполагаемое) заняться такой деятельностью. [RFC2828].
- Потенциальная причина нежелательного инцидента, который может кончаться причинением ущерба информационной системе или организации. [SC27] . [ISO/IEC PDTR 13335-1 (11/2001)].
- Действие или случай, который мог бы нанести ущерб системе защиты. [ITSEC].
- Любое обстоятельство или случай, потенциально способные причинить вред системе в форме разрушения, раскрытия, модификации данных или отказа в обслуживании (DoS). [NCSC/TG004] [SRVBOOKS].
- Потенциал для реализации уязвимости. [SRVBOOKS].
- Объект или события, которые потенциально могут навредить системе. [SRVBOOKS].
- Способности, намерения, и методы нападения противников, имеющих возможность воспользоваться совокупностью обстоятельств, позволяющих использовать имеющийся потенциал для причинения вреда информации или информационной системе. [IATF].
- Средства, при помощи которых агент угрозы намеривается причинить ущерб информационной системе, отдельным информационным ресурсам или операциям. [AFSEC] [NSAINT].
- Потенциально возможное нарушение защиты. [AFSEC] [NSAINT].

- Потенциал реализации уязвимости, имеющий последствием компрометацию защиты системы или сетей. Даже если уязвимость не известна, это представляет угрозу в соответствии с этим определением. [RFC2504].

Действие угрозы (threat action)

- Нападение на системную защиту. [RFC2828].
- Правильно построенная архитектура подсистемы информационной безопасности должна быть рассчитана на следующие виды воздействий:
  - Нападения.
  - Случайные события.
- Различные виды возможных воздействий угрозы определяются как подклассы 'множества последствий угрозы'. [RFC2828].

Агент угрозы (threat agent)

- Метод, использующий уязвимость в системе, операциях (технологическом процессе) или отдельных средствах (элементах системы). [AJP] [NCSC/TG004] [SRVBOOKS].
- Методы и средства, основанные на использовании уязвимостей в информационной системе, операциях или средстве; пожар, природные катаклизмы и т.д. [AFSEC] [NSAINT].

Анализ угрозы (threat analysis)

- Оценка вероятности событий и анализ возможных последствий разрушительных действий к системе. [RFC2828].
- Экспертиза всех действий и событий, которые могли бы неблагоприятно воздействовать на систему или результат ее функционирования. [AFSEC] [AJP] [NCSC/TG004] [SRVBOOKS].

Процесс оценки угрозы (threat assessment) — процесс формальной оценки степени серьезности угрозы информационной системе и описание характера угрозы. [AFSEC] [NSAINT].

Литература

[1] С. Симонов. Анализ рисков, управление рисками. — Jet Info, 1, 1999

[2] С.В. Симонов. Методология анализа рисков в информационных системах «Конфидент» , № 1, 2001

[3] С.В. Симонов. Анализ рисков в информационных системах. Практические аспекты. «Конфидент» , № 2, 2001

[4] Обзор модели приводится на http://krylov.lib.ru/maturity_man.html

[5] Risk Management Guide for Information Technology Systems, NIST, Special Publication 800-30

[6] Anne Marie Willhite Systems Engineering at MITRE Risk Management MP96B0000120, R1 September 1998 http://www.mitre.org/resources/centers/sepo/risk/sys_eng_mitre.html

[7] Risk Matrix http://www.mitre.org/resources/centers/sepo/risk/risk_matrix.html

[8] Петренко С.А., Симонов С.В. Анализ и управление информационными рисками. «АйТи» 2003 (в печати)

[9] The ISO 17799 Service & Software Directory http://www.iso17799software.com

[10] Сайт компании MethodWare http://www.methodware.com

[11] http://www.computer-security-policies.com

[12] Сайт компании RiskWatch http://www.riskwatch.com.

[13] RA Software Tool Демо -версия метода: http://www.aexis.de/RA%20ToolPage.htm

[14] С. В. Вихорев, Р. Ю. Кобцев. Как узнать — откуда напасть или откуда исходит угроза безопасности информации. Конфидент, № 2 2002

[15] А. Кононов. Страхование нового века. Как повысить безопасность информационной инфраструктуры. // M. Connect № 12, 2001

[16] Глоссарий терминов по информационной безопасности http://www.garlic.com/~lynn/secure.htm

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Овчинникова Г.Ю. *(galya@jet.msk.su)*
Россия, 127006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати **32555**