Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 12 (163)/2006

Управление рисками: обзор употребительных подходов

Часть II

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Управление рисками: обзор употребительных подходов

СОДЕРЖАНИЕ

Детальное рассмотрение процесса оценки рисков 2

- **Определение характеристик информационной системы 2**
- **Идентификация уязвимостей 5**
- **Идентификация угроз 5**
- **Анализ регуляторов безопасности 5**
- **Определение вероятностей 5**
- **Анализ воздействия 6**
- **Определение рисков 6**
- **Рекомендуемые контрмеры 6**
- **Результирующая документация 6**

Нейтрализация рисков 6

Возможный формат отчета об оценке рисков 8

Возможный формат плана реализации контрмер 8

Возможные трактовки и способы вычисления рисков 8

Заключение 19

Детальное рассмотрение процесса оценки рисков

Процесс оценки рисков можно подразделить на девять основных этапов:

- определение характеристик информационной системы;
- идентификация уязвимостей;
- идентификация угроз;
- анализ регуляторов безопасности;
- определение вероятностей;
- анализ воздействий;
- определение рисков;
- рекомендуемые контрмеры;
- результирующая документация.

Идентификация уязвимостей и угроз, а также анализ регуляторов безопасности и воздействий могут выполняться относительно независимо и параллельно после того, как завершен первый этап и определены характеристики информационной системы.

На рис. 6.1 показаны основные этапы процесса оценки рисков вместе с входной и выходной информацией для каждого из них.

Опишем выделенные этапы более детально.

Определение характеристик информационной системы

Первым шагом в процессе оценки рисков является определение объекта оценки, то есть границ анализируемой информационной системы, а также ресурсов и информации, образующих ИС.

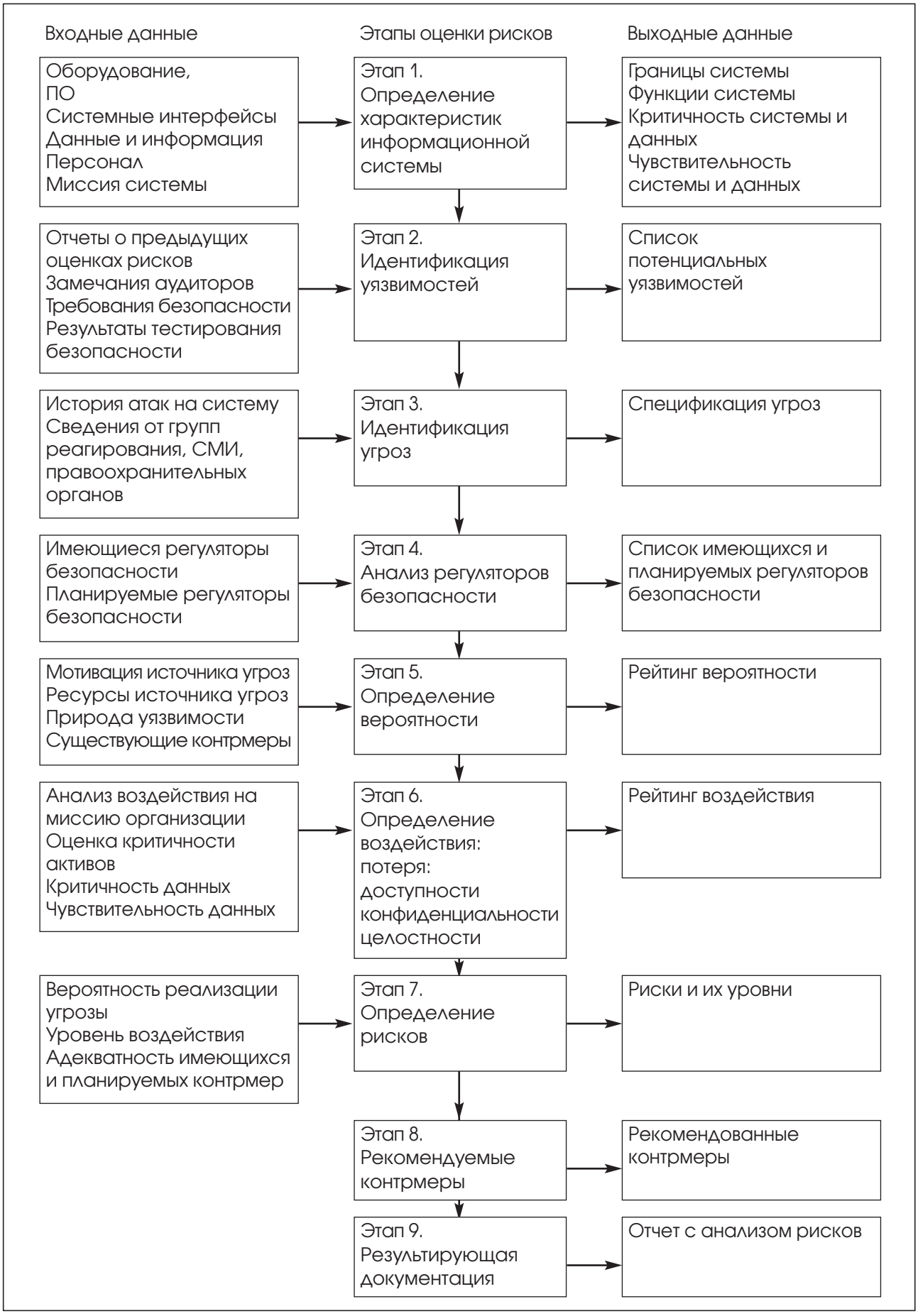

Рис. 6.1. Основные этапы процесса оценки рисков, их входная и выходная информация.

О системе необходимо собрать следующую информацию:

- архитектура ИС;
- используемое аппаратное обеспечение;
- используемое программное обеспечение;
- системные интерфейсы (внутренняя и внешняя связность);
- топология сети;
- присутствующие в системе данные и информация;
- поддерживающий персонал и пользователи;
- миссия системы (то есть процессы, выполняемые ИС);
- критичность системы и данных;
- чувствительность (то есть требуемый уровень защищенности) системы и данных.

Требуется также собрать информацию об эксплуатационном окружении системы:

- функциональные требования к ИС;
- политики безопасности, положения которых затрагивают ИС;
- меры защиты доступности, конфиденциальности и целостности хранимых данных;
- потоки данных, принадлежащих системе, входные и выходные данные;
- существующие программно-технические регуляторы безопасности (то есть встроенные или дополнительные защитные средства, поддерживающие идентификацию и аутентификацию, управление доступом, протоколирование и аудит, защиту остаточной информации, криптографические функции и т.д.);
- существующие регуляторы безопасности административного уровня (политика и программы безопасности, меры планирования безопасности, правила поведения и т.п.);
- существующие регуляторы безопасности процедурного уровня (кадровая безопасность, процедуры управления пользователями, управление разделением обязанностей пользователей, обеспечение бесперебойной работы, резервное копирование, хранение данных вне производственных площадей, восстановление после аварий, сопровождение системы);
- меры физической защиты ИС (физическая защита производственных площадей, контроль доступа в центр обработки данных и т.п.);
- защита ИС от угроз со стороны окружающей среды (средства контроля температуры, влажности, загрязнения, электропитание, водоснабжение и т.д.).

Если информационная система находится в стадии инициации или проектирования, необходимые сведения могут быть получены из проектной документации или спецификаций (требований). Если система находится в стадии разработки, необходимо определить ключевые правила и атрибуты безопасности, которые предполагается реализовать. В таком случае полезными источниками информации являются проектная документация и план обеспечения информационной безопасности.

Для информационных систем, находящихся в производственной эксплуатации, собираются сведения об их эксплуатационном окружении, включая данные о конфигурации системы, ее связности, документированных и недокументированных процедурах и сложившейся практике эксплуатации. Таким образом, описание системы может основываться на мерах безопасности, реализованных в рамках существующей инфраструктуры, или на имеющихся планах повышения уровня безопасности ИС.

Для сбора сведений об информационной системы в пределах ее эксплуатационных границ могут использоваться следующие методы.

Вопросники. Они могут касаться прежде всего административных и процедурных регуляторов безопасности, существующих или планируемых. Вопросники распространяются среди административного и технического персонала, проектирующего и/или обслуживающего систему.

Интервью. Обычно беседы проводятся у заказчика с административным и техническим персоналом и концентрируются на темах эксплуатации и управления. Кроме того, визиты к заказчику позволяют увидеть и оценить меры физической и эксплуатационной безопасности, защиту от угроз со стороны окружающей среды.

Просмотр документации. Политика безопасности, нормативные документы, техническая документация (например, руководства пользователя и администратора, требования безопасности, архитектурная и закупочная документация), предыдущие отчеты по оценке рисков, анализ воздействий на миссию организации, оценка критичности ресурсов, результаты аудита и тестирования, планы безопасности и т.п. — ценный источник информации о существующих и планируемых регуляторах безопасности, о степени критичности и чувствительности систем и данных.

Применение инструментов автоматического сканирования. Проактивные технические средства, такие как инструменты автообнаружения и анализа защищенности, позволяют эффективно собирать системную информацию, строить карту информационной системы, получать профили отдельных хостов и подсистем.

Идентификация уязвимостей

Напомним определение: уязвимость — это дефект или слабое место в системных защитных процедурах, проекте, реализации или внутренних регуляторах безопасности, которые могут проявиться (будучи случайно активизированы или умышленно проэксплуатированы) и привести к нарушению безопасности или отступлению от политики безопасности.

Анализ угроз ИС включает анализ уязвимостей информационной системы и ее окружения. Цель данного шага — получить список рассматриваемых уязвимостей.

Для достижения поставленной цели рекомендуется использовать источники информации об уязвимостях, проводить тестирование защищенности ИС, применять контрольные перечни с требованиями безопасности.

Типы рассматриваемых уязвимостей и методы их выявления зависят от специфики информационной системы и этапа жизненного цикла, на котором она находится.

На стадии проектирования ИС основное внимание уделяется требованиям безопасности, политике безопасности организации, планируемым процедурам, анализу доступных защитных средств.

На этапе реализации привлекается дополнительная, конкретная информация, например, предусмотренные проектом средства безопасности, результаты анализа проекта и т.д.

На этапе эксплуатации производится анализ имеющихся защитных средств, регуляторов безопасности, программно-технических и организационных.

Технические и организационные уязвимости могут быть выявлены посредством применения методов сбора информации о характеристиках информационной системы. Предварительно проведенный обзор источников информации об уязвимостях, таких как сайты производителей и групп реагирования, помогает подготовить вопросники и контрольные перечни, целенаправленно проводить интервью.

Тестирование является проактивным средством безопасности. Тестовый инструментарий включает:

- автоматические средства сканирования;
- средства тестирования и оценки;
- тестирование проникновением.

Идентификация угроз

К идентификации угроз можно подходить двояко, отправляясь либо от уязвимостей ИС, либо от возможных источников угроз. Уязвимости рассматривались выше, сосредоточимся теперь на источниках угроз, которые можно подразделить на природные, людские и принадлежащие окружению ИС.

К числу природных угроз принадлежат наводнения, землетрясения, ураганы, обвалы, лавины, грозы и другие стихийные бедствия.

От людей могут исходить случайные и умышленные действия. К числу первых принадлежат ошибки и упущения, к числу вторых — сетевые атаки, внедрение вредоносного программного обеспечения, несанкционированный доступ и т.п.

В роли внешних злоумышленников могут выступать хакеры, преступники, террористы и шпионы. У каждой из выделенных категорий свой уровень мотивации (нарастающий от хакеров к шпионам) и вооруженности ресурсами. Внутренними злоумышленниками могут быть как плохо подготовленные, так и обиженные или уволенные сотрудники. Внешний злоумышленник может стать внутренним, если ему удастся взломать систему и начать действовать от имени легального пользователя.

От окружения ИС могут исходить угрозы долговременного отключения электропитания, загрязнение окружающей среды, разного рода утечки и протечки и т.п. Как показывает опыт, возможны и более серьезные происшествия — обрушение зданий, взрыв газа и т.п.

С практической точки зрения угроз и их источников бесконечного много, однако, с другой стороны, весьма важна полнота их идентификации, так как неожиданные угрозы наносят особенно крупный ущерб. Например, информационной системе, расположенной в пустыне, не грозит природное наводнение, однако разрыв водопроводной трубы может привести к затоплению ИС, так что угроза затопления должна входить в число рассматриваемых.

Анализ регуляторов безопасности

Основная цель анализа регуляторов безопасности — определить, удовлетворяют ли существующие и планируемые контрмеры предъявляемым к ИС требованиям безопасности. Попутно определяются вероятности реализации идентифицированных угроз с учетом нейтрализующего действия регуляторов безопасности.

Определение вероятностей

При определении вероятности того, что потенциальная уязвимость может быть использована

в конкретном окружении, необходимо рассмотреть следующие факторы:

- мотивация и вооруженность ресурсами источника угрозы;
- природа уязвимости;
- наличие и эффективность контрмер.

Вероятность можно оценить по трехбалльной шкале как низкую, умеренную или высокую.

Анализ воздействия

Предварительным условием проведения анализа воздействия является получение следующих сведений:

- миссия информационной системы организации (то есть процессы, выполняемые ИС);
- критичность систем и данных (то есть ценность и важность систем и данных для организации);
- чувствительность систем и данных.

Воздействие, как и вероятность, можно оценить по трехбалльной шкале.

Определение рисков

Для определения рисков можно, оставаясь в рамках трехбалльной шкалы, выбрать для вероятностей реализации угроз значения 0.1, 0.5 и 1.0, а для уровней воздействия — 10, 50 и 100. Тогда, если произведение вероятности на воздействие не превосходит 10, риск можно считать низким. Значения от 10 до 50 соответствуют умеренному риску, свыше 50 — высокому.

Высокий риск требует незамедлительного планирования и реализации корректирующих действий. Если по какой-либо причине планирование или реализация затягиваются, может ставиться вопрос о приостановке работы ИС или ее частей.

Умеренный риск также требует планирования и реализации корректирующих действий за разумный период времени.

При низком риске следует решить, нужны ли какие-то корректирующие действия, или можно принять риск.

Рекомендуемые контрмеры

Назначение рекомендуемых контрмер заключается в том, чтобы нейтрализовать (в достаточной степени уменьшить или устранить) идентифицированные риски. При планировании дополнительных регуляторов безопасности обязательно следует учитывать следующие факторы:

- совместимость с существующим аппаратно-программным обеспечением;
- соответствие действующему законодательству;
- соответствие практике организации, ее политике безопасности;
- воздействие на эксплуатационное окружение;
- безопасность и надежность.

Рекомендуемые контрмеры являются результатом процесса оценки рисков и, одновременно, входными данными для процесса нейтрализации рисков.

Результирующая документация

Отчет с результатами оценки рисков помогает руководству организации, владельцам информационных систем принимать обоснованные решения по изменению политики, процедур и регуляторов безопасности, по корректировке бюджета и т.п. В отличие от результатов работы аудиторов, которые заботятся, прежде всего, о выявлении недостатков, отчет об оценке рисков не должен носить обвинительного характера. Нужен систематический, аналитический подход, чтобы высшее руководство осознало имеющиеся риски и выделило на их нейтрализацию необходимые ресурсы.

Нейтрализация рисков

Нейтрализация рисков — вторая фаза процесса управления рисками — включает определение приоритетов, оценку и реализацию контрмер, уменьшающих риски и рекомендованных по результатам оценки рисков.

Поскольку полное устранение рисков невозможно и/или бессмысленно, руководство организации должно следовать принципу минимальной достаточности, реализуя только необходимые, наиболее подходящие регуляторы безопасности с целью уменьшения рисков до приемлемого уровня с минимальным негативным воздействием на бюджет, ресурсы и миссию организации.

В процессе управления рисками могут использоваться различные возможности:

- принятие риска;
- уклонение от риска (ликвидация причин и/или последствий риска, например, путем добавления регуляторов безопасности, устранения небезопасных функций ИС, приос-

тановки работы ИС в небезопасных ситуациях и т.п.);
- ограничение (нейтрализация) риска (например, путем реализации контрмер, уменьшающих воздействие угроз);
- переадресация риска (например, путем приобретения страхового полиса).

С практической точки зрения нет смысла и возможности учитывать все риски; их следует ранжировать, выделив наиболее опасные для миссии организации или грозящие наиболее крупными потерями.

Действия по управлению рисками могут производиться на различных этапах жизненного цикла информационной системы, а именно:
- при выявлении дефекта или слабого места целесообразно применить меры, повышающие доверие безопасности ИС, чтобы устранить обнаруженные уязвимости и уменьшить вероятность появления новых;
- при выявлении уязвимости, допускающей использование, целесообразно применить эшелонированную оборону, другие принципы архитектурной безопасности или нетехнические контрмеры, чтобы затруднить или воспрепятствовать использованию уязвимости;
- в ситуациях, когда затраты атакующего меньше потенциальной выгоды от атаки, целесообразно принять меры для уменьшения мотивации источника угрозы путем увеличения стоимости или уменьшения выгоды от атаки (например, может быть применен административный регулятор безопасности, ограничивающий типы данных, подлежащих обработке информационной системой организации, после чего выгода от атаки на ИС должна существенно уменьшиться);
- в ситуациях, когда ущерб слишком велик, целесообразно применить принципы проектирования и архитектурной безопасности, а также технические и организационные контрмеры, чтобы уменьшить возможный масштаб атак и, следовательно, снизить потенциальный ущерб от них (и здесь административный регулятор безопасности, ограничивающий типы данных, подлежащих обработке информационной системой организации, может оказаться самым эффективным способом управления рисками).

Основное правило управления рисками можно сформулировать следующим образом: начните с наибольших рисков и стремитесь к их уменьшению до приемлемого уровня при минимальных затратах и с минимальным воздействием на другие возможности информационной системы организации.

Реализацию приведенного правила целесообразно оформить в виде процесса со следующими шагами:
- Шаг 1 — ранжирование действий. При выделении ресурсов высший приоритет должен отдаваться неприемлемо высоким рискам, требующим немедленных корректирующих действий. Результат шага 1 — упорядоченный по убыванию приоритетов перечень действий.
- Шаг 2 — оценка возможных способов реализации рекомендованных контрмер. Цель состоит в том, чтобы выбрать наиболее подходящие контрмеры, минимизирующие риски. Результат шага 2 — список пригодных регуляторов безопасности.
- Шаг 3 — оценка экономической эффективности, выбор наиболее практичных контрмер. Результат шага 3 — отчет об экономическом анализе, описывающий затраты и выгоды от реализации контрмер или от отсутствия таковой.
- Шаг 4 — выбор контрмер. По результатам технического и экономического анализа руководство организации выбирает оптимальный способ нейтрализации рисков. Результат шага 4 — список выбранных регуляторов безопасности.
- Шаг 5 — распределение обязанностей. Выбираются должностные лица, обладающие достаточной квалификацией для реализации выбранных контрмер. На этих сотрудников возлагаются обязанности по реализации регуляторов безопасности. Результат шага 5 — список ответственных и их обязанностей.
- Шаг 6 — разработка плана реализации контрмер. План должен содержать по крайней мере следующие сведения:
  - риски (пары уязвимость/угроза) и их уровни, полученные в результате оценки рисков;
  - рекомендованные регуляторы безопасности;
  - действия, упорядоченные по приоритетам (высший приоритет получают действия, направленные на нейтрализацию самых высоких рисков);
  - регуляторы безопасности, выбранные из числа рекомендованных;
  - ресурсы, необходимые для реализации выбранных регуляторов безопасности;
  - список ответственных за реализацию выбранных контрмер;
  - календарный план реализации контрмер;

  - требования к сопровождению. Результат шага 6 — план реализации контрмер.
- Шаг 7 — реализация выбранных контрмер. Результат шага 7 — остаточные риски.

Необходимым элементом управления рисками является оценка экономической эффективности, цель которой — продемонстрировать, что затраты на реализацию дополнительных контрмер окупаются за счет снижения рисков. При вычислении затрат на реализацию регуляторов безопасности следует учитывать:

- затраты на приобретение аппаратного и программного обеспечения;
- снижение эксплуатационной эффективности ИС, если производительность или функциональность системы падает в результате усиления мер безопасности;
- затраты на разработку и реализацию дополнительных политик и процедур;
- дополнительные затраты на персонал, вовлеченный в реализацию предложенных регуляторов безопасности;
- затраты на обучение персонала;
- затраты на сопровождение.

Возможный формат отчета об оценке рисков

Отчет об оценке рисков может иметь следующий формат.

- Краткое содержание.
- Введение.
  - Цель.
  - Область охвата оценки рисков. Описываются компоненты информационной системы, ее пользователи, расположение удаленных производственных площадок (при наличии таковых) и т.п.
  - Подход к оценке рисков. Кратко описывается выбранный подход к оценке рисков, в том числе:
  - состав группы, оценивающей риски;
  - методы сбора информации (вопросники, инструментальные средства и т.п.);
  - описание применяемой шкалы рисков.
- Характеристика системы. Описывается система, включая аппаратуру (серверы, активное сетевое оборудование и т.д.), программное обеспечение (приложения, базовое ПО, протоколы), системные интерфейсы (коммуникационные каналы), данные, пользователи. Приводится диаграмма связности, входные и выходные потоки данных.
- Перечень уязвимостей. Составляется список потенциальных уязвимостей, возможно, присутствующих в оцениваемой системе.
- Перечень источников угроз. Составляется список потенциальных источников угроз, актуальных для оцениваемой системы.
- Результаты оценки рисков. Приводится перечень выявленных рисков (пар уязвимость/угроза). Каждый элемент данного перечня должен включать:
  - номер и краткое описание (например: 1. Пользовательские пароли могут быть угаданы или подобраны);
  - обсуждение пары уязвимость/угроза;
  - набор существующих регуляторов безопасности, уменьшающих риск;
  - обсуждение вероятности реализации угрозы и ее оценка (высокая, умеренная, низкая);
  - анализ воздействия, его оценка (высокое, умеренное, низкое);
  - оценка (рейтинг) рисков (высокий, умеренный, низкий);
  - рекомендуемые регуляторы безопасности или иные способы снижения рисков.
- Выводы. Приводится сводка рисков и их уровней, рекомендации и комментарии, разъясняющие реализацию рекомендованных контрмер в процессе нейтрализации рисков.

Возможный формат плана реализации контрмер

План реализации контрмер можно оформить в виде таблицы (см. табл. 9.1).

Возможные трактовки и способы вычисления рисков

Риски и управление ими исследуются в нескольких предметных областях, таких как страхова-

ние, экономика, управление, медицина, исследование операций, инженерия, и рассматриваются с разных точек зрения.

В простейшем случае риск приравнивается к возможному негативному событию и определяется как «событие, представляющее материальную угрозу чьему-либо состоянию». Иными словами, риски приравниваются к возможным нежелательным событиям (или к возможному снижению полезности). В контексте управления рисками под «чьим-либо состоянием» понимается благополучие организации. С этой точки зрения управлять рисками можно, применяя страхование и получая компенсацию, если негативное событие произойдет. Другой возможный подход — планирование бесперебойной работы, позволяющее продолжить функционирование после нежелательных событий.

В некоторых предметных областях, таких как медицина, акцент делается на вероятности негативных событий, а не на их последствиях, поскольку последние зачастую являются необратимыми, фатальными (например, смерть пациента в результате инфаркта) и заострять внимание на них нет смысла. Определяются факторы, влияющие на вероятности (наследственность, вредные привычки и т.п.), а риск трактуется как «вероятность опасного неблагоприятного исхода». Данный подход применяется при страховании жизни, где для получения оценок вероятностей используются таблицы смертности, а «приемлемый риск» относится к людям с низкой вероятностью умереть в течение страхового периода (и, соответственно, с низкой вероятностью выплаты компенсации страховой компанией).

Финансисты считают риском вариацию распределения исходов, а мерой риска — диапазон колебаний. Риск определяется как непостоянство стоимости портфеля ценных бумаг, а управление рисками означает решение минимаксной задачи — выбор между риском и доходами. Портфель ценных бумаг пытаются комплектовать так, чтобы обеспечить наивысшие ожидаемые доходы при заданном уровне рисков и наименьший уровень рисков для заданного ожидаемого дохода.

При страховании от несчастных случаев (в частности, при страховании автомобилей) риск трактуется как ожидаемые потери и определяется как произведение возможного ущерба на его вероятность. И ожидаемый ущерб, и его вероятность могут меняться в широких пределах (от незначительного до полной утраты автомобиля, от очень небольшой для аккуратных водителей до заметной для лихачей).

При проведении анализа рисков важно различать риски экзогенные и эндогенные. Первые не поддаются управлению, они не зависят от

Угроза (пара уязвимость/угроза)	Неавторизованные пользователи могут зайти на сервер X по протоколу telnet под именем guest и просмотреть файлы организации
Уровень риска	Высокий
Рекомендованные контрмеры	Запретить входящие соединения по протоколу telnet. Запретить доступ «прочих» пользователей к чувствительным файлам организации Отключить счет guest или присвоить ему трудный для подбора пароль
Приоритет действия	Высокий
Выбранные планируемые контрмеры	Запретить входящие соединения по протоколу telnet. Запретить доступ «прочих» пользователей к чувствительным файлам организации Отключить счет guest
Требуемые ресурсы	10 часов на реконфигурирование и тестирование системы
Ответственные	С. Иванов, администратор сервера X. А. Петров, администратор межсетевых экранов
Даты начала и завершения работ	01/09/2006 – 02/09/2006
Сопровождение: требования/ комментарии	Периодически пересматривать и тестировать защищенность сервера X

Табл. 9.1 Возможный формат сводной таблицы плана реализации контрмер.

чьих-либо действий. Примером могут служить землетрясения. Можно в какой-то степени влиять на размер ущерба, строя здания по определенным стандартам, но предотвратить землетрясение пока невозможно. Эндогенные риски зависят от действий людей. Многие риски, например, риск автомобильной аварии, являются смешанными. Водитель не может влиять на поведение других участников движения, но от его собственного поведения, его манеры езды (и от выбора автомобиля) зависит многое, в том числе ущерб от аварии, если таковая произойдет. Чтобы стимулировать поведение водителей, минимизирующее эндогенные риски, в страховой сумме предусматривают удерживаемую составляющую. Будучи ответственным за часть ущерба, водитель должен действовать с осторожностью.

Инструментальные средства управления рисками реализуются с учетом различия между экзогенными и эндогенными рисками. Например, финансисты считают неопределенность экзогенным риском и для управления рисками применяют такие методы, как диверсификация, страхование и распределение активов. Нет возможности непосредственно повлиять на вероятности событий. В медицине и инженерии часть рисков всегда являются эндогенными, поддающимися уменьшению. Пациентов информируют о том, на что они могут вилять, им рекомендуют здоровый образ жизни и специальные диеты. Работников знакомят с правилами техники безопасности, принимают меры по снижению аварийности и травматизма.

В информационных технологиях принят по сути тот же взгляд на риски, что и при страховании от несчастных случаев. Суммарный риск определяется как математическое ожидание ущерба, то есть как сумма произведений вероятностей каждого из негативных событий на величины потерь от них:

$$R = \text{Сумма (по i)} \{P(Ui) * L(Ui)\}$$

Несмотря на кажущуюся простоту и очевидность, приведенная формула не подчиняется обычным арифметическим законам, поэтому желательно рассматривать не только итоговую величину риска, но и ее составляющие. Причин тому несколько.

Оценка рисков действует на протяжении определенного периода. Чтобы иметь основания применять аппарат теории вероятностей, этот период должен быть достаточно большим (три-пять лет). Если вероятность события (например, пожара) мала, рассматриваемый период следует еще увеличить. Но за это время ИС существенно изменится и старые оценки потеряют смысл. Следовательно, при оценке рисков событиями с вероятностью меньше определенного порогового значения можно пренебречь, несмотря на то, что потенциальный ущерб от них может быть велик. Отметим, что это противоречит традиционной практике, когда руководители склонны уделять чрезмерное внимание рискам с большим ущербом и малой вероятностью. На самом деле, на первом плане должны быть риски с умеренным ущербом, но высокой вероятностью (например, атаки вредоносного программного обеспечения), многократно реализующиеся в течение рассматриваемого периода.

Вероятность негативного события нет возможности оценить сколько-нибудь точно. Для этого нет ни теоретических предпосылок, ни накопленного статистического базиса. Нет возможности и для обоснованной оценки влияния контрмер на вероятности; можно воздействовать на факторы, от которых вероятности зависят, но количественный эффект воздействий предсказать нельзя.

Наконец, негативные события могут не быть независимыми. Одно из них может исключать другое (например, пожар и затопление) или, напротив, вызывать каскадный эффект, как это бывает при перегрузке критически важных компонентов.

В силу приведенных здесь соображений целесообразно трактовать риски не как числовые значения, а как точки на плоскости, где координатными осями служат вероятности и потери (см. рис. 10.1). Линиями уровня для функции риска служат гиперболы.

Риск события U1 относится к числу обычно переоцениваемых руководителями; на практике, в силу низкой вероятности, большей частью подобных рисков целесообразно пренебречь.

Управлению рисками соответствует перемещение точек по плоскости. Обычно стремятся приблизиться к началу координат вдоль одной оси, не меняя значения другой координаты. Впрочем, если удастся уменьшить сразу обе координаты, это будет еще лучше.

Обоснованное управление рисками возможно только в сравнительно узких областях, когда известны возможные негативные события, когда число их относительно невелико (обозримо, в пределах нескольких десятков) и когда существуют реалистичные оценки вероятностей и потерь. В других случаях экономическая целесообразность нейтрализации рисков может оцениваться только интуитивно. Правда, нейт-

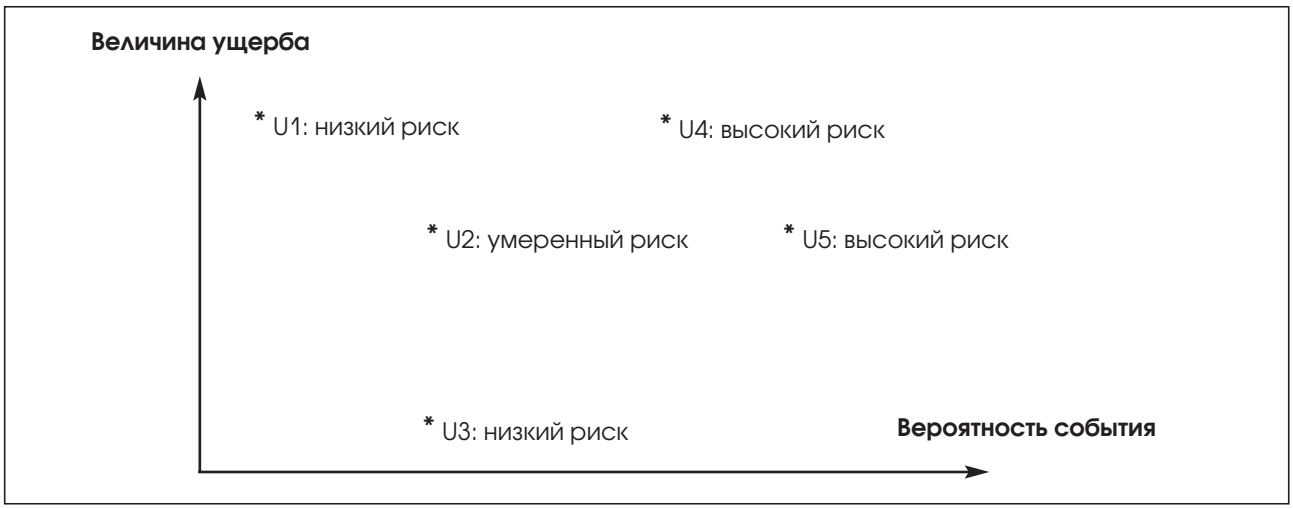

Рис. 10.1 Представление рисков в виде точек на координатной плоскости.

ализация многих рисков требуется действующим законодательством (например, обеспечение противопожарной безопасности), поэтому соответствующие контрмеры можно считать обязательными.

Одной из областей, важных с практической точки зрения и хорошо проработанных в плане управления рисками, является аутсорсинг по управлению информационной системой (в частности, контроль ее информационной безопасности). Здесь выделены восемь угроз:

- (1) Непредвиденно высокие затраты на переход на новую дисциплину управления ИС. «Уязвимостями» (то есть факторами, способствующими негативному событию) являются отсутствие у организации опыта аутсорсинга, неопределенность в законодательстве.
- (2) Затраты на переход на обслуживание другой организацией (включая попадание в заложники обслуживающей организации, возврат к исходному состоянию и переход на обслуживание новой организацией). Уязвимости: специфичность ИС, узкий выбор обслуживающих организаций, размеры и сложность ИС, взаимосвязь разных видов деятельности.
- (3) Дорогостоящие поправки к контракту. Уязвимости: неопределенность, технологический разрыв, сложность задачи.
- (4) Споры и тяжбы с обслуживающей организацией. Уязвимости: проблемы измеримости, недостаток опыта (у одной или обеих сторон) по заключению контрактов на аутсорсинг, неопределенность законодательства, недостаток культуры.
- (5) Снижение качества обслуживания. Уязвимости: взаимосвязь разных видов деятельности, недостаток опыта, слишком большой размер и/или финансовая нестабильность обслуживающей организации, проблемы измеримости.
- (6) Превышение затрат. Уязвимости: недостаток опыта по управлению контрактом на аутсорсинг, проблемы измеримости, недостаток опыта у поставщика услуг.
- (7) Потеря компетенции. Уязвимости: размеры и сложность ИС, близость к основной деятельности организации, взаимосвязь разных видов деятельности.
- (8) Скрытые затраты на обслуживание. Уязвимости: сложность разных видов деятельности, проблемы измеримости.

Рассмотрим управление идентифицированными рисками на примере страховой компании, отдавшей на аутсорсинг решение проблемы 2000 года для своих унаследованных систем. Вероятности и потери оценивались по семибалльной шкале. В табл. 10.1 и на рис. 10.2 (стр. 12) показаны риски до и после применения мер управления.

Из таблицы и рисунка видно, что удалось снизить три риска с номерами (2), (5) и (6), причем в первых двух случаях уменьшались только возможные потери, а в последнем — и вероятность, и потери. Отметим, что единственным серьезным был риск номер (6), хотя руководители в первую очередь обращали внимание на риски (2) и (5), игнорируя их относительно небольшую вероятность.

Чтобы не стать заложником внешней организации (управление риском (2)), страховая компания разбила проект на этапы и заключала отдельный контракт для каждого из них. Тем самым каждый контракт имел обозримый срок, а его результаты могли реально контролироваться. Если работа внешней организации оказалась бы неудовлетворительной, отношения с ней

Номер риска	Вероятности:		Потери:	
	до	после	до	после
(1)	1	1	1	1
(2)	1	1	4	1
(3)	1	1	2	2
(4)	1	1	3	3
(5)	1	1	5	3
(6)	1	1	4	1
(7)	4	2	1	1
(8)	1	1	1	1

Табл. 10.1 Риски при аутсорсинге проекта Y2K до и после применения мер управления.

Рис. 10.2 Риски при аутсорсинге проекта Y2K до и после применения мер управления.

могли быть оперативно прекращены. Со снижением качества обслуживания (риск (5)) страховая компания боролась, предусмотрев в контракте систему штрафов (в пять раз превышающих общую стоимость контракта). Для противодействия превышению затрат, страховая компания заранее оговорила гарантированную плату и методику измерения дополнительных расходов с учетом особенностей отдельных компонентов ИС. Тем самым понижалась и вероятность, и воздействие риска.

Представление рисков в виде точек на плоскости является удачным с психологической точки зрения, поскольку оно разделяет два разных аспекта риска — вероятность и воздействие, и наглядно показывает, с чем в первую очередь нужно бороться и насколько это удалось.

Можно воспользоваться еще одним представлением рисков — в виде деревьев уязвимостей, угроз и контрмер (см. рис. 10.3). Здесь Vi — уязвимости, Ti,j — угрозы, эксплуатирующие уязвимости, Ci,j — контрмера, нейтрализующая угрозу i,j, Li,j — недостаток контрмер для угрозы i,j.

Значение для Vi, Ti,j, Li,j и Ci,j целесообразно нормировать, так чтобы суммы по i Vi и Ti,j равнялись 1, а также Li,j + Ci,j = 1.

Кроме вероятностных параметров, в оценке рисков участвуют константы — критичность активов (CA) и их стоимость (CC). Общая ожидаемая сумма потерь выражается соотношением

Общий остаточный риск * CA * CC

Предположим, имеется домашний компьютер, по отношению к которому рассматриваются пять уязвимостей с вероятностями 0.2, 0.2, 0.1, 0.05 и 0.45. Первую из них могут использовать две угрозы с вероятностями 0.35 и 0.65, вторую — три (0.4, 0.2, 0.4), третью — две (0.3, 0.7), Четвертую — три (0.25, 0.25, 0.5), пятую — две (0.3, 0.7). Пусть, наконец, значения недостатков контрмер оцениваются как 0.3, 0.4, 0.4, 0.1, 0.25, 0.25, 0.15, 0.25, 0.4, 0.4, 0.2, 0.15. Тогда общий остаточный риск составит 0.239375. Если критичность компьютера оценена как 0.4, а стоимость — как 2500, то ожидаемая сумма потерь составляет 239.38.

Можно предложить и другие формализмы для управления рисками. Предположим, имеется M пар (актив, угроза). Для каждой такой пары риск вычисляется по обычной формуле

Rk = Pi * Ij

Здесь k — номер пары, Pi — вероятность реализации угрозы по отношению к «парному» активу, Ij — воздействие реализации этой угрозы на актив, Rk — величина риска.

Пусть, далее, риски считаются допустимыми, если для всех k Rk <= Ra, где Ra — порог допустимости. Избыточные риски, которые требуется нейтрализовать, можно выразить соотношениями вида:

$$rk = \begin{cases} Rk - Ra, & \text{если } Rk > Ra \\ 0, & \text{если } Rk <= Ra \end{cases}$$

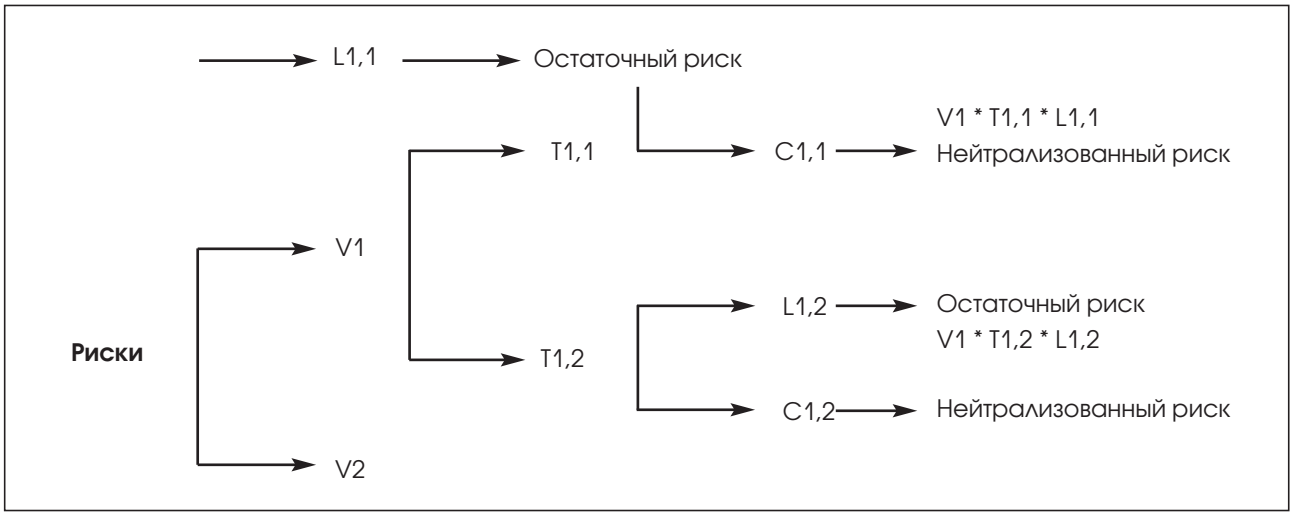

Рис. 10.3 Представление рисков в виде дерева уязвимостей, угроз и контрмер.

Пусть N — число положительных rk, то есть число пар (актив, угроза), риски которых нуждаются в нейтрализации. Отбросим нулевые избыточные риски и перенумеруем оставшиеся. Можно вычислить среднее значение избыточного риска rMean, воспользовавшись формулой

rMean = ((сумма по k от 1 до N) rk) / N

Значение rMean можно рассматривать не только как средний избыточный риск, но и как оценку безопасности информационной системы в целом. Эту оценку можно нормализовать, воспользовавшись формулой

rMeanNrorm = rMean / (Rmax — Ra)

где Rmax — максимальный из возможных рисков Rk, то есть произведение максимального из возможных значений Pi и Ij в выбранной шкале измерений.

Значения rMeanNrorm, близкие к 0, характеризуют уровень информационной безопасности ИС как весьма высокий. Близкие к 1 значения, напротив, характерны для слабо защищенных информационных систем. При желании отрезок [0, 1] можно разбить на интервалы, выделив тем самым нужное число уровней безопасности.

Кроме среднего арифметического, можно вычислить среднее квадратичное значение положительных избыточных рисков:

sigma = кв.корень (((сумма по k от 1 до N) (rk*rk)) / N)

Как и средний избыточный риск, среднее квадратичное значение можно нормализовать:

sigmaNorm = sigma / (Rmax — Ra)

Нормализованное среднее квадратичное значение, как и величину rMeanNrorm, можно напрямую использовать для оценки уровня информационной безопасности организации, если разбить отрезок [0, 1] на соответствующее число интервалов. Значения, близкие к 0, свидетельствуют о высоком уровне защищенности, близкие к 1 — о низком. Преимущество среднего квадратичного значения по сравнению со средним арифметическим в том, что первое более устойчиво к добавлению пар с небольшими избыточными рисками и более чувствительно к аномально высоким рискам.

Рассмотрим пример. Пусть вероятности и воздействия оцениваются по шестибалльной шкале, от 0 до 5, а приемлемым считается риск, равный 8. Тогда Ra = 8, Rmax = 25

(5*5). Пусть, далее, имеются две организации. Для первой из них рассматриваются следующие пары (актив, угроза) и ассоциированные с ними характеристики (см. табл. 10.2).

Пусть для второй организации аналогичная таблица выглядит так (см. табл. 10.3).

Средние значения рисков сведены в таблицу 10.4. Видно, что нормализованные средние арифметические значения избыточных рисков у двух организаций близки, в то время как нормализованное среднее квадратичное значение у первой организации заметно выше (а уровень безопасности, соответственно, ниже). Причина в аномально высоком риске внешнего физического вторжения, то есть в наличии ярко выраженного слабого звена.

Для оценки прогресса организации в области информационной безопасности важны не абсолютные значения рисков, а их уменьшение в результате выбора и реализации контрмер.

При этом в качестве количественной меры риска может быть использовано время, требующееся на успешную атаку системы при заданных мотивации и квалификации злоумышленника. Увеличение этого времени свидетельствует о повышении уровня безопасности.

Рассматриваются два варианта информационной системы — первоначальный и укрепленный, то есть полученный в результате выбора и реализации контрмер. Методология оценки времени, требующегося на успешную атаку, включает следующие шаги:

- формирование анализируемой конфигурации системы;
- формирование количественной модели рисков для анализируемой конфигурации системы;
- формирование и ранжирование требований безопасности для анализируемой конфигурации системы;
- идентификация уязвимостей;
- категорирование уязвимостей каждого компонента системы по типу компрометации;
- оценка времени компрометации каждого компонента системы;
- генерация графа компрометации и путей атаки;
- нахождения путей атак с минимальным временем;
- повторение предыдущих шагов для первоначальной и укрепленной конфигурации системы;
- получение оценки снижения рисков.

На первом шаге, при формировании анализируемой конфигурации системы предлагается ограничиться двумя типами компонентов. К первому относятся граничные устройства, то есть устройства, входящие в систему и непосредственно (без маршрутизации, экранирования, фильтрации и т.п.) доступные из внешних сетей. Во второй тип входят основные цели потенциальных злоумышленников, то есть устройства, контроль над которыми дает атакующим нужную степень контроля над всей ИС организации.

Актив / угроза	Уровень вероятности	Уровень воздействия	Риск	Избыточный риск
Отдел кадров / вирусы	3	5	15	7
Отдел кадров / физический доступ сотрудников	2	5	10	2
Отдел кадров / физический доступ внешних лиц	5	5	25	17
Бухгалтерская система / шпионское ПО	2	5	10	2
Бухгалтерская система / поломка	1	1	1	0

Табл. 10.2 Таблица рисков для первой организации.

Актив / угроза	Уровень вероятности	Уровень воздействия	Риск	Избыточный риск
Отдел кадров / вирусы	3	5	15	7
Отдел кадров / физический доступ сотрудников	3	5	15	7
Отдел кадров / физический доступ внешних лиц	3	4	12	4
Бухгалтерская система / шпионское ПО	4	4	16	8

Табл. 10.3 Таблица рисков для второй организации.

Средние значения избыточных рисков	Организация 1	Организация 2
Среднее арифметическое	7	6.5
Нормализованное среднее арифметическое	0.41	0.38
Среднее квадратичное	9.30	6.67
Нормализованное среднее квадратичное	0.55	0.39

Табл. 10.4 Средние значения избыточных рисков для рассматриваемых организаций.

Количественная модель рисков базируется на стандартной формуле

$$R = P * D$$

где R — величина риска, P — вероятность успешной атаки, D — ущерб от нее.

Вероятность P можно представить в виде произведения следующих условных вероятностей:

$$P = Pi * Pa * Pb * Pc * Pd$$

где

- Pi — вероятность того, что данная информационная система попадет в список возможных целей злоумышленника;
- Pa — вероятность того, что система будет выбрана из списка и атакована;
- Pb — вероятность того, что будут взломаны граничные компоненты;
- Pc — вероятность того, что атака окажется успешной, то есть достигшей основных целей;
- Pd — вероятность того, что злоумышленником будет нанесен предполагаемый ущерб.

Снижение рисков путем выбора и реализации контрмер воздействует на вероятности Pb и Pc взлома граничных и целевых систем; их и требуется оценить. Предполагается, что укрепление системы не влияет ни на другие вероятности, ни на размер ущерба. Далее, можно считать, что вероятность успешной атаки обратно пропорциональна времени, которое на подобную атаку требуется (чем длительнее атака, тем больше шансов обнаружить и пресечь ее). Таким образом, в конечном счете снижение рисков определяется увеличением общего времени, требующегося на успешные атаки цепочки компонентов ИС, начинающейся граничным устройством и оканчивающейся основной целью.

Формирование и ранжирование требований безопасности для анализируемой конфигурации системы необходимо для того, чтобы определить понятие успешной атаки. Обычно требования выражаются в терминах доступности, конфиденциальности и целостности. Например, для систем управления на первом плане находятся доступность и целостность; конфиденциальность не имеет особого значения.

Идентификация уязвимостей может выполняться с помощью средств анализа защищенности и путем анализа общедоступных источников соответствующей информации. В специфических случаях требуется привлечение специальных знаний об особенностях системы и ее конфигурации.

Категорирование уязвимостей каждого компонента системы по типу компрометации необходимо для того, чтобы связать с каждым ребром графа компрометации набор уязвимостей, делающих переход по данному ребру возможным. Граф компрометации — это направленный граф, вершины которого соответствуют стадиям атаки, а ребра — переходам между стадиями; с каждым ребром связывается время, требующееся на успешное проведение очередной стадии атаки.

Каждая вершина графа компрометации относится к одному из следующих типов:

- Старт. На этой стадии злоумышленник ничего не знает об устройстве целевой системы. Это — единственная входная вершина графа.
- Начало атаки. Собрано достаточно данных, чтобы начать разработку программ использования уязвимостей или применить известные средства взлома. Для каждого граничного устройства в графе имеется один узел этого типа (точка развертывания потенциальной атаки).
- Получение привилегий обычного пользователя. Это состояние относится к конкретной машине, на которой атакующий сумел стать обычным пользователем. Для каждой машины целевой информационной системы имеется только одно состояние этого типа.
- Получение привилегий суперпользователя. Это состояние относится к конкретной машине, на которой атакующий сумел стать суперпользователем. Для каждой машины целевой информационной системы имеется только одно состояние этого типа.
- Целевой узел. Любое состояние, означающее успех атаки.

Ребра графа представляют этапы успешной компрометации и помечаются длительностью этапа, которая зависит от сложности эксплуатации имеющихся уязвимостей (с учетом квалификации злоумышленника). Естественно считать, что вероятность перехода по данному ребру обратно пропорциональна ассоциированной с ним длительности. Ребра (и уязвимости, позволяющие осуществлять соответствующие переходы между состояниями) подразделяются на следующие типы:

- Разведка (зондирование) (P).
- Нарушение (взлом) (H). Это ребра, выходящие из узла начала атаки.

- Проникновение (П). Это ребра, выходящие и из узлов с привилегиями обычного пользователя или суперпользователя, и входящие в узлы того же типа.
- Эскалация (Э). Эти ребра означают получение дополнительных привилегий на той же машине.
- Нанесение ущерба (У). Эти ребра входят в целевой узел.

Оценка времени компрометации каждого компонента системы (Т) означает оценку времени на получение атакующим каких-либо пользовательских привилегий на данном устройстве. Компрометация моделируется случайным процессом, который подразделяется на три подпроцесса:

- Подпроцесс 1 осуществляется в ситуации, когда известна по крайней мере одна уязвимость, и атакующий располагает средствами ее использования.
- Подпроцесс 2 осуществляется в ситуации, когда имеются известные уязвимости, но атакующий не располагает средствами их использования.
- Подпроцесс 3 состоит в идентификации новых уязвимостей и средств их эксплуатации. Он может функционировать в фоновом режиме параллельно с подпроцессами двух первых типов. Злоумышленник может быть пользователем или участником подпроцессов данного типа, то есть он может ждать, когда станет известно о новых уязвимостях и средствах их эксплуатации, или разрабатывать и пробовать их.

Каждый из перечисленных подпроцессов характеризуется своим распределением вероятностей. Подпроцессы 1 и 2 являются взаимоисключающими. Подпроцесс 3 можно считать непрерывным.

Для оценки времени Т можно воспользоваться следующей формулой:

$$T = t1 * P1 + t2 * (1 - P1) * P2 + t3 * (1 - P1) * (1 - P2)$$

здесь

- t1 — ожидаемое время завершения подпроцесса 1 (обычно — 1 день);
- t2 — ожидаемое время завершения подпроцесса 2, которое вычисляется по эмпирической формуле:

t2 = 5.8 * (ожидаемое число неудачных попыток взлома), причем ожидаемое число неудачных попыток взлома обратно пропорционально числу имеющихся уязвимостей и прямо пропорционально среднему числу уязвимостей, для которых средства использования могут быть найдены или созданы злоумышленником с данным уровнем квалификации;

- t3 — ожидаемое время завершения подпроцесса 3, которое можно считать прямо пропорциональным числу имеющихся уязвимостей и обратно пропорциональным среднему числу уязвимостей, для которых средства использования могут быть найдены или созданы злоумышленником с данным уровнем квалификации;
- P1 — вероятность успешного завершения подпроцесса 1;
- P2 — вероятность успешного завершения подпроцесса 2.

Генерация графа компрометации и путей атаки выполняется с использованием полученных оценок.

Нахождения путей атак с минимальным временем означает оценку максимального риска. Подобный путь всегда проходит через компонент ИС с наибольшим числом уязвимостей.

На рис. 10.4 приведен пример фрагмента графа компрометации. Время указано в днях. Кратчайший путь показан сверху.

Повторение предыдущих шагов для первоначальной и укрепленной конфигурации системы требует генерации двух графов компрометации. Если в укрепленной системе уязвимостей меньше, а кратчайший путь успешной атаки имеет большую длину для произвольной квалификации злоумышленников, можно переходить к оценке снижения рисков.

Получение оценки снижения рисков основывается на предположении, что вероятность успешной атаки на укрепленную систему задается следующим соотношением:

$$Pnew = Pold * («Старое\_время» / «Новое\_время»)$$

где

- Pold — вероятность успешной атаки на ИС в базовой (старой) конфигурации;
- «Старое_время» — ожидаемое время успешной атаки с минимальной длительностью на ИС в базовой (старой) конфигурации;
- «Новое_время» — ожидаемое время успешной атаки с минимальной длительностью на ИС в укрепленной (новой) конфигурации

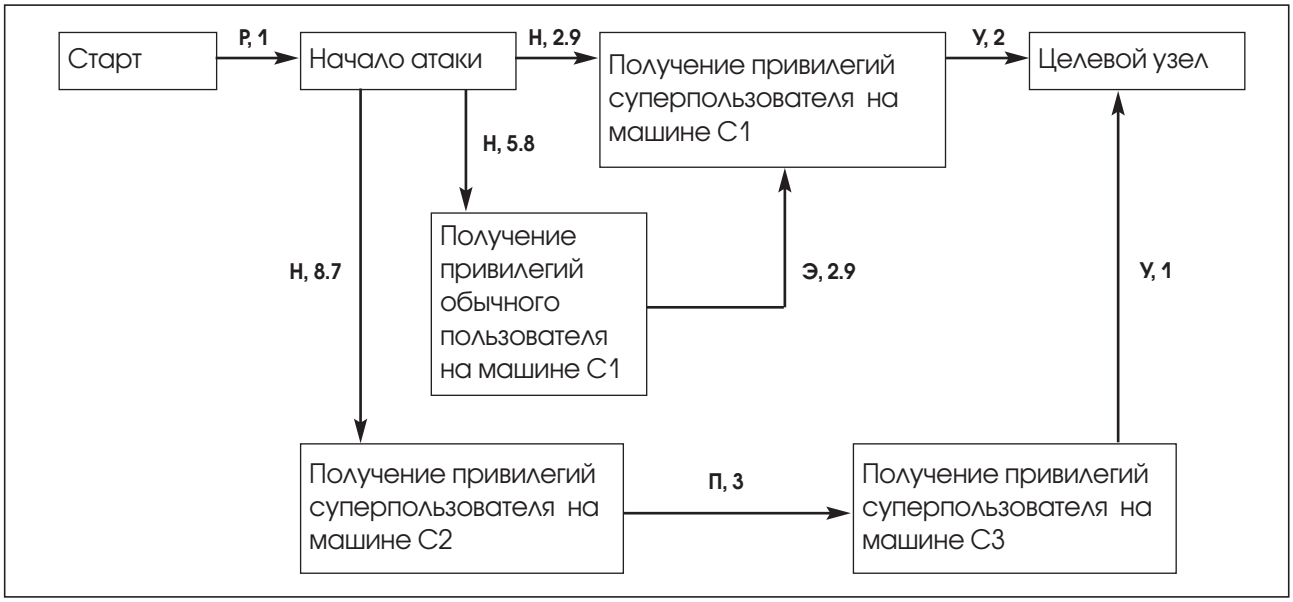

Рис. 10.4 Фрагмент графа компрометации.

(естественно предполагать, что «Новое_время» не меньше, чем «Старое_время»).

Нормализованное снижение риска определяется как

dR = 1 − (Pnew / Pold) = 1 − («Старое_время» / «Новое_время»)

Оно стремится к 1, если «Новое_время» стремится к бесконечности. Напротив, если «Новое_время» и «Старое_время» совпадают, снижение риска оказывается нулевым.

Время успешной атаки имеет постоянную и переменную составляющие. К первой относятся длительности разведки и нанесения ущерба, ко второй − нарушение (взлом), проникновение и эскалация. Можно предположить, что укрепление системы влияет только на переменную часть. Если постоянная часть велика, существенного снижения рисков добиться не удастся, но это означает лишь то, что система и так хорошо защищена (в эшелонированной обороне имеются хорошо укрепленные рубежи − первый и последний).

Укрепление системы может достигаться путем уменьшения числа уязвимостей и увеличения длительности нахождения и/или создания средств их использования. Первый путь сам по себе не дает заметного эффекта: почти полное устранение уязвимостей увеличивает длину кратчайшего пути лишь на несколько процентов. Это понятно: для успешного взлома достаточно одной уязвимости.

На риски и уменьшающие их контрмеры можно смотреть не только со стороны защищающейся организации, но и со стороны атакующего злоумышленника. Чем сильнее регуляторы безопасности затрудняют вредоносную активность, тем более удачным можно считать их выбор. В качестве формализма, поддерживающего данный подход, целесообразно использовать графы атак, вершины которых помечены возможными контрмерами и их количественной экономической оценкой с точки зрения защищающегося и атакующего.

Однократный ущерб на ресурс будем определять по формуле

SLE = AV * EF

где AV − ценность ресурса, в которую входят все виды затрат на него (установка, сопровождение и т.п.), а EF − доля этой величины, утрачиваемая в результате вредоносного действия (относительный ущерб от однократной компрометации ресурса).

Поскольку не все угрозы равновероятны, введем годичную частоту реализации угрозы (ARO). Тогда ожидаемый годовой ущерб от данной угрозы будет вычисляться по формуле

ALE = SLE * ARO

Оценка значения ARO может производиться на основе анализа статистики нарушений информационной безопасности.

Экономический эффект от реализации контрмеры (то есть от расходов на информационную безопасность) можно оценить по формуле

ROI = ((ALE * RM) − CSI) / CSI

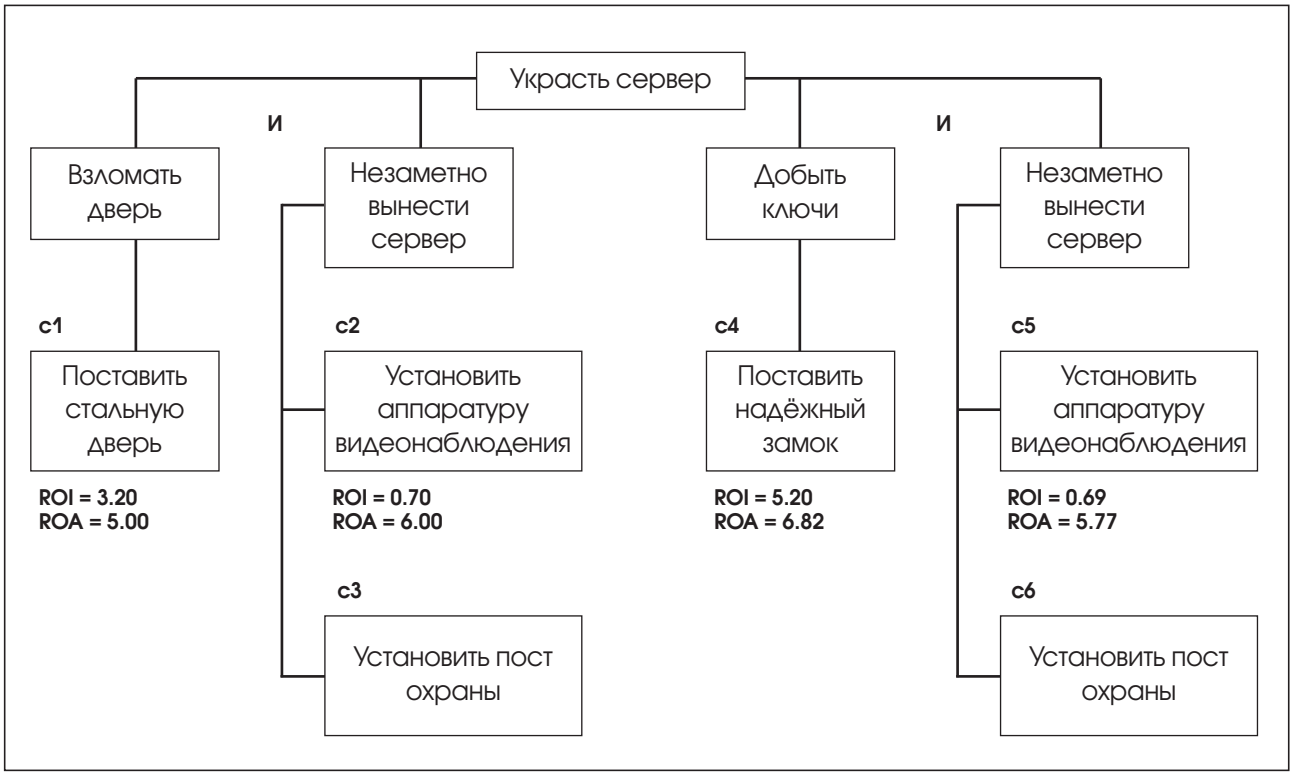

Рис. 10.5 Фрагмент графа атак, аннотированного контрмерами и показателями экономической эффективности.

где RM — коэффициент уменьшения риска в результате реализации контрмеры (лежит в промежутке от 0 до 1), а CSI — стоимость этой реализации. При положительном значении ROI реализация регулятора безопасности является экономически оправданной; в противном случае в ней нет смысла. ROI — это инструмент экономической оценки эффективности действий (защищающейся) организации в области информационной безопасности. Цель состоит в максимизации значения ROI.

Экономическая эффективность действий атакующего оценивается с помощью величины ROA, вычисляемой по формуле

$$ROA = GI / (EBS + EAS)$$

где GI — ожидаемая выгода от успешной атаки, EBS — затраты на компрометацию ресурса до реализации контрмеры S, EAS — дополнительные затраты на компрометацию после реализации контрмеры S. Цель защищающейся организации состоит в минимизации значения ROA, то есть в уменьшении привлекательности ресурсов организации как объектов возможных атак.

Атаки проводятся путем использования уязвимостей. В графах атак уязвимости ассоциируются с концевыми вершинами, то есть вершинами, из которых не выходит ни одного ребра. С этими же вершинами ассоциируются контрмеры, ликвидирующие или уменьшающие уязвимости.

Графы атак называют также И-ИЛИ графами, так как для успешного проведения атаки может быть достаточно одного из нескольких условий (связка ИЛИ), либо требуется одновременное выполнение всех условий из некоторого множества (связка И). Из технических соображений (упрощения перебора различных сценариев атак) графы атак целесообразно представлять в дизъюнктивной нормальной форме, при которой связка И может относиться только к концевым вершинам. Преобразование к дизъюнктивной нормальной форме основывается на логическом тождестве

$$(A \text{ ИЛИ } B) \text{ И } C = (A \text{ И } C) \text{ ИЛИ } (B \text{ И } C)$$

Рассмотрим пример компрометации конфиденциальных данных путем кражи сервера, на котором они хранятся (см. рис. 10.5). Чтобы украсть сервер, нужно сначала проникнуть в серверную комнату, а затем незаметно вынести сервер. Чтобы проникнуть в серверную комнату, можно взломать дверь или раздобыть (подобрать) ключи.

Пусть стоимость сервера составляет 100000 условных единиц, относительный ущерб от однократной компрометации (EF) при взломе двери и применении ключей равняется, соответ-

ственно, 0.9 и 0.93 (умный злоумышленник, сумевший заполучить в свое распоряжение ключи от серверной комнаты, опаснее прямолинейного вредителя, идущего к цели в буквальном смысле напролом), а годичная частота реализации угрозы (ARO) — 0.1. Тогда SLE составит, соответственно, 90000 и 93000 у.е., а ALE — 9000 и 9300 у.е.

В качестве контрмер против проникновения в серверную комнату можно установить надежный замок, к которому трудно подобрать ключи (RM = 0.2, CSI = 300 у.е.) или поставить стальную дверь, которую трудно взломать (RM = 0.7, CSI = 1500 у.е.). Чтобы противодействовать незаметному выносу сервера, можно установить аппаратуру видеонаблюдения (RM = 0.1, CSI = 3000 у.е.) или учредить пост охраны (RM = 0.5, CSI = 12000 у.е.). Значение ROI для каждой из контрмер вычисляется по приведенной выше формуле. Например, для стальной двери оно составит:

ROI = ((ALE * RM) − CSI) / CSI = ((9000 * 0.7) − 1500) / 1500 = 3.20

Чтобы противодействовать всем возможным (идентифицированным) атакам необходимо установить регуляторы безопасности на каждом пути в графе атак от концевых вершин к целевой (точнее, как минимум одна контрмера нужна для каждой связки И), отдавая предпочтение контрмерам с максимальным значением ROI. Если один регулятор безопасности противодействует нескольким атакам, затраты на него следует поделить поровну между соответствующими вариантами атак.

При рассмотрении ситуации с точки зрения атакующего предположим, что экономическая выгода от кражи сервера (GI) составляет 30000 у.е., затраты на первый вариант атаки (взломать дверь) (EBS) — 4000 у.е., затраты на второй — 4200 у.е. Для проведения успешной атаки при применении контрмеры в виде стальной двери от злоумышленника потребуется дополнительно 2000 у.е. (EAS), на борьбу с надежным замком понадобится дополнительно 200 у.е., с аппаратурой видеонаблюдения — 1000 у.е., с постом охраны — 1500 у.е. Таким образом, показатель экономической эффективности (ROA) первого варианта атаки после установки стальной двери составит:

ROA = GI / (EBS + EAS) = 30000 / (4000 + 2000) = 5.00

Анализ экономической эффективности контрмер для ROA проводится сходным с ROI образом, только значение ROA следует не максимизировать, а минимизировать (атаки на ресурсы организации должны иметь для злоумышленника минимальную привлекательность). Если одновременная максимизация ROI и минимизация ROA невозможна, для осуществления выбора регуляторов безопасности необходимо привлечь дополнительные соображения.

Для первой атаки (взломать дверь) контрмера c1 доминирует остальные, поскольку на ней достигается максимум ROI и минимум ROA. Для второй атаки (добыть ключи) доминирующей контрмеры нет: на c4 достигается максимум ROI, на c6 — минимум ROA. Отметим, что регулятор безопасности «установить пост охраны» уменьшает риск обеих атак и минимизирует ROA для второй атаки, но у него слишком мал показатель ROI, поэтому в данном случае целесообразно предпочесть комбинацию контрмер c1 и c4: поставить стальную дверь с надежным замком.

Заключение

Большинство организаций на собственном опыте осознали актуальность и важность проблем информационной безопасности. Следующим шагом должен стать количественный подход к их решению, основанный на управлении рисками.

Первым этапом в этом процессе является сбор данных о расходах на безопасность, об имевших место нарушениях ИБ и ущербе от них. Базируясь на этих данных, организация может построить количественную модель рисков для своей информационной системы, запланировать меры по усилению защиты слабых мест, сформировать обоснованный бюджет для защитных мероприятий.

Регулярная переоценка рисков позволит поддерживать данные о безопасности ИС организации в актуальном состоянии, оперативно выявлять новые опасные риски и нейтрализовывать их экономически целесообразным образом.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Редактор: Лапина И.К. *(lapina@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555