Петренко С. А.

Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. - М.: Компания АйТи ; ДМК Пресс, 2004. - 384 с.: ил. - (Информационные технологии для инженеров).

ISBN 5-98453-001-5 (АйТи) - **ISBN 5-94074-246-7** (ДМК Пресс)

В книге подробно рассмотрены возможные постановки задач анализа информационных рисков и управления ими при организации режима информационной безопасности в отечественных компаниях. Рассмотрена международная концепция обеспечения информационной безопасности, а также различные подходы и рекомендации по решению задач анализа рисков и управления ими. Дан обзор основных стандартов в области защиты информации и управления рисками: ISO 17799, ISO 15408, BSI, NIST, MITRE.

В настоящем издании обсуждаются инструментальные средства для анализа рисков (COBRA CRAMM, MethodWare, RiskWatch, Авангард). Даны рекомендации по использованию указанных средств на практике для анализа рисков информационных систем. Показана взаимосвязь задач анализа защищенности и обнаружения вторжений с задачей управления рисками. Предложены технологии оценки эффективности обеспечения информационной безопасности в отечественных компаниях.

Книга будет полезна руководителям служб автоматизации (CIO) и служб информационной безопасности (CISO), внутренним и внешним аудиторам (CISA), менеджерам высшего эшелона компаний, занимающимся оценкой информационных рисков компании и их управлением, а также студентам и аспирантам соответствующих технических специальностей.

Содержание

Предисловие

В настоящее время *организация режима информационной безопасности* становится критически важным *стратегическим фактором* развития любой отечественной компании. При этом, как правило, основное внимание уделяется требованиям и рекомендациям соответствующей российской нормативно-методической базы в области защиты информации. Вместе с тем многие ведущие отечественные компании сегодня используют некоторые *дополнительные инициативы,* направленные на *обеспечение устойчивости и стабильности функционирования корпоративных информационных систем для поддержания непрерывности бизнеса* в целом. В чем сущность этих инициатив и насколько они могут быть полезными для вашей компании? Давайте посмотрим вместе. Для этого сначала вспомним основные успехи развития российской нормативно-методической базы в области защиты информации в 2001-2003 гг., а затем остановимся на некоторых инициативах ведущих отечественных компаний.

В 2002 году в рамках деятельности Гостехкомиссии при Президенте РФ подготовлены и согласованы специальные требования и рекомендации по защите конфиденциальной информации, а также соответствующие методики. Летом 2002 года был утвержден ГОСТ Р ИСО/МЭК 15408-2002 (части 1, 2, 3) «Критерии оценки безопасности информационных технологий» на основе прямого применения международного стандарта ИСО/МЭК 15408-99. Продолжается работа над следующими нормативными документами по стандартизации (РД Гостехкомиссии):

- Руководство по разработке профилей защиты и заданий по информационной безопасности;
- Руководство по регистрации профилей защиты;
- Методика оценки профилей защиты и заданий по информационной безопасности;
- Автоматизированный комплекс разработки профилей защиты и заданий по информационной безопасности.

Кроме того, разрабатывается шесть профилей защиты для конкретных систем и средства информационных технологий, в том числе для некоторых операционных систем, межсетевых экранов и других компонент информационных технологий. В дальнейшем планируется создание более 20 профилей защиты.

В январе 2002 года в рамках деятельности ФАПСИ принят Федеральный закон «Об электронной цифровой подписи». С 1 июля 2002 года введена в действие новая версия стандарта ЭЦП ГОСТ РЗИ.10-01 на основе операций в группе точек эллиптических кривых. Новый стандарт по своим характеристикам, например криптостойкости и скорости, существенно превосходит предыдущий стандарт ЭЦП. Продолжается подготовка отечественных нормативных документов для создания национальной инфраструктуры с открытым распределением ключей (Public Key Infrastructure - PKI) и национальной иерархической системы удостоверяющих центров.

Дополнительные инициативы отечественных компаний в области защиты конфиденциальной информации обусловлены ростом интереса со стороны директоров служб автоматизации (CIO), служб безопасности (CISO), а также исполнительных директоров (CEO) ведущих отечественных компаний к постановке и решению следующих задач:

- анализа информационных рисков компании и управления ими;
- оценки непрерывности бизнеса организации;
- оценки экономической эффективности корпоративных систем защиты информации;
- оценки совокупной стоимости владения (TCO) системы защиты информации;
- оценки возврата инвестиций (ROI) компании в информационную безопасность (ИБ);
- планирования и управления бюджетом на ИБ.

Основной из перечисленных задач является *анализ и управление информационными рисками.* Действительно, большинство руководителей, ответственных за организацию режима информационной безопасности, наверняка задавалось вопросом: «Как оценить уровень безопасности корпоративной информационной системы нашего предприятия для управления им в целом и определения перспектив его развития?». Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Российской Федерации. Поэтому выбор методов оценки уровня безопасности корпоративной информационной системы обязательно требует ответа на следующие вопросы: в соответствии с какими критериями и показателями производить оценку эффективности системы защиты информации, и в том числе - как оценить и/или переоценить информационные риски предприятия? Вот почему в дополнение к имеющимся требованиям, рекомендациям и руководящим документам Гостехкомисии при Президенте РФ и ФАПСИ приходится адаптировать к российским условиям и применять на практике методики международных стандартов (ISO 17799, ISO 9001, ISO 15408, BSI и пр.), а также использовать внутренние корпоративные методики количественного анализа информационных рисков и оценивания экономической эффективности инвестиций в защиту информации, например, методики совокупной стоимости владения (TCO) и возврата инвестиций (ROI).

Современные технологии анализа рисков позволяют оценить существующий уровень остаточных информационных рисков в отечественных компаниях. Подобная оценка особенно важна в тех случаях, когда к информационной системе предприятия предъявляются повышенные требования в области информационной безопасности. Сегодня есть ряд методик анализа информационных рисков, в том числе с привлечением CASE-средств, адаптированных к применению в отечественных условиях. Существенно, что квалифицированно выполненный анализ информационных рисков позволяет:

- провести сравнительную оценку по критерию «эффективность-стоимость» различных вариантов защиты информации;
- выбрать адекватные контрмеры для защиты информации;
- оценить уровень остаточных информационных рисков компании.

Кроме того, инструментальные средства анализа рисков, основанные на современных базах данных и знаний в области защиты информации, дают возможность построить:

- структурные и объектно-ориентированные модели современных корпоративных информационных систем;
- модели угроз и модели рисков, связанных с отдельными составляющими элементами КИС, и таким образом выявлять те сегменты и объекты информационных систем, риск нарушения безопасности которых является критическим, то есть неприемлемым;
- различные модели защиты информационных систем, а также сравнивать между собой по критерию «эффективность-стоимость» варианты мер по защите (контрмер) и также вести контроль выполнения требований к организации режима информационной безопасности на предприятии.

По мнению авторов, настоящая книга является первым полным русскоязычным практическим руководством по вопросам анализа информационных рисков и управления ими. Основное отличие этой книги от других источников, преимущественно изданных за рубежом, заключается в том, что в ней последовательно изложены все основные идеи, методы и способы практического решения задач анализа информационных рисков и управления ими в различных государственных и коммерческих организациях и структурах.

Эта книга может быть полезна следующим основным группам читателей:

– руководителям служб автоматизации (*CIO*) и служб информационной безопасности (CISO), ответственным за организацию режима информационной безопасности, адекватного текущим целям и задачам бизнеса компании;
– внутренним и внешним аудиторам (CISA), которым приходится комплексно оценивать текущее состояние организации режима информационной безопасности компании на соответствие некоторым требованиям корпоративных, национальных и международных стандартов, например ISO 15408, ISO 17799, BSI, COBIT и пр.;
– менеджерам высшего эшелона управления компанией (TOP-менеджерам), занимающимся оценкой информационных рисков компании и их управлением.

Книгу могут также использовать в качестве учебного пособия студенты и аспиранты соответствующих технических специальностей, тем более что материалы многих глав основаны на опыте преподавания авторов в Московском и Санкт-Петербургском госуниверситетах.

Книга состоит из семи глав:

– Анализ рисков в области защиты информации;
– Управление рисками и международные стандарты;
– Технологии анализа рисков;
– Инструментальные средства анализа рисков;
– Аудит безопасности и анализ рисков;
– Анализ защищенности информационной системы;
– Выявление атак и управление рисками.

В первой главе показана роль и задачи анализа рисков и управления ими при организации режима информационной безопасности российских компаний. Подробно рассмотрена международная концепция обеспечения информационной безопасности компаний, а также различные подходы и рекомендации по решению задач анализа рисков и управления ими.

Во второй главе приведен обзор основных стандартов в области защиты информации и управления рисками: ISO 17799, ISO 15408, BSI, NIST, MITRE. Отмечены главные достоинства и недостатки существующих подходов к анализу информационных рисков и управлению ими.

Третья глава содержит описание основных технологий анализа рисков, возможных проблем и их решений, а также примеры разработки корпоративных методик анализа рисков. Кроме того, здесь представлен положительный практический опыт работы в данной предметной области.

В четвертой главе обсуждаются инструментальные средства для анализа рисков (COBRA CRAMM, MethodWare, RiskWatch, Авангард). Даны рекомендации по использованию указанных средств при анализе рисков информационных систем.

Пятая, шестая и седьмая главы посвящены практике решения задач анализа защищенности и выявления атак. Показана взаимосвязь с задачей анализа рисков и управления ими, а также роль «активного аудита» и обнаружения вторжений для оптимизации рисков. Рассмотрены технология работ аудита безопасности и оценки эффективности обеспечения информационной безопасности в отечественных компаниях. Имеется пример построения корпоративной системы защиты информации на основе решений Symantec.

Книга написана кандидатом технических наук Петренко С. А. (CISO) и кандидатом технических наук Симоновым С. В., за исключением следующих ее частей:

– раздел 1.1 - совместно с Березиным А. С. (Элвис+);
– раздел 1.2 - совместно с Муравьевой И. В. (Конфидент);
– разделы 1.3.1, 3.2.4 - совместно с Нестеровым С. А. (СПбПГУ);
– раздел 3.2 - совместно со Шпак В. Ф. (СЗО РАН);
– главы 6 и 7 - соавтор Астахов А. (CISA Вимм-Билль-Данн);

– приложение 1 - © KPMG, Российский член KPMG International, Швейцарская ассоциация, перевод 2002 г.;
– приложение 2 - © Эрнст энд Янг (СНГ) Лимитед, перевод 2002 г.;
– приложение 7 - совместно с Кисловым Р. И. (Конфидент) и Поповым Ю. И. (компания АйТи).

Авторы выражают особую благодарность докторам технических наук профессорам А. Д. Хомоненко, Ю. И. Рыжикову, В. Н. Кустову, Б. Н. Соколову, А. Г. Ломако и кандидату технических наук профессору В. В. Ковалеву за ценные советы и замечания по рукописи, которые помогли улучшить ее качество. Авторы благодарят кандидата технических наук А. А. Кононова за предоставленные материалы по экспертной системе «Авангард» и активное обсуждение глав книги.

Благодарим также центр GIAC и институт SANS в лице Стивена Нортката (Stephen Northcutt)) и Эрика Коула (Eric Cole), общество ISC^2 в лице CISSP Дмитрия Шепелявого, CISSP Чарльза Крессона Вуда (Charles Cresson Wood) и CISSP Шон Харрис (Shon Harris), ассоциацию ISACA в лице президента Лондонского отделения CISA Чарльза Мансура (Charles Mansour), CISA Андрея Дроздова (KPMG) и CISA Александра Астахова, а также компании «Эрнст энд Янг» (СНГ) в лице Мишель Мур и Cisco Systems в лице CCIE Максима Мамаева, CCIE Михаила Кадера, CCIE Мерике Кэо (Merike Kaeo).

Будем признательны всем читателям, которые готовы сообщить свое мнение о данной книге. Вы можете направлять письма в компанию АйТи по адресу: itpress@it.ru.

Глава 1
Анализ рисков в области защиты информации

1.1 Информационная безопасность бизнеса

В настоящее время проблемы обеспечения информационной безопасности корпоративных информационных систем (КИС) все чаще и чаще обсуждаются на страницах различных компьютерных изданий. При этом, как правило, значительное внимание уделяется описанию различных технических решений, анализу преимуществ и недостатков известных аппаратных и программных средств и технологий защиты информации. В меньшей степени затрагиваются вопросы и меры организационного обеспечения ИБ компании - стратегия и тактика защиты информации, концепция и политика безопасности, планы защиты информационных ресурсов компании в штатных и внештатных условиях функционирования КИС. При этом считается само собой разумеющимся, что данная проблема безусловно актуальна для представителей отечественного бизнеса. Однако за кадром остается вопрос: а каковы, собственно, интересы представителей отечественного бизнеса в решении этой проблемы? Ведь стандартных слов о том, что критичная для бизнеса информация должна быть *доступной, целостной и конфиденциальной,* здесь явно недостаточно, поскольку информация - понятие достаточно абстрактное; угрозы ее безопасности носят вероятностный характер (как известно, пока гром не грянет, никто ничего делать не будет), к тому же технические и организационные решения по безопасности стоят немалых денег!

Видимо, объяснение указанному явлению кроется в том, что обсуждается данная проблема в основном в среде технических специалистов или специалистов, имеющих явные «технические корни». Однако с уровня бизнес-управления компанией существование потенциальных угроз для информационных ресурсов компании и наличие критичных технических уязвимостей КИС «не видны», поэтому проблема обеспечения информационной безопасности КИС представляется весьма туманной. Зато вполне понятна такая постановка проблемы: стоит ли тратить деньги на корпоративную систему защиты информации, полезность которой для бизнеса далеко не очевидна? Более того, часто можно услышать такой вопрос: «А зачем нам вообще нужна информационная безопасность? На этом же нельзя заработать!» Или, если говорить на языке бизнеса, - зачем нам создавать еще один затратный центр? Их у нас и так слишком много! И с этими аргументами достаточно трудно спорить. Особенно, если не владеть контраргументами, понятными для представителей отечественного бизнеса. К сожалению, часто российские директора и начальники служб автоматизации (*CIO*), исполнительные директора (CEO), начальники служб информационной безопасности (CISO) таких контраргументов не имеют, хотя интуитивно абсолютно уверены в необходимости решения данной задачи. Итак, что же нужно сделать, чтобы информационная безопасность воспринималась как один из корпоративных бизнес-процессов? Другими словами, как представить ИБ с точки зрения бизнеса?

Очевидно, для этого надо сначала попробовать определить бизнес-задачу ИБ. Одним из основных двигателей рынка автоматизации бизнеса является стремление самого бизнеса стать более эффективным и конкурентоспособным за счет использования современных информационных технологий и совершенствования своей собственной модели. Такое стремление вполне понятно: не так уж много осталось реальных механизмов повышения конкурентоспособности, и все они в основном уже исчерпаны, а информационные технологии предлагают поистине неограниченные возможности. В том, что в автоматизации бизнеса заложен огромный потенциал для его динамического развития, не сомневается сегодня, наверное, уже

никто. Достаточно сравнить эффективность и оперативность работы, например, корпоративной электронной почты с эффективностью и оперативностью многочисленной армии секретарей и машинисток, качество и сроки разработки сложных технических систем посредством CAD/CAM/CAE-систем и с помощью традиционного кульмана и др. Можно сказать, что бизнес-задача КИС, как и любой другой технической системы, состоит в том, чтобы упростить, ускорить или сделать более удобными ранее рутинные и потому медленные и изобилующие ошибками бизнес-процессы. Или, если говорить более строго, любая действующая в интересах бизнеса техническая система в принципе должна предоставлять бизнесу какой-то тип сервиса. Сервис может быть самым разнообразным: доменная печь «оказывает услуги», выплавляя сталь, транспортный цех - транспортируя грузы, заводская столовая - обеспечивая питание сотрудников и т.д. Также и КИС, будучи сугубо технической системой, предлагает бизнесу свой тип сервиса - в данном случае сервис информационный. И этот сервис заключается в предоставлении бизнесу необходимой для принятия решений информации нужного качества, в нужное время и в нужном месте, то есть информации для управления самим бизнесом.

По своей сути информация постепенно становится одним из ключевых элементов бизнеса. Ведь что такое информация с точки зрения бизнеса? В сущности, это не что иное, как некий набор формализованных (в смысле структурированных, разложенных по полочкам и имеющих средства для поиска и представления) знаний бизнеса о самом себе. При этом под информацией можно понимать не только какие-то статичные информационные ресурсы, например бухгалтерский баланс за прошедший год или текущие настройки какого-либо оборудования, но и динамические информационные процессы обработки знаний в виде запрограммированной бизнес-логики работы компании в среде таких популярных приложений, как электронный документооборот, ERP, CRM, службы каталогов и др.

Времена Генри Форда, когда управляющий компанией самостоятельно привинчивал гайки на конвейере, давно миновали. Сегодня высшее руководство любой компании по существу имеет дело только с информацией - и на ее основе принимает решения. Понятно, что эту самую информацию готовят множество нижестоящих слоев достаточно сложной организационной системы, которая называется современным предприятием. И нижние слои этой системы вообще могут не иметь понятия о том, что они производят не только какую-то продукцию или услугу, но и информацию для руководства. По нашему мнению, глубинный смысл автоматизации бизнеса заключается как раз в том, чтобы ускорить и упорядочить информационные потоки между функциональными уровнями и слоями этой системы и представить руководству компании лишь самую необходимую, достоверную и структурированную в удобной для принятия решения форме информацию.

Заметим, информацию *достоверную*! Отсюда нетрудно сделать вывод, что ключевой бизнес-задачей корпоративной системы ИБ является обеспечение гарантий достоверности информации, или, говоря другими словами, гарантий доверительности информационного сервиса КИС.

Попробуем спросить любого представителя отечественного бизнеса, готов ли он потратить, скажем, сто тысяч долларов на закупку, например, пяти межсетевых экранов и ста лицензий на антивирусное ПО. А потом зададим тот же самый вопрос по-другому: готов ли он потратить сто тысяч долларов на защиту информации о самом себе и на защиту сервиса, на котором основано управление компанией? Скорее всего, ответ в первом случае будет таким: либо традиционное для России «Денег нет», либо, как в Одессе, вопросом на вопрос: «А зачем?». Во втором случае вариантов ответов больше: «В какие сроки управимся? А где вы были раньше?». И даже: «А почему так мало? Разве мой бизнес так мало стоит?».

Кроме того, по всей видимости, здесь последует другой интересный вопрос: «А почему именно сто тысяч, а не пятьдесят или, скажем, четыреста семьдесят пять?». И в таком случае CIO, CEO, CISO просто необходимо предоставить понятный для бизнеса ответ, аргументированный

соответствующими экономическими выкладками. То есть по сути предложить обоснование стоимости системы ИБ для бизнеса.

Можно ли провести такой анализ и обосновать стоимость корпоративной системы защиты информации? Внимательный читатель, наверное, уже заметил, что в последнее время в печати все чаще и чаще появляются новые для ИБ темы: анализ угроз ИБ, анализ информационных рисков, оценка совокупной стоимости владения системой безопасности, оценка возврата инвестиций от такой системы и т.д. Все это в виде метрики и меры информационной безопасности представляет собой некий экономический инструментарий, преломленный в область ИБ, который и позволяет ответить на вопрос: «А почему сто тысяч?». И еще - это яркий показатель того, что наиболее «продвинутые» российские CIO, CEO, CISO уже пытаются на него ответить.

Посмотрим, как можно обосновать стоимость корпоративной системы защиты информации. По нашему мнению, таких подходов как минимум два.

Первый подход - назовем его наукообразным - заключается в том, чтобы освоить, а затем применить на практике необходимый инструментарий получения метрики и меры безопасности, а для этого привлечь руководство компании (как ее собственника) к оценке стоимости защищаемой информации, определению вероятностей потенциальных угроз и уязвимостей, а также потенциального ущерба. В этом случае от результатов таких оценок будет во многом зависеть дальнейшая деятельность *CIO* и CISO в области ИБ. Если информация не стоит ничего, существенных угроз для информационных активов компании нет, а потенциальный ущерб минимален - и руководство это *подтверждает* (!) - проблемой ИБ можно, наверное, не заниматься. Если же информация стоит определенных денег, угрозы и потенциальный ущерб ясны, то понятны и рамки бюджета на корпоративную систему ИБ. Существенно, что при этом становится возможным привлечь руководство компании к осознанию проблем ИБ и построению корпоративной системы защиты информации и заручиться его поддержкой.

Второй подход (назовем его практическим) состоит в следующем: можно попробовать найти инвариант разумной стоимости корпоративной системы защиты информации. Ведь существуют аналогичные инварианты в других областях, где значимые для бизнеса события носят вероятностный характер. Например, на рынке автострахования некоторая общая оценка разумной стоимости такой услуги, как страхование собственного автомобиля, составляет оТ5 до 15% его рыночной цены - в зависимости от локальных условий эксплуатации, культуры и опыта вождения водителя, интенсивности движения, состояния дорог и т.д.

По аналогии с автострахованием можно вообще не заниматься ИБ в компании, и не исключен вариант, что принятый риск себя вполне оправдает. А можно потратить на создание корпоративной системы защиты информации немало денег, и все равно останется некоторая уязвимость, что рано или поздно приведет к утечке или хищению конфиденциальной информации. Поэтому эксперты-практики в области защиты информации нашли некий оптимум, позволяющий чувствовать себя относительно уверенно, - стоимость системы ИБ должна составлять примерно 10-20% от стоимости КИС - в зависимости от уровня конфиденциальности информации. Это и есть та самая оценка на основе практического опыта (best practice), на которую можно положиться. И на вопрос «А почему для создания адекватной целям и задачам бизнеса корпоративной системы защиты информации требуется сто тысяч долларов?» отвечать «Потому что на сегодняшний день стоимость нашей КИС составила один миллион долларов!».

Очевидно, что второй подход не лишен недостатков. Здесь, скорее всего, не удастся заставить руководство глубоко осознать проблемы ИБ. Но зато можно смело прогнозировать объем бюджета на ИБ и существенно сэкономить на услугах внешних консультантов.

1.2 Развитие службы информационной безопасности

Вместе с развитием любой отечественной компании (и ростом стоимости ее информационных активов) в той же мере развивается и служба информационной безопасности.

При этом определение стратегии и тактики работы службы информационной безопасности становится одной из основных функций TOP-менеджмента компании. Действительно, сегодня успех реализации политики информационной безопасности компании зависит не только от организационных и технических решений в области защиты информации, но и от квалификации и компетентности соответствующих кадров. Вспомним известный тезис: «Кадры решают все!».

Покажем роль и место службы информационной безопасности в организационной структуре компании, а также попробуем сформулировать современные квалификационные требования к сотрудникам этой службы.

Возможная организационная структура TOP-менеджмента компании, ответственного за организацию режима информационной безопасности, представлена на рис. 1.1.

Согласно исследованию KPMG за 2002 год (см. приложение 1) в наиболее благополучных с точки зрения ИБ западных компаниях функцией обеспечения информационной безопасности занимается отдельное подразделение, наделенное полномочиями и имеющее поддержку высшего руководства компании. При этом почти в половине «успешных» компаний ответственность за ИБ закреплена за советом директоров, что наиболее характерно для финансового сектора. Действительно, непосредственное участие TOP-менеджмента организации требуется для корректного определения и постановки «правильных» целей и задач в области ИБ, позволяющих без ущерба для бизнеса компании обеспечивать информационную безопасность. Кроме того, как правило, только руководство компании способно поддержать обеспечение безопасности надлежащим уровнем инвестирования и другими необходимыми ресурсами.

В российских компаниях в настоящее время наблюдаются следующие основные тенденции развития службы ИБ:

– ранее (а зачастую и сейчас) в большинстве российских компаний проблемой информационной безопасности организации занимались отделы и службы автоматизации. Сегодня ведущие отечественные компании идут путем выделения подразделения информационной безопасности в отдельную службу с соответствующими организационными, кадровыми и финансовыми изменениями. При этом создаются две ключевые позиции специалистов, ответственных за информационную безопасность: CISO (Chief Information Security Officer) –

Рис. 1.1. Организационная структура TOP-менеджмента компании, ответственного за обеспечение безопасности

- директор службы информационной безопасности, который отвечает, главным образом, за разработку и реализацию политики безопасности компании, адекватной целям и задачам бизнеса компании; BISO (Business Information Security Officer) - менеджер службы информационной безопасности, занимающийся практической реализацией политики ИБ на уровне подразделения, например планово-экономического отдела, службы маркетинга или автоматизации;
- в некоторых компаниях наблюдается слияние служб информационной и физической безопасности в единое подразделение, в задачу которого входит обеспечение безопасности в целом, включая защиту перспективных планов развития компании и ее активов, а также решение вопросов контроля и управления доступом и пр.;
- статус CISO становится адекватным (равным) статусу ведущих TOP-менеджеров компании, отвечающих за стратегическое развитие компании.

Посмотрим теперь, каким квалификационным требованиям должен соответствовать руководитель современной службы информационной безопасности (CISO).

Главная задача CISO - оценка технологических, производственных и информационных рисков компании и управление ими. Это предполагает, что данный специалист должен быть

способен идентифицировать риски и управлять ими в соответствии с целями и задачами компании и текущим уровнем ее развития. Дополнительно свою специфику вносит сфера деятельности компании, а также ее размер и стоимость информационных активов.

Основными функциями CISO могут быть следующие:

- разработка концепции и политики информационной безопасности компании, включая регламенты, корпоративные стандарты, руководства и должностные инструкции;
- выработка принципов классификации информационных активов компании и оценивания их защищенности;
- оценка информационных рисков и управление ими;
- обучение сотрудников компании методам обеспечения ИБ, проведение инструктажей и контроль знаний и практических навыков выполнения политики безопасности сотрудниками компании;
- консультирование менеджеров компании по вопросам управления информационными рисками;
- согласование частных политик и регламентов безопасности среди подразделений компании;
- работа в составе рабочих групп или экспертных советов для оценивания рисков исполнения и развития бизнеса компании;
- контроль работы служб качества и автоматизации компании с правом проверки и утверждения внутренних отчетов и документов;
- совместная деятельность со службой физической безопасности в части, касающейся их обоих, например обеспечение конфиденциальности научно-исследовательской работы (НИОКР) или поддержание контрольно-пропускного режима;
- взаимодействие со службой персонала компании по проверке личных данных сотрудников при найме на работу;
- организация мероприятии по устранению нештатных ситуаций или чрезвычайных происшествий в области защиты информации в случае их возникновения;
- информационное обеспечение руководства компании регулярными обзорами и аналитическими справками о текущем состоянии информационной безопасности компании, выдержками о результатах проверки выполнения политики безопасности;
- предоставление менеджерам компании информационной поддержки по вопросам ИБ, в частности сведений об изменениях в законодательстве и нормативной базе в сфере защиты информации, о технических новинках и пр.

Представляется разумным, чтобы руководитель службы информационной безопасности (CISO) входил в верхний эшелон управления компанией и умел увязывать потребности бизнеса и требования безопасности с учетом степени развития информационных технологий, возросшей активности разного рода злоумышленников, изменяющихся положений законодательства, а также ожиданий партнеров по бизнесу. При этом отметим, что потребности бизнеса могут вступать в противоречие с требованиями обеспечения информационной безопасности. В этом случае CISO должен быть в состоянии «переводить» технические вопросы и проблемы на язык, понятный представителям отечественного бизнеса. В свою очередь это означает, что в дополнение к солидному основному и дополнительному образованию (сертификация CISSP (ISC^2), SANS, MCSE, CISA, ABCP и пр.), а также опыту работы в области защиты информации (не менее 3-5 лет) CISO, несомненно, должен обладать некоторыми личностными качествами. Например, аналитическим складом ума, способностями в области стратегического и операционного менеджмента, лояльностью к организации и пр. Понятно, что для этого недостаточно иметь лишь специальное техническое образование, так же как только экономическое или управленческое.

Поэтому позицию CISO, скорее всего, будут занимать аудиторы или аналитики с достаточным опытом работы в сфере защиты информации.

1.3 Международная практика защиты информации

В настоящее время сложилась общепринятая международная практика (best practice) обеспечения режима информационной безопасности, применяемая как в России, так и в других странах. Здесь и далее под информационной безопасностью (ИБ) понимается защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий естественного или искусственного характера, приводящих к нанесению ущерба владельцам и пользователям информации, а также поддерживающей инфраструктуре в целом.

При обеспечении режима ИБ достаточно важное место отводится задачам анализа информационных рисков компании и управления ими. Действительно, в на- различных представителей отечественного бизнеса. Рассмотрим подробнее работы по обеспечению режима ИБ и покажем роль и место задач анализа и управления рисками.

Вне зависимости от размеров организации и специфики ее информационной системы работы по обеспечению режима ИБ обычно состоят из следующих этапов (рис. 1.2):

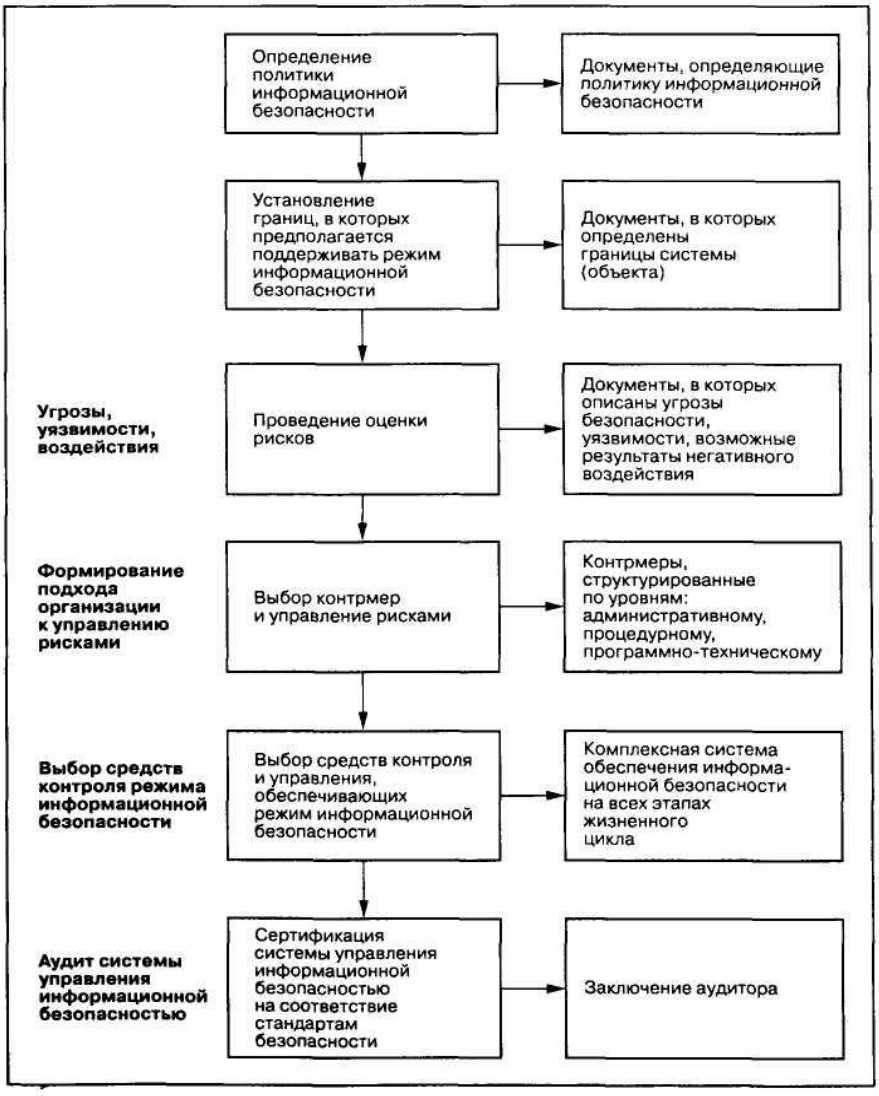


Рис.1.2. Обеспечение режима информационной безопасности. Основные этапы

- выработка политики безопасности;
- определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания;
- оценка рисков;
- выбор контрмер, обеспечивающих режим ИБ;
- управление рисками;
- аудит системы управления ИБ.

Ниже представлен развернутый комментарий для каждого из перечисленных этапов.

Как правило, *определение политики безопасности* сводится к ряду практических этапов.

Этап 1. Выбор национальных и международных руководящих документов и стандартов в области ИБ и формулирование на их базе основных требований и положений политики ИБ компании, включая:

- управление доступом к средствам вычислительной техники (СВТ), программам и данным, а также антивирусную защиту;
- вопросы резервного копирования;
- проведение ремонтных и восстановительных работ;
- информирование об инцидентах в области ИБ и пр.

Этап 2. Выработка подходов к управлению информационными рисками и принятие решения о выборе уровня защищенности КИС. Уровень защищенности в соответствии с зарубежными стандартами может быть минимальным (базовым) либо повышенным. Этим уровням защищенности соответствует минимальный (базовый) или полный вариант анализа информационных рисков.

Этап 3. Структуризация контрмер по защите информации по следующим основным уровням: административному, процедурному, программно-техническому.

Этап 4. Установление порядка сертификации и аккредитации КИС на соответствие стандартам в сфере ИБ. Назначение периодичности проведения совещаний по тематике ИБ на уровне руководства, в том числе периодического пересмотра положений политики ИБ, а также порядка обучения всех категорий пользователей информационной системы в области ИБ.

Известно, что выработка политики безопасности организации - наименее формализованный этап. Однако в последнее время именно здесь сосредоточены усилия многих специалистов по защите информации. В результате этот этап удается формализовать все в большей степени. Примером является доступное в Internet «Руководство по политике безопасности для автоматизированных информационных систем» [199], в котором достаточно подробно рассмотрены:

- общие положения политики безопасности;
- жизненный цикл безопасности КИС;
- минимальные (базовые) требования в области ИБ.

Следующий этап - определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания.

На этом этапе определяются границы системы, для которой должен быть обеспечен режим ИБ. Соответственно, система управления ИБ строится именно в этих границах. Само описание границ системы рекомендуется выполнять по следующему плану:

- структура организации. Представление существующей структуры и изменений, которые предполагается внести в связи с разработкой (модернизацией) автоматизированной системы;

- ресурсы информационной системы, подлежащие защите. Целесообразно рассмотреть ресурсы автоматизированной системы следующих классов: СВТ, данные, системное и прикладное ПО. Все ресурсы представляют ценность с точки зрения организации. Для их оценки должна быть выбрана система критериев и методика получения результатов по этим критериям;
- технология обработки информации и решаемые задачи. Для решаемых задач следует построить модели обработки информации в терминах ресурсов;
- размещение средств СВТ и поддерживающей инфраструктуры.

Как правило, на этом этапе составляется документ, в котором фиксируются границы информационной системы, перечисляются информационные ресурсы компании, подлежащие защите, приводятся система критериев и методики для оценки ценности информационных активов компании.

На этапе *постановки задачи оценки рисков* обосновываются требования к методике оценки информационных рисков компании.

В настоящее время существуют различные подходы к оценке рисков. Выбор подхода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер по защите информации. В частности, различают минимальные, или базовые, и повышенные, или полные, требования к режиму ИБ.

Минимальным требованиям к режиму ИБ соответствует базовый уровень ИБ. Такие требования применяются, как правило, к типовым проектным решениям. Существует ряд стандартов и спецификаций, в которых приводится минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ и т.д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры - вне зависимости от вероятности их осуществления и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать необязательно. Зарубежные стандарты в этой области обсуждаются в главе 2.

В случаях, когда нарушения режима ИБ ведут к тяжелым последствиям, базового уровня требований к режиму ИБ недостаточно и предъявляются дополнительно повышенные требования. Для формулирования дополнительных повышенных требований необходимо:

- определить ценность ресурсов;
- к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;
- рассчитать вероятности угроз;
- выявить уязвимости ресурсов;
- оценить потенциальный ущерб от воздействий злоумышленников.

Возможные подходы к выбору дополнительных требований описаны в главе 3.

Несмотря на существенную разницу в методологии обеспечения базового и повышенного уровней безопасности, можно говорить о едином подходе к организации режима ИБ (рис. 1.3).

Рис. 1.3. Организация режима информационной безопасности

На этапе управления рисками разрабатывается некоторая стратегия управления рисками. Например, здесь возможны следующие подходы к управлению информационными рисками компании:

- уменьшение риска;
- уклонение от риска;
- изменение характера риска;
- принятие риска.

Рассмотрим указанные подходы подробнее.

Уменьшение рисков. Многие риски удается значительно уменьшить за счет весьма простых и дешевых контрмер. Например, грамотное управление паролями снижает риск несанкционированного доступа.

Уклонение от риска. От некоторых классов рисков можно уклониться. Так, вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов.

Изменение характера риска. Если не удается уклониться от риска или эффективно его уменьшить, можно принять некоторые меры страховки. Например:

- застраховать оборудование от пожара;
- заключить договор с поставщиками СВТ о сопровождении и компенсации ущерба, вызванного нештатными ситуациями.

Принятие риска. Многие риски нельзя довести до пренебрежимо малой величины. На практике после принятия стандартного набора контрмер некоторые риски уменьшаются, но остаются все еще значимыми. Необходимо знать остаточную величину риска.

В результате выполнения данного этапа для принимаемых во внимание информационных рисков компании должна быть предложена стратегия управления рисками.

Следующий этап - *выбор контрмер,* обеспечивающих режим ИБ. На этом этапе обоснованно выбирается комплекс различных контрмер для защиты информации, структурированных по нормативно-правовому, организационно-управленческому,

технологическому и аппаратно-программному уровням обеспечения информационной безопасности. В дальнейшем предлагаемый комплекс контрмер реализуется в соответствии с принятой стратегией управления информационными рисками. Если проводится полный вариант анализа рисков, то для каждого риска дополнительно оценивается эффективность комплекса контрмер защиты информации.

И наконец, на этапе *аудита системы управления ИБ* проверяется соответствие выбранных контрмер по защите информации целям и задачам бизнеса, декларированным в политике безопасности компании, выполняется оценка остаточных рисков и, в случае необходимости, оптимизация рисков. Вопросам аудита и процедуре сертификации информационной технологии на соответствие требованиям ИБ посвящена глава 5.

1.3.1 Модель Symantec LifeCycle Security

В качестве примера возможной организации режима ИБ рассмотрим модель Lifecycle Security, разработанную компанией Axent (после приобретения Axent компанией Symantec модель получила название Symantec Lifecycle Security). Модель Lifecycle Security регламентирует и описывает этапы построения корпоративной системы защиты информации и организации режима ИБ компании в целом. Выполнение представленного в ней набора процедур позволяет системно решать задачи, связанные с защитой информации, и дает возможность оценить эффект от затрат на технические и организационные средства и меры защиты информации. С этой точки зрения идеология Lifecycle Security может быть противопоставлена тактике «точечных решений», заключающейся в том, что все усилия сосредотачиваются на внедрении отдельных частных решений (например, межсетевых экранов или систем аутентификации пользователей на основе смарт-карт или e-Token). Без предварительного анализа и планирования подобная тактика нередко приводит к появлению в корпоративной информационной системе набора разрозненных средств защиты информации, которые несовместимы между собой и не интегрируются друг с другом, что не позволяет эффективно решить проблему обеспечения информационной безопасности предприятия.

Модель Lifecycle Security состоит из семи основных этапов (рис. 1.4).

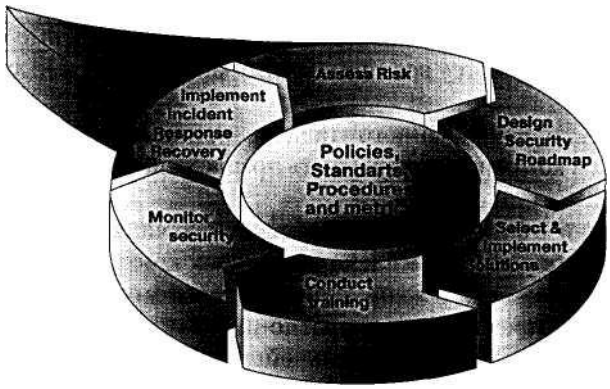


Рис. 1.4. Этапы модели LifeCyde Security

Политики безопасности, стандарты, процедуры и метрики. На этом этапе определяются границы и рамки, в которых осуществляются мероприятия по обеспечению информационной безопасности, и задаются критерии для оценивания полученных результатов. Отметим, что под стандартами здесь понимаются не только государственные и международные стандарты в сфере информационной безопасности, но и корпоративные стандарты, в ряде случаев существенно влияющие на проект создаваемой корпоративной системы защиты информации. Рекомендуемое введение метрики позволяет оценить состояние системы до начала, а также после проведения работ по защите информации. Кроме того, метрика устанавливает единицы измерения и порядок

измерения защищенности КИС, что дает возможность соотнести затраты предприятия на ИБ и полученный эффект от внедренной корпоративной системы защиты информации.

Анализ рисков. Этот этап является своего рода отправной точкой для установления и поддержки эффективного управления системой защиты. По данным анализа рисков удается подробно описать состав и структуру информационной системы (если по каким-то причинам это не было сделано ранее), ранжировать имеющиеся ресурсы по приоритетам, базируясь на степени их важности для нормальной работы предприятия, выявить угрозы и идентифицировать уязвимости системы.

Стратегический план построения системы защиты. Результаты анализа рисков используются как основа для разработки стратегического плана построения системы защиты. Наличие подобного плана помогает распределить по приоритетам бюджеты и ресурсы, а в последующем выбрать средства защиты информации и разработать стратегию и тактику их внедрения.

Выбор и внедрение решений. Четкие критерии принятия решений в сфере защиты информации и наличие программы внедрения уменьшают вероятность приобретения средств защиты информации, которые становятся «мертвым грузом», мешающим развитию информационной системы предприятия. На данном этапе следует также учитывать качество предоставляемых поставщиками сервисных и обучающих услуг. Кроме того, необходимо четко определить роль внедряемого решения в выполнении разработанных планов и достижении поставленных целей в области защиты информации.

Обучение персонала. Знания в области информационной безопасности и технические тренинги нужны для построения и обслуживания безопасной вычислительной среды компании. Усилия, затраченные на обучение персонала, окупаются значительным повышением шансов на успех мероприятий по защите КИС.

Мониторинг защиты. Данный этап помогает выявить аномалии или вторжения в корпоративную информационную систему, а также позволяет оперативно контролировать эффективность системы защиты информации.

Разработка методов реагирования в случае инцидентов и восстановление. Без наличия заранее разработанных и «отрепетированных» процедур реагирования на инциденты в сфере безопасности невозможно гарантировать, что в случае обнаружения атаки действиям злоумышленника будут противопоставлены эффективные меры защиты и работоспособность системы удастся быстро восстановить.

Существенно, что в модели Lifecycle Security все вышеуказанные этапы взаимосвязаны между собой и предполагается непрерывность процесса совершенствования корпоративной системы защиты информации. При этом этапу анализа информационных рисков в данной модели отводится достаточно важная роль. Анализ рисков рекомендуется проводить в случаях:

- обновления информационной системы или существенных изменений в ее структуре;
- перехода на новые информационные технологии построения КИС;
- организации новых подключений в компании (например, подключения локальной сети филиала к сети головного офиса);
- подключения к глобальным сетям (в первую очередь к Internet);
- изменений в стратегии и тактике ведения бизнеса (например, при открытии электронного магазина);
- проверки эффективности корпоративной системы защиты информации.

Ключевыми моментами анализа информационных рисков КИС являются:

- подробное документирование и картирование системы, причем особое внимание необходимо уделять критически важным для бизнеса приложениям;

- определение степени зависимости организации от штатного функционирования и структурных элементов системы, безопасности хранимых и обрабатываемых данных;
- обнаружение и учет уязвимых мест;
- выявление и учет потенциальных угроз;
- оценка и учет информационных рисков;
- оценка потенциального ущерба собственникам информации и КИС в целом.

Отметим, что метрика и мера защищенности КИС определяют процедуру анализа рисков. С другой стороны, результаты анализа информационных рисков предоставляют необходимые начальные условия для разработки или совершенствования существующей корпоративной системы защиты информации.

1.4 Постановка задачи анализа рисков

Постановка задачи обеспечения информационной безопасности может варьироваться в широких пределах. Соответственно, варьируется и постановка задач анализа рисков.

Основным фактором, от которого зависит отношение организации к вопросам информационной безопасности, является степень ее зрелости. Так, например, известная аналитическая компания Gartner Group и университет Carnegie Mellon предложили свои модели определения зрелости компании. Различным уровням зрелости соответствуют разные потребности в области информационной безопасности. Далее упомянутые модели обсуждаются подробнее.

1.4.1 Модель Gartner Group

Gartner Group выделяет четыре уровня зрелости компании - начиная с нулевого и заканчивая третьим (см. табл. 1.1).

Согласно данным Gartner Group, на начало 2002 года компании распределились по уровням зрелости следующим образом: 30% компаний - 0-го уровня, 55% - 1-го уровня, 10% - 2-го уровня и 5% - 3-го уровня. В 2005 году, по мнению Gartner Group, процентное соотношение между компаниями разного уровня изменится так: 20% - компаний 0-го уровня, 35% - 1-го уровня, 30% - 2-го уровня и 15% - 3-го уровня зрелости.

1.4.2 Модель Carnegie Mellon University

Несколько расширенную модель определения уровня зрелости компании с точки зрения информационной безопасности предложил университет Carnegie Mellon

Таблица 1.1. Уровни зрелости компании с точки зрения ИБ

Уровень зрелости	Характеристика организации режима информационной безопасности компании
0	Необходимость обеспечения ИБ компании в должной мере не осознана и формально такая задача не ставится. Выделенной службы информационной безопасности нет. Служба автоматизации использует традиционные механизмы и средства защиты информации стека протоколов TCP/IP и сервисов Intranet, а также операционной среды и приложений (ОС, СУБД, СППР, ERP, ERP II, CRM)
1	Проблема обеспечения ИБ рассматривается управлением компании как исключительно техническая. Выделенной службы защиты информации нет. Организационные меры поддержания ИБ не принимаются. Финансирование осуществляется в рамках единого бюджета на IT-технологии. Служба автоматизации дополнительно к средствам защиты информации уровня 0 может привлекать средства отказоустойчивости, резервного копирования информации, источники бесперебойного питания, а также межсетевые экраны, виртуальные частные сети (VPN), антивирусные средства, средства прозрачного шифрования и e-Token

2	Проблема обеспечения ИБ компании осознана и рассматривается как взаимно увязанный комплекс организационных и технических мер. Внедрены методики анализа информационных рисков, отвечающие минимальному, базовому, уровню защищенности КИС. В компании определены состав и структура штатной службы ИБ. Принята корпоративная политика информационной безопасности. Финансирование ведется в рамках отдельного бюджета на создание и поддержку корпоративной системы защиты информации. Служба ИБ дополнительно к средствам защиты информации уровней 0 и 1 привлекает средства защиты от НСД, системы обнаружения вторжений (IDS), инфраструктуру открытых ключей (PKI), а также соответствующие политике безопасности компании организационные меры (внешний и внутренний аудит, разработка планов защиты и непрерывного ведения бизнеса, действия во внештатных ситуациях и пр.)
3	Проблема обеспечения ИБ компании осознана в полной мере. Наряду с бизнес-культурой существует понятие культуры информационной безопасности компании. Активно применяются методики полного количественного анализа информационных рисков, а также соответствующие инструментальные средства. Введена штатная должность — директор службы информационной безопасности (CISO). Определены состав и структура группы внутреннего аудита безопасности КИС (CISA), группы предупреждения и расследования компьютерных преступлений, группы экономической безопасности. Руководством компании утверждены концепция и политика безопасности, план защиты и другие нормативно-методические материалы и должностные инструкции. Финансирование выделяется исключительно в рамках отдельного бюджета. Служба ИБ дополнительно к средствам защиты информации уровней 0-2 обращается к средствам централизованного управления ИБ компании и средствам интеграции с платформами управления сетевыми ресурсами

[344]. В соответствии с этой моделью выделяется пять уровней зрелости компании, которым можно поставить в соответствие различное понимание проблем информационной безопасности организации (см. табл. 1.2).

Таблица 1.2. Модель определения уровня зрелости компании

Уровень зрелости организации	**Признаки**	**Характеристика организации в области информационной безопасности**
1. Анархия	Сотрудники сами определяют, что хорошо, а что плохо Затраты и качество не прогнозируются Отсутствуют формализованные планы Отсутствует контроль изменений Высшее руководство плохо представляет реальное положение дел	Политика в области ИБ не формализована, руководство не занимается этими вопросами Обеспечением информационной безопасности сотрудники могут заниматься по своей инициативе, в соответствии со своим пониманием задач
2. Фольклор	Выявлена определенная повторяемость организационных процессов Опыт организации представлен в виде преданий корпоративной мифологии Знания накапливаются в виде личного опыта сотрудников и пропадают при их увольнении	На уровне руководства существует определенное понимание задач обеспечения информационной безопасности. Существуют стихийно сложившиеся процедуры обеспечения информационной безопасности, их полнота и эффективность не анализируются. Процедуры не документированы и полностью зависят от личностей вовлеченных в них сотрудников. Руководство не ставит задач формализации процедур защиты информации

3, Стандарты	Корпоративная мифология записана на бумаге Процессы повторяемы и не зависят от личных качеств исполнителей Информация о процессах для измерения эффективности не собирается Наличие формализованного описания процессов не означает, что они работают Организация начинает адаптировать свой опыт к специфике бизнеса Производится анализ знаний и умений сотрудников с целью определения необходимого уровня компетентности Вырабатывается стратегия развития компетентности	Руководство осознает задачи в области информационной безопасности. В организации имеется документация (возможно, неполная), относящаяся к политике информационной безопасности. Руководство заинтересовано в использовании стандартов в области информационной безопасности, оформлении документации в соответствии с ними. Осознается задача управления режимом ИБ на всех стадиях жизненного цикла информационной технологии
4. Измеряемый	Процессы измеряемы и стандартизованы	Имеется полный комплект документов, относящихся к обеспечению режима информационной безопасности и оформленных в соответствии с каким-либо стандартом. Действующие инструкции соблюдаются, документы служат руководством к действию должностных лиц. Регулярно проводится внутренний (и, возможно, внешний) аудит в области ИБ. Руководство уделяет должное внимание вопросам информационной безопасности, в частности имеет адекватное представление относительно существующих уровней угроз и уязвимостей, потенциальных потерь в случае возможных инцидентов
5. Оптимизируемый	Фокус на повторяемости, измерении эффективности, оптимизации Вся информация о функционировании процессов фиксируется	Руководство заинтересовано в количественной оценке существующих рисков, готово нести ответственность за выбор определенных уровней остаточных рисков, ставит оптимизационные задачи построения системы защиты информации

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

На первом уровне эта проблема, как правило, руководством формально не выдвигается. Но это не значит, что она не решается сотрудниками по собственной инициативе - и, возможно, эффективно.

В качестве положительного примера можно привести один случай. Сравнительно небольшая организация (порядка 80 компьютеров, три файл-сервера), занимающаяся рекламным бизнесом, в результате пожара в арендуемом ею здании потеряла всю вычислительную технику и данные.

Однако уже через неделю она полностью смогла восстановить свою работу. Дело в том, что некоторые сотрудники по своей инициативе копировали наиболее важную информацию на CD, что-то хранилось на их домашних компьютерах, что-то отправлялось по электронной почте различным адресатам и было затребовано обратно. В результате большую часть самых ценных информационных ресурсов удалось оперативно восстановить (а технику быстро закупили), что позволило фирме успешно продолжить работу.

При этом вопросы информационной безопасности руководством никогда не ставились и, по-видимому, ставиться не будут.

Наряду со случаями, в которых все кончалось благополучно, есть и много иных примеров, когда пренебрежение информационной безопасностью 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. И все же такие 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 поднимается. Таким образом, постепенно складывается неформальный список актуальных для организации классов рисков, который постепенно пополняется.

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

В случае серьезного инцидента сложившаяся система обеспечения безопасности корректируется, а необходимость поиска других возможных уязвимостей в защите иногда осознается руководством.

Один из вариантов определения риска в этом случае может выглядеть так: известны уязвимости, потенциальные нарушители и их мотивация (модель нарушителя), а также сценарии развития событий, связанные с выявленными уязвимос-тями [334].

Для данного уровня зрелости организации типичной является локальная (не связанная с другими этапами жизненного цикла технологии) постановка задачи анализа рисков: считается достаточным перечислить актуальные для конкретной информационной системы классы рисков и, возможно, описать модель нарушителя, а задача анализа вариантов контрмер, их эффективности, управления рисками, как правило, не рассматривается в качестве актуальной.

На третьем уровне в организации принято следовать в той или иной мере (возможно, частично) стандартам и рекомендациям, обеспечивающим базовый уровень информационной безопасности (например, ISO 17799 [209]). Вопросам документирования уделяется должное внимание.

Задача анализа рисков не является, по мнению руководства, своевременной. Анализ рисков рассматривается как один из элементов технологии управления режимом информационной безопасности на всех стадиях жизненного цикла. Понятие риска включает несколько аспектов: вероятность, угрозу, уязвимость, иногда стоимость.

Один из вариантов оценки 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 содержит 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 управления 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 главе 3.

На четвертом уровне для руководства организации актуальны вопросы измерения параметров, характеризующих режим информационной безопасности. На этом уровне руководство отвечает 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 и эффективность различных вариантов контрмер при управлении рисками.

На пятом уровне ставятся и решаются различные варианты оптимизационных задач в области обеспечения режима информационной безопасности. Примеры постановки 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 установленном уровне остаточных рисков.

1.4.3 Различные взгляды на защиту информации

Распределение организаций по их подходам к вопросам информационной безопасности иллюстрируют следующие диаграммы, относящиеся к развитым зарубежным странам (заимствованы из обзора компании KPMG), - см. рис. 1.5 и 1.6.

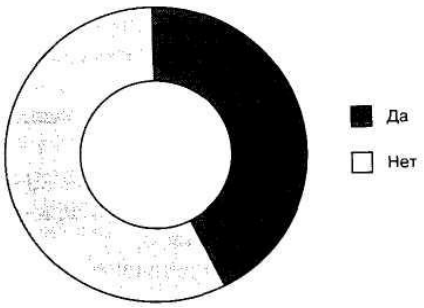


Рис 1.5. Контролируются ли в вашей организации инциденты в области информационной безопасности?

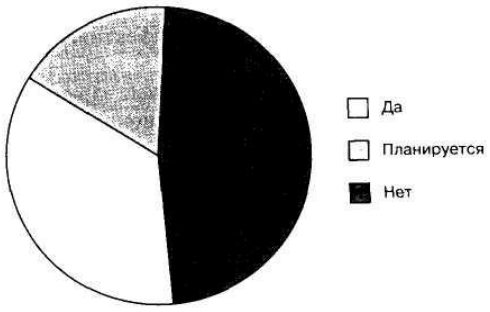


Рис. 1.6. Применяете ли вы формальные критерии для оценки системы информационной безопасности?

В табл. 1.3 показано, по каким критериям (если они используются) организации оценивают систему информационной безопасности.

Таблица 1.3. Критерии оценки корпоративной системы защиты информации

Критерии	Процент использования
Корпоративные стандарты (собственная разработка)	43
Замечания аудиторов	40
Стандарты лучшей мировой практики (например, BS 7799/ISO 17799)	29
Число инцидентов в области безопасности	22
Финансовые потери в результате инцидентов	22
Расходы на ИБ	16
Эффективность в достижении поставленных целей	14

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), пользующиеся (или планирующие пользоваться) какими-либо подходами к оценке системы информационной безопасности, следуют стандартным рекомендациям и руководствам класса «Good Practice», относящимся к базовому уровню информационной безопасности. Эти организации внедряют или планируют внедрить систему управления рисками базового уровня (возможно, ее элементы) на всех стадиях жизненного цикла информационной технологии.

Организации, принадлежащие к четвертому и пятому уровням зрелости, составляют 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 дополнительные возможности, позволяющие выполнять количественный анализ и оптимизацию 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 востребованы в настоящее время простейшие методики анализа рисков, являющиеся частью методик управления рисками базового уровня.

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

1.5 Национальные особенности защиты информации

При выполнении работ в области защиты информации и, в частности, при анализе информационных рисков необходимо учитывать некоторые специфические национальные особенности организации режима информационной безопасности на объектах информатизации в России. Как минимум можно выделить две такие особенности:

- концептуальные отличия действующих российских руководящих документов от аналогичных зарубежных стандартов;
- отсутствие в подавляющем большинстве случаев настоящих неформальных собственников информационных ресурсов, то есть лиц, заинтересованных в реальном обеспечении режима информационной безопасности, принятии на себя ответственности за выбор определенных величин остаточных рисков (которые всегда присутствуют в КИС).

Рассмотрим указанные особенности подробнее.

1.5.1 Особенности отечественных нормативных документов

Большинство документов Гостехкомиссии при Президенте РФ в области защиты информации датируются 1992 годом и относятся к информационным технологиям на базе уже устаревших аппаратных средств. Документы отражают «военную» точку зрения на проблемы информационной безопасности, в соответствии с которой основные усилия направлены на обеспечение конфиденциальности (защищенности от несанкционированного доступа - НСД). Другим аспектам - сохранению целостности и доступности — уделено гораздо меньше внимания. При этом особенности современных автоматизированных систем (АС) гражданского применения не учитываются.

Требования к безопасности АС сформулированы по подсистемам. Устанавливается 9 классов защищенности АС от НСД к информации. Каждый класс характеризуется некоторой минимальной совокупностью требований к защите. Классы подразделяются на три группы в зависимости от специфики обработки информации в АС: группа 3 - это АС, где работает один пользователь, допущенный ко всей информации; группа 2 - пользователи имеют одинаковые права доступа к информации разного уровня конфиденциальности; группа 1 - многопользовательские АС с разными правами доступа пользователей к различным категориям информации.

В пределах каждой группы соблюдается иерархия требований по защите.

Представление об этих требованиях дает таблица из документа «Классификация автоматизированных систем и требования по защите информации» [23].

Эксперты утверждают, что в настоящее время в России действует нормативная база в области безопасности информационных технологий, разработанная в начале 90-х годов. Данная нормативная база уже не в полной мере соответствует уровню развития информационных технологий и не обеспечивает требуемого уровня защиты информационных ресурсов. Поэтому следует продолжать поступательное совершенствование нормативной базы на основе развития отечественной науки и использования опыта передовых мировых держав, постепенно переходя к принятым в настоящее время в Европе «Общим критериям» [41].

В 2004 году в России вводится в экспериментальном режиме международный стандарт ISO 15408 («Общие критерии»), который можно будет применять как альтернативу действующим РД Гостехкомиссии при обеспечении информационной безопасности в автоматизированных системах, не содержащих сведения, относящиеся к государственной тайне. В международном стандарте ISO 15408 «Общие критерии оценки безопасности информационных технологий» обобщен опыт использования «Оранжевой книги» - Европейских критериев ITSEC. Требования по ИБ хорошо структурированы и сформулированы для большого числа классов ИС. Стандартом можно пользоваться как при задании требований к продуктам и системам ИТ, так и при оценке их безопасности на всех этапах жизненного цикла.

Документ состоит из следующих основных частей:

Часть 1. «Представление и общая модель». Определяются общая концепция, принципы и цели оценки безопасности ИТ [211].

Часть 2. «Требования к функциям безопасности». Приведены требования к функциям безопасности и установлен набор показателей для оценки безопасности информационных технологий. Имеется каталог требований к различным семействам и классам ИС [215].

Часть 3. «Требования гарантированности безопасности». Перечислены требования к гарантиям безопасности, сгруппированные в семейства, классы и уровни. Определены критерии оценки для профилей защиты и заданий по безопасности [216].

С практической точки зрения существенным является то, что в документе формулируются только критерии оценки и не содержатся методики ее проведения. В значительной мере остается

открытым вопрос выбора комплекса мер безопасности применительно к рассматриваемым классам информационных технологий.

Однако, по мнению авторов, принятие и ввод в действие в России международного стандарта «Общие критерии» ИСО/МЭК 15408 - безусловно нужный, но явно запоздалый шаг. Эксперты отмечают, что на апробацию и практическое освоение этого стандарта уйдет несколько лет. Сегодня этим стандартом пользуются только отдельные энтузиасты.

В целом же в России мало известны документы класса «Good Practice» - многочисленные зарубежные стандарты и рекомендации, например ISO 17799 (BS 7799), BSI, которые отвечают на вопрос, как обеспечить режим информационной безопасности на практике.

В результате большинство российских КИС не соответствует даже начальному, так называемому базовому, уровню защищенности, который определяется в соответствии с современными зарубежными стандартами, например ISO 17799.

1.5.2 Учет остаточных рисков

Второй национальной особенностью организации режима информационной безопасности в отечественных компаниях является специфическое отношение к остаточным информационным рискам. При построении корпоративной системы защиты информации необходимо помнить, что абсолютной 100-процентной защиты не существует, остаточные риски присутствуют при любом варианте создания или реорганизации корпоративной системы защиты информации. Понятно, что чем больше защищена КИС, тем меньше такие риски.

Настоящий собственник информационных ресурсов должен сам выбирать допустимый уровень остаточных рисков и нести ответственность за свой выбор. К сожалению, в российских компаниях это делается крайне редко. В соответствии с РД Гостехкомиссии при Президенте РФ автоматизированным системам отечественных предприятий, в зависимости от своего класса, надлежит иметь подсистемы безопасности с определенными формальными свойствами. При этом зачастую существует мнение, что сама постановка задачи об остаточных информационных рисках в области информационной безопасности, неизбежно присутствующих в любой АС (и об ответственности за их уровень), некорректна, особенно в случае обработки сведений, составляющих государственную тайну.

В плане подхода к обеспечению ИБ в АС можно выделить четыре группы отечественных заказчиков работ в области защиты информации:

- государственные структуры;
- коммерческие структуры с формальными собственниками информационных ресурсов компании;
- коммерческие структуры с настоящими собственниками информационных ресурсов компании;
- структуры, для которых обязательно соответствие зарубежным стандартам в области информационной безопасности.

Как правило, *в государственных структурах* ответственные лица и руководители, занимающиеся организацией режима информационной безопасности на предприятии, пока не заинтересованы в том, чтобы нести бремя ответственности за выбор остаточных информационных рисков. Поэтому решения относительно построения корпоративной системы защиты информации отвечают в обязательном порядке только принятым и утвержденным российским стандартам и РД. Как следствие, исполнители работ в области защиты информации, например системные интеграторы, вынуждены предлагать решения, удовлетворяющие лишь формальным требованиям существующих нормативов и РД. При этом предлагаемые и внедряемые решения не соответствуют в целом даже начальному базовому уровню обеспечения информационной безопасности, который определяется согласно современным международным стандартам в

области информационной безопасности. К сожалению, в настоящее время государственные структуры уделяют мало внимания новым идеям и направлениям развития в области защиты информации. По мнению аналитиков, ситуация начнет изменяться в течение ближайших двух-пяти лет - после принятия новых российских стандартов и РД, адекватных целям и задачам развития национальной системы информационной безопасности.

Вторая группа - *коммерческие структуры с формальными собственниками* информационных ресурсов (сюда же относятся структуры, для которых информационные ресурсы не являются особенно ценными, что характерно для 80% случаев) -склонна заказывать проектирование подсистемы безопасности в соответствии с передовыми зарубежными стандартами базового уровня.

Третья группа - *коммерческие структуры с настоящими собственниками* информационных ресурсов в случае, если информационные ресурсы представляют для них существенную ценность (как правило, финансовые структуры). В этой ситуации руководство осознанно выбирает остаточные риски, производит анализ по критерию «стоимость-эффективность» различных вариантов защиты. Как следствие, затраты на выбор подсистем безопасности являются обоснованными с точки зрения заказчика. Такие заказчики предлагают проектировщикам выполнить полный цикл работ, начиная с анализа рисков и кончая системой поддержания режима информационной безопасности на всех стадиях жизненного цикла.

Этот класс заказчиков отличается недоверием к любым посторонним подрядчикам, поэтому проблемы безопасности они стараются решать сами. Зачастую заказываются методики внутреннего аудита или анализа рисков для данной системы с апробацией на отдельном некритичном фрагменте системы и обучением местных специалистов.

Четвертую группу составляют организации, по разным причинам заинтересованные в получении формальных документов о том, что отдельные аспекты их деятельности отвечают зарубежным стандартам, в частности стандартам в области информационной безопасности. Такого рода документы обычно выдают крупные зарубежные аудиторские фирмы. При этом подготовку к сертификации проводят, как правило, отечественные организации, имеющие в этой области соответствующий опыт.

В заключение отметим, что вместе с развитием теории и практики защиты информации среди отечественных руководителей различных коммерческих структур и организаций растет понимание важности и необходимости соответствия автоматизированных систем предприятия некоторому базовому уровню безопасности (согласно зарубежным стандартам). Число «настоящих собственников», осознанно выбирающих уровень остаточных рисков, также увеличивается. Все это вместе внушает определенный оптимизм относительно становления и развития отечественной практики защиты информации и, в частности, решения задач анализа информационных рисков и управления ими, что необходимо для определения перспектив развития и управления развитием отечественных предприятий и организаций.

Глава 2
Управление рисками и международные стандарты

В последнее время в разных технологически развитых странах появилось новое поколение стандартов информационной безопасности, посвященных практическим вопросам организации режима ИБ на предприятии. Это прежде всего международные и национальные стандарты оценки информационной безопасности и управления ею - ISO 15408, ISO 17799 (BS7799), BSI; стандарты аудита, отражающие вопросы информационной безопасности, - COBIT, SAC, COSO, SAS 55/78 и некоторые другие, аналогичные им. В соответствии с этими стандартами организация режима ИБ в любой компании предполагает следующее.

Во-первых, определение целей обеспечения информационной безопасности компании.

Во-вторых, создание эффективной системы управления информационной безопасностью.

В-третьих, расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям.

В-четвертых, применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния.

В-пятых, использование методик (с понятной системой критериев и мер обеспечения информационной безопасности) в процессе анализа рисков и управления ими, позволяющих объективно оценить текущее состояние дел.

Новое поколение стандартов отличается как от предыдущих, так и от основных документов Гостехкомиссии России 1992-1998 гг. большей формализацией технологии организации режима ИБ и детальным комплексным учетом измеримых показателей информационной безопасности компании. Комплексный учет показателей предполагает и комплексный подход к организации режима ИБ, когда проверяется на соответствие определенным правилам, контролируется и поддерживается не только программно-техническая составляющая информационной безопасности КИС, но и организационно-административные меры по ее обеспечению.

Наличие системы управления информационной безопасностью (Information Security Management), и в частности анализа информационных рисков и управления ими (Risk Management), является обязательным условием организации режима ИБ на предприятии. Предприятия, начиная с рассмотренного в первой главе третьего уровня зрелости, применяют какой-либо вариант системы управления рисками. Многие зарубежные национальные институты стандартов и организации, специализирующиеся в решении комплексных проблем информационной безопасности, предложили похожие концепции управления информационными рисками. Рассмотрим концепции Британского стандарта BS 7799 (ISO 17799), Германского стандарта BSI, стандарта США NIST, а также ряда других аналогичных стандартов различных ведомств и организаций.

2.1 Международный стандарт ISO 17799

В 1993 г. министерство торговли Великобритании опубликовало пособие о практических аспектах обеспечения информационной безопасности в коммерческих организациях и компаниях. Пособие оказалось удачным, его стали использовать администраторы безопасности многих организаций. Позже доработанная версия этого пособия была принята в качестве Британского стандарта BS 7799 «Практические правила управления информационной безопасностью» (1995 г.). Стандарт начали применять на добровольной основе не только в Великобритании, но и в других

странах. В 1998 г. вышла вторая часть стандарта, относящаяся к вопросам аудита информационной безопасности. В 2000 г. был принят международный стандарт ISO 17799 [209], основанный на BS 7799. В сентябре 2002 г. главные положения ISO 17799 были пересмотрены и дополнены с учетом развития современных информационных технологий и требований к организации режима ИБ. В настоящее время это наиболее распространенный документ среди организаций и предприятий, которые пользуются подобными стандартами на добровольной основе, однако в нем отсутствует раздел, посвященный аудиту (аналог BS 7799, часть 2).

2.1.1 Обзор стандарта BS 7799

Часть 1: Практические рекомендации, 2000 г. Определяются и рассматриваются следующие аспекты организации режима ИБ:

- политика безопасности;
- организация защиты;
- классификация информационных ресурсов и управление ими;
- управление персоналом;
- физическая безопасность;
- администрирование компьютерных систем и сетей;
- управление доступом к системам;
- разработка и сопровождение систем;
- планирование бесперебойной работы организации;
- проверка системы на соответствие требованиям ИБ.

Часть 2: Спецификации, 2000 г. [208]. Посвящена тем же аспектам, но с точки зрения сертификации режима ИБ на соответствие требованиям стандарта.

Рассмотрим основные положения стандарта ISO 17799 (BS 7799). При этом будем придерживаться методологической схемы, предложенной Национальным институтом стандартов Великобритании, а именно: сначала сформулируем проблемную ситуацию стандарта, основные цели ее разрешения, а затем укажем рекомендации по управлению ИБ на предприятии.

Раздел 1. Политика ИБ

Цель. Сформулировать задачи и обеспечить поддержку мер в области информационной безопасности со стороны руководства организации.

Часть 1. Высшее руководство должно поставить четкую цель и показать свою поддержку и заинтересованность в вопросах ИБ и распространении политики безопасности среди сотрудников организации.

Необходимо, чтобы документ, в котором изложена политика ИБ, был доступен всем сотрудникам, отвечающим за обеспечение режима ИБ, и содержал рассмотрение следующих вопросов:

- определение ИБ;
- причины, по которым ИБ имеет большое значение для организации;
- цели и показатели ИБ, допускающие возможность измерения.

Часть 2. Обращается внимание на отсутствие специальных формальных требований к политике безопасности.

Раздел 2. Организация защиты

2.1. Инфраструктура ИБ

Цель. Управлять ИБ в организации.

Часть 1. Для обеспечения режима ИБ надо создать в организации соответствующую структуру управления. Должны проводиться регулярные совещания руководства, посвященные коррекции политики ИБ, распределению обязанностей по обеспечению защиты и координации действий, направленных на поддержание режима безопасности. В случае необходимости следует привлечь для консультаций специалистов в области защиты информации. Рекомендуется установить контакты с аналогичными специалистами других организаций, чтобы быть в курсе современных тенденций и стандартов, а также для рассмотрения случаев нарушения защиты. Надо всячески поощрять комплексный подход к проблемам ИБ, например совместную работу аудиторов, пользователей и администраторов, в целях более эффективного решения проблем.

Часть 2. Должно быть выполнено независимое тестирование. Возможно проведение тестирования внешней организацией либо внутренними аудиторами, не занимающимися данной системой управления ИБ.

2.2. Обеспечение безопасности при доступе сторонних пользователей и организаций

Цель. Обеспечить безопасность информационных ресурсов организации, к которым имеют доступ посторонние.

Часть 1. Следует провести анализ рисков нарушения защиты, чтобы определить требования к средствам контроля. Эти средства должны быть согласованы и определены в договоре, заключенном со сторонней организацией.

Часть 2. Анализ договорных требований и проверка их выполнения являются обязательными.

Раздел 3. Классификация ресурсов и их контроль

3.1. Ответственность за ресурсы

Цель. Обеспечить надлежащую защиту ресурсов организации.

Часть 1. Все основные информационные ресурсы должны быть учтены и иметь ответственных. Кроме того, следует назначить ответственных за реализацию соответствующих защитных мер.

Часть 2. При проведении аудита необходимо проверить список ресурсов, в котором должны быть указаны:

- тип ресурса, серийный номер;
- ответственный;
- уровень секретности;
- местонахождение;
- носители информации (для данных);
- дата ввода и контрольной проверки.

3.2. Классификация информации

Цель. Обеспечить надлежащий уровень защиты информационных ресурсов.

Часть 1. Чтобы задать приоритеты в области обеспечения ИБ, надлежит классифицировать информацию по категориям критичности. Некоторые виды информации могут потребовать дополнительной защиты или специального обращения. Категории критичности информации позволяют определить уровни ее защиты и уведомить пользователей о необходимости специального обращения с этой информацией.

Часть 2. Аудиторы должны убедиться, что система классификации по категориям критичности является четкой и полной, соответствует политике ИБ, понимается сотрудниками и периодически пересматривается.

Раздел 4. Управление персоналом

4.1. Вопросы безопасности в должностных инструкциях по доступу к ресурсам

Цель. Уменьшить риск ошибок персонала, краж, мошенничества или незаконного использования ресурсов:

Часть 1. Аспекты, связанные с безопасностью, следует учитывать еще на стадии набора персонала, включать их в должностные инструкции и договоры, а также контролировать в течение всего времени работы данного сотрудника. Руководителям необходимо убедиться в том, что в должностных инструкциях отражена вся соответствующая данной должности ответственность за безопасность. Обязательно надлежащим образом проверить принимаемых на работу лиц, особенно если они будут иметь дело с критичной информацией. Весь персонал организации и пользователи информационных ресурсов из сторонних организаций должны подписать обязательство о конфиденциальности (неразглашении).

Часть 2. Аудиторам надо проверить должностные инструкции персонала и процедуру отбора кандидатов на должности, связанные с доступом к критически важной информации.

4.2. Обучение пользователей

Цель. Убедиться в том, что пользователи осведомлены об угрозах нарушения режима ИБ и понимают значение защиты, а также имеют навыки выполнения процедур, необходимых для нормального функционирования системы безопасности организации.

Часть 1. Пользователи должны быть обучены процедурам защиты и правильному обращению с информационными ресурсами. Необходимо также официально, в письменной форме, утвердить разрешенный пользователям доступ (права и ограничения).

Часть 2. Проверка выполнения требований, изложенных в части 1, обязательна.

4.3. Реагирование на события, таящие угрозу безопасности

Цель. Минимизировать ущерб от нарушений режима ИБ и не допускать повторений инцидентов.

Часть 1. О нарушениях режима ИБ необходимо немедленно довести до сведения руководства по административным каналам. Всех сотрудников следует ознакомить с процедурой уведомления о различных типах инцидентов (нарушение безопасности, угроза безопасности или сбои). Они обязаны сообщать обо всех случаях такого рода в соответствующую службу. В организации должна быть установлена формальная процедура наложения дисциплинарных взысканий на сотрудников, которые нарушают режим безопасности.

Часть 2. Аудиторам необходимо проверить, существует ли четкое определение того, что является нарушением режима ИБ, и знает ли персонал об этом.

Раздел 5. Физическая безопасность

5.1. Зоны безопасности

Цель. Предотвратить несанкционированный доступ к СВТ и сервисам, их повреждение и вмешательство в их работу.

Часть 1. Информационные системы, поддерживающие критически важные или уязвимые сервисы организации, должны быть размещены в защищенных местах. Для уменьшения риска несанкционированного доступа или повреждения бумажной документации и носителей информации рекомендуется установить правила использования рабочего стола.

Часть 2. Аудиторам следует удостовериться, что критически важные ресурсы размещены в зонах безопасности, имеющих соответствующий пропускной режим.

5.2. Защита оборудования

Цель. Предотвратить потерю, повреждение и компрометацию ресурсов, а также перебои в работе организации.

Часть 1. Необходимо обеспечить физическую защиту оборудования, чтобы не допустить его повреждения. Следует уделить внимание проблемам размещения оборудования и его утилизации. Могут потребоваться специальные меры для защиты от несанкционированного

доступа и других угроз, а также для сохранности вспомогательного оборудования, например системы электропитания и кабельных сетей.

Часть 2. Аудиторы должны проверить состояние физической защиты оборудования, поддерживающей инфраструктуры, защиту от аварий электроснабжения, техническое обслуживание. Особое внимание уделяется обследованию оборудования, расположенного вне здания.

Раздел 6. Администрирование информационных систем

6.1. Правила эксплуатации и ответственные за их соблюдение

Цель. Обеспечить правильную и надежную работу информационных систем.

Часть 1. Необходимо определить обязанности и процедуры по администрированию и обеспечению функционирования компьютеров и сетей. Все это должно быть зафиксировано в инструкциях и процедурах реагирования на инциденты. Для уменьшения риска некорректных или несанкционированных действий следует применять принцип разделения обязанностей.

Часть 2. Аудиторам надо проверить наличие правил по эксплуатации, разработке, сопровождению, тестированию и убедиться, что все необходимые операции должным образом документированы.

6.2. Проектирование информационных систем и их приемка

Цель. Свести риск отказов информационных систем к минимуму.

Часть 1. Доступность ресурсов и требуемая производительность информационных систем обеспечивается предварительным планированием и подготовкой. Чтобы уменьшить риск перегрузки систем, необходимо оценить будущие потребности и нужную производительность. Эксплуатационные требования к новым системам следует определить, документировать и проверить до их приемки. Должны быть выработаны требования к переходу на аварийный режим для сервисов, поддерживающих несколько приложений.

Часть 2. Аудиторам надлежит проверить критерии приемки информационных систем и оценки их производительности, а также планы восстановительных работ по каждому сервису.

6.3. Защита от вредоносного программного обеспечения

Цель. Обеспечить целостность данных и программ.

Часть 1. Предотвращение и выявление случаев внедрения вредоносного программного обеспечения достигается путем принятия соответствующих мер предосторожности. В настоящее время существует целый ряд вредоносных программ («компьютерные вирусы», «сетевые черви», «троянские кони» и «логические бомбы»), которые используют уязвимость программного обеспечения по отношению к несанкционированной модификации. Администраторы информационных систем должны быть всегда готовы к проникновению вредоносного программного обеспечения в информационные системы и принимать специальные меры, позволяющие предотвращать или обнаруживать его внедрение. В частности, важно принять меры предосторожности, чтобы не допускать появления компьютерных вирусов на персональных компьютерах или выявлять их.

Часть 2. Аудиторам следует убедиться, что процедуры, препятствующие внедрению вредоносного программного обеспечения, должным образом документированы, приняты адекватные меры предосторожности, случаи заражения регистрируются.

6.4. Обслуживание систем

Цель. Обеспечить целостность и доступность информационных сервисов.

Часть 1. Поддерживать целостность и доступность сервисов позволяет выполнение некоторых служебных процедур. Должны быть сформированы стандартные процедуры резервного копирования, регистрации событий и сбоев, а также контроля условий функционирования оборудования.

Часть 2. Аудиторам необходимо убедиться, что процедуры резервного копирования соответствуют требованиям организации, операторы ведут протоколы всех производимых операций, неисправности регистрируются и принимаются меры по их устранению.

6.5. Сетевое администрирование

Цель. Обеспечить защиту информации в сетях.

Часть 1. Управление безопасностью сетей, отдельные сегменты которых находятся за пределами организации, требует особого внимания. Для защиты конфиденциальных данных, передаваемых по открытым сетям, могут понадобиться специальные меры.

Часть 2. Аудиторы должны проверить защитные меры, применяемые в организации.

6.6. Защита носителей информации

Цель. Предотвратить повреждение информационных ресурсов и перебои в работе организации.

Часть 1. Необходимо контролировать носители информации и обеспечивать их физическую защиту. Следует определить процедуры для защиты носителей информации (магнитных лент, дисков, кассет), входных/выходных данных и системной документации от повреждения, хищения и несанкционированного доступа.

Часть 2. Аудиторы должны проверить установленные процедуры контроля, режим хранения носителей информации.

6.7. Обмен данными и программным обеспечением

Цель. Предотвратить потери, модификацию и несанкционированное использование данных.

Часть 1. Обмены данными и программами между организациями необходимо осуществлять на основе формальных соглашений. Должны быть установлены процедуры и стандарты для защиты носителей информации во время их транспортировки. Необходимо уделять внимание обеспечению безопасности при использовании электронного обмена данными и сообщениями электронной почты.

Часть 2. Аудиторам надлежит проверить существующие меры защиты электронного обмена данными и меры ИБ внутреннего электронного документооборота.

Раздел 7. Управление доступом

7.1. Управление доступом к служебной информации

Цель. Обеспечить контроль доступа к информации.

Часть 1. В организации должны быть установлены правила распространения информации и разграничения доступа. Доступ к сервисам и данным в системе необходимо контролировать в соответствии с требованиями организации.

Часть 2. Аудиторам следует проверить соответствие установленных правил доступа к информации существующей производственной необходимости.

7.2 Управление доступом пользователей

Цель. Предотвратить несанкционированный доступ к информационной системе.

Часть 1. Для управления процессом предоставления прав доступа к информационным системам требуются формальные процедуры. Эти процедуры должны включать все стадии жизненного цикла управления доступом пользователей - от начальной регистрации до удаления учетных записей пользователей, для которых доступ закрывается. Особое внимание следует уделить процессу предоставления прав суперпользователя, позволяющих обойти средства системного контроля.

Часть 2. Аудиторы должны проверить формальные процедуры регистрации и соответствие фактического положения вещей установленным процедурам. Необходимо проконтролировать предоставление особых привилегий.

7.3. Обязанности пользователей

Цель. Предотвратить несанкционированный доступ пользователей.

Часть 1. Важным условием поддержания режима ИБ является помощь зарегистрированных пользователей. Пользователи должны знать свои обязанности по обеспечению контроля доступа, особенно в части использования паролей и защиты пользовательского оборудования.

Часть 2. Аудиторам надлежит проверить знание пользователями своих обязанностей и фактическое их выполнение.

7.4. Управление доступом к сети

Цель. Предотвратить несанкционированный доступ к сервисам, включенным в сеть.

Часть 1. Подключение сервисов в сеть следует контролировать, чтобы защитить другие сетевые сервисы. К числу средств контроля должны относиться:

- интерфейсы между сетевыми сервисами;
- механизмы аутентификации удаленных пользователей и оборудования;
- контроль доступа пользователей к информационным системам.

Часть 2. Аудиторы должны убедиться, что пользователи имеют доступ только к тем сервисам, которые им необходимы. Если проводится политика управления маршрутизацией, требуется выяснить, как она реализуется на практике.

7.5. Управление доступом к компьютерам

Цель. Предотвратить несанкционированный доступ к компьютерам.

Часть 1. Доступ следует предоставлять только зарегистрированным пользователям. Многопользовательские системы должны:

- идентифицировать и проверять подлинность пользователей, а также, если это потребуется, терминал и/или местонахождение пользователя;
- фиксировать удачные и неудачные попытки входа;
- предоставить систему управления паролями, которая обеспечивает выбор надежных паролей;
- в случае надобности ограничивать длительность сеансов работы пользователей.

Существуют также более мощные и дорогостоящие системы управления доступом, обращение к которым оправдано в ситуации высокого риска нарушения режима безопасности.

Часть 2. Аудиторы должны проверить как минимум применение парольной защиты: периодичность смены паролей, использование общих паролей, длину и структуру паролей. При необходимости контролируются прочие механизмы: идентификация терминалов для некоторых соединений, система сигнализации о попытках несанкционированного доступа.

7.6. Управление доступом к приложениям

Цель. Предотвратить несанкционированный доступ к информации, хранимой в информационных системах.

Часть 1. Для управления доступом к прикладным системам и данным нужны средства логического контроля доступа. Доступ к программам и данным следует предоставлять только зарегистрированным пользователям. Прикладные системы должны:

- контролировать доступ пользователей к данным и приложениям в соответствии с политикой управления доступом, принятой в организации;
- обеспечивать защиту от несанкционированного доступа утилит, которые способны обойти средства системного контроля;
- не нарушать защиту других систем, с которыми они разделяют информационные ресурсы.

Часть 2. Аудиторам следует проверить существующие ограничения на доступ.

7.7. Слежение за доступом к системам и их использованием

Цель. Выявить несанкционированные действия.

Часть 1. Чтобы выяснить, как осуществляется политика управления доступом, необходимо проводить текущий контроль системы. Это требуется для определения эффективности принятых мер и установления соответствия политики управления доступом существующей практике.

Часть 2. Аудиторам следует убедиться, что политика управления доступом отвечает существующей практике.

Раздел 8. Разработка и сопровождение информационных систем

8.1. Требования к ИБ систем

Цель. Обеспечить встраивание средств защиты в информационные системы.

Часть 1. Требования к безопасности должны быть сформулированы и согласованы до разработки информационных систем. Средства защиты оказываются более дешевыми и эффективными, если их встроить на стадиях задания требований и проектирования. Все требования к безопасности, включая необходимость перехода на аварийный режим для продолжения обработки информации, следует определить на стадии формирования требований к проекту, обосновать, согласовать и документировать в рамках общего плана работ по созданию информационной системы.

Часть 2. Аудиторы должны убедиться, что на стадии проектирования был проведен анализ вопросов безопасности.

8.2. Средства обеспечения ИБ в прикладных системах

Цель. Предотвратить потерю, модификацию и несанкционированное использование данных в прикладных системах. При проектировании прикладных систем необходимо встроить в них надлежащие средства управления безопасностью, в том числе средства протоколирования и аудита.

Часть 1. Проектирование и эксплуатация систем должны соответствовать стандартам базового уровня защищенности.

Системы, которые поддерживают исключительно уязвимые, ценные или критически важные информационные ресурсы организации или оказывают на них влияние, могут потребовать принятия дополнительных мер противодействия. Такие меры следует определить исходя из рекомендаций специалиста по безопасности с учетом идентифицированных угроз и возможных последствий их реализации.

Часть 2. Аудиторам надлежит убедиться, что обеспечивается базовый уровень защищенности при вводе данных, информация большой степени секретности шифруется, используются механизмы проверки подлинности сообщений.

8.3. Защита файлов

Цель. Обеспечить информационную безопасность при разработке и поддержке информационных систем.

Часть 1. Доступ к системным файлам необходимо контролировать. Поддержание целостности прикладных систем должно быть обязанностью пользователя или группы разработки, которой принадлежит данная прикладная система или программное обеспечение.

Часть 2. Аудиторам следует выяснить, как устанавливаются и тестируются новые версии, регистрируются изменения, хранятся рабочие версии ПО.

8.4. Безопасность в среде разработки и эксплуатационной среде

Цель. Обеспечить информационную безопасность прикладного ПО и данных.

Часть 1. Среду разработки и эксплуатационную среду необходимо жестко контролировать. Администраторы, отвечающие за прикладные системы, должны анализировать изменения, которые предлагаются для внесения в системы, чтобы убедиться, что они не нарушат безопасность среды разработки или эксплуатационной среды.

Часть 2. Аудиторам надо проверить наличие процедур контроля на всех этапах жизненного цикла.

Раздел 9. Планирование бесперебойной работы организации

9.1. Вопросы планирования бесперебойной работы организации

Цель. Составить планы предотвращения перебоев в работе организации.

Часть 1. Для защиты критически важных производственных процессов от последствий крупных аварий и катастроф требуются планы обеспечения бесперебойной работы организации. Должен существовать процесс разработки и реализации планов быстрого восстановления критически важных производственных процессов и сервисов. В процесс планирования бесперебойной работы необходимо включать меры по идентификации и уменьшению рисков, ликвидации последствий реализации угроз и быстрому восстановлению основных производственных процессов и сервисов.

Часть 2. Аудиторам следует проверить общие принципы имеющихся планов обеспечения бесперебойной работы организации и практику их реализации.

Раздел 10. Проверка системы на соответствие требованиям ИБ

10.1. Выполнение требований действующего законодательства

Цель. Избежать нарушений договорных обязательств и требований действующего законодательства при поддержании режима ИБ.

Часть 1. При разработке, сопровождении и эксплуатации информационных систем должны учитываться правовые и договорные требования к безопасности. Их необходимо сформулировать в явном виде и документировать. То же самое относится и к выбранным средствам контроля.

Часть 2. Аудиторы должны убедиться в соблюдении норм действующего законодательства, а также мер по защите важных документов и личной информации.

10.2. Проверка режима ИБ на соответствие политике безопасности

Цель. Обеспечить соответствие режима ИБ политике и стандартам безопасности организации.

Часть 1. Состояние режима ИБ требует регулярной проверки.

Следует удостовериться, что режим ИБ отвечает декларированной политике безопасности и принятым стандартами обеспечения безопасности.

Часть 2. Должны регулярно контролироваться все стороны деятельности, имеющие отношение к безопасности, и степень их соответствия политике безопасности.

10.3. Меры безопасности при тестировании

Цель. Минимизировать вмешательство в процесс тестирования и воздействие тестирования на штатную работу.

Часть 1. Необходимо иметь средства для защиты рабочих и тестируемых систем.

Часть 2. Аудиторы проверяют наличие планов тестирования и организацию доступа к инструментальным средствам тестирования.

2.1.2 Развитие стандарта BS 7799 (ISO 17799)

Британский институт стандартов BSI выпустил серию практических рекомендаций [146, 188, 189, 190, 198, 199, 200, 210], посвященных различным вопросам: оценке и управлению рисками, аудиту режима ИБ, сертификации информационной системы на соответствие стандартам

BS 7799, организации работы персонала. Эта серия существенно дополняет международный стандарт ISO 17799 [208, 209].

В сентябре 2002 г. стандарт BS 7799 был пересмотрен. В его новом варианте много внимания уделено вопросам обучения и изначальной интеграции процедур и механизмов ИБ в информационные технологии корпоративных систем, а также дальнейшему развитию технологий оценивания рисков и управления ими. По мнению специалистов, обновление этого стандарта позволит не только создать новую культуру ИБ, но и скоординировать действия различных государственных структур и представителей международного бизнеса в области защиты информации.

В табл. 2.1 дается сравнение содержания стандартов BS 7799 (разных версий) и ISO 9001.

Таблица 2.1. Сравнение содержания стандартов BS 7799 и ISO 9001

Разделы BS 7799-2, 1998 г.	Разделы BS 7799-2, 2002 г.	Разделы ISO 9001, 2000 г. в части ИБ
-	Введение	Введение
1. Границы применимости	1. Границы применимости	1. Границы применимости
	2. Нормативные ссылки	2. Нормативные ссылки
2. Термины и определения	3. Термины и определения	3. Термины и определения
	3.1. Доступность 3.2. Конфиденциальность 3.3. Информационная безопасность 3.4. Система управления режимом информационной безопасности 3.5. Целостность 3.6. Принятие рисков 3.7. Анализ рисков 3.8. Оценка рисков 3.9. Определение рисков 3.10. Управление рисками 3.11. Действия по уменьшению рисков	
2.1. Ведомость соответствия	3.12. Ведомость соответствия	
3. Системные требования в области управления информационной безопасности	4. Управление информационной безопасностью	4. Требования к системе управления качеством (QMS)
3.1. Общие требования	4.1. Общие требования	4.1. Общие требования
3.2. Создание и организация системы управления режимом информационной безопасности	4.2. Создание и организация системы управления режимом информационной безопасности 4.2.1. Создание системы управления режимом информационной безопасности	
3.3. Инструментарий	4.2.2. Средства и действия в рамках системы управления режимом информационной безопасности 4.2.3. Отслеживание событий в системе управления режимом информационной безопасности 4.2.4. Обслуживание и модернизация системы управления режимом информационной безопасности	
3.4. Документирование	4.3. Документирование требований	4.2. Документирование требований

Разделы BS 7799-2, 1998 г.	Разделы BS 7799-2, 2002 г.	Разделы ISO 9001, 2000 г. в части ИБ
	4.3.1. Общие требования	4.2.1. Общие требования
3.5. Управление документами	4.3.2. Управление документами	4.2.3. Управление документами
3.6. Записи	4.3.3. Управление записями	4.2.4. Управление записями
-	5. Распределение обязанностей персонала	5. Распределение обязанностей персонала
	5.1. Передача полномочий	5.1. Передача полномочий
	5.2. Управление ресурсами	5.2. Управление ресурсами
	6. Управление процедурой пересмотра некоторых положений	6. Управление процедурой пересмотра некоторых положений
	6.1. Общие положения	6.1. Общие положения
	6.2. Пересмотр входа	6.2. Пересмотр входа
	6.3. Пересмотр выхода	6.3. Пересмотр выхода
	6.4. Внешний аудит	6.4. Внешний аудит
	7. Модернизация системы управления режимом информационной безопасности	
	7.1. Непрерывная модернизация	
	7.2. Корректирующие действия	
	7.3. Превентивные действия	
4. Детализированное описание управления	Приложение А Цели управления и средства управления	
	A1. Введение	
	A2. Обзор передового опыта	
4.1. Политика безопасности	A3. Политика безопасности	
4.2. Организационные аспекты безопасности	A4. Организационные аспекты безопасности	
4.3. Классификация ресурсов и управляющих воздействий	A5. Классификация ресурсов и управляющих воздействий	
4.4. Безопасность персонала	A6. Безопасность персонала	
4.5. Безопасность инфраструктуры и физическая безопасность	A7. Безопасность инфраструктуры и физическая безопасность	
4.6. Безопасность инфраструктуры и физическая безопасность	A8. Управление коммуникациями и процессами	
4.7. Управление доступом	A9. Управление доступом	
4.8. Развитие системы и обслуживание	A10. Развитие системы и обслуживание	
4.9. Обеспечение бесперебойной работы	A11. Обеспечение бесперебойной работы	
4.10. Технические требования	A12. Технические требования	
	Приложение В Руководство по использованию стандарта	
	Приложение С	Приложение А
	Соответствие между ISO 9001:2000, ISO14001:1996 и BS7799 part 2:2002	Связь между ISO 14001 и ISO 9001

2.2 Германский стандарт BSI

В Германии в 1998 г. вышло «Руководство по защите информационных технологий для базового уровня защищенности» [345]. Оно представляет собой гипертекстовый справочник объемом около 4 Мб (в формате HTML). Общая структура документа приведена на рис. 2.1.

Можно выделить следующие блоки этого документа:

- методология управления ИБ (организация менеджмента в области ИБ, методология использования руководства);
- компоненты информационных технологий:
  - основные компоненты (организационный уровень ИБ, процедурный уровень, организация защиты данных, планирование действий в чрезвычайных ситуациях);
  - инфраструктура (здания, помещения, кабельные сети, организация удаленного доступа);

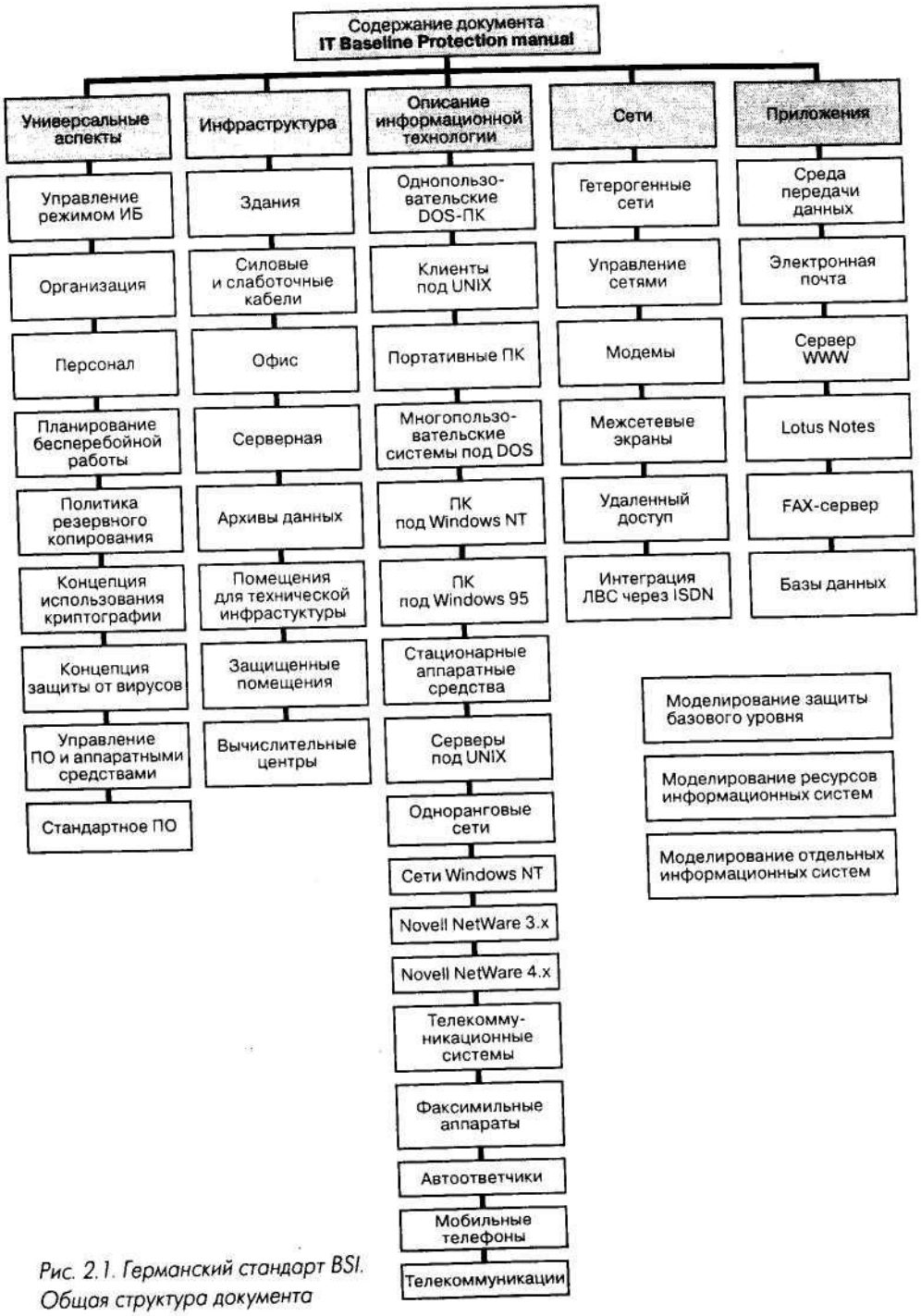


Рис. 2.1. Германский стандарт BSI. Общая структура документа

- клиентские компоненты различных типов (DOS, Windows, UNIX, мобильные компоненты, прочие типы);

- сети различных типов (соединения «точка-точка», сети Novell NetWare, сети с ОС UNIX и Windows, разнородные сети);
- элементы систем передачи данных (электронная почта, модемы, межсетевые экраны и т.д.);
- телекоммуникации (факсы, автоответчики, интегрированные системы на базе ISDN, прочие телекоммуникационные системы);
- стандартное ПО;
- базы данных;

- каталоги угроз безопасности и контрмер (около 600 наименований в каждом каталоге).

При этом все каталоги структурированы следующим образом.

Угрозы по классам:

- форс-мажорные обстоятельства;
- недостатки организационных мер;
- ошибки человека;
- технические неисправности;
- преднамеренные действия.

Контрмеры по классам:

- улучшение инфраструктуры;
- административные контрмеры;
- процедурные контрмеры;
- программно-технические контрмеры;
- уменьшение уязвимости коммуникаций;
- планирование действий в чрезвычайных ситуациях.

Все компоненты рассматриваются по такому плану: общее описание, возможные сценарии угроз безопасности (перечисляются применимые к данному компоненту угрозы из каталога угроз безопасности), возможные контрмеры (перечисляются возможные контрмеры из каталога контрмер). Фактически сделана попытка описать с точки зрения ИБ наиболее распространенные компоненты информационных технологий и максимально учесть их специфику. Предполагается оперативное пополнение и обновление стандарта по мере появления новых компонентов. Версии стандарта на немецком и английском языках имеются на сайте BSI [346].

Этот информационный ресурс, безусловно, заслуживает внимания. Каталоги угроз безопасности и контрмер, содержащие по 600 позиций, являются наиболее подробными из общедоступных. Ими можно пользоваться самостоятельно - при разработке методик анализа рисков, управления рисками и при аудите информационной безопасности. Обзор каталогов (названия позиций) приводится в приложении 4.

2.2.1 Сравнение стандартов ISO 17799 и BSI

В стандарте ISO 17799 (BS 7799) декларируются общие принципы, которые предлагается конкретизировать применительно к исследуемым информационным технологиям. Во второй части основное внимание уделено сертификации информационной системы на соответствие стандарту, то есть формальной процедуре, позволяющей убедиться, что декларируемые принципы реализованы. Объем стандарта сравнительно невелик - менее 120 страниц в обеих частях.

В германском стандарте BSI, напротив, обсуждается много «частных случаев» -различных элементов информационных технологий. Объем документа очень велик - несколько тысяч страниц; несомненно, он будет возрастать. Такой подход имеет свои достоинства и недостатки. К

числу его достоинств относится учет специфики различных элементов. В частности, гораздо лучше, по сравнению с Британским стандартом, рассмотрены особенности обеспечения ИБ в современных сетях. Другим достоинством является гипертекстовая структура документа, что позволяет оперативно вносить изменения и корректировать связи между частями стандарта. Последняя версия стандарта всегда доступна в Internet. Недостаток -невозможность объять необъятное: для всего множества элементов современных информационных технологий сохранить одинаковый уровень детализации. Неизбежно приходится вводить раздел «Прочее», в котором в общем виде описываются менее распространенные элементы.

Что касается Британского стандарта, то его недостаток заключается в высоких требованиях к квалификации специалистов, осуществляющих проверку на соответствие требованиям стандарта. Кроме того, в нем не в полной мере учитывается специфика современных распределенных систем.

Таким образом, оба подхода, имеющие свои достоинства и недостатки, продолжают эволюционировать, и только практика их внедрения позволит выявить лучший или, возможно, предложить иной подход.

2.3 Стандарт США NIST 800-30

Данный стандарт [291] подробно рассматривает вопросы управления информационными рисками. Считается, что система управления рисками организации должна минимизировать возможные негативные последствия, связанные с использованием информационных технологий, и обеспечить выполнение основных бизнес-целей предприятия.

Для этого система управления рисками интегрируется в систему управления жизненным циклом информационных технологий компании (см. табл. 2.2).

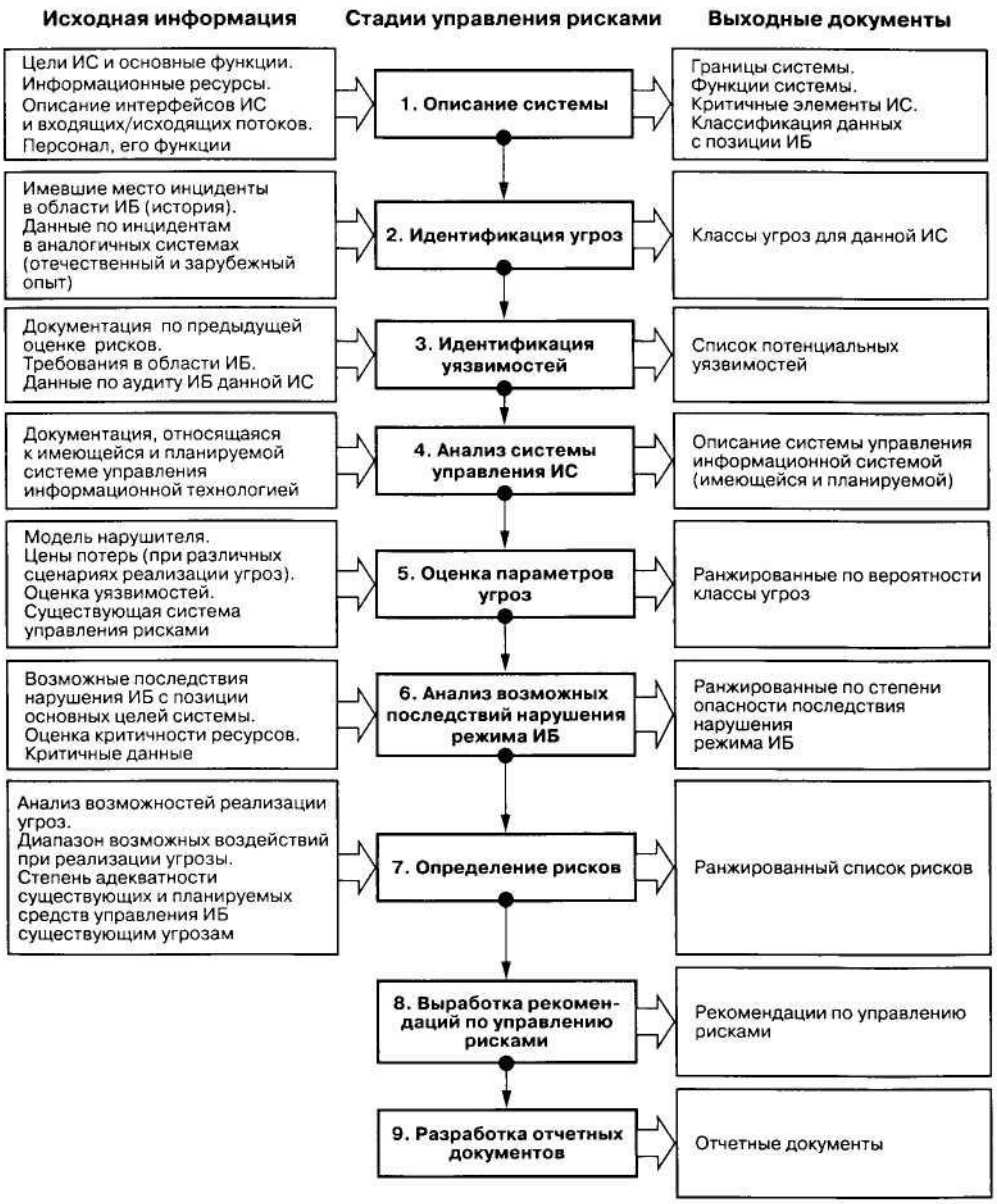


Рис. 2.2. Технология управления рисками NIST 800-30

Таблица 2.2. Управление рисками на различных стадиях жизненного цикла информационной технологии

Фаза жизненного цикла информационной технологии	**Соответствие фазе управления рисками**
1. Предпроектная стадия (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 внимание 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

Основные стадии, которые согласно стандарту NIST 800-30 должна включать технология управления рисками, показаны на рис 2.2.

Обсудим эти стадии технологии управления информационными рисками подробнее.

2.3.1 Алгоритм описания информационной системы

На данном шаге описываются цели создания информационной системы, ее границы, информационные ресурсы, требования в области ИБ и компонентов управления информационной системой и режимом ИБ.

Описание рекомендуется делать в соответствии со следующим планом:

- аппаратные средства ИС, их конфигурация;
- используемое ПО;
- интерфейсы системы, то есть внешние и внутренние связи с позиции информационной технологии;
- типы данных и информации;
- персонал, работающий в данной ИС (обязанности);
- миссия данной ИС (основные цели);
- критичные типы данных и информационные процессы;
- функциональные требования к ИС;
- категории пользователей системы и обслуживающего персонала;
- формальные требования в области ИБ, применимые к данной ИС (законодательство, ведомственные стандарты и т.д.);
- архитектура подсистемы ИБ;
- топология локальной сети;
- программно-технические средства обеспечения ИБ;
- входные и выходные потоки данных;
- система управления в данной ИС (должностные инструкции, система планирования в сфере обеспечения ИБ);
- существующая система управления в области ИБ (резервное копирование, процедуры реагирования на нештатные ситуации, инструкции по ИБ, контроль поддержания режима ИБ и т.д.);
- организация физической безопасности;
- управление и контроль внешней по отношению к ИС средой (климатическими параметрами, электропитанием, защитой от затоплений, агрессивной среды и т.д.).

Для системы, находящейся в стадии проектирования, и для уже существующей системы характер описания и степень подробности ответов будут разными. В первом случае (стадия проектирования) достаточно указать общие требования в области ИБ.

Технология описания системы

Для получения информации по перечисленным пунктам на практике рекомендуется использовать:

- разнообразные вопросники (check-листы), которые могут быть адресованы к различным группам управленческого и обслуживающего персонала;
- интервью аналитиков (внешних), которые проводят неформальные беседы с персоналом и затем готовят формализованное описание;
- анализ формальных документов и документации предприятия;

– специализированный инструментарий (ПО). Существует разнообразное ПО, благодаря которому удается частично автоматизировать процесс описания. К нему относятся разнообразные сканеры, дающие возможность составить схему информационной системы, программы для структурированного описания информационных систем, позволяющие создать необходимые отчетные формы (описываются в главе 4).

2.3.2 Идентификация угроз и уязвимостей

На данном шаге идентифицируются угрозы. Основные применяющиеся при этом понятия:

– источник угрозы - событие либо ситуация и способ, который может привести к реализации угрозы (в результате использования потенциальной уязвимости);
– угроза - потенциал (или мера) возможности реализации источника угрозы;
– уязвимость - слабость в защите.

Одним из способов идентификации угроз является построение модели нарушителя (см. табл. 2.3).

Таблица 2.3. Пример модели нарушителя

Источник угрозы	Мотивация	Результат реализации угрозы (сценарий)
Хакер	Хулиганство, самоутверждение	Неавторизованный доступ к ИС с использованием известных уязвимостей ОС (описание сценария)
Криминальные структуры	Получение финансовой информации	Проникновение в ИС с целью получить конфиденциальные данные (описание сценария)

При составлении перечня угроз и оценке их уровня обращаются к спискам классов угроз различных организаций и информации об их рейтингах либо к средним значениям вероятности реализации данной угрозы. Подобные списки составляются и поддерживаются в актуальном состоянии несколькими организациями: The Federal Computer Incident Response Center (FedCIRC), Federal Bureau of Investigation's National Infrastructure Protection Center, SecurityFocus и др.

Технологии и инструментарий для оценки уровней угроз рассматриваются в главах 3 и 4.

Идентификация уязвимостей

В результате выполнения данного шага составляется список потенциальных уязвимостей И С и возможные результаты их реализации. Одним из способов является представление в виде таблицы (см. табл. 2.4).

Таблица 2.4. Идентификация уязвимостей

Уязвимости	Источник угрозы	Результат реализации угрозы (сценарий)
МЭ допускает доступ из публичной сети к серверу А по протоколу Telnet, в том числе в гостевом режиме (ID= guest)	Неавторизованные пользователи извне	При использовании уязвимости протокола возможен доступ к файловой системе сервера А (описание сценария)
Учетные записи сотрудников, покидающих компанию, удаляются из ИС системы с запаздыванием в 1-2 дня	Внутренние нарушители, возможно в сговоре с увольняющимися сотрудниками	Незаконные финансовые операции (описание сценария)

Для существующей ИС при составлении списков прибегают к ряду источников: сетевые сканеры уязвимостей, каталоги уязвимостей разных организаций (например, база данных по уязвимостям института стандартов **США (NIST) [347]**), специализированные методы анализа рисков. При оценке уровня уязвимости принимаются во внимание существующие процедуры и методы обеспечения режима информационной безопасности, данные внутреннего аудита и результаты анализа имевших место инцидентов.

Если ИС находится в стадии проектирования, учитываются планируемые процедуры обеспечения ИБ, статистика по уязвимостям, данные производителей средств защиты информации.

2.3.3 Организация защиты информации

Формирование списка управляющих воздействий организации

Составляется список управляющих воздействий, структурированный по уровням или областям ответственности, в соответствии с принятой моделью комплексного обеспечения режима информационной безопасности (см. табл. 2.5).

Таблица 2.5. Управление ИБ

Уровень	Классы управляющих воздействий и критерии безопасности
Организационный уровень	- разграничение ответственности; - периодический пересмотр системы управления в области ИБ; - протоколирование и разбор инцидентов в области ИБ; - оценка рисков; - обучение в области ИБ; - процедура авторизации в ИС и удаления учетных записей; - поддержание в актуальном состоянии плана обеспечения ИБ
Процедурный уровень	Обеспечение правил поддержания режима ИБ, в частности: - доступ к носителям информации; - контроль за работой сотрудников в ИС; - обеспечение должного качества работы силовой сети, климатических установок; - контроль за поступающими в ИС данными
Программно-технический уровень	Комплекс мер защиты программно-технического уровня: - активный аудит и система реагирования; - идентификация и аутентификация; - криптографическая защита; - реализация ролевой модели доступа; - контроль за режимом работы сетевого оборудования

Подробно эти и некоторые другие средства управления описываются в различных руководствах, например в NIST SP 800-26.

Анализ системы управления ИС

Параметры угроз, определяемых на следующем шаге, зависят от организации системы управления ИС. На данном шаге анализируется система управления с позиции возможного воздействия на выявленные угрозы и уязвимости.

Обычно рассматриваются две категории методов управления: технического и нетехнического уровня.

Методы технического уровня, в свою очередь, подразделяются на:

- обеспечение требований базового уровня (идентификация, управление системой распределения ключей, администрирование, способы защиты элементов системы и ПО);
- упреждающие меры (аутентификация, авторизация, обеспечение безотказности, контроль доступа, сохранение конфиденциальности транзакций);
- обнаружение нарушений в области ИБ и процедуры восстановления (аудит, выявление вторжений, антивирусная защита, проверка целостности ПО и данных).

Методы нетехнического уровня - множество методов управления организационного и процедурного характера.

Выбор шкалы для оценки параметров рисков

Под оценкой параметров рисков понимается определение вероятности реализации потенциальной уязвимости, которая приведет к инциденту.

Типичной (наиболее распространенной) шкалой является качественная (балльная) шкала с несколькими градациями, например: низкий средний и высокий уровень. Оценка производится экспертом с учетом ряда объективных факторов. Уровни рисков устанавливаются, например, как в табл. 2.6.

Таблица 2.6. Пример качественной шкалы для оценки риска

Уровень риска	Определение
Высокий	Источник угрозы (нарушитель) имеет очень высокий уровень мотивации, существующие методы уменьшения уязвимости малоэффективны
Средний	Источник угрозы (нарушитель) имеет высокий уровень мотивации, однако используются эффективные методы уменьшения уязвимости
Низкий	Источник угрозы (нарушитель) имеет низкий уровень мотивации, либо существуют чрезвычайно эффективные методы уменьшения уязвимости

Анализ возможных последствий нарушения режима ИБ

Определяется цена нарушения режима ИБ. Последствия нарушения режима ИБ могут быть разноплановыми, например: прямые финансовые убытки, потеря репутации, неприятности со стороны официальных структур и т.д.

На данном шаге выбирается система критериев для оценки последствий нарушения режима ИБ и принимается интегрированная шкала для оценки тяжести последствий.

Пример шкалы приводится в табл. 2.7.

Оценка рисков

На этом шаге измеряется уровень рисков нарушения конфиденциальности, целостности и доступности информационных ресурсов. Уровень риска зависит от уровней угроз, уязвимостей и цены возможных последствий.

Таблица 2.7. Оценка тяжести последствий нарушения режима ИБ

Уровень тяжести последствий нарушения режима ИБ	Определение
Высокий	Происшествие оказывает сильное (катастрофичное) воздействие на деятельность организации, что выражается в одном или нескольких проявлениях: - большая сумма (должна быть конкретизирована) прямых финансовых потерь; - существенный ущерб здоровью персонала (гибель, инвалидность или необходимость длительного лечения сотрудника); - потеря репутации, приведшая к существенному снижению деловой активности организации; - дезорганизация деятельности на длительный (конкретизируется) период времени
Средний	Происшествие приводит к заметным негативным результатам, выражающимся в одном или нескольких проявлениях: - заметная сумма (должна быть конкретизирована) прямых финансовых потерь; - потеря репутации, которая может вызвать уменьшение потока заказов и негативную реакцию деловых партнеров; - неприятности со стороны государственных органов, в результате чего снизилась деловая активность компании
Низкий	Происшествие сопровождается небольшими негативными последствиями, выражающимися в одном или нескольких проявлениях: - небольшая сумма (должна быть конкретизирована) прямых финансовых потерь; - задержки в работе некоторых служб либо дезорганизация деятельности на непродолжительный период времени; - необходимость восстановления информационных ресурсов

Существуют различные методики измерения рисков. Чаще всего используются табличные методы, рассматриваемые в главе 3.

Если применяются качественные методы, возможные риски нарушения ИБ должны быть ранжированы по степени их опасности с учетом таких факторов, как цена возможных потерь, уровень угрозы и уязвимости.

Риски могут быть оценены с помощью количественных шкал. Это даст возможность упростить анализ по критерию «стоимость-эффективность» предлагаемых контрмер. Однако в этом случае предъявляются более высокие требования к шкалам измерения исходных данных и проверке адекватности принятой модели.

Выработка рекомендаций по управлению рисками

Рекомендации по уменьшению рисков до допустимого уровня являются необходимыми. Они должны быть комплексными и учитывать возможные меры различных уровней, например:

- внесение изменений в политику ИБ;
- изменения в регламентах обслуживания и должностных инструкциях;
- дополнительные программно-технические средства.

Разработка итоговых отчетных документов

Существуют определенные требования к содержанию отчетных документов. Обязательно наличие следующих разделов:

- цели работы;
- принятая методология;
- описание ИС с позиции ИБ;
- угрозы;
- уязвимости;
- риски;
- предлагаемые контрмеры.

2.4 Ведомственные и корпоративные стандарты управления ИБ

Рядом организаций и ведомств предложены свои спецификации для базового уровня ИБ. Ниже рассматриваются некоторые из них: спецификация сервисов базового уровня XBSS, стандарт NASA «Безопасность информационных технологий» и др.

2.4.1 XBSS-спецификации сервисов безопасности X/Open

Консорциум X/Open выпустил документ под названием «Спецификации сервисов базового уровня ИБ» [129][1)].

Спецификация применима к информационным системам, построенным на базе типовых проектных решений. Предполагается, что концепция обеспечения ИБ организации соответствует стандарту BS 7799 (ISO 17799). При разработке спецификации использовалось понятие профиля защиты с компонентами, удовлетворяющими требованиям «Good Practice», формализованным в виде четких критериев.

В спецификации определены:

- требования в области ИБ к сервисам информационной системы;

[1)] Встречающееся в тексте понятие «база данных» означает состоящую из одного или нескольких компонентов (включая СВТ и ПО) часть системы, имеющую собственные механизмы безопасности и защищенную в соответствии с политикой безопасности.

- параметры, устанавливаемые по умолчанию, соответствующие требованиям ИБ.

Требования к подсистеме идентификации и аутентификации

- администрирование для непривилегированного пользователя запрещено;
- требуется возможность разграничения доступа по группам пользователей, местоположению, времени;
- перед сменой пароля необходима аутентификация;
- выполняется отслеживание неудачных попыток входа в систему, задержка после ввода неверного пароля перед следующей попыткой, оперативное оповещение администратора безопасности при нескольких последовательных неудачных попытках входа в систему;
- обеспечивается системная защита данных, которые служат для аутентификации, и регистрационных данных пользователей;
- требования к паролям (по длине, допустимым символам и т.п.) следует проверять;
- установлено ограничение на доступ к системной базе паролей и на показ паролей на экране;
- данные, необходимые при аутентификации, защищаются, а пароли хранятся только в зашифрованном виде;
- пароли обязательно периодически сменяются, новые пароли непременно должны отличаться от старых;
- пользователи при доступе к базе данных аутентифицируются в обязательном порядке;
- производится смена стандартных паролей, вводимых при установке;
- при входе пользователя в систему выдаются сведения о времени последнего входа/выхода, сервисах, числе неудачных попыток входа с данным именем после последнего сеанса.

Требования к подсистеме протоколирования/аудита

- данные, относящиеся к протоколу (регистрационный журнал), необходимо защитить от изменения;
- система должна позволять идентифицировать и показывать текущие события;
- события, которые могут привести к нарушению целостности регистрационного журнала, следует перечислить в документации администратора безопасности;
- протоколирование доступа к базе данных является обязательным;
- события, подлежащие регистрации, устанавливаются для пользователей, групп пользователей, объектов базы данных;
- действия пользователей с полномочиями администраторов подвергаются аудиту на предмет адекватности текущей ситуации;
- средства протоколирования/аудита должны иметь возможность отслеживать события следующих классов:
  - использование механизмов идентификации и аутентификации;
  - помещение объектов в адресное пространство пользователя;
  - создание, модификация, удаление объектов;
  - действия привилегированных пользователей;
  - передача данных за пределы системы;
  - начало и окончание работы системы, сеансов, точки входа;
  - модификация прав доступа и привилегий.

Минимальные требования к протоколированию/аудиту

- следует регистрировать удачные и неудачные попытки входа в систему;
- необходимо регистрировать изменения, вносимые в процессе администрирования базы данных, и использовать системные сервисы;
- при попытке несанкционированного доступа к регистрационным журналам надо отправлять сообщение администратору безопасности, а процесс-нарушитель - блокировать;
- записи о событиях в регистрационном журнале должны содержать информацию о типе (классе) события, дате и времени начала и окончания, удачном/ неудачном завершении, пользователе.

Требования к подсистеме управления доступом

- для управления доступом служат следующие атрибуты: идентификатор пользователя и права доступа на чтение, запись, выполнение программ; профиль пользователя; подразделение;
- должны быть установлены правила доступа, основанные на атрибутах доступа, и правила доступа по умолчанию;
- доступ к устройствам ввода/вывода следует регламентировать административными и программно-техническими мерами;
- в базе данных необходимо определить атрибуты доступа для объектов и субъектов, причем для объектов атрибуты устанавливаются в процессе операций импорта/экспорта;
- правила доступа распространяются только на пользователей, прошедших авторизацию;
- наличие утвержденных списков управления доступом или правил управления доступом является обязательным;
- если права доступа для объектов и субъектов различаются, их надо проверять на согласованность;
- в базе данных должна быть обеспечена защита от чтения и модификации информации, относящейся к политике безопасности, в частности данных, касающихся идентификации и аутентификации, а также точек входа и соответствующих им параметров (системных и пользовательских);
- запрещается разглашать атрибуты, относящиеся к политике безопасности и устанавливаемые по умолчанию;
- пользователи должны иметь возможность в любой момент закрыть (приостановить) свой сеанс и возобновить его после повторной аутентификации.

Требования к подсистеме защиты повторного использования объектов

- всю информацию, касающуюся атрибутов безопасности и авторизации, не содержащуюся в объекте, следует выгружать из памяти (уничтожать) после выгрузки объекта;
- необходимо запретить доступ к данным (включая зашифрованные), относящимся к незагруженному объекту, для любых других объектов, в том числе тех, которые используют незагруженный объект.

Требования к защите критичной информации

- когда пользовательский сеанс приостановлен (блокирован), вывод также необходимо приостановить, а экран монитора погасить;
- база данных должна иметь возможность перед процедурой инициализации сеанса выдать пользователю предупреждение об ограничениях, связанных с текущей ситуацией.

Требования к средствам обеспечения целостности

- процедуры (решаемые задачи) требуется документировать, в частности описать вопросы восстановления в случае сбоев оборудования и нарушения целостности данных;
- после успешного входа в систему пользователю следует предоставить следующую информацию:
  - кто последний раз входил в систему (пользователь, процесс и т.п.);
  - дату и время последнего успешного входа/выхода в систему;
  - сервис, который был использован во время сеанса;
  - число неудачных попыток входа в систему после завершения последнего сеанса;
  - данные о пользовательском идентификаторе;
- база данных должна ограничивать возможности незарегистрированного пользователя при попытках входа в систему посредством применения задержки после неудачной попытки входа в систему или блокирования доступа к данным пользователя, не вошедшего в систему;
- для базы данных необходимо обеспечить возможность работы в нормальном режиме и режиме технического обслуживания (технологическом);
- по умолчанию для пользователей недоступны каталоги, созданные другими пользователями и программами;
- функции администратора, связанные с обеспечением информационной безопасности, недоступны прочим пользователям и процессам;
- восстановление данных всех категорий - вплоть до минимального уровня защищенности - в результате работы процедуры восстановления данных является обязательным;
- процедуру восстановления можно проводить только в режиме технического обслуживания.

Требования к средствам обеспечения доступности

Должны быть определены требования по доступности для данной информационной технологии.

Обеспечение безопасности порождения и получения информации

- обычным пользователям необходимо запретить переводить систему из нормального режима в режим технического обслуживания;
- в режиме технического обслуживания обычным пользователям не следует предоставлять доступ в систему;
- база данных должна вести отчетность по каждому пользователю отдельно.

Требования к средствам управления ИБ

- надежность средств управления безопасностью обеспечивается разделением ролей и обязанностей администраторов;
- должны присутствовать как минимум администратор безопасности, системный администратор, пользователи;
- следует особо контролировать вопросы перераспределения и добавления должностных обязанностей, связанных с ИБ;
- средства администрирования, относящиеся к ИБ, необходимо контролировать на предмет их несанкционированного использования, модификации, уничтожения;
- в системе нужны механизмы защиты при регистрации новых пользователей;
- обязательным является присутствие в базе данных механизмов защиты, обеспечивающих невозможность включать/выключать механизмы защиты; выбирать

или изменять события, подлежащие протоколированию/аудиту; изменять установленные по умолчанию события и атрибуты защиты;

- требуется установить предельное время пассивности пользователей, после которого они исключаются из числа легальных пользователей;
- системный администратор должен проводить аудит действий одного или выбранной группы пользователей; а средства проведения аудита необходимо защитить от неавторизованного использования, модификации, уничтожения;
- в базе данных:
  - при установке обязательно наличие механизма выбора и обновления параметров конфигурации;
  - любые установки администратора могут производиться только после этого;
  - нужна защита механизма регистрации параметров пользователя от несанкционированного удаления, модификации, ознакомления;
  - следует предусмотреть механизм удаления пассивных пользователей;
  - администратор должен иметь возможность отменить команду удаления пользователя из списков;
  - необходим защитный механизм, предоставляющий доступ только авторизованному персоналу к выполнению функций администратора.

2.4.2 Стандарт NASA «Безопасность информационных технологий»

Минимальные требования к базовому уровню защищенности соответствуют документу «Руководство по политике безопасности для автоматизированных информационных систем» [206] и конкретизируют его положения. Принят дифференцированный подход: вводится 4 уровня критичности технологии, для которых по 30 позициям специфицируются требования. Следует отметить, что подобный подход - определение нескольких вариантов базовых требований для различных типов технологий - безусловно оправдан и позволяет принять во внимание их специфику. Этот документ доступен в Internet и является весьма полезным при разработке спецификаций на подсистему информационной безопасности с учетом ее специфики.

2.4.3 Концепция управления рисками MITRE

Организацией MITRE [319] была предложена концепция управления рисками при построении различных систем (не только информационных). В целом эта концепция близка к рекомендациям рассмотренного выше стандарта США NIST 800-30. MITRE бесплатно распространяет простейший инструментарий на базе электронной таблицы, предназначенный для применения на этапе идентификации и оценки рисков, а также выбора возможных контрмер в соответствии с этой концепцией, - Risk Matrix [340].

В данной концепции риск не разделяется на составляющие его части (угрозы и уязвимости), что в некоторых случаях может оказаться более удобным с точки зрения владельцев информационных ресурсов. Например, в России на этапе анализа рисков весьма распространено построение модели нарушителя с прямой экспертной оценкой рисков. По этой причине простейшие методики и инструменты типа Risk Matrix наиболее востребованы на отечественном рынке услуг в области защиты информации.

Глава 3
Технологии анализа рисков

Опубликованные документы различных организаций и положения описанных выше стандартов в области защиты информации, посвященные вопросам анализа информационных рисков и управления ими, не содержат ряда важных деталей, которые надо обязательно конкретизировать при разработке применимых на практике методик. Необходимая степень конкретизации этих деталей зависит от уровня зрелости организации, специфики ее деятельности и ряда других факторов. Таким образом, невозможно предложить какую-либо единую, приемлемую для всех отечественных компаний и организаций, универсальную методику, соответствующую определенной концепции управления рисками. В каждом частном случае приходится адаптировать общую методику анализа рисков и управления ими под конкретные нужды предприятия с учетом специфики его функционирования и ведения бизнеса. Рассмотрим сначала типичные вопросы и проблемы, возникающие при разработке таких методик, возможные подходы к решению этих проблем, а затем обсудим примеры адаптации и разработки соответствующих корпоративных методик.

3.1 Вопросы анализа рисков и управления ими

3.1.1 Идентификация рисков

В любой методике необходимо идентифицировать риски, как вариант - их составляющие (угрозы и уязвимости). Естественным при этом является требование полноты списка. Сложность задачи составления списка и доказательства его полноты зависит от того, какие требования предъявляются к детализации списка. На базовом уровне безопасности (третий уровень зрелости организации) специальные требования к детализации классов, как правило, отсутствуют, так что достаточно воспользоваться каким-либо подходящим в данном случае стандартным списком классов рисков. Оценка величины рисков не рассматривается, что приемлемо для некоторых разновидностей методик базового уровня. Списки классов рисков содержатся в ряде руководств, в специализированном ПО анализа рисков. Пример -Германский стандарт BSI [346], в котором имеется каталог угроз применительно к различным элементам информационной технологии. Достоинством подобных списков является их полнота: классов, как правило, немного (десятки), они достаточно широкие и заведомо покрывают все существующее множество рисков. Недостаток - сложность оценки уровня риска и эффективности контрмер для широкого класса, поскольку подобные расчеты удобнее проводить по более узким (конкретным) классам рисов. К примеру, класс рисков «неисправность маршрутизатора» может быть разбит на множество подклассов, включающих возможные виды неисправности (уязвимости) ПО конкретного маршрутизатора и неисправности оборудования.

3.1.2 Оценивание рисков

При оценивании рисков рекомендуется рассматривать следующие аспекты:

- шкалы и критерии, по которым можно измерять риски;
- оценку вероятностей событий;
- технологии измерения рисков.

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 шкалы для измерения объемов жидкости в литрах, шкалы для измерения длины в метрах. В ряде случаев прямых шкал не существует, приходится использовать либо прямые шкалы других свойств, связанных с интересующими нас, либо определять новые шкалы. Пример - шкала для измерения субъективного свойства «ценность информационного ресурса». Эта ценность может измеряться в единицах измерения производных шкал, таких как стоимость восстановления ресурса, время восстановления ресурса и др. 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 утраты он может быть восстановлен за время, не превышающее критически допустимое, но 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. Пример субъективного критерия - оценка владельцем информационного ресурса риска выхода из строя ПК. В последнем случае обычно разрабатывается качественная шкала с несколькими градациями, например: низкий, средний, высокий уровень. В методиках анализа рисков, как правило, используются субъективные критерии, измеряемые в качественных единицах, поскольку:

- оценка должна отражать субъективную точку зрения владельца информационных ресурсов;
- следует учитывать 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 либо воспользоваться прямой экспертной оценкой, либо определить функцию, преобразующую объективные данные (вероятность) в субъективную шкалу рисков.

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

Объективные и субъективные вероятности

Термин «вероятность» имеет несколько различных значений. Наиболее часто встречаются два толкования, 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 количеству наблюдений. Это понятие применяется при анализе результатов большого числа наблюдений, имевших место в прошлом, а также полученных как следствия из моделей, описывающих некоторые процессы.

Под субъективной вероятностью имеется в виду мера уверенности некоторого человека или группы людей в том, что данное событие в действительности будет иметь место. Как мера уверенности в возможности наступления события субъективная вероятность может быть формально представлена различными способами: вероятностным распределением на множестве

событий, бинарным отношением на множестве событий, не полностью 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 позволяет определить меру уверенности на множестве событий, а увязывается с системой предпочтений лица, принимающего решения (ЛПР), и в конечном итоге с функцией полезности, отражающей его предпочтения из множества альтернатив. Тесная связь между субъективной вероятностью и полезностью используется при построении некоторых методов получения субъективной вероятности.

Получение оценок субъективной вероятности

Процесс получения субъективной вероятности обычно разделяют на три этапа: подготовительный этап, получение оценок, этап анализа полученных оценок.

Первый этап. Во время этого этапа формируется объект исследования - множество событий, а также выполняется 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 (обзор основных методов рассматривается в приложении 6) определения субъективной вероятности. На этом же этапе производится подготовка эксперта или группы экспертов, ознакомление их с методом и проверка понимания ими поставленной задачи.

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 окончательным распределением, поскольку нередко оказывается противоречивым.

Третий этап. На этом этапе исследуются результаты опроса. Если вероятности, представленные экспертами, не согласуются с аксиомами вероятности, то на это обращается внимание экспертов и ответы уточняются с целью приведения их в соответствие с выбранной системой аксиом.

Для некоторых методов получения субъективной вероятности третий этап исключается, поскольку сам метод состоит в выборе подчиняющегося аксиомам ве-роятности вероятного распределения, которое в том или ином смысле наиболее близко к оценкам экспертов. Особую важность третий этап приобретает при агрегировании оценок, предложенных группой экспертов. Более подробно технология агрегирования групповых оценок применительно к факторам риска рассмотрена в приложении 6.

3.1.3 Измерение рисков

Сегодня существует ряд подходов к измерению рисков. Обсудим наиболее распространенные из них, а именно - оценку рисков по двум и по трем факторам.

Оценка рисков по двум факторам

В простейшем случае производится 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: РИСК = $Р_{происшествия}$ × ЦЕНА ПОТЕРИ.

Если переменные являются количественными величинами, то риск - это оценка математического ожидания потерь.

Когда переменные - качественные величины, метрическая операция умножения не определена. Таким образом, в явном виде эту формулу применять не следует. Рассмотрим вариант использования качественных величин (наиболее часто встречающаяся ситуация).

Сначала должны быть определены шкалы.

Приведем пример субъективной шкалы вероятностей событий [291]:

A - событие практически никогда не происходит;

B - событие случается редко;

C - вероятность события за рассматриваемый промежуток времени - около 0,5;

D - скорее всего, событие произойдет;

E - событие почти обязательно произойдет.

Кроме того, устанавливается субъективная шкала серьезности происшествий, скажем, в соответствии с [291]:

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

Для оценки рисков устанавливается шкала из трех значений:

- низкий риск;
- средний риск;
- высокий риск.

Риск, связанный с конкретным событием, зависит от двух факторов и может быть определен так, как в табл. 3.1.

Таблица 3.1. Определение риска в зависимости от двух факторов

Шкала	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

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

Подобный подход к оценке рисков достаточно распространен.

При разработке (использовании) методик оценивания рисков надо учитывать следующие особенности:

- значения шкал должны быть четко определены (необходимо их словесное описание) и пониматься одинаково всеми участниками процедуры экспертной оценки;
- требуется обоснование выбранной таблицы. Следует 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 приложении 5.

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. В этих методиках под понятиями «угроза» и «уязвимость» понимается следующее.

Угроза - совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.

Уязвимость - слабость в системе защиты, которая делает возможным реализацию угрозы.

Другие определения понятий «угроза» и «уязвимость» даны в приложении 3. Вероятность происшествия, которая в данном подходе может быть объективной либо субъективной величиной, зависит от уровней (вероятностей) угроз и уязвимостей:

$P_{происшествия} = P_{угрозы} \times P_{уязвимости}$

Соответственно, риск рассчитывается следующим образом:

РИСК = $P_{угрозы}$ x $P_{уязвимости}$ × 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 применяются различного рода табличные методы для расчета риска в зависимости от трех факторов.

Например, показатель риска измеряется по 8-балльной шкале следующим образом:

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 построена так, как в табл. 3.2.

Таблица 3.2. Определение 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

В данной таблице уровни уязвимости Н, С, В означают, соответственно, низкий, средний и высокий. Некоторые другие варианты таблиц рассмотрены ниже, в разделе 3.2.3.

Такие 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.

Технология оценки угроз и уязвимостей

Как правило, для оценки угроз и уязвимостей применяются 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 об имевших место происшествиях, анализ и классификация их причин, выявление факторов, от которых они зависят. Эта информация позволяет оценить угрозы и уязвимости в других информационных системах.

Однако при практической реализации такого подхода возникают следующие сложности.

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

Во-вторых, данный подход оправдан 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 же система сравнительно невелика и эксплуатирует новейшие элементы технологии (для которых пока нет достоверной статистики), оценки угроз и уязвимостей могут оказаться недостоверными.

Наиболее распространен в настоящее время подход, основанный на учете различных факторов, влияющих на уровни угроз и уязвимостей. Он позволяет абстрагироваться от малосущественных технических деталей, принять во внимание не только программно-технические, но и иные аспекты.

Рассмотрим пример реализации подобного подхода, используемого в методе CRAMM 4.0 (описывается в главе 4) для одного из классов рисков.

Оценка факторов риска использования 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.

Оценка *уязвимостей* выполняется на основе следующих косвенных факторов:

– количество рабочих мест (пользователей) в системе;

– размер рабочих групп;

– осведомленность руководства о действиях сотрудников (разные аспекты);

– характер установленного 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 три года сотрудники организации пытались получить несанкционированный доступ к хранящейся в информационной системе информации с использованием прав других пользователей?

Варианты ответов

a	Ни разу	0
Ь	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 к несанкционированному доступу 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
Ь	Нет	0

5. Есть 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 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. Имеются 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 три 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	ОТ51 до 200	10
d	От 200 до 1000	14
e	Свыше 1000	20

2. Будет ли руководство осведомлено о том, что сотрудники, работающие под его 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, а также 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 и ограничения данного подхода

Несомненным достоинством данного подхода является возможность учета многих 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.

К недостаткам относится то, что косвенные факторы и их вес 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 мало формализованная и сложная, которая 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 создатели CRAMM, выпустив 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 и решении оптимизационных задач. Для этого применяется ряд методов, позволяющих установить на упорядоченном множестве оценок систему расстояний (обзор приводится в приложении 6).

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.

3.1.4 Выбор допустимого уровня риска

Выбор допустимого уровня риска связан с затратами на реализацию подсистемы информационной безопасности. Как минимум 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, системы резервного копирования, системы контроля доступа), являются обязательными, их целесообразность 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 и характера основной деятельности обоснование выбора допустимого уровня риска может проводиться разными способами.

Наиболее распространенным является анализ по критерию «стоимость-эффективность» различных вариантов защиты. Приведем примеры постановки задач:

1) стоимость подсистемы безопасности должна составлять не более 20% от стоимости информационной системы. Найти вариант контрмер, максимально снижающих уровень интегральных рисков.

2) риски по всем классам не должны превышать очень низкий уровень. Найти вариант контрмер с минимальной стоимостью.

Если ставятся оптимизационные задачи, важно правильно выбрать комплекс контрмер (перечислить возможные варианты) и оценить его эффективность.

3.1.5 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. Приведем пример классификатора контрмер CRAMM 4.

Классы контрмер CRAMM (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 Legalization
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 Legalization
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 Legalization
Incident Handling
Compliance Checks

Подобные классификаторы позволяют автоматически выбирать и предлагать конкретные варианты контрмер, возможных для рассматриваемой информационной системы. Владельцу информационных ресурсов остается отобрать из них приемлемые. Следующий шаг - оценка эффективности контрмер.

Задача оценки эффективности контрмер не проще, чем оценка рисков.

Это объясняется тем, 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 ограничиваются упрощенными, качественными оценками эффективности контрмер.

Примером является таблица (см. табл. 3.3) типичных значений эффективности контрмер, используемых в методе анализа рисков RiskWatch, который рассматривается в следующей главе.

Таблица 3.3. Ориентировочная эффективность мероприятий в области защиты информации по критерию ROI (Return of Investment - возврат вложений)

Мероприятия	Степень эффективности
Разработка и внедрение политики информационной безопасности	2
Работа с персоналом (наведение справок, контроль поведения и т.п.)	3
Совершенствование организационной структуры	4
Анализ рисков	5
Управление жизненным циклом (управление рисками)	5
Совершенствование должностных инструкций и условий контрактов	5
Меры контроля за посетителями	6
Управление имуществом компании	7
Обучение персонала и контроль соблюдения режима ИБ	9
Меры контроля за работой приложений	10

Указанные в таблице значения представляют собой ориентировочные оценки эффективности вложений в различные классы мероприятий в области защиты информации.

В ряде случаев применяются более сложные таблицы, в которых отражена зависимость эффективности от ряда факторов (аналогичные примеру оценки угроз и уязвимостей в разделе 3.1.4).

На основе подобных таблиц делаются качественные оценки эффективности контрмер.

3.2 Разработка корпоративной методики анализа рисков

3.2.1 Постановка задачи

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

Такой анализ производится исходя из непосредственных целей и задач по защите конкретного вида информации конфиденциального характера. Одна из важнейших задач в рамках такой защиты информации - обеспечение ее целостности и доступности. Часто забывают, что нарушение целостности может произойти не только вследствие преднамеренных действий, но и по ряду других причин: сбоев оборудования, ведущих к потере или искажению информации; физических воздействий, в частности в результате стихийных бедствий; ошибок в программном обеспечении (в том числе из-за недокументированных возможностей). Поэтому под термином «атака» будем понимать воздействия на информационные ресурсы не только человеческие, но и окружающей среды, в которой функционирует система обработки информации предприятия.

Анализ риска можно проводить согласно методике по сценарию, представленному на рис. 3.1.

Каждый из шести этапов анализа риска должен быть конкретизирован.

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

Понятно, что такие сведения хранятся в установленных местах и на конкретных носителях, передаются по каналам связи и обрабатываются в соответствии с принятым регламентом. При этом основным фактором в технологии обращения с информацией является архитектура КИС, от которой во многом зависит защищенность информационных ресурсов предприятия.

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

Третий этап анализа риска - построение схем каналов доступа, утечки или воздействия на информационные ресурсы основных узлов КИС. Каждый канал

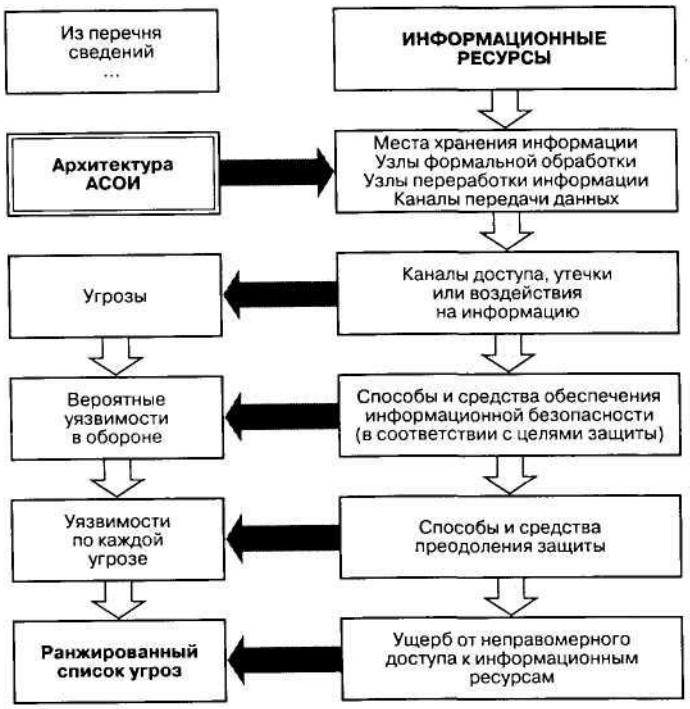


Рис. 3.1. Сценарий анализа информационных рисков компании

доступа характеризуется множеством точек, с которых можно «снять» информацию. Именно они представляют собой уязвимости и требуют применения средств недопущения нежелательных воздействий на информацию.

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

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

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

Результаты работы представляются в виде, удобном для их восприятия и выработки решений о коррекции существующей системы защиты информации. При этом важно, что каждый информационный ресурс может быть подвержен воздействию нескольких потенциальных угроз. Принципиальное же значение имеет суммарная вероятность доступа к информационным ресурсам, которая складывается из элементарных вероятностей доступа к отдельным точкам прохождения информации.

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

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

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

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

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

Наконец, в ряде случаев допустимо принятие риска. В этой ситуации важно определиться со следующей дилеммой: что для предприятия выгоднее - бороться с рисками или же с их последствиями. Здесь приходится решать оптимизационную задачу.

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

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

3.2.2 Методы оценивания информационных рисков

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

1) Идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса.
2) Оценивание возможных угроз.
3) Оценивание существующих уязвимостей.
4) Оценивание эффективности средств обеспечения информационной безопасности.

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

- показателей ценности информационных ресурсов;
- вероятности реализации угроз для ресурсов;
- эффективности существующих или планируемых средств обеспечения информационной безопасности.

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

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

- привлекательностью ресурса (учитывается при рассмотрении угрозы от умышленного воздействия со стороны человека);
- возможностью использования ресурса для получения дохода (также в случае угрозы от умышленного воздействия со стороны человека);
- техническими возможностями реализации угрозы при умышленном воздействии со стороны человека;
- степенью легкости, с которой уязвимость может быть использована.

3.2.3 Табличные методы оценки рисков

В настоящее время известно множество табличных методов оценки информационных рисков компании. Важно, чтобы компания выбрала для себя подходящий метод, который обеспечивал бы корректные и достоверные воспроизводимые результаты. Рассмотрим несколько примеров подобных методов, рекомендованных стандартами в области информационной безопасности [209, 291], и методические рекомендации к ним [189, 200, 210, 284, 285]. Важно, что в этих методах количественные показатели имеющихся или предлагаемых физических ресурсов компании оцениваются с точки зрения стоимости их замены или восстановления работоспособности ресурса. А существующие или предполагаемые программные ресурсы оцениваются так же, как и физические, то есть путем определения затрат на их приобретение или восстановление. Если обнаружится, что к какому-либо прикладному программному обеспечению предъявляются особые требования к конфиденциальности или целостности, например исходный текст ПО обладает высокой коммерческой ценностью, то оценка этого ресурса производится в стоимостном выражении по той же схеме, что и для информационных ресурсов.

Количественные показатели информационных ресурсов рекомендуется оценивать по результатам опросов сотрудников компании - владельцев информации, то есть должностных лиц компании, которые в состоянии определить ценность информации, ее характеристики и степень критичности исходя из фактического положения дел. На основе результатов опроса оцениваются показатели и степень критичности информационных ресурсов в случае несанкционированного ознакомления с конфиденциальной информацией, нарушения ее целостности или доступности.

Пример оценки рисков по двум факторам

В таблице можно наглядно отразить связь факторов негативного воздействия (показателей ресурсов) и вероятностей реализации угрозы с учетом показателей уяз-вимостей.

На первом шаге оценивается негативное воздействие по заранее определенной шкале, например от 1 до 5, для каждого ресурса, которому угрожает опасность (колонка В в табл. 3.4).

На втором шаге по заданной шкале, например от 1 до 5, оценивается вероятность реализации каждой угрозы.

На третьем шаге вычисляется показатель риска. В простейшем варианте методики это делается путем умножения (В × С). Необходимо помнить, что операция умножения определена для количественных шкал. Для ранговых (качественных) шкал измерения показатель риска, соответствующий ситуации В = 1, С = 3, совсем не обязательно эквивалентен случаю В = 3, С = 1. Соответственно, должна быть разработана методика оценивания показателей рисков применительно к конкретной организации.

На четвертом шаге угрозы ранжируются по значениям их фактора риска.

В рассматриваемом примере для наименьшего негативного воздействия и для наименьшей возможности реализации угрозы выбран показатель 1.

Таблица 3.4. Ранжирование рисков

Дескриптор угрозы	Показатель	Возможность негативного воздействия (ресурса)	Показатель риска реализации угрозы (субъективная оценка)	Ранг риска
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Данная процедура позволяет сравнивать и ранжировать угрозы с различными негативными воздействиями и вероятностями реализации. В случае необходимости дополнительно могут приниматься во внимание стоимостные показатели.

Разделение рисков на приемлемые и неприемлемые

Другой способ оценивания рисков состоит в разделении их только на приемлемые и неприемлемые риски. Подход основывается на том, что количественные показатели рисков служат лишь для того, чтобы их упорядочить и определить, какие действия необходимы в первую очередь. Но этого можно достичь и с меньшими затратами.

Матрица, используемая в данном подходе, содержит не числа, а только символы Д (риск допустим) и Н (риск недопустим). Например, матрица может иметь вид табл. 3.5.

Таблица 3.5. Разделение рисков на приемлемые и неприемлемые

Показатель ценности ресурса	Показатель возможности реализации угрозы				
	0	1	2	3	4
0	Д	Д	Д	Д	Н
1	Д	Д	Д	Н	Н
2	Д	Д	Н	Н	Н
3	Д	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

Вопрос о том, как провести границу между приемлемыми и неприемлемыми рисками, остается на усмотрение аналитика, подготавливающего данную таблицу, и руководящих специалистов в области информационной безопасности.

Пример оценки рисков по трем факторам

По каждой группе ресурсов, связанной с данной угрозой, оценивается уровень угрозы (вероятность реализации) и уровень уязвимости (степень легкости, с которой реализованная угроза способна привести к негативному воздействию). Оценивание производится в качественных шкалах.

Сначала определим уровни угроз, уязвимостей, тяжести последствий и рисков. Уровни угроз:

- низкий (Н) - реализация данной угрозы маловероятна, за последние два года подобных случаев не зафиксировано;
- средний (С) - угроза может реализоваться в течение одного года с вероятностью около 0,3;
- высокий (В) - угроза, скорее всего, реализуется в течение года и, возможно, не один раз.

Уровни уязвимостей:

- низкий (Н) - защищенность системы очень высока, реализация угроз почти никогда не приводит к происшествию;
- средний (С) - защищенность системы средняя, реализация около 30% угроз приводит к происшествию;
- высокий (В) - защищенность системы низкая, реализация угрозы практически всегда приводит к происшествию.

Показатель негативного воздействия (тяжесть последствий)

Используем введенную в главе 2 классификацию последствий:

1) Negligible (менее $100).
2) Minor (менее $1000).
3) Moderate (менее $10 000).
4) Serious (существенное негативное влияние на бизнес).
5) Critical (катастрофическое воздействие, возможно прекращение функционирования системы).

Уровни рисков

Показатель риска измеряется по шкале от 0 до 8, уровни риска определяются следующим образом:

1 - риск пренебрежимо мал. Ситуации, при которых событие наступает, практически исключены, а последствия незначительны, потери менее 100 долларов;

2 - риск незначителен. Событие наступает редко, последствия (потери) находятся в допустимых пределах (не более 1000 долларов);

…

8 - риск очень высок. Событие, скорее всего, наступит, и последствия будут катастрофическими (возможно полное прекращение деятельности организации).

Примером таблицы, с помощью которой задается значение уровня риска в зависимости от уровней угроз и уязвимостей при фиксированной стоимости потерь (Moderate), является табл. 3.6.

Таблица 3.6. Определение уровня риска в зависимости от уровней угроз и уязвимостей

Уровень угрозы								
низкий			средний			высокий		
Уровни уязвимости			Уровни уязвимости			Уровни уязвимости		
Н	С	В	Н	С	В	Н	С	В
2	3	4	3	4	5	4	5	6

Далее строится таблица для различных уровней потерь. Пример такой таблицы (табл. 3.2) был представлен ранее.

3.2.4 Методика анализа рисков Microsoft

В качестве возможного примера корпоративной методики анализа рисков рассмотрим методику компании Microsoft.

В методике риск определяется как возможность понести убытки из-за нарушения безопасности сети изнутри или извне. Управление рисками предприятия в сфере информационной безопасности требует выполнения четырех этапов:

1) Распознавание (идентификация) рисков.
2) Определение размера риска.
3) Разработка плана управления рисками.
4) Текущий контроль и управление рисками.

При ограниченном времени для идентификации рисков рекомендуется применять методики получения сведений от экспертов, в частности метод «мозгового штурма». Для каждого выявленного риска требуется оценить его стоимость (то есть определить ущерб в том случае, если рассматриваемое нежелательное событие произошло) и вероятность возникновения риска.

Оценка для каждой из угроз может производиться следующими способами:

- с использованием группы нападения - имитируется атака на систему группой специалистов;
- методом накопления идей - создается группа сотрудников и/или консультантов, которые обсуждают возможные риски и предлагают контрмеры;
- путем применения формальных оценок угроз, методов управления рисками и интеграции защитных мер.

Предлагаемая Microsoft стратегия оценки рисков включает следующие этапы:

- определение допустимого уровня рисков (то есть того уровня рисков, который приемлем);
- оценка вероятности возникновения каждого риска;
- присвоение стоимости каждому риску;
- расстановка приоритетов.

В процессе оценки для каждого риска вычисляется вероятность его возникновения и размер связанных с ним потерь. Далее используется одна из разновидностей табличной оценки рисков - строится матрица следующего вида (см. табл. 3.7).

Таблица 3.7. Табличная оценка риска в зависимости от факторов

Вероятность	Стоимость		
	высокая	средняя	низкая
Высокая	Красная	Красная	Синяя
Средняя	Желтая	Желтая	Зеленая
Низкая	Синяя	Синяя	Зеленая

В зависимости от полученных оценок риск относится к одной из следующих групп:

- высокий риск (красная область). Предполагается, что без снижения таких рисков обращение к информационной системе предприятия может оказать отрицательное влияние на бизнес;
- существенный риск (желтая область). Здесь требуется эффективная стратегия управления рисками, которая позволит уменьшить или полностью исключить отрицательные последствия нападения;
- умеренный риск (синяя область). В отношении рисков, попавших в эту область, достаточно применить основные процедуры управления рисками;

– незначительный риск (зеленая область). Усилия по управлению рисками в данном случае не будут играть важной роли.

На основании уровня допуска (уровня допустимых рисков), размера потенциальных потерь и вероятности их возникновения рискам назначаются приоритеты. Они служат для того, чтобы определить те риски, которые в первую очередь надо предотвратить (рекомендуется создать список десяти основных рисков, которым в первую очередь уделяется внимание), после чего составляется план по управлению рисками.

Планирование заключается в следующем:

– идентификации триггеров для каждого риска (*триггер,* или пусковое событие - идентификатор риска, реализованного или ожидаемого в скором времени);
– подготовке плана превентивных мероприятий, планов реагирования на непредвиденные ситуации и планов по уменьшению последствий каждого риска.

Выделяются четыре составные части планирования управления рисками:

– исследование;
– принятие (можно ли принять данный риск?);
– управление (можно ли сделать что-то, чтобы уменьшить риск?);
– исключение (что можно сделать, чтобы предотвратить риск или блокировать его?).

При этом исследование применяется по отношению к каждому риску, а остальные стадии могут комбинироваться. Предположим, исследование системы показало, что на предприятии установлено потенциально уязвимое приложение, причем полностью отказаться от работы с ним в данный момент невозможно. Допустим, далее данное приложение удалили на всех узлах, где это было допустимо, а на остальных, соответственно, оставили. Получается, что в отношении этого риска были выполнены следующие этапы: исследование, исключение (частичное), принятие (частичное).

Не менее важна и задача контроля рисков (отслеживания рисков), которая заключается в том, чтобы при изменении внешних или внутренних условий скорректировать сделанные ранее оценки рисков.

Глава 4
Инструментальные средства анализа рисков

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

В России в настоящее время чаще всего используются разнообразные «бумажные» методики, достоинствами которых являются 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 (имеется 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, описанных в первой главе.

В 2000 году принят международный стандарт ISO 17799, за основу которого взят британский стандарт BS 7799. В результате большинство инструментальных средств (ПО анализа риска) было в последнее время модифицировано так, чтобы обеспечить соответствие требованиям именно этого стандарта. Рассмотрим специализированное ПО, условно разделив его на две группы: ПО базового уровня и ПО полного анализа рисков.

4.1 Инструментарий базового уровня

Прежде всего обсудим инструментарий, соответствующий ISO 17799:

- справочные и методические материалы;
- ПО анализа рисков и аудита Cobra

Затем изучим ПО обеспечивающее дополнительные возможности по сравнению с базовым уровнем защищенности, но еще не достаточное для выполнения полного анализа рисков.

4.1.1 Справочные и методические материалы

Некоторые британские фирмы предлагают следующие продукты:

- политику информационной безопасности (Information Security Police)>
- гипертекстовые справочники по вопросам защиты информации (SOS -INTERACTIVE "ONLINE" SECURITY POLICIES AND SUPPORT);
- руководства для сотрудников служб безопасности (Security Professionals Guide).

Эти продукты представляют собой справочники, посвященные практическим аспектам реализации политики безопасности в соответствии с ISO 17799 (вид справочника приводится на рис. 4.1). Демонстрационные версии (Evaluation version) можно загрузить с сайта [341].

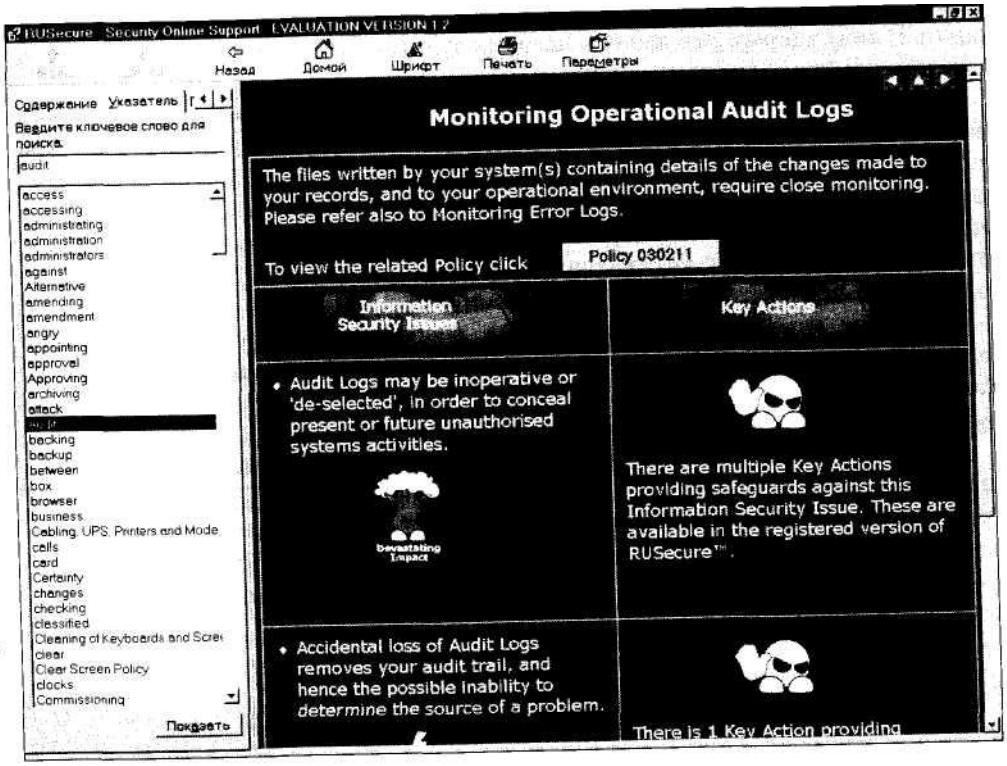


Рис. 4.1. Справочник для разработки политики безопасности

Данные методические материалы детализируют требования ISO 17799 и выполнены в стиле этого стандарта. Их достоинством является гипертекстовая структура, удобная навигация.

Еще один продукт подобного рода - руководство по применению стандарта ISO 17799 (THE ISO 17799 TOOLKIT), текст стандарта ISO 17799 с комплектом методических материалов по его применению и презентацией.

4.1.2 COBRA

Программный продукт для анализа и управления рисками COBRA [348], 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 простейший анализ рисков. Имеется несколько баз знаний: общие требования BS 7799 (ISO 17799) и специализированные базы, ориентированные на различные области применения. Доступна демонстрационная версия этого ПО.

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

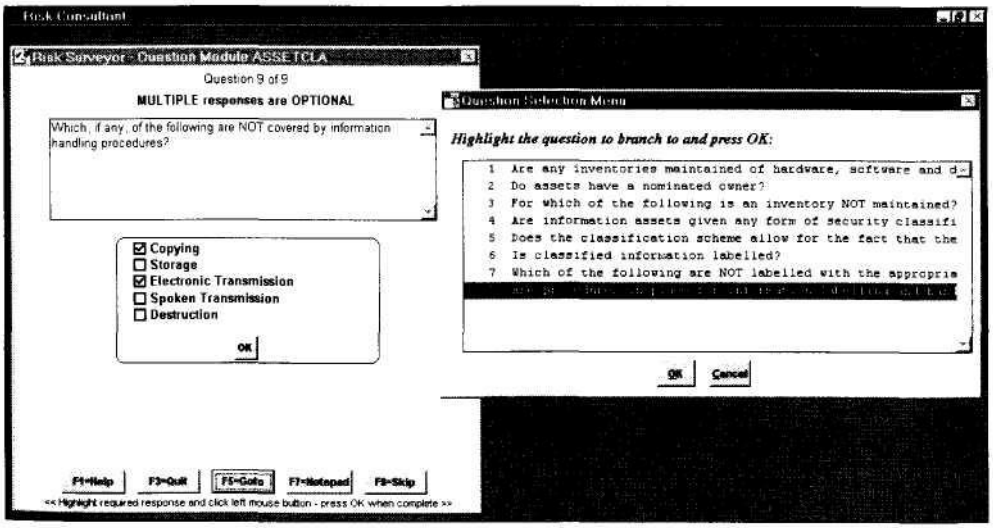


Рис. 4.2. Анализ рисков с использованием ПО Cobra

Анализ рисков, выполняемый данным методом, отвечает базовому уровню безопасности, то есть уровни рисков не определяются. Достоинство методики - в ее простоте. Необходимо ответить на несколько десятков вопросов, затем автоматически формируется отчет.

Этот программный продукт может применяться при проведении аудита ИБ или для работы специалистов служб, ответственных 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 [349] - базируется на британском стандарте BS 7799, части 1 и 2, на 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 стандарте ISO 13335, части 3 и 4 (Руководство по управлению режимом информационной безопасности, технологии управления безопасностью и выбор средств защиты). Основные модули метода перечислены на рис. 4.3.

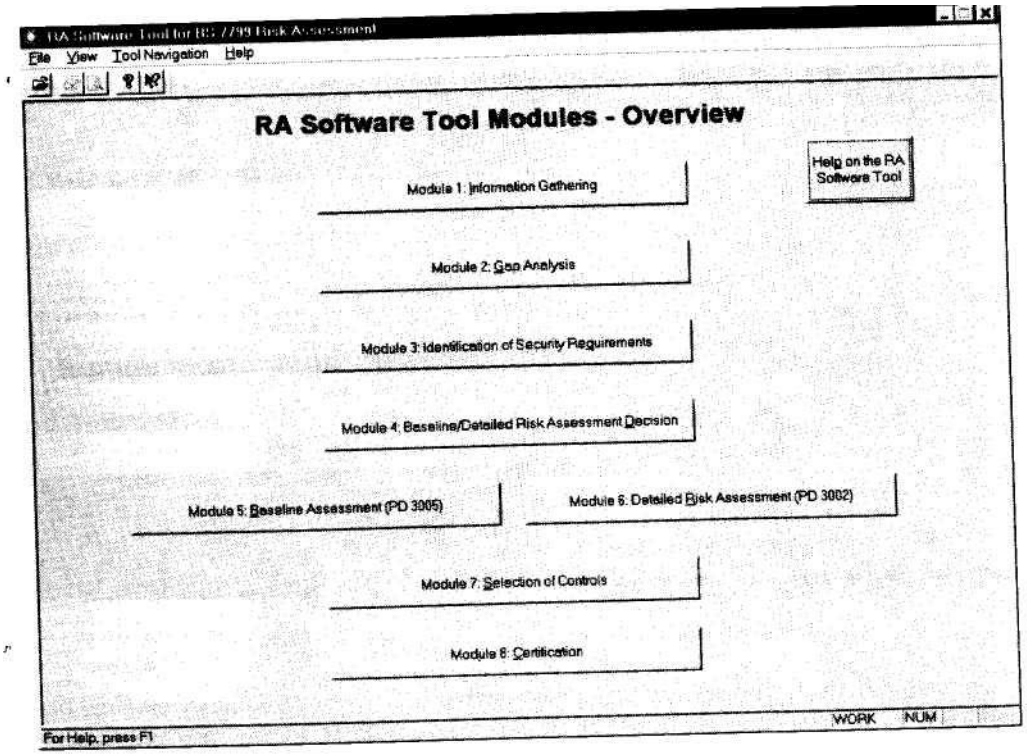


Рис. 4.3. Модули RA Software Tool

Этот инструментарий позволяет выполнять оценку рисков (модули 4 и 5) в соответствии как с требованиями базового уровня, так и с более детальными спецификациями PD 3002 Британского института стандартов.

Каждый из модулей разбивается на ряд шагов.

Демонстрационная версия данного метода, доступная на сайте [349], отличается от полной небольшими купюрами и будет полезна при разработке собственных методик и инструментария для анализа рисков и управления ими.

4.2 Средства полного анализа рисков

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. Например, упомянутый выше RA Software Tool имеет ряд простейших средств, которые дают возможность формально отнести его к средствам полного анализа рисков. Ниже рассматривается инструментарий с более развитыми средствами анализа рисков и управления ими.

Программные средства, позволяющие провести полный анализ рисков, создаются с использованием структурных методов системного анализа и проектирования (SSADM - Structured Systems Analysis and Design) и относятся к категории средств автоматизации разработки или CASE-средств (Computer Aided System Engineering).

Такие методы представляют собой инструментарий для:

- построения модели ИС с позиции ИБ;
- оценки ценности ресурсов;
- составления списка угроз и оценки их вероятностей;
- выбора контрмер и анализа их эффективности;

– анализа вариантов построения защиты;
– документирования (генерации отчетов).

Один из наиболее известных продуктов этого класса, CRAMM, рассмотрен в следующем разделе.

4.2.1 Метод CRAMM

История создания метода

В 1985 году Центральное агентство по компьютерам и телекоммуникациям (ССТА) Великобритании начало исследования существующих методов анализа ИБ, чтобы рекомендовать методы, пригодные для использования в правительственных учреждениях, занятых обработкой несекретной, но критичной информации. Ни один из рассмотренных методов не подошел. Поэтому был разработан новый метод, соответствующий требованиям ССТА Он получил название CRAMM - метод ССТА анализа и контроля рисков. Затем появилось несколько версий метода, ориентированных на требования Министерства обороны, гражданских государственных учреждений, финансовых структур, частных организаций, Одна из версий, «коммерческий профиль», представляет собой коммерческий продукт.

Целью разработки метода являлось создание формализованной процедуры, позволяющей:

– убедиться, что требования, связанные с безопасностью, полностью проанализированы и документированы;
– избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;
– оказывать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем:
– обеспечить проведение работ в сжатые сроки;
– автоматизировать процесс анализа требований безопасности;
– представить обоснование для мер противодействия;
– оценивать эффективность контрмер, сравнивать различные их варианты;
– генерировать отчеты.

CRAMM, судя по числу ссылок в Internet, - самый распространенный метод анализа рисков и управления ими.

В настоящее время продается версия CRAMM 5 [350], соответствующая стан-дарту BS 7799 (ISO 17799).

Концепция, положенная в основу метода

Анализ рисков включает идентификацию и вычисление уровней (мер) рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимостям ресурсов.

Контроль рисков состоит в идентификации и выборе контрмер, благодаря ко-х>рым удается снизить риски до приемлемого уровня.

Формальный метод, основанный на этой концепции, позволяет убедиться, что защита охватывает всю систему и существует уверенность в том, что:

– все возможные риски идентифицированы;
– уязвимости ресурсов идентифицированы и их уровни оценены;
– угрозы идентифицированы и их уровни оценены;
– контрмеры эффективны;
– расходы, связанные с ИБ, оправданы.

Исследование ИБ системы с помощью CRAMM проводится в несколько этапов (рис. 4.4).

На первой стадии (см. рис. 4.4), Initiation, производится формализованное описание границ информационной системы, ее основных функций, категорий пользователей, а также персонала, принимающего участие в обследовании.

На стадии идентификации и оценки ресурсов, Identification and Valuation of Assets, описывается и анализируется все, что касается идентификации и определения

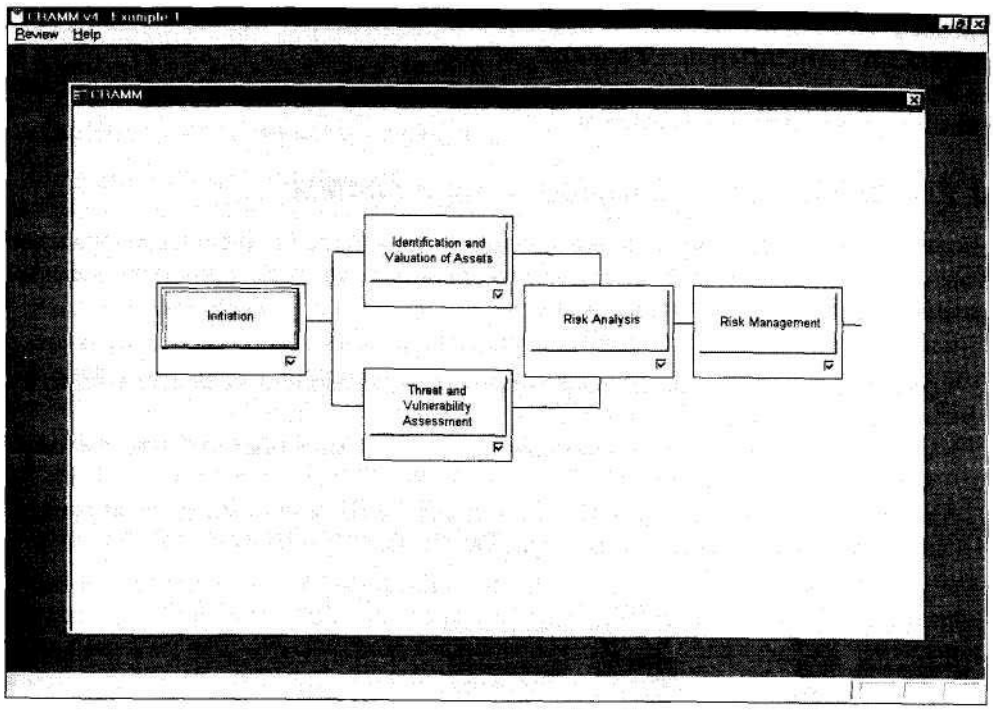


Рис. 4.4. Основные этапы метода CRAMM

ценности ресурсов системы. В конце этой стадии заказчик исследования будет знать, удовлетворит ли его существующая традиционная практика или он нуждается в проведении полного анализа рисков. В последнем случае будет построена модель информационной системы с позиции информационной безопасности.

Стадия оценивания угроз и уязвимостей, Threat and Vulnerability Assessment, не является обязательной, если заказчика удовлетворит базовый уровень информационной безопасности. Эта стадия выполняется при проведении полного анализа рисков. Принимается во внимание все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. В конце стадии заказчик получает идентифицированные и оцененные уровни угроз и уязвимостей для своей системы.

Стадия анализа рисков, Risk Analysis, позволяет оценить риски либо на основе сделанных оценок угроз и уязвимостей при проведении полного анализа рисков, либо путем использования упрощенных методик для базового уровня безопасности.

На стадии управления рисками, Risk Management, производится поиск адекватных контрмер. По существу речь идет о нахождении варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика. В конце стадии он будет знать, как модифицировать систему в терминах мер уклонения от риска, а также путем выбора специальных мер противодействия, ведущих к снижению или минимизации оставшихся рисков.

Каждая стадия объявляется законченной после детального обсуждения и согласования результатов с заказчиком.

4.2.2 Пример использования метода CRAMM

Возможности метода лучше всего продемонстрировать на небольшом примере. Рассмотрим рис. 4.5 - информационную систему поддержки принятия решений аварийно-спасательной службы.

Система состоит из следующих элементов:

- рабочие места, с которых операторы вводят информацию, поступающую по телефонам, радиоканалам и др.;
- почтовый сервер, куда информация приходит с удаленных узлов ведомственной сети и через Internet;
- сервер обработки, на котором установлена СУБД и производится автоматизированный анализ текущей ситуации;

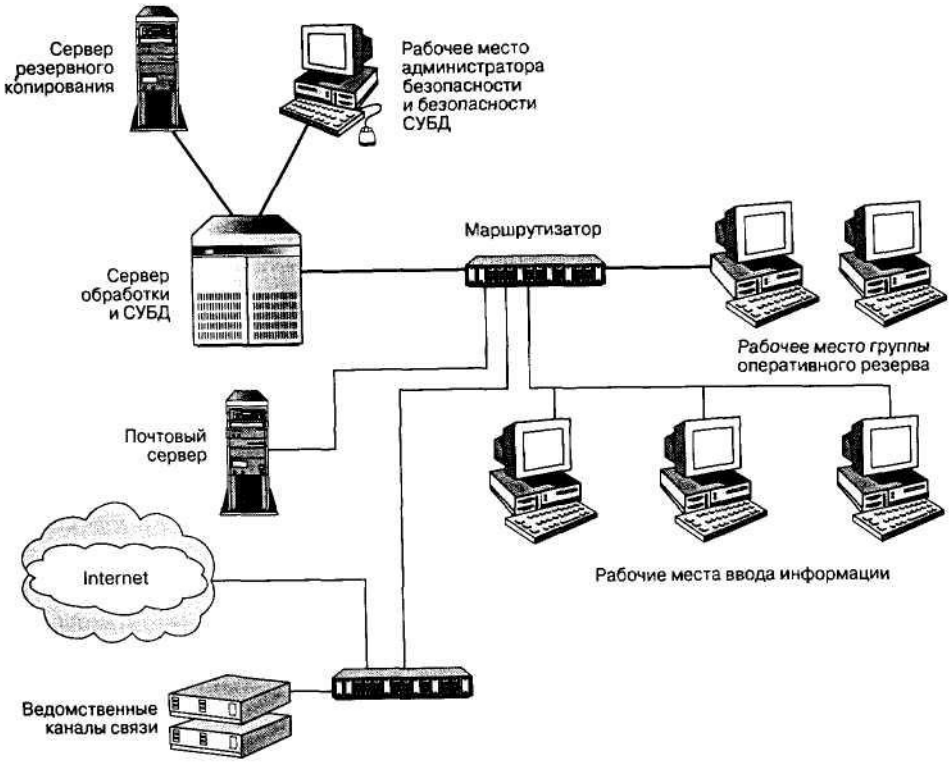


Рис. 4.5. Информационная система для поддержки принятия решений

- сервер резервного копирования;
- рабочие места группы оперативного реагирования;
- рабочее место администратора безопасности;
- рабочее место администратора БД.

Система функционирует следующим образом. Информация, введенная с рабочих мест и поступившая на почтовый сервер, направляется на сервер обработки. Затем она приходит на рабочие места группы оперативного реагирования, которая принимает решения.

Постановка задачи. Требуется провести анализ рисков системы и предложить контрмеры для обеспечения должного уровня ИБ.

Стадия идентификации и оценки ресурсов. Основные шаги: определение границ исследования (границы системы); идентификация ресурсов (оборудование, данные, программное обеспечение); построение модели с точки зрения ИБ; определение ценности ресурсов; составление отчета и обсуждение его с заказчиком.

Определение границ исследования

Стадия начинается с решения задачи определения границ исследуемой системы. Для этого собирается такая информация: ответственные за физические и программные ресурсы; кто является пользователем и как пользователи применяют или будут применять систему; конфигурация системы. Первичная информация добывается в процессе бесед с менеджерами проектов, менеджером пользователей или другими сотрудниками.

Идентификация ресурсов и построение модели системы с точки зрения ИБ

Проводится идентификация следующих ресурсов: физических (для рассмотренного примера - рис. 4.6), программных и информационных, содержащихся внутри границ системы. Каждый ресурс необходимо отнести к одному из предопределенных классов. Классификация физических ресурсов представлена в приложении 5. Затем строится модель информационной системы с позиции ИБ. Для каждого информационного процесса, имеющего самостоятельное значение с точки зрения пользователя и называемого пользовательским сервисом (End-User-Service), формируется дерево связей применяемых ресурсов. В рассматриваемом примере будет единственный подобный сервис (см. рис. 4.7). Построенная модель позволяет выделить критичные элементы.

Ценность ресурсов

Метод позволяет установить ценность ресурсов. Этот шаг является обязательным в полном варианте анализа рисков. Ценность физических ресурсов в данном методе зависит от цены их восстановления в случае разрушения. Ценность данных и программного обеспечения определяется в следующих ситуациях:

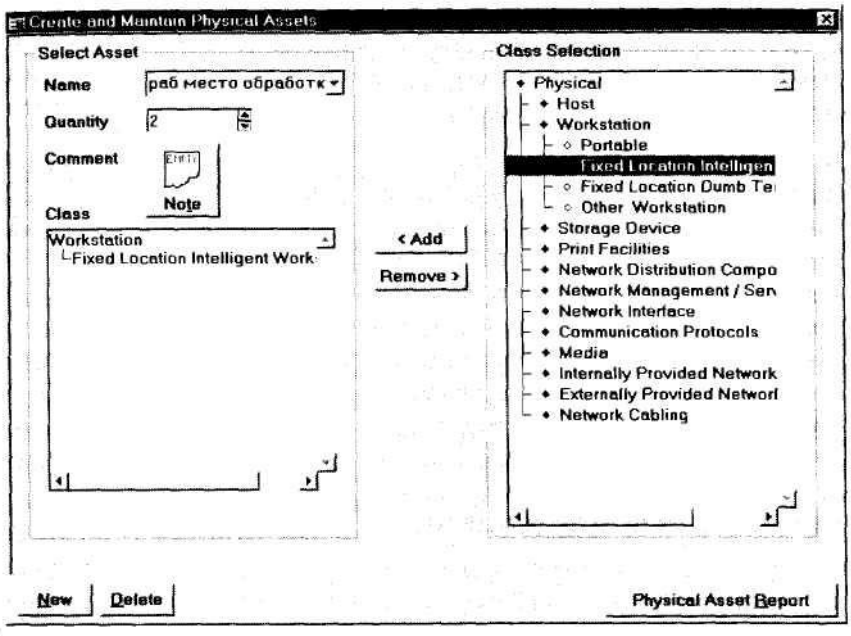


Рис. 4.6. Идентификация физических ресурсов

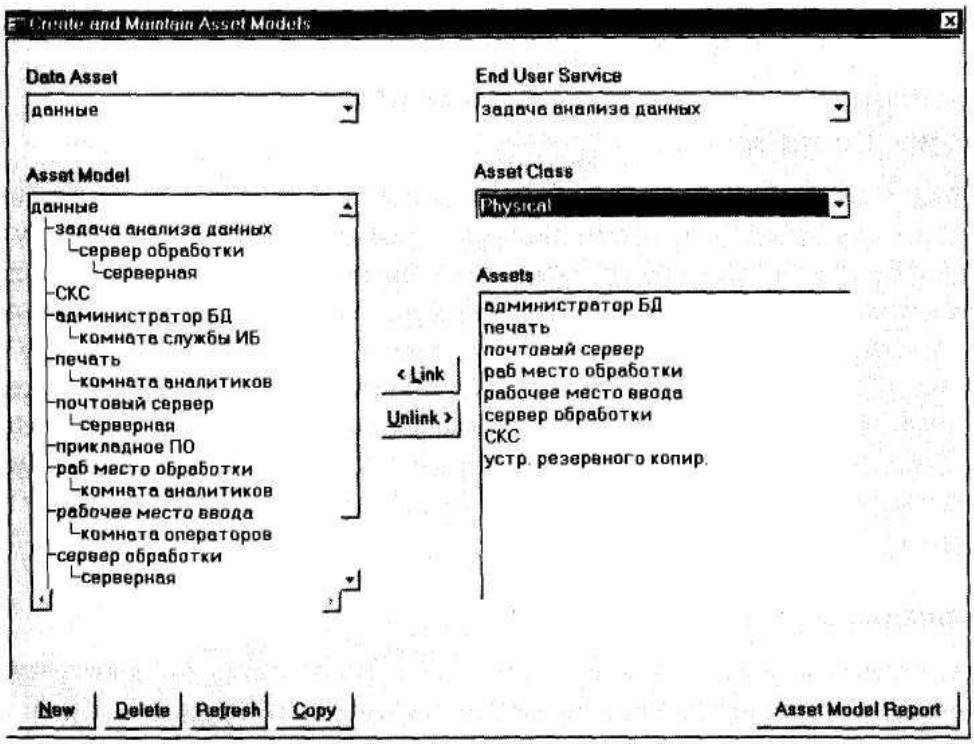


Рис. 4.7. Построение модели информационной системы с точки зрения ИВ

– недоступность ресурса в течение определенного периода времени;
– разрушение ресурса - потеря информации, полученной со времени последнего резервного копирования, или ее полное разрушение;
– нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц;
– модификация данных - рассматривается для случаев мелких ошибок персонала (ошибки ввода), программных ошибок, преднамеренных ошибок;
– наличие ошибок, связанных с передачей информации; отказ от доставки, недоставка информации, доставка по неверному адресу.

Для оценки возможного ущерба рекомендуется воспользоваться некоторыми из перечисленных критериев;

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

Приведенная совокупность критериев характерна для коммерческого варианта метода (профиль Standard). В других версиях совокупность будет иной. Так, в версии, применяемой в правительственных учреждениях, добавляются параметры, отражающие такие области, как национальная безопасность и международные отношения.

Для данных и программного обеспечения выбираются применимые к исследуемой ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10.

К примеру, если данные содержат подробности коммерческой конфиденциальной (критичной) информации, эксперт, проводящий исследование, задает вопрос: «К каким последствиям для организации может привести несанкционированный доступ посторонних лиц к этой информации?». Возможен такой ответ: «К провалу сразу по нескольким параметрам из перечисленных выше, причем каждый параметр следовало бы рассмотреть подробнее и присвоить ему самую высокую из возможных оценок».

Далее следует выбор существенных параметров и разработка шкал. В обсуждаемом примере анализ, проведенный экспертом совместно с руководством организации, показал, что для данной информационной технологии будут приниматься во внимание такие параметры:

– ущерб для здоровья персонала;
– ущерб репутации организации;
– финансовые потери, связанные с восстановлением ресурсов;
– дезорганизация деятельности в связи с недоступностью данных.

Затем разрабатываются шкалы для выбранной системы параметров. Они могут выглядеть следующим образом.

Ущерб репутации организации:

– 2 - негативная реакция отдельных чиновников, общественных деятелей;
– 4 - критика в средствах массовой информации, не получившая широкого общественного резонанса;
– 6 - негативная реакция отдельных депутатов Государственной Думы, Совета Федерации;
– 8 - критика в средствах массовой информации, имеющая последствия в виде крупных скандалов, парламентских слушаний, широкомасштабных проверок и т.п.;
– 10 - негативная реакция на уровне президента и правительства.

Ущерб для здоровья персонала:

– 2 - минимальный ущерб (последствия не связаны с госпитализаций или длительным лечением);
– 4 - ущерб среднего размера (необходимо лечение для одного или нескольких сотрудников, но длительных отрицательных последствий нет);
– 6 - серьезные последствия (продолжительная госпитализация, инвалидность одного или нескольких сотрудников);
– 10 - гибель людей.

Финансовые потери, связанные с восстановлением ресурсов:

– 2 - менее 1000 долл.;
– 6 - от 1000 до 10 000 долл.;
– 8 - от 10 000 до 100 000 долл.;
– 10 - свыше 100 000 долл.

Дезорганизация деятельности в связи с недоступностью данных - отсутствие доступа к информации;

– 2 - до 15 минут;
– 4 - до 1 часа;
– 6 - до 3 часов;
– 8 - от 12 часов;
– 10 - более суток.

Далее рассматриваются основные сценарии, приводящие к различным негативным последствиям, описываемым в терминах выбранных параметров (см. рис. 4.8).

На данной стадии может быть подготовлено несколько типов отчетов (границы системы, модель, определение ценности ресурсов).

Если ценности ресурсов низкие, допускается ограничиться базовым вариантом защиты. В таком случае исследователь может перейти от этой стадии сразу к анализу рисков. Однако для адекватного учета потенциального воздействия какой-либо угрозы, уязвимости или комбинации угроз и уязвимостеи, которые имеют

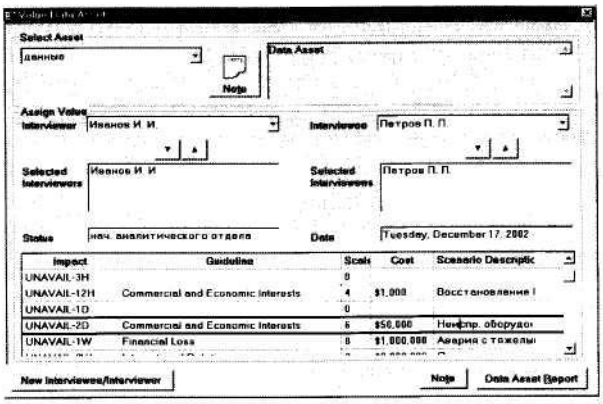


Рис. 4.8. Определение ценности информационных ресурсов

высокие уровни, следует обратиться к сокращенной версии стадии оценки угроз и уязвимостей. Это позволит разработать более эффективную схему защиты. На стадии оценивания угроз и уязвимостей:

– оценивается зависимость пользовательских сервисов от определенных групп ресурсов;
– оценивается существующий уровень угроз и уязвимостей;
– анализируются результаты.

Зависимость системы от групп ресурсов

Ресурсы группируются в соответствии с угрозами и уязвимостями. Например, в случае существования угрозы пожара или кражи в качестве группы ресурсов разумно объединить все ресурсы, находящиеся в одном месте (серверный зал, комната средств связи и т.д.).

Оценка уровней угроз и уязвимостей

Для уровней угроз и уязвимостей возможна оценка, выполненная по результатам исследования косвенных факторов, либо прямая оценка экспертов (упрощенным способом). В первом случае программное обеспечение CRAMM для каждой группы ресурсов и каждого отдельного ресурса генерирует список вопросов, допускающих однозначный ответ (см. рис. 4.9). Методика оценки рисков и уязвимостей на основе косвенных факторов для данного метода рассматривалась в главе 3. Уровень угроз оценивается, в зависимости от ответов, как (см. рис. 4.10):

– очень высокий;
– высокий;
– средний;
– низкий;
– очень низкий.

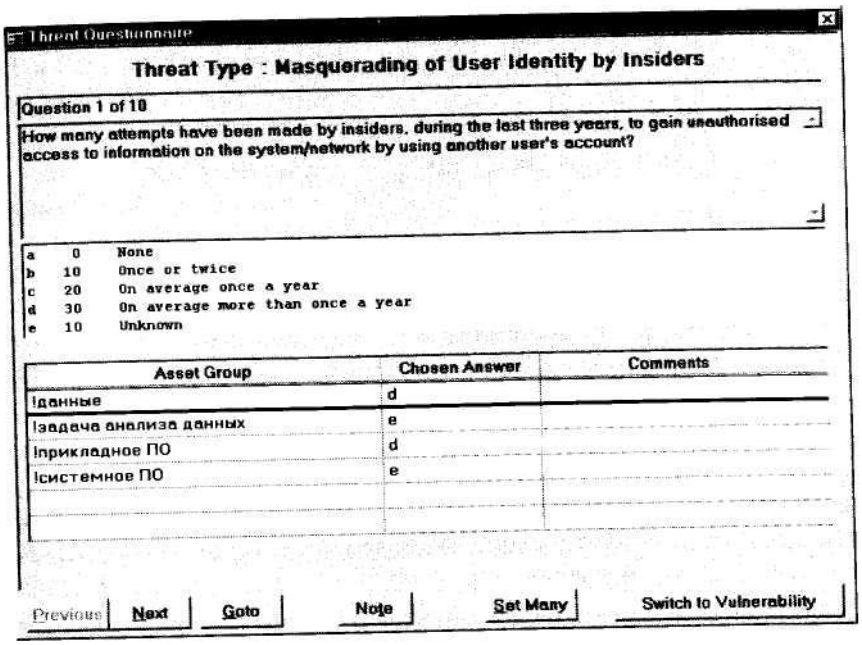


Рис. 4.9. Оценка уровня угрозы безопасности по косвенным факторам

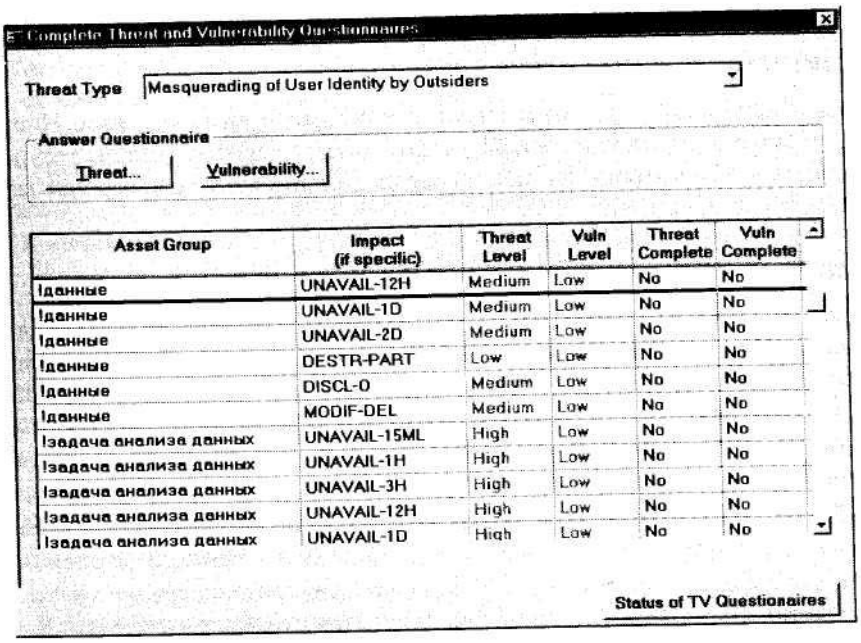


Рис. 4.10. Оценка угроз безопасности и уязвимости ресурсов

Уровень уязвимости оценивается, в зависимости от ответов, как:

– высокий;
– средний;
– низкий;
– отсутствует.

Возможно проведение коррекции результатов или использование других методов оценки.

На основе этой информации рассчитываются уровни рисков в дискретной шкале с градациями от 1 до 7 (этап анализа рисков) - фрагмент результирующего отчета см. на рис. 4.11.

CRAMM V4 Measure of Risk Summary Review: tstnew 0			
Max. Threat	Max. Vuln	Threat Overide	Vuln Overide	Max MoR
Masquerading of User Identity by Insiders			
Задача анализа данных	*Very High*	*Medium*	5
Прикладное ПО	*Very High*	*High*	6
Системное ПО	*Medium*	*Medium*	4
Данные	*Very High*	*Medium*	5

Рис. 4.11. Оценка рисков на основе уровней угроз и уязвимостей

Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком. Только после этого можно переходить к заключительной стадии метода.

Управление рисками

Основные шаги стадии управления рисками приведены на рис. 4.12.

На этой стадии CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Контрмеры разбиты на группы (см. приложение 5). Условно их можно разделить на пять категорий:

1) рекомендации общего плана, относящиеся к технологии в целом;
2) обеспечение безопасности на сетевом уровне;
3) обеспечение физической безопасности;
4) обеспечение безопасности поддерживающей инфраструктуры;
5) меры безопасности на уровне системного администратора.

В результате выполнения данной стадии формируются несколько видов отчетов.

Рассмотренная методология анализа рисков и управления ими полностью применима и в российских условиях, хотя показатели защищенности от НСД и требования по защите информации различаются в российских РД и зарубежных стандартах.

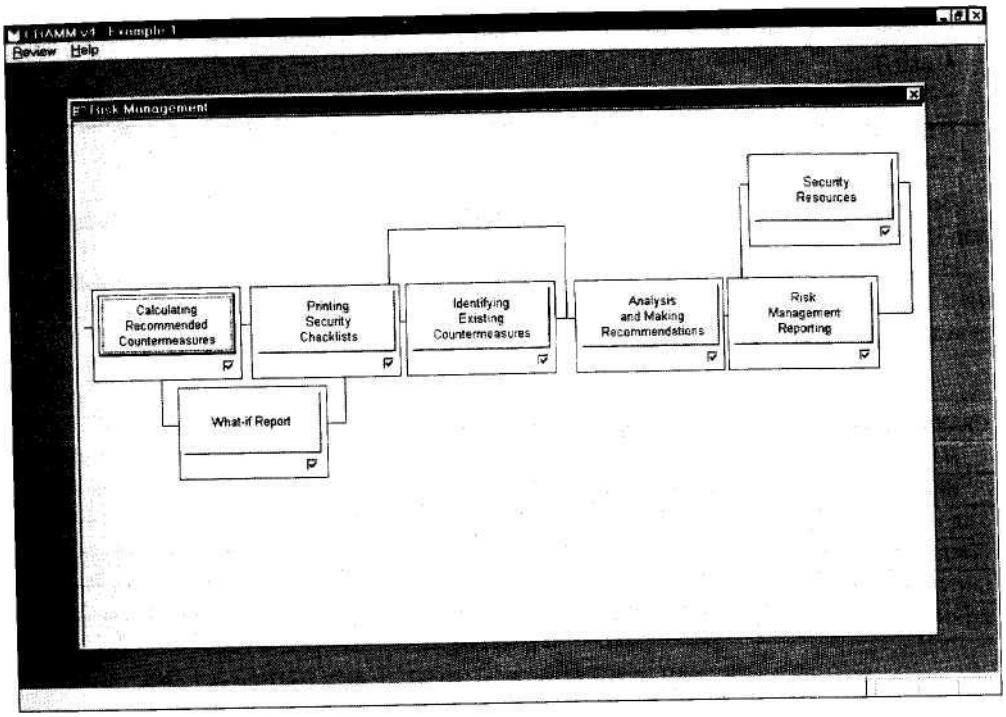


Рис. 4.12. Управление рисками в CRAMM 4

Особенно полезным представляется обращение к инструментальным средствам типа метода CRAMM при проведении анализа рисков информационных систем с повышенными требованиями в области ИБ. Это позволяет получать обоснованные оценки существующих и допустимых уровней угроз, уязвимостей, а также эффективности защиты.

CRAMM как инструментарий аудитора

CRAMM имеет средства генерации отчетов, необходимые при проведении аудита информационной безопасности в соответствии с BS 7799 (ISO 17799). Это следующие отчеты:

- политика информационной безопасности;
- система управления информационной безопасностью;
- план обеспечения бесперебойной работы;
- ведомость соответствия.

Метод CRAMM в настоящее время применяется наиболее часто, если требуется провести аудит в соответствии с требованиями Британского стандарта.

Его достоинства заключаются в использовании технологии оценки угроз и уязвимостей по косвенным факторам с возможностью верификации результатов, удобной системе моделирования информационной системы с позиции безопасности, обширной базе данных по контрмерам. Этот метод - самый «мощный» и самый трудоемкий из рассмотренных в настоящем обзоре, он позволяет весьма детально оценить риски и различные варианты контрмер.

Его недостаток с позиции отечественного потребителя состоит в сложности русификации и большом объеме выходных документов (сотни страниц). Аналитик (аудитор) обычно вынужден на основе полученных документов сам писать отчет для заказчика.

4.2.3 Средства компании MethodWare

Компания MethodWare [342] выпускает ряд продуктов, которые могут быть полезными для аналитиков в области информационной безопасности при проведении анализа рисков, управлении рисками, аудите информационной безопасности. Речь идет о:

- ПО анализа и управления рисками Operational Risk Builder и Risk Advisor. Методология отвечает австралийскому стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999). Имеется версия, соответствующая ISO 17799;
- ПО управления жизненным циклом информационной технологии в соответствии с открытым стандартом в области информационных технологий 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.

Демонстрационную версию этого ПО можно загрузить с сайта компании Methodware [342].

Рассмотрим ПО Risk Advisor. Оно 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;
- описание рисков;
- описание угроз;
- оценка потерь;
- анализ управляющих воздействий;

– предложение контрмер и плана действий.

Описание контекста

На этом этапе рассматривается несколько аспектов модели взаимодействия организации с внешним миром: стратегический, организационный, бизнес-цели, управление рисками, а также критерии оценивания рисков.

В стратегическом аспекте анализируются сильные и слабые стороны организации с внешних позиций, варианты развития, классы угроз и отношения с партнерами.

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

Контекст управления рисками представляет собой концепцию информационной безопасности.

Контекст бизнес-целей - основные бизнес-цели.

Критерии оценивания рисков - имеются в виду критерии, принятые при управлении рисками.

Описание рисков

Задается матрица рисков (рис. 4.13), поэтому риски описываются в соответствии с определенным шаблоном и устанавливаются связи этих рисков с другими элементами модели.

Риски оцениваются по качественной шкале и разделяются на приемлемые и неприемлемые (рис. 4.14) на основе простейшей модели.

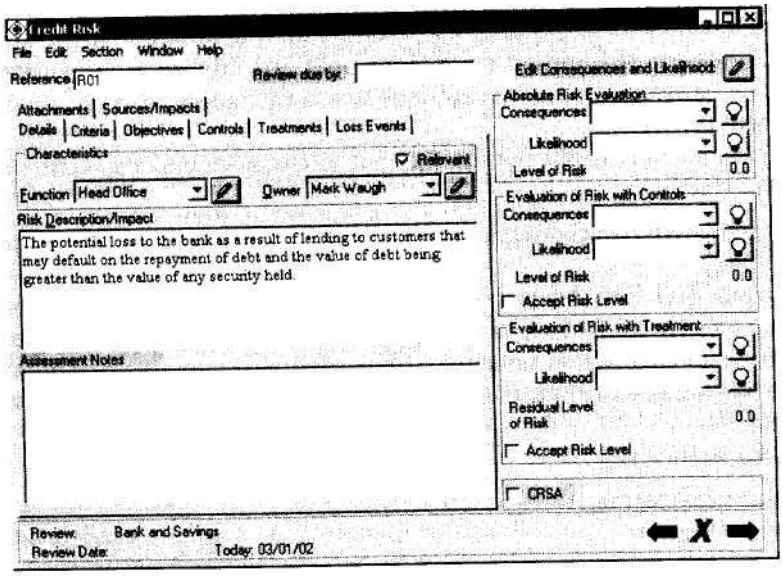


Рис. 4.13. Идентификация и определение рисков в Risk Advisor

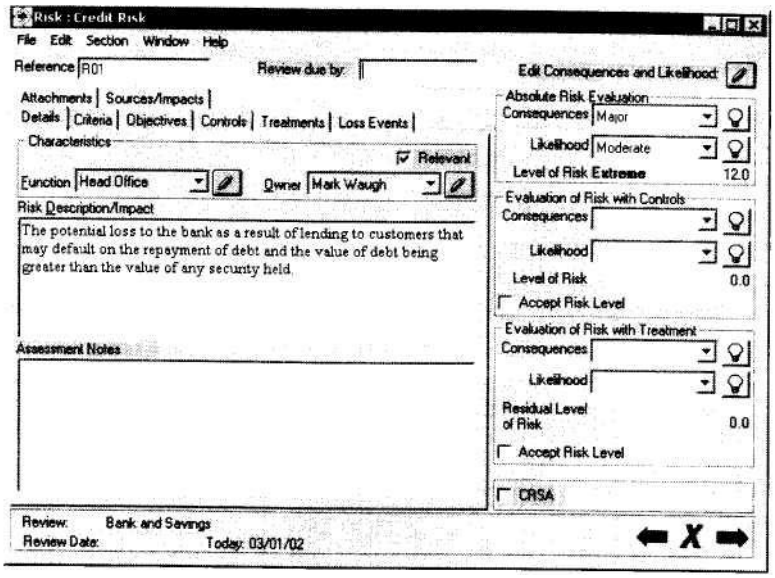


Рис. 4.14. Разделение рисков на приемлемые и неприемлемые в Risk Advisor

Затем выбираются управляющие воздействия (контрмеры) с учетом зафиксированной ранее системы критериев, эффективности контрмер и их стоимости. Стоимость и эффективность также оцениваются в качественных шкалах.

Описание угроз

Прежде всего формируется список угроз. Угрозы определенным образом классифицируются, затем рассматривается связь между рисками и угрозами. Описание также делается на качественном уровне и позволяет зафиксировать эти взаимосвязи.

Описание потерь

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

Анализ результатов

В результате построения модели можно сформировать подробный отчет (около 100 разделов), посмотреть на экране агрегированные описания в виде графика рисков (рис. 4.15).

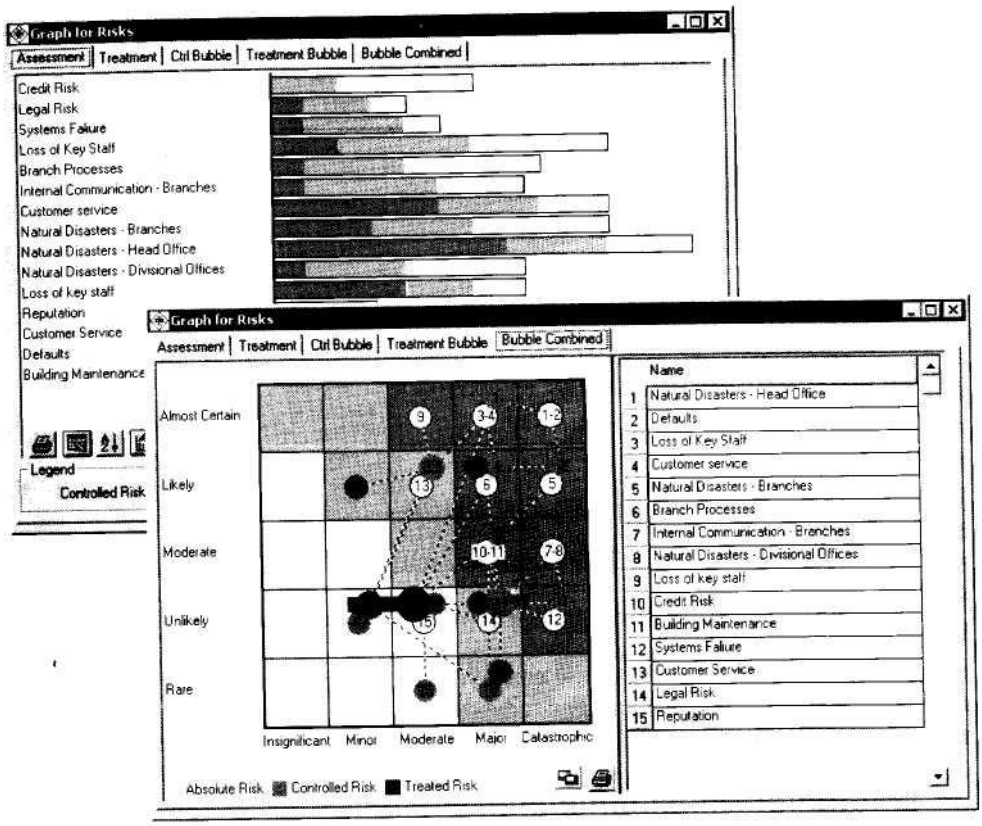


Рис. 4.15. Анализ результатов в Risk Advisor

Оценка возможностей метода Risk Advisor

Данный инструмент позволяет документировать всевозможные аспекты, связанные с управлением риском, на верхних уровнях - административном и организационном. А программно-технические аспекты фиксировать в этой модели не очень удобно. Оценки даются в качественных шкалах, подробного анализа факторов рисков не предусмотрено.

Сильной стороной данного метода является возможность представления разноплановых взаимосвязей, адекватного учета многих факторов риска и существенно меньшая трудоемкость по сравнению с CRAMM.

4.2.4 Экспертная система «АванГард»

В настоящее время на российском рынке продается отечественное ПО «АванГард», разработка Института системного анализа РАН, подробное описание которого можно найти в [46].

«АванГард» позиционируется как экспертная система управления информационной безопасностью. Структура и функции комплекса приведены на рис. 4.16.

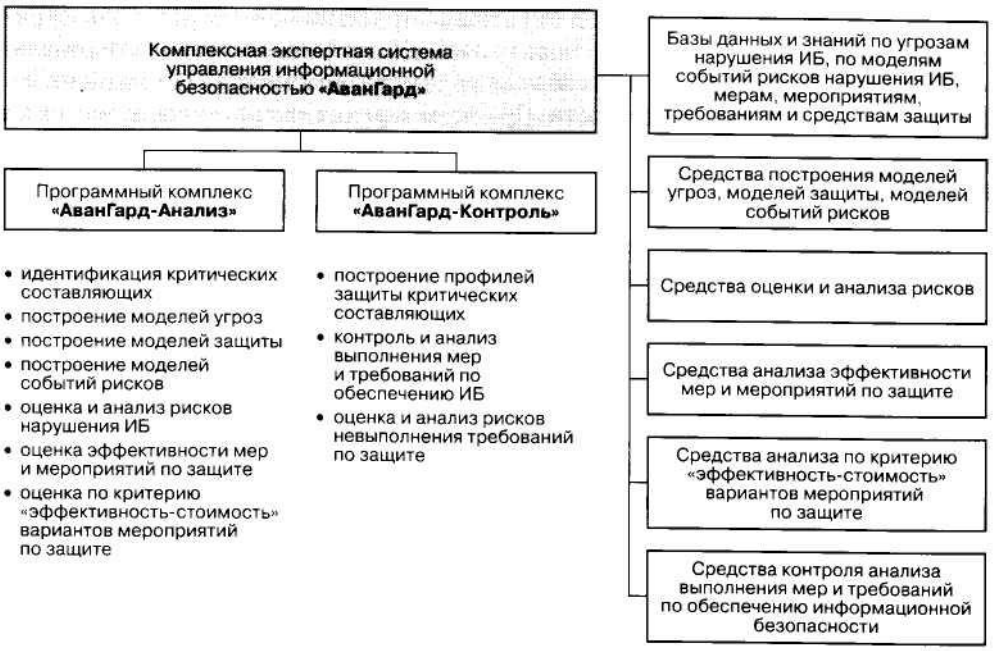


Рис. 4.16. Структура и функции ПО «АванГард»

Типовой пакет программных средств КЭС «АванГард» включает два программных комплекса - «АванГард-Анализ» и «АванГард-Контроль». Каждый из этих комплексов базируется на своей методике оценки рисков.

В первом предполагается оценка рисков на основе расчета рискообразующих потенциалов компонентов оцениваемой системы. При этом под рискообразующим потенциалом понимается та часть совокупного риска, связанного с системой, которая может быть отнесена на счет этого компонента. Расчет рискообразующих потенциалов выполняется следующим образом.

Сначала строятся модели событий рисков, содержащие по возможности подробное неформальное описание этих событий и перечень угроз, которые могут привести к ним. Далее по каждой модели события риска рассчитывается оценка риска -как произведение оценки вероятности события риска и оценки степени опасности события риска. При этом оценки, как вероятностей событий риска, так и степени опасности этих событий, предлагается получать с помощью ранговых шкал. Шкала вероятности имеет фиксированный размер от 0 до 100 (от нулевой до 100-процентной вероятности возникновения события риска в течение года). Нижняя граница шкалы опасности - 0, верхняя граница отсутствует, поэтому шкала строится по следующему принципу. Сначала на нее наносятся те риски, вся опасность которых сводится к материальному ущербу и может быть выражена в денежных единицах. В результате получается базовая шкала опасности событий рисков. Далее пользователям предлагается абстрагироваться от «денежной» метрики и воспринимать шкалу как выражающую лишь относительную степень опасности отдельных событий и указывать на ней события рисков путем сравнения степени их нежелательности или недопустимости. При этом верхняя граница шкалы может по мере надобности подниматься. Предусмотрен мощный механизм верификации даваемых оценок путем попарного сравнения вероятностей и степеней опасности каждого вновь указываемого события риска с теми, которые уже определены. Если для какой-либо пары соотношение в оценках не соответствует взглядам экспертов, то ранее выставленные оценки должны быть пересмотрены. Кроме того, предусматривается возможность распечатки выставленных оценок и их обсуждения и корректировки множеством экспертов (метод Дельфийских групп).

Методика предполагает, что любое событие риска происходит в результате реализации некоторого множества угроз, причем каждая из них может быть определена как угроза безопасности какого-либо компонента оцениваемой системы. Таким образом удается определить

рискообразующий потенциал каждой из угроз в зависимости от ее «вклада» в события риска, а также рискообразующие потенциалы тех компонентов, к которым эти угрозы относятся, и рассчитать риски по всём структурным составляющим оцениваемой системы и по системе в целом.

В то же время предлагаемый разработчиками программный комплекс «Аван-Гард-Анализ» призван выполнять вспомогательную роль в решении задач управления ИБ, а именно: обеспечивать полноценный всесторонний анализ, позволяющий аргументированно сформулировать набор целей безопасности, обосновать политику безопасности, гарантировать полноту требований безопасности, контроль выполнения которых нужно осуществлять. Соответственно оценка рисков в нем проводится с целью разрешения указанных проблем.

Методика оценки рисков комплекса «АванГард-Контроль» подчинена задаче контроля уровня защищенности АИС и потому отличается от методики комплекса «АванГард-Анализ». Если методика комплекса «АванГард-Анализ» относится к *рискам возможных нарушений безопасности оцениваемой системы,* то методика комплекса «АванГард-Контроль» посвящена *рискам, являющимся результатом невыполнения требований обеспечения безопасности оцениваемой системы и ее компонентов.*

Следовательно, для применения комплекса «АванГард-Контроль» необходимо для каждого компонента оцениваемой системы иметь полный набор требований, выполнение которых означает нулевой риск нарушения безопасности системы. В то же время подразумевается, что при невыполнении всех требований риск нарушения безопасности системы будет 100-процентным.

Значительно облегчить работу по составлению полных наборов требований позволяет использование профилей защиты для отдельных компонентов оцениваемой системы, построенных на основе принятого в конце 2002 г. ГОСТ Р ИСО/МЭК 15408-2002 по критериям оценки безопасности информационных технологий. В связи с тем, что в 2004 г. планируется введение этого ГОСТа в действие, рассмотрим подробнее возможности оценить риски невыполнения его требований с помощью системы «АванГард-Контроль» .

Предварительно поясним, что программный комплекс «АванГард-Контроль», в свою очередь, состоит из двух частей - программного комплекса (ПК) «АванГард-Центр» и ПК «АванГард-Регион». Первый предназначен для нескольких целей, таких как разработка профилей защиты (ПЗ); подготовка и рассылка ПЗ посредством электронной почты по подконтрольным частям АИС; автоматизированный сбор отчетности о выполнении требований безопасности в частях АИС; оценка рисков невыполнения требований безопасности в АИС; идентификация узких мест в защите. Второй - для получения профилей защиты в отдельных частях АИС, автоматизации ведения отчетности о выполнении ПЗ и отсылки этой отчетности для ее обработки ПК «АванГард-Центр».

Разработка профилей защиты в ПК «АванГард-Центр» проводится в разделе ведения каталогов программного комплекса. Изначально в КЭС «АванГард» было определено несколько ключевых понятий, таких как метакласс, класс, мера, требование. *Метаклассы* предназначены для группировки классов объектов АИС по каким-либо конкретным признакам. *Классы* определяют классы объектов, для которых формируются типовые наборы требований (профили защиты). *Меры* устанавливают функциональные классы и классы гарантий требований в терминологии ГОСТ Р ИСО/МЭК 15408-2002. *Требования* включают функциональные семейства, семейства гарантий, функциональные компоненты, компоненты гарантий, функциональные элементы и элементы гарантий в соответствии с ГОСТ Р ИСО/ МЭК 15408-2002.

Для профилей защиты, создаваемых на основе ГОСТ Р ИСО/МЭК 15408-2002, в каталогах ПК «АванГард-Центр» выделен метакласс «Требования и профили защиты по ГОСТ Р ИСО/МЭК 15408-2002» (рис. 4.17). В этом метаклассе создан один «базовый» класс, в который входят все требования, содержащиеся в ГОСТ Р ИСО/МЭК 15408-2002 (рис. 4.18), как функциональные, так и касающиеся гарантий безопасности.

По каждому из уровней в нижней правой части формы выводится подробная информация, относящаяся к выбранной записи каталога. На рис. 4.19 представлен набор требований по мере в ПК «АванГард-Центр». В рассматриваемом примере FAU_GEN.l будет преобразован из формы, содержащей указания на необходимость определения списков назначения, в форму, где такие списки будут сформированы для конкретного профиля защиты.

Профили защиты по ГОСТ Р ИСО/МЭК 15408-2002 строятся следующим образом. Средствами ПК «АванГард-Центр» делается копия класса «Требования ГОСТ Р ИСО/МЭК 15408-2002». Далее выполняется операция «Вставить как шаблон профиля защиты» в метакласс «Требования и профили защиты по

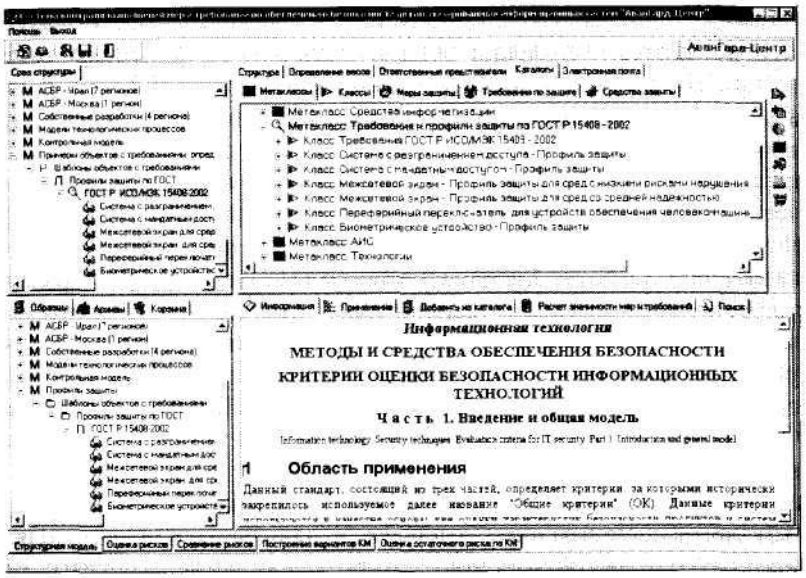


Рис. 4.17. Состав метакласса «Требования и профили защиты по ГОСТ Р ИСО/МЭК 15408-2002» в ПК «АванГард-Центр»

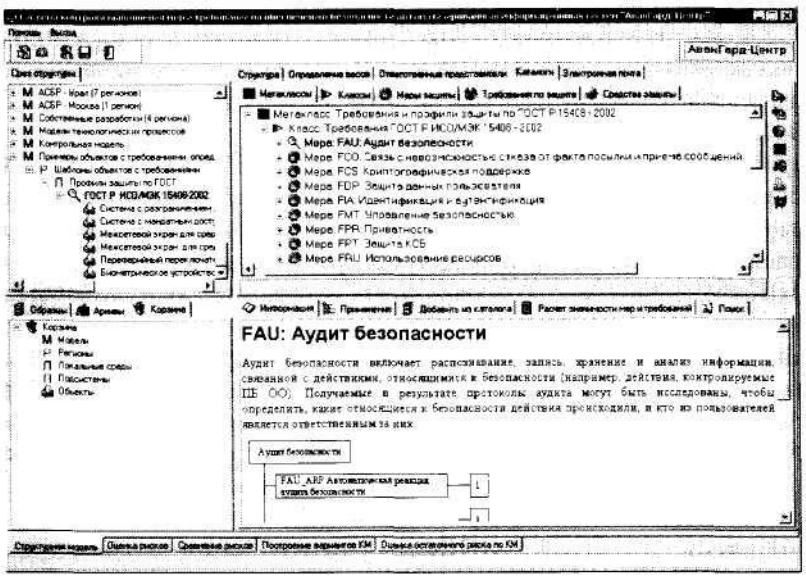


Рис. 4.18. Состав класса «Требования ГОСТ Р ИСО/МЭК 15408-2002» в ПК «АванГард-Центр»

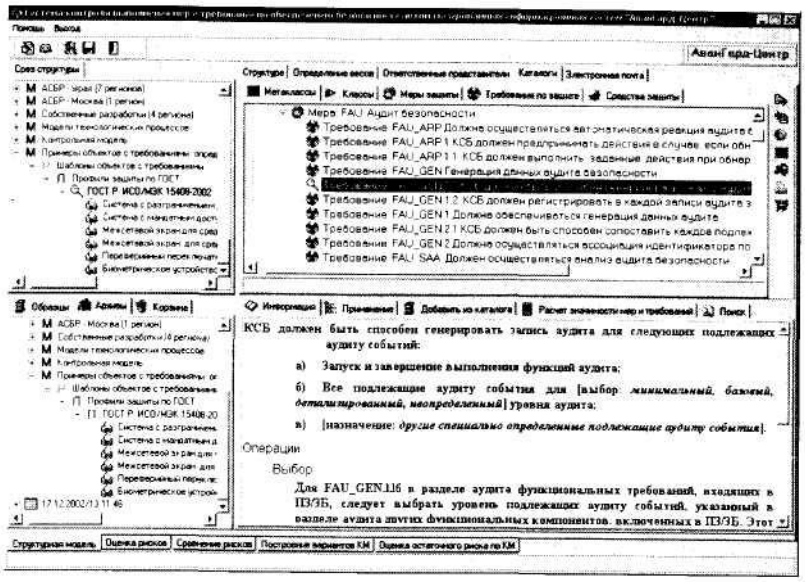


Рис. 4.19. Состав требований по мере (функциональному классу) в ПК «АванГард-Центр»

ГОСТ Р ИСО/МЭК 15408-2002». При этом предлагается поменять название класса. Предположим, что оно было заменено на следующее: «Система с разграничением доступа - Профиль защиты». В результате создается шаблон, который путем последовательного анализа требований корректируется так, что в нем остаются только меры и требования, необходимые для поддержания безопасности объектов того типа, для которого строится этот профиль защиты (рис. 4.20). Все ненужные в данном профиле меры и требования удаляются, а в оставшихся содержимое приводится в соответствие задачам обеспечения безопасности заданного типа объектов.

На рис. 4.21 показано, как было изменено и конкретизировано требование FAU_GEN.l в профиле защиты для систем с разграничением доступа (ПЗ СРД).

В рассмотренном примере в качестве шаблона использовался полный набор требований ГОСТ Р ИСО/МЭК 15408-2002, но в принципе шаблоном для создания нового профиля может послужить и любой другой из уже готовых профилей защиты, причем допускается не только удалять из него ненужные меры и требования, но при необходимости добавлять новые, а также изменять их для достижения нужной степени адекватности целям безопасности, которым должен удовлетворять новый ПЗ.

Созданные профили защиты могут быть либо распечатаны на бумаге, либо экспортированы в файл формата редактора WinWord. Фрагмент генерируемого отчета представлен на рис. 4.22.

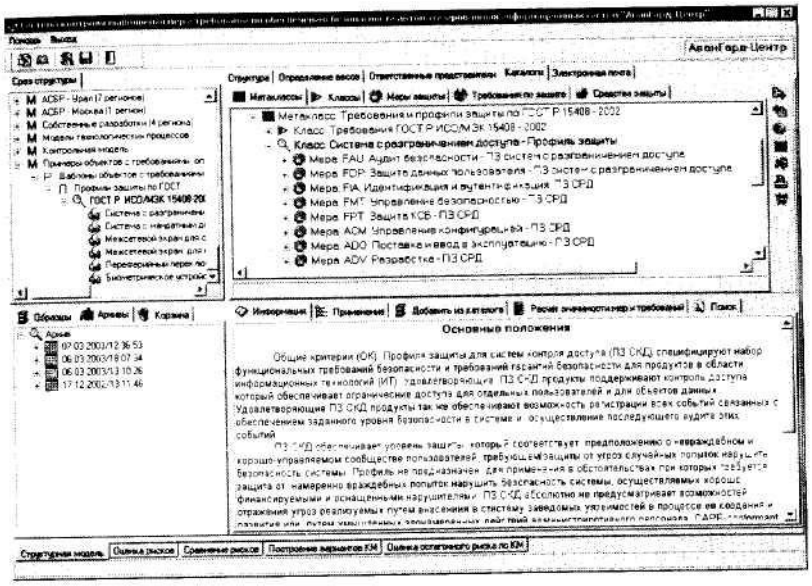


Рис. 4.20. Профиль защиты для систем с разграничением доступа (ПЗ СРД), в котором убраны все записи с функциональными классами и классами гарантий, не отвечающими целям безопасности ПЗ СРД

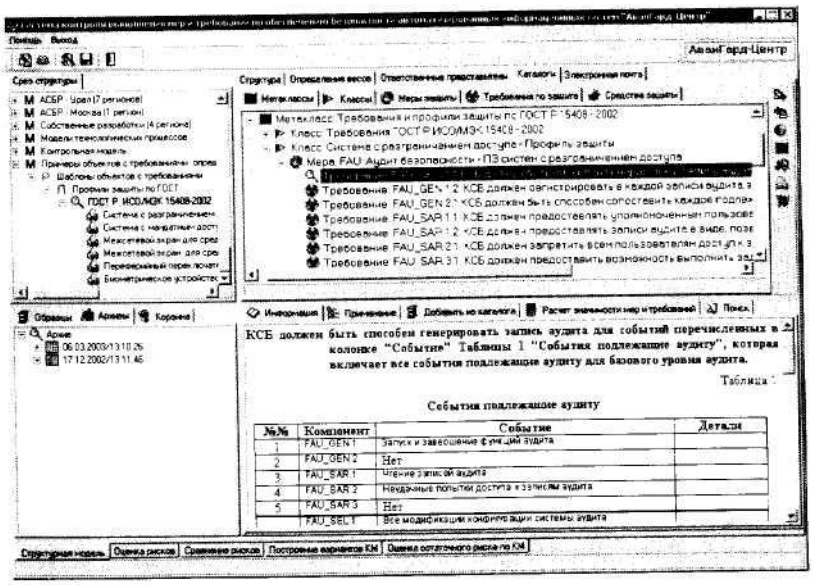
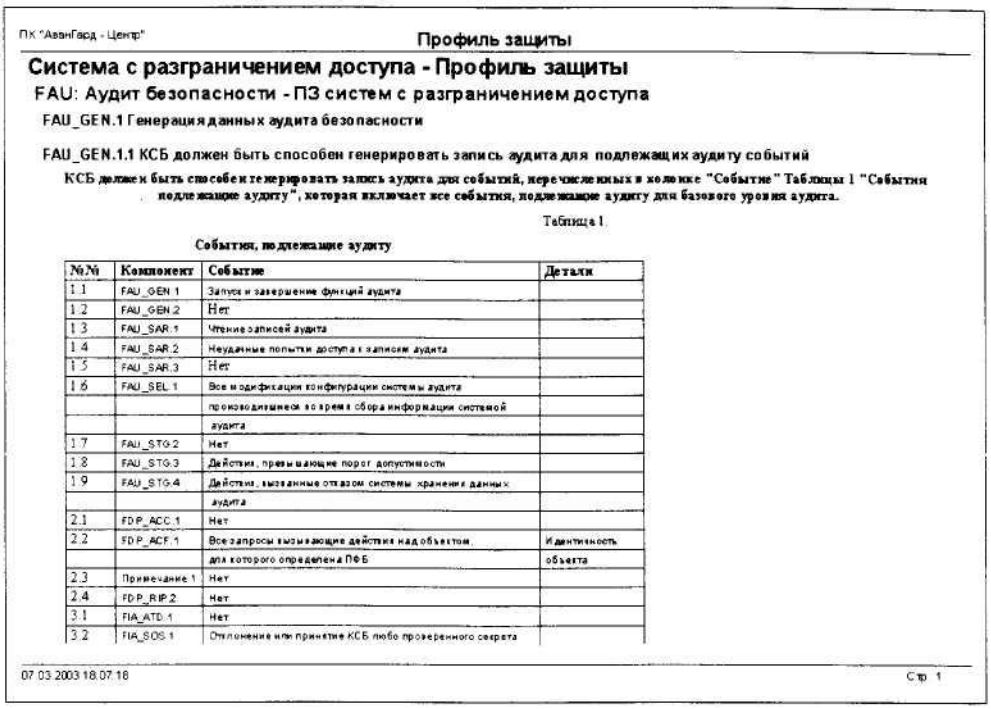


Рис. 4.21. Конкретизация профиля защиты



ПК "АванГард - Центр" Профиль защиты

Система с разграничением доступа - Профиль защиты

FAU: Аудит безопасности - ПЗ систем с разграничением доступа

FAU_GEN.1 Генерация данных аудита безопасности

FAU_GEN.1.1 КСБ должен быть способен генерировать запись аудита для подлежащих аудиту событий

КСБ должен быть способен генерировать запись аудита для событий, перечисленных в колонке "Событие" Таблицы 1 "События подлежащие аудиту", которая включает все события, подлежащие аудиту для базового уровня аудита.

Таблица 1

События, подлежащие аудиту

№№	Компонент	Событие	Детали
1.1	FAU_GEN.1	Запуск и завершение функций аудита	
1.2	FAU_GEN.2	Нет	
1.3	FAU_SAR.1	Чтение записей аудита	
1.4	FAU_SAR.2	Неудачные попытки доступа к записям аудита	
1.5	FAU_SAR.3	Нет	
1.6	FAU_SEL.1	Все модификации конфигурации системы аудита	
		производимые во время сбора информации системой	
		аудита	
1.7	FAU_STG.2	Нет	
1.8	FAU_STG.3	Действия, превышающие порог допустимости	
1.9	FAU_STG.4	Действия, вызванные отказом системы хранения данных	
		аудита	
2.1	FDP_ACC.1	Нет	
2.2	FDP_ACF.1	Все запросы вызывающие действия над объектом,	Идентичность
		для которого определена ПФБ	объекта
2.3	Примечание 1	Нет	
2.4	FDP_RIP.2	Нет	
3.1	FIA_ATD.1	Нет	
3.2	FIA_SOS.1	Отклонение или принятие КСБ любо проверенного секрета	

07.03.2003 18:07:18 Стр. 1

Рис. 4.22. Фрагмент отчета «Профиль защиты», генерируемого ПК «АванГард-Центр»

С помощью разрабатываемых в системе ПК «АванГард-Центр» профилей защиты в структурную модель анализируемой системы заносятся объекты, оцениваемые по заданному ПЗ. Для создания таких объектов оценки (ОО) выполняется операция перетаскивания (drug and drop) нужного профиля защиты на ту составляющую структурной модели, в качестве элемента которой должен быть показан объект, отвечающий требованиям безопасности и соответствующий выбранному ПЗ. Результат такого рода операции и пример оценок, отражающих фиксацию фактов выполнения отдельных требований, демонстрируется на рис. 4.23.

«АванГард-Центр» позволяет по результатам анализа выполнения требований ПЗ по отдельным ОО оценить риски невыполнения требований в информационной системе. Пример представления в виде гистограмм оценок рисков невыполнения требований демонстрируется на рис. 4.24. Чем больше требований не выполняется, тем больше риски и тем выше столбики гистограммы. В рассмотренном примере значимости отдельных требований приняты одинаковыми, но в принципе можно задавать различные значения, отражающие реальную важность отдельных требований для обеспечения безопасности ОО.

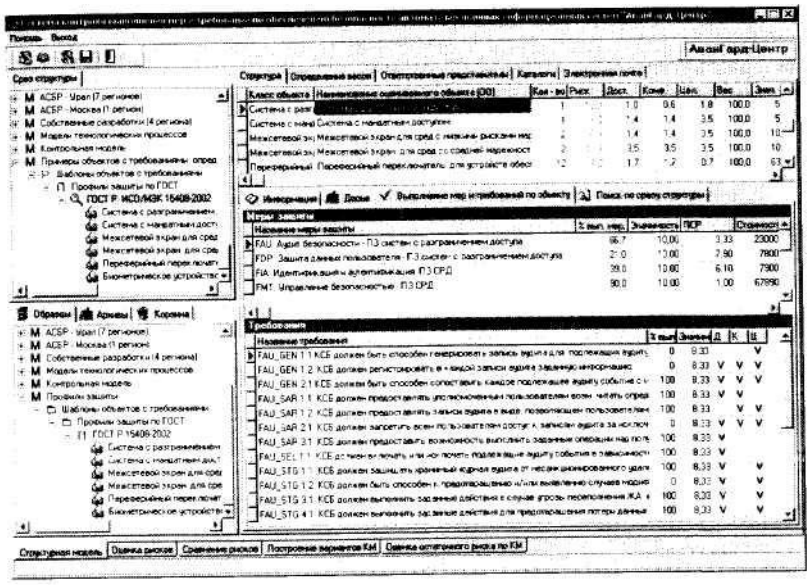


Рис. 4.23. Пример оценки выполнения требований ПЗ по конкретному оцениваемому объекту

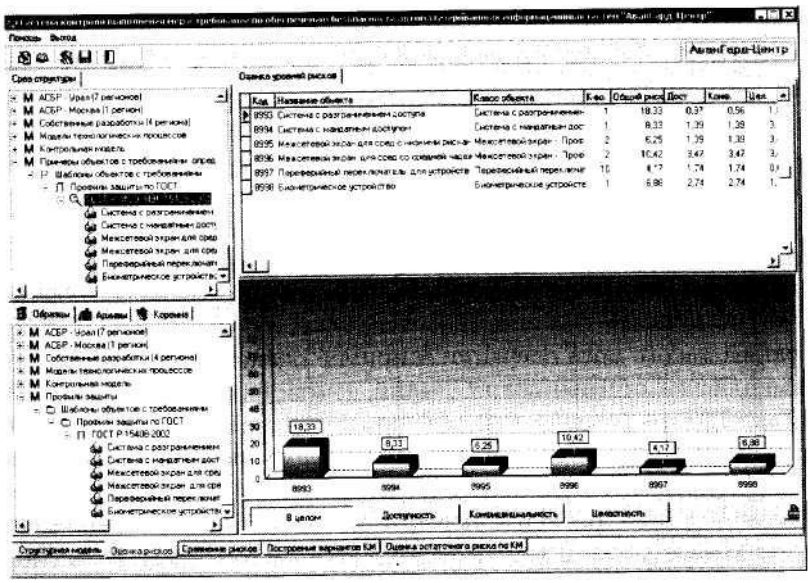


Рис. 4.24. Пример графической иллюстрации оценок рисков невыполнения требований ПЗ в ПК «Аван[ард-Центр»

Таким образом, КЭС «АванГард» позволяет не только автоматизировать процесс разработки профилей защиты в соответствии с ГОСТ Р ИСО/МЭК 15408-2002, но и использовать ПЗ для оценки выполнения этих требований в информационных системах организации.

В заключение следует отметить, что экспертная система «АванГард» хорошо подходит для построения ведомственных и корпоративных методик анализа рисков и управления ими. Ее можно рассматривать как полноценный универсальный инструментарий и для анализа и оценки рисков, и для решения задач всеобъемлющего систематического контроля безопасности АИС (в том числе в таких аспектах, как выполнение политик безопасности, ГОСТов и требований Гостехкомиссии, законодательства, внутренних приказов и распоряжений, касающихся безопасности, а также должностных инструкций) во всех подразделениях, использующих АИС.

4.2.5 RiskWatch

Компания RiskWatch [343] предлагает два продукта: один относится к информационной, второй - к физической безопасности. ПО предназначено для идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в области 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 состоит из четырех этапов.

Первый этап - определение предмета исследования. На данном этапе описываются параметры организации: ее тип, состав исследуемой системы, базовые требования в области безопасности (рис. 4.25). Описание формализуется в ряде подпунктов, которые можно отметить для подробной детализации (рис. 4.26) или пропустить.

Далее каждый из указанных пунктов описывается подробно.

Для облегчения работы аналитика в шаблонах даются списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно отобрать те, которые реально присутствуют в организации.

На рис. 4.26 представлен пример описания различных категорий ресурсов.

Допускается модификация названий и описаний, а также добавление новых категорий, что позволяет достаточно просто русифицировать данный метод.

Второй этап - внесение данных, касающихся конкретных характеристик системы (рис. 4.27). Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей.

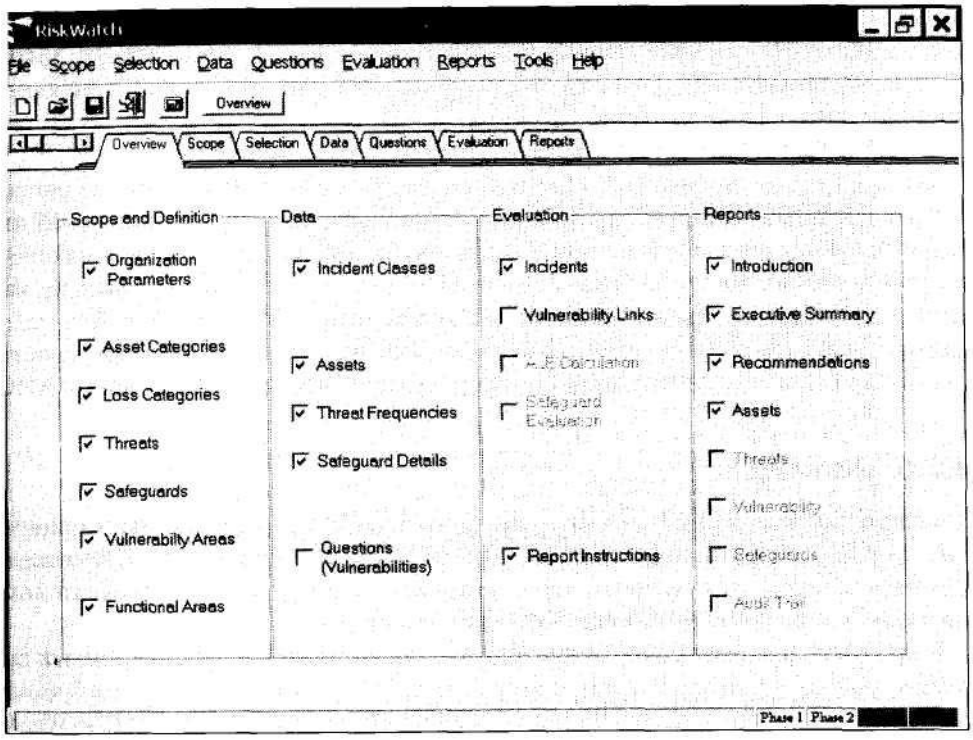


Рис. 4.25. Описание информационной системы с позиции безопасности в RiskWatch

На этом этапе:

– подробно описываются ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов;
– с помощью опросника, база которого содержит более 600 вопросов, выявляются возможные уязвимости. Вопросы связаны с категориями ресурсов. Допускается корректировка и исключение вопросов или добавление новых;
– задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Все это служит в дальнейшем для расчета эффективности внедрения средств защиты.

Третий этап - оценка рисков (см. рис. 4.28). Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих этапах.

Для рисков рассчитываются математические ожидания потерь за год по формуле:

$m = p \times v$,

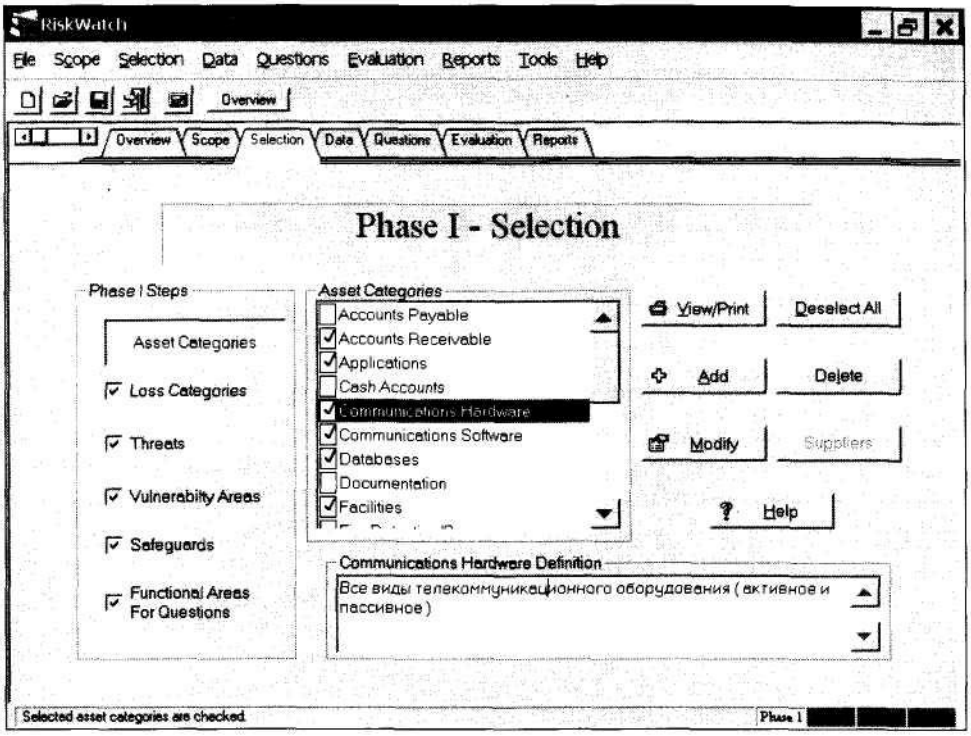


Рис. 4.26. Описание ресурсов информационной системы

где p - частота возникновения угрозы в течение года,

v - стоимость ресурса, который подвергается угрозе.

Например, если стоимость сервера составляет 150 000 долл., а вероятность его уничтожения пожаром в течение года - 0,01, то ожидаемые потери будут равны 1500 долл.

Дополнительно рассматриваются сценарии «что если...», которые позволяют описать аналогичные ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при наличии защитных мер и без них, можно оценить эффект от таких мероприятий.

Четвертый этап - генерация отчетов. 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.

Ниже (рис. 4.29) приводится фрагмент отчета.

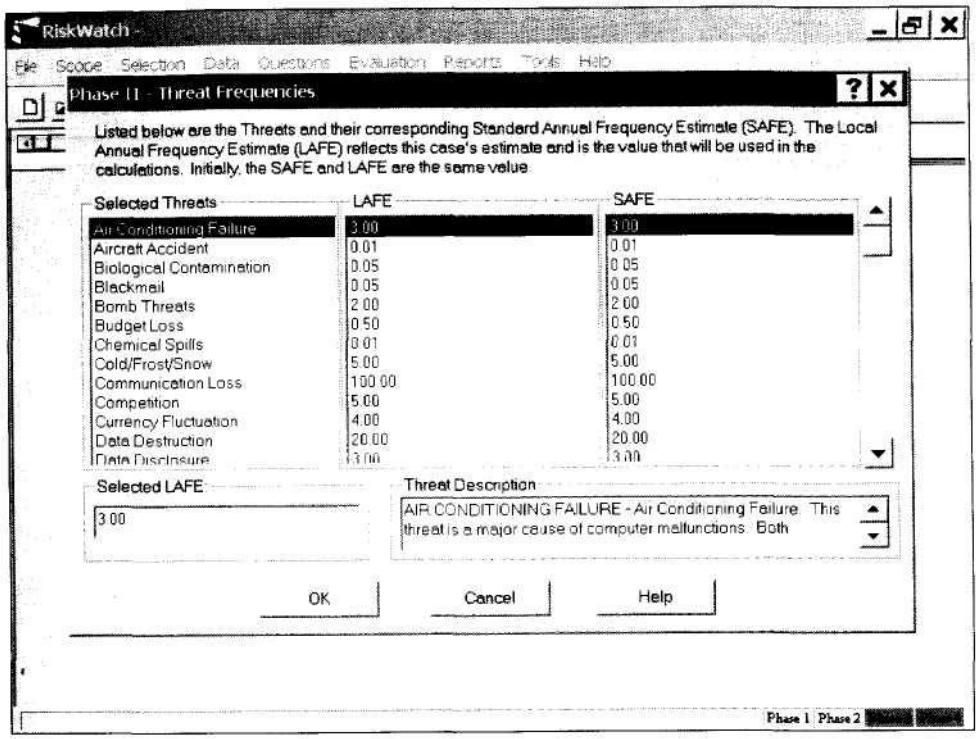


Рис. 4.27. Оценка параметров угроз с использованием статистических данных

Возможности RiskWatch

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

Трудоемкость работ по анализу рисков этим методом сравнительно невелика. Такой метод удобен, если требуется провести анализ рисков на программно-техническом уровне защиты без учета организационных и административных факторов. Однако следует иметь в виду, что полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывают понимание риска с системных позиций.

Существенным достоинством RiskWatch с точки зрения отечественного потребителя является его 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, отражающие отечественные требования в области безопасности, разрабатывать ведомственные методики анализа и управления рисками.

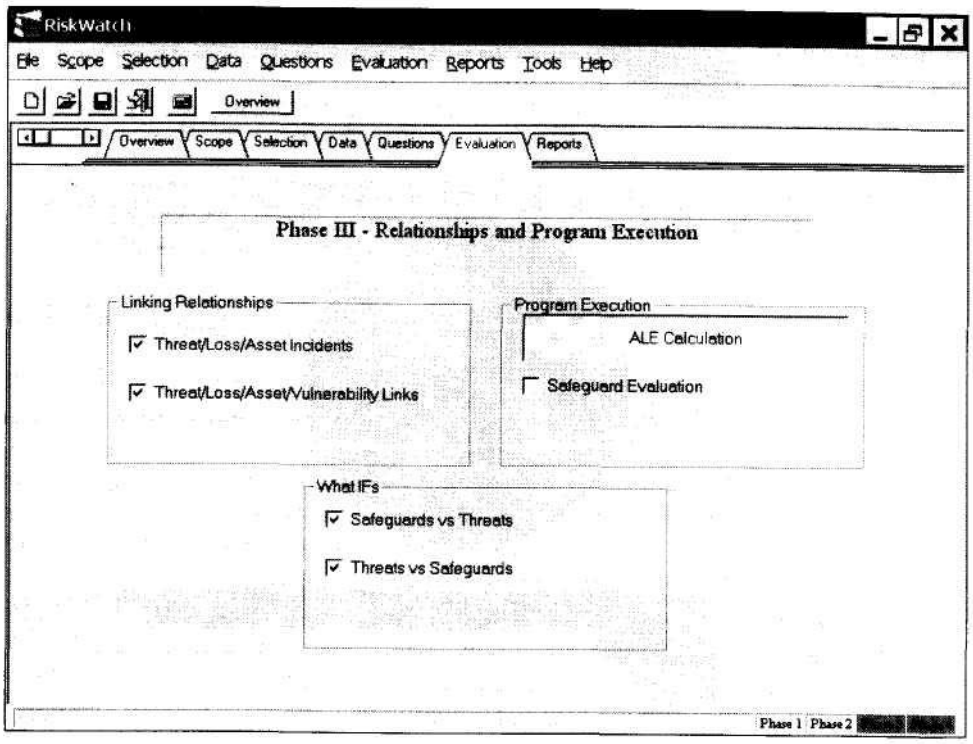


Рис. 4.28. Содержание третьей стадии в RiskWatch

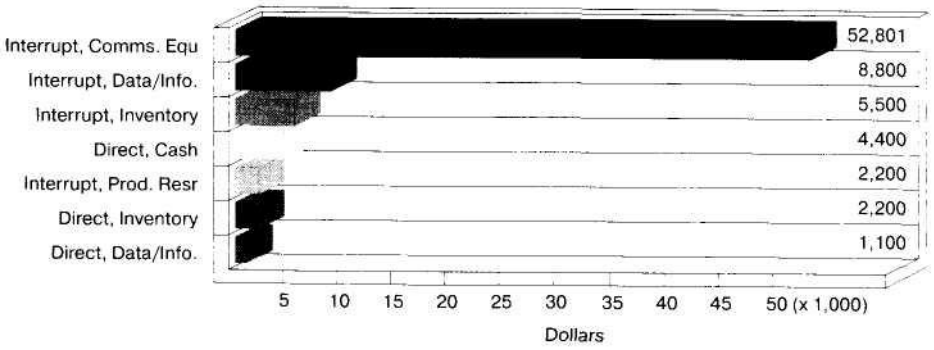


Рис. 4.29. Результирующие оценки по одной из угроз - кражи (начало)

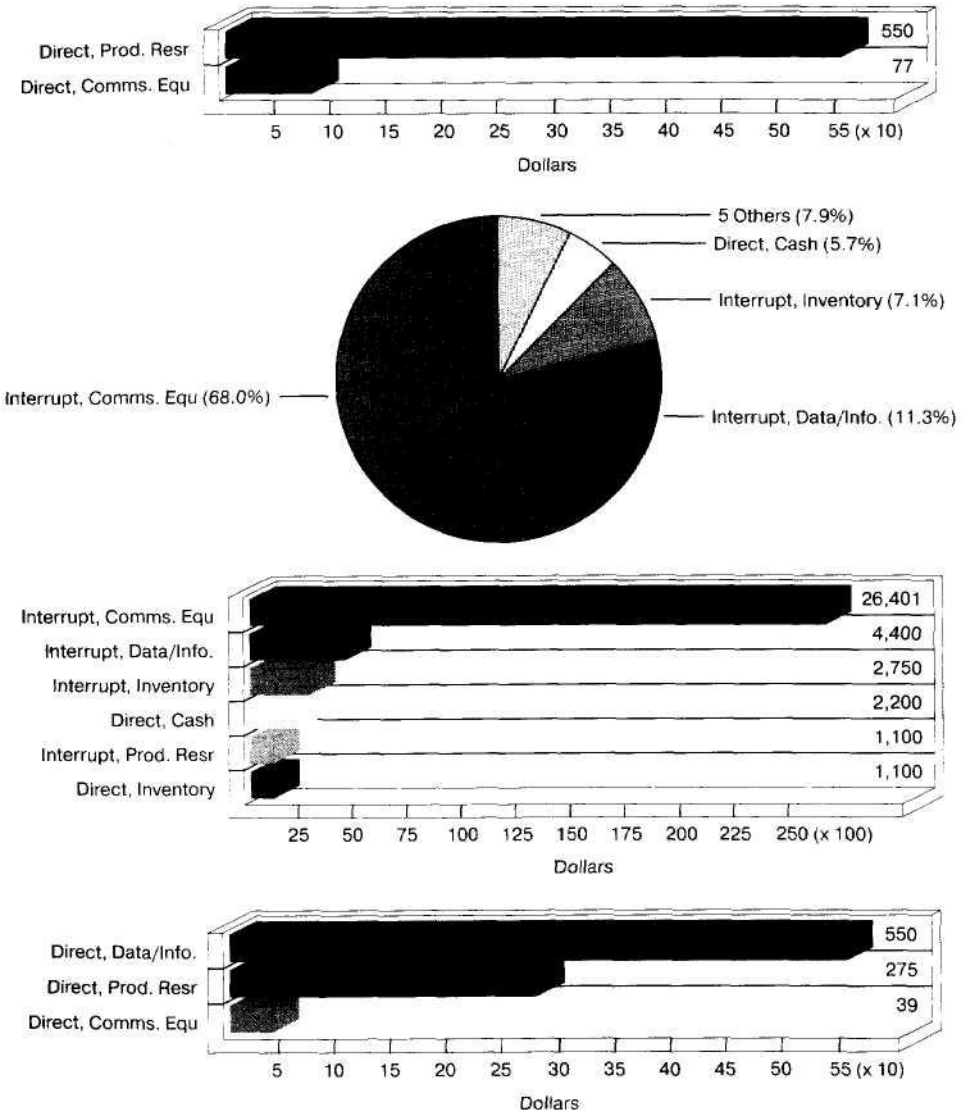


Рис. 4.29. Результирующие оценки по одной из угроз ~ кражи (окончание)

Глава 5
Аудит безопасности и анализ рисков

5.1 Актуальность аудита безопасности

Понятие «аудит информационной безопасности» появилось сравнительно недавно. Тем не менее в настоящее время аудит информационной безопасности корпоративных систем представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области безопасности этих систем и вызывает постоянный интерес специалистов. Его основная задача - объективно оценить текущее состояние ИБ компании, а также ее адекватность поставленным целям и задачам бизнеса для увеличения эффективности и рентабельности экономической деятельности компании. Поэтому под аудитом информационной безопасности корпоративной системы обычно понимается системный процесс получения объективных качественных и количественных оценок о текущем состоянии ИБ компании в соответствии с определенными критериями и показателями безопасности. Считается, что результаты квалифицированно выполненного аудита ИБ компании позволяют построить оптимальную по эффективности и затратам корпоративную систему защиты, адекватную ее текущим задачам и целям бизнеса.

Насколько аудит безопасности может быть полезным для вашей компании? Попробуем разобраться вместе. Не секрет, что сейчас наблюдается повсеместное усиление зависимости успешности деятельности компании от корпоративной системы защиты информации. Связано это с увеличением объема жизненно важных для компании данных, обрабатываемых в корпоративной информационной системе. Тем же объясняются и дополнительные капиталовложения в информационные системы компании. Вот почему актуальность аудита информационной безопасности резко возрастает.

Практика внедрения новых корпоративных информационных систем свидетельствует, что компании не всегда получают полную отдачу капиталовложений, и прежде всего из-за усложнения современных корпоративных систем и большей их уязвимости. Можно выделить две основные причины увеличения уязвимости корпоративных систем. Во-первых, возросла уязвимость собственно корпоративных информационных систем за счет обоснованного усложнения их аппаратно-программных элементов, повышения структурной и функциональной сложности системного и прикладного программного обеспечения, применения новых технологий обработки, передачи и хранения данных. А во-вторых, расширился спектр угроз корпоративным информационным системам из-за передачи информации по открытым каналам сетей общего назначения, «информационных войн и электронных диверсий» конкурирующих организаций, активного промышленного шпионажа с привлечением профессионалов в области защиты информации и пр. Современный рынок безопасности насыщен средствами обеспечения информационной безопасности. Постоянно изучая существующие предложения этого рынка, многие компании видят неадекватность ранее вложенных средств в системы ИБ, например по причине морального старения оборудования и программного обеспечения. Поэтому они ищут варианты решения этой проблемы. Таких вариантов может быть два: с одной стороны - полная замена системы корпоративной защиты информации, что потребует больших капиталовложений, а с другой - модернизация существующих систем безопасности. Последний вариант менее затратный, но несет новые сложности, например требует ответа на следующие вопросы: Как совместить старые, сохраненные из имеющихся, аппаратно-программные средства безопасности с новыми элементами системы защиты информации? Как организовать централизованное управление разнородными средствами обеспечения безопасности? Как оценить, а при

необходимости и переоценить информационные риски компании? Более существенная причина необходимости проведения аудита безопасности состоит в том, что при модернизации и внедрении новых технологий защиты информации их потенциал полностью не реализуется. Здесь аудит дает возможность анализировать текущую безопасность функционирования корпоративной информационной системы, оценивать и прогнозировать риски, управлять их влиянием на бизнес-процессы компании, корректно и обоснованно подойти к вопросу поддержания безопасности ее информационных активов - стратегических планов развития, маркетинговых программ, финансовых и бухгалтерских ведомостей, содержимого корпоративных баз данных. В итоге грамотно проведенный аудит безопасности корпоративной информационной системы позволяет добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание систем безопасности.

Аудит ИБ выполняет команда специалистов по безопасности корпоративных систем и специалистов в области менеджмента. Проведение аудита способствует формированию единого взгляда на проблемы безопасности компании среди специалистов разного профиля. В данном случае они объединяются в одну команду, ориентированную на повышение экономической эффективности и рентабельности бизнес-деятельности компании. Другой существенный плюс подобного подхода - поддержка полного жизненного цикла корпоративной системы защиты информации, начиная с анализа требований и заканчивая этапами эксплуатации и сопровождения системы. Примечательно, что с помощью структурных и объектно-ориентированных CASE-средств анализа рисков и управления ими удается наглядно и эффективно представлять компоненты информационной инфраструктуры компании, выделять наиболее критичные из них, а также оценивать информационные риски. Результаты приводятся в удобной графической форме, с выделением существенных с точки зрения управления компанией компонентов информационной инфраструктуры компании и связей по управлению и данными между этими компонентами. Благодаря такой общей визуализации бизнес-процессов и информационной безопасности компании можно оперативно анализировать различные варианты защиты, сравнивать их между собой с позиций экономической эффективности и в итоге выбирать оптимальный вариант построения или модификации защиты корпоративной системы.

В настоящее время многие поставщики средств защиты информации декларируют поставку полного, законченного решения в области безопасности корпоративных систем. К сожалению, в лучшем случае все сводится к проектированию и поставке соответствующего оборудования и программного обеспечения. Построение комплексной корпоративной системы безопасности «остается в тени» и к решению, как правило, не прилагается. Поэтому у TOP-менеджеров компаний зачастую возникает целый ряд вопросов:

- Соответствует ли наша корпоративная система информационной безопасности целям и задачам бизнеса компании?
- Адекватна ли принятая в компании политика безопасности целям и задачам бизнеса?
- Каким образом эффективно контролировать реализацию и выполнение политики безопасности в компании?
- Когда следует провести модернизацию системы безопасности? Как обосновать необходимость модернизации и затрат?
- Как быстро окупятся инвестиции в корпоративную систему безопасности? Где здесь точка безубыточности?
- Насколько правильно и корректно сконфигурированы и настроены штатные средства поддержания информационной безопасности компании?
- Как убедиться в том, что существующие в компании средства защиты - межсетевые экраны (firewall), системы обнаружения вторжений (IDS), антивирусные шлюзы, VPN-шлюзы - эффективно справляются со своими задачами?
- Как решаются вопросы обеспечения конфиденциальности, доступности и целостности?

- Как оценить работу подрядных организаций и компаний, которые выполнили проектирование, поставку, монтаж и пуско-наладку средств безопасности? Есть ли недостатки, и если да, то какие?
- Как обеспечить столь необходимую в практике «вертикаль власти» для централизованного управления безопасностью компании?
- Как контролировать состояние информационной безопасности компании? Какие методы и средства здесь требуются?
- Что делать после того, как корпоративная система обеспечения безопасности построена (имеются стратегический и тактический планы защиты компании, планы работы при возникновении чрезвычайных ситуаций)?
- Есть ли необходимость постоянно обучать сотрудников службы информационной безопасности компании? И если да, то какие бюджетные средства нужны?
- Как управлять информационными рисками компании? Какие инструментальные средства для этого необходимо задействовать?
- Удовлетворяет ли организация информационной безопасности компании требованиям международных стандартов оценки и управления безопасностью, например ISO 15408, ISO 17799 (BS 7799), BSI?

Очевидно, что на перечисленные вопросы нельзя сразу дать однозначный ответ. Только объективный и независимый аудит безопасности корпоративной системы предоставит достоверную и обоснованную информацию. Такой аудит, который позволит комплексно проверить все основные уровни обеспечения информационной безопасности компании: нормативно-правовой, организационный, технологический и аппаратно-программный.

Как оценить уровень безопасности КИС?

Современные методики анализа рисков информационной безопасности, проектирования и сопровождения систем безопасности дают возможность:

- количественно оценить текущий уровень безопасности, обосновать допустимые уровни рисков, разработать план мероприятий по поддержанию требуемого уровня безопасности на организационно-управленческом, технологическом и техническом уровнях;
- рассчитать и экономически обосновать размер необходимых вложений в систему безопасности, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;
- выявить и провести первоочередные мероприятия для уменьшения наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;
- определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц, ответственных за информационную безопасность предприятия, создать или модифицировать необходимый пакет организационно-распорядительной документации;
- разработать и согласовать со службами организации и надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;
- организовать поддержание внедренного комплекса защиты в соответствии с изменяющимися условиями работы организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

5.2 Основные понятия и определения

Рассмотрим особенности современных зарубежных стандартов в области аудита и сертификации и их отличие от действующих в настоящее время в России руководящих документов в области сертификации и аттестации.

Российские термины, относящиеся к сертификации и аттестации по требованиям ИБ (определения Гостехкомиссии), и аналогичные термины зарубежных стандартов зачастую трактуются по-разному. Проведем сравнение определений и терминов следующих российских и зарубежных стандартов и руководств в области защиты информации:

- РД Гостехкомиссии при президенте РФ 1992-1998 гг.;
- Практические рекомендации по управлению информационной безопасностью - стандарт BS 7799 (Великобритания);
- Управление в информационных технологиях - CobiT (Международная ассоциации аудита и управления информационными системами);
- стандарты NIST (США) по обеспечению ИБ NIST 800-16, 800-18, 800-30.

В российской нормативно-методической базе основными терминами являются: сертификация средств защиты информации и аттестация объектов информатизации.

Под *сертификацией средств защиты информации* по требованиям безопасности информации понимается деятельность, позволяющая убедиться в их соответствии требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Гостехкомиссией РФ.

Под *аттестацией объектов информатизации* подразумевается комплекс организационно-технических мероприятий, в результате которых подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией РФ.

В стандартах NIST аналогичные термины определяются следующим образом.

Сертификация (Certification) - подтверждение соответствия заявленных и фактических технических характеристик в области ИБ для приложений, компьютерных систем, инфраструктуры.

Аккредитация (Accreditation) — разрешение использования информационной системы общего применения или специализированных приложений (имеющих специальные требования к ИБ) для обработки информации. Основанием для выдачи разрешения служит сертификация выбранных решений на соответствие заданным требованиям по ИБ.

Ответственный за выдачу разрешения (Designated Approving Authority) - лицо, уполномоченное принять решение о допустимости определенного уровня рисков для рассматриваемой информационной системы или технологии обработки информации.

Сравнение приведенных определений показывает, что:

- термин сертификация понимается одинаково;
- приблизительным аналогом российского термина «аттестация объектов информатизации» является термин «аккредитация» - с одним существенным отличием: в американском варианте явно указано, что аккредитация производится специалистами, уполномоченными принять решение о допустимости определенного уровня рисков для рассматриваемой информационной системы или технологии.

При этом в российской нормативно-методической базе аспект рисков, допустимый уровень остаточных рисков, ответственность за принятие определенного уровня рисков не рассматриваются. После аккредитации информационной системы возможно проведение независимой экспертизы существующего режима ИБ -аудит ИБ в информационной системе. Этот

термин также встречается в англоязычной литературе и трактуется следующим образом [124]. *Аудит ИБ* в информационной системе - процесс сбора сведений, позволяющих установить, поддерживается ли безопасность ресурсов организации (включая данные); обеспечиваются ли необходимые параметры целостности и доступности данных; достигаются ли цели организации в части эффективности информационных технологий.

Важно также, что аудиторы ИБ и лица, проводящие аккредитацию информационной системы, должны представлять разные организации.

В российских РД не предусматривается возможность проведения аудита ИБ, вместо этого допускается повторная аттестация (возможно, другим органом по аттестации).

Российские РД и рассматриваемые зарубежные стандарты относятся фактически к различным классам, их системы понятий различаются. Существенными отличиями зарубежных стандартов являются:

- большое внимание к выбору и формальному описанию целей, которые ставятся в области ИБ для конкретной информационной системы. Используются механизмы оценки соответствия декларированных целей существующим показателям ИБ;
- учет аспектов, связанных с рисками, что позволяет оптимизировать построение подсистемы безопасности по критериям «цена-эффективность»;
- лучший учет таких составляющих ИБ, как целостность и доступность. Российские РД в основном ориентированы на обеспечение конфиденциальности;
- большая степень формализации требований к подсистеме ИБ. В современных стандартах и руководствах формальные требования и рекомендации излагаются в нескольких сотнях подразделов. Соответственно методики построения подсистем ИБ более конкретны, процедуры проведения аудита ИБ достаточно формализованы.

В настоящее время наиболее известны три схемы аудита ИБ:

- на соответствие Британскому стандарту BS 7799, часть 2;
- на соответствие требованиям Ассоциации аудита и управления информационными системами (The Information Systems Audit and Control Association & Fondation - ISACA);
- на соответствие требованиям Американского института общественных бухгалтеров (AICPA);

Рассмотрим наиболее распространенные в Европе BS 7799 и COBIT.

5.3 Аудит безопасности в соответствии с BS 7799, часть 2

5.3.1 Сертификация и аудит: организационные аспекты

Международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «Информационные технологии - управление информационной безопасностью» (Information technology - Information security management) на сегодняшний день наиболее распространен. Он был разработан на основе первой части Британского стандарта BS 7799-1 «Практические рекомендации по управлению информационной безопасностью» (Information security management, Part 1: Code of practice for information security management), однако не включает вторую часть стандарта BS 7799-2:2002, посвященного вопросам аудита безопасности. Таким образом, можно говорить о соответствии информационной системы требованиям ISO/IEC 17799:2000 (BS 7799-1:2000), но сертификацию информационной системы можно выполнять только в соответствии с BS 7799-2:2002 (Part II). Сертификация информационной системы подтверждает ее соответствие требованиям BS 7799-1 со стороны независимого аудитора.

Вопросами сертификации в Великобритании ведает Британский институт стандартов (British Standards Institution - BSI) (www.bsi-global.com) под его контролем организация UKAS (United Kingdom Accredited Service) занимается аккредитацией организаций на право аудита ИБ в соответствии со стандартом BS 7799. Сертификаты, выданные этими организациями, признаются не только в Великобритании, но и во многих странах мира.

Организация, решившая провести аудит ИБ, должна выполнить подготовительные мероприятия, привести в соответствие с требованиями стандарта документацию и систему управления ИБ. После этого приглашается аудитор. Процедура аудита описана ниже. Ее трудоемкость для крупных организаций может достигать 25-30 человеко-дней работы аудитора.

Сертификаты выдаются после завершения аудита подсистемы ИБ на соответствие стандартам BS 7799 и действительны в течение 3 лет.

Общими вопросами управления информационной безопасности компаний и организаций, а также развитием аудита безопасности занимаются международный комитет Joint Technical Committee ISO/IEC JTC 1 совместно с институтом стандартов BSI и, в частности, служба UKAS. Эта служба производит аккредитацию организаций на право аудита информационной безопасности в соответствии со стандартом BS 7799-1.

Обсудим процедуру проведении аудита информационных систем.

5.3.2 Методика проведения аудита

Рассмотрим основные положения методики проведения аудита и рекомендованные средства и способы оценки рисков Guide to BS 7799 risk assessment and risk management [145], Guide to BS 7799 auditing [167]. Эти рекомендации вполне применимы к отечественным условиям и могут быть использованы при разработке соответствующих методик. Особенно полезными представляются простейшие годы оценки рисков и управления ими, не требующие установки сложного и дорогостоящего программного обеспечения.

Каждая компания, решившая провести аудит информационной безопасности в соответствии с требованиями стандарта BS 7799 (ISO/IEC 17799), должна осуществить подготовительные мероприятия, которые включают приведение в надлежащий вид нормативно-методической документации компании по организации информационной безопасности и внутреннюю проверку соответствия системы обеспечения информационной безопасности компании требованиям стандарта. Только после этого компания приглашает аудитора.

Процедура аудита информационной безопасности компании начинается с составления детальных и подробных планов проведения аудита. Планы должны быть представлены соответствующим лицам компании до начала процесса аудита. При этом важно, чтобы аудиторы были ознакомлены с тем, каким законодательно-правовым нормам и требованиям отраслевых и ведомственных стандартов следует проверяемая организация или компания. Далее начинается проверка нормативно-методической документации компании, которая может происходить как внутри компании, так и за ее пределами. К проверяемой документации может относиться концепция и политика безопасности, описание границ защищаемой системы (карта корпоративной системы, в том числе описание состава и структуры ;пользуемого в компании прикладного и системного программного обеспечения), должностные инструкции корпоративных пользователей, положения о департаменте информационной безопасности, описания методик оценки и управления информационными рисками, оценки состояния информационной безопасности компании, правил и норм эксплуатации программно-технических средств обеспечения информационной безопасности и пр. Если компания уже проходила процедуру аудита, то также предъявляется отчет о предыдущей проверке и данные обо всех выявленных ранее несоответствиях. Кроме того, должна быть составлена ведомость соответствия (Statement of Applicability) - документ, в котором оценивается соответствие поставленных целей и средств управления информационной безопасностью требованиям стандарта.

Сущность процедуры аудита безопасности на соответствие системы управления информационной безопасностью компании требованиям стандарта заключается проверке выполнения всех положений стандарта. По каждому такому положению проверяющие должны ответить, выполняется ли данное требование и, если нет, каковы причины невыполнения. На базе ответов составляется ведомость соответствия, основная цель которой - аргументированное обоснование имеющихся отклонений от требований стандарта. По завершении аудита безопасности выявленные несоответствия при необходимости могут быть устранены. Другими словами, в ходе аудита всей компании специалист должен собрать доказательства того, что организация отвечает всем требованиям стандарта BS 7799. Это делается по результатам анализа документов, бесед с экспертами, а если потребуется - проведения соответствующих организационных проверок режима безопасности и инструментальных проверок компонентов корпоративной системы Internet/Intranet. В итоге должны быть проверены организация информационной безопасности компании, обязанности по обеспечению информационной безопасности сотрудников, наличие документированной политики и стратегии информационной безопасности для компании и, в частности, документированной стратегии и общих положений подхода к оцениванию рисков и управлению ими. При этом обращается внимание на наличие документированных, применимых на практике методик оценивания рисков и управления ими, а также обоснования правильности выбора средств защиты для информационной системы компании. Выявляется, имеются ли документированные процедуры оценки остаточного риска, проверки режима информационной безопасности и журналов, в которых фиксируются результаты проверки. У аудитора должна быть полная ясность относительно того, утверждены ли правила обслуживания и администрирования информационной системы, есть ли распоряжения должностных лиц о проведении периодических проверок оценивания рисков и управления ими, документация по системе управления информационной безопасностью и реестр необходимых средств.

Специалист, отвечающий за аудит информационной безопасности компании, обязан выполнить, по меньшей мере, выборочные проверки выводов, сделанных при оценке рисков. В каждом случае нужно убедиться, что вся информация, подвергавшаяся проверке, подтверждена документально в должном объеме, риски оценивались в соответствии с корректными методиками, а результаты достоверны и могут быть использованы в дальнейшем. Кроме того, следует удостоверить факт соответствия рассматриваемым рискам средств обеспечения информационной безопасности, выбранных на основе рекомендаций BS ISO/IEC, их правильного применения и прохождения ими тестирования, а также знание сотрудниками политики информационной безопасности компании. Принятую систему управления информационной безопасностью необходимо надлежащим образом документировать и составить ведомость соответствия, в которой описать риски, используемые законодательные и нормативные требования, указать выбранные средства обеспечения информационной безопасности и обосновать их выбор. По итогам работы аудитор обязательно оформляет заключение.

5.3.3 Варианты аудита безопасности

Возможны два варианта аудита информационной безопасности: аудит компании в целом и аудит только информационной системы.

В первом случае компания должна подготовить для проверки:

- документы, подтверждающие внедрение в организации выработанной политики информационной безопасности и, в частности, наличие документированного подхода к оцениванию рисков и управлению ими в рамках всей компании;
- описание организационной инфраструктуры информационной безопасности на местах - распределение обязанностей сотрудников по обеспечению безопасности;
- обоснование выбора средств защиты для рассматриваемой системы;

- документацию на процессы обслуживания и администрирования информационной системы;
- документацию с описанием подходов к оцениванию рисков и управлению ими;
- документацию по подготовке периодических проверок, касающихся оценивания рисков, и управлению ими;
- описание процедуры принятия уровня остаточного риска с документированным выводом о реализации необходимых средств обеспечения информационной безопасности, степени их тестирования и корректности работы с ними;
- документацию по системе управления информационной безопасностью и реестр средств управления безопасностью в ведомости соответствия;
- результаты оценивания рисков по информационной системе;
- описание мер для противодействия выявленным рискам.

Все перечисленные проверки выполняются в соответствии с принятыми в компании подходами к оценке рисков и управлению ими.

В случае аудита только информационной системы компания должна подготовить для проверки:

- описание политики информационной безопасности, документацию по системе управления информационной безопасностью и ведомость соответствия, отражающую реальное состояние оцениваемой системы;
- документацию по проведенному оцениванию рисков;
- документацию по средствам управления информационной безопасностью;
- доказательства эффективности принятых контрмер и результаты их тестирования.

Кроме того, при аудите только информационной системы аудитор обязан удостоверить документированность вопросов, рассматриваемых в ходе проведения периодических проверок системы управления информационной безопасностью, а также корректность оценки рисков, выполненных посторонними или рекомендуемыми стандартом методами. Ему надлежит подтвердить, что результаты оценивания рисков достоверны, приемлемы и документированы должным образом. Познакомившись со средствами обеспечения информационной безопасности, аудитор должен убедиться, что необходимые средства обеспечения информационной безопасности были установлены корректно, прошли тестирование и правильно используются, сотрудники знакомы с политикой информационной безопасности, система управления информационной безопасностью должным образом документирована и подготовлена ведомость соответствия. В итоге проводящему аудит сотруднику необходимо стандартным образом оформить заключение.

По результатам успешно выполненного аудита компании или ее информационной системы и подсистемы информационной безопасности выдаются сертификаты на соответствие стандарту BS 7799, которые считаются действительными в течение трех лет.

В процессе аудита подсистемы информационной безопасности компании на соответствие этому стандарту аудиторам приходится анализировать наиболее важные аспекты информационной безопасности с учетом объема подлежащей защите информации, ее специфики и ценности для проверяемой компании. Поскольку подобная деятельность аудитора в настоящее время с большим трудом поддается формальному описанию, требует знаний системного анализа и значительной практики аналогичной работы, опыт и компетентность аудитора являются важными условиями квалифицированного выполнения аудита безопасности корпоративной информационной системы.

По результатам аудита создается список замечаний, выявленных несоответствий требованиям стандарта и рекомендаций по их исправлению. При этом аудиторы должны гарантировать выполнение всех требований процедуры аудита. Поскольку и аудиторам, и

проверяемой компании необходимо знать, насколько серьезны обнаруженные недостатки и каковы способы их исправления, в стандарте рассматриваются следующие категории несоответствия.

Существенное несоответствие: не выполняется одно или несколько базовых требований стандарта либо принимаются неадекватные меры по обеспечению конфиденциальности, целостности или доступности критически важной информации компании, приводящие к недопустимому информационному риску.

Несущественное несоответствие: не соблюдаются некоторые второстепенные требования, что несколько повышает информационные риски компании или снижает эффективность мер обеспечения ее информационной безопасности.

Каждое выявленное несоответствие непременно должно иметь ссылку на требование стандарта BS 7799. При обнаружении в процессе проверки значительного числа несущественных несоответствий аудитор обязан исследовать возможность возникновения серьезного несоответствия. После выявления несоответствий аудитору и представителям компании надлежит наметить пути их устранения. По результатам проверки аудитор может сформулировать в отчетных документах замечание, если он допускает возможность усовершенствования подсистемы информационной безопасности компьютерной информационной системы. Реакция компании на замечания аудитора бывает различной, поскольку компании сами в добровольном порядке определяют свои действия по их устранению. Замечания фиксируются и при последующих проверках. Аудиторам следует выяснить действия компании по устранению недостатков.

Аудитор анализирует представленные компанией ранее описанные документы. В случае повторного аудита компании или ее подсистемы информационной безопасности заполняется ведомость соответствия - документ, составленный аудитором при предыдущей проверке.

5.3.4 Организация проведения аудита

Работы по аудиту безопасности должны начинаться с официального вступительного собрания. На собрании до сведения сотрудников, занимающихся вопросами безопасности, и руководства среднего и верхнего звена (TOP-менеджеров компании) доводится следующее:

- предоставляется план проведения аудита с описанием, что и когда планируется проверять;
- поясняются методы оценки рисков, намеченные для использования в процессе проверки;
- объясняется процедура определения несоответствий, их квалификация и действия по их устранению;
- разъясняются причины, по которым в результате проверки могут быть сделаны замечания, и возможная реакция на них;
- перечисляются руководящие документы аудитора и компании и правила доступа к ним;
- выясняется, какие трудности могут возникнуть в процессе работы (к примеру, отсутствие ведущих специалистов и т.д.);
- обговаривается организация работы с конфиденциальными сведениями компании, необходимыми для выполнения аудита, включая отчет о проведении аудита и замечания о несоответствиях.

Администрация компании должна быть готова к тому, что аудитору потребуется обратиться к потенциально уязвимым участкам компьютерной информационной системы и конфиденциальной информации компании, например к спискам паролей и учетных записей корпоративных пользователей, личным делам сотрудников, результатам проверки лояльности

сотрудников и пр. По завершении аудита проводится заключительное собрание с руководителями верхнего звена, на которое выносится:

- подтверждение заявленных перед проверкой объема проверок и рамок аудита;
- краткое изложение найденных несоответствий и согласованных изменений;
- ознакомление присутствующих с замечаниями и предложениями по их устранению;
- общие замечания по ходу аудита и комментарии к отчету;
- оглашение выводов - положительное заключение, отказ в сертификации или продолжение аудита;
- подтверждение взятых обязательств по сохранению конфиденциальности сведений, полученных в ходе аудита.

Участники вступительного и заключительного собраний должны быть официально зарегистрированы. Главным результатом аудита является официальный отчет, в котором:

- отражена степень соответствия проверяемой компьютерной информационной системы стандарту BS 7799 и собственным требованиям компании в области информационной безопасности согласно плану проведения аудита и ведомости соответствия;
- приведена подробная ссылка на основные документы предприятия, включая политику безопасности, ведомость соответствия, описания процедур обеспечения информационной безопасности, дополнительные обязательные и необязательные стандарты и нормы, применяемые к данной компании;
- представлены общие замечания по выводам проведения аудита;
- указаны количество и категории полученных несоответствий и замечаний;
- обоснована необходимость дополнительных действий по аудиту (если таковая имеется) и составлен их общий план;
- приведен список сотрудников, принимавших участие в тестировании.

Этот отчет является официальным документом проведения аудита. Оригинал отчета должен быть доступен сертифицирующему органу. В документе необходимо определить установленные проверяемой организацией и стандартами BS (ISO/ IEC) аспекты обеспечения безопасности, которые будут рассматриваться при любой проверке. Отчет будет обновляться при каждом аудите.

Отметим, что в случае сертификации компании по стандартам ISO 9001 или ISO 9002 стандарт BS 7799 разрешает совместить сертификацию системы информационной безопасности с сертификацией на соответствие стандартам ISO 9001 или 9002 как на первоначальном этапе, так и при контрольных проверках. Для этого необходимо выполнить условие участия в совмещенной сертификации зарегистрированного аудитора по стандарту BS 7799. При этом в планах совместного тестирования надлежит четко указать процедуры проверки системы информационной безопасности, а сертифицирующие органы обязаны гарантировать тщательность проверки информационной безопасности.

5.4 Аудит информационной системы: рекомендации COBIT 3rd Edition

К настоящему времени аудиторскими компаниями образованы различные государственные и негосударственные ассоциации, объединяющие профессионалов в области аудита информационных систем, которые занимаются созданием и сопровождением, как правило, закрытых и тщательно охраняемых от посторонних глаз стандартов аудиторской деятельности в области информационных технологий (табл. 5.1).

Таблица 5.1. Сравнение некоторых стандартов и концепций аудита информационных технологий

	COBIT	SAC	COSO	SAS 55/78

Целевая аудитория	TOP-менеджеры, пользователи, аудиторы информационных систем	Внутренние аудиторы компании	TOP-менеджеры	Внешние аудиторы
Понятие аудита	Системный процесс проверки на соответствие декларируемым целям политики безопасности, организации обработки данных, норм эксплуатации	Системный процесс проверки на соответствие декларируемым целям бизнес-процессов, политики безопасности и кадровой политики	Системный процесс проверки на соответствие декларируемым целям бизнес-процессов, а также политики безопасности компании	Системный процесс проверки на соответствие декларируемым целям бизнес-процессов, а также политики безопасности компании
Цели аудита	Развитие бизнеса, повышение его эффективности и рентабельности, следование нормативно-правовой базе	Развитие бизнеса, финансовый контроль, следование нормативно-правовой базе	Развитие бизнеса, финансовый контроль, следование нормативно-правовой базе	Развитие бизнеса, финансовый контроль, следование нормативно-правовой базе
Область применения	Планирование и организация, постановка задач и выполнение, эксплуатация и сопровождение, мониторинг	Управление производством, эксплуатация автоматизированных и автоматических систем управления	Управление производством, риск-менеджмент, управление информационными системами, мониторинг корпоративных информационных систем	Управление производством, управление рисками, мониторинг и управление корпоративными информационными системами
Акцент	Менеджмент информационных технологий	Менеджмент информационных технологий	Менеджмент	Финансовый менеджмент
Срок действия сертификата аудита	Интервал времени	Время проверки	Интервал времени	Интервал времени
Заинтересованные лица	TOP-менеджеры компании	TOP-менеджеры компании	TOP-менеджеры компании	TOP-менеджеры компании
Объем документов, регламентирующих проведение аудита	4 документа общим объемом 187 страниц	12 частей общим объемом 1193 страницы	4 тома общим объемом 353 страницы	2 документа общим объемом 63 страницы

Ассоциация аудиторов (Information Systems Audit and Control Association - ISACA), в отличие от других организаций, занимается открытым аудитом информационных систем. Она основана в 1969 г. и в настоящее время объединяет свыше 23 000 членов из более 100 стран, в том числе из России. Ассоциация ISACA координирует деятельность более чем 26 000 аудиторов информационных систем (CICA - Certified Information System Auditor), имеет свою систему стандартов в этой области, ведет исследовательские работы, готовит кадры, проводит конференции.

Ассоциация ISACA под аудитом информационной безопасности в информационной системе понимает процесс сбора сведений, позволяющих установить, обеспечиваются ли безопасность ресурсов компании, необходимые параметры целостности и доступности данных, достигаются ли цели предприятии в части эффективности информационных технологий.

По заявлениям руководящих органов ISACA основная цель ассоциации - исследование, разработка, публикация и продвижение стандартизованного набора документов по управлению

информационной технологией для ежедневного использования администраторами и аудиторами информационных систем. В интересах профессиональных аудиторов, руководителей информационных систем, администраторов и всех заинтересованных лиц ассоциация развивает свою концепцию управления информационными технологиями в соответствии с требованиями информационной безопасности. На основе этой концепции описываются элементы информационной технологии, даются рекомендации по системе управления и обеспечению режима информационной безопасности. Концепция изложена в документе под названием COBIT 3rd Edition - Control Objectives for Information and related Technology (контрольные объекты информационной технологии), который состоит из четырех частей.

Часть 1: Краткое описание концепции (Executive Summary).

Часть 2: Определения и основные понятия (Framework). Помимо требований и основных понятий в этой части сформулированы требования к ним.

Часть 3: Спецификации управляющих процессов и возможный инструментарий (Control Objectives).

Часть 4: Рекомендации по выполнению аудита компьютерных информационных систем (Audit Guidelines).

Третья часть этого документа в некотором смысле аналогична международному стандарту BS ISO/IEC 7799 (BS 7799). Примерно так же подробно изложены практические рекомендации по управлению информационной безопасностью, но модели систем управления в сравниваемых стандартах сильно различаются. Стандарт COBIT - пакет открытых документов, первое издание которого было опубликовано в 1996 г. Он описывает универсальную модель управления информационной технологией, представленную на рис. 5.1 [351].

Основная идея данного стандарта выражается следующим образом: все ресурсы информационной системы должны управляться набором естественно сгруппированных процессов для обеспечения компании необходимой и надежной информацией. В модели COBIT присутствуют ресурсы информационных технологий,

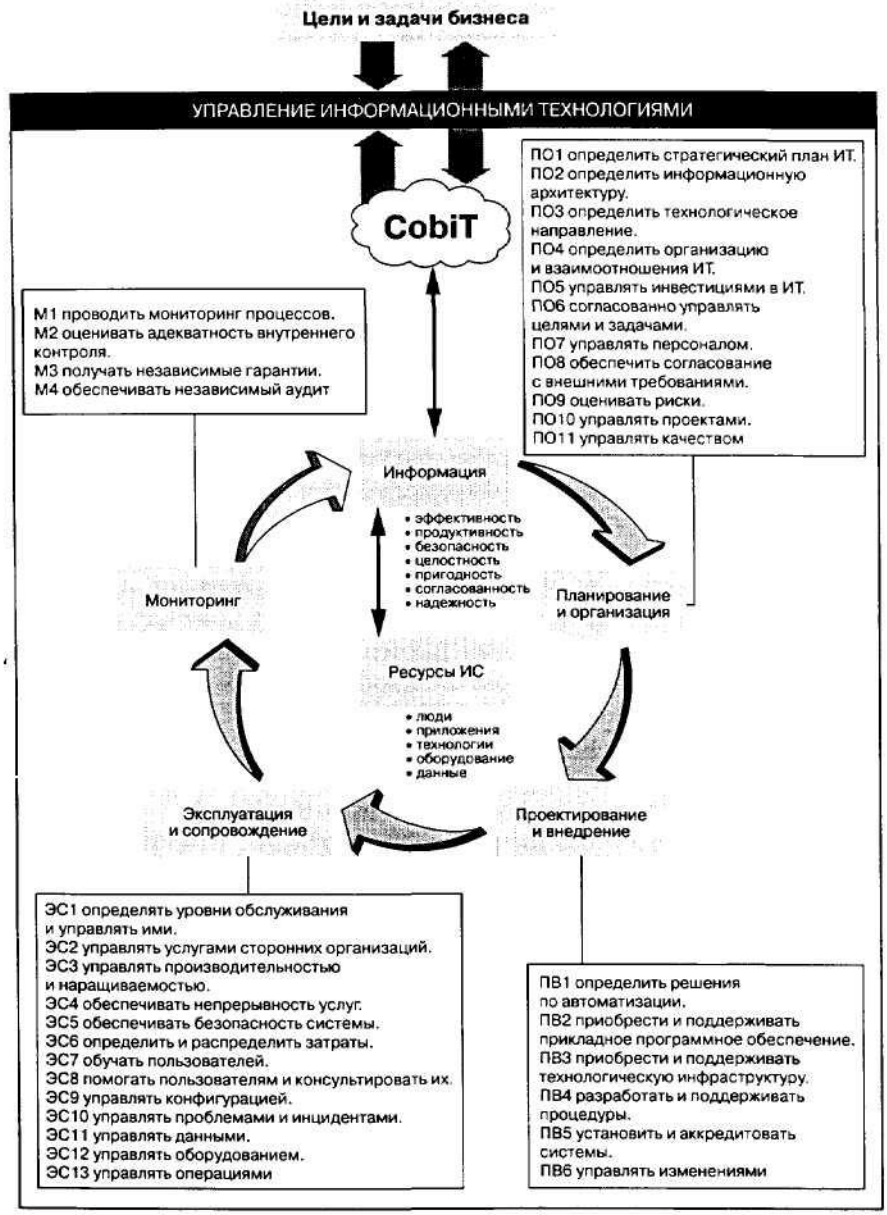


Рис. 5.1. Модель управления информационной технологией

являющиеся источником информации, которая используется в бизнес-процессе. Информационная технология должна удовлетворять требованиям бизнес-процесса. Эти требования сгруппированы следующим образом.

Во-первых, требования к качеству технологии составляют показатели качества и стоимости обработки информации, характеристики ее доставки получателю. Показатели качества подробно описывают возможные негативные аспекты, которые в обобщенном виде входят в понятия целостности и доступности. Кроме того, в эту группу включаются показатели, относящиеся к субъективным аспектам обработки информации, например стиль и удобство интерфейсов. Характеристики доставки информации получателю - это показатели, в обобщенном виде входящие в показатели доступности и частично в показатели конфиденциальности и целостности. Рассмотренная система показателей используется при управлении рисками и оценке эффективности информационной технологии.

Во-вторых, доверие к технологии - группа показателей, описывающих соответствие компьютерной информационной системы принятым стандартам и требованиям, достоверность обрабатываемой в системе информации, ее действенность.

В-третьих, показатели информационной безопасности - конфиденциальность, целостность и доступность обрабатываемой в системе информации.

5.4.1 Этапы проведения аудита

В стандарте COBIT выделены следующие этапы проведения аудита.

На этапе подписания договорной и исходно-разрешительной документации назначаются ответственные лица со стороны предприятия и аудиторской компании, устанавливаются рамки проведения аудита, указываются контролируемые элементы информационной системы, составляется и согласовывается необходимая документация. По результатам предварительного аудита всей информационной системы проводится углубленная проверка подозрительных с позиции проводимого аудита компонентов системы.

Далее следует этап сбора информации с применением стандарта COBIT, который в данном случае регламентирует состав объектов контроля исследуемой системы. Степень детализации описания объектов контроля определяется на этапе разработки исходно-разрешительной документации. При этом стараются добиться оптимального соотношения между временными, стоимостными и прочими затратами на получение исходных данных и их важностью для целей исследования. Диапазон представления исходных данных меняется от бинарных ответов типа ДА/НЕТ до развернутых отчетов. Ассоциация ISACA выдвинула ряд требований к представлению информации при проведении аудита, которые были реализованы в стандарте COBIT. Основное требование к информации - это требование полезности, то есть информация должна быть понятной, уместной (относящейся к делу) и достоверной (надежной), причем понятной для грамотного пользователя, что не исключает рассмотрения сложной информации, если она действительно необходима. Информация уместна, если она влияет на решения пользователей и помогает им оценивать прошлые, настоящие или будущие события или подтверждать и исправлять прошлые оценки. Уместность информации зависит от ее содержания, существенности и своевременности. Информация называется существенной, если ее отсутствие или неправильная оценка могут повлиять на решение пользователя. Иногда полагают, что аналогом уместности информации является полнота освещения операций за отчетный период. Информация достоверна, если она не содержит существенных ошибок или пристрастных оценок и правдиво отражает производственную деятельность. Чтобы быть достоверной, информации надлежит быть правдивой, нейтральной и достаточной для принятия решений.

При анализе учитываются только достоверные исходные данные. Требования к проведению анализа определяются на этапе сбора исходных данных. Стандарт COB1T рекомендует применять описанные в нем методики анализа данных, но при необходимости допускается использование разрешенных ISACA разработок других членов ассоциации. На этапе анализа возможен возврат к этапу сбора информации для получения недостающих исходных данных.

Следующий этап - выработка рекомендаций. Полученные в результате проведенного анализа рекомендации после предварительного согласования с руководством компании следует обязательно проверить на выполнимость и актуальность с учетом рисков внедрения. Стандарт COBIT советует оформлять рекомендации в виде отчета о текущем состоянии информационных систем, технического задания на внесение изменений, отчета о проведенном аудите. Результаты проведения аудита можно разделить на три условные группы: организационные, технические и методологические. Каждая из названных групп связана с улучшением организационного, технического или методологического обеспечения информационной системы.

К организационной группе относятся оценки стратегического планирования, общего управления и инвестиций в информационную систему, рекомендации, способствующие повышению конкурентоспособности компании и уменьшению затрат на обслуживание информационной системы, результаты проверки соответствия информационной системы решаемым бизнес-задачам, мероприятия по снижению стоимости эксплуатации информационной

системы, управление рисками, проектами, выполняемыми в рамках информационных систем, и др. Техническая группа результатов позволяет лучше понять проблемы информационных систем и разработать пути их решения с минимальными затратами, оценить технологические решения, реализовать весь потенциал новых технологий, системно решить вопросы безопасности, осуществить профессиональный прогноз функционирования и необходимости модернизации информационных систем, повысить эффективность функционирования информационной системы, определить уровень обслуживания информационных систем. Методологические результаты дают возможность предоставить апробированные подходы к стратегическому планированию и прогнозированию, оптимизации документооборота, повышению трудовой дисциплины, обучению администраторов и пользователей информационных систем, получению своевременной и объективной информации о текущем состоянии информационной системы компании.

Контроль за выполнением рекомендаций подразумевает постоянное отслеживание аудиторской фирмой выполнения компанией рекомендаций.

Затем следует подписание отчетных актов приемки работы с графиком проведения последующих проверок, разработкой такой дополнительной документации, как долгосрочные и краткосрочные планы развития информационной системы, план восстановления информационной системы в чрезвычайных ситуациях, порядок действий при нарушении защиты, концепция политики безопасности. Постоянное проведение аудита гарантирует работоспособность системы, поэтому составление графика дальнейших проверок является одним из условий выполнения профессионального аудита. На этапе разработки дополнительной документации создаются документы, отсутствие которых (или недочеты в них) могут вызвать сбои в работе информационной системы.

Любая работающая информационная технология в модели COBIT проходит ряд стадий жизненного цикла.

Планирование и организация работы. На этой стадии определяется стратегия и тактика развития информационных технологий в интересах достижения основных целей бизнеса, а затем рассматриваются вопросы реализации: построение архитектуры системы, решение технологических и организационных задач, обеспечение финансирования и т.д. Всего на этой стадии выделяется 11 основных задач.

Приобретение и ввод в действие. Выбранные на этой стадии решения должны быть документально оформлены и спланированы. Выделяется шесть основных задач, решаемых на данной стадии.

Поставка и поддержка. Выделяется 13 основных задач данной стадии, предназначенных поддерживать эксплуатацию информационной технологии.

Мониторинг. За процессами информационной технологии необходимо наблюдать и контролировать соответствие их параметров выдвинутым требованиям. Выделяется четыре основные задачи, решаемые на данной стадии.

Всего в стандарте COBIT выделяется 34 задачи верхнего уровня обработки информации.

Кроме традиционных свойств информации (конфиденциальности, целостности и доступности) в модели дополнительно используются еще четыре свойства -действенность, эффективность, соответствие формальным требованиям и достоверность. Эти свойства не являются независимыми, поскольку частично связаны с первыми тремя. Но их введение объясняется соображениями удобства интерпретации результатов.

В соответствии с решаемыми компанией бизнес-задачами стандарт COBIT предлагает (с учетом заданных критериев оценки и имеющихся в распоряжении ресурсов) описание основных работ по планированию и разработке информационных систем, их комплектации и внедрению, мониторингу, управлению и обслуживанию. В стандарте четыре базовые группы (домена) разбиты на 34 подгруппы, состоящие из 318 объектов контроля, каждый из которых поставляет аудитору достоверную актуальную информацию о текущем состоянии информационной системы.

Системно скоординировав все лучшее в области аудита безопасности информационных систем, стандарт предоставляет аудиторам пакет руководящих документов. Документы стандарта на современном уровне описывают концептуальную последовательность действий аудитора по сбору данных об исследуемых информационных системах и выдаче рекомендаций относительно их совершенствования. Стандарт COBIT базируется на стандартах ISA ISACF и других международных стандартах и таких нормативных документах, как технические стандарты, кодексы, критерии оценки информационных систем, профессиональные стандарты, требования к банковским услугам, системам электронной торговли, производству и т.д. Стандарт написан и проанализирован сотрудниками ведущих консалтинговых компаний, и они работают с ним наряду с другими документами. Несмотря на сравнительно малый объем, стандарт отвечает потребностям практики, сохраняя независимость от конкретных производителей, технологий и платформ. При разработке стандарта была заложена возможность его использования как для проведения аудита информационной системы компании, так и для проектирования информационной системы. В первом случае он позволяет определить степень соответствия исследуемой системы лучшим образцам, а во втором - спроектировать систему, почти идеальную по своим характеристикам.

Стандарт COBIT выгодно отличается от многочисленных аналогичных разработок. К достоинствам стандарта следует отнести его достаточность, сравнительно несложную адаптацию к специфике решаемой задачи, допустимость масштабирования и наращивания возможностей исследуемых информационных систем. Он применим к любым программно-аппаратным решениям без изменения собственной структуры и заложенных в нем принципов. Стандарт характеризуется широким диапазоном решаемых задач - от стратегического планирования до анализа работы отдельных элементов информационной системы путем перекрестного контроля критически важных объектов.

Ассоциация ISACA уделяет большое внимание регламентации различных аспектов деятельности аудитора. Разумная система регламентации в сочетании с высокой квалификацией аудиторов обеспечивает профессиональность аудита информационной безопасности. Основным регламентирующим документом является мандат аудитора. Каждый сертифицированный аудитор CICA имеет мандат на проведение аудита, в котором содержится следующая информация:

- ответственность (Responsibility) и обязанности аудитора - официальное разрешение на проведение работ с указанием целей, рамок деятельности аудитора, объекта, на котором проводится аудит, гарантии независимой проверки аудитором информационной системы, специальных требований к выполнению аудита, критически важных факторов, обеспечивающих успех проводимых работ, и отчетных материалов (показатели работы аудитора);
- полномочия (Authority) аудитора - комплекс мероприятий по оценке оговоренных рисков, право доступа к необходимым для проведения аудита сотрудникам и информации, выбор подлежащих аудиту подсистем компьютерной информационной системы;
- подотчетность (Accountability) аудитора - порядок представления отчета руководству компании, перечень доводимых до персонала основных результатов аудита, процедуры независимой оценки результатов аудита, правила информирования проверяемых о действиях аудитора. Кроме того, процедура аудита должна соответствовать стандартам и предварительному плану, а сам аудитор отвечает за качество проверки, соблюдение сроков и сметной стоимости и может быть подвергнут штрафу.

Современные методы управления информационной безопасностью позволяют решать любые корректно поставленные задачи в области информационной безопасности. Уровень безопасности любой технологии может быть сколь угодно высоким. Однако не исключено, что затраты на поддержание высокого уровня безопасности окажутся чрезвычайно большими. Выбор приемлемого уровня безопасности при допустимых затратах является обязательным условием постановки задачи обеспечения информационной безопасности. Постановка задачи нахождения

компромисса между эффективностью подсистемы безопасности и ее стоимостью предполагает наличие системы показателей эффективности этой подсистемы, методики их измерения, должностных лиц, уполномоченных принимать решение о допустимости определенного уровня остаточного риска, и системы мониторинга для отслеживания текущих параметров подсистемы безопасности. Сложность этой задачи заключается в необходимости найти подобный компромисс.

Умение правильно оценить угрозы ИБ в конкретной ситуации, выбрать систему контрмер, обладающих приемлемым соотношением стоимость-эффективность, является одним из необходимых качеств аудитора.

В ISACA существуют учебные программы, помогающие овладеть необходимыми для этого навыками. В качестве примера рассмотрим интерактивную обучающую программу под названием TAKO, доступную по адресу: http://www.isaca.org/ tako.htm.

5.4.2 Пример аудита системы расчета зарплаты

Корпорация, имеющая около 5000 сотрудников, территориально расположена в центральном офисе и восьми филиалах, находящихся в других городах.

Расчет зарплаты производится в центральном офисе.

Требуется оценить угрозы ИБ и предложить адекватную систему контрмер.

План проведения аудита ИБ предусматривает рассмотрение следующих технологических стадий (рис. 5.2) решения этой задачи:

- учет фактически отработанного сотрудниками времени;
- передача данных для расчета в центральный офис;
- работа с массивом персональных данных, которые требуются при начислении зарплаты;
- расчет зарплаты;
- передача платежных ведомостей в банк;
- формирование отчетов и справок по зарплате;
- работа с управляющей информацией подсистемы (временные зоны, ставки по категориям, фиксированная часть премиальных и т.д.).

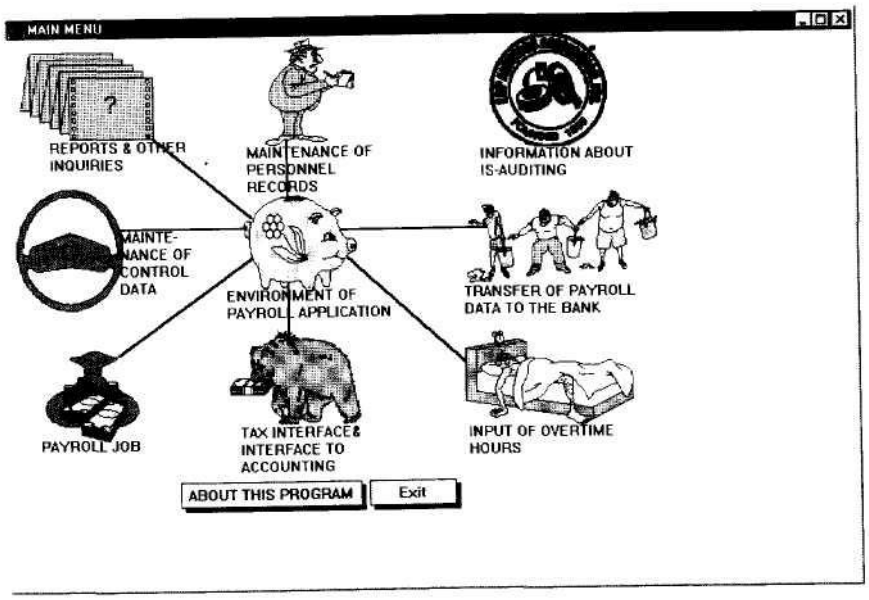


Рис. 5.2. Стадии проведения аудита ИБ подсистемы расчета и выдачи зарплаты

Для каждой стадии составляется список факторов риска, эксперту предлагается выбрать наиболее значимый фактор и ранжировать остальные. Затем рассматриваются возможные контрмеры, характеризуемые стоимостью и эффективностью. Требуется подобрать набор мер с оптимальным (по мнению аудитора) соотношением стоимость-эффективность.

Опишем, например, технологическую стадию - работу с массивом персональных данных, используемых при начислении зарплаты (рис. 5.3).

Рассматривался следующий набор угроз:

- Т1 - данные вводит неавторизованный пользователь (оператор);
- Т2 - данные, нужные для выдачи зарплаты, посылаются в банк с неверными банковскими реквизитами;
- Т3 - оператором вводятся фиктивные данные на несуществующих людей (мошенничества с получением денег за несуществующих сотрудников);

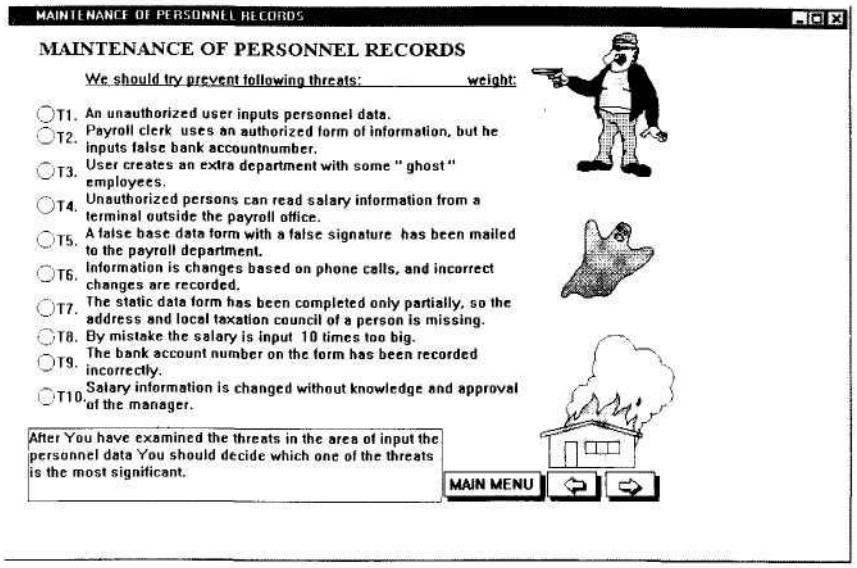


Рис. 5.3. Угрозы безопасности при работе с массивом персональных данных

- Т4 - несанкционированный доступ (для чтения) к платежным документам получает внешний нарушитель;
- Т5 - в бухгалтерию поступают фальсифицированные платежные ведомости;
- Т6 - информация в базе меняется в результате телефонного разговора, данные оказываются некорректными;
- Т7 - частично отсутствуют необходимые для начисления зарплаты данные.
- Т8 - описки в количестве нулей - по ошибке оператора размер зарплаты сотрудника увеличивается в 10 раз;
- Т9 - банковские реквизиты в базе данных некорректны;
- Т10 - информация, на основе которой начисляется зарплата, изменяется без уведомления ответственного за это лица.

Аудитору предлагается выбрать наиболее значимую (вероятную) угрозу. Правильный ответ: ошибки оператора (Т8), остальные угрозы могут быть ранжированы, как показано на рис. 5.4.

Затем выбирается подходящий набор контрмер из следующего списка (рис. 5.5);

- доступ к базе данных по расчету зарплаты разрешен только имеющему к этому отношение персоналу;

– другие пользователи должны одобрить вносимые изменения;
– при внесении изменений обязателен двойной ввод;
– отсутствует возможность изменения данных, касающихся себя самого, любым сотрудником;

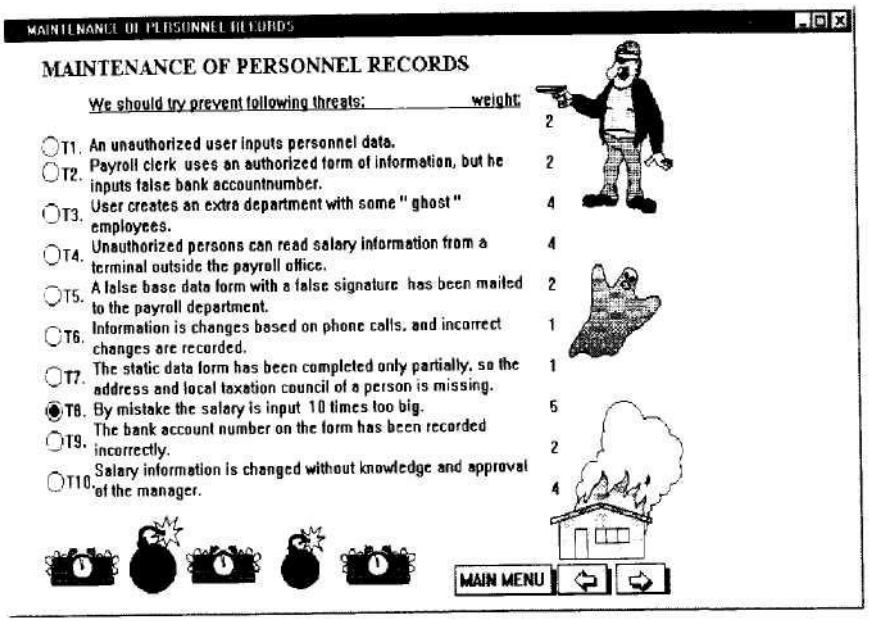


Рис. 5.4. Ранжирование угроз безопасности

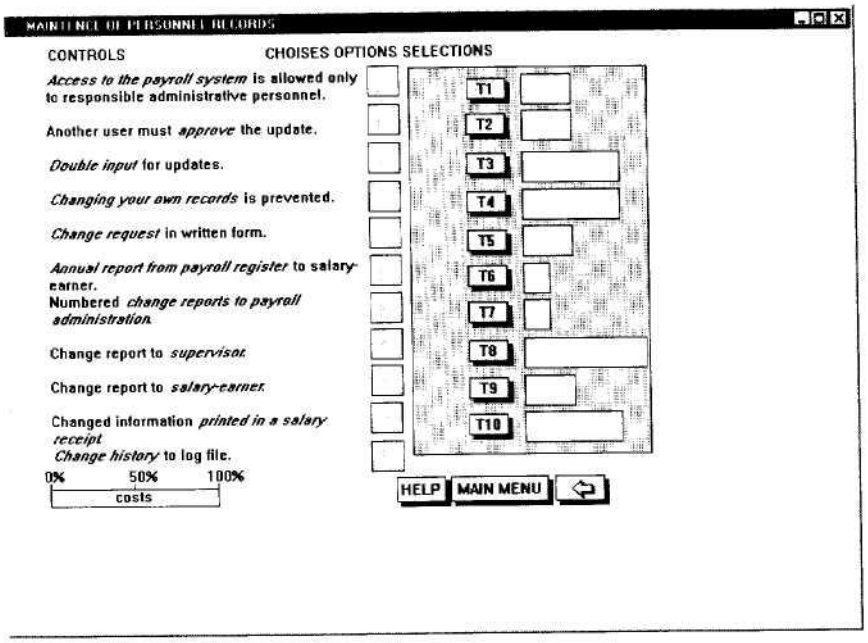


Рис. 5.5. Набор контрмер

– запрос на изменение данных делается в письменном виде;
– составляется ежегодный отчет о выданной зарплате по получателям;
– администратором ведется журнал изменений базы данных бухгалтерии;
– журнал изменений направляется контролеру;
– об изменениях базы данных сообщается получателю зарплаты;

– информация об изменениях вносится в распечатку расчета зарплаты;
– журнал изменений сохраняется в файле.

Каждая из контрмер требует некоторых затрат и уменьшает вероятность реализации нескольких угроз. Аудитор выбирает набор контрмер, обладающий подходящим соотношением стоимость-эффективность.

Например, сравнительно дешевая контрмера - просмотр журнала изменений контролером - является достаточно эффективной: она уменьшает вероятности реализации практически всех угроз (рис. 5.6), а более дорогая контрмера - двойной ввод при внесении изменений - в этом смысле менее эффективна (рис. 5.7).

Подходящий по соотношению стоимость-эффективность набор контрмер может выглядеть, как на рис 5.8. Здесь указан дополнительный эффект применения контрмеры: доступ к базе данных по расчету зарплаты может получить только персонал, имеющий к этому отношение.

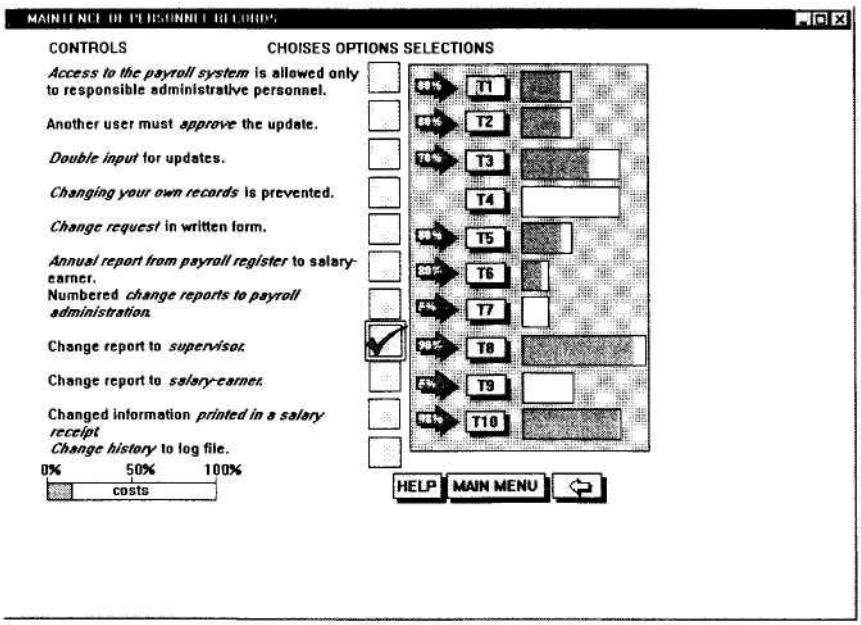


Рис. 5.6. Эффективность просмотра журнала изменений

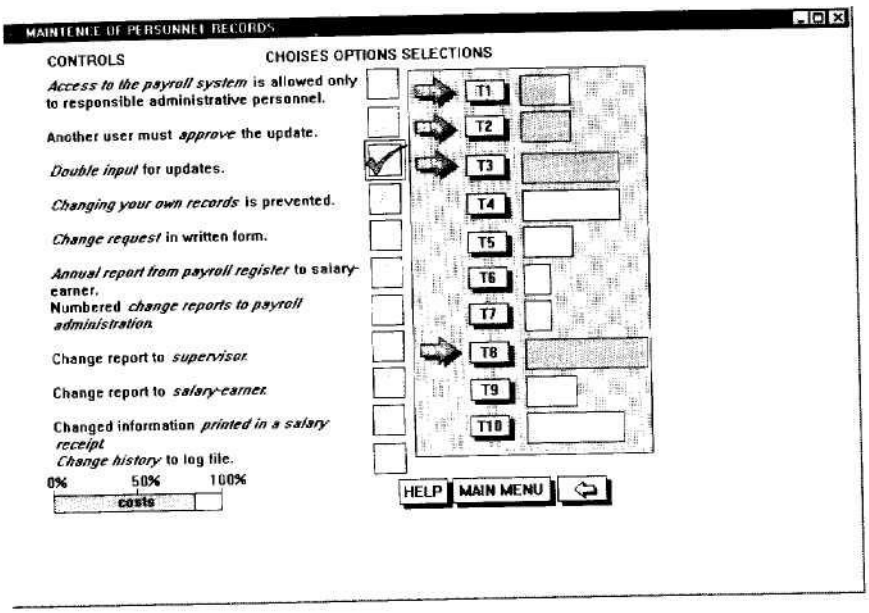


Рис. 5.7. Эффективность дублирования ввода при внесении изменений

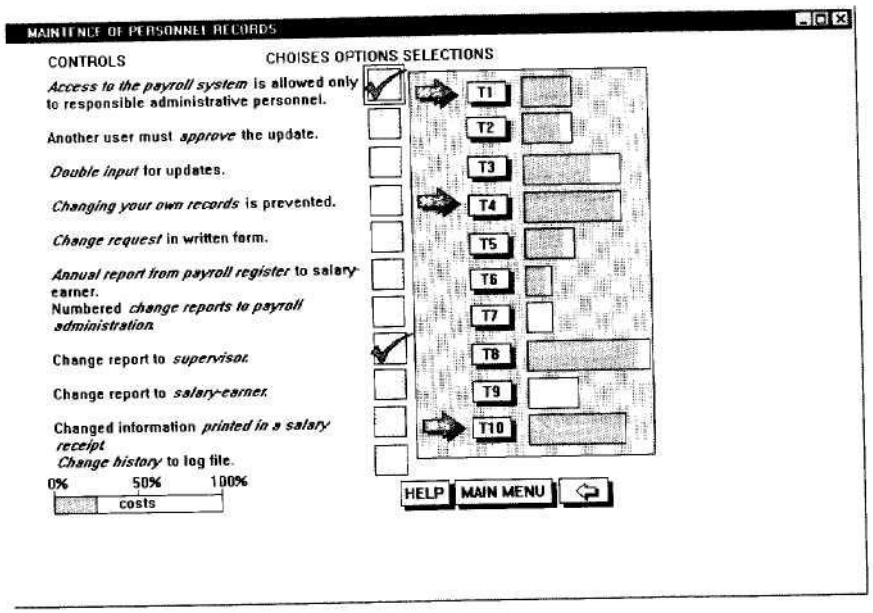


Рис. 5.8. Суммарная эффективность набора контрмер

Глава 6
Анализ защищенности информационной системы

В настоящее время не существует каких-либо стандартизированных методик анализа защищенности автоматизированной системы (АС), поэтому в конкретных ситуациях алгоритмы действий аудиторов могут серьезно различаться. Однако типовую методику анализа защищенности корпоративной сети предложить все-таки можно. И хотя данная методика не претендует на всеобщность, ее эффективность многократно проверена на практике.

Типовая методика включает использование следующих методов:

- изучение исходных данных по АС;
- оценка рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС;
- анализ механизмов безопасности организационного уровня, политики безопасности организации и организационно-распорядительной документации по обеспечению режима информационной безопасности и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности имеющимся рискам;
- анализ конфигурационных файлов маршрутизаторов, межсетевых экранов (МЭ) и proxy-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS-серверов, а также других критических элементов сетевой инфраструктуры;
- сканирование внешних сетевых адресов локальной вычислительной сети (ЛВС) из сети Internet;
- сканирование ресурсов ЛВС изнутри;
- анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.

Перечисленные методы исследования предусматривают проведение как активного, так и пассивного тестирования системы защиты. Активное тестирование системы защиты заключается в эмуляции действий потенциального злоумышленника для преодоления механизмов защиты. Пассивное тестирование предполагает анализ конфигурации ОС и приложений по шаблонам с привлечением списков проверки. Тестирование может выполняться вручную либо посредством специализированных программных средств.

6.1 Исходные данные

В соответствии с требованиями РД Гостехкомиссии при проведении работ по аттестации безопасности АС, включающих предварительное обследование и анализ защищенности объекта информатизации, заказчиком должны быть предоставлены следующие исходные данные:

- полное и точное наименование объекта информатизации и его назначение;
- характер информации (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень ее секретности (конфиденциальности), в соответствии с какими перечнями (государственным, отраслевым, ведомственным, предприятия) он определен;
- организационная структура объекта информатизации;
- перечень помещений, состав комплекса технических средств (основных и вспомогательных), входящих в объект информатизации, в которых (на которых) обрабатывается указанная информация;

- особенности и схема расположения объекта информатизации с указанием границ контролируемой зоны;
- структура программного обеспечения (общесистемного и прикладного), установленного на аттестуемом объекте и предназначенного для обработки защищаемой информации, принятые протоколы обмена информацией;
- общая функциональная схема объекта информатизации, включая схему информационных потоков и режимы обработки защищаемой информации;
- наличие и характер взаимодействия с другими объектами информатизации;
- состав и структура системы защиты информации на аттестуемом объекте;
- перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, внедренных на аттестуемом объекте и имеющих соответствующий сертификат, предписание на эксплуатацию;
- сведения о разработчиках системы защиты информации, наличие у сторонних (по отношению к предприятию, на котором расположен аттестуемый объект) разработчиков лицензий на проведение подобных работ;
- присутствие на объекте (на предприятии, на котором расположен этот объект) службы безопасности информации, службы администратора (автоматизированной системы, сети, баз данных);
- существование и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители);
- наличие и готовность проектной и эксплуатационной документации и другие исходные данные по аттестуемому объекту, определяющие безопасность информации.

Опыт показывает, что перечисленных исходных данных явно недостаточно для анализа защищенности АС, и приведенный в РД Гостехкомиссии список нуждается в расширении и конкретизации. Последний пункт этого списка предполагает предоставление других исходных данных по объекту информатизации, влияющих на безопасность информации. Как раз эти «дополнительные» данные и являются наиболее значимыми для оценки текущего положения дел с обеспечением безопасности АС. Ниже перечислены соответствующие документы.

Дополнительная документация:

- нормативно-распорядительные документы по проведению регламентных работ;
- нормативно-распорядительные документы по обеспечению политики безопасности;
- должностные инструкции для администраторов, инженеров технической поддержки и службы безопасности;
- процедуры и планы предотвращения попыток НСД к информационным ресурсам и реагирования на них;
- схема топологии корпоративной сети с указанием IP-адресов и структурная схема;
- данные по структуре информационных ресурсов с указанием степени критичности или конфиденциальности каждого ресурса;
- размещение информационных ресурсов в корпоративной сети;
- схема организационной структуры пользователей;
- схема организационной структуры обслуживающих подразделений;
- схемы размещения линий передачи данных;
- схемы и характеристики систем электропитания и заземления объектов АС;
- данные об эксплуатируемых системах сетевого управления и мониторинга.

Проектная документация:

- функциональные схемы;
- описание автоматизированных функций;
- описание основных технических решений.

Эксплуатационная документация: руководства для пользователей и администраторов применяемых программных и технических средств защиты информации (СЗИ) в случае необходимости.

6.1.1 Анализ конфигурации средств защиты внешнего периметра ЛВС

При анализе конфигурации средств защиты внешнего периметра ЛВС и управления межсетевыми взаимодействиями особое внимание обращается на следующие аспекты, определяемые их конфигурацией:

- настройка правил разграничения доступа (правил фильтрации сетевых пакетов) на МЭ и маршрутизаторах;
- принятые схемы и настройка параметров аутентификации;
- настройка параметров системы регистрации событий;
- применение механизмов, обеспечивающих сокрытие топологии защищаемой сети и включающих трансляцию сетевых адресов (NAT), и привлечение системы защиты службы доменных имен split DNS;
- настройка механизмов оповещения об атаках и реагирования на них;
- наличие и работоспособность средств контроля целостности;
- версии установленного ПО и наличие пакетов программных коррекций.

6.1.2 Методы тестирования системы защиты

Тестирование системы защиты АС проводится с целью проверки эффективности имеющихся в ней механизмов защиты, их устойчивости в отношении возможных атак, а также с целью поиска уязвимостей в защите. Традиционно используются два основных метода тестирования:

- метод «черного ящика»;
- метод «белого ящика».

Тестирование по методу «черного ящика» предполагает отсутствие у тестирующей стороны каких-либо специальных знаний о конфигурации и внутренней структуре объекта испытаний. При этом против объекта испытаний реализуются все известные типы атак и проверяется устойчивость системы защиты в отношении этих атак. Такие методы тестирования эмулируют действия потенциальных злоумышленников, пытающихся взломать систему защиты. Основным средством тестирования являются сетевые сканеры, располагающие базами данных известных уязвимостей.

Метод «белого ящика» предусматривает составление программы тестирования на основании знаний о структуре и конфигурации объекта испытаний. В ходе тестирования проверяются наличие и работоспособность механизмов безопасности, соответствие состава и конфигурации системы защиты требованиям безопасности и существующим рисками. Выводы о наличии уязвимостей делаются на основании анализа конфигурации внедренных средств защиты и системного ПО, а затем проверяются на практике. Основной инструмент анализа - программные агенты средств анализа защищенности системного уровня, рассматриваемые ниже.

6.2 Средства анализа защищенности

Арсенал программных средств, посредством которых анализируется защищенность АС, достаточно широк. При этом во многих случаях свободно распространяемые программные продукты ничем не уступают коммерческим. Достаточно сравнить некоммерческий сканер NESSUS с его коммерческими аналогами.

Удобным и мощным средством анализа защищенности ОС является описанный далее, свободно распространяемый программный продукт CIS Windows 2000 Level 1 Scoring Tool, а также аналогичные средства разработчиков ОС, предоставляемые бесплатно, такие как ASET для ОС Solaris или MBSA (Microsoft Security Baseline Analyzer) для ОС Windows 2000.

Один из методов автоматизации процессов анализа и контроля защищенности распределенных компьютерных систем состоит в использовании технологии интеллектуальных программных агентов. Система защиты строится на архитектуре консоль/менеджер/агент. На каждую из контролируемых систем устанавливается программный агент, который выполняет соответствующие настройки ПО и проверяет их правильность, контролирует целостность файлов, своевременность установки пакетов программных коррекций, а также выполняет другие полезные задачи контроля защищенности АС. (Управление агентами реализуется по сети программой-менеджером.) Менеджеры являются центральными компонентами подобных систем. Они посылают управляющие команды всем агентам контролируемого ими домена и сохраняют все данные, полученные от агентов в центральной базе данных. Администратор управляет менеджерами при помощи графической консоли, позволяющей выбирать, настраивать и создавать политики безопасности, анализировать изменения состояния системы, ранжировать уязвимости и т.п. Все взаимодействия между агентами, менеджерами и управляющей консолью осуществляются по защищенному клиент-серверному протоколу. Такой подход был применен при построении комплексной системы управления безопасностью организации Symantec ESM.

Другим широко распространенным методом анализа защищенности является активное тестирование механизмов защиты путем эмуляции действий злоумышленника, предпринимающего попытки сетевого вторжения в АС. Для этих целей служат сетевые сканеры, эмулирующие действия потенциальных нарушителей. В основе работы сетевых сканеров лежит база данных, содержащая описание известных уязвимостей ОС, МЭ, маршрутизаторов и сетевых сервисов, а также алгоритмов попыток вторжения (сценариев атак). Рассматриваемые далее сетевые сканеры Nessus и Symantec NetRecon достойно представляют данный класс программных средств анализа защищенности. Таким образом, эти программные средства условно можно разделить на два класса. Первый класс, к которому принадлежат сетевые сканеры, иногда называют средствами анализа защищенности сетевого уровня. Второй класс, к которому относятся все остальные рассмотренные здесь средства, иногда называют средствами анализа защищенности системного уровня. Данные классы средств имеют свои достоинства и недостатки, а на практике взаимно дополняют друг друга.

Для функционирования сетевого сканера необходим только один компьютер, имеющий сетевой доступ к анализируемым системам, поэтому в отличие от продуктов, построенных на технологии программных агентов, нет необходимости устанавливать в каждой анализируемой системе своего (для каждой ОС) агента.

К недостаткам сетевых сканеров можно отнести большие временные затраты, необходимые для сканирования всех сетевых компьютеров из одной системы, и создание большой нагрузки на сеть. Кроме того, в общем случае трудно отличить сеанс сканирования от действительных попыток атак. Сетевыми сканерами также с успехом пользуются злоумышленники.

Системы анализа защищенности, построенные на интеллектуальных программных агентах, - потенциально более мощные средства, чем сетевые сканеры. Однако, несмотря на все их достоинства, обращение к программным агентам не может заменить сетевого сканирования, так что эти средства лучше применять совместно. Кроме того, сканеры представляют собой более

простое, доступное, дешевое и во многих случаях более эффективное средство анализа защищенности.

6.2.1 Спецификации Security Benchmarks

Уровень защищенности компьютерных систем от угроз безопасности зависит от многих факторов. При этом одним из определяющих факторов является адекватность конфигурации системного и прикладного ПО, средств защиты информации и активного сетевого оборудования существующим рискам. Перечисленные компоненты АС имеют сотни параметров, значения которых влияют на защищенность системы, что делает их анализ трудновыполнимой задачей. Поэтому в современных АС для анализа конфигурационных параметров системного и прикладного ПО, технических средств и средств защиты информации обычно используются специализированные программные средства.

Анализ параметров защиты осуществляется по шаблонам, содержащим списки параметров и их значений, которые должны быть установлены для обеспечения необходимого уровня защищенности. Различные шаблоны задают конфигурации для разных программно-технических средств.

Относительно коммерческих корпоративных сетей, подключенных к сети Internet, можно говорить о базовом уровне защищенности, который в большинстве случаев допустимо признать достаточным. Спецификации (шаблоны) для конфигурации наиболее распространенных системных программных средств, позволяющих поддерживать базовый уровень защищенности, в настоящее время разрабатываются представителями международного сообщества в лице организаций и частных лиц, профессионально занимающихся вопросами ИБ и аудита АС, под эгидой международной организации, которая называется Центр безопасности Интернет (Center of Internet Security). На данный момент закончены либо находятся в процессе подготовки следующие спецификации (Security Benchmarks):

- Solaris (Level-1);
- Windows 2000 (Level-1);
- CISCO IOS Router (Level-l/Level-2);
- Linux (Level-1);
- HP-UX (Level-1);
- AIX (Level-1);
- Check Point FW-l/VPN-1 (Level-2);
- Apache Web Server (Level-2);
- Windows NT (Level-1);
- Windows 2000 Bastion Host (Level-2);
- Windows 2000 Workstation (Level-2);
- Windows IIS5 Web Server (Level-2).

В приведенном списке спецификации первого уровня (Level-1) соответствуют базовому (минимальному) уровню защиты, требуемому для большинства систем с подключениями к Internet. Спецификации второго уровня (Level-2) соответствуют продвинутому уровню защиты, необходимому для систем, в которых предъявляются повышенные требования по безопасности.

Перечисленные спецификации являются результатом обобщения мирового опыта в области информационной безопасности.

Для анализа конфигурации компонентов АС на соответствие этим спецификациям предназначены специализированные тестовые программные средства (CIS-certified scoring tools).

В качестве примера рассмотрим спецификацию базового уровня защиты ОС MS Windows 2000 и соответствующий программный инструментарий для анализа конфигурации ОС.

6.2.2 Спецификация Windows 2000 Security Benchmark

CIS Windows 2000 Security Benchmark - это программа для проверки соответствия настроек ОС MS Windows 2000 минимальному набору требований безопасности, определяющих базовый уровень защищенности, который в общем случае является достаточным для коммерческих систем. Требования к базовому уровню защищенности ОС Windows 2000 были выработаны в результате обобщения практического опыта (рис. 6.1). Свой вклад в разработку этих спецификаций внесли такие организации, как SANS Institute, Center for Internet Security, US NSA и US DoD.

В состав инструментария CIS Windows 2000 Security Benchmark входит шаблон политики безопасности (cis.inf), позволяющий сравнивать текущие настройки ОС с эталонными и автоматически переконфигурировать ОС для обеспечения соответствия базовому уровню защищенности, задаваемому данным шаблоном.

CIS Windows 2000 Security Benchmark дает возможность количественно оценивать текущий уровень защищенности анализируемой ОС по 10-балльной шкале. Уровень 0 соответствует минимальному уровню защищенности (после установки ОС ее уровень защищенности как раз будет равен 0). Уровень 10 является максимальным и означает полное соответствие анализируемой системы требованиям базового уровня защищенности для коммерческих систем.

Все проверки, выполняемые при анализе системы, делятся на три категории:

- Service Packs and Hotfixes (пакеты обновлений и программные коррекции);
- Account and Audit Policies (политика управления пользовательскими бюджетами и политика аудита безопасности);
- Security Options (опции безопасности).

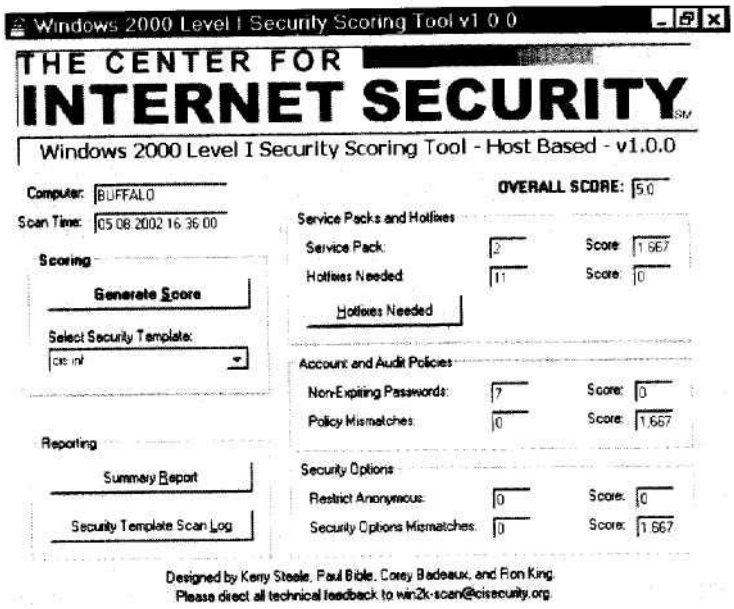


Рис. 6.1. Windows 2000 Level 1 Security Scoring Too!

Первая категория включает проверку установки последних пакетов обновлений (Service Packs) и текущих программных коррекций (Hotfixes) от Microsoft.

Вторая категория включает проверки параметров политики безопасности по управлению пользовательскими бюджетами (включая политику управления паролями) и осуществлению аудита безопасности.

Третья категория включает проверки всех остальных параметров безопасности ОС, не относящиеся к первым двум категориям, в том числе запрет анонимных сессий (NULL sessions), правила выделения внешних устройств, параметры защиты протокола TCP/IP, установки прав доступа к системным объектам и т.п.

Для проверки наличия установленных текущих программных коррекций используется утилита MS Network Security Hotfix Checker (HFNetCheck), которая автоматически скачивается с сайта Microsoft и устанавливается во время осуществления проверок. Подробную информацию об этой утилите можно получить по адресу: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/ hfnetchk.asp.

Используя список недостающих программных коррекций (Hotfixes), сгенерированный утилитой HFNetCheck, следует осуществить поиск и установку этих коррекций. Для этого используется Microsoft Security Bulletin Search (http:// www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Default.asp),

Для осуществления мониторинга установки необходимых программных коррекций, помимо утилит Microsoft, можно использовать более мощные средства

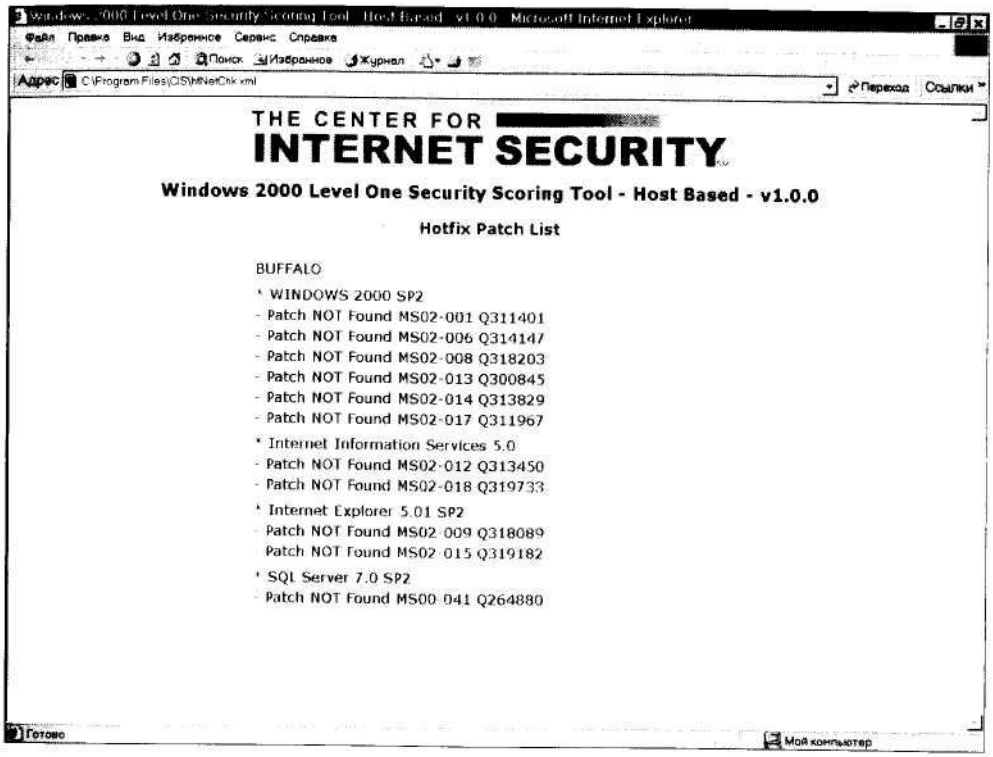


РИС. 6.2. Список недостающих программных коррекций

третьих фирм, например программу UpdateExpert, разработки St. Bernard Software (www.stbernard.comV

Для настройки ОС с использованием шаблона CIS.INF служит Security Configuration and Analysis Snap-In - стандартное средство ОС Windows 2000 для анализа и установки параметров безопасности ОС.

Порядок подключения данного средства к MMC (Microsoft Management Console), загрузки шаблона, его использования для анализа и изменения конфигурации ОС описывается в руководстве «CIS Win2K Level 1 Implementation Guide», входящем в комплект программной

документации, которая содержит также подробное описание всех производимых проверок и соответствующих параметров настройки ОС.

6.3 Возможности сетевых сканеров

Основным фактором, определяющим защищенность АС от угроз безопасности, является наличие в АС уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов АС, так и другими причинами, к числу которых относятся ошибки и программные закладки в коде ПО, отсутствие механизмов безопасности, их неправильное использование либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты АС в конечном счете приводит к успешному осуществлению атак, использующих эти уязвимости.

Сетевые сканеры являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемого локально с использованием списков проверки. Сканер является необходимым инструментом в арсенале любого администратора либо аудитора безопасности АС.

Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х годов прошлого века и не потерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP-порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования.

Современный сетевой сканер выполняет четыре основные задачи:

- идентификацию доступных сетевых ресурсов;
- идентификацию доступных сетевых сервисов;
- идентификацию имеющихся уязвимостей сетевых сервисов;
- выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему доступные сетевые сервисы.

Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и т.п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для реализации удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

В настоящее время существует большое количество коммерческих и свободно распространяемых сканеров, как универсальных, так и специализированных, предназначенных для выявления только определенного класса уязвимостей. Многие из них можно найти в Internet. Число уязвимостей в базах данных современных сканеров медленно, но уверенно приближается к 1000.

Одним из наиболее «продвинутых» коммерческих продуктов этого класса является сетевой сканер NetRecon компании Symantec, база данных которого содержит около 800 уязвимостей систем UNIX, Windows и NetWare и постоянно обновляется через Web. Рассмотрение его свойств позволит составить представление о всех продуктах этого класса.

6.3.1 Сканер Symantec NetRecon

Сетевой сканер NetRecon является инструментом администратора безопасности, предназначенным для исследования структуры сетей и сетевых сервисов и анализа защищенности сетевых сред. NetRecon позволяет осуществлять поиск уязвимостей в сетевых сервисах, ОС, МЭ, маршрутизаторах и других сетевых компонентах. Например, NetRecon помогает находить уязвимости в таких сетевых сервисах, как ftp, telnet, DNS, электронная почта, Web-сервер и др. При этом проверяются версии и конфигурации сервисов, их защищенность от сетевых угроз и устойчивость к попыткам проникновения. Для поиска уязвимостей используются как стандартные средства тестирования и сбора информации о конфигурации

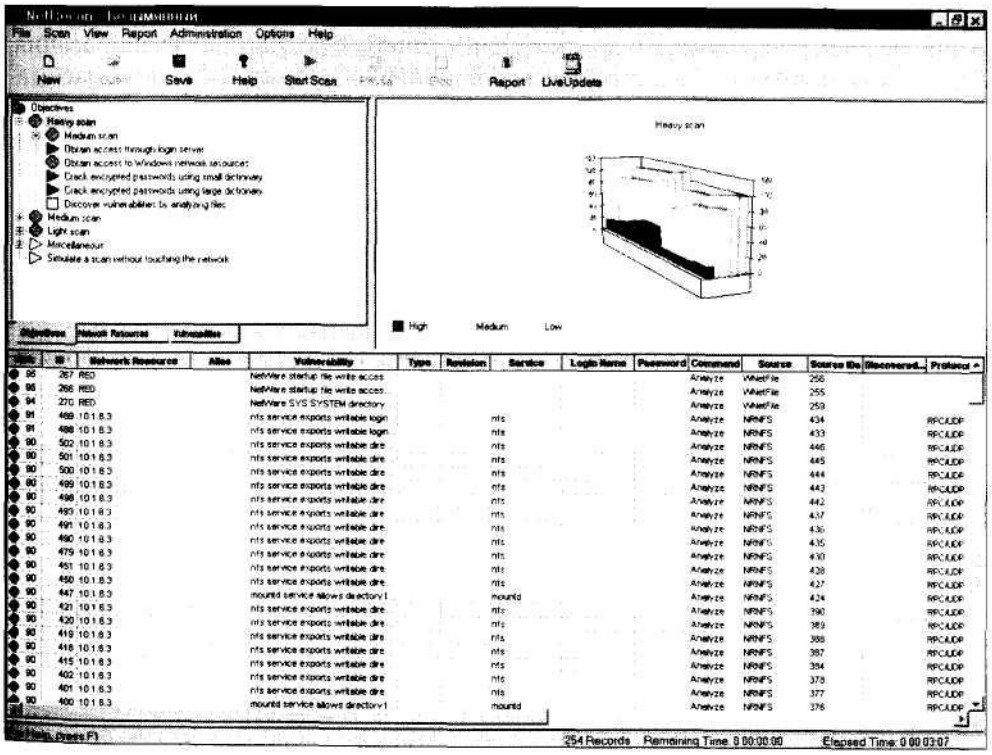


Рис. 6.3. Сетевой сканер NetRecon

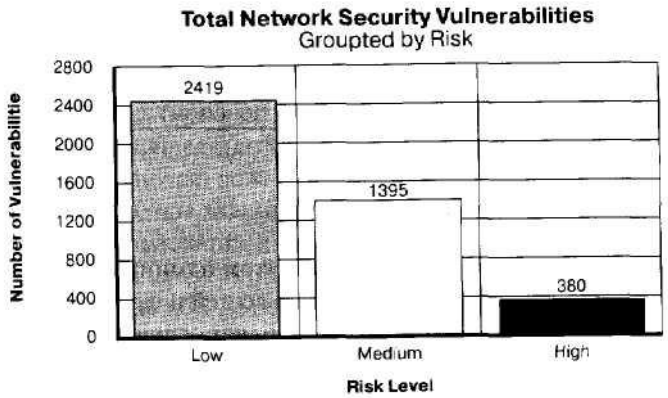


Рис. 6.4. Суммарное количество уязвимостей, обнаруженных сканером NetRecon

и функционировании сети, так и специальные средства, которые реализуют алгоритмы, эмулирующие действия злоумышленника по осуществлению сетевых атак.

Программа работает в среде ОС Windows и имеет удобный графический интерфейс, позволяющий определять параметры сканирования, наблюдать за ходом сканирования, генерировать и просматривать отчеты о результатах сканирования. Результаты отображаются в графической и табличной форме в реальном масштабе времени.

Создаваемые NetRecon отчеты содержат подробную информацию о найденных уязвимостях, включая слабость паролей пользователей, подверженность определенных сервисов угрозам отказа в обслуживании, уязвимые для сетевых атак конфигурации ОС и др. Наряду с сообщениями о найденных уязвимостях и их описаниями приводятся рекомендации по их устранению. Отчет о результатах сканирования позволяет наметить план мероприятий по устранению выявленных недостатков.

Для генерации отчетов в NetRecon используется ПО Crystal Report, предоставляющее удобные средства для просмотра отчетов и их экспорта во все популярные форматы представления данных. Найденные уязвимости ранжируются, при этом каждой из них присваивается числовой рейтинг, что позволяет отсортировать их по степени критичности для облегчения последующего анализа результатов сканирования.

Пример описания уязвимости в отчете, сгенерированном сканером NetRecon, приведен на рис. 6.5. В NetRecon используется следующий формат описания уязвимости (который, однако, является общим для всех остальных сетевых сканеров):

- Vulnerability Name (название уязвимости);
- Risk (уровень риска);
- Description (описание уязвимости);
- Solution (способы ликвидации уязвимости);
- Additional Information (дополнительная информация);
- Links (ссылки на источники информации о данной уязвимости);
- of Network Resources (количество сетевых ресурсов, подверженных данной уязвимости);
- • Network Resource (список сетевых ресурсов).

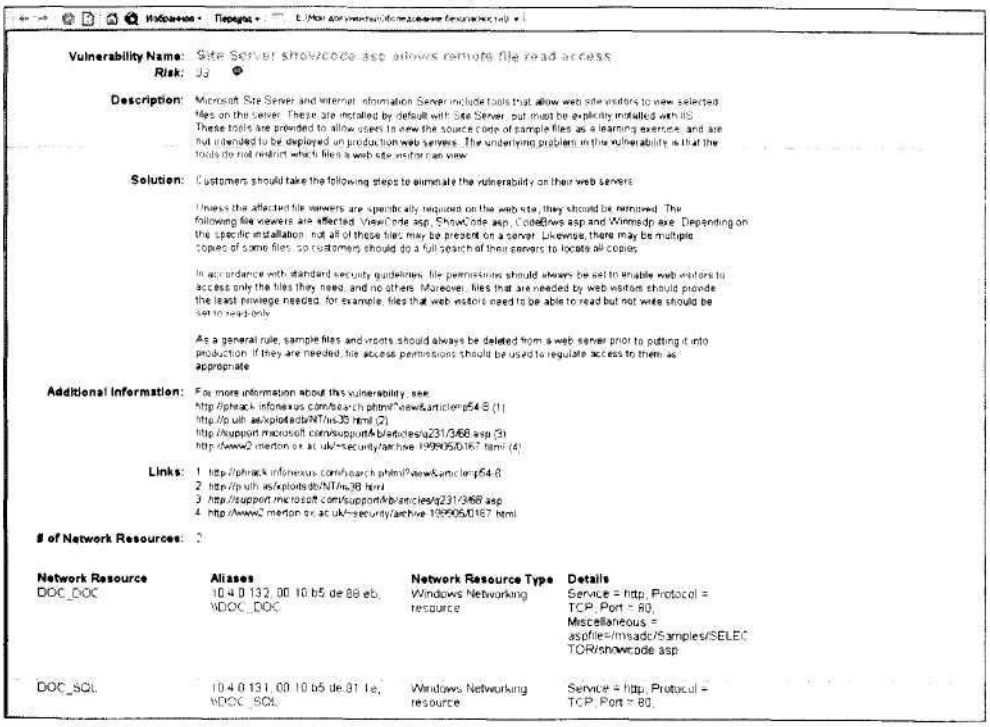


Рис. 6.5. Описание уязвимости в отчете, сгенерированном сканером NetRecon

NetRecon самостоятельно определяет конфигурацию сети и позволяет выбрать сетевые ресурсы для сканирования. Может осуществляться параллельное сканирование всех сетевых ресурсов, сканирование по диапазону сетевых адресов, сканирование отдельных систем или подсетей. Сеанс сканирования может включать все виды проверок либо отдельные проверки по выбору пользователя. Глубина сканирования определяется продолжительностью сеанса сканирования, которая задается пользователем. Например, проверки, связанные с подбором пользовательских паролей по словарю, сопряжены с существенными временными затратами и не могут быть завершены в течение короткого сеанса сканирования.

Для поиска сетевых уязвимостей в NetRecon используется запатентованная технология UltraScan. Производимые NetRecon проверки тесно взаимосвязаны, и результаты одной проверки используются для выполнения другой. Как и в случае реальных атак, в технологии UltraScan информация об обнаруженных уязвимостях нужна для выявления других связанных с ними уязвимостей. Например, если

NetRecon удалось получить доступ к файлу, содержащему пароли пользователей, и расшифровать несколько паролей, то эти пароли будут применены для имитации атак на другие системы, входящие в состав сети.

NetRecon дает возможность пользователю отслеживать путь поиска уязвимости, представляющий собой последовательность проверок, производимых NetRecon, которая привела к выявлению данной уязвимости. Путь поиска уязвимости позволяет проследить действия возможного нарушителя, осуществляющего атаку на сетевые ресурсы.

Используемая NetRecon база данных содержит описание известных уязвимостей и сценариев атак. Она регулярно пополняется новыми данными. Обновление этой базы данных производится через Web-узел компании Symantec автоматически, при помощи механизма LiveUpdate.

6.3.2 Сканер NESSUS

Сетевой сканер Nessus может рассматриваться в качестве достойной альтернативы коммерческим сканерам. Nessus является свободно распространяемым и постоянно обновляемым программным продуктом. Удобный графический интерфейс позволяет определять параметры сеанса сканирования, наблюдать за ходом сканирования, создавать и просматривать отчеты.

По своим функциональным возможностям сканер Nessus находится в одном ряду, а по некоторым параметрам превосходит такие широко известные коммерческие сканеры, как NetRecon компании Symantec, Internet Scanner компании ISS и CyberCop Scanner компании NAI.

Версия 0.99 серверной части сканера Nessus была сертифицирована в Гостехкомиссии России (сертификат № 361 от 18 сентября 2000 г.).

Сценарии атак реализованы в NESSUS в качестве подключаемых модулей (plugins). Количество подключаемых модулей постоянно увеличивается, в настоящее время насчитывается более 700. Новые внешние модули, эмулирующие атаки, можно инсталлировать, скопировав файлы, содержащие их исходные тексты, с Web-сервера разработчиков (www.nessus.org).

Nessus предоставляет очень широкие возможности по поиску уязвимостей корпоративных сетей и исследованию структуры сетевых сервисов. Помимо использования стандартных способов сканирования портов TCP и UDP, Nessus позволяет осуществлять поиск уязвимостей в реализациях протоколов управления сетью ICMP и SNMP. Кроме того, поддерживаются различные стелс-режимы сканирования, реализуемые популярным некоммерческим стелс-сканером nmap, который можно рассматривать в качестве одного из компонентов сканера Nessus. Другой популярный некоммерческий сканер queso используется в составе Nessus для определения типа и номера версии сканируемой ОС.

Высокая скорость сканирования достигается за счет использования при реализации сканера Nessus многопотоковой архитектуры программирования, позволяющей осуществлять одновременное параллельное сканирование сетевых хостов.

Для сканирования каждого хоста сервером nessusd создается отдельный поток выполнения.

Подробное описание используемых методов сканирования портов TCP/UDP можно найти в документации на сканер nmap. К ним относятся:

- TCP connect scan;
- TCP SYN scan;
- TCP FIN scan;
- TCP Xmas Tree scan;
- TCP Null scan;
- UDP scan.

При реализации Nessus использована нетипичная для сетевых сканеров клиент-серверная архитектура. Взаимодействие между клиентом и сервером осуществляется по защищенному клиент-серверному протоколу, предусматривающему использование надежной схемы аутентификации и шифрование передаваемых данных. Сервер nessusd работает только в среде UNIX и предназначен для выполнения сценариев сканирования. Механизмы собственной безопасности, реализованные в сервере nessusd, позволяют осуществлять аутентификацию пользователей сканера, ограничивать полномочия пользователей по выполнению сканирования и регистрировать все действия пользователей в журнале регистрации событий на сервере.

Клиентская часть Nessus работает в среде UNIX и Windows и реализует графический интерфейс пользователя для управления сервером nessusd. Пользователь сканера перед запуском сеанса сканирования определяет параметры сканирования, указывая диапазон сканируемых IP-адресов и TCP/UDP-портов, максимальное количество потоков сканирования (число одновременно сканируемых хостов), методы и сценарии сканирования (plugins), которые будут использоваться.

Все сценарии сканирования разделены на группы по типам реализуемых ими сетевых атак (рис. 6.6), обнаруживаемых уязвимостей, а также по видам тестируемых сетевых сервисов. Так, имеются специальные группы сценариев:

- Backdoors - для обнаружения «троянских» программ;
- Gain Shell Remotely - для реализации атак на получение пользовательских полномочий на удаленной UNIX-системе;
- Firewalls - для тестирования МЭ;
- FTP - для тестирования FTP-серверов;
- Windows - для поиска уязвимостей Windows-систем и т.п.

Особую группу сценариев сканирования составляют атаки «отказ в обслуживании» (Denail of Service - DoS). Единственный способ убедиться в том, что сканируемая система подвержена той или иной DoS, - выполнить эту атаку и посмотреть на реакцию системы. Данная группа сценариев, однако, является потенциально опасной, так как их запуск может привести к непредсказуемым последствиям для сканируемой сети, включая сбои в работе серверов и рабочих станций, потерю данных

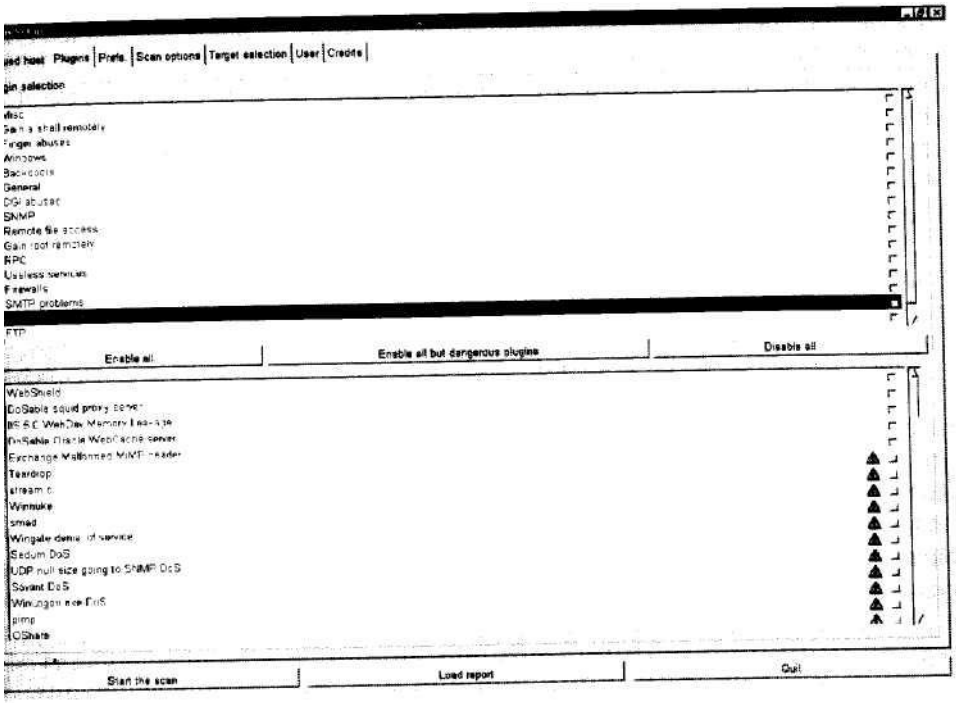


Рис. 6.6. Выбор сценариев сканирования в сканере Nessus

и «полный паралич» корпоративной сети. Поэтому большинство DoS в данной группе по умолчанию отключено (рис. 6.6).

Для написания сценариев атак служит специализированный С-подобный язык программирования высокого уровня NASL (Nessus Attack Scripting Language). Существует также интерфейс прикладного программирования (API) для разработки подключаемых модулей со сценариями атак на языке С, однако предпочтительнее использовать NASL.

NASL является интерпретируемым языком программирования, что обеспечиваег его независимость от платформы. Он предоставляет мощные средства для реализации любых сценариев сетевого взаимодействия, требующих формирования IP-пакетов произвольного вида.

Результаты работы сканера Nessus представлены на рис. 6.7. Данные об обнаруженных уязвимостях отсортированы по IP-адресам просканированных хостов. Найденные уязвимости проранжированы. Наиболее критичные (security holes) выделены красным цветом, менее критичные (security warning) - желтым. По каждой уязвимости приводится ее описание, оценка ассоциированного с ней риска Risk Factor) и рекомендации по ее ликвидации (Solution).

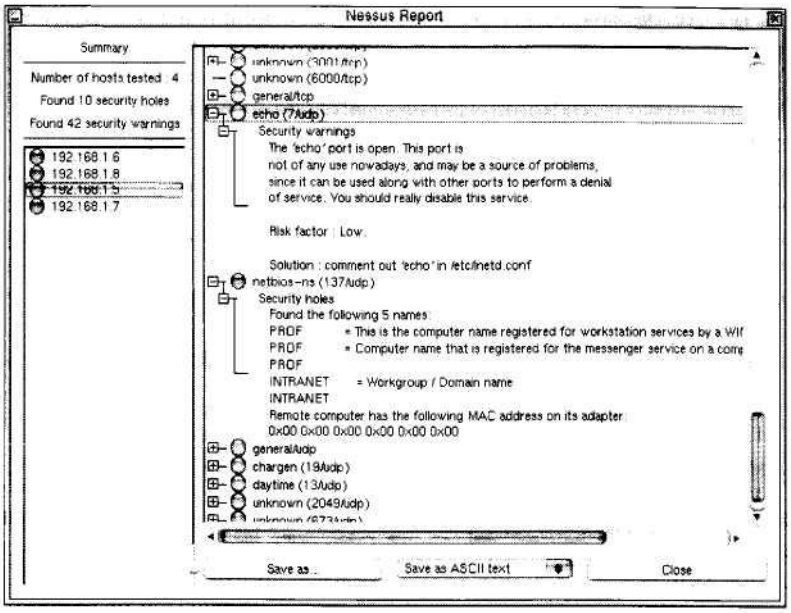


Рис. 6.7. Результаты сканирования в сканере Nessus

6.4 Средства контроля защищенности системного уровня

Обеспечение безопасности компьютерных систем, по существу, заключается в определении множества возможных угроз, оценке величины связанных с ними рисков, выборе адекватных контрмер, реализации этих контрмер процедурными и программно-техническими средствами и контроле их осуществления. Последний вопрос является, пожалуй, одним из наиболее сложных. Реализация программно-технических мер защиты требует настроек большого количества параметров ОС, МЭ, СУБД, сетевых сервисов, прикладных программ и активного сетевого оборудования. Когда речь идет о защите отдельного сервера или рабочей станции, то задача хоть и является сложной, но ее решение вполне по силам опытному системному администратору. В этом случае для контроля значений параметров программ, связанных с безопасностью, используются специальные списки проверки. Когда же речь заходит о настройке десятков и сотен сетевых устройств, функционирующих на различных программно-аппаратных платформах, в соответствии с единой политикой безопасности, контроле параметров защиты и мониторинге безопасности в реальном масштабе времени, то без специальных средств автоматизации уже не обойтись. Производители ОС предоставляют специальный инструментарий для контроля целостности и анализа защищенности ОС (утилита C2 Configuration в Windows NT Resource Kit, утилита ASET в ОС Solaris и т.п.). Имеется немало свободно распространяемых и широко используемых продуктов, предназначенных для решения подобных задач, таких как программа COPS для ОС UNIX. Однако эти средства, функционирующие на системном уровне, позволяют обеспечить только некоторый базовый уровень защищенности самой ОС. Для контроля приложений, сетевых сервисов, активного сетевого оборудования в распределенных системах, функционирующих в динамичной агрессивной среде, необходимо использовать специализированный инструментарий, поддерживающий распределенные архитектуры, централизованное управление, различные программно-аппаратные платформы, различные виды приложений, реализующий изощренные алгоритмы поиска и устранения уязвимостей, интегрированный с другими средствами защиты и удовлетворяющий многим требованиями, предъявляемым к современным продуктам этого класса.

6.4.1 Система Symantec Enterprise Security Manager

Мощным средством анализа защищенности системного уровня, выполняющим проверки конфигурационных параметров ОС и приложений «изнутри», является автоматизированная система управления безопасностью предприятия ESM компании Symantec. Программные агенты ESM устанавливаются на каждом контролируемом компьютере сети, выполняя проверки параметров ПО, связанных с безопасностью, и корректируя их по мере необходимости. Программные агенты обычно способны выполнять более сложные проверки и анализировать параметры ПО, недоступные сетевым сканерам, так как они действуют изнутри. Анализ защищенности, выполняемый программными агентами, может планироваться по времени и выполняться одновременно на всех контролируемых компьютерах. Кроме того, в отличие от сетевых сканеров, программные агенты не оказывают большого влияния на пропускную способность сети и осуществляют шифрование результатов проверок при передаче данных по сети.

Архитектура ESM

Система ESM построена на архитектуре консоль/менеджер/агент. Она состоит из трех типов компонентов, которые могут быть распределены по сети произвольным образом, - административной консоли (ESM Console), менеджеров (ESM Manager) и агентов (ESM Agent) - см. рис. 6.8.

Консоль ESM

Административная консоль представляет собой графический пользовательский интерфейс для управления менеджерами и функционирует в среде Windows NT. Для управления менеджерами может также использоваться интерфейс командной строки (CLI).

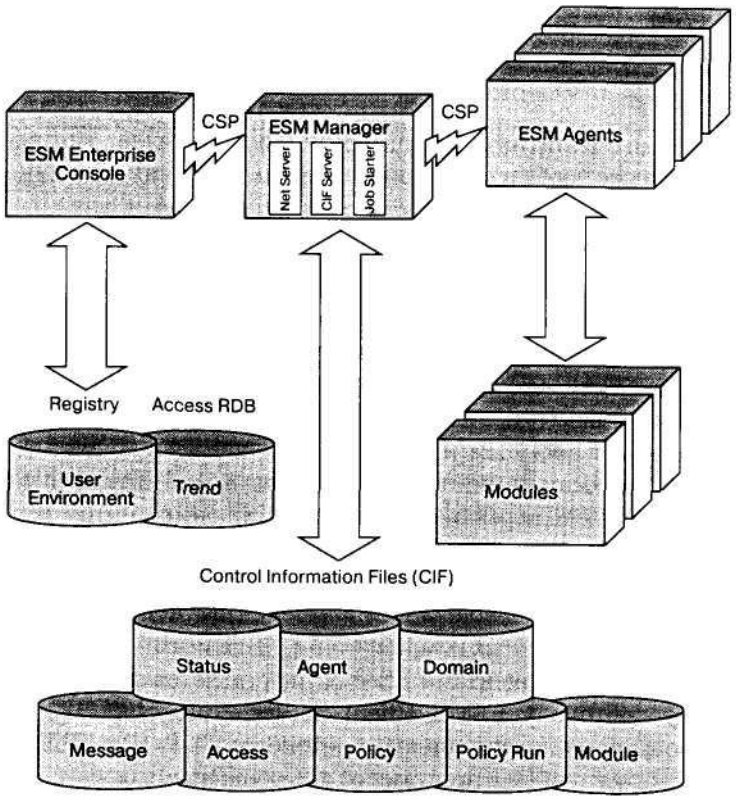


Рис. 6.8. Архитектура ESM

Административная консоль используется для выполнения следующих задач:

– правления регистрационными записями пользователей на ESM-менеджере;

- определения пользовательских полномочий в системе ESM;
- сбора и анализа информации о состоянии сети от ESM-менеджеров;
- ранжирования уязвимостей и определения уровней защищенности контролируемых систем;
- создания и изменения политик безопасности;
- активизации политик безопасности на контролируемых доменах;
- установки расписания выполнения проверок;
- отображения результатов выполнения проверок в табличной и графической формах;
- генерации и просмотра отчетов по результатам выполняемых проверок;
- коррекции некоторых параметров ОС.

Менеджер ESM

Центральным компонентом системы является ESM-менеджер. Он выполняет две основные функции:

- хранит данные о политиках безопасности и осуществляет управление этими данными, а также передает эти данные агентам и административной консоли;
- осуществляет управление данными о результатах выполненных проверок, получает эти данные от ESM-агентов и передает их на административную консоль.

Основным компонентом менеджера является сервер управления данными -CIF-сервер. Все данные о пользователях ESM, полномочиях, агентах, доменах, политиках безопасности, результатах проверок и шаблонах, а также сообщения от агентов хранятся в файлах управляющей информации (Control Information Files). CIF-сервер управляет доступом к CIF-файлам. Он предоставляет необходимую информацию по запросам административной консоли и интерфейса командной строки. CIF-сервер также перенаправляет запросы на выполнение другим компонентам менеджера. Например, сообщает менеджеру задач (Job Starter) о необходимости активизировать выполнение политики безопасности на домене. Сетевой сервер (Net Server) является еще одним компонентом менеджера, обеспечивающим связь CIF-сервера и других компонентов с удаленными агентами. Связь между распределенными компонентами ESM осуществляется по защищенному клиент-серверному протоколу ESM's Client Server Protocol (CSP) прикладного уровня, реализованному поверх сетевых протоколов TCP/IP и SPX/IPX. Защита трафика между менеджерами и агентами от прослушивания осуществляется шифрованием по алгоритму DESX, являющемуся усовершенствованной версией американского стандарта шифрования DES.

Агенты ESM

Агенты ESM, так же как и менеджеры, имеют модульную структуру. Они включают серверную часть, модули безопасности и средства коммуникаций. Они собирают информацию о безопасности системы. Сбор и анализ информации начинается с момента получения указания от менеджера на активизацию политики безопасности. Серверный компонент агента собирает данные о результатах проверок от модулей безопасности и посылает их менеджеру. Агенты выполняют также ряд других важных функций:

- сохраняют мгновенные снимки, содержащие данные о состоянии системы и пользовательских бюджетах;
- осуществляют обновление мгновенных снимков состояния системы;
- осуществляют коррекцию некоторых параметров системы по запросам пользователя.

Политики безопасности ESM

Политика безопасности ESM представляет собой совокупность модулей безопасности. ESM содержит набор предопределенных политик безопасности, предназначенных для обеспечения различных уровней защищенности. Политика безопасности предприятия реализуется на основе предопределенных политик ESM путем настройки модулей безопасности с целью изменения

количества и содержания выполняемых ими проверок. Доменная организация агентов позволяет распространить действие политик безопасности на отдельные системы, группы систем и предприятие в целом.

Политика безопасности задает набор правил, которым должны соответствовать контролируемые системы. ESM осуществляет анализ защищенности систем путем сравнения значений их конфигурационных параметров с теми, которые заданы в политике безопасности. ESM выполняет ранжирование результатов проверок по степени критичности и определяет общий уровень защищенности системы, суммируя числовые рейтинги обнаруженных уязвимостей.

Задачу начального конфигурирования ESM существенно облегчает наличие предопределенных политик безопасности, перечисляемых в порядке увеличения строгости и глубины проверок:

- Phase 1;
- Phase 2;
- Phase 3:a Relaxed;
- Phase 3:b Cautious;
- Phase 3:c Strict.

Политика первого уровня (Phase 1) включает модули безопасности, предназначенные для проверки наиболее существенных и потенциально опасных видов уязвимостей, устранение которых позволяет обеспечить минимально необходимый для большинства систем уровень защищенности.

Политика второго уровня (Phase 2) включает все имеющиеся в ESM модули безопасности, в которых активизированы только основные виды проверок, являющиеся наиболее важными.

Политики третьего уровня (Phase 3) включают:

- базовую версию, идентичную политике второго уровня (Relaxed);
- усиленную версию, содержащую дополнительные виды проверок (Cautious);
- строгую версию, включающую все виды проверок во всех модулях безопасности, поддерживаемых для данной ОС (Strict).

Помимо перечисленных в ESM имеется еще несколько специализированных политик безопасности. Предопределенная политика Queries включает только информационные модули, предоставляющие информацию о пользователях, группах и системах, на которых не установлены ESM- и ITA-агенты. Она разработана для платформ NetWare и Windows.

Специальная политика NetRecon используется для интеграции со сканером NetRecon на платформе Windows, позволяя просматривать и анализировать результаты сканирования средствами ESM-консоли. Она осуществляет преобразование записей об уязвимостях, сгенерированных сканером NetRecon, в формат сообщений ESM.

Контроль защищенности корпоративной сети при помощи ESM обычно производится путем постепенного ужесточения требований безопасности, предъявляемых к информационной системе. Начинать следует с активизации политик первого и второго уровней на контролируемых системах. Для большинства коммерческих систем такой уровень защищенности является вполне приемлемым. В случае успешного завершения всех проверок на особо критичных системах можно активизировать политики безопасности третьего уровня, которые позволяют осуществлять наиболее глубокий анализ параметров защиты.

Имеется возможность на основе предопределенных политик создавать свои собственные, которые наилучшим образом соответствуют требованиям организации. Для создания политик безопасности в составе ESM имеется графический инструментарий, полностью исключающий какое-либо программирование.

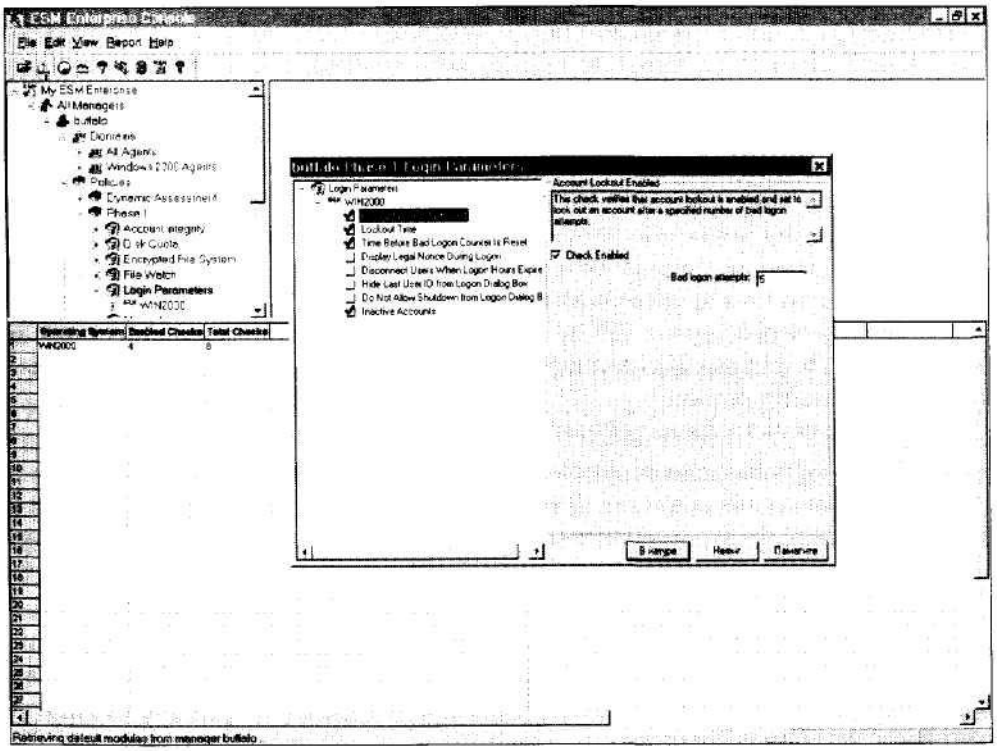


Рис. 6.9. Управляющая консоль ESM (проверки, выполняемые модулем Login Parameters)

Модули ESM

Модули ESM-агентов - это программные модули, осуществляющие проверки, предписываемые политикой безопасности. Имеется две разновидности модулей ESM: модули безопасности и модули запросов. Первые контролируют различные области безопасности, включая управление пользовательскими бюджетами и параметрами авторизации, настройку сетевых параметров и параметров сервера, атрибуты файловых систем и каталогов. Вторые предназначены для сбора информации о состоянии системы. Например, получение списка пользователей, входящих в определенную группу, либо пользователей, наделенных административными полномочиями.

Модули запросов (информационные модули)

Информационные модули служат для сбора информации о различных параметрах системы, существенных при выполнении задач администрирования безопасности. В табл. 6.1 приводится описание некоторых информационных модулей.

Таблица 6.1. Информационные модули ESM

Название модуля	Описание
Account Information	Данный модуль служит для получения информации о регистрационных записях пользователей ОС. В Windows NT он возвращает информацию о полномочиях пользователей, список пользователей с правами администратора, список заблокированных и отключенных регистрационных записей пользователей, список групп и списки пользователей, входящих в каждую группу. В ОС NetWare модуль возвращает список групп и списки пользователей, входящих в каждую группу, эквиваленты безопасности, эффективные права доступа, отношения доверия и т.п.
Discovery	Этот модуль сканирует TCP-порты (с целью выявления активных), пытается идентифицировать сетевые ресурсы и составляет список хостов, которые не находятся под контролем программных агентов ESM и ITA
File Information	Возвращает список параметров доступа к файлам, специфичных для ОС NetWare

Модули безопасности

Назначение модулей безопасности:

- идентификация, аутентификация и авторизация пользователей при входе в систему, управление паролями и пользовательскими бюджетами;
- конфигурация сетевых протоколов и сервисов;
- управление доступом к файлам и каталогам.

Пользователь имеет возможность выбрать проверки, доступные внутри данного модуля. Каждая проверка осуществляет поиск некоторого типа уязвимостей. Например, проверки, входящие в состав модуля Login Parameters, определяют неактивных пользователей, зарегистрированных в системе, на наличие паролей с истекшим сроком действия и установку ограничения на количество неудачных попыток входа в систему. (Одни модули безопасности используются только для проверки параметров определенных ОС и приложений, другие - более универсальные - охватывают несколько ОС.) В табл. 6.2 приводится описание основных модулей безопасности.

Таблица 6.2. Модули безопасности ESM

Модуль безопасности	Описание
Account Integrity	Проверяются привилегии пользователей, политика управления паролями и регистрационными записями пользователей
Backup Integrity	Проверяются параметры подсистемы резервного копирования, выявляются файлы, для которых не были созданы резервные копии
File Access	Проверяется соответствие прав доступа к файлам установленным правилам политики безопасности
File Attributes	Контроль целостности атрибутов файлов данных
File Find	Проверяется целостность файлов и контроль файлов на наличие вирусов
Login Parameters	Проверяются параметры регистрации в системе на соответствие установленным правилам политики безопасности
Object Integrity	Контролируются изменения прав владения, прав доступа и других атрибутов исполняемых файлов
Password Strength	Проверяется соответствие паролей пользователей установленным правилам политики управления паролями. Выявляются «слабые» пароли, о также их отсутствие
Startup Files	Проверяются командные файлы, исполняемые при загрузке системы, на наличие в них уязвимостей
System Auditing	Проверяются параметры подсистемы аудита и осуществление мониторинга журналов аудита Windows
System Mai	Проверяются конфигурационные параметры системы электронной почты, связанные с безопасностью
System Queues	Проверяются параметры настройки очередей системных утилит cron, patch и at ОС UNIX, а также параметры подсистемы спулинга ОС OpenVMS
User Files	Проверяются права владения и права доступа к файлам пользователей
Registry	Проверяются права доступа и атрибуты ключей реестра ОС Windows
Network Vulnerabilies	Анализируются уязвимости настроек сетевых параметров Windows, обнаруженных сетевым сканером NetRecon

С целью упрощения задачи управления безопасностью при помощи ESM все агенты ESM объединяются в домены. Доменом ESM называется группа агентов, объединенных по определенному признаку. Это позволяет активизировать политику безопасности одновременно на всех агентах, входящих в домен. По умолчанию все агенты объединены в домены по типу операционной системы. Таким образом, изначально существует Windows-домен, UNIX-домен, NetWare-домен и OpenVMS-домен. Доменная организация может также отражать организационную или территориальную структуру предприятия.

В ходе проверок ESM выполняет поиск нарушений политики безопасности. Нарушения политики безопасности могут быть двух типов:

- несоответствие правилам политики безопасности;

– несоответствие текущего состояния системы последнему мгновенному снимку, сохраненному в момент проведения предыдущих проверок.

Мгновенные снимки состояния системы

Мгновенные снимки используются ESM для контроля целостности программной и информационной частей ОС и приложений и для отслеживания изменений в конфигурации системы. Мгновенные снимки содержат значения атрибутов объектов, специфичные для данной системы, такие как время создания и модификации, контрольные суммы и права доступа к файлам, привилегии пользователей и т.п. Файлы, содержащие мгновенные снимки, создаются при первом запуске политики безопасности на контролируемой системе. В ходе последующих запусков состояние системы сравнивается с мгновенными снимками предыдущих состояний и все различия, обнаруженные в параметрах конфигурации и атрибутах системных объектов, рассматриваются в качестве потенциальных уязвимостей. Состояния объектов сравниваются с мгновенными снимками, и сообщения обо всех отличиях посылаются менеджеру, где они записываются в базу данных безопасности.

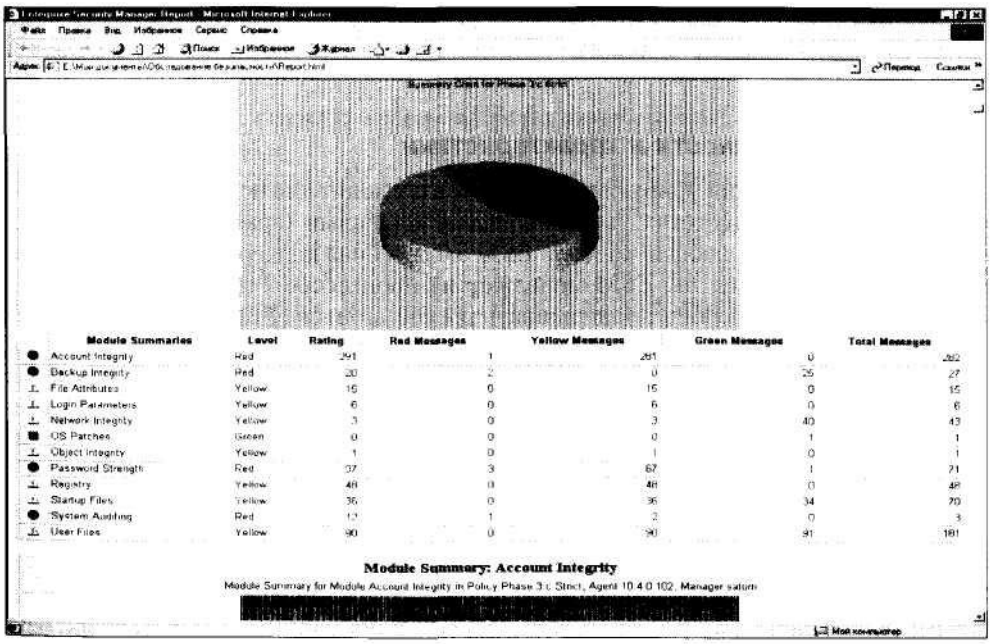


Рис. 6.10. Результаты проверки системы на соответствие политике безопасности 3:c Strict при помощи ESM

Каждый агент ESM создает несколько файлов мгновенных снимков с названиями File, User, Group, Device и т.п. Файлы User, Group и Device информируют о состоянии соответствующих системных объектов. Файл User содержит данные пользовательских бюджетов, в том числе пользовательские полномочия и привилегии. Файл Group содержит данные о группах пользователей, в том числе полномочия и привилегии для группы, а также список членов группы. Файл Device содержит имена владельцев, права доступа и атрибуты устройств.

В отличие от других файлов мгновенных снимков, File используется для сравнения со специальными шаблонами с целью обнаружения подозрительных изменений файлов, вирусов и «троянских» коней.

Специализированные модули безопасности, дополнительно устанавливаемые на агенты Oracle modules, Web modules и т.п., могут использовать собственные виды мгновенных снимков.

Шаблоны ESM

Шаблоны используются для выявления несоответствий конфигурации системы правилам политики безопасности. Они представляют собой списки системных объектов и их состояний. Так,

модуль File Attributes проверяет атрибуты системных файлов ОС Windows 2000 Professional по шаблону (fileatt.w50), а модуль OS Patches проверяет по шаблону (patch.pw5) наличие установленных программных коррекций для ОС.

Файлы шаблонов хранятся на менеджере. При запуске политики модули безопасности определяют по шаблонам объекты и атрибуты объектов, которые будут проверяться.

Основные возможности и характеристики

ESM лучше других конкурирующих продуктов подходит для использования в крупных и быстрорастущих сетях, так как обладает хорошими характеристиками масштабируемости. Управляющая консоль ESM 5.0 способна поддерживать до 40 менеджеров и до 10000 агентов. ESM-менеджер на процессоре Pentium 120 МГц или SPARC 276 МГц способен поддерживать до 400 агентов. Управляющая консоль функционирует в различных графических средах, включая X-Window, Windows 3.x, Windows 95/98/NT. В настоящее время ESM осуществляет более 1000 проверок параметров настройки ОС и приложений, Поддерживается 55 различных продуктов, в том числе ОС, маршрутизаторы, МЭ, Web-серверы, СУБД Oracle и Lotus Notes. Среди поддерживаемых ОС различные версии UNIX, а также Windows NT, NetWare, OpenVMS и т.д.

Возможности ESM могут быть расширены с целью обеспечения поддержки новых приложений. Программный инструментарий ESM SDK позволяет создавать новые модули безопасности для поддержки новых приложений, таких как серверы СУБД, Web-серверы, почтовые серверы, МЭ и т.п. Разработка новых модулей осуществляется при помощи библиотечных функций ESM API. В настоящее время созданы политики безопасности для контроля соответствия настроек ОС требованиям стандарта ISO 17799, а также специализированная антивирусная политика для

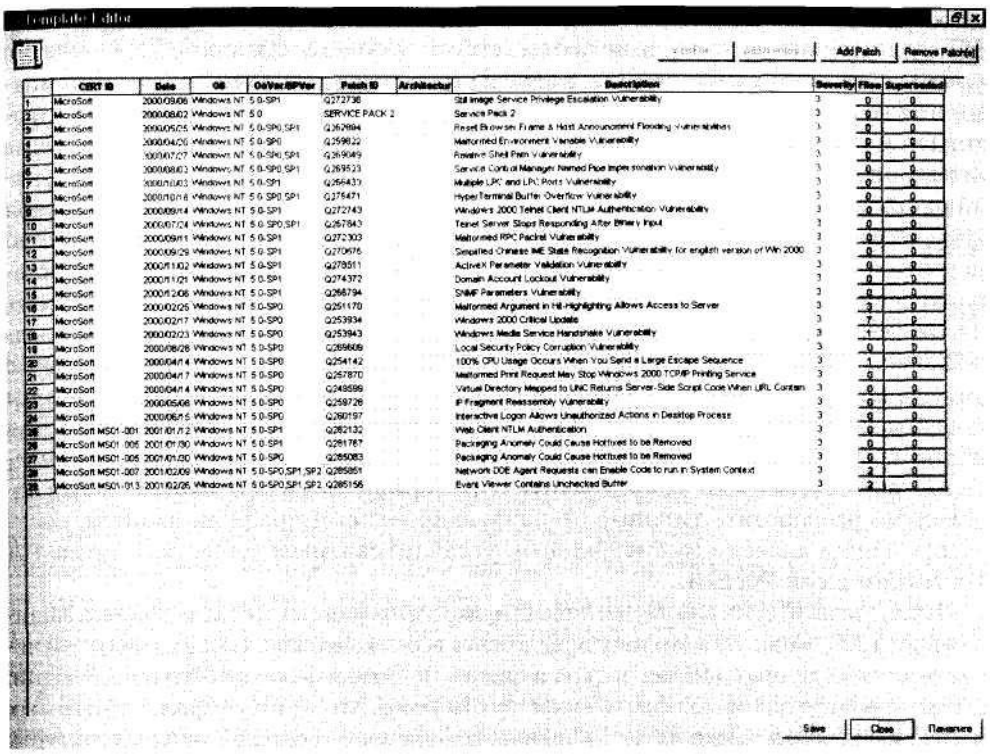


Рис. 6.11. Редактор шаблонов ESM (загружен шаблон OS Patches)

контроля серверной части NAV Corporate Edition 7.6. Количество политик безопасности, предназначенных для контроля разных аспектов функционирования АС и различных видов приложений, постоянно увеличивается. Список доступных политик и реализующих их модулей

безопасности ESM можно найти на Web-сайте Symantec Security Response Team: http://securityresponse.symantec.com/.

В состав ESM также входят специальные модули для интеграции со средствами сетевого управления HP OpenView и IBM (среда Tivoli).

Несмотря на все достоинства, использование программных агентов не может заменить сетевого сканирования, поэтому их лучше применять совместно с сетевыми сканерами.

6.5 Перспективы развития

В основе современных методик, используемых для анализа защищенности АС, лежат критерии оценки безопасности ИТ, устанавливающие классы и уровни защищенности. Методики и концепции оценки безопасности, а также набор критериев в достаточном объеме приведены в международных стандартах ISO 15408 и ISO 17799 (BS 7799), руководящих документах Гостехкомиссии России, других нормативных документах.

К сожалению, отечественная нормативная база в области оценки безопасности ИТ существенно устарела и не соответствует текущему состоянию ИТ. Однако работы по ее совершенствованию в нашей стране идут довольно быстрыми темпами под руководством Гостехкомиссии России. К настоящему времени подготовлен и утвержден Госстандартом ГОСТ Р ИСО/МЭК 15408-1-2002 «Общие критерии оценки безопасности ИТ» (постановление № 133-СТ от 04.04.02), являющийся переводом ISO 15408. Данный ГОСТ вводится в действие с 1 января 2004 г. Это объясняется неготовностью российского ИТ-сообщества немедленно перейти к использованию концепции и методики оценки безопасности ИТ, устанавливаемых этим стандартом. Потребуется приложить немало усилий для того, чтобы схема проведения оценки безопасности ИТ, основанная на подходе, предложенном в «Общих критериях», заработала и позволила бы получить реальные результаты. К настоящему времени на основе этого стандарта уже подготовлены проекты профилей защиты для МЭ и других средств защиты информации. Для обеспечения преемственности результатов работ в области анализа защищенности АС, выполненных по ныне действующим нормативным документам, также необходимо разработать типовые стандартизированные профили защиты, соответствующие классам защищенности, устанавливаемым существующими РД Гостехкомиссии России.

Несмотря на отсутствие каких-либо стандартизированных методик анализа защищенности АС, типовую методику предложить все-таки можно. Она включает изучение исходных данных; анализ рисков и оценку политики безопасности организации; анализ конфигурационных файлов маршрутизаторов, МЭ и proxy-серверов, почтовых и DNS-серверов, а также других критических элементов сетевой инфраструктуры; сканирование ЛВС снаружи и изнутри; анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.

Перечисленные методы исследования предполагают использование как активного, так и пассивного тестирования системы защиты, производимого вручную либо с применением специализированных программных средств.

Арсенал программных средств, используемых для анализа защищенности АС, достаточно широк. Причем во многих случаях свободно распространяемые программные продукты ничем не уступают коммерческим. Достаточно сравнить некоммерческий сканер NESSUS с его коммерческими аналогами. Однако на практике, при проведении достаточно глубоких исследований защищенности АС, полностью обойтись без коммерческих программных продуктов такого уровня, как, например, Symantec ESM и NetRecon, непросто.

Подводя итог всему вышесказанному, отметим, что в настоящее время вопросы анализа защищенности корпоративных АС хорошо проработаны. Имеется богатый арсенал средств и методов для проведения подобных мероприятий. Отработанные методики проведения обследования (аудита) безопасности АС в соответствии с проверенными критериями,

утвержденными в качестве международных стандартов, делают возможным получение исчерпывающей информации о свойствах АС, имеющих отношение к безопасности. На практике анализ защищенности АС проводится при помощи мощного программного инструментария, в достаточном объеме представленного на рынке средств защиты информации.

Глава 7
Обнаружение атак и управление рисками

Понятие риска является фундаментальным для любой области человеческой деятельности. Чем бы мы ни занимались, всегда есть вероятность того, что цели нашей деятельности по тем или иным причинам не будут достигнуты. Само наше существование сопряжено с серьезными рисками, в результате реализации которых мы можем понести более или менее серьезный ущерб. Таким образом, *под риском понимается возможность понести ущерб.* На протяжении всей нашей жизни мы постоянно вполне осознанно или подсознательно занимаемся оценкой различных рисков: переходя через дорогу, обменивая рубли на доллары или вставляя дискету в дисковод.

В сфере информационной безопасности оценка рисков играет такую же первостепенную роль, как и во всех других областях человеческой деятельности. Из-за неадекватной оценки рисков, связанных с осуществлением угроз информационной безопасности в современном высокотехнологичном обществе, государство, организации и отдельные личности несут весьма ощутимый ущерб, подсчитать который вряд ли кому-либо удастся.

Величина риска определяется вероятностью успешного выполнения угрозы и величиной ущерба, который в результате будет нанесен. Возможный ущерб далеко не всегда может быть выражен в денежных единицах, а вероятность успешной реализации угрозы вообще не поддается точной оценке. Поэтому наши оценки рисков весьма приблизительны. Их точность зависит от того, насколько хорошо мы ориентируемся в текущей ситуации, правильно ли представляем себе природу и способы реализации угроз, а также от нашей способности анализировать и оценивать их последствия.

Оценив риски, необходимо решить, что с ними делать. Этот процесс называется управлением рисками.

Задача управления рисками включает выбор контрмер, позволяющих снизить величины рисков до приемлемой величины, и обоснование этого выбора.

Управление рисками предполагает оценку стоимости реализации контрмер, которая должна быть меньше величины возможного ущерба. Разница между стоимостью принятия контрмер и величиной возможного ущерба должна быть тем больше, чем меньше вероятность причинения ущерба.

Контрмеры могут снизить уровни рисков различны жми способами:

- уменьшая вероятность осуществления угроз безопасности;
- ликвидируя уязвимости или понижая их величину;
- уменьшая величину возможного ущерба;
- способствуя восстановлению ресурсов АС, которым был нанесен ущерб;.
- выявляя атаки и другие нарушения безопасности.

В этой главе рассматривается комплекс вопросов, касающихся выявления атак.

7.1 Сетевые атаки

С увеличением зависимости мировой экономики и государственных структур от Internet возрастает и уровень риска, связанного с сетевыми атаками на ресурсы сетей, подключенных к Internet. Атаки через Глобальную сеть становятся мощным средством ведения информационных войн между государствами, совершения преступлений в финансовой и других сферах, включая акты терроризма. 22 сентября 2001 г. Американским институтом изучения технологий

обеспечения безопасности (Institute for Security Technology Studies At Dartmouth College) был опубликован отчет под названием «Кибератаки во время войны с терроризмом» (Cyber Attacks During The War on Terrorism: A Predictive Analysis). Данный отчет содержит анализ ситуаций, в которых политические конфликты стимулировали рост числа сетевых атак на ресурсы Internet. С этой точки зрения изучались конфликты между Индией и Пакистаном, Израилем и Палестиной, NATO и Сербией, США и Китаем из-за столкновения между китайским истребителем и американским самолетом-разведчиком. Целью предпринятого исследования было прогнозирование ситуации в Internet в результате проведения США широкомасштабной антитеррористической кампании после трагедии 11 сентября 2001 г. Хотя в данном исследовании как объекты нападения рассматривались Internet-ресурсы, принадлежащие США, сделанные выводы применимы и ко всем остальным государствам, включая Россию.

Потенциальные источники сетевых атак были разделены на следующие группы:

- террористические группы;
- хакеры, одобряющие действия террористов или ненастроенные против США;
- государства, считающиеся оплотом мирового терроризма, против которых может быть направлена антитеррористическая кампания США (в том числе Афганистан, Сирия, Иран, Ирак, Судан и Ливия);
- любопытствующие и самоутверждающиеся хакеры.

В качестве основных целей сетевых атак обсуждались:

- подмена страниц на Web-серверах (Web defacing) в США и странах-союзницах, распространение дезинформации и пропаганды;
- атаки «отказ в обслуживании» (DoS) на критичные элементы информационной инфраструктуры в США и странах-союзницах с использованием сетевых червей и вирусов, уязвимостей сетевого ПО;
- НСД к Internet-ресурсам США и стран-союзниц, результатом которых является повреждение критичных элементов информационной инфраструктуры и нарушение целостности жизненно важной информации.

Основные выводы по результатам анализа:

- физические атаки сразу же сопровождаются ростом числа сетевых атак;
- количество, сложность и скоординированность сетевых атак неизменно возрастают;
- сетевые атаки направлены против особо критичных сетевых ресурсов, к числу которых относятся серверы и активное сетевое оборудование, подключенные к Internet.

Проведенное исследование позволило рекомендовать в качестве первоочередных мер обеспечения безопасности во время войны с терроризмом следующие:

- повышение документирования (logging) и оповещения (alert) в системах выявления сетевых атак;
- незамедлительное сообщение о подозрительной активности в правоохранительные органы с целью проведения расследования и принятия предупредительных мер;
- следование стандартам и внедрение передового опыта в области обеспечения информационной и физической безопасности, регулярное обновление ПО, защита от вирусов, установка систем выявления атак и МЭ;
- принятие рекомендованных мер защиты против известных программных средств реализации атак (exploites) и резервное копирование критичных информационных ресурсов;
- применение методов фильтрации IP-пакетов (ingress and egress filtering) на маршрутизаторах и МЭ для защиты от DoS-атак.

Как видно из представленных рекомендаций, наряду со стандартными средствами защиты, без которых немыслимо нормальное функционирование АС (таких как МЭ, системы резервного копирования и антивирусные средства), необходимы еще и IDS (системы выявления атак) - основное средство борьбы с сетевыми атаками.

В настоящее время IDS начинают все шире внедряться в практику обеспечения безопасности корпоративных сетей. Однако имеется ряд проблем, с которыми неизбежно сталкиваются организации, развертывающие у себя систему выявления атак. Эти проблемы существенно затрудняют, а порой и останавливают процесс внедрения IDS. Приведем некоторые из них:

- большая стоимость коммерческих IDS;
- малая эффективность современных IDS, характеризующихся большим числом ложных срабатываний и несрабатываний (false positives and false negatives);
- требовательность к ресурсам и порой неудовлетворительная производительность IDS уже на скорости 100 Мбит/с в сетях;
- недооценка рисков, связанных с сетевыми атаками;
- отсутствие в организации методики анализа рисков и управления ими, позволяющей руководству адекватно оценивать величину риска и обосновывать стоимость реализации контрмер;
- необходимость в высокой квалификации экспертов по выявлению атак, без которой невозможно внедрение и развертывание IDS.

Для России характерны также незначительная зависимость информационной инфраструктуры предприятий от Internet и финансирование мероприятий, обеспечивающих информационную безопасность, по остаточному принципу, что не способствует приобретению дорогостоящих средств защиты для противодействия сетевым атакам.

Тем не менее процесс внедрения IDS в практику поддержания ИБ продолжается, в том числе и в России.

Американский институт SANS учредил программу профессиональной сертификации специалистов по выявлению атак - GIAC Certified Intrusion Analyst (GCIA). Сертификат GCLA, будучи свидетельством практических навыков специалиста, ценится в США даже выше, чем, скажем, CISSP (Certified Information Systems Security Professional), учрежденный ISC (International Security Consortium) и являющийся эталоном профессиональной зрелости в сфере ИБ.

В основе большинства ошибок при принятии решений, в том числе по защите от сетевых атак, лежит неправильная оценка рисков. Точность идентификации и оценки рисков, связанных с любым видом деятельности, выступает в качестве основной характеристики профессиональной зрелости специалиста в предметной области. При отсутствии адекватной оценки рисков сложно ответить на вопросы о том, с чего следует начинать построение системы защиты информации, какие ресурсы и от каких угроз надо защищать и какие контрмеры считать приоритетными. Трудно также решать проблему необходимости и достаточности того или иного набора контрмер и их адекватности существующим рискам.

Таким образом, вопрос оценки рисков, связанных с сетевыми атаками, является важнейшим и рассматривается в первую очередь.

7.2 Обнаружение атак как метод управления рисками

Обнаружение атак сегодня - один из методов управления рисками. Деятельность по обнаружению сетевых атак при помощи сетевых IDS заключается в мониторинге сетевого трафика между атакующими и атакуемыми системами, нахождении и анализе подозрительного трафика, оценке уровня серьезности атаки и величины риска, связанного с ее реализацией, а также

принятии решения о реагировании на атаку. Поиск подозрительного трафика, а зачастую и определение уровня серьезности атаки выполняется IDS автоматически. Наиболее распространенным методом обнаружения атак является сигнатурный анализ, используемый во всех коммерческих IDS и рассматриваемый ниже. Оценка величины риска, связанного с сетевой атакой, требует участия эксперта. На основании оценки риска решается вопрос о реагировании на атаку. Если риск незначителен, то не исключено, что атака вообще не заслуживает внимания. В то же время, в отдельных случаях, может понадобиться принятие незамедлительных мер реагирования.

Рассмотрим методику оценки рисков, связанных с реализацией сетевых атак, принятую в SANS/GIAC.

7.2.1 Оценка серьезности сетевой атаки

Атаки разной степени критичности требуют разного уровня реагирования. Критичность атаки (Severity) определяется величиной риска в результате ее реализации. Величина риска, в свою очередь, зависит от вероятности успешного проведения атаки и величины возможного ущерба, а величина возможного ущерба - от степени критичности ресурсов (Criticality), против которых направлена атака. На вероятность успешного выполнения атаки (Lethality) влияет эффективность методов и величина уязвимости системы защиты, с помощью которых она предпринимается. Величина уязвимости напрямую связана с эффективностью контрмер на системном (System countermeasures) и сетевом уровнях (Network countermeasures), применяемых для противодействия данному виду угроз.

Формула для нахождения уровня серьезности атаки выглядит следующим образом:

SEVERITY = (CRITICALITY + LETHALITY) - (SYSTEM COUNTERMEASURES + NETWORK COUNTERMEASURES).

Данной формулой можно воспользоваться для оценки величины рисков из-за атак, выявленных при помощи IDS, при анализе результатов мониторинга сетевого трафика. Обычно интерес представляют только те атаки, для которых величина риска превышает некоторое пороговое значение.

Уровень серьезности атаки (SEVERITY) устанавливается по числовой шкале от -10 до+10.

SEVERITY {-10,10} - величина риска, связанного с реализацией сетевой атаки.

Критичность сетевого ресурса (CRITICALITY) определяется по 5-балльной шкале исходя из предназначения данного сетевого ресурса и выполняемых им функций. На практике обычно ориентируются на следующую шкалу:

- 5 - МЭ, DNS-сервер, маршрутизатор;
- 4 - почтовый шлюз;
- 2 - рабочая станция UNIX;
- 1 - персональные компьютеры MS-DOS, Windows 3.11.

Для определения вероятности успешного выполнения атаки и возможного ущерба (LETHALITY) принята следующая шкала:

- 5 - атакующий может получить права суперпользователя на удаленной системе;
- 4 - отказ в обслуживании в результате реализации сетевой атаки;
- 3 - получение прав непривилегированного пользователя на удаленной системе, например путем перехвата пароля, передаваемого по сети в открытом виде;
- 2 - раскрытие конфиденциальной информации из-за несанкционированного сетевого доступа, например атака null session на системы Windows;
- 1 - вероятность успеха предпринятой атаки очень мала.

Эффективность принятых контрмер системного уровня (SYSTEM COUNTERMEASURES) можно оценить по следующей шкале:

- 5 - современная ОС, загружены все программные коррекции (пакеты обновления), имеются дополнительные (наложенные) сетевые средства защиты (например, tcp wrappers или secure shell);
- 3 - устаревшая версия ОС, не установлены некоторые программные коррекции;
- 1 - отсутствуют специализированные средства защиты, не сформирована политика управления паролями, пароли передаются по сети в открытом виде.

Следующая шкала служит для оценки эффективности контрмер сетевого уровня (NETWORK COUNTERMEASURES):

- 5 - МЭ, реализующий принцип минимизации привилегий, является единственной точкой входа в сеть;
- 4 - МЭ и наличие дополнительных точек входа в сеть;
- 2 - МЭ, разрешающий все, что явным образом не запрещено (разрешительная политика управления доступом).

Как уже было отмечено, данная методика оценки рисков, связанных с сетевыми атаками, используется в SANS/GIAC при анализе подозрительных фрагментов сетевого трафика (detects), обнаруженных с помощью сетевых IDS.

7.3 Ограничения межсетевых экранов

В настоящее время становится очевидным недостаточность традиционных МЭ для защиты сетей от угроз со стороны Internet, поскольку они не обеспечивают защиту от целого класса угроз безопасности (в том числе от угроз, направленных против самих МЭ). Традиционные средства защиты информации, включая МЭ, эффективны только против известных уязвимостей. Они вряд ли способны помешать хакерам в поиске новых способов реализации атак. Для этого предназначены специальные средства выявления атак - IDS. Мало того, нередко приходится наблюдать ситуации, когда установка МЭ только снижает общую защищенность корпоративной сети от угроз со стороны Internet. Неправильно настроенный МЭ создает в системе защиты «дырку», порой большую, чем его отсутствие.

Напрашивается аналогия с американским экспериментом по оснащению всех такси антиблокировочными системами тормозов (ABS), предназначенными для увеличения безопасности автомобиля. По статистике число ДТП с участием таксистов в результате этого эксперимента увеличилось, так как водители стали вести себя на дорогах более рискованно, больше доверяя тормозам. Таким образом, оказалось, что ABS увеличивает безопасность только в случае сохранения водителем прежнего стиля управления автомобилем.

Тот же самый принцип справедлив по отношению к МЭ и любым другим средствам защиты.

Добавление в систему нового средства защиты увеличивает общую защищенность системы лишь при условии, что существующая практика обеспечения безопасности не изменилась в сторону ослабления механизмов защиты.

Устанавливая МЭ, сетевые администраторы, полагаясь на реализуемые МЭ механизмы защиты, нередко отказываются от каких-либо дополнительных мер по поддержанию защиты от угроз со стороны внешней сети, которые необходимы при отсутствии МЭ. В результате общая защищенность сети от внешних атак может либо увеличиться, либо остаться неизменной, либо (и это вполне вероятно) снизиться. Происходит это потому, что администраторы и пользователи сети склонны всецело доверять МЭ и переоценивать его роль в деле защиты сети от внешних угроз со стороны Internet. Они представляют себе МЭ как некий щит, закрывающий их от дождя, града,

снега, штормов и прочей непогоды. При этом забывают, что в щите имеется немало дырок, а иногда он даже может напоминать решето. «Дырки» в щите нужны для общения с внешним враждебным миром. По ошибке, и это совсем не исключено, могут быть открыты не те «дырки» или «дырки» окажутся слишком большими, к тому же «дырки» в щите иногда удается пробить снаружи.

Таким образом, для обеспечения адекватного уровня защиты МЭ следует обязательно дополнять специальными средствами выявления атак. На эту тему имеется уже достаточно много публикаций, поэтому нет необходимости еще раз отстаивать данный тезис, иллюстрируя его большим количеством примеров, взятых из печального опыта российских и зарубежных компаний. Однако, устанавливая МЭ, руководство российских компаний пока не торопится выделять средства на приобретение и эксплуатацию систем выявления атак.

7.4 Анализ подозрительного трафика

7.4.1 Сигнатуры как основной механизм выявления атак

Системы выявления атак IDS решают задачу мониторинга информационной системы на сетевом, системном и прикладном уровнях с целью обнаружения нарушений безопасности и оперативного реагирования на них. Сетевые IDS служат в качестве источника данных для анализа сетевых пакетов, а IDS системного уровня (хостовые - host based) анализируют записи журналов аудита безопасности ОС и приложений. При этом методы анализа (выявления атак) остаются общими для всех классов IDS.

Было предложено немало различных подходов к решению задачи обнаружения атак (в общем случае речь идет о преднамеренной активности, включающей, помимо атак, действия, выполняемые в рамках предоставленных полномочий, но нарушающие установленные правила политики безопасности). Однако все существующие IDS можно разделить на два основных класса: одни применяют статистический анализ, другие - сигнатурный анализ.

Статистические методы базируются на предположении о том, что активность злоумышленника всегда сопровождается какими-то аномалиями, изменением профиля поведения пользователей, программ и аппаратуры.

Основным методом выявления атак, принятым в большинстве современных коммерческих продуктов, является сигнатурный анализ. Относительная простота данного метода позволяет с успехом внедрять его в практику. IDS, применяющие сигнатурный анализ, обычно ничего «не знают» о правилах политики безопасности, реализуемых МЭ (поэтому в данном случае речь идет не о преднамеренной активности, а только об атаках). Основной принцип их функционирования - сравнение происходящих в системе/сети событий с сигнатурами известных атак - тот же, что используется в антивирусном ПО.

Общие критерии оценки безопасности ИТ (ISO 15408) содержат набор требований FAU_SAA под названием «Анализ данных аудита безопасности» (Security audit analysis). Эти требования определяют функциональность IDS, которые ищут злоумышленную активность методами как статистического, так и сигнатурного анализа.

Компонент FAU_SAA2 «Выявление аномальной активности, основанное на применении профилей» (Profile based anomaly detection) предполагает обнаружение аномальной активности с помощью профилей системы, определяющих опасные с точки зрения безопасности действия пользователей системы, и выявление этих действий. С целью установления степени опасности действий того или иного пользователя вычисляются соответствующие «рейтинги недоверия» к пользователям. Чем больше опасность действий пользователя, тем выше его «рейтинг недоверия». Когда «рейтинг недоверия» достигает установленного критического значения, предпринимаются

предусмотренные политикой безопасности действия по реагированию на злоумышленную активность.

Компоненты FAU_SAA3 «Простая эвристика атаки» (Simple attack heuristics) и FAU_SAA4 «Сложная эвристика атаки» (Complex attack heuristics) предусматривают выполнение сигнатурного анализа для поиска злоумышленной активности. В случае атаки FAU_SAA4 сигнатура задает последовательность событий, являющуюся признаком нарушения установленных в системе правил политики безопасности.

7.4.2 Анализ сетевого трафика и анализ контента

Существует два не исключающих друг друга подхода к выявлению сетевых атак: анализ сетевого трафика и анализ контента. В первом случае изучаются лишь заголовки сетевых пакетов, во втором - их содержимое.

Конечно, наиболее полный контроль информационных взаимодействий обеспечивается только путем анализа всего содержимого сетевых пакетов, включая их заголовки и области данных. Однако с практической точки зрения такая задача трудновыполнима из-за огромного объема данных, которые пришлось бы обрабатывать. Современные IDS начинают испытывать серьезные проблемы с производительностью уже при скорости 100 Мб/с в сетях. Поэтому в большинстве случаев целесообразно прибегать для выявления атак к анализу сетевого трафика, в некоторых случаях сочетая его с анализом контента.

Концептуально сигнатура сетевой атаки практически не отличается от сигнатуры вируса. Она представляет собой набор признаков, позволяющих отличить сетевую атаку от других видов сетевого трафика. Так, перечисленные ниже признаки могут рассматриваться в качестве сигнатур атак:

- примеры сигнатур атак, используемых при анализе трафика (заголовков сетевых пакетов):
  - в заголовке TCP-пакета установлен порт назначения 139 и флаг OOB (Out of Band), что является признаком атаки аля WinNuke;
  - установлены одновременно противоречащие друг другу флаги TCP-паке-та: SYN и FIN. Посредством данной комбинации флагов во многих атакующих программах удается обходить фильтры и мониторы, проверяющие только установку одиночного SYN-флага;
- пример сигнатуры атаки, применяемой при анализе контента:
  - "GET. cgi-bin/etc/passwd". Появление такой строки в области данных HTTP-пакета свидетельствует о наличии эксплойтов типа phf, php или aglimpse.

Методы анализа контента имеют еще один существенный недостаток. Они не работают, когда атакующие программы (DDoS, trojans) обращаются к шифрованию трафика. Например, в Back Orifice trojan или Barbwire DDoS-команды, передаваемые между клиентом и сервером (менеджером и агентом), шифруются посредством алгоритма blowfish. Методы обнаружения такого рода атак ограничиваются анализом заголовков сетевых пакетов.

7.4.3 Пример анализа подозрительного трафика

Покажем, как управление рисками, связанными с сетевыми атаками, реализуется на практике. Прежде всего необходимо установить и настроить какую-нибудь систему мониторинга сетевого трафика, например NFR, NetProwler, Tcpdump+Shadow и т.п. После этого можно приступать к анализу подозрительного трафика, событий и разного рода сетевых атак, оценивать риски и управлять ими.

В качестве примера подозрительного трафика, заслуживающего внимания эксперта, рассмотрим фрагмент журнала регистрации событий программы Tcpdump - листинг 1.

Листинг 1

```
7:50:22.499014 eth0 > intruderhost.4265 > myhost.netbios-ssn: S
2828114481:2828114481(0) win 32120 sackOK,timestamp 17250647 0,nop,wscale
0> (DF) (ttl 64, id 11091)

17:50:22.499428 eth0 < myhost.netbios-ssn > intruderhost.4265: S
1070635944:1070635944(0) ack 2828114482 win 17520 nop,wscale
0,nop,nop,timestamp 0 0,nop,nop,sackOK> (DF) (ttl 128, id 33514)

17:50:22.499462 eth0 > intruderhost.4265 > myhost.netbios-ssn: . 1:1(0)
ack 1 win 32120 nop,timestamp 17250647 0> (DF) (ttl 64, id 11093)

17:50:22.500379 eth0 > intruderhost.4265 > myhost.netbios-ssn: P 1:13(12)
ack 1 win 32120 urg 12 nop,timestamp 17250647 0>>>> NBT (DF) (ttl 64, id
11095)
          4500 0040 2b57 4000 4006 78e4 c0a8 0aae
          c0a8 0a7e 10a9 008b a891 9a32 3fd0 9ba9
          8038 7d78 7dcb 000c 0101 080a 0107 3957
          0000 0000 796f 7520 6172 6520 6465 6164
           E^@ ^@ @  + W  @^@  @^F  x.. .... ^J..
          .... ^J ~ ^P.. ^@.. .... .. 2  ?.. ....
          .. 8  } x  }.. ^@^L ^A^A ^H^J ^A^G  9 W
          ^@^@ ^@^@  y o u    a r e    d e a d

17:50:22.500791 eth0 > intruderhost.4265 > myhost.netbios-ssn: F 13:13(0)
ack 1 win 32120 nop,timestamp 17250647 0> (DF) (ttl 64, id 11097)

17:50:22.500873 eth0 < myhost.netbios-ssn > intruderhost.4265: FP 1:6(5)
ack 13 win 17509 nop,timestamp 6007121 17250647>>>> NBT (DF) (ttl 128, id
33517)
          4500 0039 82ed 4000 8006 e154 c0a8 0a7e
          c0a8 0aae 008b 10a9 3fd0 9ba9 a891 9a3e
          8019 4465 7642 0000 0101 080a 005b a951
          0107 3957 8300 0001 8f

           E^@ ^@ 9 ....  @^@ ..^F .. T .... ^J ~
          .... ^J.. ^@.. ^P..  ?.. .... .... .. >
          ..^Y  D e  v B ^@^@ ^A^A ^H^J ^@ [ .. Q
          ^A^G  9 W ..^@ ^@^A
          ..

17:50:22.500920 eth0 > intruderhost.4265 > myhost.netbios-ssn: . 14:14(0)
ack 7 win 32120 nop,timestamp 17250647 6007121> (DF) (ttl 64, id 11098)
```

```
17:50:22.501139 eth0 < myhost.netbios-ssn > intruderhost.4265: . 7:7(0)
ack 14 win 17509 nop,timestamp 6007121 17250647> (DF) (ttl 128, id 33518)

17:50:22.516930 eth0 > intruderhost.4265 > myhost.netbios-ssn: R 14:14(0
ack 7 win 32120 nop,timestamp 17250647 6007121> (DF) (ttl 64, id 11111)

17:50:32.508044 eth0 > intruderhost.www > myhost.www: .
2493876034:2493876034(0) ack 749177432 win 8 (ttl 64, id 16912)
17:50:32.508096 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)

17:50:32.508179 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)
17:50:32.508262 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)

17:50:32.508344 eth0 > intruderhost.www > myhost.www: . 0:0(0) ack 1 win 8
(ttl 64, id 16912)
17:50:32.508514 eth0 < myhost.www > intruderhost.www: R
749177432:749177432(0) win 0 (ttl 128, id 33778)

17:50:32.508672 eth0 < myhost.www > intruderhost.www: R
749177432:749177432(0) win 0 (ttl 128, id 33779)
17:50:32.508739 eth0 < myhost.www > intruderhost.www: R
749177432:749177432(0) win 0 (ttl 128, id 33780)

17:50:32.508821 eth0 < myhost.www > intruderhost.www: R
749177432:749177432(0) win 0 (ttl 128, id 33781)
17:50:32.508902 eth0 < myhost.www > intruderhost.www: R
749177432:749177432(0) win 0 (ttl 128, id 33782)
```

Данный формат удобен для выполнения практических работ при сдаче экзамена на степень GCIA (GIAC Intrusion Analyst) в SANS/GIAC.

Источник данных. Тестовая ЛВС.

IDS, сгенерировавшая сообщение об атаке. Tcpdump v.3.6.2.

Формат данных сообщения. Tcpdump пользуется следующим форматом для отображения TCP-пакетов:

- time (hh:mm:ss.microseconds);
- network interface name [ethO in our case];
- source IP address . source port > destination IP address . destination port;
- TCP flags ["" - indicates that all the flag bits set to 0, "P" - PUSH flag, "F" - FIN flag, "S" - SYN flag, "R" - RESET flag];
- beginning sequence number:ending sequence number(data bytes transfered);
- ack the sequence number of the next block of data expected from the other end of the TCP connection;
- win the number of bytes free in the receive buffer for receipt of data from the other end of the TCP connection;
- <nop,nop,timestamp 6007121 17250647> - tcp options:
- пор - no operation [pad options to 4-byte boundaries];
- timestamp - carries a timestamp for each segment;
- (DF) don't fragment flag set;

– (ttl time to live value, id IP identifier).

Вероятность подделки IP-адреса отправителя атакующей стороной. В данном случае между сторонами был установлен сеанс связи, поэтому вероятность подделки IP-адреса невелика. Однако нельзя исключать возможность внедрения атакующего в сеанс связи (session hijacking) - в случае взаимодействия между системами Windows предсказание номера TCP-пакета является тривиальной задачей. Для осуществления атаки такого вида атакующий хост должен быть подключен к линии связи между взаимодействующими сторонами (man-in-the-middle).

Описание атаки. Данный фрагмент трафика свидетельствует об атаке «отказ в обслуживании», направленной против ОС Windows 95/NT через порт NetBIOS, известной под названием WinNuke (CVE-1999-0153).

Атака выполняется путем отправки out-of-band data на 139-й порт атакуемого хоста, что нередко приводит к «зависанию» Windows-системы. И другие ОС могут оказаться уязвимыми по отношению к этому виду атаки, например SCO OpenServer 5.0 также ей подвержен.

Ожидаемый результат данного вида DoS-атаки - «зависание» атакуемой системы.

Механизм осуществления атаки. Программу, реализующую данный вид атаки, можно найти в Internet. Когда Windows-система получает пакет с установленным флагом URGENT, она ожидает, что за этим флагом последуют данные. Отсутствие данных после флага URG приводит ее в замешательство. Эта особенность Windows-систем (на которых не установлены соответствующие программные коррекции) способствует успеху DoS-атаки Winnuke. Сервис Netbios (TCP-порт 139) известен в качестве наиболее подверженного данной уязвимости и чаще всего атакуемого. Однако потенциально не исключена возможность успешного проведения данного вида атаки и через другие порты.

Такая атака может быть предпринята как удаленно, так и локально (то есть с той же машины, на которой запускается программа Winnuke).

Система Windows NT. Успех данной атаки против системы Windows NT приводит к зависанию системы и появлению «синего экрана смерти». Последствия атаки обычно заключаются в потере пользователем несохраненных документов (изменений).

Системы Windows 95, Windows for Workgroups 3.11. В случае успешного проведения этой атаки против систем Windows for Workgroups или Windows 95 на экране выводится сообщение о программной ошибке - «синий экран», уведомляющий пользователя о том, что приложение не отвечает. Последствия атаки: пользователь, как правило, теряет несохраненные документы (изменения).

Ссылки на источники информации об атаке/уязвимости. Описание атаки Win-nuke можно найти по следующим ссылкам:

– http://support.microsoft.com/support/kb/articles/q179/1/29.asp:
– http://ciac.llnl.gov/ciac/bulletins/h-57.shtml:
– ftp://ftp.sco.com/SSE/security_bulletins/SB.98:01a

Цели атаки и мотивация атакующей стороны (адресность и целенаправленность атаки). На вопрос о целях и мотивации атакующей стороны существует два ответа: 1. Данная атака является адресной и направлена против конкретной системы, содержащей соответствующую уязвимость. 2. Это сканирование сети в поисках систем, в которых имеется данная уязвимость.

Для правильного ответа необходимо дополнительное изучение журналов регистрации событий на МЭ и IDS с целью выяснения предыстории рассматриваемого события.

Величина риска. Величина риска (Severity), ассоциированного с этим событием, рассчитывается по формуле:

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity.

Оцениваем:

- критичность атакуемого хоста - Criticality: 2 (хост Windows 2000);
- возможные последствия - Lethality: 0 (хосты Win2000 не подвержены данной уязвимости, следовательно, последствия отсутствуют);
- эффективность контрмер системного уровня - Sys Counters: 5 (установлены последние программные коррекции);
- эффективность контрмер сетевого уровня - Net Counters: 5 (атакуемый хост расположен за фильтрующим маршрутизатором и МЭ во внутренней сети).

Тогда Severity: (2 + 1) - (5 + 5) = -7.

Таким образом, уровень риска в данном случае существенно меньше 0 (событие, не заслуживающее серьезного внимания эксперта).

Рекомендации по защите. Поскольку величина риска очень мала, о защите в данном случае вообще не стоит беспокоиться. Однако в общем случае можно дать следующие рекомендации по защите:

- лучшим способом защиты от подобного рода атак со стороны внешней сети традиционно признается применение МЭ. Блокирование сервиса Netbios на МЭ и маршрутизаторе, выполняющих функции внешнего шлюза корпоративной сети, является обычной практикой;
- периодическое сканирование сети при помощи сканера - хорошая профилактическая мера против таких атак (конечно, если базы данных уязвимостей сканера регулярно обновляются);
- если результаты сканирования сети выявили Windows-системы, уязвимые по отношению к данному виду атаки, то на них необходимо установить пакет программных коррекций от Microsoft (SP4 или более старшая версия), который можно найти по адресу: http://support.microsoft.com/support/ntserver/content /servicepacks/.

7.5 IDS как средство управления рисками

7.5.1 Типовая архитектура системы выявления атак

Типовая архитектура системы выявления атак, как правило, включает следующие компоненты:

- сенсор (средство сбора информации);
- анализатор (средство анализа информации);
- средства реагирования;
- средства управления.

Конечно, все эти компоненты могут функционировать на одном компьютере и даже в рамках одного приложения, однако чаще всего они территориально и функционально распределены. Такие компоненты IDS, как анализаторы и средства управления, опасно размещать за МЭ во внешней сети, так как если они будут скомпрометированы, то злоумышленник сможет получить доступ к информации о структуре внутренней защищаемой сети на основе анализа базы правил, используемой IDS.

Типовая архитектура системы выявления атак изображена на рис. 7.1. Сетевые сенсоры перехватывают сетевой трафик, в качестве источников информации для хостовых сенсоров служат журналы регистрации событий ОС, СУБД и приложений. Информация о событиях также может быть получена хостовым сенсором непосредственно от ядра ОС, МЭ или приложения. Анализатор, размещаемый на сервере безопасности, проводит централизованный сбор и анализ информации, поступающей от сенсоров.

Средства реагирования могут находиться на станциях мониторинга сети, МЭ, серверах и рабочих станциях ЛВС. Типичный набор действий по реагированию на атаки включает оповещение администратора безопасности (посредством электронной почты, вывода сообщения на консоль или отправки на пейджер), блокирование сетевых сессий и пользовательских регистрационных записей с целью немедленного прекращения атак, а также протоколирование действий атакующей стороны.

Средства управления предназначены для администрирования всех компонентов системы обнаружения атак, разработки алгоритмов выявления нарушений безопасности и реагирования на них (политик безопасности), а также для просмотра информации о нарушениях и генерации отчетов.

Рис. 7.1. Типовая архитектура системы выявления атак

7.5.2 Стандарты, определяющие правила взаимодействия между компонентами системы выявления атак

Необходимость стандартизации форматов данных и протоколов обмена данными, применяемых в IDS, обусловлена причинами, перечисленными ниже. Для защиты ЛВС, подключенных к сети Internet, от распределенных скоординированных атак необходимо обеспечить определенную степень взаимодействия между IDS, предназначенными для защиты различных точек входа в разные ЛВС. Например, в случае атаки против одной ЛВС, правила реагирования на которую предусматривают изменение конфигурации МЭ путем блокирования IP-адреса источника атаки, соответствующие изменения должны быть произведены на всех МЭ, служащих для защиты остальных ЛВС. Для этого необходим обмен информацией об источнике атаки и способе реагирования между различными IDS.

Центральным компонентом IDS является анализатор (analysis engine) - специализированное программное ядро, предназначенное для анализа данных, поступающих от сенсоров, и принятия решений о способах реагирования на подозрительные события. Стандартизация протоколов и форматов обмена данными между анализатором, с одной стороны, и сенсорами и средствами реагирования, с другой, позволяет применять общее программное ядро анализатора с различными типами сенсоров и средств реагирования.

Процесс стандартизации протоколов и форматов обмена данными, используемых в IDS, начался уже довольно давно. Рассмотрим несколько популярных форматов данных, с помощью которых через Internet обмениваются информацией о нарушениях безопасности.

7.5.3 Форматы обмена данными

AusCERT (portmap probe)

Source: 210.177.64.1

Ports: tcp 111

Incident type: network scan

re-distribute: yes

timezone: GMT + 1300

reply: no

Date: 30th Jan 2000 at 22:01 (UTC)

Система AusCERT применяется для сбора и анализа статистической информации об атаках. Данный формат записи позволяет автоматически добавлять данные об атаках в базу данных AusCERT.

Списки Грифина (Griffin list)

Посредством списков Грифина в казино идентифицируются карточные шулеры. Файлы с фотографиями известных шулеров сравниваются с изображением, полученным с видеокамеры. В качестве идентифицирующих признаков выступают черты лица, не подверженные изменению с течением времени.

Списки Грифина, установленные в системах выявления атак, содержат сетевые адреса компьютеров, с которых наиболее часто осуществляются подозрительные действия. Internet-центры по реагированию на компьютерные инциденты, такие как CERT или GIAC, занимаются формированием таких списков и предоставлением доступа к ним для широкой общественности (www.incidents.org). Эти данные могут использоваться в IDS. При анализе подозрительного трафика особое внимание следует уделять скомпрометировавшим себя IP-адресам.

7.5.4 CVE - тезаурус уязвимостей

CVE (Common Vulnerabilities and Exposures) - это единый тезаурус всех известных уязвимостей, определяющий общие правила их именования, доступ к которому через Internet открыт для всех заинтересованных лиц (cve.mitre.org) CVE не представляет собой классификацию уязвимостей и не претендует на их систематизацию. Приведем краткую историю его возникновения.

Дэвид Манн (David Mann) и Стивен Кристи (Steven Christey) из американской корпорации MITRE работали над созданием базы данных уязвимостей. Необходимо было установить соответствие между уязвимостями, обнаруживаемыми при помощи различных видов сканеров защищенности, предупреждающими сообщениями и рекомендациями по устранению этих уязвимостей. Здесь они столкнулись с проблемой именования уязвимостей. Например, известная уязвимость CGI phi позволяет удаленно выполнять команды с использованием метасимволов командного интерпретара SHELL. Классическим является пример получения с помощью этой уязвимости файла с паролями путем выполнения команды cat/etc/passwd. В сообщениях CERIAS данная уязвимость называется httpd_escshellcmd, а в сообщениях CERT – CA-96-06.CGI_Example_code. В различных сетевых сканерах, например в Internet Scanner и CyberCop Scanner, также применяются разные способы именования уязвимостей.

Изучение проблемы классификации уязвимостей информационных ресурсов позволило Дэвиду Манну и Стивену Кристи выполнить работы, проводимые в CERIAS, в рамках которых была создана концепция единообразного именования уязвимостей. Эта концепция была сформулированна в отчете Towards a Shareable Vulnerability Database, представленном на конференции CERIAS Workshop for Vulnerability Databases, проведенной CERIAS в 1999 г.

CVE существенно упрощает задачу сравнения возможностей различных сетевых сканеров. Для CVE-совместимых сканеров достаточно сопоставить между собой списки обнаруживаемых уязвимостей. Если же сканеры используют для именования уязвимостей разные системы обозначений, то задача их сравнения становится совсем нетривиальной.

В настоящее время большинство разработчиков сетевых сканеров и других средств контроля защищенности, включая Symantec, NAI, ISS, Cisco и др., заявили о поддержке CVE в качестве стандартного способа именования уязвимостей в своих продуктах.

7.5.5 CIDF

Единая архитектура систем выявления атак CIDF (Common Intrusion Detection Framework) является инициативой, в рамках которой разрабатываются сетевые протоколы и интерфейсы прикладного программирования, предназначенные для взаимодействия компонентов IDS.

CIDF определяет следующее:

- модель данных для представления информации об атаках, уязвимостях, событиях и способах реагирования на события;
- модель взаимодействия компонентов IDS;
- протоколы и интерфейсы взаимодействия компонентов IDS.

В модели CIDF атаки и уязвимости описываются при помощи S-выражений. Чтобы понять, что это такое, не углубляясь в теорию, приведем пример S-выражения для события, связанного с удалением файла (см. листинг 2).

Листинг 2

```
Delete
    (Context
        (HostName 'first.example.com')
        (Time  '16:40:32 Jun 14 1998')
    )
    (Initiator
        (UserName 'lp')


        )
        (Source
            (FileName '/etc/passwd')
        )
    )
```

Данное S-выражение относится к событию, заключающемуся в том, что пользователь lp в 16:40:32 14 июня 1998 г. удалил файл /etc/passwd на компьютере first.example.com.

В настоящее время статус CIDF не определен, однако он остается концептуальной базой для разработки стандартов в области ID и, возможно, будет взят за основу при создании стандартов IDWG.

7.5.6 Рабочая группа IDWG

IDWG (Intrusion Detection Working Group) является рабочей группой IETF, сформированной для создания Internet-стандартов, в области выявления атак. IDWG решает задачу назначения общих форматов данных и протоколов взаимодействия и обмена информацией между различными компонентами IDS.

При создании рабочей группы IDWG перед ее участниками были поставлены следующие задачи:

- обоснованный выбор функциональных требований высокого уровня, задающих правила взаимодействия между системами выявления атак, а также между IDS и средствами сетевого управления;
- спецификация единого языка взаимодействия IDS, отвечающего этим требованиям и устанавливающего форматы обмена данными между IDS;
- составление документа, описывающего существующие протоколы взаимодействия между IDS, и предоставление возможности использования в этих протоколах единого формата обмена данными.

К настоящему времени силами рабочей группы IETF IDWG уже закончена разработка основных стандартов Internet на форматы и протоколы обмена данными между IDS.

Существующие проекты стандартов сети Internet, предложенные IDWG:

- Intrusion Detection Message Exchange Format Extensible Markup Language (XML) Document Type Definition;
- The TUNNEL Profile;
- The Intrusion Detection Exchange Protocol (IDXP).

IDMEF (Intrusion Detection Message Exchange Format) - формат обмена данными между компонентами IDS. Он служит для передачи предупреждающих сообщений о подозрительных событиях между системами выявления атак. Данный формат должен обеспечить совместимость между коммерческими и свободно распространяемыми IDS и их взаимодействие для поддержания наивысшего уровня защищенности.

Модель данных IDMEF описывается в виде XML DTD.

Сообщение сетевого сенсора/анализатора об атаке ping of death представлено в листинге 3. Имеется несколько объектов атаки. IP-адрес атакующего подделан.

Листинг 3

```
?xml version="1.0" encoding="UTF-8"?>
      sensor.bigcompany.com
   2000-03-09T10:01:25.93464Z
222.121.111.112
123.234.231.121
      lollipop
      Cabinet B10
   Cisco.router.b10
   CVE-1999-128
   http://www.cve.mitre.org/
```

Сообщение сетевого сенсора/анализатора о сканировании портов, представленное в формате IDMEF (элемент языка разметки <portlist> обозначает номера сканируемых портов), приведено в листинге 4.

Листинг 4

```
?xml version="1.0" encoding="UTF-8"?>
      Headquarters Web Server
   analyzer62.bigcompany.com
   2000-03-09T15:31:00-08:00
222.121.111.112
      www.bigcompany.com
123.234.231.121
   5-25,37,42,43,53,69-119,123-514
```

IAP (Intrusion Alert Protocol) - протокол прикладного уровня, предоставляющий возможность обмениваться сообщениями об атаках (alerts) компонентам системы выявления атак: сенсорам/анализаторам (S) и менеджерам (M), между которыми могут также находится proxy-сервисы (P) и шлюзы (G). Протокол не зависит от формата представления данных.

7.6 Возможности коммерческих IDS

7.6.1 Средства защиты информации компании Symantec

Компания Symantec является в настоящее время крупнейшим разработчиком программных средств защиты информации и наряду с IBM, CA, ISS, Cisco Systems, Check Point и некоторыми другими компаниями занимает лидирующее положение на рынке. Предлагаемые компанией Symantec программные продукты позволяют строить систему защиты корпоративной сети на базе интегрированных между собой инструментальных средств одного разработчика. Программные средства защиты информации Symantec ориентированы на корпоративных клиентов и включают следующие классы аппаратно-программных продуктов:

- межсетевые экраны и средства VPN (Symantec Enterprise Firewall/VPN);
- средства контроля защищенности (Symantec Enterprise Security Manager (ESM), Symantec NetRecon);
- системы обнаружения атак и аномалий (Symantec Intruder Alert, Symantec ManHunt);
- средства антивирусные и анализа контента (Symantec AntiVirus, Symantec Web Security);
- средства централизованного управления (Symantec Gateway Security, Symantec Client Security);
- средства администрирования (Symantec pcAnywhere, Symantec Ghost) и пр.

Продукты компании Symantec позволяют создавать комплексные системы выявления атак для защиты корпоративных сетей любого уровня сложности. Не претендуя на исчерпывающее описание функциональных возможностей, рассмотрим программный продукт Symantec Intruder Alert в качестве примера современных коммерческих IDS.

7.6.2 Symantec Intruder Alert

Назначение и основные возможности

Программный продукт Symantec Intruder Alert (ITA) является достойным представителем IDS системного уровня (host-based), построенных на технологии интеллектуальных программных агентов. Выявление локальных и удаленных атак осуществляется путем анализа журналов регистрации событий системного и прикладного ПО. Отличительные черты этой системы -

гибкость, масштабируемость и простота администрирования. ITA может быть легко интегрирован практически с любыми типами приложений.

Обнаружение атак и реагирование на них происходит в реальном времени, при этом предусмотрено 14 вариантов действий по автоматическому реагированию на атаки.

Значительное количество предопределенных политик безопасности сочетается с возможностью создания собственных политик без программирования.

В состав ITA входят программные агенты для 35 различных программно-аппаратных платформ, включая разные версии ОС UNIX, Windows и NetWare. По широте охвата платформ продукт не имеет себе равных.

Архитектура Intruder Alert и описание основных компонентов

ITA построен на распределенной трехкомпонентной архитектуре агент/менеджер/консоль. Все компоненты ITA взаимодействуют между собой по защищенному клиент-серверному протоколу. Аутентификация между компонентами и выработка сеансовых ключей осуществляется по алгоритму Диффи-Хелмана. Защита сеанса связи реализуется посредством алгоритма шифрования с 400-битными ключами.

Средства управления ITA представлены двумя графическими приложениями: ITA Admin и ITA View.

Приложение ITA Admin предназначено для управления компонентами системы, создания и настройки политик безопасности, определяющих правила выявления подозрительной активности и реагирования на нее. При помощи приложения ITA Admin администратор безопасности может производить следующий набор действий по администрированию системы обнаружения атак:

- объединять агентов в домены;
- формировать политики безопасности и применять их на контролируемых доменах;
- загружать новые политики безопасности с Web-сервера компании Symantec;
- экспортировать политики безопасности в файлы экспорта;
- настраивать параметры программных агентов;
- подключать дополнительные источники данных для анализа программными агентами;
- определять привилегии пользователей ITA и распределять административные роли по управлению системой выявления атак.

ITA View является средством просмотра регистрационной информации об атаках и других подозрительных событиях, зарегистрированных агентами ITA согласно установленным правилам политики безопасности. Данное средство позволяет составлять запросы к базе данных ITA содержащей консолидированные данные обо всех контролируемых системах, а также формировать на основании результатов запроса отчеты, представленные в различных графических форматах.

Центральным компонентом системы выявления атак является ITA Manager. Он занимается регулированием подключаемых к нему агентов, получая от них информацию о состоянии контролируемых объектов, поддерживает список доменов и активизированных на них политик безопасности и управляет базой данных безопасности. База данных безопасности содержит консолидированные данные о нарушениях безопасности на контролируемых объектах.

В ОС UNIX приложение ITA Manager реализовано в виде демона, представляет собой службу в ОС Windows NT и NLM-модуль в ОС NetWare.

ITA Agent является "рабочей лошадкой" системы выявления атак, выполняющей одновременно функции сенсора, анализатора и средства реагирования на атаки. В его функции входит сбор и анализ данных аудита безопасности из различных источников с использованием сигнатур атак, задаваемых правилами политик безопасности ITA В случае обнаружения в составе

исходных данных сигнатуры атаки предпринимается набор действий, предписываемый соответствующим правилом.

Выявление атак и реагирование на них происходит в реальном масштабе времени по специальным алгоритмам (в терминологии ITA - политики безопасности). В среде ОС UNIX агенты реализованы в виде демонов, в ОС Windows NT -в виде служб, а в NetWare представляют собой NLM-модули. Для каждой поддерживаемой ОС привлекаются собственные источники информации аудита. В системах UNIX и Windows события, связанные с безопасностью, фиксируются при помощи стандартных средств регистрации системных событий и средств аудита безопасности (syslog, wtmp, process accounting, btmp, подсистема C2 и т.п. в ОС UNIX и системный журнал, журнал приложений и журнал безопасности в ОС Windows NT). Сенсорные модули ITA Agent с определенной периодичностью сканируют файлы системных журналов и журналов аудита, считывают данные аудита и преобразуют их в свой внутренний формат. В NetWare сенсорные модули ITA Agent самостоятельно регистрируют и обрабатывают данные о событиях, получая эту информацию непосредственно от ядра ОС.

Процесс сбора информации о состоянии системы в среде UNIX показан на рис. 7.2. Intruder Alert автоматически проводит мониторинг следующих источников информации:

- файла syslog, содержащего данные от ядра ОС и приложений, которые регистрируются через систему syslog;
- файла wtmp, включающего информацию о пользователях, зарегистрировавшихся в системе, и запущенных ими процессах;
- файла btmp, в котором имеются сведения обо всех неудачных попытках входа в систему;
- системы учета пользовательских процессов pacct, регистрирующей различную информацию, связанную с их функционированием и использованием системных ресурсов;
- журналов аудита безопасности C2 (обращение к этому источнику возможно после специальной настройки ITA, поскольку подсистема аудита безопасности в различных реализациях UNIX устроена по-разному).

Помимо перечисленных источников информации, представляющих собой файлы, данные в которых хранятся в двоичном формате, возможно подключение дополнительных информационных источников, применяющих текстовый формат хранения данных, например файла /var/adm/messages и любых других текстовых файлов журналов регистрации событий ОС и приложений.

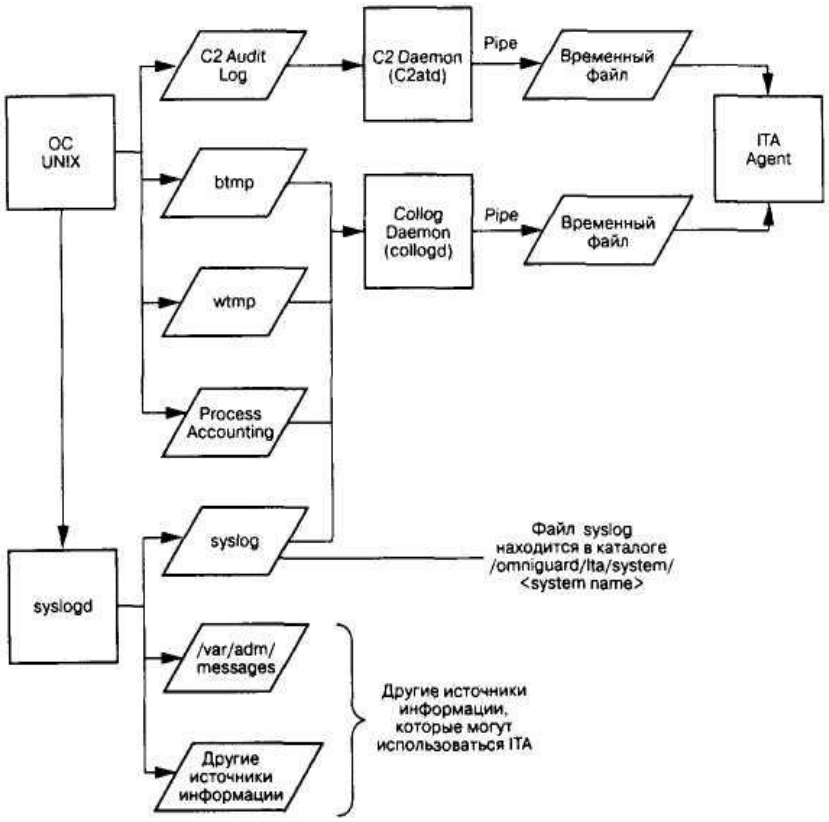


Рис. 7.2. Источники информации о событиях для ITA в ОС UNIX

Сведения из журналов регистрации событий собирает демон collogd и передает их агенту ITA по программному каналу. Сбор данных от подсистемы аудита безопасности C2 - функция демона C2atd, который преобразует эти данные во внутренний формат ITA и направляет агенту. По умолчанию сканирование источников информации происходит с интервалом в одну секунду.

Использование программного модуля FileWatch для контроля целостности системных файлов

Сценарий проведения многих атак предполагает подмену важных системных файлов «троянскими программами», заражение программ вирусами либо модификацию системных конфигурационных файлов с целью создания «черного входа» в систему. Для контроля целостности программной и информационной частей на контролируемых системах в составе ITA имеется специальный модуль под названием FileWatch, способный обнаруживать нарушения целостности, связанные с добавлением, удалением и модификацией файлов и каталогов. Нарушения целостности выявляются путем сравнения атрибутов этих файлов и каталогов с эталонными значениями. Отслеживание изменения содержимого файлов производится по контрольным суммам. Вычислять контрольные суммы файлов можно по различным алгоритмам, в том числе с помощью хэш-функций MD5.

Принцип функционирования модуля FileWatch представлен на рис. 7.3. Создаваемый пользователем FileWatch List определяет список контролируемых файлов, виды предпринимаемых проверок и их периодичность. База данных атрибутов файлов (File Attribute Database) формируется модулем FileWatch и содержит эталонные значения атрибутов файлов и контрольные суммы, служащие для проверки целостности. Сообщения о результатах проверок, выполняемых модулем FileWatch, передаются агенту ITA, который обрабатывает их в соответствии с заданной политикой безопасности. Чтобы агент ITA мог воспринимать и обрабатывать сообщения FileWatch, а также реагировать на них, на нем должна быть активизирована специальная политика безопасности (UNIX Critical Files для UNIX и NT Critical Files для Windows NT).

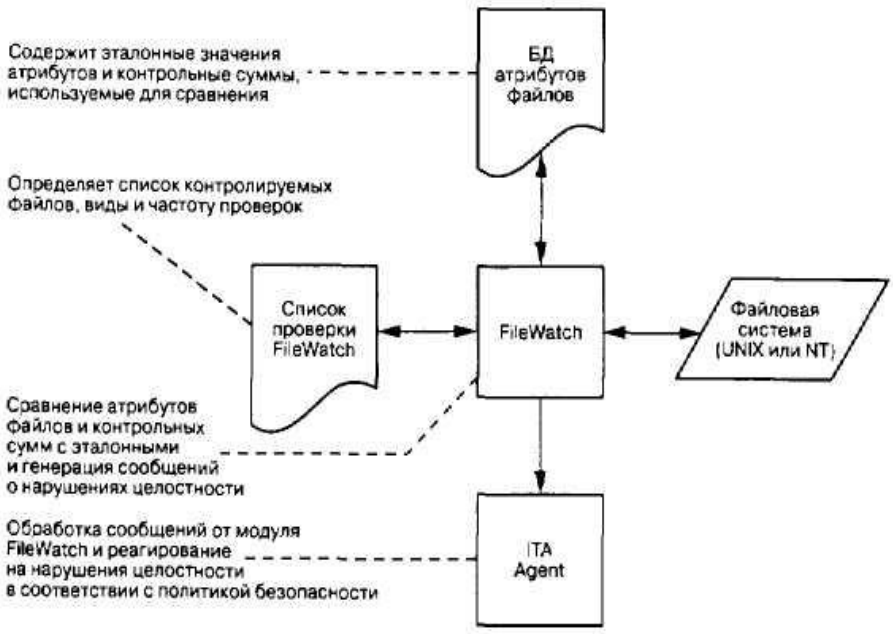


Рис. 7.3. Контроль целостности системных файлов при помощи модуля FiSeWatch

Политики безопасности Intruder Alert

Политика безопасности Intruder Alert описывается набором правил. Правила представляют собой логические выражения, построенные на предикатах первого порядка. Посредством предикатов определяются условия возникновения отслеживаемых ситуаций, а логические выражения задают способы реагирования в зависимости от истинности или ложности предикатов.

Правила политики безопасности

Правило политики безопасности - это импликация трех логических высказываний: предиката SELECT, предиката IGNOR и логического высказывания ACTION. Предикат SELECT определяет условия возникновения отслеживаемой ситуации, предикат IGNOR - исключения из этих условий, а логическое высказывание ACTION предписывает выполнение одного из 14 действий по реагированию на возникшую ситуацию.

На языке алгебры логики правило политики безопасности устанавливается тождеством:

ACTION = SELECT $\rightarrow$ IGNOR.

В табл. 7.1 показано, как выглядит таблица истинности данной логической функции.

Таблица 7.1. Таблица истинности логической функции ACTION

SELECT	IGNOR	ACTION
True	False	True
True	True	False
False	False	False
False	True	False

Истинность высказывания ACTION означает необходимость выполнения действий, предписываемых этим высказыванием. Высказывание ACTION бывает простым или составным, во втором случае оно может состоять из нескольких высказываний, разделенных операцией $\wedge$ (логическое «И»):

ACTION = Действие1 $\wedge$ Действие2 $\wedge$ ... Действие N, N ={ 1,14}.

В табл. 7.2 описаны способы реагирования на попытки НСД, поддерживаемые ITA

Таблица 7.2. Способы реагирования на попытки НСД, поддерживаемые программой ITA

Название способа	Назначение
Execute Command	Выполнить команду операционной системы, файл сценария или исполняемый файл
Record To ITA View	Поместить запись с данными о событии в базу данных безопасности менеджера ITA
Disable User Account	Заблокировать регистрационную запись пользователя
Run Shared Actions	Выполнить действие, определяемое другим правилом политики безопасности, активизированной на агенте ITA

Ранжирование попыток НСД

Правила политики безопасности ранжируются с целью определения степени критичности тех или иных событий, происходящих в системе. Каждому правилу присваивается номер в диапазоне от 0 до 100. Все события, отслеживаемые правилами политики безопасности, в зависимости от их приоритета делятся на три уровня критичности (обозначаемые на диаграммах ITA различными цветами) в соответствии с табл. 7.3.

Таблица 7.3. Уровни приоритетов событий, отслеживаемых программой ITA

Приоритет	Уровень критичности	Угроза безопасности
0-33	Зеленый	Некритичные события, не требующие немедленного реагирования
34-66	Желтый	Критичные события средней важности, требующие реагирования
67-100	Красный	Критичные события высокой важности, представляющие серьезную угрозу безопасности и требующие немедленного реагирования

Предопределенные политики безопасности

ITA содержит базовый набор предопределенных политик безопасности для каждой из поддерживаемых операционных систем, который устанавливается вместе с продуктом. Часть предопределенных политик безопасности активизируется сразу же после загрузки ITA. Остальные требуют дополнительной настройки.

Например, политика ITA Reports генерирует отчеты о работе программного агента при получении им команды report от ITA View (ITA View позволяет также управлять ITA-агентами путем посылки им команд по сети). Политика UNX Failed telnet служит для выявления неудачных попыток удаленной регистрации в системе Solaris 2.5 с применением сервиса telnet, а посредством политики UNX System Problems обнаруживаются проблемы, возникающие при выполнении системных задач, таких как неудачная операция монтирования тома, истечение времени ожидания ответа на запрос, неверный IP-адрес или MAC-адрес. Для ОС Windows NT политика NT SYN Flood отыскивает атаки «отказ в обслуживании» SYN Flood, а политика NT Guest User Logon регистрирует случаи локального или удаленного входа пользователя с именем «Гость» в систему.

Часть предопределенных политик перед активацией должны быть дополнительно настроены. Среди них политика APACHE HTTP Start/Stop, обнаруживающая запуск и останов Web-сервера Apache 1.1.1, и политика Cisco Config Change, выявляющая изменение конфигурации маршрутизатора Cisco v11.1.

7.6.3 Пример использования Symantec IDS

Типовая схема размещения средств поиска атак компании Symantec для защиты корпоративной сети, подключенной к Internet, приведена на рис. 7.4. Состав, конфигурация и размещение отдельных компонентов IDS определяются по результатам обследования безопасности и анализа рисков.

Агенты ITA размещаются на всех контролируемых системах корпоративной сети, включая серверы и рабочие станции, и проводят мониторинг системных журналов и журналов приложений,

находя различные виды аномальной активности. Пользовательские рабочие станции, как правило, являются менее критичными элементами информационной инфраструктуры, поэтому на них устанавливаются облегченные версии агентов, обозначенных на рис. 7.5, как ITA Workstation Agents. Чтобы контролировать события, происходящие при функционировании

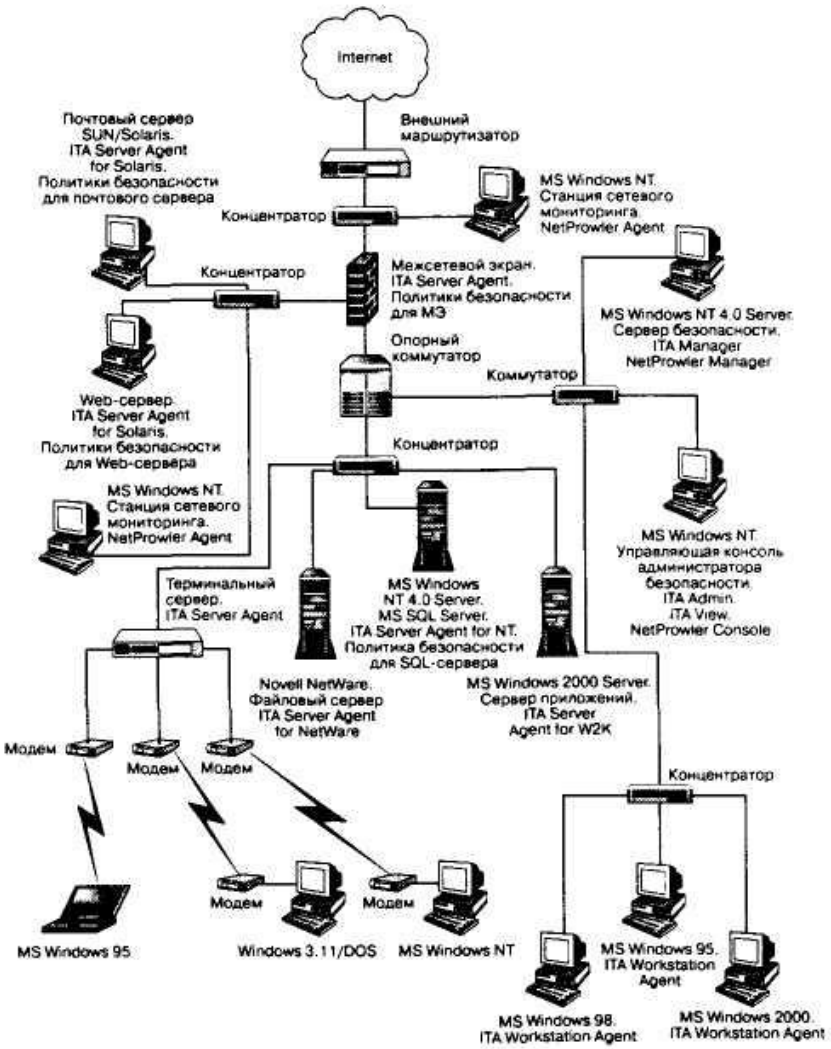


Рис. 7.4. Применение средств выявления атак компании Symantec для защиты корпоративной сети

прикладных подсистем, на серверных агентах ITA активизированы специализированные политики безопасности для МЭ, почтового и Web-серверов, а также для SQL-сервера.

Ядром системы выявления атак является сервер безопасности, на котором функционируют ITA Manager. На сервере безопасности накапливается вся информация о событиях, происходящих в сети, поступающая от агентов. Здесь размещается вся конфигурационная информация IDS, в том числе сигнатуры атак и политики безопасности. С сервера безопасности осуществляется управление всеми агентами IDS путем отправки им управляющих сообщений.

Конфигурирование системы выявления атак, создание собственных сигнатур атак и политик безопасности, просмотр и анализ данных аудита, а также генерация отчетов производится с управляющей консоли администратора безопасности, на которой устанавливаются графические средства администрирования ITA Admin и ITA View. Данные приложения реализуют интерфейс для взаимодействия администратора с сервером безопасности.

7.7 Тенденции развития

Для решения задачи защиты от сетевых атак необходима концепция, определяющая объекты защиты, цели, задачи и основные принципы защиты, а также состав и последовательность работ по предупреждению и выявлению атак и реагированию на них.

Достаточно простым и эффективным подходом к обеспечению защиты внешнего периметра, который хотелось бы порекомендовать, является обращение к публикуемому институтом SANS списку (http://www.sans.org/topten.htm) десяти уязвимостей (Top Ten List), чаще всего подвергающихся атакам. (Данный список содержит описание уязвимостей, которыми более чем в 80% случаев пользуются хакеры, предпринимающие сетевые атаки, и способов их ликвидации.) Большинство хакеров не утруждают себя поиском уникальных уязвимостей конкретных хостов. Вместо этого, располагая небольшим арсеналом средств для осуществления атак, они просто сканируют сети, надеясь найти одну из известных им уязвимостей. Современные сетевые сканеры способны обнаруживать эти уязвимости. Выявление и ликвидация таких уязвимостей может существенно затруднить жизнь современным взломщикам сетей. Им придется прибегать к новым более изощренным способам взлома, пополнять свой арсенал атакующих средств, разрабатывая новые методы и средства. Это значительно сузит круг возможных взломщиков и уменьшит общее количество предпринимаемых ими атак.

В настоящее время список наиболее часто атакуемых уязвимостей расширен и включает порядка 20 уязвимостей (http:/www.sans.org/top20.htm).

Конечно, предложенный подход не отличается полнотой и не в состоянии обеспечить защиту от многих видов сетевых атак. Комплексная концепция защиты сети от внешних атак предполагает проведение следующих мероприятий:

- разработку политики контроля сетевого доступа;
- анализ рисков и уязвимостей, использование положительного опыта и существующих решений по обеспечению безопасности;
- создание инфраструктуры (назначение ответственных, распределение ролей и т.п.);
- проектирование системы защиты, определение требований, предъявляемых к установленным средствам и механизмам защиты;
- выделение ресурсов, ранжирование выбранных контрмер по степени важности и реализация приоритетных;
- проведение аудита и периодического тестирования эффективности принятых контрмер;
- формирование и сопровождение системы выявления атак и реагирования на них.

Приложение 1
Исследование состояния информационной безопасности в мире

Введение

Это первое исследование, посвященное вопросам состояния информационной безопасности (ИБ), предпринятое KPMG (Российский член KPMG International, Швейцарская ассоциация, перевод 2002 г.). Спонсорами исследования выступили компании Check Point, Symantec, RSA и InfoSecurity Magazine.

Исследование проходило в начале 2002 г. Результаты распределены по следующим регионам: Европа, включая Ближний Восток и Африку (EMEA), Азиатско-Тихоокеанский регион и Американский континент. Такое распределение облегчает сравнение на региональном уровне.

В ходе исследования было проведено 641 телефонное интервью с руководящими работниками, отвечающими за информационную безопасность в организациях из основных секторов экономики (см. табл. П1.1).

Таблица П1.1. Число участников исследования

Респонденты	%
Директора службы информационных технологий (ИТ)	14
ИТ-менеджеры	38
Сотрудники службы информационной безопасности	10
Кураторы ИТ (Chief Information Officer - CIO)	7
Начальники службы информационной безопасности	8
Директора/начальники операционной службы	4
Руководители отделов системного сопровождения/администраторы сетей	9
Другие	10

Исследование охватывало крупные организации, объем продаж которых (или аналогичный показатель для организаций государственного сектора) превышаеТ50 млн. долл.

Данные о размере организаций представлены в табл. П1.2 и П1.3.

Таблица П1.2. Количество сотрудников в организации

Число сотрудников	%
<100	4
101-500	16
501-1000	17
1001-5000	31
5001-10000	10
10001-50000	15
50001-100000	5
100001+	2

Таблица П1.3 Оборот организации

Оборот, млн. долларов	%
50-100	28
101-500	41
501-1000	11
1000-5000	10

5000+	10

Получена представительная выборка организаций из основных коммерческих и государственных секторов, результаты сгруппированы для облегчения сравнения по следующими критериям (табл. П1.4):

- • финансовый сектор;
- • промышленность и торговля;
- • коммуникации и сфера услуг;
- • государственный сектор и инфраструктура.

Таблица П1.4. Области деятельности предприятий

Финансовый сектор		Промышленность и торговля		Коммуникации и сфера услуг		Государственный сектор и инфраструктура	
Кредитные организации	15%	Добывающая промышленность	2%	Общественное питание и гостиничное хозяйство	3%	Строительство	5%
Страхование	7%	Машиностроение	12%	ИТ	4%	Коммунальные услуги	5%
		Химическая промышленность	3%	Телекоммуникации	3%	Транспорт	8%
		Розничная торговля	4%	Профессиональные услуги	10%	Государственный сектор	7%
		Оптовая торговля	5%	СМИ	7%		

Респонденты отвечали на следующий вопрос: с какой наиболее существенной, с их точки зрения, проблемой в области ИБ сталкиваются организации? Полученные ответы перечислены в табл. П1.5.

Таблица П1.5. Ответы респондентов

Проблемы в области ИБ	%
Инциденты с компьютерными вирусами	22
Атаки со стороны хакеров	21
Контроль удаленного доступа	17
Безопасность при работе с Internet	10
Нарушение конфиденциальности личной информации	5
Недостаточный уровень обучения пользователей	5
Безопасность систем электронной коммерции B2B	5
Мошенничество со стороны сотрудников	4
Похищение или повреждение данных/информации	4
Прочее	7

Нарушения системы ИБ

Респондентов спросили, пострадали ли в прошлом году от нарушений системы ИБ их организации, и если да, то какой финансовый ущерб они понесли, сколько в результате было потеряно человеко-дней (см. табл. П1.6).

Таблица П1.6. Нарушения системы ИБ

Виды инцидентов	Число организаций, сообщивших о нарушениях	Доля пострадавших от нарушений, %	Среднее число потерянных дней за год	Средний размер убытков за год, тыс. долл. США	Наибольший зарегистрированный убыток за год, млн. долл. США

Инциденты с компьютерными вирусами	390	61	68	162	10
Хищение оборудования ИТ	246	38	21	98	3
Проникновение через электронную почту (например, посредством спама)	183	29	12	16	0,2
Утрата программного обеспечения	102	16	19	104	3
Атаки, направленные на сбой систем при обслуживании клиентов	91	14	24	53	0,5
Взлом сайта	79	12	84	32	0,2
Критичный системный сбой	79	12	80	155	4
Утрата документов организации (на бумажных носителях)	78	12	11	37	0,2
Утрата конфиденциальных данных	35	5	18	197	1,5
Подмена исходных данных и результата	23	4	14	14	0,1

Комментарий KPMG

Доля не зарегистрированных, не оцененных с точки зрения величины принесенного ущерба или неточно оцененных нарушений велика. И это беспокоит, поскольку заставляет предположить, что реальные цифры нарушений и убытков могут быть еще выше (например, в отношении вирусов 19% организаций не знают, сколько было потерянно времени, 42% не представляют себе размеров финансовых потерь). В тех случаях, когда организации не определяют размер издержек, связанных с нарушениями системы ИБ, они также не могут рассчитать, окупают ли себя ранее принятые ими защитные меры.

Профилактика лучше, чем лечение. В среднем прямой ущерб, понесенный каждой организацией, составляет 108 000 долл. Кроме того, существуют косвенные издержки, связанные с простоем и уменьшением производительности персонала, а также с необходимостью совершенствования системы информационной безопасности после конкретного нарушения (что обычно гораздо дороже, чем создание системы ИБ). Если добавить к этому ущерб репутации в результате неполадок в системе ИБ, то общий размер последствий может оказаться огромным. В итоге дешевле и менее болезненно осуществить эффективное инвестирование в предупреждение нарушения, нежели устранять ущерб после происшествия (см. табл. П1.7).

Таблица П1.7. Модель KPMG

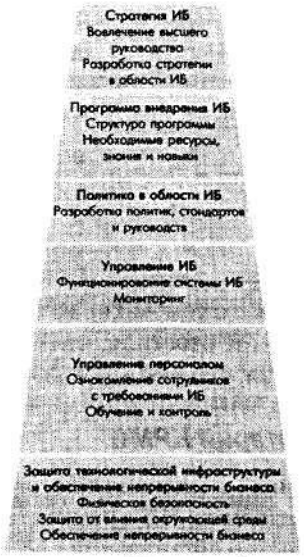
Модель KPMG

1. Комплексный подход к построению системы ИБ организации, интегрированный с задачами по ее обеспечению
2. При недостаточной эффективности хотя бы одного звена пирамиды в системе ИБ возникают бреши
3. Модель нацелена на совершенствование каждого звена, чтобы немедленно реагировать на ситуации, сопряженные с высоким риском, при одновременном построении фундамента для будущего развития

Для удобства результаты нашего исследования классифицируются в соответствии с данной моделью

Преимущества

1. По мере роста организации и развития ее связей с внешним миром в той же степени совершенствуется система безопасности
2. Модель позволяет легко интегрировать тактические решения с общим стратегическим курсом развития



Все звенья системы ИБ должны быть развиты пропорционально и в достаточной мере

Вовлечение высшего руководства

Для постановки правильных целей в области ИБ, способствующих деятельности организации и ее развитию без ущерба, необходимо непосредственное участие ее высшего руководства. Руководство должно обеспечить функцию безопасности надлежащим уровнем инвестирования и ресурсов, а также оценивать ее эффективность.

Респондентам был задан ряд вопросов, ответы на которые позволили составить мнение о степени внимания руководства к проблемам ИБ. Например, о бюджетах службы ИБ, уровне соблюдения требований ИБ и осведомленности о них высшего руководства организаций.

Респондентов спросили, какая часть от общего бюджета ИТ была потрачена на ИБ в прошлом году и увеличится или уменьшится эта доля в следующем году.

В результате удалось установить, что в среднем на безопасность ИТ было израсходовано 2,6 млн. долл., из них около 10,1% бюджета ИТ пришлось на ИБ (на финансовый сектор - 11,6%, на промышленность и торговлю - 8,3%, на коммуникации и сферу услуг - 11,6%, на госсектор и инфраструктуру - 8,7%) - см. табл. П1.8.

Таблица П1.8. Бюджет на ИБ

% от бюджета ИТ	Потрачено на ИБ, %
1-5	46
5-10	31
10-15	7
15-20	6
20-25	3
25-30	3
30-35	0
35-40	2
40-45	0
45-50	2

На вопрос о том, какие изменения возможны в бюджете в следующем году, 63% респондентов ответили, что он, вероятно, возрастет, а 10% - что уменьшится. Те, кто полагал, что бюджет возрастет, в среднем оценили этот рост в 19%.

Комментарий KPMG

В условиях замедления темпов экономического роста появляется соблазн уменьшить расходы на ИБ в рамках общего сокращения издержек. Однако тот факт, что большинство организаций рассчитывает на увеличение бюджетов на ИБ в следующем году, показывает, насколько за последние несколько лет возросло внимание к управлению информационными рисками. Это отчасти объясняется повышенным интересом к вопросам ИБ в связи с последними террористическими актами, а также значительным повышением требований со стороны регламентирующих органов и деловых партнеров. Обстоятельства подтверждают необходимость и своевременность увеличения затрат на ИБ, так как инциденты, связанные с нарушением ИБ, становятся более частыми и более обременительными в финансовом отношении.

Степень вовлечения высшего руководства

Следующий вопрос респондентам формулировался так: кто и на каком уровне отвечает за информационную безопасность в их организациях?

Оказалось, что почти в половине организаций ответственность за информационную безопасность была определена на уровне Совета директоров. Такое положение характерно в основном для организаций финансового сектора (см. табл. П1.9).

Таблица П1.9. Степень вовлечения руководства

Направление деятельности организации	Степень вовлечения, %
Финансовый сектор	60
Промышленность и торговля	43
Коммуникации и сфера услуг	52
Госсектор и инфраструктура	42

В 53% случаев ответственность за поддержание ИБ находится в пределах функции ИТ и возложена на директора/менеджера отдела ИТ или на руководителя отдела системного обеспечения.

В четырех организациях сказали, что за ИБ никто конкретно не отвечает!

Комментарий KPMG

Несмотря на участившиеся случаи упоминания в прессе громких нарушений систем ИБ, многие организации все еще рассматривают информационную безопасность как технический вопрос «битов и байтов», который относится к компетенции специалистов по технологиям. Однако причиной многих типичных нарушений системы ИБ является не технология, а люди. Пользователи небрежно относятся к хранению паролей, забывают корректно настроить параметры безопасности в эксплуатируемых системах. Без понимания высшим руководством важности информационной безопасности последняя будет оставаться техническим вопросом и не получит достаточного обеспечения ресурсами и соответствующего отношения, что необходимо для эффективной минимизации рисков.

Кроме того, определение «узких мест» в информационной защите и последствий нарушения системы ИБ требует координации со стороны высшего руководства, в том числе принятия на себя части ответственности. Поиск виноватого, в свою очередь, приводит к сокрытию проблем до возникновения более серьезных нарушений в системе ИБ, «крайним» за которые становится отдел ИТ.

По степени вовлечения высшего руководства в вопросы ИБ лидирует финансовый сектор, традиционно более серьезно относящийся к данному вопросу, - отчасти из-за предписаний регулирующих органов, отчасти из-за понимания того, что финансовые транзакции нуждаются в большей защите, чем другие типы электронной информации. Однако по мере того, как мир становится все более взаимосвязанным, значительно возрастают риски в отношении всех типов информации и организациям следует уделять внимание ИБ без принуждения к этому со стороны законодательства.

Формальные критерии оценки функционирования системы ИБ

Респондентов спросили, есть ли у них формализованная система оценки эффективности работы системы безопасности.

Выяснилось, что только 35% организаций в настоящее время оценивают эффективность системы безопасности с помощью формализованных критериев.

В финансовом секторе 42% организаций уже пользуются формализованными критериями и еще 17% планируют их вводить, но это очень мало (см. рис. П1.1).

А в вашей организации есть формальные критерии оценки эффективности ИБ?

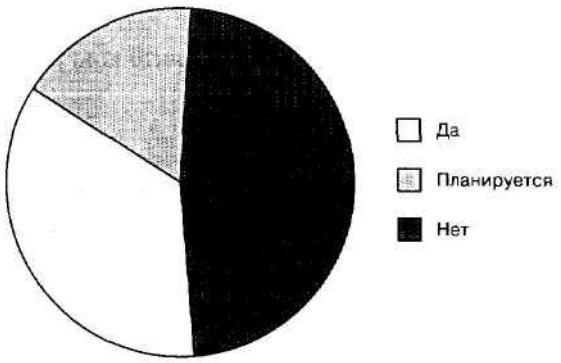


Рис. П1.1. Организации, использующие критерии эффективности

Комментарий KPMG

Формализованные критерии оценки системы ИБ важны, поскольку позволяют организации отслеживать, насколько успешно работает система ИБ, исходя из конкретных показателей результативности, эффективности и рисков, таких как число нарушений, соблюдение политики в рамках организации, качество работы в зависимости от бюджета и уровни риска. Не имея возможности анализировать эти виды показателей эффективности, нельзя утверждать, что информационные ресурсы компании достаточно защищены. Без четких критериев и ясной отчетности трудно обеспечить надлежащее внимание высшего руководства к вопросам ИБ.

Один участник опроса сказал: «Необходимо, чтобы капиталовложения, которые вы делаете, окупались. Надо обязательно определить количество имевших место нарушений и то, как быстро устранялись их последствия, а также оценить, улучшаются или ухудшаются эти показатели».

Определить оптимальные затраты на ИБ поможет использование формализованных критериев и методик, например сбалансированной карты оценок безопасности.

Американский континент занимает первое место по сбору и оценке параметров эффективности работы систем безопасности (см. рис. П1.2). Возможно, это объясняется тем, что организации в этом регионе традиционно придерживаются формализованного подхода к оценке эффективности менеджмента и применяют этот подход по отношению ко всем сферам управления в организации. Пожалуй, неожиданным является то, что в промышленности и торговле этого региона показатели наихудшие: 60% опрошенных не применяют формализованные критерии.

Используют критерии оценки эффективности в финансовом секторе 42%, в сферах коммуникаций и услуг - 43%, в государственном секторе и организациях инфраструктуры - 49% опрошенных.

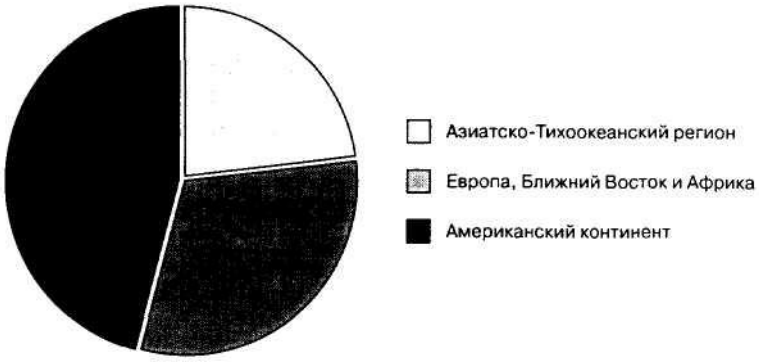


Рис. П1.2. Использование оценок эффективности ИБ

Комментарий KPMG

Мониторинг позволяет организации идентифицировать проблемные участки, а затем осуществить необходимые усовершенствования, задействовав финансовые ресурсы и персонал.

Изменение эффективности работы системы ИБ

У респондентов спросили, какие критерии в их организациях служат для оценки эффективности систем ИБ.

Было установлено, что среди организаций, применяющих формализованный подход к оценке эффективности работы системы ИБ, приняты критерии, приведенные в табл. ШЛО.

Таблица П1.10. Критерии оценки эффективности системы ИБ

Критерии оценки	Эффективность, %
Корпоративные стандарты контроля собственной разработки	43
Замечания аудиторов	40
Стандарты лучшей мировой практики (например, BS 7799/ISO 17799)	29
Число инцидентов в области безопасности	22
Финансовые потери в результате инцидентов	22
Расходы на ИБ	16
Эффективность в достижении поставленных целей	14

Комментарий KPMG

Среди немногих организаций, оценивающих эффективность работы системы безопасности посредством формализованных критериев, почти нет таких, которые обращались бы к комплексной методологии, объединяющей различные подходы. Лишь совсем незначительное число из них работают с экономическими показателями, такими как оценка снижения издержек и повышения эффективности.

Контроль и регистрация инцидентов в области ИБ

Далее респонденты отвечали на вопрос о том, ведется ли формальная регистрация инцидентов, связанных с нарушением ИБ. Полученный результат отражен на рис. П1.3.

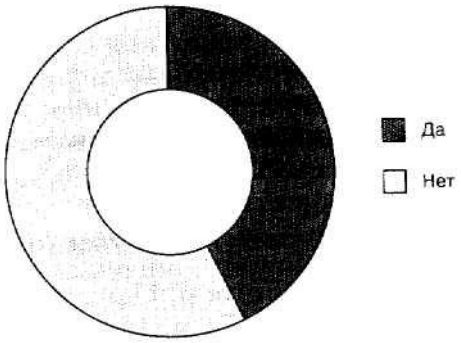


Рис. П1.3. Регистрация инцидентов ИБ

Комментарий KPMG

Только 34% респондентов проводят формальную регистрацию инцидентов в области ИБ. Остальные организации не имеют информации о числе инцидентов и, соответственно, не могут судить о величине понесенного ими ущерба. Статистика контроля и регулирования происшествий образует ядро оценки эффективности работы системы ИБ, и на ее основе должны формироваться требования к дальнейшему совершенствованию этой системы. Незнание того, что фактически происходит внутри организации, ведет к неверной расстановке приоритетов и, возможно, к неэффективному расходованию средств.

Меры воздействия на нарушителей ИБ

Респондентов спросили, принимают ли они формальные меры против нарушителей системы безопасности: дисциплинарные наказания собственных сотрудников или судебное преследование внешних нарушителей. В табл. П1.11 показаны результаты опроса.

Таблица П1.11. Процент применения мер против нарушителей системы безопасности

Меры	Азиатско-Тихоокеанский регион, %	Европа, Ближний Восток и Африка, %	Американский континент, %
Против внутренних нарушителей	71	83	76
Против внешних нарушителей	61	71	68

Комментарий KPMG

Бездействие в отношении злоумышленников укрепляет их в мысли, что нарушения системы ИБ незначительные и не влекут за собой наказания. Это способствует продолжающемуся увеличению числа людей, пытающихся взламывать корпоративные системы или осуществлять несанкционированный доступ к ним. Они надеются, что вероятность их поимки весьма низка, а наказание будет минимальным или вовсе не последует.

Результаты исследования показывают, что организации принимают меры скорее против собственных сотрудников, нежели против внешних нарушителей. Возможно, это отчасти обусловлено опасением нанести урон репутации организации в результате оглашения факта нарушения системы ИБ - гораздо легче приструнить сотрудника, не слишком привлекая к этому общественное внимание.

Еще одна причина, по которой организации неохотно идут на преследование нарушителей, заключается в трудности их идентификации и сбора доказательств, которые можно было бы предъявить в суде. Зачастую при происшествии приоритетом является не поиск доказательств, а восстановление функционирования систем. К тому же не исключено, что доказательства факта нарушения окажутся уничтоженными.

Программа внедрения ИБ

Программа внедрения ИБ является комплексом мероприятий и видов деятельнос ти, которые обеспечивают реализацию стратегии информационной безопасности Респондентам был задан ряд вопросов, относящихся к квалификации и опыт) сотрудников в области ИБ, а также к организации этих ресурсов и управлении: ими.

Численность персонала службы ИБ

Респондентов спросили, какое количество сотрудников выполняют обязанности связанные с ИБ.

Из полученных ответов следует, что численность персонала, занятого в службе ИБ, приблизительно пропорциональна размеру организации (в расчет принималась общая численность сотрудников и объем продаж в организации) - см табл. П1.12 и П1.13.

Таблица П1.12. Численность персонала в службе ИБ

Общая численность сотрудников, чел.	Средняя численность штата службы ИБ, чел.
<1000	4,89
1001-10000	9,38
10 001-50000	20,76
>50000	39,21

Таблица П1.13. Штат службы ИБ

Объем продаж, млн. долл.	Средняя численность штата службы ИБ, чел.
50-100	5,5
101-500	10,02
>500	20,55

При этом были выявлены региональные расхождения, которые невозможно объяснить различием в размерах организаций. В европейских организациях в службах ИБ в среднем занято вдвое меньше персонала, чем в азиатско-тихоокеанских и американских. Персонал служб ИБ организаций госсектора и инфраструктурных отраслей составляет 2/3 персонала службы безопасности всех других секторов.

Неожиданным оказалось и то, что в организациях финансового сектора численность персонала ИБ в среднем не намного больше, чем в других секторах.

Комментарий KPMG

Численность персонала в службах ИБ выступает показателем того, какое значение организация придает вопросам безопасности. Эта численность должна определяться исходя из задач, поставленных перед службой ИБ. А масштаб задач зависит от размера организации, от наличия или отсутствия крупных изменений в системах ИТ и в деятельности организации и от степени интенсивности развития самой системы безопасности.

Квалификация персонала службы ИБ

Респондентам было предложено перечислить, какие квалификационные удостоверения (сертификаты) в области ИБ они имеют.

Оказалось, что 73% сотрудников вообще не имеют никаких формальных сертификатов, подтверждающих их квалификацию в вопросах обеспечения информационной безопасности.

Комментарий KPMG

Самое большое число сотрудников службы ИБ, имеющих удостоверение «Сертифицированный специалист по безопасности информационных систем» (CISSP), отмечено на Американском континенте. Этот сертификат стал выдаваться раньше всего в США, где он был изначально разработан. Такая сертификация постепенно получает распространение в Азиатско-Тихоокеанском регионе и Европе. В целом установлено, что среди ответственных за информационную безопасность лишь немногие имеют соответствующее квалификационное удостоверение (см. табл. П1.14).

Таблица П1.14. Сертификация службы ИБ

Квалификационное удостоверение	В среднем, %	Азиатско-Тихоокеанский регион, %	Европа, Ближний Восток и Африка, %	Американский континент, %
CISSP	8	3	8	14
Университетский диплом по специальности «Информационная безопасность»	5	4	5	7
Сертификация производителя или поставщика средств защиты	7	6	8	7
Прочие документы	7	3	9	8

Респондентов попросили указать, сколько лет работают в области ИБ те, кто за нее отвечает.

Результаты приведены в табл. П1.15.

Таблица П1.15. Стаж работы в области ИБ

Регион	Год или меньше	2-5 лет	6-10 лет	>10 лет
Азиатско-Тихоокеанский регион, %	12	54	22	13
Европа, Ближний Восток и Африка, %	13	42	23	22
Американский континент, %	12	55	15	19

Комментарий KPMG

Формальная сертификация углубляет и расширяет знания, но их нужно применять на практике, подкрепляя опытом работы. Большинство руководящих сотрудников по ИБ не имеет ни длительного опыта, ни соответствующих сертификаций или квалификаций. Возможно, это объясняется сравнительной молодостью профессии как таковой и связанным с этим дефицитом опытных специалистов, которые могли бы занять руководящие должности.

Независимость службы информационной безопасности от ИТ

Затем респонденты отвечали, является ли служба ИБ выделенной структурой в организации, управляемой независимо от службы ИТ (см. рис. П1.4).

Выяснилось, что в финансовом секторе больше организаций, в которых эти две службы управляются раздельно: 45% против 29% в промышленности и торговле.

Большинство организаций в Азиатско-Тихоокеанском регионе рассматривают безопасность информации как функции ИТ, причем 77% осуществляют совместное управление ИБ и

безопасностью ИТ (в Европе, на Ближнем Востоке и в Африке таких организаций 59%, на Американском континенте - 55%).

Комментарий KPMG

Целенаправленные усилия компаний в деле дальнейшего повышения эффективности ИТ должны привести к разумным затратам на информационную безопасность.

Политика в области ИБ

Политики ИБ, соответствующие стандарты и правила безопасности определяют перечень целей и требований ИБ, которые необходимо довести до сотрудников.

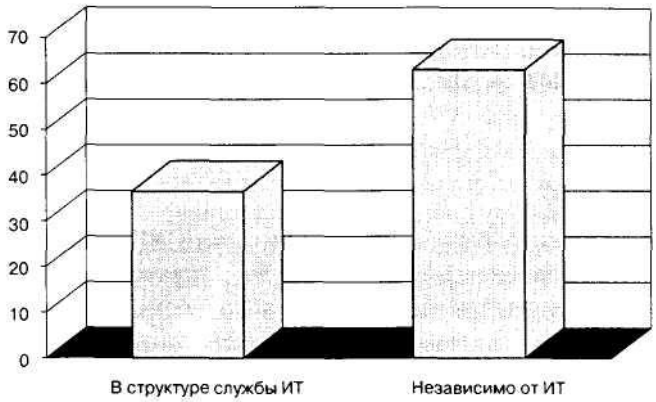


Рис. П1.4. Место службы ИБ в организации

Был задан ряд вопросов, относящихся к сфере и границам применения политик, стандартов и правил.

Респондентов спросили, утверждена ли политика ИБ Советом директоров.

Было установлено (см. рис. П1.5), что в большинстве организаций в Европе, на Ближнем Востоке и в Африке политика утверждена или находится в процессе утверждения на этом уровне, а в большинстве организаций Азиатско-Тихоокеанского региона - нет. Кроме того, оказалось, что более чем в половине организаций

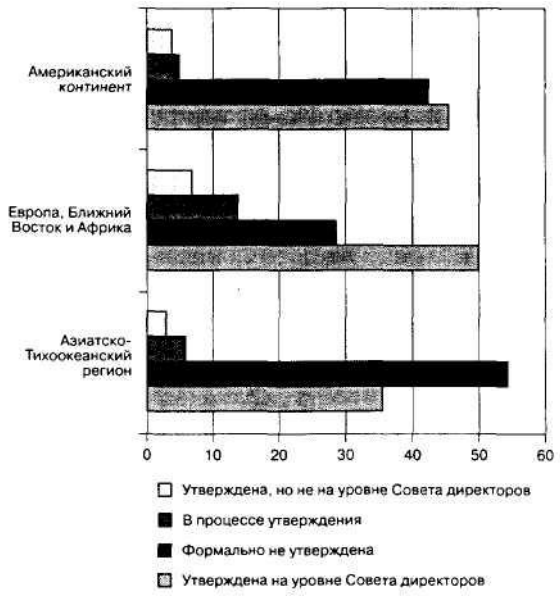


Рис. П1.5. Утвержденные политики ИБ

промышленного сектора и сферы услуг политика безопасности Советом директоров утверждена (в промышленности и торговле - 53% организаций, в госсекторе и инфраструктуре - 41%, в сферах коммуникации и услуг - 43%, в финансовом секторе - 46%).

Комментарий KPMG

Информационная безопасность - проблема не только ИТ. Недостаточный уровень информационной безопасности может привести к утрате репутации, сокращению рыночной доли, росту издержек и снижению доходности. В лучших организациях существует политика ИБ, охватывающая все сегменты деятельности, а не только ИТ (см. рис. П1.6). Один из респондентов самую серьезную проблему в системе ИБ сформулировал следующим образом: «Недостаточная осведомленность руководства о необходимых условиях обеспечения информационной безопасности». Содействие на уровне Совета директоров поддержанию ИБ способствует увеличению осведомленности о требованиях ИБ и, таким образом, приводит к общему улучшению практического обеспечения безопасности внутри организации.

55% респондентов Азиатско-Тихоокеанского региона ответили, что у них нет политики безопасности, утвержденной Советом директоров.

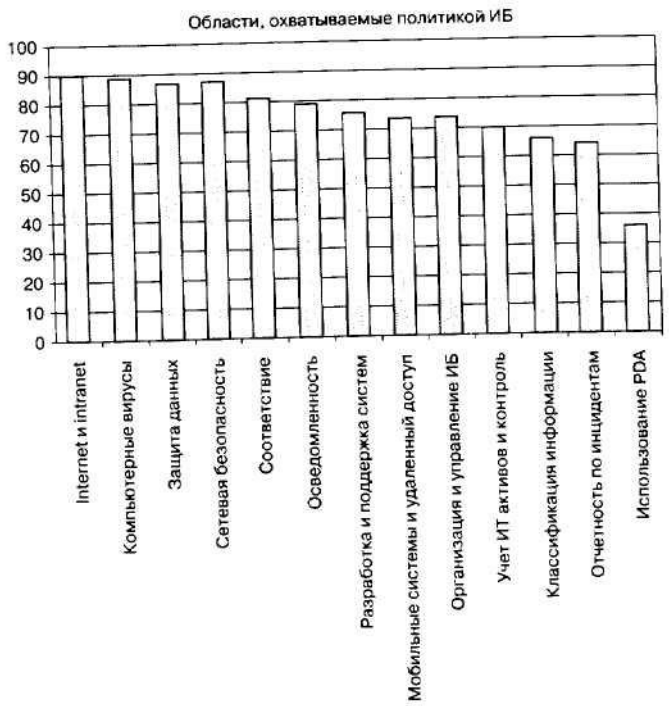


Рис. П1.6. Границы политики ИБ

Области, охваченные политикой ИБ

Респондентов попросили перечислить области, которые охвачены принятой у них политикой информационной безопасности.

Выяснилось, что в основном это сферы, доставившие больше всего хлопот и причинившие наибольший ущерб за последние годы: нарушения в области Internet-и Intranet-доступа, компьютерные вирусы, защита и конфиденциальность данных и доступ к информации. Наименее охваченными остаются области, которые, скорее всего, принесут множество неприятностей в самом ближайшем будущем: безопасность информации, хранящейся на портативных компьютерах PDA-класса и портативных устройствах, регистрация и расследование инцидентов ИБ, классификация информации по степени конфиденциальности.

У респондентов спросили, используется ли в их организациях стандарт ISO 17799 «Правила управления информационной безопасностью».

ISO 17799 - общепринятый в международной практике стандарт по управлению информационной безопасностью, распространяющийся на такие сферы, как, в частности, политика и организация безопасности, контроль доступа, средства коммуникаций и выполнение установленных требований.

В этом отношении лидирует финансовый сектор (см. рис. П1.7): на него приходится 42% организаций, уже принявших или готовящихся принять данный стандарт. В Европе больше, чем в других регионах, организаций, которые им пользуются или собираются пользоваться. Возможно, это связано с тем, что стандарт был принят в Великобритании и европейские организации имели больше времени, чтобы рассмотреть вопрос о его применении.

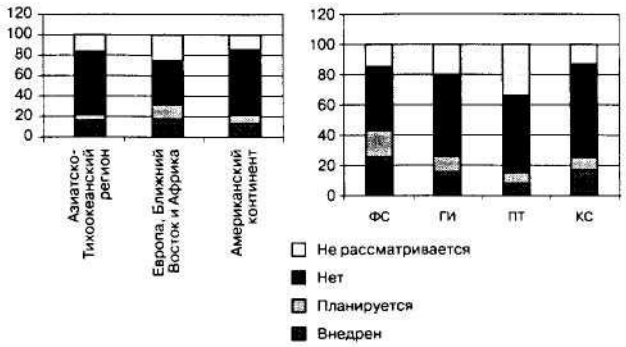


Рис. П1.7. Внедрение стандарта ISO 17799

Из организаций, внедривших этот стандарт, 49% провели процедуру независимой сертификации на соответствие.

Интересно отметить, что уже пользуются данным стандартом именно крупные организации. Можно предположить, что небольшие организации считают издержки на принятие международных стандартов слишком высокими (по сравнению на получаемые в обмен выгоды на местном рынке), тогда как крупные международные корпорации полагают, что тратить деньги на сертификацию по единому международному стандарту в масштабах всей организации экономически эффективнее, чем подтверждать соответствие требованиям различных национальных стандартов. Доля организаций разного размера, применяющих ISO 17799, составляет:

- 51-100 млн. долл. - 13%;
- 100-500 млн. долл. - 16%;
- свыше 500 млн. долл. - 23%.

Комментарий KPMG

Никто не в состоянии работать в вакууме - сегодня, в обстановке расширяющихся границ деятельности компаний и возрастания интенсивности использования Internet в коммерческой деятельности, это становится все более очевидным. Стандарты ISO были разработаны лидерами в данной области, и соблюдение требований стандарта поможет обеспечить комплексный методический подход к требованиям информационной безопасности. Выбор в пользу прохождения сертификации также продиктован маркетинговыми соображениями: соответствие требованиям общепринятого стандарта способствует формированию доверия и привлечению потенциальных клиентов. Однако, как заметил один из респондентов: «Тенденция в направлении открытых систем, расширяющих границы бизнеса, требует единой методологии информационной безопасности как самостоятельного направления». Сертификация на соответствие ISO 17799

призвана помочь сосредоточить внимание руководства и персонала на улучшениях, необходимых для достижения поставленных целей.

Управление ИБ

Управление ИБ охватывает вопросы повседневных операций и текущего контроля безопасности.

Ряд вопросов, заданных респондентам, относился к управленческой, операционной и контролирующей деятельности.

Делегирование функций ИБ внешним организациям

Респондентов спросили, привлекают ли они какие-либо сторонние организации для оказания помощи в вопросах функционирования системы ИБ.

Из ответов следовало, что около 1/3 организаций (31%) вообще не прибегают к сторонней помощи, а 16% полностью делегировали функции поддержки ИБ внешним организациям.

Функции, которые организации делегируют, описаны в табл. П1.16.

Таблица П1.16. Функции ИБ, которые делегируют сторонним организациям

Функции поддержки ИБ	%
Управление межсетевыми экранами	33
Проектирование/разработка систем безопасности	23
Обнаружение вторжения	19
Управление ИБ	17
Управление системой обнаружения вторжения	16
Все услуги по обеспечению безопасности ИТ	16
Мониторинг журналов событий ИБ	9

Выяснилось, что в Европе, в частности в Великобритании, Нидерландах и Германии, на делегирование внешним организациям приходится гораздо больше составляющих ИБ, чем в остальном мире, особенно в сфере управления межсетевыми экранами, системами обнаружения вторжения и проектирования и разработки систем безопасности.

Оказалось также, что из организаций, полностью делегировавших функции поддержки ИБ, свыше половины составляют небольшие компании. Зачастую это такие компании, которые функционируют только в национальном, а не в мировом масштабе. В свою очередь, более половины крупных организаций пользуются внешними услугами в таких областях, как обнаружение вторжения и управление межсетевыми экранами.

Комментарий KPMG

Факторы, побуждающие прибегать к внешними услугам, видимо, разные у разных типов организаций. Крупные организации стремятся передать часть своих функций внешним организациям для эффективного управления системой ИБ. Небольшим организациям, вероятно, сложно привлекать персонал нужной квалификации и руководить им, чтобы обеспечить эффективное управление системой ИБ ежедневно в течение долгого времени (в режиме 24x7x365). С другой стороны, для этих организаций внешняя поддержка и обслуживание - почти единственная реальная возможность добиться необходимого уровня качества обслуживания, независимо от того, меньшие или большие издержки при этом потребуются.

Что касается организаций, которые ни в какой форме не обращаются к внешним услугам по обеспечению безопасности, то респонденты из 81 такой организации (41%) сказали, что не собираются рассматривать этот вопрос - по-видимому, на том основании, что риск делегирования подобной деятельности слишком высок.

В табл. П1.17 представлены обоснования тех, кто уже пользуется внешними услугами.

Таблица П1.17. Обоснования использования внешних услуг безопасности

Факторы, побуждающие прибегать к внешним услугам	%
Нехватка специальных технических знаний внутри компании	49
Улучшение обслуживания	40
Сокращение издержек	36
Стратегия компании	32
Трудность поиска/удержания персонала	28
Является частью соглашения о делегировании функций ИТ	27
Трудности в обеспечении режима 24x7x365	25
Преимущество обслуживания за фиксированную плоту	24
Сдерживающие факторы скорости развития	20
Для делегирования рисков ИБ	18

Многие организации рассматривают передачу функций по обеспечению ИБ внешним организациям как способ избавиться от проблем, но внешние услуги -не панацея. Невозможно делегировать сам риск, а предъявление судебного иска поставщику внешних услуг вряд ли будет решением проблемы, если бизнес разорился в результате серьезного нарушения ИБ.

Организациям необходимо понять, какие виды деятельности нельзя ни в коем случае передавать вовне. А относительно тех, которые передать можно, следует четко представлять себе, как их контролировать, когда они выполняются другой организацией. В случае правильного выбора можно ожидать успешного и взаимовыгодного сотрудничества.

Тестируют ли компании надежность системы ИБ?

Этот вопрос был задан, чтобы понять, спроектирована ли компания надлежащим образом и отвечает ли поставленным задачам, а также проверить, эффективно ли функционирует система ИБ (как было запланировано).

Из ответов следовало, что 77% всех организаций тестирует надежность своей системы ИБ. Однако заметны некоторые существенные расхождения в разных регионах (см. рис. П1.8). Меньше всего тестируют надежность своей системы ИБ организации в Азиатско-Тихоокеанском регионе (64% по сравнению с 82% в Европе, на Ближнем Востоке и в Африке и 88% на Американском континенте). Кроме того, те организации в Азиатско-Тихоокеанском регионе, которые все-таки тестируют надежность своей системы ИБ, делают это реже, чем все прочие организации: лишь 18% организаций в Азиатско-Тихоокеанском регионе проводят тестирование каждую неделю (против 38% на Американском континенте).

Рис. П1.8. Процент тестирования надежности систем ИВ

Комментарий KPMG

Организации, не тестирующие надежность своих систем ИБ, строят замки на песке. В связи с постоянным усложнением систем и их защитных механизмов достаточно всего одного недобросовестного технического работника, вносящего одно-единственное техническое изменение, чтобы поставить под угрозу всю систему ИБ предприятия.

Один респондент сказал, что самым большим риском безопасности были «неизвестные бреши в защите системы». Проведение регулярных проверок системы ИБ укрепит уверенность в том, что принимаемые меры являются надлежащими. Интересно, что 20% тех организаций, которые были убеждены в действенности принятых мер по защите своей информации, не проверяли эффективность этих мер. Напрашивается вопрос - на чем основана их уверенность, если они не знают, какие меры оправдывают себя на практике?

Управление персоналом

Управление пользователями включает процесс предоставления и аннулирования их доступа к информационным ресурсам.

Респондентам был задан ряд вопросов, связанных с доступом пользователей к информации, в частности к системам ИТ.

Осведомленность в вопросах безопасности за пределами организации

Респондентов спросили, насколько, по их мнению, осведомлены в вопросах информационной безопасности их клиенты, торговые партнеры, регулирующие органы и законодатели.

Общий ответ был таким: «Не очень хорошо» (см. рис. П1.9).

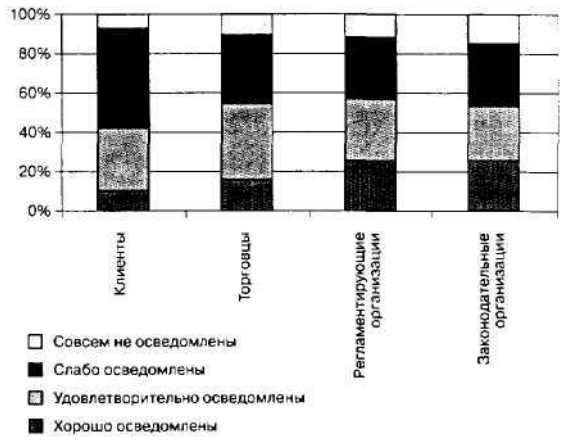


Рис. П1.9. Процент информирования по вопросам безопасности

Комментарий KPMG

Представления об осведомленности деловых партнеров в вопросах информационной безопасности весьма неоднозначны и противоречивы. При этом недоверие между бизнес-партнерами может быть обоюдным. Многие организации не раскрывают перед своими клиентам и партнерами мер по обеспечению ИБ. Однако многочисленные исследования последнего времени показывают, что клиенты неохотно заключают сделки через Internet из опасения стать жертвами мошенничества. Поэтому в сфере электронной коммерции проблема повышения общей осведомленности пользователей по вопросам ИБ стоит очень остро, поскольку от уверенности пользователей в защищенности информации при проведении той или иной сделки через Internet зависит увеличение объемов таких сделок и доходов от них.

Кампании по повышению осведомленности в вопросах ИБ

Респондентов попросили ответить, проводят ли их организации мероприятия по повышению осведомленности в вопросах информационной безопасности.

Затем уровни осведомленности персонала организаций, в которых проводятся и не проводятся подобные мероприятия, сравнивались (см. табл. П1.18).

Таблица П1.18. Уровни осведомленности персонала организаций

Степень осведомленности	Кампания по повышению осведомленности	
	проводится, %	не проводится, %
Хорошая	29	18
Удовлетворительная	46	45
Слабая	24	32
Отсутствует	1	5

Комментарий KPMG

Кампании по повышению осведомленности персонала в области информационной безопасности, похоже, дают свои результаты. Там, где реализуется непрерывная программа обучения и подготовки сотрудников, достигается уменьшение числа нарушений ИБ.

Осознание рисков внутри организации оказывает большое влияние на эффективность применения защитных мероприятий. Выработка надлежащего отношения руководства и персонала к информационной безопасности помогает в формировании полноценной системы ИБ.

Защита технологической инфраструктуры и обеспечение непрерывности ведения бизнеса

Защита технологической инфраструктуры и обеспечение непрерывности бизнеса охватывает «бито-байтовые» элементы системы ИБ - от межсетевых экранов и систем обнаружения вторжения до инфраструктуры хранения данных.

Ряд вопросов к респондентам относился к использованию передовых технологий информационной безопасности.

Внедрение инфраструктуры открытых ключей (PKI)

Один из таких вопросов был сформулирован так: внедрена ли в организациях инфраструктура открытых ключей (PKI)?

Из ответов следовало, что такие технологии только начинают распространяться (см. табл. П1.19). И это несмотря на то, что технологии PKI хорошо известны и одно время их провозглашали универсальным решением всех проблем ИБ, связанных с угрозами сети Internet.

Таблица П1.19. Распространение технологии PKI

Степень распространенности	%
Полностью внедрили PKI	10
Внедрили пробную версию PKI	11
Планируют внедрить PKI	17
Подумали и отказались внедрять PKI	11
Еще не думали об этом	51

Комментарий KPMG

PKI обеспечивает инфраструктуру управления и поддержку цифровых сертификатов, которые предназначены для шифрования документов или сообщений, для верификации их источников, а также для гарантии того, что отправитель не сможет утверждать впоследствии, что он не отправлял сообщение (свойство невозможности отрицания). Поэтому такая инфраструктура идеальна для создания доверия в мире электронных сообщений, в котором два участника сделки зачастую никогда не видят друг друга. Тем не менее низкое восприятие этой технологии указывает на наличие определенных проблем. Так, например, внедрение и обслуживание PKI является достаточно дорогостоящим процессом. Информационные системы развивались без учета необходимости взаимосвязи и сопряжения между организациями, а также особенностей и целей введения сертификатов. Однако за последние несколько лет PKI была существенно усовершенствована и издержки на ее внедрение и сопровождение снизились. В настоящее время некоторые стандартные операционные системы содержат базовые средства обеспечения PKI и большинство систем PKI демонстрируют совместимость друг с другом.

Беспроводные сети

Респондентов спросили, пользуются ли они беспроводными сетями, и если да, то какие методы защиты применяются в отношении данных, передаваемых по этим сетям.

Табл. П1.20 отражает полученные результаты.

Таблица П1.20. Использование технологии беспроводных сетей

Степень распространенности	%
Полностью внедрили беспроводную сеть	13
Внедрили пробную версию	17
Планируют внедрить беспроводную сеть	13

Подумали и отказались от внедрения беспроводной сети	15
Еще не думали об этом	42

Из организаций, в которых полностью внедрена беспроводная сеть, 38% не привлекают виртуальные частные сети (VPN) или иные технологии шифрования/ туннелирования для защиты передаваемых данных.

Комментарий KPMG

В прессе не раз высказывалась озабоченность относительно передачи данных посредством беспроводных сетей и существующих при этом угроз «взлома» (несанкционированного доступа и т.п.). Беспроводная технология еще сравнительно молодая и «не без огрех» - так, например, в алгоритме «эквивалент проводной конфиденциальности» (Wired Equivalent Privacy или WEP), который предполагает защиту беспроводного трафика, были обнаружены проблемы уязвимости в управлении ключами и в других элементах защиты. В большинстве случаев внедрение версий WEP, их соответствующая конфигурация и обслуживание - достаточно трудоемкие процессы. Многие организации, по-видимому, все еще не придают должного значения защите информации, циркулирующей по беспроводным сетям. Эти сети просты в установке, и многие специалисты не знают, где или сколько беспроводных сетей функционирует внутри организаций, хотя это именно те области, в которых самое слабое звено может поставить под угрозу безопасность всей системы!

Защита портативных устройств

У респондентов спросили, разрешают ли они своим сотрудникам использовать портативные устройства PDA-класса, известные еще как «карманные компьютеры», для работы, и если да, то устанавливают ли они какое-либо программное обеспечение для защиты информации, хранящейся в данных устройствах.

Оказалось, что 43% организаций позволяют персоналу пользоваться PDA причем в 67% случаев активно стимулируется внедрение данных устройств и даже проводятся централизованные закупки. Однако очень немногие компании обеспечивают в том или ином виде защиту информации, содержащейся в PDA (лишь 7% установили средства защиты и 13% планируют сделать это).

Комментарий KPMG

Современные PDA позволяют хранить и обрабатывать огромные объемы информации. Эта информация, загружаемая из корпоративных систем (например, дневники, сообщения электронной почты, списки контактов и задач), бывает конфиденциальной.

По всей видимости, организации не осознают угрозу, которую представляют собой утерянные или украденные устройства PDA Конфиденциальные данные компании с легкостью переносятся в PDA для работы дома, в самолете или поезде. PDA все еще сравнительно дороги и поэтому весьма привлекательны для любого рода посягательств.

PDA и портативные устройства больше нельзя классифицировать только как технические новинки и забывать о необходимости защиты данных. В то же время вопросы информационной безопасности, связанные с подобными устройствами, все еще решаются недостаточно полно.

Идентификация пользователей

Респондентам был задан вопрос о методе идентификации, принятом в их организациях для установления личности пользователя в прикладных системах.

Из ответов следовало, что подавляющее большинство организаций (82%) полагаются на классический метод - учетную запись и пароль пользователя (см. табл. П1.21).

Таблица П1.21. Методы идентификации пользователей

Принятые методы	% использования
Учетная запись пользователя и пароль	82
Смарт-карта	19
Жетоны	10
Биометрия	2

Комментарий KPMG

Освоение надежных форм идентификации происходит медленно. Двухфакторная идентификация («что у вас есть» и «что вы знаете») все еще редко привлекается для идентификации пользователей прикладных систем, а биометрия встречается еще реже.

Причиной такого положения может быть дороговизна. Биометрия требует установки считывающего устройства для каждого компьютера, с которого должен быть обеспечен вход пользователя; смарт-карты и жетоны нуждаются в распределении, внедрении процедур и систем сопровождения, что также не дешево. Скорее всего, это окажется крайне дорогостоящим мероприятием, если в организации тысячи пользователей и персональных компьютеров. Руководители многих организаций закрывают глаза на данные риски на том основании, что даже серьезное нарушение ИБ может обойтись дешевле, нежели внедрение систем надежной идентификации, способствующих снижению вероятности таких нарушений.

Удаленный доступ к корпоративным системам

Респондентам предложили описать способы защиты удаленного доступа к корпоративным сетям в их организациях.

Было установлено, что в подавляющем большинстве организаций (76%) защита обеспечивается только посредством учетной записи и пароля пользователя. При этом лишь 14% организаций прибегают к более надежной двухфакторной аутентификации, например смарт-картам или жетонам. Всего 1% пользуется биометрией, что неудивительно из-за высокой стоимости внедрения биометрических считывающих устройств.

Респондентов спросили также, осуществляется ли регистрация и отчетность применительно к нарушениям безопасности в системах удаленного доступа.

Выяснилось, что только 60% организаций регистрируют и расследуют нарушения безопасности систем удаленного доступа. Однако этот показатель отличается для разных регионов: Азиатско-Тихоокеанский регион - 47%, Европа, Ближний Восток и Африка - 65%, Американский континент - 63%.

Комментарий KPMG

Системы удаленного доступа обычно предоставляют полные права доступа к внутренним информационным ресурсам организации. Традиционные методы обеспечения безопасности доступа с помощью учетной записи и пароля пользователя позволяют хакеру получить доступ, подобрав пароль.

В организацию не поступят предупреждающие сигналы о попытках проникновения в ее внутренние ресурсы и никто не узнает, насколько успешными были эти попытки, если отсутствуют системы регистрации и расследования нарушений безопасности. При похищении других корпоративных ресурсов владельцу обычно известно об этом уже после того, как он лишится их! Владелец может никогда не догадаться, что информация украдена, если только она не попадет в руки конкурента или проходимца.

Парольная защита

Респондентов попросили ответить, сколько паролей должен помнить каждый пользователь в их организации, чтобы получить доступ в корпоративные системы.

Результаты опроса представлены в табл. П1.22.

Таблица П1.22. Количество паролей пользователей

Число паролей	%
Один	25
Два	38
Три	22
Четыре	9
Пять	4
Шесть или больше	2

Респондентов спросили, как часто в их организациях приходится менять пароли доступа к приложениям.

Ответы отражены в табл. П1.23.

Таблица П1.23. Частота изменения пароля

Обновление паролей	%
Ежемесячно	44
Каждые 1-3 месяца	36
Каждые 4-6 месяцев	7
Более чем через 6 месяцев	3
По-разному - решает пользователь	6
Никогда	4

Комментарий KPMG

Большинству пользователей для получения доступа к банковским счетам или Internet-услугам приходится помнить два или более паролей на работе и, вероятно, еще два-три дома. В настоящее время средняя длина пароля составляеТ5-8 символов, и его нужно менять каждый месяц. Поэтому не удивительно, что люди записывают свои пароли и выбирают предсказуемую последовательность при создании новых. Подбор/нахождение паролей пользователей является самым простым способом проникновения в системы.

Система обнаружения вторжений (IDS)

У респондентов спросили, внедрена ли в их организациях система обнаружения вторжений (Intrusion Detection System или IDS), и если да, то какого типа.

Оказалось, что только 14% организаций эксплуатируют сетевой вариант системы обнаружения вторжений и 15% - систему защиты единичных узлов сети.

Комментарий KPMG

Системы обнаружения вторжения - одно из новейших средств безопасности, предназначенных оказывать помощь в устранении угрозы внешних и внутренних хакеров. Эти системы в сетевом исполнении анализируют сетевой трафик, отслеживая известные комбинации, свидетельствующие о попытках вторжения. А системы обнаружения вторжения для защиты единичных узлов сети анализируют регистрационные записи (log-файлы), формируемые операционными системами, и таким образом распознают ситуации, связанные с вопросами безопасности.

Одной из распространенных проблем, с которыми сталкиваются организации при рассмотрении вопроса внедрения систем обнаружения, является численность персонала, необходимого для их обслуживания. Вторжение может произойти в любой момент дня или ночи, однако не все организации имеют штат, который мог бы круглосуточно, еженедельно и в течение года обслуживать эти системы.

При этом издержки на аппаратное и программное обеспечение систем поддаются контролю и позволительны для многих организаций, а вот расходы на персонал могут оказаться значительными. Возможно, именно это удерживает многие небольшие организации от внедрения данных систем, что, в свою очередь, стимулирует обращение к внешним организациям по оказанию услуг, связанных с обнаружением вторжений.

Отчетность о нарушениях

Респондентам был задан вопрос о том, существует ли в их организациях система отчетности по нарушениям.

Полученные результаты представлены в табл. П1.24.

Таблица П1.24. Ведение отчетности о нарушениях

Системы отчетности	%
Нарушения в прикладных системах	52
Нарушения в корпоративных сетях	43
Нарушения в ЛВС	61
Нарушения в системах удаленного доступа	60

Кроме того, прозвучал вопрос о том, как часто просматриваются в их организациях регистрационные записи (log-файлы) по каждому из вышеперечисленных направлений.

Было установлено, что большинство организаций просматривают файлы регистрации событий ежедневно. Вместе с тем значительное число организаций делают это еженедельно (около 20%), ежемесячно (около 15%) либо от случая к случаю (около 10%).

Комментарий KPMG

Поскольку степень распространения систем IDS для защиты единичных узлов сети невысока, организациям приходится полагаться на просмотр файлов регистрации событий вручную, чтобы определить, имели ли место нарушения системы информационной безопасности. Еще многие организации либо не формируют отчетность о нарушениях, либо не просматривают эти сообщения с частотой, необходимой для эффективного обнаружения таких нарушений.

Информация, предоставленная в настоящем обзоре, имеет только общий характер и не может служить основанием для каких-либо действий со стороны физического или юридического лица без профессиональной консультации относительно специфики конкретных обстоятельств.

Компания KPMG не несет никакой ответственности за убыток, причиненный любому физическому или юридическому лицу, предпринявшему какие-либо действия или воздержавшемуся от таковых на основе информации, изложенной в данном обзоре.

Хотя мы стремимся обеспечивать точную и своевременную информацию, не существует никаких гарантий ни относительно полноты и справедливости приведенных сведений на дату их фактической публикации, ни относительно того, что они будут оставаться такими в дальнейшем.

Дополнительную информацию по всем вопросам, затронутым в данном документе, можно получить в Отделе по управлению информационными рисками компании KPMG (тел. (095) 937-4477, факс: (095) 937-4400).

Приложение 2
Международное исследование по вопросам информационной безопасности

Цифры и факты

- только 40% организаций уверены в том, что сумеют обнаружить атаку на информационную систему;
- 40% организаций не проводят расследования случаев нарушения информационной безопасности;
- постоянно растет число сбоев в работе жизненно важных систем - более 75% организаций испытывали неожиданные сбои в своей работе;
- только у 53% организаций есть план поддержания деятельности в чрезвычайных ситуациях;
- лишь 41% организаций обеспокоены вторжениями в систему внутри предприятия, несмотря на бесчисленные доказательства большого количества таких вторжений;
- менее чем у 50% организаций имеются программы обучения по вопросам информационной безопасности и осведомленности персонала.

Отмечены тревожные пробелы в системе ИБ. Подход некоторых организаций к вопросам ИБ можно охарактеризовать как безответственный. Управление вопросами ИБ имеет принципиальное значение для выживания компании и получения преимущества перед конкурентами.

Путеводитель по исследованию

- управление безопасностью:
  - вопросы, которые должны задать себе члены правления;
  - текущие приоритеты деятельности;
- использование системы ИБ:
  - тревожные симптомы, причины для беспокойства и угрозы;
  - необходимые меры;
- доступность информационных технологий:
  - причины сбоев в работе компании;
  - ИТ и непрерывность деятельности;
- взгляд в будущее:
  - препятствия на пути к успеху;
  - новые технологии;
- что делать дальше:
  - необходимые действия руководителей компании;
  - создание структуры безопасности.

Резюме исследования

В 2002 г. компания «Эрнст энд Янг» предприняла очередное исследование состояния информационной безопасности. Фоном для него стали экономическая нестабильность, постоянные публикации в прессе о нарушениях ИБ предприятий и вирусных атаках, а также террористические акты 11 сентября 2001 г. К моменту проведения исследования панические настроения улеглись и уступили место взвешенному анализу вероятности возникновения рисков. Мы беседовали с директорами по информационным технологиям и руководителями крупнейших компаний, чтобы понять, что, с их точки зрения, представляет наибольшую опасность и что препятствует дальнейшему развитию в этой сфере.

Ожидается, что экономическая нестабильность продолжится, риски вторжения в информационные системы компаний сохранятся, а обмен информацией будет возрастать. Все это означает наличие следующих важных проблем, которые компании должны быть готовы решать:

- возможность нанесения вреда информационным системам со стороны недовольных сотрудников;
- чрезмерная зависимость от небольшого числа сотрудников;
- увеличение финансовых расходов, приводящее к повышению уязвимости компании;
- необходимость принимать экстренные решения о снижении расходов;
- попытки сторонних поставщиков услуг экономить за счет компании;
- повышенная вероятность мошенничества.

Выполняя это исследование, мы хотели получить ответы на ряд непростых вопросов. Привели ли события 11 сентября вкупе с экономической нестабильностью к выдвижению безопасности информационных систем в качестве первоочередной задачи руководства и появлению возможности для внедрения передовой практики и улучшения дисциплины? Или они стали причиной принятия краткосрочных и, может быть, недальновидных финансовых решений? Способствовали ли эти события повышению интереса к тестированию или внедрению новых технологий, в частности биометрических средств контроля, призванных помочь в решении таких актуальных вопросов, как подтверждение прав доступа? Достаточно ли усилий, прилагаемых в этой области компаниями? Движутся ли компании в правильном направлении? В настоящем отчете анализируются практические последствия основных выводов нашего исследования. Перечислим вкратце несколько тревожных симптомов:

- сбои в работе *жизненно важных систем* происходят все чаще. Несмотря на это, только у 53% компаний существуют планы поддержания непрерывной деятельности. 40% организаций не проводят расследований по случаям нарушения информационной безопасности. Складывается впечатление, что в настоящий момент отсутствуют элементарные основы информационной безопасности;
- *скорость изменений* и растущая сложность рисков названы в числе главных препятствий на пути обеспечения ИБ. 60% респондентов ожидают, что с увеличением обмена информацией финансовые и репутационные риски будут возрастать. При этом лишь 40% организаций «полностью уверены», что они смогут обнаружить попытки вторжения в систему. Менее половины принимают меры по тестированию систем безопасности;
- отмечается недостаточная *информированность сотрудников.* 66% опрошенных сообщили, что отсутствие информации является препятствием на пути к построению эффективной системы безопасности. При этом менее половины организаций внедряют программы обучения и информирования сотрудников;
- *отсутствие квалифицированных сотрудников* в самой компании составляет проблему более чем для 50% организаций.

При определении приоритетов руководство компании должно помнить, что задачу по преодолению огромной дистанции от выявления рисков до внедрения механизмов защиты следует поручать специалистам, обладающим глубоким пониманием бизнеса компании, твердыми техническими знаниями слабых сторон предприятия и тех опасностей, которые ему угрожают. Важно осознать задачи, которые стоят перед компанией, но останавливаться на этом нельзя.

Насколько вы уверены в своем предприятии

Обеспечение информационной безопасности по-прежнему часто рассматривается как технический вопрос, решать который должен только отдел ИТ. В результате:

- внедряются средства защиты только «нижнего уровня»;
- принимаются технологические решения, не поддерживающие бизнес-процессы;
- принимаются «точечные» решения - установка межсетевых экранов или антивирусного программного обеспечения.

Опаснее всего ситуация, при которой руководство считает, будто компания должным образом защищена, в то время как на самом деле затраты на техническое обеспечение в значительной степени обесцениваются в силу следующих причин:

- неадекватность средств защиты информации бизнес-процессам компании;
- недостаточная информированность или уровень подготовки персонала;
- действия третьих лиц и деловых партнеров;
- отсутствие процедур тестирования систем.

Сеть партнеров и клиентов компании имеет принципиальное значение для построения эффективной и удобной системы ИБ. Оценивая ситуацию, выйдите за рамки своей организации и проанализируйте поведение всей сети, ее партнеров и клиентов: их вклад в работу вашей компании, их надежность (или ненадежность) имеют решающее значение для построения эффективной и действующей системы ИБ. Следует иметь в виду, что:

- доступность систем и непрерывность ведения операций принципиально важны для поддержания доверия клиентов;
- информированность сотрудников может привести к успеху ваших инвестиций в технологию и методику обеспечения безопасности или к их провалу;
- у компаний-поставщиков товаров и услуг тоже есть сотрудники. Отсутствие понимания этими сотрудниками вопросов ИБ может поставить под угрозу безопасность как их, так и вашей компании;
- угрозы и нарушения ИБ в состоянии серьезно повлиять на стоимость акций и доверие акционеров и инвесторов.

Управление безопасностью

Основная задача управления безопасностью - поддержка стратегии безопасности, обеспечение реальной отдачи, управление рисками и общая оценка результатов деятельности. Информационные технологии жизненно важны для многих организаций как со стратегической, так и с оперативной точки зрения. Какие вопросы информационной безопасности являются в этих условиях первоочередными? Каким образом это отражается на инвестициях компании?

Результаты исследования

74% опрошенных считают, что в их организации стратегия обеспечения информационной безопасности существует. Если это на самом деле так, данные сведения обнадеживают, поскольку

это база, на основе которой отдел ИТ может строить планы и определять приоритетные направления работы по достижению стратегических и оперативных целей. Однако далее мы покажем, что при осуществлении политики ИБ возникает вопрос, способна ли данная стратегия поддерживать безопасность деятельности компании.

Одним из главных компонентов управления является контроль результатов работы. Необходимое условие контроля результатов - их оценка. Полученные в ходе исследования ответы в области ИТ указывают на тревожные тенденции. Затраты на информационную безопасность могут быть отражены в общей смете расходов на ИТ или в бюджете отдельных подразделений. При этом респонденты отметили ряд компонентов, которые не контролируются и которые сложно выделить в бюджете как службы ИТ, так и отдельных подразделений. Как правило, это безопасность прикладных программ и управление этой безопасностью, а также меры по обнаружению вторжений в систему. Кроме того, некоторые затраты, включая оплату труда сотрудников службы безопасности, установка прикладных программ обеспечения безопасности и программы поддержания непрерывной деятельности отражаются в бюджетах отдельных подразделений и отдела ИТ. Это может помешать более широкому взгляду на проблему и эффективному использованию немногочисленных квалифицированных кадров. 73% опрошенных считают, что имеющийся бюджет помогает решать задачи в краткосрочной перспективе.

61% респондентов сообщили, что в целом в области ИТ наблюдается определенная рационализация, однако информационная безопасность, как им кажется, обладает в данный момент некоторым преимуществом. Лишь 34% опрошенных находятся в процессе рационализации информационной безопасности и всего 7% планируют провести сокращение штатов в отделах ИТ. 51% считают, что информационная безопасность важнее других проектов в области ИТ, а 35% полагают, что это направление такое же важное. Только 13% планируют снизить затраты на обеспечение информационной безопасности, а 41% респондентов не знают, как они поступят. 70% организаций заявили, что намерены расширить масштабы планов поддержания непрерывной деятельности в чрезвычайных обстоятельствах и восстановления работы ИТ после аварий. Такие сведения внушают оптимизм, но при этом беспокоит тот факт, что лишь 29% организаций распределяют затраты по составлению планов поддержания непрерывной деятельности на бюджеты отдельных подразделений, а 45% заявили, что их следует учитывать в бюджете отдела ИТ. Такая позиция может свидетельствовать о том, что многие организации по-прежнему рассматривают поддержание непрерывной деятельности как проблему отдела ИТ, а не компании в целом. Возможно, эти организации не осознают, что обеспечение непрерывной деятельности является более масштабной задачей, чем восстановление нормальной работы вычислительного оборудования и программного обеспечения после аварии.

Что это может означать для вашего предприятия

Стратегия обеспечения информационной безопасности дает основу для принятия решений и согласования приоритетных направлений деятельности. Многие предприятия формируют технические планы. В этих планах могут быть отражены политика и процедуры, содержаться некоторые указания на внедренные предприятием технологии. Иными словами, они сосредоточены на описании технических аспектов деятельности. Чтобы стратегия информационной безопасности приносила реальную пользу, она должна быть составлена с учетом пожеланий руководителей линейных и функциональных подразделений во всех областях деятельности предприятия, содержать тщательный анализ корпоративной культуры и характера рисков. Нужен реалистичный документ, который послужит основой для тактических и оперативных решений по всем направлениям деятельности. При разработке стратегии часто упускается из виду обучение и информирование персонала, стратегия выбора поставщиков, меры по оценке результатов и тестированию систем.

Чтобы обеспечить на предприятии должный контроль над инвестициями и получение прибыли, следует информировать сотрудников о финансовых планах и жестко контролировать выполнение этих планов. Отсутствие такого информирования и контроля может повлечь за собой низкую заинтересованность сотрудников и невнимательное отношение к экономии средств компании, что нередко приводит к ненужному росту расходов. Кроме того, не исключено появление необходимости в незапланированных дополнительных затратах в течение года. Например, расходы на внедрение могут быть отражены в бюджете конкретного подразделения, а затраты по технической поддержке - в балансе отдела ИТ. При этом ни в одном из этих бюджетов не учитываются расходы, связанные с поддержанием безопасности.

Если вы считаете, что в краткосрочной перспективе ваши финансовые планы достаточны для обеспечения требуемого уровня ИБ в компании, то задайте себе следующие вопросы:

1) Основана ли ваша уверенность на проверенной и объективной оценке деятельности предприятия, его слабых сторон и грозящих ему рисков?

2) Реалистично ли вы смотрите на производимые затраты и их необходимость для обеспечения деятельности предприятия?

Что может предпринять руководство

Управление эффективной системой обеспечения безопасности и ее координация -задача, которую следует решать на уровне правления компании. Слабое знание этого вопроса не может стать поводом для уклонения от его обсуждения.

Как добиться того, чтобы рассмотрение вопросов поддержания безопасности отражало потребности предприятия, а не было реакцией на нашумевшие статьи в прессе?

Задавайте правильные вопросы, критически анализируйте ответы и оценивайте результаты. Перечисленные ниже вопросы помогут вам в этом.

1) Понимает ли правление вашего предприятия, что задачу обеспечения информационной безопасности следует решать на уровне правления и нельзя передавать исключительно под ответственность отдела ИТ? Согласована ли стратегия обеспечения ИБ предприятия с его общей стратегией?

2) Существует ли в вашей организации четкое распределение обязанностей по поддержанию ИБ?

3) Могут ли члены правления определить риски и опасные зоны деятельности предприятия? С какой периодичностью эти данные пересматриваются?

4) Знаете ли вы, сколько средств тратится на ИБ, и на что именно? В состоянии ли вы оценить отдачу от этих вложений?

5) Какие последствия для предприятия будет иметь серьезное нарушение безопасности (для репутации и доходов, юридические последствия, для результатов операционной деятельности и доверия инвесторов)?

6) Считается ли в вашей компании, что система ИБ может быть инструментом, стимулирующим новые виды деятельности (например, если вы внедрите эффективную систему ИБ, удастся ли организации увеличить объем операций в Internet)?

7) Насколько вам грозит риск приобрести репутацию компании, небрежно относящейся к вопросам ИБ?

8) Какие меры вы приняли, чтобы действующие из лучших побуждений (или наоборот) третьи лица не смогли нанести ущерб информационной безопасности вашей компании?

9) Каким образом вы проводите независимую проверку с целью убедиться в том, что управление ИБ организовано в компании должным образом?

10) Как вы оцениваете эффективность предпринимаемых вами мер по обеспечению ИБ?

Что можно сделать

Если вы считаете, что у вашего предприятия есть стратегия обеспечения информационной безопасности, убедитесь в том, что (1) в ней учтены все риски, с которыми компания сталкивается, а не только используемые вашей компанией информационные технологии, (2) эта стратегия правильно понята и (3) выполняется. Удостоверьтесь, что вы получаете объективное подтверждение эффективности своей стратегии. Если у предприятия стратегии нет, то действовать нужно уже сейчас:

1) Вне зависимости от того, тестируете ли вы существующую стратегию ИБ или разрабатываете новую с нуля, удостоверьтесь в том, что окончательный вариант стратегии будет давать положительные ответы на приведенные ниже вопросы:

- учитывает ли данная стратегия общую стратегию деятельности вашего предприятия, его опыт и культуру;
- соответствует ли она общей стратегии в области ИТ и обеспечения безопасности коммерческой деятельности предприятия;
- служит ли она основой для программ информирования о целях информационной безопасности, стратегии выбора поставщиков, привлечения финансирования, определения приоритетов, поиска ресурсов, внедрения технологий и оборудования;
- дает ли она рекомендации для принятия решений по основным партнерам-поставщикам услуг, клиентам и продавцам;
- существует ли ясно сформулированный и согласованный список расположенных в порядке значимости слабых сторон предприятия и угрожающих ему рисков? Регулярно ли производится пересмотр этого списка?

1) Если у вашего предприятия есть стратегия, проанализируйте следующие аспекты планов и бюджетов обеспечения безопасности в области ИТ во всех подразделениях компании:

- существуют ли параметры, на основании которых вы можете принимать инвестиционные решения и определять последствия сокращения расходов на проекты обеспечения безопасности;
- знаете ли вы, сколько и на что именно вы тратите;
- как вы оцениваете эффективность инвестиций.

2) Если безопасность информационных систем не входит в круг постоянных задач, решаемых правлением, необходимо ее включить, не дожидаясь возникновения неприятностей. Информация - это ваш актив, поэтому ее безопасность - слишком важный вопрос, который нельзя оставлять в ведении только отдела ИТ. Способность и желание предприятия управлять рисками зависят от инициативы руководства, а эффективное управление безопасностью ИТ может дать преимущество перед конкурентами. Поэтому задайтесь такими вопросами:

- оказывает ли правление явную и ощутимую поддержку вашей деятельности;
- определилась ли организация в своем отношении к безопасности и рискам;
- отражена ли важность ИБ в структуре затрат и специальных программах;
- каким образом вы реализуете связь технологий, сотрудников и процессов в областях, касающихся ИБ.

3) Убедитесь, что ответственность за информационную безопасность четко распределена и осознается теми, на кого она возложена:

- определены ли контрольные показатели деятельности? Есть ли у вас система оценки выполнения плана;
- существуют ли механизмы получения из независимых источников подтверждения эффективного управления ИБ;

– все ли сотрудники организации согласны с распределением обязанностей по обеспечению ИБ.

Как используется система информационной безопасности

В данном разделе описываются основные задачи и проблемы, стоящие перед респондентами на пути к достижению нужного уровня информационной безопасности. Где, с их точки зрения, кроются основные риски? Какие шаги были сделаны для решения этих задач?

Результаты исследования

Наше исследование показывает, что программу обучения и информирования по проблемам ИБ осуществляют менее половины опрошенных, а 31% респондентов только собираются начать это делать, что свидетельствует об опасных пробелах в реализации программы ИБ.

Такой факт тем более удивителен, поскольку две трети опрошенных объявили, что у них есть четкая и понятная стратегия обеспечения безопасности.

С нашей точки зрения, программа обучения по информационной безопасности и понимание ее значения - краеугольные камни эффективной стратегии в данной области. Это подтверждают 66% опрошенных. По их словам, низкая информированность сотрудников является препятствием на пути к достижению необходимого уровня безопасности.

Самый высокий уровень обеспечения ИБ достигнут в объеме, который мы считаем минимальным для безопасности систем, например:

– применение антивирусных программ;
– контроль прав доступа;
– установка межсетевых экранов.

40% организаций не проводят расследований фактов нарушения информационной безопасности. Однако, если не изучать такие случаи, повышается вероятность незамеченного ущерба и создания «черного входа» в систему, который впоследствии может быть использован в преступных целях.

Только 40% опрошенных признали, что в течение последних шести месяцев была обнаружена попытка вторжения в компьютерную сеть предприятия, получения несанкционированного доступа к информации или нарушения работы Internet-серверов. По нашему мнению, эти данные не совпадают с помещаемой практически в каждой статье о нарушениях информационной безопасности статистикой, которая свидетельствует о том, что такие попытки вторжения производятся гораздо чаще. С другой стороны, мы понимаем, что многие организации не станут открыто признавать факт нарушения информационной безопасности или попыток вторжения в систему.

Кроме того, только 40% респондентов (наблюдается прирост по сравнению с 33% в прошлом году) выразили уверенность в своей способности выявить вторжение в систему. Некоторые компании, сомневающиеся, что им удастся заметить вторжение в систему, почти наверняка подвергались вторжению, но не знают об этом.

Мероприятия по проверке систем обеспечения информационной безопасности проводят менее половины опрошенных компаний. Как же они могут быть уверены, что им известны реальные источники опасности и что их политика и процедуры в области обеспечения безопасности организованы эффективно?

С другой стороны, мы отмечаем более высокую озабоченность уязвимостью к вторжениям извне (57%) по сравнению с атаками изнутри (41%). При этом ведущие исследовательские группы по-прежнему подтверждают, что более двух третей атак производится изнутри организации.

Опасаются респонденты также попыток нанести ущерб программному обеспечению, например заражения системы компьютерными вирусами и «червями» (59%).

Немногим более 50% респондентов указывают на страх раскрывать конфиденциальную информацию. Конфиденциальность информации может быть важна не для всех организаций, тем не менее стремление обезопасить данные и сохранить их конфиденциальность все еще остаются основными препятствиями на пути к увеличению обмена информацией.

Может вызвать удивление тот факт, что только одна треть опрошенных сильно обеспокоена соблюдением законодательства и отраслевых норм, несмотря на растущее внимание к вопросам конфиденциальности и защиты данных. В качестве примера можно привести директиву ЕС в Европе и акт Грамма-Лича-Блайли в США. Также следует отметить предстоящие отраслевые меры по улучшению распознавания и подтверждения пользователей.

Основные проблемы, стоящие на пути к достижению необходимого уровня безопасности, - это:

- высокая скорость изменений и сложность рисков (70%);
- недостаточная информированность сотрудников (66%);
- нехватка квалифицированных сотрудников (53%).

Только 13% опрошенных считают, что отсутствие поддержки со стороны руководителей отделов ИТ является препятствием к повышению качества ИБ. С точки зрения 24% опрошенных таким препятствием может стать отсутствие поддержки со стороны руководства компании.

Независимым подрядчикам в настоящее время передаются, прежде всего, внутренний аудит ИТ (21%) и тестирование систем безопасности (20%). Клиенты не совсем довольны качеством услуг, которые предоставляют независимые подрядчики. Это неудивительно, если учесть количество самых разнообразных требований в разных ситуациях.

Какие последствия могут ожидать вашу компанию

Наше исследование показывает, что в некоторых областях (например, в защите от вирусов) был достигнут прогресс. Тем не менее по-прежнему многое указывает на отсутствие в компаниях базовой управленческой информации о случаях нарушения ИБ. Это заставляет усомниться, что при принятии решений о расходах и инвестициях в сфере ИТ учитываются потребности предприятия и реальные сведения о происходящем.

Даже для тех 40% респондентов, которые уверены в своей способности обнаружить атаку, существует два вопроса: (1) Когда именно она будет выявлена - в момент атаки или после нее, и если после, то в течение какого времени? (2) Каким образом можно оценить последствия этой атаки?

Хотелось бы верить, что две трети респондентов не очень обеспокоены соблюдением законодательства и отраслевых норм потому, что им хорошо известно, какие требования современная ситуация предъявляет к системам ИТ, и у них есть четкий план решения насущных задач. Однако тревожит тот факт, что многие организации, возможно, не знают о существовании отраслевых норм или риске их нарушения. Деловые партнеры и регулирующие органы могут потребовать от этих компаний подтвердить свое серьезное отношение к вопросам ИБ.

Статистические данные показывают, что многие предприятия не практикуют комплексный подход к вопросам ИБ. Так, в компании могут быть установлены антивирусная защита и контроль доступа, но при этом слабо развиты программы обучения и информирования сотрудников, призванные помочь им эффективно пользоваться этими инструментами, и лишь в ограниченном объеме применяются процедуры тестирования систем, способствующие обеспечению соблюдения норм законодательства.

В результате компании в своем стремлении поддерживать безопасность могут возлагать неоправданные надежды на малоэффективные меры. Отсутствие комплексного подхода увеличивает обеспокоенность по поводу возможных источников рисков, грозящих компании. СМИ по-прежнему регулярно пишут о хакерах и взломах компьютерных систем. Может быть, поэтому компании считают более серьезной опасность вторжения в систему извне, чем исходящую от сотрудников.

Опубликованные статистические данные указывают, что большое количество атак на системы производится внутри компании. Кроме того, мы сейчас находимся в периоде экономической нестабильности. Когда экономика переживает сложные времена, растет стимул к личному обогащению и риск мошеннических или вредительских действий со стороны сотрудников. Следует также учитывать вероятность действий недовольных сотрудников, просто желающих нанести вред компании и ее репутации.

Различная степень удовлетворенности услугами сторонних подрядчиков может навести на мысль, что в этой области заказчик вынужден полагаться на волю случая. Однако на практике ситуация выглядит иначе: компании, которые удовлетворены качеством предоставляемых услуг, заключали с подрядчиком договор, предварительно четко уяснив и согласовав взаимные ожидания и составив для себя план, отражающий ряд переменных параметров, способных повлиять на удовлетворенность качеством услуг, например:

- учет потребностей предприятия;
- понимание корпоративной культуры предприятия;
- уровень предоставляемых услуг;
- уровень квалификации и опыта;
- способность компании обеспечить технически грамотное управление деятельностью стороннего подрядчика.

Набор услуг, для выполнения которых привлекаются сторонние подрядчики, свидетельствует о том, что услуги в области информационной безопасности передаются независимым подрядчикам, как правило, по следующим причинам: (1) предприятие признает, что требуются квалификация и опыт, выходящие за рамки сферы его основной компетентности; (2) нужен независимый анализ ситуации. Разумеется, помимо этих причин могут существовать и «традиционные» причины - такие как желание оптимизировать затраты или необходимость в более высоком качестве услуг.

Что вы можете сделать

1) Необходимо понять, что представляет ценность для вашей организации. Это может быть стратегический план, финансовая информация, сведения о продуктах и ценах, данные о сотрудниках, подробная информация о поставщиках и т.д. Поэтому большое значение имеет:

- провели ли вы тщательный анализ рисков и уязвимых мест, в том числе оценку способности и заинтересованности третьих лиц в организации атак на ваши системы;
- ценили ли вы свою способность противостоять этим рискам;
- внедрена ли у вас процедура регулярной переоценки рисков и уязвимых мест.

2) Утвердите приоритетные направления работы. Решите самые главные вопросы. Для эффективной работы системы безопасности необходима согласованная работа людей, процессов и оборудования. Подумайте:

- уверены ли вы в том, что вашей политике и технологии антивирусной защиты не может быть нанесен ущерб, например из-за ненадлежащего обучения и информирования сотрудников;

- не снижается ли надежность ваших межсетевых экранов, например из-за отсутствия ясной политики и стандартов по контролю информационного обмена компании с внешним миром;
- учитываете ли вы при составлении финансовых и общих планов работы необходимость проведения эффективного и регулярного тестирования систем обеспечения безопасности.

3) Определив основные направления своей работы, оцените сильные стороны вашей системы информационной безопасности по таким критериям:

- есть ли в вашей компании талантливый и опытный сотрудник, способный умело управлять ИБ по всем направлениям работы компании и подразделения ИТ, а также при контактах с третьими лицами;
- какие операции имеет смысл производить силами самой компании, а какие лучше передать сторонним исполнителям, потому что у них больше опыта, или нужен взгляд со стороны;
- если вы пользуетесь услугами третьих лиц, провели ли вы тщательный анализ их квалификации, возможностей, производственной культуры и уровня понимания вашей деятельности.

4) Убедитесь в том, что вы располагаете управленческой информацией, на основании которой сможете принимать решения и эффективно управлять ИБ. Для этого ответьте себе на следующие вопросы:

- регулярно ли вы получаете сведения, которые позволяют вам оценить приемлемость постоянного поддержания информационного обмена с третьими лицами;
- каким образом вы оцениваете и контролируете уровень информированности своих сотрудников о принципах работы системы ИБ;
- к каким последствиям привел последний случай заражения компьютерным вирусом, можно ли сказать, что компания действовала лучше, чем прежде в аналогичной ситуации;
- когда вы в последний раз пересматривали методику обнаружения и контроля попыток нарушения целостности системы, производимых внутри компании и извне.

Доступность информационных технологий

В конце 2001 г. изменился набор вероятностей, рассматриваемых компаниями при подготовке к возможным нарушениям своей работы. В данном разделе мы приводим ответы респондентов на несколько важных вопросов:

- каковы основные причины сбоев в работе жизненно важных для бизнеса информационных систем;
- понимают ли компании последствия для бизнеса и репутации, к которым может привести невозможность использовать ИТ;
- какие планы поддержания непрерывной деятельности есть у компаний и какова вероятность их эффективного применения в нужный момент.

Выводы

Среди главных причин прерывания деятельности компании были названы отказы в работе вычислительного оборудования и программного обеспечения (56%), а также средств связи (49%). Около четверти всех отказов было вызвано ошибками в обращении с системой, техническими

характеристиками системы и сбоями в работе третьих лиц. Респонденты считают, что такие нарушения в деятельности влияют на решение оперативных вопросов больше, чем на финансовое положение или репутацию компании.

Немногим более половины опрошенных указали, что у них имеется план поддержания непрерывной деятельности при возникновении чрезвычайных ситуаций. Многие из тех, у кого такой план есть, в процессе его подготовки пропустили ряд необходимых этапов. Так, только чуть более 40% респондентов провели анализ возможных последствий и определили основные бизнес-процессы в своей компании, а в 21% компаний план не тестировался. Кроме того, чуть менее половины всех опрошенных организаций не согласовали график восстановления функционирования подразделения ИТ с коммерческими подразделениями. В результате не исключено возникновение серьезных расхождений между тем, что сможет предложить подразделение ИТ, и тем, в чем нуждается компания.

Несколько большее количество организаций (71%) сообщили о том, что у них есть план восстановления деятельности ИТ при возникновении чрезвычайных ситуаций, хотя 16% этот план не тестировали. Возможно, руководителям компаний следует проверить, насколько эффективны планы восстановления работы оборудования и программного обеспечения, а также имеются ли у сотрудников подразделения ИТ средства и процедуры, которые позволят восстановить функционирование производственных подразделений.

Что это может означать для вашей компании

Стремление предотвратить чрезвычайные ситуации имеет, как минимум, такое же большое значение, как и знание того, что делать после наступления этой ситуации. Вот почему мы решили выяснить основные причины нарушений в работе. Не вызывает удивления тот факт, что в числе основных причин были отмечены сбои в функционировании оборудования, программного обеспечения и средств связи. Однако настораживает количество ответов, в которых причиной сбоев в работе были названы ошибки в управлении системами, технические характеристики системы и сбои в работе третьих лиц. Это может быть результатом плохой организации главных элементов оперативного управления, таких как процесс установки нового ПО, управление изменениями и планирование технических потребностей в ИТ.

Анализ результатов исследования заставляет также задать вопрос: способны ли компании определить, к какому количественному ущербу для финансового положения и репутации компании приведет перерыв в ее работе, а не просто признать, что такие последствия для текущей деятельности существуют? Беспокоит также и то, что большинство респондентов не смогли определить операционные убытки в коммерческих терминах (например, какие могут быть потери из-за упущенных благоприятных возможностей или финансовые убытки в результате того, что 10 000 сотрудников не имели доступа к системам в течение четырех часов). Ответы показывают, что очень многие компании, деятельность которых зависит от функционирования информационных систем и не опирается на проверенный план поддержания непрерывности операций, в случае наступления чрезвычайных обстоятельств прекратят свою работу. В современном мире сложно найти такую организацию, чья деятельность не зависела бы от информационных систем, поэтому серьезные основания для тревоги дают многочисленные ответы об отсутствии плана поддержания непрерывной деятельности. Даже в тех случаях, когда такие планы существуют, они зачастую могут оказаться неэффективными, если были разработаны без согласования с коммерческими подразделениями компании или не подвергались тестированию.

Что вы можете сделать

1) Следует представлять себе, что именно важно для вашей компании и что ей может угрожать. Это основное условие для последовательного понимания целей деятельности компании. Подумайте:

- известно ли вам, к каким последствиям для компании приведет серьезное нарушение системы безопасности или временная недоступность системы в плане репутации, доходов, юридических последствий, операционной деятельности и доверия инвесторов;
- каковы главные риски, грозящие компании, и как их можно оценить в цифровом выражении.

2) Убедитесь в том, что функционирование жизненно важных информационных систем основано на хорошо продуманных операционных процедурах. Для этого ответьте себе на следующие вопросы:

- известны ли вам причины сбоев в работе систем и последствия этих сбоев;
- хорошо ли отработаны у вас процедуры внесения изменений в ПО;
- насколько вы уверены в том, что имеется резервная копия данных и эта копия с определенной периодичностью направляется в специальное место для хранения.

3) Проанализируйте применяемый в вашей компании подход к составлению планов поддержания непрерывной деятельности (которые учитывают действия третьих лиц) по таким критериям:

- используете ли вы формализованный подход для составления планов восстановления деятельности при возникновении чрезвычайных ситуаций;
- достаточно ли принятых вами мер для определения и сведения к минимуму рисков, грозящих вашей коммерческой деятельности;
- проводите ли вы анализ всех процессов деятельности от начала до конца, привлекались ли бизнес-подразделения к оценке ресурсов, необходимых для восстановления прерванных операций, и к согласованию графика восстановления;
- учитывается ли в составленных вами планах вероятность наступления целого ряда чрезвычайных обстоятельств одновременно;
- подвергали ли вы критическому анализу предположения, взятые за основу при составлении плана;
- не слишком ли большая роль в деле управления выходом из кризиса отводится в ваших планах отдельным лицам;
- сохранится ли при наступлении чрезвычайных обстоятельств доступ к основному месту хранения данных и месту хранения резервных копий данных;
- насколько точно вам известно, что именно смогут предложить вам ваши поставщики услуг, если вы к ним обратитесь.

4) Проводите регулярные проверки и вносите соответствующие изменения в порядок своих действий. При этом очень важно, каким образом у вас организовано регулярное оповещение сотрудников и партнеров о планах поддержания непрерывной деятельности, тестирование и анализ этих планов. Для тестирования планов попробуйте применить разнообразные сценарии чрезвычайных обстоятельств (например, невозможность попасть в главное здание компании, банкротство поставщика, широкомасштабная вирусная атака на ваши компьютерные системы). Проанализируйте результаты тестирования своих планов и внесите в них необходимые изменения.

Что в будущем

Считают ли компании, что с развитием обмена информацией возрастает и подверженность рискам? Что мешает росту компаний? Как они могут использовать новые технологии?

Информационная безопасность должна быть встроена в новые системы в момент их создания. Поэтому в основание стратегии ИБ следует положить контроль всех ее параметров и подготовку к будущему. Наши респонденты делятся своими взглядами на повышение подверженности рискам компаний с ростом обмена информацией, говорят о планах более широкого внедрения технологий по мере расширения предприятия и строят прогнозы относительно препятствий, с которыми им предстоит столкнуться.

Выводы

Две трети опрошенных считают, что в связи с развитием обмена информацией риски будут возрастать. Как и в прошлом году, главными препятствиями на пути развития обмена информацией считается стремление обеспечить безопасность и сохранить конфиденциальность информации. Только 22% респондентов назвали препятствием низкий уровень доверия к деловым партнерам или третьим лицам. При этом для эффективной работы системы ИБ решающую роль играют основные участники этого процесса, в том числе сотрудники, поставщики и деловые партнеры. Информационная безопасность поддерживается с помощью стандартного ПО, разрабатываемого специализированными компаниями и применяемого в соответствии с определенными стандартами безопасности. Тенденции к модернизации технологий ИБ пока что незначительны. 19% компаний проводят пробную эксплуатацию или внедряют системы защиты на базе открытых ключей (Public Key Infrastructure - PKI), а еще 26% планируют начать их пробную эксплуатацию. Средства биометрического контроля внедрены только в 5% организаций, и всего 11% планируют приступить к их пробной эксплуатации. 36% компаний имеют системы обнаружения вторжений (Intrusion Detection Systems), и еще 24% собираются их установить.

Перечислено несколько препятствий, мешающих более широкому распространению этих технологий. 38% опрошенных назвали основным препятствием стоимость технологий, хотя указывают также отсутствие квалификации, плохое понимание будущих технологий и технические вопросы.

Что это может означать для вашей компании

Уменьшение масштабов общения с деловыми партнерами не является выходом из положения. Обмен информацией растет, и вместе с ним растут риски. Постоянные усилия по обеспечению и контролю необходимого уровня безопасности должны стать одной из приоритетных задач для руководителей подразделений ИТ и компаний в целом. Поддержание безопасности и сохранение конфиденциальности информации по-прежнему остаются для респондентов главным препятствием обмену информацией. Поэтому организациям необходимо научиться быстро определять, какие типы рисков им могут угрожать, какие конкретные риски опасны для них в данный момент и какие действия следует предпринять для их минимизации. Результаты исследования говорят об упорном сопротивлении внедрению новых технологий, таких как средства биометрического контроля, беспроводные технологии и независимая сертификация киберпроцессов. Указан ряд причин, по которым эти технологии не внедряются. Очевидно, что компании недостаточно ясно представляют себе степень отработанности новых технологий, масштаб их распространения на рынке, равно как и возможность их привлечения к решению таких первоочередных задач, как установление личности и подтверждение подлинности документов.

Забота о безопасности является одной из главных причин инвестиций в ИТ во многих отраслях экономики, и недавние события это только подтвердили. Те компании, которые не

анализируют, каким образом новые технологии могут помочь им в работе, рискуют упустить шанс укрепить свою информационную безопасность.

Что вы можете сделать

1) Попробуйте в рамках бизнес-стратегии проанализировать (или повторно рассмотреть), в каком направлении с точки зрения безопасности и рисков должна двигаться ваша компания, ответив на такие вопросы:

- когда вы внедряете серьезные изменения в структуре организации для достижения конкурентных преимуществ, учитываете ли вы способность принятой системы безопасности обеспечить поддержку ваших планов;
- привели ли затраты на обеспечение безопасности к снижению рисков для компании. Не успокаивайте себя - проверьте.

2) Проанализируйте те аспекты информационной безопасности, которые играют для вашей организации решающую роль, например идентификацию и установление подлинности пользователей, по следующим показателям:

- проводили ли вы оценку рисков. Подумайте, является ли ваша информационная безопасность избыточной или недостаточной;
- известно ли вашим сотрудникам о необходимости не разглашать служебную информацию, беречь системы и оборудование.

3) Проанализируйте, какие технологии могли бы повысить эффективность безопасности в плане затрат, уровня услуг, надежности и т.п. Как и при работе с другими технологиями, сначала оцените ваши потребности:

- учитываете ли вы необходимость соблюдения безопасности с самого начала при разработке новых систем. Внедрение изменений для учета требований безопасности после того, как система уже разработана, всегда обходится дороже;
- принимаются ли во внимание будущие потребности организации при покупке новых вспомогательных технологий. Затраты на технологии имеют тенденцию увеличиваться при неправильном планировании.

4) Внедрите программу тщательной оценки инвестиций в информационную безопасность. При этом очень важно понять:

- позволяет ли эта программа проводить оценку портфеля затрат, разделять их на приоритетные направления;
- можно ли с помощью данной программы производить тщательную оценку эффективности инвестиций.

Что делать дальше

1) Несмотря на информированность сотрудников и понимание рисков, грозящих компании, опрос выявил тревожные пробелы в системе информационной безопасности респондентов.

2) Результаты опроса указывают на то, что успешному развитию многих организаций мешают постоянно увеличивающееся количество сбоев в работе жизненно важных систем, отсутствие расследований по случаям нарушения информационной безопасности и планов поддержания непрерывной деятельности, недостаточная информированность сотрудников и постоянно возрастающая сложность рисков, с которыми сталкивается организация.

3) Попытки устранить отдельные недостатки без учета остальных подвергают организацию целому ряду рисков, возникающих при недальновидном подходе.

4) Для эффективного функционирования системы ИБ необходима структура, устремленная в будущее. С помощью этой структуры компании смогут сделать безопасность одним из компонентов общей стратегии и планирования деятельности, управлять инвестициями и повышать доверие клиентов и инвесторов.

5) Использование данной структуры гарантирует, что при разработке и внедрении любых мер по укреплению безопасности будут приняты во внимание жизненно важные составные части бизнеса.

6) Имея в виду риски, с которыми сталкиваются компании, их уязвимые стороны, а также важность информационных систем и информации, мы считаем недопустимым, чтобы компания реагировала на события после того, как они произошли.

7) Если по какому-либо из приведенных далее пунктов ответ будет отрицательным, то руководителям предприятий необходимо срочно принять меры по повышению уровня ИБ в компании.

Вы используете последовательный, комплексный подход к вопросам обеспечения информационной безопасности во всей организации.

Ваш подход сбалансирован и учитывает возможности информационных технологий, технологических процессов и кадровых ресурсов.

Вы имеете четкое представление о затратах на ИБ и вам известна отдача от вложенных средств.

В компании реализованы регулярные и разумные меры по проверке эффективности систем и процедур защиты информации.

Служба безопасности знает и умело использует критерии качества и показатели защищенности, помогающие оценить эффективность системы ИБ в целом.

Введен план периодической переоценки информационных рисков и систем информационной безопасности.

Наступило время, когда руководителям компаний необходимо осознать важность информационной безопасности, научиться предвидеть будущие тенденции и управлять ими. Эффективная работа систем безопасности должна стать первоочередной задачей для всего предприятия.

Методология проведения исследования

В октябре и ноябре 2001 г. фирма «Эрнст энд Янг» опросила в ходе личных встреч и бесед по телефону репрезентативную группу директоров компаний по информационным технологиям и представителей руководства в 17 регионах мира. Беседы проводились в соответствии со специально подготовленным списком вопросов. Всего было охвачено 459 респондентов. Ответы обрабатывались на анонимной основе. Анализ ответов проводило известное агентство по исследованию рынка (IDA). Результаты были собраны в сводные таблицы, всесторонне проанализированы в рамках каждого вопроса и распределены по странам и отраслям экономики. С точки зрения статистики, полученная выборка обеспечивает достоверность 95±4%. Обрабатывая результаты, мы ссылались на исследования в области безопасности, предпринятые ранее фирмой «Эрнст энд Янг», чтобы определить существующие тенденции, а не с целью прямого сопоставления (рис. П2.1).

Дополнительную информацию вы можете получить на сайте www.ey.com/russia/security-risk или у консультантов в компании «Эрнст энд Янг».

«Эрнст энд Янг» - решение реальных проблем

Фирма «Эрнст энд Янг» оказывает профессиональные услуги организациям, представленным на рынках СНГ. К ее комплексными услугами в области аудита, налогов, законодательства и корпоративных финансов обращаются крупнейшие национальные и международные компании. Огромный опыт и высокая квалификация сотрудников - местных и иностранных специалистов - позволяет творчески подходить к решению стоящих перед ними задач. В 2002 г. фирмы «Эрнст энд Янг» и «Андерсен» объединили свою практику в более чем 50 странах мира. Благодаря этому масштаб деятельности новой объединенной фирмы расширился, и теперь их услугами могут пользоваться клиенты по всему миру.

Рис. П2.1. Подход компании к обеспечению безопасности

Международная сеть специалистов фирмы «Эрнст энд Янг» дает возможность воспользоваться уникальным опытом и высочайшей квалификацией в области информационной безопасности и контроля.

Приложение 3
Основные понятия и определения управления рисками

В этом приложении даются определения основных терминов по тематике анализа рисков, используемые различными авторами и организациями.

Терминология и определения в публикациях на русском языке

Базовый (Baseline) **анализ рисков** [123] - 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 безопасности.

Полный (Full) **анализ рисков** [123] - анализ рисков для информационных систем с повышенными требованиями в области ИБ (более высокие, чем базовый уровень защищенности). Это предполагает:

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

Угроза (Threat) [123] - 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 и проявляющегося в искажении и/или потере информации.

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

Последствия (атака) [14] - возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы с системой через имеющиеся факторы (уязвимости).

Как видно из определения, атака - это всегда пара «источник-фактор», реализующая угрозу и приводящая к ущербу.

Уязвимость (Vulnerability) [123] - слабость в системе защиты, которая делает возможной реализацию угрозы.

Уязвимость (Vulnerability) [123] - присущие объекту особенности, 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 [123] - процесс определения угроз, уязвимостей, возможного ущерба, а также контрмер.

Оценка рисков [123] (Risk Assessment) - идентификация рисков, выбор параметров для их описания и получение оценок по этим параметрам.

Риск нарушения ИБ (Security Risk) [123] - возможность реализации угрозы.

Цена риска [46] - размер ущерба, который может быть нанесен в результате некоторого события риска.

Вероятность риска [46] - вероятность возникновения события риска с определенной ценой риска в результате реализации некоторой комбинации угроз.

Размер риска [46] (ожидаемый ущерб или степень риска) - математическое ожидание (произведение цены риска на вероятность риска) возникновения события риска с определенной ценой и вероятностью риска этого события.

Рискообразующий потенциал [46] (угрозы объекту, структурной составляющей некоторой системы или системы в целом) - суммарный размер риска, который зависит от этого фактора при анализе возможных событий риска, обусловленных наличием указанной сущности со всеми характерными для нее на момент анализа качествами и характеристиками.

Терминология и определения на английском языке (определения взяты из глоссария [334] и даются в переводе)

Риск (risk):

- ожидаемые потери или возможный результат реализации угрозы при существовании уязвимости и определенных обстоятельств или событий, приводящих к реализации угрозы;
- возможность того, что определенная угроза реализуется из-за наличия определенной уязвимости системы;
- вероятность потерь в результате того, что определенная угроза при наличии уязвимости реализуется и приведет к негативным последствиям;
- возможность потери из-за одной или более угроз для информационных ресурсов (не путать с финансовым или деловым риском);
- ситуация, в которой существует уязвимость и потенциальный нарушитель имеет возможность и желание воспользоваться ею;
- возможность того, что специфическая уязвимость будет использована;
- потенциал, присущий данной угрозе из-за наличия уязвимости информационных ресурсов. При реализации этого потенциала организации может быть причинен вред;
- вероятность того, что специфическая угроза будет выполнена из-за наличия специфической уязвимости системы.

Анализ риска (risk analysis):

- процесс идентификации рисков, определения их величины и выделения областей, требующих защиты. Анализ риска - часть управления рисками;
- систематический процесс оценки величины рисков.

Оценка риска (risk assessment):

- процесс идентификации информационных ресурсов системы и угроз этим ресурсам, а также 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;
- составление списка рисков, ранжированных по цене и критичности. Список позволяет определить, где контрмеры должны примениться в первую очередь. Обычно невозможно предложить контрмеры, снижающие все аспекты рисков до нуля, так что некоторые остаточные риски сохраняются даже после того, как все доступные (по цене) контрмеры были приняты;
- изучение уязвимостей, угроз, вероятности, возможных потерь и теоретической эффективности контрмер. Определить ожидаемые потери и установить степень их

приемлемости позволяет процесс оценки угроз и уязвимости, описываемый в общедоступной методике, ставшей стандартом де-факто;

- процесс, который включает идентификацию риска, анализ риска, оценку риска;
- оценка угроз, воздействия на уязвимости информационных ресурсов и информационных процессов, а также вероятности их возникновения.

Идентификация риска - процесс идентификации рисков, при котором рассматриваются бизнес-цели, угрозы и уязвимость как основа для дальнейшего анализа.

Управление рисками (risk management):

- процесс идентификации, управления, устранения или уменьшения вероятности событий, способных негативно воздействовать на ресурсы системы;
- процесс, включающий идентификацию, управление и устранение или уменьшение вероятности событий, которые могут затрагивать информационные ресурсы системы;
- процесс идентификации, управления и уменьшения рисков безопасности, потенциально имеющих возможность воздействовать на информационную систему, при условии приемлемой стоимости средств защиты;
- процесс идентификации, управления, устранения или уменьшения вероятности событий, которые в состоянии негативно воздействовать на системные ресурсы системы. Этот процесс содержит анализ риска, анализ параметра «стоимость-эффективность», выбор, построение и испытание подсистемы безопасности и исследование всех аспектов безопасности;
- 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).

Учет рисков (risk treatment) - процесс планирования системы управления рисками, основанный на оценке рисков.

Уязвимость (vulnerability):

- слабость в защите, которая может стать объектом воздействия (например, из-за неверно проведенного анализа, планирования или реализации системы защиты);
- слабость в информационной системе или составляющая (например, системные процедуры защиты, аппаратная реализация или внутренние средства управления), способная привести к реализации негативных событий, связанных с информацией;
- слабость в процедурах защиты, проектировании информационной системы, реализации системы, внутренней системе управления и т.д., которая в состоянии способствовать нарушению политики информационной безопасности;
- недостатки или бреши на этапе проектирования информационной системы, ее реализации или управления ею, которые могут стать причиной нарушения политики информационной безопасности;
- слабость защиты в объекте потенциальной атаки (например, из-за недоработок на стадиях анализа, проектирования, построении системы или эксплуатации);
- существование слабости, ошибок проектирования или построения системы, из-за которых возможно наступление неожиданного, нежелательного события, компрометирующего систему ИБ, сеть, приложения или протоколы;
- слабость в информационной системе или компонентах (например, в процедурах обеспечения безопасности на системном уровне, проектных решениях на аппаратном уровне, системах управления), с помощью которых можно реализовать угрозу, связанную с информационными ресурсами;

– слабость в процедурах обеспечении безопасности, системном проекте, системе управления и т.д., способная случайно или преднамеренно вызвать нарушение политики ИБ. Свойство или слабость в процедурах обеспечения информационной безопасности, системе управления техническими средствами или физической защите, способствующие реализации угрозы;
– слабость ресурса или группы ресурсов информационной системы, помогающая реализовать угрозу;
– слабость в аппаратных средствах, программном обеспечении и потоках данных, которые составляют систему обработки информации. Слабости в автоматизированных системах обеспечения ИБ на программно-техническом уровне, системе административного управления, размещении оборудования и т.д., которые могут способствовать реализации угроз несанкционированного доступа к информации или привести к нарушениям в критически важном процессе обработки информации.

Анализ уязвимости (vulnerability analysis):

– систематически проводимая экспертиза информационной системы, позволяющая определять адекватность мер защиты целям и задачам организации, идентифицировать погрешности в построении защиты, собрать исходные данные, чтобы оценить эффективность предложенных мер защиты и подтвердить действенность таких мер после их реализации;
– систематически проводимая экспертиза информационной системы, предоставляющая возможность определить адекватность мер защиты целям и задачам организации, идентифицировать погрешности в построении защиты, собрать исходные данные для оценки эффективности предложенных мер защиты.

Объект оценки (Target of Evaluation (TOE)):

– отдельные элементы и результаты работы информационной системы или вся система в целом, включая администратора, пользовательскую документацию и руководства, которая является объектом оценки;
– отдельные элементы и результаты работы информационной системы или вся система, рассматриваемая на предмет оценки защищенности.

Оценка уязвимости (vulnerability assessment):

– аспект оценки эффективности защиты объекта оценки (TOE), а именно: определение, могла ли уязвимость в объекте оценки на практике компрометировать (поставить под угрозу) его защиту;
– оценка уязвимости, которая заключается в восприимчивости исследуемой системы к определенному виду атаки и возможности агента осуществить нападение.

Угроза (threat):

– действие или событие, способное нанести ущерб безопасности;
– последовательность обстоятельств и событий, позволяющих человеку или другому агенту воспользоваться уязвимостью информационной системы и причинить ущерб информационным ресурсам;
– любое обстоятельство или события, которые в состоянии причинить вред информационной системе в виде разрушения, раскрытия, модификации данных или отказа в обслуживании;
– потенциал нарушения режима безопасности, существующий, если складываются обстоятельства, производятся определенные действия или происходят события, способные нарушить режим безопасности и причинить вред;

– опасность, которая может иметь место в случае использования уязвимости. Угроза бывает либо умышленной (то есть задуманной и спланированной, например хакером или преступной организацией), либо случайной (скажем, результат сбоев компьютера или стихийного бедствия - землетрясения, пожара, урагана).

В некоторых контекстах термин «угроза» понимается узко и относится только к умышленным угрозам:

– в американских (US) 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;
– потенциальная причина нежелательного инцидента, который может завершиться причинением ущерба информационной системе или организации;
– действие или случай, которые в состоянии нанести ущерб системе защиты;
– любое обстоятельство или случай, имеющие возможность причинить вред системе в виде разрушения, раскрытия, модификации данных или отказа в обслуживании (DoS);
– потенциал для реализации уязвимости;
– объект или события, которые потенциально могут навредить системе;
– способности, намерения и методы нападения противников, обладающих возможностью воспользоваться совокупностью обстоятельств и реализовать существующий потенциал для причинения вреда информации или информационной системе;
– средства, посредством которых агент угрозы намеревается причинить ущерб информационной системе, отдельным информационным ресурсам или операциям;
– потенциальное нарушение защиты;
– потенциал реализации уязвимости, последствия которой выражаются в компрометации защиты системы или сетей.

Действие угрозы (threat action):

– нападение на системную защиту.

Агент угрозы (threat agent):

– метод, использующий уязвимость в системе, операциях (технологическом процессе) или отдельных средствах (элементах системы);
– методы и средства, основанные на применении уязвимостей в информационной системе, операциях или средстве; пожар, природные катаклизмы и т.д.

Анализ угрозы (threat analysis):

– оценка вероятности событий и определение возможных последствий разрушительных действий в системе;
– экспертиза всех действий и событий, которые могли бы неблагоприятно воздействовать на систему или результат ее функционирования.

Процесс оценки угрозы (threat assessment) - процесс формальной оценки степени серьезности угрозы информационной системе и описание характера угрозы.

Приложение 4
Каталоги угроз и контрмер IT Baseline

Каталоги угроз и контрмер, используемые в Германском стандарте IT Baseline Protection Manual

Каталог угроз

Содержит следующие группы угроз:

T1. Угрозы в связи с форс-мажорными обстоятельствами.

T2. Угрозы на организационном уровне.

T3. Угрозы, связанные с ошибками людей.

T4. Угрозы, связанные с техникой.

T5. Угрозы, возникающие на предпроектном этапе.

Ниже перечислены угрозы, входящие в каждую из групп. Детальное описание угроз на английском языке можно посмотреть по адресу http://www.bsi.bund.de/gshb/english/t/t1000.htm.

T 1. Угрозы в связи с форс-мажорными обстоятельствами

T1.1. Потеря персонала.

T1.2. Отказ информационной системы.

T1.3. Молния.

T1.4. Пожар.

T1.5. Затопление.

T1.6. Возгорание кабеля.

T1.7. Недопустимая температура и влажность.

T1.8. Пыль, загрязнение.

T1.9. Потеря данных из-за воздействия интенсивных магнитных полей.

T1.10. Отказ сети на большой территории.

T1.11. Катастрофы в окружающей среде.

T1.12. Проблемы, вызванные неординарными общественными событиями.

T1.13. Шторм.

T2. Угрозы на организационном уровне

T2.1. Отсутствие или недостатки регламентирующих документов.

T2.2. Недостаточное знание требований регламентирующих документов.

T2.3. Недостаточно совместимые или неподходящие ресурсы.

T2.4. Недостатки контроля и измерения уровня безопасности в информационной технологии.

T2.5. Недостатки в обслуживании.

T2.6. Несоответствие помещений требованиям в области безопасности.

T2.7. Превышение полномочий.

T2.8. Нерегламентированное использование ресурсов.

T2.9. Недостатки в процедурах отслеживания изменений в информационной технологии.

T2.10. Несоответствие среды передачи данных предъявляемым требованиям.

T2.11. Недостаточный горизонт планирования.

T2.12. Недостатки в документировании коммуникаций.

T2.13. Недостаточная защищенность от действий дистрибьюторов.

T2.14. Ухудшение использования информационных технологий из-за плохих условий на рабочих местах.

T2.15. Возможность несанкционированного доступа к конфиденциальным данным в ОС UNIX.

T2.16. Несанкционированное (недокументированное) изменение пользователей портативной ЭВМ.

T2.17. Неправильная маркировка носителей данных.

T2.18. Неверная доставка носителей данных.

T2.19. Некорректная система управления криптографическими ключами.

T2.20. Неподходящее обеспечение расходными материалами факсов.

T2.21. Ненадлежащая организация изменения пользователей.

T2.22. Отсутствие должной оценки результатов аудита данных.

T2.23. Подключение ПК под DOS в сеть, содержащую серверы.

T2.24. Несанкционированный доступ к конфиденциальным данным в сети.

T2.25. Уменьшение скорости обмена, вызванное вспомогательными функциями взаимодействия одноуровневых объектов.

T2.26. Недостаточное тестирование ПО.

T2.27. Неправильная документация.

T2.28. Нарушение авторского права.

T2.29. Несанкционированное тестирование программ на этапе эксплуатации ИС.

T2.30. Неправильное планирование доменной структуры.

T2.31. Некорректная защита систем под управлением ОС Windows NT.

T2.32. Неподходящая пропускная способность телекоммуникационных линий.

T2.33. Размещение Novell Netware Servers в опасном окружении.

T2.34. Отсутствие или некорректная настройка механизмов безопасности Novell Netware.

T2.35. Отсутствие аудита ОС Windows 95.

T2.36. Неправильные ограничения пользовательской среды.

T2.37. Неконтролируемое использование коммуникационных линий.

T2.38. Недостаточное или неправильное использование штатных механизмов защиты базы данных.

T2.39. Сложность DBMS.

T2.40. Сложность доступа к базам данных.

T2.41. Неверная организация обмена данных пользователей с базой данных.

T2.42. Сложность NDS.

T2.43. Миграция с ОС Novell 3.x на ОС Novell версии 4 и 5.

T2.44. Несовместимые активные и пассивные сетевые компоненты.

T2.45. Концептуальные ошибки проектирования сети.

T2.46. Превышение максимально допустимой длины кабеля.

T2.47. Передача данных по коммуникациям, не соответствующим требованиям безопасности.

T2.48. Неадекватное использование информации и документов при работе в домашних условиях.

T2.49. Недостаточное или неверное обучение телеобработке.

T2.50. Задержки, вызванные временными сбоями при удаленной работе.

T2.51. Плохая интеграция удаленных рабочих мест в информационную технологию.

T2.52. Более длинные временные периоды реакции системы в случае неверного выбора архитектуры системы.

T2.53. Неполные инструкции относительно замены аппаратно-программных средств на удаленных рабочих местах.

Т2.54. Несанкционированный доступ к данным через скрытые элементы данных.
Т2.55. Неконтролируемое использование электронной почты.
Т2.56. Ненадлежащее описание файлов.
Т2.57. Неправильное хранение носителей информации в случае аварий.
Т2.58. ОС Novell Netware и «проблема 2000».
Т2.59. Работа с незарегистрированными компонентами.
Т2.60. Недостаточная детализация стратегии сети и системы управления сетевыми ресурсами.
Т2.61. Неразрешенная совокупность личных данных.
Т2.62. Неподходящая обработка инцидентов в области безопасности.
Т2.63. Бесконтрольное использование факсов.
Т2.64. Недостатки или отсутствие правил для RAS.
Т2.65. Сложность конфигурации сервера SAMBA
Т2.66. Недостатки или неадекватность системы управления в области безопасности.
Т2.67. Недостатки администрирования прав доступа.

Т3. Угрозы, связанные с ошибками людей

Т3.1. Нарушение конфиденциальности/целостности данных в результате ошибок пользователей.
Т3.2. Разрушение оборудования или данных в результате небрежности.
Т3.3. Несоблюдение правил поддержания режима ИБ.
Т3.4. Несанкционированные подключения кабелей.
Т3.5. Повреждения кабелей из-за небрежности.
Т3.6. Опасности, связанные с увольнением или выведением персонала за штат.
Т3.7. Сбои АТС и ошибки оператора.
Т3.8. Запрещенные действия в информационной системе.
Т3.9. Запрещенные действия системного администратора.
Т3.10. Некорректный перенос файловой системы ОС UNIX.
Т3.11. Некорректная конфигурации сервера электронной почты sendmail.
Т3.12. Потери носителей с данных при их перевозке (перемещении).
Т3.13. Передача неправильных или нежелательных данных.
Т3.14. Неправильное (с юридической позиции) оформление факса.
Т3.15. Неправильное использование автоответчиков.
Т3.16. Неправильное администрирование сайта и прав доступа.
Т3.17. Смена пользователей ПК, не соответствующая внутренним правилам.
Т3.18. Совместное использование информационных ресурсов и оборудования.
Т3.19. Хранение паролей в ОС Windows 95 в открытом виде.
Т3.20. Неумышленное предоставление доступа для чтения.
Т3.21. Использование ключей с нарушениями правил.
Т3.22. Модификация системного реестра.
Т3.23. Нарушение правил администрирования DBMS.
Т3.24. Небрежность манипуляций с данными.
Т3.25. Небрежность при стирании (уничтожении) информации.
Т3.26. Небрежность при совместном использовании файловой системы.
Т3.27. Неверная синхронизация времени.
Т3.28. Неправильные конфигурации активных сетевых компонентов.
Т3.29. Недостатки системы сегментации.
Т3.30. Использование удаленных рабочих станций для личных нужд.

Т3.31. Хаотичность в организации данных.

Т3.32. Нарушение законодательства в использовании криптографии.

Т3.33. Неправильное использование криптомодулей.

Т3.34. Неудачная конфигурация системы управления.

Т3.35. Отключение сервера во время работы.

Т3.36. Неверное истолкование событий.

Т3.37. Непродуктивные исследования.

Т3.38. Ошибки в конфигурации и операциях.

Т3.39. Неправильное администрирование RAS.

Т3.40. Несоответствие используемых процедур аутентификации требованиям, предъявляемым к удаленным рабочим местам.

Т3.41. Неправильное использование сервисов удаленного доступа.

Т3.42. Опасные конфигурации RAS-клиентов.

Т3.43. Нарушение инструкций использования паролей.

Т3.44. Небрежности в обработке информации.

Т3.45. Некорректно работающая система идентификации партнеров.

Т3.46. Ошибки в конфигурации сервера Lotus Notes.

Т3.47. Ошибки в конфигурации доступа браузера к Lotus Notes.

Т4. Угрозы, связанные с техникой

Т4.1. Разрушения системы электроснабжения.

Т4.2. Отказы внутренних сетей электроснабжения.

Т4.3. Недействительность имеющихся гарантий.

Т4.4. Ухудшение состояния линий из-за воздействия окружающей среды.

Т4.5. Перекрестные подключения.

Т4.6. Броски напряжения в системе электроснабжения.

Т4.7. Дефекты кабелей информационных сетей.

Т4.8. Обнаруженные уязвимости ПО.

Т4.9. Разрушение внутренних источников электропитания.

Т4.10. Сложности доступа к сетевым ресурсам.

Т4.11. Недостатки аутентификации между NIS-сервером и NIS-клиентом.

Т4.12. Недостатки аутентификации между серверами и клиентами.

Т4.13. Потеря хранимых данных.

Т4.14. Отсутствие специальной бумаги для факсов.

Т4.15. Отправка сообщения по факсу неправильному получателю из-за неверной коммутации.

Т4.16. Неполучение сообщения, отправленного по факсу, из-за ошибки передачи.

Т4.17. Дефект факсимильного аппарата.

Т4.18. Разрядка аккумулятора или неправильное электропитание в автоответчиках.

Т4.19. Потери информации из-за старения (ухудшения качества) носителя данных.

Т4.20. Потери данных из-за старения (ухудшения качества) носителя данных.

Т4.21. Неправильное экранирование от транзитных потоков.

Т4.22. Уязвимости ПО или ошибки.

Т4.23. Уязвимости системы распознавания CD-ROM.

Т4.24. Преобразования имени файла при резервном копировании данных в ОС Windows 95.

Т4.25. Все еще активные подключения.

Т4.26. Отказ базы данных.

Т4.27. Несанкционированный доступ через ODBC.

Т4.28. Потери данных в базе данных.

Т4.29. Потери данных в базе данных, вызванные недостатком емкости диска.

Т4.30. Потеря целостности базы данных.

Т4.31. Отказ или сбой компонентов сети.

Т4.32. Отказ при отправке сообщений.

Т4.33. Отсутствие процедуры идентификации или ненадлежащее ее качество.

Т4.34. Отказ криптомодулей.

Т4.35. Некорректность криптоалгоритма.

Т4.36. Ошибки при кодировании данных.

Т4.37. Неполучение (несвоевременная доставка) электронной почты или квитанций.

Т4.38. Отказы компонентов системы управления сетью или информационной системой.

Т4.39. Концептуальные ошибки ПО.

Т4.40. Некорректная настройка RAS-клиента операционной среды.

Т4.41. Недостатки в мобильной сети связи.

Т4.42. Отказ мобильного телефона.

Т4.43. Недокументированные возможности.

Т5. Угрозы, возникающие на предпроектном этапе

Т5.1. Разрушение оборудования или вспомогательной инфраструктуры информационной системы.

Т5.2. Манипуляция данными или ПО.

Т5.3. Нарушения системы контроля доступа в помещениях.

Т5.4. Воровство.

Т5.5. Вандализм.

Т5.6. Нападения.

Т5.7. Перехват в линиях связи.

Т5.8. Манипуляции линиями связи.

Т5.9. Неавторизованное использование информационной системы.

Т5.10. Злоупотребления, связанные с удаленным доступом.

Т5.11. Несанкционированный доступ к конфиденциальным данным, сохраненным в процессе инсталляции офисной АТС.

Т5.12. Перехват телефонных звонков и передаваемых данных.

Т5.13. Подслушивание.

Т5.14. Пользование телефоном для личных нужд.

Т5.15. «Любознательные» сотрудники.

Т5.16. Угрозы, исходящие от персонала (штатных сотрудников) в процессе обслуживания/администрирования информационной системы.

Т5.17. Угрозы, исходящие от посторонних специалистов, привлекаемых для обслуживания элементов информационной системы.

Т5.18. Подбор паролей.

Т5.19. Злоупотребления правами пользователей.

Т5.20. Злоупотребления правами администратора.

Т5.21. Вредоносное ПО. «Троянские» кони.

Т5.22. Воровство мобильных элементов информационной системы.

Т5.23. Враждебные апплеты и вирусы.

Т5.24. Закладки.

Т5.25. Маскарад.

Т5.26. Подслушивание и перехват сообщений.

Т5.27. Отказ от авторства сообщения.

Т5.28. Недоступность сервисов.

Т5.29. Несанкционированное копирование носителей данных.

Т5.30. Несанкционированное использование факсимильных машин.

Т5.31. Несанкционированный просмотр поступающих по факсу сообщений.

Т5.32. Информация, остающаяся в факсимильных машинах.

Т5.33. Использование факсимильных машин для доставки поддельных писем.

Т5.34. Преднамеренное перепрограммирование факсимильных машин.

Т5.35. Манипуляции с поступающими по факсу сообщениями.

Т5.36. Перезагрузка автоответчиков.

Т5.37. Определение кодов доступа.

Т5.38. Неправильные употребления отдаленного запроса.

Т5.39. Проникновение в информационную систему через системы связи.

Т5.40. Ненадлежащий контроль помещений, в которых установлены компьютеры, оборудованные микрофонами.

Т5.41. Некорректное использование программ под управлением ОС UNIX, использующих протокол uucp.

Т5.42. Враждебное использование методов социальной инженерии.

Т5.43. Макровирусы.

Т5.44. Злоупотребление доступом к отдаленным портам для получения чужих данных.

Т5.45. Подбор пароля в ОС Windows.

Т5.46. Маскарад в АРМ под управлением ОС Windows.

Т5.47. Уничтожение почтового сервера.

Т5.48. Атака IP Spoofing.

Т5.49. Злоупотребления с маршрутизацией данных.

Т5.50. Злоупотребления с протоколом ICMP.

Т5.51. Злоупотребления с протоколом маршрутизации.

Т5.52. Злоупотребления правами администратора в системах под Windows NT.

Т5.53. Неправильное использование защитных кабинетов.

Т5.54. Преднамеренные действия, приводящие к аварийному завершению.

Т5.55. Вход в обход системы аутентификации.

Т5.56. Ненадлежащий учет пользователей, имеющих свободный доступ к сетевым ресурсам.

Т5.57. Несанкционированный запуск сканеров сети.

Т5.58. Взлом ОС Novell Netware.

Т5.59. Злоупотребление правами администратора в сетях Novell Netware 3.x.

Т5.60. Рекомендации по обходу системы.

Т5.61. Злоупотребления, связанные с удаленным управлением маршрутизатором.

Т5.62. Злоупотребления, связанные с удаленным управлением ресурсами информационной системы.

Т5.63. Манипуляции через D-канал ISDN.

Т5.64. Манипуляции данными или программным обеспечением базы данных.

Т5.65. Отказ в обслуживании базы данных.

Т5.66. Неразрешенные подключения в ЛВС информационной системы.

Т5.67. Несанкционированное управление сетевыми ресурсами.

T5.68. Несанкционированный доступ к активному сетевому оборудованию.

T5.69. Риск воровства на домашнем рабочем месте.

T5.70. Манипуляции, выполняемые родственниками или посетителями.

T5.71. Несанкционированный доступ к конфиденциальной информации определенных категорий пользователей.

T5.72. Неразрешенное использование почтовых услуг.

T5.73. Маскарад отправителя.

T5.74. Манипуляции файлами рассылки и псевдонимами.

T5.75. Перегрузка при получении письма по электронной почте.

T5.76. Вредоносное ПО в почте.

T, 5.77. Несанкционированное ознакомление с электронной почтой.

T5.78. Атака DNS spoofing.

T5.79. Несанкционированное приобретение прав администратора под Windows NT.

T5.80. Атака Hoaxes.

T5.81. Неразрешенное использование криптомодулей.

T5.82. Манипуляции криптомодулями.

T5.83. Компрометация криптографических ключей.

T5.84. Подделка удостоверений.

T5.85. Потеря целостности информации, которая должна быть защищена.

T5.86. Манипуляции параметрами управления.

T5.87. Атака Web spoofing.

T5.88. Неправильное использование активного контента.

T5.89. Захват сетевых подключений.

T5.90. Манипуляции списками рассылки и адресными книгами.

T5.91. Отключение механизма защиты доступа RAS.

T5.92. Использование клиента RAS в качестве сервера.

T5.93. Разрешение третьим лицам использовать RAS-компоненты.

T5.94. Неправильное употребление компонентов оборудования.

T5.95. Подслушивание конфиденциальных переговоров по мобильным телефонам.

T5.96. Вмешательство с использованием мобильных телефонов.

T5.97. Неразрешенная передача данных по мобильным телефонам.

T5.98. Перехват телефонных звонков с мобильных телефонов.

T5.99. Перехват трафика мобильных телефонов.

T5.100. Злоупотребление активным контентом для доступа к Lotus Notes.

T5.101. Взлом Lotus Notes.

T5.102. Саботаж.

Каталог контрмер

Каталог, доступный по адресу http://www.bsi.bund.de/gshb/english/menue.htm. содержит следующие группы контрмер для обеспечения безопасности:

- поддерживающей инфраструктуры;
- на организационном уровне;
- на кадровом уровне;
- программного обеспечения и вычислительной техники;

– коммуникаций;

– непрерывности бизнеса.

Далее перечисляются контрмеры, входящие в каждую из групп. Детальное описание контрмер на английском языке можно найти на сайте http://www.bsi.bund.de/gshb/english/s/s1000.htm.

S1. Обеспечение безопасности на уровне поддерживающей инфраструктуры

S1.1. Соответствие стандартам и отраслевым спецификациям элементов инфраструктуры.

S1.2. Система контроля со стороны правительства над производителями и дистрибьюторами электроэнергии, телефонными сетями, газо- и водоснабжением.

S1.3. Периодические проверки поддерживающей инфраструктуры (электропитания, климатических систем и т.д.) на соответствие предъявляемым к ним (на текущий момент) требованиям.

S1.4. Грозо- и молниезащита.

S1.5. Гальваническая развязка с внешними сетями.

S1.6. Соответствие помещений требованиям стандартов в области пожарной безопасности.

S1.7. Автоматические (дистанционные) системы пожаротушения.

S1.8. Использование отделочных материалов, соответствующих требованиям в области пожарной безопасности.

S1.9. Использование силовых и информационных кабелей с пожароустойчивой изоляцией.

S1.10. Наличие запасных выходов для персонала.

S1.11. Наличие планов коммуникаций, относящихся к инфраструктуре (электро-, газо- и водоснабжению).

S1.12. Организация защиты воздухозаборников, климатического оборудования, распределительных щитов.

S1.13. Организация защиты зданий и прилегающей территории от внешних факторов: затопления, автомобильного движения и т.п.

S1.14. Автоматизация дренажных работ. В некоторых помещениях (в подвалах, подверженных частым затоплениям) необходимо установить насосы, включающиеся автоматически в случае возникновения угрозы затопления.

S1.15. Контроль доступа. Окна и двери должны быть закрыты в отсутствие

людей.

S1.16. Схемы размещения. Распределение персонала по комнатам следует производить с учетом требований минимизации перемещения людей. Подразделения, не связанные технологически, должны быть по возможности изолированы.

S1.17. Наличие эффективного контроля на входе в помещение.

S1.18. Наличие приборов (датчиков) охранной и пожарной сигнализации.

S1.19. Комплекс мер защиты от проникновения посторонних в помещения.

S1.20. Разделение кабелей с разными требованиями в области защиты (с разными физическими и механическими свойствами).

S1.21. Соответствие мест прокладки кабелей необходимым требованиям.

S1.22. Физическая защита мест прокладки кабелей.

S1.23. Отсутствие открытых неиспользуемых дверей.

S1.24. Отсутствие близко расположенных трубопроводов (тепло- и водоснабжения).

S1.25. Защита от высокого напряжения.

S1.26. Защита силовых проводов от обрывов и повреждений.

S1.27. Климатическое оборудование.

S1.28. Использование UPS.

S1.29. Правильное расположение элементов информационной системы.

S1.30. Обеспечение сохранности регистрационной информации о входящих/ исходящих сообщениях.

S1.31. Удаленная индикация сбоев (неисправностей) оборудования.

S1.32. Корректная настройка консолей, устройств передачи данных, принтеров.

S1.33. Обеспечение сохранности переносных (мобильных) ПК при использовании их вне территории организации.

S1.34. Обеспечение сохранности переносных (мобильных) ПК при использовании их в качестве офисных ПК.

S1.35. Организация хранения временно не используемых переносных (мобильных) ПК.

S1.36. Организация хранения носителей данных с записанными на них резервными копиями и другими данными.

S1.37. Меры безопасности при эксплуатации факсов.

S1.38. Меры безопасности при эксплуатации модемов.

S1.39. Защита данных в линиях связи.

S1.40. Обеспечение сохранности кабелей.

S1.41. Защита от ПЭМИН.

S1.42. Обеспечение безопасности сервисов Novell.

S1.43. Обеспечение безопасности маршрутизации ISDN.

S1.44. Меры безопасности при организации рабочих мест в домашних условиях.

S1.45. Организация надежного хранения важных данных и документов.

S1.46. Использование техники, предотвращающей кражи.

S1.47. Локализация пожароопасных мест.

S1.48. Противопожарная сигнализация.

S1.49. Формализация технических и административных требований к организации рабочих мест и других элементов информационной системы.

S1.50. Защита от курения на рабочих местах.

S1.51. Уменьшение возможных последствий пожара.

S1.52. Уменьшение избыточности технологической инфраструктуры.

S1.53. Видеонаблюдение.

S1.54. Раннее обнаружение пожара.

S1.55. Защита периметра.

S1.56. Альтернативные источники электропитания.

S1.57. Документирование инфраструктуры и планы здания.

S1.58. Технические и организационные требования к помещениям для размещения серверов.

S2. Обеспечение безопасности на организационном уровне

S2.1. Распределение должностных обязанностей в сфере IT.

S2.2. Управление ресурсами.

S2.3. Контроль за средой передачи данных.

S2.4. Планирование мероприятий в области ремонта и поддержки.
S2.5. Разделение ответственности и функций.
S2.6. Регламентация доступа к информационным ресурсам.
S2.7. Регламентация привилегий различных групп пользователей.
S2.8. Регламентация правил доступа к приложениям и данным.
S2.9. Запрещение использования ПО, не входящего в список официально разрешенного.
S2.10. Список разрешенного ПО и его владельцев.
S2.11. Правила использования паролей.
S2.12. Служба поддержки для пользователей.
S2.13. Правильное расположение информационных ресурсов, требующих защиты.
S2.14. Управление доступом к ключам от помещений.
S2.15. Инспекция пожарной безопасности.
S2.16. Сопровождение посетителей.
S2.17. Правила доступа на территорию посторонних.
S2.58. Ограничение времени сообщения.
S2.59. Приобретение подходящего модема.
S2.60. Администрирование модемов с учетом требований ИБ.
S2.61. Документирование процедур пользования модемами.
S2.62. Разрешенное к применению ПО и процедуры санкционирования его применения.
S2.63. Права доступа.
S2.64. Просмотр log-файлов.
S2.65. Проверка эффективности разграничения пользователей в информационной системе.
S2.66. Приобретение только сертифицированных элементов.
S2.67. Стратегии для одноранговых сетей.
S2.68. Применение процедур контроля безопасности в одноранговых сетях.
S2.69. Стандарты на рабочие станции.
S2.70. Использование МЭ.
S2.71. Политика ИБ для МЭ.
S2.72. Требования к МЭ.
S2.73. Выбор подходящего МЭ.
S2.74. Выбор подходящего пакетного фильтра.
S2.75. Выбор подходящего шлюза.
S2.76. Определение правил фильтрации.
S2.77. Конфигурация компонентов, соответствующая требованиям безопасности.
S2.78. Правила работы с МЭ.
S2.79. Определение ответственных за использование стандартного ПО.
S2.80. Каталоги используемого стандартного ПО.
S2.81. Выбор подходящего стандартного ПО.
S2.82. Разработка плана тестирования стандартного ПО.
S2.83. Тестирование стандартного ПО.
S2.84. Разработка инструкций по инсталляции стандартного ПО
S2.85. Санкционирование установки стандартного ПО.

S2.86. Гарантии совместимости стандартного ПО.

S2.87. Инсталляция и конфигурирование стандартного ПО.

S2.88. Управление лицензированием и контроль за версиями ПО.

S2.89. Деинсталляция стандартного ПО.

S2.90. Контроль поставок ПО.

S2.91. Определение стратегии безопасности для клиент-серверных приложений Windows NT.

S2.92. Выбор способов контроля безопасности для клиент-серверных приложений Windows NT.

S2.93. Планирование конфигурации сети на основе ОС Windows NT.

S2.94. Совместное использование директорий в сетях под управлением ОС Windows NT.

S2.95. Обеспечение должной защиты шкафов.

S2.96. Блокирование шкафов с важными ресурсами.

S2.97. Корректные процедуры для электронных замков.

S2.98. Безопасность при инсталляции Novell Netware servers.

S2.99. Штатные механизмы безопасности Novell Netware servers.

S2.100. Обеспечение ИБ при использовании Novell Netware servers.

S2.101. Проверка Novell Netware servers.

S2.102. Активизация удаленных консолей.

S2.103. Профили пользователей в ОС Windows 95.

S2.104. Руководство пользователя по безопасности для ОС Windows 95.

S2.105. Расширение учрежденческой АТС.

S2.106. Выбор подходящих ISDN-плат.

S2.107. Документирование конфигурации ISDN-плат.

S2.108. Удаленная поддержка ISDN gateways.

S2.109. Назначение прав при удаленном доступе.

S2.110. Руководство по работе с log-файлами.

S2.111. Сохранность руководств.

S2.112. Соблюдение правил обмена файлами и данными между рабочими станциями и получателями.

S2.113. Документирование процедурных вопросов, связанных с использованием телекоммуникаций.

S2.114. Потоки информации вовне и извне.

S2.115. Поддержка удаленного доступа.

S2.116. Использование телекоммуникаций.

S2.117. Управление доступом к телекоммуникациям.

S2.118. Политика безопасности при использовании e-mail.

S2.119. Инструкции по использованию e-mail.

S2.120. Конфигурирование почтового сервера.

S2.121. Регулярное уничтожение писем e-mail.

S2.122. Стандартизация адресов e-mail.

S2.123. Выбор провайдера.

S2.124. Выбор подходящей СУБД.

S2.125. Инсталляция и конфигурирование СУБД.
S2.126. Разработка концепции безопасности для СУБД.
S2.127. Интерфейс.
S2.128. Управление доступом к СУБД (организационные аспекты).
S2.129. Управление доступом к информации в СУБД.
S2.130. Гарантии целостности СУБД.
S2.131. Разделение задач администрирования и поддержания СУБД.
S2.132. Конфигурирование доступа пользователей и групп пользователей.
S2.133. Контроль за log-файлами.
S2.134. Руководства по использованию СУБД.
S2.135. Безопасность обмена данными с СУБД.
S2.136. Правила безопасности для вычислительной среды рабочих станций.
S2.137. Процедуры резервного копирования.
S2.138. Структурирование данных при хранении.
S2.139. Обзор сетевой инфраструктуры.
S2.140. Анализ сетевой инфраструктуры.
S2.141. Концепция развития сетевой инфраструктуры.
S2.142. Разработка планов развития сетевой инфраструктуры.
S2.143. Система управления сетевыми протоколами.
S2.144. Выбор протокола управления сетевыми ресурсами.
S2.145. Средства управления сетью.
S2.146. Обеспечение ИБ системы управления сетью.
S2.147. Вопросы ИБ при миграции на старшие версии Novell.
S2.148. Конфигурирование Novell Netware 4.x networks.
S2.149. Обеспечение безопасности Netware 4.x networks.
S2.150. Аудит сетей Novell Netware 4.x.
S2.151. Разработка концепции NDS.
S2.152. Разработка концепции синхронизации времени.
S2.153. Документирование на Novell Netware 4.x networks.
S2.154. Концепция защиты от вирусов.
S2.155. Идентификация уязвимостей для вирусов.
S2.156. Выбор подходящей стратегии антивирусной защиты.
S2.157. Выбор подходящей антивирусной программы.
S2.158. Обработка сообщений о заражении вирусами.
S2.158. Обновление антивирусных программ.
S2.160. Управление антивирусными программами.
S2.161. Разработка концепции использования криптографии.
S2.162. Необходимость использования криптографических продуктов.
S2.163. Факторы, влияющие на выбор криптографических продуктов.
S2.164. Выбор адекватных процедур криптографической защиты.
S2.165. Выбор подходящих криптографических продуктов.
S2.166. Организационные аспекты использования криптографии.

S2.167. Обеспечение безопасности при уничтожении носителей информации.

S2.168. Системный анализ информационной системы, предшествующий выбору системы управления.

S2.169. Разработка стратегических целей системы управления.

S2.170. Требования к системе управления.

S2.171. Выбор продуктов для использования в системе управления.

S2.172. Разработка концепции использования WWW.

S2.173. Определение стратегии безопасности для WWW.

S2.174. Вопросы безопасности, связанные с сервером WWW.

S2.175. Настройки сервера WWW.

S2.176. Выбор Internet-провайдера.

S2.177. Обеспечение безопасности при переездах.

S2.178. Руководство по использованию факса.

S2.179. Процедуры управления факс-сервером.

S2.180. Настройки fax/mail-серверов.

S2.181. Выбор подходящего факс-сервера.

S2.182. Регулярный пересмотр критериев безопасности.

S2.183. Анализ аспектов безопасности, связанных с удаленным доступом.

S2.184. Разработка концепции безопасности удаленного доступа.

S2.185. Выбор архитектуры удаленного доступа.

S2.186. Выбор продукта, обеспечивающего безопасность удаленного доступа.

S2.187. Определение настроек продукта, обеспечивающего безопасность удаленного доступа.

S2.188. Правила использования мобильной связи.

S2.189. Блокирование мобильных телефонов в случае их утраты.

S2.190. Настройки пула мобильных телефонов.

S2.191. Процедуры, обеспечивающие ИБ (организационные аспекты).

S2.192. Политика безопасности и ее изменение.

S2.193. Организационная структура в области ИБ.

S2.194. Описание существующей информационной системы.

S2.195. Разработка (модернизация) концепции ИБ.

S2.196. Синхронизация этапов концепции ИБ и этапов развития системы.

S2.197. Концепция обучения в области ИБ.

S2.198. Проведение обучения персонала.

S2.199. Поддержание режима ИБ.

S2.200. Подготовка докладов в области ИБ.

S2.201. Документирование процедур и процессов в области ИБ.

S2.202. Подготовка руководства по обеспечению ИБ (организационные аспекты).

S2.203. Подготовка взаимосвязанных документов в области ИБ.

S2.204. Предотвращение несанкционированного доступа в сетях.

S2.205. Обмен персональными данными.

S2.206. Планирование использования Lotus Notes.

S2.207. Руководство по безопасности Lotus Notes.

S2.208. Планирование доменной структуры и иерархии сертификатов Lotus Notes.

S2.209. Планирование использования Lotus Notes в системе Intranet.

S2.210. Планирование использования Lotus Notes в системе Intranet с доступом через браузер.

S2.211. Планирование использования Lotus Notes в демилитаризованной зоне.

S2.212. Организационные аспекты, связанные с уборкой помещений и техники.

S2.213. Поддержка технической инфраструктуры.

S2.214. Концепция операций в информационной технологии.

S2.215. Меры по коррекции ошибок.

S2.216. Санкционирование процедур для отдельных компонентов информационной технологии.

S2.217. Классификация информационных ресурсов.

S2.218. Процедуры контроля обмена данными в информационной системе.

S2.219. Постоянное документирование изменений в информационной системе.

S2.220. Руководство по управлению доступом.

S2.221. Управление изменениями.

S2.222. Регулярная проверка параметров режима ИБ.

S2.223. Аспекты безопасности при использовании стандартного ПО.

S2.224. Защита от вредоносного ПО.

S2.225. Назначение ответственных за информационные ресурсы и отдельные компоненты информационной системы.

S2.226. Использование специалистов по временным трудовым договорам и специалистов сторонних организаций по договорам.

S3. Обеспечение безопасности на кадровом уровне

S3.1. Система обучения нового (поступающего на работу) персонала.

S3.2. Обязательства персонала в части следования законам и внутренним инструкциям.

S3.3. Проверка знаний сотрудников по исполнению своих обязанностей.

S3.4. Обучение перед использованием приложений.

S3.5. Обучение измерению параметров режима ИБ.

S3.6. Процедуры в отношении заканчивающих работу в компании.

S3.7. Пункты контракта в отношении личных проблем.

S3.8. Предотвращение конфликтов в коллективе.

S3.9. Эргономика рабочих помещений.

S3.10. Выбор надежного администратора безопасности и его замена.

S3.11. Обучение по вопросам эксплуатации средств защиты.

S3.12. Информирование персонала о возможностях местной АТС и о предупредительных сигналах.

S3.13. Уменьшение численности персонала, имеющего доступ к АТС и ее настройкам.

S3.14. Информирование персонала о процедурах корректного обмена данными с посторонними.

S3.15. Информирование персонала о процедурах корректного использования факсов.

S3.16. Информирование персонала о корректном использовании автоответчика.

S3.17. Информирование персонала о корректном использовании модема.

S3.18. Выключение ПК при уходе.

S3.19. Инструкции относительно корректного (безопасного) соединения взаимодействующих систем.

S3.20. Инструкции по защите служебных помещений от доступа посторонних.

S3.21. Обучение вопросам безопасности при использовании телекоммуникаций.

S3.22. Вопросы замены телекоммуникационного оборудования.

S3.23. Основы криптографической защиты.

S3.24. Обучение администраторов архитектуре Lotus Notes.

S3.25. Обучение пользователей механизмам безопасности Lotus Notes.

S3.26. Инструктаж персонала по вопросам безопасного использования (конфигурирования) элементов информационной технологии.

S4. Защита программного обеспечения и вычислительной техники

S4.1. Парольная защита.

S4.2. Использование экранных заставок для блокировки доступа.

S4.3. Периодическое использование антивирусных средств.

S4.4. Блокирование дисковода.

S4.5. Протоколирование действий администратора учрежденческой АТС.

S4.6. Аудит конфигурации учрежденческой АТС.

S4.7. Замена паролей.

S4.8. Защита консоли оператора учрежденческой АТС.

S4.9. Использование механизмов безопасности X Windows.

S4.10. Парольная защита терминалов учрежденческой АТС.

S4.11. Экранирование интерфейсов учрежденческой АТС.

S4.12. Удаление неиспользуемого оборудования.

S4.13. Выбор идентификаторов.

S4.14. Парольная защита в ОС UNIX.

S4.15. Безопасность при входе в систему.

S4.16. Ограничение доступа к терминалам.

S4.17. Блокирование доступа к неиспользуемым устройствам и терминалам.

S4.18. Административные и технические средства контроля работы пользователей.

S4.19. Ограничения на атрибуты файлов и директорий в UNIX (правила администрирования).

S4.20. Ограничения на атрибуты файлов и директорий в UNIX (правила для пользователей).

S4.21. Предотвращение незаконного использования прав администратора.

S4.22. Предотвращение потери конфиденциальных и важных данных в UNIX.

S4.23. Обеспечение безопасности EXE-файлов.

S4.24. Обеспечение управления системой.

S4.25. Использование log-файлов в ОС UNIX.

S4.26. Проверка режима безопасности в ОС UNIX.

S4.27. Парольная защита в портативных ПК.

S4.28. Смена системного ПО в случае изменения пользователя портативного ПК.

S4.29. Криптографическая защита в портативных ПК.

S4.30. Использование штатных средств безопасности прикладного ПО.

S4.31. Обеспечение электропитания при мобильном использовании портативного ПК.

S4.32. Уничтожение информации до и после использования средств хранения данных.

S4.33. Антивирусный контроль при передаче данных.

S4.34. Использование криптографии, контрольных сумм, ЭЦП.

S4.35. Проверка правильности перенаправления потоков данных.

S4.36. Блокирование учетной информации, передаваемой по факсу.

S4.37. Блокирование номера отправителя факса.

S4.38. Удаление сервисов, не являющихся необходимыми.

S4.39. Отключение автоответчиков на период длительного отсутствия.

S4.40. Предотвращение несанкционированного использования микрофонов.

S4.41. Использование подходящих программных продуктов для защиты информации.

S4.42. Инструментарий для обеспечения безопасности при работе приложений.

S4.43. Факсы с системой защиты от изменения установок.

S4.44. Проверка входящих файлов на отсутствие макровирусов.

S4.45. Обеспечение безопасности среды при взаимодействии объектов с равными правами.

S4.46 Использование паролей в ОС Windows 95.

S4.47. Ведение журналов при работе МЭ.

S4.48. Парольная защита в ОС Windows NT.

S4.49. Обеспечение защиты от загрузки с дискеты в ОС Windows NT.

S4.50. Системное администрирование в ОС Windows NT.

S4.51. Профили пользователей и ограничения в ОС Windows NT.

S4.52. Защита оборудования, функционирующего под управлением ОС Windows NT.

S4.53. Ограничения на доступ к файлам и директориям под управлением ОС Windows NT.

S4.54. Документирование событий в ОС Windows NT.

S4.55. Инсталляция ОС Windows NT в соответствии с требованиями безопасности.

S4.56. Уничтожение информации в ОС Windows NT и ОС Windows 95.

S4.57. Отключение возможности использования CD-ROM.

S4.58. Совместное использование файлов в ОС Windows 95.

S4.59. Отключение неиспользуемых функций ISDN.

S4.60. Отключение ненужных функций маршрутизации ISDN.

S4.61. Использование штатных механизмов безопасности компонентов ISDN.

S4.62. Использование фильтров.

S4.63. Выполнение требований в области информационной безопасности.

S4.64. Проверка данных перед отправкой и уничтожением.

S4.65. Предварительное тестирование оборудования и данных.

S4.66. Novell Netware - проверка решения «проблемы 2000».

S4.67. Блокирование и удаление регистрации пользователей баз данных, которым она более не требуется.

S4.68. Управление базой данных.

S4.69. Регулярная проверка состояния безопасности в СУБД.

S4.70. Мониторинг состояния базы данных.
S4.71. Ограничение на использование связей, имеющихся в СУБД.
S4.72. Криптографическая защита СУБД. S4.73. Спецификация на ограничение.
S4.74. Сети с ПК под управлением ОС Windows 95.
S4.75. Защита регистра в ПК под управлением ОС Windows NT.
S4.76. Версии ОС Windows NT с повышенным уровнем безопасности.
S4.77. Защита администратора в сетях на основе ОС Windows NT.
S4.78. Безопасность при модернизации.
S4.79. Механизмы безопасности при локальном администрировании.
S4.80. Механизмы безопасности при удаленном администрировании.
S4.81. Аудит журналов (log-файлов) с записями о сетевой активности.
S4.82. Вопросы безопасности при конфигурировании активного сетевого оборудования.
S4.83. Обновление компонентов сетевой инфраструктуры и ПО.
S4.84. Использование механизмов безопасности BIOS.
S4.85. Интерфейс модулей криптозащиты.
S4.86. Безопасность при разделении ролей персонала и конфигурировании криптомодулей.
S4.87. Физическая безопасность криптографических устройств.
S4.88. Требования к операционным системам, в которых устанавливаются криптомодули.
S4.89. Безопасность излучения (уровней полей) приборов.
S4.90. Использование криптографической защиты на разных уровнях модели ISO/OSI.
S4.91. Безопасность при инсталляции системы управления.
S4.92. Безопасность выполнения операций в системе управления.
S4.93. Регулярная проверка целостности.
S4.94. Защита WWW-файлов.
S4.95. Минимизация действий в информационной системе.
S4.96. Отключение DNS.
S4.97. Один сервис на один сервер.
S4.98. Ограничение потоков информации путем использования пакетных фильтров.
S4.99. Защиты от изменения информации.
S4.100. Межсетевые экраны и защита информационных ресурсов.
S4.101. Межсетевые экраны и криптография.
S4.102. Обеспечение уровня безопасности C2 для Novell 4.11.
S4.103. Сервер DHCP (Dynamic Host Configuration Protocol) под Novell Netware 4.x.
S4.104. Сервисы LDAP для NDS.
S4.105. Первоначальные измерения после инсталляции UNIX.
S4.106. Активация системных log-файлов.
S4.107. Сервисная поддержка производителя.
S4.108. Управление сервисом DNS под Novell NetWare 4.11.
S4.109. Переустановка ПО на рабочих станциях.
S4.110. Безопасность при инсталляции службы удаленного доступа.
S4.111. Безопасная конфигурация службы удаленного доступа.
S4.112. Безопасная работа с использованием службы удаленного доступа.

S4.113. Использование сервера аутентификации внутри службы удаленного доступа.

S4.114. Безопасность при использовании мобильных телефонов.

S4.115. Безопасность электропитания в мобильных телефонах.

S4.116. Безопасность при инсталляции Lotus Notes.

S4.117. Безопасность при конфигурировании сервера Lotus Notes.

S4.118. Конфигурирование сервера Lotus Notes.

S4.119. Ограничения по доступу к серверу Lotus Notes.

S4.120. Конфигурирование доступа к управляющим спискам базы данных Lotus Notes.

S4.121. Конфигурирование прав доступа к Lotus Notes Name и Address Book.

S4.122. Конфигурирование браузера доступа к Lotus Notes.

S4.123. Конфигурирование SSL в браузере доступа к Lotus Notes.

S4.124. Конфигурирование механизма аутентификации при доступе к Lotus Notes.

S4.125. Установление ограничений доступа к базам данных Lotus Notes через браузер.

S4.126. Безопасность при конфигурировании клиента Lotus Notes.

S4.127. Конфигурация браузера доступа к Lotus Notes, соответствующая требованиям безопасности.

S4.128. Работа в Lotus Notes (аспекты безопасности).

S4.129. Поддержка файлов Notes ID (аспекты безопасности).

S4.130. Оценка уровня безопасности при создании базы данных Lotus Notes.

S4.131. Использование криптографии в базе данных Lotus Notes.

S4.132. Мониторинг в Lotus Notes.

S4.133. Выбор подходящего механизма аутентификации.

S4.134. Выбор подходящих форматов данных.

S4.135. Ограничения, которые позволят контролировать доступ к файлам.

S5. Защита коммуникаций

S5.1. Удаление или заземление неиспользуемых линий.

S5.2. Выбор подходящей топологии сети.

S5.3. Выбор кабелей.

S5.4. Документирование и маркировка кабелей.

S5.5. Прокладка кабелей с учетом минимизации возможных повреждений.

S5.6. Разрешение использования сетевых паролей.

S5.7. Управление сетью.

S5.8. Ежемесячные проверки сети с позиции безопасности.

S5.9. Ведение журналов.

S5.10. Ограничение прав доступа.

S5.11. Блокировка консоли сервера.

S5.12. Конфигурации для второго (дублирующего) администратора.

S5.13. Оборудование для соединения сетей.

S5.14. Экранирование удаленного доступа.

S5.15. Экранирование доступа извне.

S5.16. Обзор сетевых сервисов.

S5.17. Использование механизмов безопасности для NFS.

S5.18. Использование механизмов безопасности для NIS.

S5.19. Использование механизмов безопасности для sendmail.

S5.20. Использование механизмов безопасности для rlogin, rsh. rcp.

S5.21. Безопасность для telnet, ftp, tftp. rexec.

S5.22. Проверка совместимости систем приема и передачи.

S5.23. Выбор подходящего телекоммуникационного оборудования.

S5.24. Список доступа для fax.

S5.25. Анализ принятых и посланных log-файлов.

S5.26. Извещение о пришедших факсах по телефону.

S5.27. Подтверждение о пришедших факсах по телефону.

S5.28. Подтверждение корректности пришедших факсов по телефону.

S5.29. Периодические проверки списков рассылки.

S5.30. Включение опции call-back.

S5.31. Конфигурирование модемов.

S5.32. Вопросы безопасности при использовании коммуникационного ПО.

S5.33. Безопасность при использовании удаленных модемов.

S5.34. Одноразовые пароли.

S5.35. Использование механизмов безопасности UUCP.

S5.36. Криптография под UNIX и Windows NT.

S5.37. Ограничение возможностей взаимодействующих объектов одного уровня при использовании ОС Windows 95 и Windows NT в сетях, поддерживающих серверы.

S5.38. Безопасность интеграции ПК под управлением ОС DOS в сети под управлением ОС UNIX.

S5.39. Безопасность использования протоколов и сервисов.

S5.40. Безопасность интеграции ПК под управлением ОС DOS в сети под управлением ОС Windows NT.

S5.41. Настройки, обеспечивающие безопасность удаленного доступа под управлением ОС Windows NT.

S5.42. Конфигурирование сетей TCP/IP под управлением ОС Windows NT.

S5.43. Конфигурирование сетевых сервисов TCP/IP под управлением ОС Windows NT.

S5.44. Однонаправленное соединение модема.

S5.45. Безопасность браузера.

S5.46. Инсталляция автономных систем при использовании Internet.

S5.47. Конфигурирование замкнутых групп пользователей.

S5.48. Аутентификация телефонных звонков с использованием определителя номера (CLIP/COLP).

S5.49. Обратный вызов по зафиксированному определителем номеру.

S5.50. Аутентификация в ISDN с использованием протоколов PAP/CHAP.

S5.51. Требования в области безопасности к телекоммуникациям через публичные сети.

S5.52. Требования в области безопасности к компьютерам, выполняющим телекоммуникационные функции.

S5.53. Защита от вредоносного ПО, передаваемого по почте.

S5.54. Защита от переполнения почтового ящика и спама.

S5.55. Проверка псевдонимов и списков рассылки.

S5.56. Безопасность почтового сервера.

S5.57. Безопасная конфигурация почтовых клиентов.

S5.58. Инсталляция драйверов ODBC (Open Database Connectivity).

S5.59. Защита от несанкционированных действий в отношении DNS.

S5.60. Выбор подходящей технологии базовых сетей (backbone).

S5.61. Выбор подходящей физической сегментации.

S5.62. Выбор подходящей логической сегментации.

S5.63. Использование криптографии с открытыми ключами (PGP).

S5.64. Безопасное окружение.

S5.65. Использование S-HTTP.

S5.66. Использование SSL.

S5.67. Использование службы контроля времени.

S5.68. Использование криптозащиты в сетях.

S5.69. Защита от активного контента.

S5.70. Использование Network address translation (NAT).

S5.71. Активный аудит.

S5.72. Удаление ненужных сетевых сервисов.

S5.73. Обеспечение безопасности при работе с факс-сервером.

S5.74. Поддержка адресной книги и списков рассылки факс-сервера.

S5.75. Защита от переполнения факс-сервера.

S5.76. Использование подходящих туннельных протоколов в сетях.

S5.77. Разбиение на подсети.

S5.78. Защита данных, передаваемых через мобильные телефоны, от использования в системе аутентификации.

S5.79. Защита от применения автоматически определенного номера мобильного телефона в системах аутентификации при использовании мобильных телефонов.

S5.80. Защита от утечки информации (подслушивания) с помощью мобильных телефонов.

S5.81. Безопасность при передаче данных через мобильные телефоны.

S5.82. Безопасность при использовании протокола SAMBA

S5.83. Безопасность при соединении с внешними сетями под Linux FreeS/WAN.

S5.84. Процедуры криптографической защиты при использовании Lotus Notes.

S5.85. Криптографическая защита e-mail Lotus Notes.

S5.86. Процедуры криптографической защиты при доступе через браузер к Lotus Notes.

S5.87. Соглашения, регулирующие связи с сетями третьих сторон.

S5.88. Соглашения, регулирующие вопросы передачи данных по сетям третьих сторон.

S6. Планирование непрерывности бизнеса

S6.1. Формулировка требований по доступности.

S6.2. Определение категорий опасности, персональная ответственность за обеспечение безопасности.

S6.3. Руководство по процедурам обеспечения безопасности.

S6.4. Требования к ресурсам, необходимым для работы приложений.

S6.5. Режим работы с минимальными ресурсами. Приоритеты информационных процессов.

S6.6. Исследование внешних и внутренних возможностей обеспечения бесперебойной работы.

S6.7. Ответственные за действия в чрезвычайных ситуациях.

S6.8. План действий в чрезвычайных ситуациях.

S6.9. План обеспечения бесперебойной работы в отдельных ситуациях.

S6.10. План обеспечения бесперебойной работы при выходе из строя связи.

S6.11. План восстановления нормальной работы.

S6.12. Тренировки по работе в чрезвычайных ситуациях.

S6.13. Резервное копирование и восстановление данных.

S6.14. План поставки оборудования.

S6.15. Соглашения с поставщиками.

S6.16. Страхование.

S6.17. Звуковая сигнализация на случай чрезвычайных обстоятельств.

S6.18. Обеспечение избыточности линий.

S6.19. Резервное копирование данных на ПК.

S6.20. Подходящие носители информации для резервного копирования.

S6.21. Резервное копирование программного обеспечения.

S6.22. Проверки качества резервных копий.

S6.23. Процедуры при обнаружении вирусов.

S6.24. Аспекты безопасности, связанные с FDD (дискеты).

S6.25. Регулярное резервное копирование жесткого диска сервера.

S6.26. Регулярное копирование данных конфигурации.

S6.27. Регулярное копирование CMOS RAM.

S6.28. Соглашение о сроках поставки отдельных элементов офисной АТС.

S6.29. Вызовы офисной АТС, связанные с авариями и безопасностью.

S6.30. Аварийные коммуникации.

S6.31. Примеры действий, приводящих к потере целостности данных.

S6.32. Регулярное резервное копирование данных.

S6.33. Политика резервного копирования.

S6.34. Определение факторов, препятствующих выполнению резервного копирования.

S6.35. Условия начала процедуры резервного копирования.

S6.36. Данные и ПО, подлежащие обязательному копированию.

S6.37. Документирование процедуры резервного копирования.

S6.38. Резервное копирование передаваемых данных.

S6.39. Процедуры, связанные с вводом в действие нового факса.

S6.40. Контроль и своевременная замена аккумуляторов.

S6.41. Обучение восстановлению данных.

S6.42. Создание start-up-дисков для Windows NT.

S6.43. Избыточность ресурсов в серверах Windows NT.

S6.44. Резервное копирование Windows NT.

S6.45. Резервное копирование Windows 95.

S6.46. Создание start-up-дисков для Windows 95.

S6.47. Хранение резервных копий как часть организации телекоммуникационных процедур.

S6.48. Процедуры в случае потери целостности базы данных.

S6.49. Резервное копирование баз данных.

S6.50. Активизация баз данных.

S6.51. Восстановление баз данных.

S6.52. Регулярное резервное копирование информации о конфигурационных данных.

S6.53. Дополнительные условия, связанные с установкой сетевых компонентов.

S6.54. Процедуры в случае нарушения целостности сети.

S6.55. Уменьшение времени нового запуска серверов под управлением ОС Novell Netware.

S6.56. Резервное копирование с криптографической защитой данных.

S6.57. Разработка планов бесперебойной работы на случай отказа системы управления.

S6.58. Система разбора и анализа инцидентов в области ИБ.

S6.59. Спецификация нарушений в области ИБ.

S6.60. Действия в случае обнаружения нарушений в области ИБ.

S6.61. Стратегия уклонения от инцидентов в области ИБ.

S6.62. Приоритеты при реагировании на инциденты в области ИБ.

S6.63. Расследование и оценка последствий инцидентов.

S6.64. Коррективы, вносимые после инцидентов.

S6.65. Оповещение об инцидентах.

S6.66. Оценка серьезности инцидентов.

S6.67. Фиксация инцидента и определение степени его серьезности.

S6.68. Проверка эффективности системы управления предотвращением инцидентов.

S6.69. Планирование бесперебойной работы для факс-серверов.

S6.70. Планирование бесперебойной работы для удаленных и мобильных элементов системы.

S6.71. Резервное копирование данных на мобильных ПК.

S6.72. Отказ мобильной связи.

S6.73. Планирование бесперебойной работы в случае сбоев Lotus Notes.

S6.74. Ведение архива аварий и инцидентов.

S6.75. Избыточность коммуникационных каналов.

Приложение 5
Классификация ресурсов, угроз и контрмер CRAMM

Классификация ресурсов, угроз и контрмер в методе CRAMM для профиля Commercial. Классификация физических ресурсов

Несетевые серверы:
– несетевые серверы общего назначения;
– прочие несетевые серверы.

Сетевые серверы:
– сетевые файл-серверы;
– сетевые серверы БД;
– сетевые серверы общего назначения;
– прочие сетевые серверы.

Несетевые рабочие станции:
– портативные, не имеющие постоянного расположения;
– стационарные рабочие станции с большим диапазоном возможностей (класса ПК);
– стационарные рабочие станции с ограниченными возможностями (класса X-терминала);
– прочие стационарные рабочие станции.

Сетевые рабочие станции:
– портативные, не имеющие постоянного расположения;
– стационарные рабочие станции с большим диапазоном возможностей (класса ПК);
– стационарные рабочие станции с ограниченными возможностями (класса X-терминала);
– прочие стационарные рабочие станции.

Локальные запоминающие устройства:
– накопители на жестких дисках;
– накопители на магнитной ленте;
– накопители на оптических дисках;
– прочие запоминающие устройства.

Сетевые запоминающие устройства:
– накопители на жестких дисках;
– накопители на магнитной ленте;
– накопители на оптических дисках:
– прочие сетевые запоминающие устройства.

Локальные печатающие устройства:
– принтер.

Сетевые печатающие устройства печати:
– сервер печати;
– сетевой принтер;
– принтер;
– другие сетевые устройства печати.

Сетевые распределительные компоненты:
- мост;
- коммутатор;
- маршрутизатор;
- повторитель;
- модем;
- мультиплексор;
- узел коммутации ATM;
- узел коммутации X.25;
- оконечный сетевой элемент;
- спутниковая станция связи;
- станция радиосвязи;
- прочие сетевые распределительные компоненты.

Сетевые шлюзы:
- шлюз трансляции сообщений;
- шлюз трансляции адресов;
- шлюз безопасности;
- управляющий шлюз;
- шлюз преобразования протоколов;
- прочие шлюзы.

Управление сетью и управляющие серверы:
- системы, обеспечивающие протоколирование сообщений и управление сообщениями;
- сетевые серверы аутентификации;
- сетевой центр управления;
- другие средства сетевого управления и управляющие серверы.

Сетевые интерфейсы:
- постоянное соединение:
  - синхронное;
  - асинхронное.
- коммутируемое соединение:
  - PSTN;
  - ISDN;
  - радиосоединение;
- прочие типы соединений.

Сетевые сервисы:
- объединение локальных сетей;
- канал с невысокой пропускной способностью;
- канал с пропускной способностью, соответствующий предъявляемым требованиям;
- маршрутизация сообщений;
- сетевое хранилище;

Сервисы общего назначения:
- Internet;

– другие сети общего назначения;
– телефония;
– прочие сетевые сервисы.

Сервисы конечного пользователя:
– электронная почта;
– прикладной обмен сообщениями;
– обмен электронными документами;
– передача файлов;
– сеансовая обработка;
– пакетная обработка;
– голос;
– видео;
– прочие сервисы конечного пользователя.

Коммуникационные протоколы:
– X.25;
– SDLS/HDLS;
– IP;
– CLNP (Connectionless Network Protocol);
– ATM;
– Frame Relay;
– TDM;
– протоколы спутникового обмена информацией;
– Ethernet;
– Token Ring;
– прочие протоколы.

Носители данных (Media):
– неэлектронные носители:
  – устройства ввода;
  – устройства вывода;
  – важные записи;
  – прочие виды носителей;
– электронные носители:
  – магнитные ленты;
  – диски;
  – прочие виды носителей.

Классы угроз

– использование чужого идентификатора сотрудниками организации (маскарад);
– использование чужого идентификатора поставщиком услуг (маскарад);
– использование чужого идентификатора посторонними (маскарад);
– несанкционированный доступ к приложению;

- внедрение вредоносного программного обеспечения;
- несанкционированное использование системных ресурсов;
- использование телекоммуникаций для несанкционированного доступа сотрудниками организации;
- использование телекоммуникаций для несанкционированного доступа поставщиком услуг;
- использование телекоммуникаций для несанкционированного доступа посторонними;
- ошибки при маршрутизации;
- неисправность сервера;
- неисправность сетевого сервера;
- неисправность запоминающих устройств;
- неисправность печатающих устройств;
- неисправность сетевых распределяющих компонент;
- неисправность сетевых шлюзов;
- неисправность средств сетевого управления или управляющих серверов;
- неисправность сетевых интерфейсов;
- неисправность сетевых сервисов;
- неисправность электропитания;
- неисправность кондиционеров;
- сбои системного и сетевого ПО;
- сбои прикладного ПО;
- ошибки пользователей;
- пожар;
- затопление;
- природные катаклизмы;
- нехватка персонала;
- кражи со стороны сотрудников;
- кражи со стороны посторонних;
- преднамеренные несанкционированные действия сотрудников;
- преднамеренные несанкционированные действия посторонних;
- терроризм.

Классы контрмер

- идентификация и аутентификация;
- логическое управление доступом;
- протоколирование;
- аудит;
- безопасность многократного использования объектов;
- тестирование систем;
- контроль целостности ПО;
- управление вводом/выводом;
- управление безопасностью в сети;

- обеспечение безотказности;
- обеспечение конфиденциальности вне соединения;
- управление доступом в сети;
- физическая безопасность сети;
- защита сообщений;
- обеспечение целостности данных вне соединения;
- сохранение правильной последовательности сообщений;
- пополнение трафика;
- контроль операций в системе;
- контроль действий системного администратора;
- контроль действий прикладных программистов;
- контроль операций по поддержке прикладного ПО;
- контроль операций по обслуживанию СВТ;
- контроль пользователей;
- контроль ввода/вывода приложений;
- финансовая отчетность;
- контроль выходных документов;
- контроль носителей данных;
- контроль транспортировки физических носителей данных;
- резервное копирование и восстановление ресурсов сервера;
- резервирование и восстановление сетевых интерфейсов;
- резервирование и восстановление сетевых сервисов;
- восстановление помещений;
- резервирование и восстановление носителей данных;
- планирование восстановления;
- резервное копирование данных;
- планирование потребностей в ресурсах;
- защита от сбоев СВТ;
- обеспечение физической безопасности помещений;
- оптимизация расположения СВТ в помещениях;
- организация зон безопасности;
- защита от краж;
- физическая защита СВТ;
- контрмеры против террористов и экстремистов;
- защита средств контроля доставки;
- обнаружение бомб и взрывчатых веществ;
- защита от минирования со стороны сотрудников и посторонних лиц;
- защита от пожара;
- защита от затоплений;
- защита от природных катаклизмов;
- защита источников электропитания;
- защита поддерживающей инфраструктуры;

- защита персонала;
- обучение персонала;
- политика безопасности;
- инфраструктура безопасности;
- оповещение об инцидентах;
- проверка жалоб.

Приложение 6
Оценка рисков экспертными методами

Оценка субъективной вероятности

Как правило, на практике субъективную вероятность приходится привлекать в следующих случаях:

- когда объективная вероятность некачественная;
- если предполагается, что полученные закономерности и объективная вероятность не будут наблюдаться в будущем;
- когда нет объективных данных о наблюдениях в прошлом.

В таких ситуациях субъективную вероятность можно рассматривать как меру уверенности эксперта в возможности наступления события. Она может быть представлена по-разному: *вероятностным распределением на множестве событий, бинарным отношением на множестве событий, не полностью заданным вероятностным распределением* или *бинарным отношением* и другими способами.

Покажем, как определить субъективную вероятность. Разделим процесс на три этапа:

- подготовительный этап;
- получение оценок;
- анализ оценок.

Первый этап позволяет выделить объект исследования - некоторое множество событий. Далее 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 определения субъективной вероятности. На этом же этапе проводится подготовка эксперта или группы экспертов, ознакомление его 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. Здесь далеко не всегда удается установить окончательное распределение, поскольку результаты могут быть противоречивыми.

Третий этап заключается в исследовании и обобщении результатов опроса. Если вероятности, представленные экспертами, не согласуются с аксиомами вероятности, то это доводится до сведения экспертов и ответ уточняются так, чтобы они соответствовали аксиомам. Для некоторых методов определения субъективной вероятности третий этап исключается, поскольку сам метод состоит в выборе распределения, подчиняющегося аксиомам вероятности, которое в том или другом смысле наиболее близко к оценкам экспертов. Примеры таких методов - *метод главного значения для конечного множества независимых событий и минимаксный метод для зависимых событий.* Особую важность третий этап приобретает при *агрегировании оценок,* полученных от группы экспертов. Например, в *методе Делфи,* после анализа вероятностей, представленных отдельными экспертами, предполагается повторение второго этапа, то есть повторный опрос. Далее вновь следует третий этап, и в случае необходимости процедура выполняется еще раз.

Классификация методов получения субъективной вероятности

Методы определения субъективной вероятности можно классифицировать в зависимости от формы поставленных перед экспертами вопросов или от характеристик событий и случайных величин, а также от числа привлекаемых экспертов. В задачах оценки рисков в условиях неопределенности требуется оценивать вероятность (возможность) состояний внешней среды (неопределенных факторов). Поскольку внешняя среда может принимать лишь одно значение из заданного множества, то при оценке субъективных вероятностей обычно применяют методы, предназначенные для множеств несовместных событий. Среди методов, служащих для оценки вероятностей в случае конечных множеств несовместных событий, наибольшее практическое значение имеют три: *метод прямого приписывания вероятностей, метод отношений и метод собственного значения,* а в случае бесконечных множеств несовместных событий - *метод изменяющегося интервала и метод фиксированного интервала.*

Для практической реализации указанных методов необходима их детальная доработка и адаптация к характеру решаемых задач. Также понадобится разработать и реализовать конкретные алгоритмы проведения опроса экспертов по этим методам. В качестве дополнения к таким алгоритмам нужны процедуры графического представления данных, подготовленных экспертом. Это позволит эксперту вносить необходимые корректировки в свои прежние оценки исходя из общей картины. А для обработки вероятностей, представленных несколькими экспертами, следует создавать процедуры агрегирования вероятностей. В их основу может быть положен *метод взвешенной суммы.* Для лучшей согласованности оценок экспертов обычно разрабатывают итеративную процедуру проведения экспертизы, основанную на методе Делфи.

Условно методы нахождения субъективной вероятности можно разделить на следующие три группы.

Первая, самая многочисленная группа, - это прямые методы, состоящие в том, что эксперт отвечает на вопрос о вероятности события. К ним относятся *метод изменяющихся интервалов, метод фиксированных интервалов, метод отношений, графический метод, метод собственного значения, методы оценки параметров распределения* и др. Независимо от конкретного метода данной группы эксперт должен оценивать непосредственно вероятность событий.

Вторую группу образуют методы, в которых вероятность событий выводится из решений экспертов в гипотетической ситуации. Примером является *метод лотерей,* а также *метод равноценной корзины.* Формально говоря, применение методов второй группы требует от эксперта сравнения не вероятностей как таковых, а полезности альтернатив, при которых исход зависит от реализации случайной величины. Многие эксперты отмечают возрастающую сложность вопросов и более существенные ошибки при применении этих методов по сравнению с методами первой группы.

Третья группа - это гибридные методы, требующие от экспертов ответов на вопросы как о вероятности, так и о полезности. К гибридным методам относятся некоторые разновидности *метода лотерей.*

Методы получения субъективной вероятности

Постановка задачи заключается в том, что путем опроса экспертов следует построить вероятностное распределение на конечном множестве несовместимых (взаимоисключающих) событий.

Прямая оценка вероятностей событий

В этом методе эксперту или группе экспертов предъявляется список всех событий. Эксперт должен указать последовательно вероятность всех событий. Возможны различные модификации метода. В одной из модификаций предлагается сначала выбрать наиболее вероятное событие из предложенного списка, а затем оценить его вероятность. После этого событие из списка удаляется,

а к оставшемуся списку применяется уже описанная процедура. Сумма всех полученных вероятностей должна равняться единице.

Метод отношений

Эксперту сначала предлагается выбрать наиболее вероятное событие. Этому событию приписывается неизвестная вероятность *P1*. Затем эксперт должен оценить отношения вероятностей всех остальных событий к вероятности *P1* выделенного события (коэффициенты *C2,..., CN).* С учетом того, что сумма вероятностей равна 1, составляется уравнение:

*P*l(l + *C2*+ *C3* + ... +*CN*) = 1.

Решив это уравнение и найдя величину *P1*, можно вычислить искомые вероятности.

Метод собственного значения

Метод основан на том, что неизвестный вектор вероятностей *(P1,..., Pn)* является собственным вектором некоторой специально построенной матрицы, отвечающим ее наибольшему собственному значению. Сначала эксперту задается вопрос, какое из двух событий более вероятно. Предположим, что более вероятно событие *S1*. Затем эксперта спрашивают, во сколько раз событие *S1* вероятнее, чем *S2*. Полученное от эксперта отношение записывается на соответствующее место в матрице.

Метод равноценной корзины

Этот метод позволяет получить вероятность исходя из экспертного сравнения полезности альтернатив. Предположим, надо вычислить вероятность некоторого события *S1*. Определим какие-либо два выигрыша, в частности денежных, которые существенно различны, например: первый выигрыш - 1 млн. руб., а второй -0 руб., и предложим эксперту на выбор участие в одной из двух лотерей. Первая лотерея состоит в том, что выигрыш в 1 млн. руб. эксперт получает, если состоится событие *S1*, а выигрыш в 0 руб. - если событие не происходит. Для организации второй лотереи представим себе гипотетическую корзину, заполненную белыми и черными шарами, первоначально в равном количестве, скажем, по 50 шаров каждого цвета. Если вынутый шар белый, то участнику достается 1 млн. руб., если черный - 0 руб. Эксперта просят отдать предпочтение одной из двух лотерей. Если с точки зрения эксперта лотереи равноценны, делается вывод о том, что вероятность события *S1* равна 0,5. Если эксперт выбирает первую лотерею, то из корзины вынимается часть черных шаров и заменяется тем же количеством белых. Если предпочтение отдается второй лотерее, то часть белых шаров заменяется черными. В обоих случаях эксперту вновь предлагается поучаствовать в одной из двух лотерей. Изменяя соотношение шаров в гипотетической корзине, добиваются равноценности двух лотерей. Тогда искомая вероятность события *S1* равна доле белых шаров в общем их количестве.

Методы оценок непрерывных распределений

Данные методы можно использовать, например, чтобы найти функцию распределения (или плотность распределения) субъективных вероятностей некоторой непрерывной случайной величины. Чаще всего для решения такой задачи применяются два метода, основанных на опросе экспертов: *метод изменяющегося интервала* и *метод фиксированного интервала.*

Метод изменяющегося интервала

Существует несколько модификаций этого метода. Но для них общим является требование к эксперту указать на множестве значений случайной величины такой интервал, чтобы вероятность того, что случайная величина принимает значение в указанном интервале, была равна заданной величине. Например, опрос эксперта может строиться по следующей схеме. Сначала эксперта просят указать такое значение *S1* случайной величины, при котором оказываются равными две вероятности: того, что случайная величина примет значение меньше *S1,* и того, что

она примет значение больше *S1*. Получив от эксперта значение *S1*, переходят ко второму этапу. На этом этапе у эксперта спрашивают, при каком значении *S2* случайной величины область значений больше *S1* поделится на две равновероятные части. Точно так же поступают с областью значений меньше *S1* и находят значение *S3*. Вслед за вторым этапом проводится третий этап, состоящий в нахождении медиан каждого из образовавшихся участков. Этот процесс не следует продолжать слишком долго, поскольку при малых величинах интервалов возрастает вероятность ошибки эксперта. При использовании данного метода обычно бывает полезно вернуться к предыдущим оценкам и проанализировать их непротиворечивость. В случае обнаружения противоречий эксперт должен изменить одну из своих прежних оценок.

В некоторых вариантах метода изменяющегося интервала перед экспертом может быть поставлена задача указать две точки на предложенном множестве значений случайной величины, которые разбивают это множество на три равновероятные части. В других вариантах эксперта могут, например, спросить, при каком значении случайной величины *S1* вероятность того, что случайная величина примет меньшее значение, чем *S1,* равна 0,1. Оценки, полученные таким способом, меньше зависят друг от друга, то есть не происходит накопления ошибки. В этом и заключается их преимущество. Существуют модификации метода, основанные на предположении, что для эксперта проще указать точку, делящую область на две равновероятные части, чем точку, отделяющую область, соответствующую вероятности 0,1, от остального множества. Таким образом, в случае применения метода изменяющегося интервала приходится выбирать между простотой сравнения и независимостью получаемых оценок.

Метод фиксированного интервала

В соответствии с этим методом множество значений случайной величины разбивается на интервалы и эксперта просят оценить вероятность того, что случайная величина примет значение из данного интервала. Обычно интервалы, за исключением крайних слева и справа, выбираются равной длины. Число интервалов определяется с учетом необходимой точности и требуемого вида распределения. После того как эксперт сообщил вероятность всех интервалов, обычно проводят проверку полученного распределения. Например, если двум различным интервалам приписана одинаковая вероятность, можно спросить у эксперта, действительно ли они равновероятны. Относительно других интервалов можно уточнить, действительно ли один из них во столько-то раз более вероятен, чем другой, как это следует из приписанных этим интервалам вероятностей. В результате такого просмотра эксперт может несколько подправить вероятности. Иногда метод фиксированного интервала применяется совместно с методом изменяющегося интервала. Так, можно сначала предложить эксперту определить медиану, то есть такое значение случайной величины, которое разбивает все множество значений на два равновероятных множества, а затем от найденной медианы отложить в обе стороны равные фиксированные интервалы.

Графический метод

Метод дает надежные результаты в том случае, когда эксперт хорошо подготовлен к восприятию графической информации о вероятности. Состоит он в том, что эксперт должен изобразить в графической форме (в виде графика функции распределения или плотности вероятности, в форме диаграммы или графа) свое представление о вероятности событий или о случайной величине. Зачастую общий вид графика известен, а от эксперта требуется лишь подобрать параметры распределения. Графический метод особенно полезен в качестве вспомогательного при анализе вероятностей, найденных каким-либо другим способом. Например, функция распределения может быть определена методом фиксированного интервала, а затем ее график, а также график функции плотности распределения представляют эксперту для окончательной доработки.

Некоторые рекомендации

Известно, что субъективная вероятность, получаемая экспертным путем, существенно зависит от используемого метода. В частности, эксперт нередко склонен преувеличивать вероятность наименее вероятного события, а также недооценивать вероятность наиболее вероятного или преувеличивать дисперсию оцениваемой случайной величины. Рассмотрим несколько рекомендаций, выполнение которых позволит корректно проводить опрос эксперта с помощью различных методов:

- необходимо обучить эксперта процедуре проведения экспертизы. Особенно это касается экспертов, имеющих слабую подготовку по теории вероятностей;
- надо отдавать себе отчет в том, что сама процедура опроса эксперта является лишь одним звеном во всем процессе определения вероятностей. Предшествующие шаги по вычленению событий и выбору подходящего метода столь же важны. Нельзя пренебрегать также и последующим анализом полученных вероятностей с целью возможной их корректировки;
- старайтесь применять объективную информацию о вероятностях событий, например данные о том, как такие события происходили в прошлом. Эта информация должна быть доведена до эксперта. Не забывайте также обрабатывать алгебраическим путем предыдущие оценки эксперта, чтобы сопоставить их с его новыми оценками;
- для проверки надежности представленных данных рекомендуется обращаться к каким-либо другим методам нахождения субъективной вероятности или даже к модификации методов. Определенные различными методами вероятности необходимо показать эксперту для уточнения его оценок;
- при выборе конкретного метода нужно учитывать опыт работы эксперта с числовыми показателями. И если такой опыт недостаточен, то метод фиксированного интервала непригоден, так как предполагает числовые оценки. Более подходящим в этом случае будет метод изменяющегося интервала, поскольку в его рамках от эксперта требуется лишь утверждение о равновероятности двух интервалов. В любом случае употребление знакомых эксперту понятий, фраз, вопросов и шкал облегчает возможности численного представления вероятности;
- всегда, когда это возможно, старайтесь получать субъективную вероятность от нескольких экспертов, а затем некоторым образом агрегировать ее в одну;
- сложные методы, требующие больших усилий от эксперта, например метод лотерей, лучше не применять, за исключением случаев, когда имеются серьезные аргументы в пользу выбора этих методов.

Выполнение этих рекомендаций позволяет существенно улучшить оценки вероятности.

Агрегирование субъективных вероятностей

Проблема агрегирования возникает в том случае, когда *m* экспертов оценивают вероятности на одном множестве событий. Существуют различные подходы к решению этой задачи:

- индивидуальные оценки рассматриваются как случайные величины на одном и том же вероятностном пространстве. Групповая вероятность представляет собой условную вероятность события *S1* в предположении, что индивидуальные оценки равны *P1,..., Pm;*
- в методе *взвешенной суммы* групповая вероятность находится по формуле: $P = W1 \times P1 + ... + Wm \times Pm$,

  где *Wi* - это веса (коэффициенты компетентности), приписанные эксперту *i*. Если оценки *Pi* являются несмещенными, то веса можно принимать так, чтобы

минимизировать дисперсию величины *P*. На практике веса следует выбирать на основе анализа оценок экспертов, полученных во время предыдущих экспертиз;

– в подходе, основанном на методе Делфи, субъективные вероятности, представленные экспертами, доводятся до сведения всех экспертов, после чего эксперты вновь сообщают свои вероятности. Таким образом выполняется итеративная процедура, которая позволяет каждому отдельному эксперту скорректировать свои оценки после ознакомления с оценками остальных.

Методы теории полезности

При решении задач выбора в условиях неопределенности и, в частности, задачи оценки рисков наиболее обоснован подход, базирующийся на теории полезности. В настоящее время теория полезности достигла весьма высокого уровня развития. Вопросы практического применения данной теории хорошо освещены в литературе: введены понятия и исследованы свойства, позволяющие разбить процесс построения функции (одномерной) полезности на этапы и сделать его максимально эффективным; разработаны методы построения, опирающиеся на эти понятия и свойства. Теоретические результаты и методы практического построения функции одномерной полезности достаточно апробированы при решении различных задач принятия решений, и их целесообразно применять в разных методиках оценивания рисков.

Постановка задачи выбора в условиях риска

Рассмотрим следующую постановку задачи.

Задано множество 5 возможных детерминированных исходов (последствий). В роли этого множества чаще всего выступает множество значений скалярного или векторного критерия, при помощи которого оценивается эффективность (качество и т.п.) вариантов решений (стратегий, планов, альтернатив и т.д.). Достигаемый исход зависит не только от реализуемого варианта решения, но и от того, какое значение примут неопределенные (случайные) факторы, распределения вероятностей которых известны. Поэтому удобно полагать, что каждому варианту решения из допустимого множества ставится в соответствие некоторая вероятностная мера, заданная на множестве 5 (например, распределение вероятностей или плотность вероятности). Принимающий решение должен выбрать наилучший вариант из множества 5 или, что эквивалентно, сделать выбор на множестве соответствующих элементам этого подмножества вероятностных мер.

Известны два основных подхода к принятию решений при риске:

– базирующийся на применении так называемых объективных критериев выбора (привлечение различных моделей стохастического программирования, применение критериев типа математического ожидания, дисперсии и т.д.);

– основанный на получении и использовании информации субъективного характера - сведений о структуре предпочтений (лицо, принимающее решение (ЛПР)), в том числе о его отношении к риску.

Как показывают многочисленные исследования, методы, реализующие первый подход, менее надежны, поскольку зачастую неадекватно описывают ситуацию. Например, два действия, характеризуемые одинаковым математическим ожиданием выигрыша, для ЛПР могут не быть равноценными. Поэтому далее будем рассматривать субъективный подход к принятию решений при риске. Среди методов этого подхода наиболее распространены и обоснованы те, которые опираются на аксиоматические построения: предпочтения формализуются с помощью некоторой модели, и формулируются условия, обеспечивающие ее существование. Важным направлением в развитии таких методов служит теория полезности, основанная на представлении структуры предпочтений ЛПР посредством одной или нескольких вещественных функций.

Необходимые сведения из теории полезности

Впервые условия, необходимые и достаточные для представления предпочтений ЛПР на множестве вероятностных мер с помощью линейной вещественно значимой функции, так называемой функции полезности, были получены Нейманом и Моргенштерном в 1947 году. В настоящее время принято разделять эти условия на две группы.

Условия из первой группы касаются множества всех рассматриваемых вероятностных мер и в современной литературе просто включаются в определение этого множества, называемого множеством вероятностных смесей. *Вторая группа условий* касается описания отношения предпочтения на множестве смесей - именно она известна сейчас как система аксиом Неймана-Моргенштерна, или аксиом классического представления полезности. Оценивается лотерея L:

$p(A) + (1 - p)(B)$,

где A - выигрыш с вероятностью p, B - выигрыш с вероятностью $(1- p)$.

Чтобы определить величину полезности, отражающую отношение индивида к какому-либо выигрышу X, мы его спрашиваем или наблюдаем за его поведением; в этом случае мы устанавливаем, при какой вероятности p' ему безразлично, что выбрать - стандартный лотерейный билет $L(p')$ или X. Оценка полезности U сводится к определению полезности $U(L(p'))$ на основе выражения, сформулированного Нейманом и Моргенштерном. Кроме того, Нейман и Моргенштерн постулировали пять аксиом, достаточных, чтобы гарантировать существование такой функции полезности, при которой ранжирование лотерей по их ожидаемой полезности полностью соответствует действительным предпочтениям индивида.

Применение методов теории полезности

Требование линейности функции полезности в классическом представлении (обеспечиваемое также почти во всех представлениях, разработанных позднее) связано с его применением для решения практических задач. Дело в том, что при выполнении ряда дополнительных предположений условие линейности дает возможность выразить функцию полезности на множестве вероятностных смесей в виде математического ожидания ее значений на множестве детерминированных исходов. Это имеет большое практическое значение, поскольку позволяет свести задачу построения функции полезности на множестве смесей к задаче ее построения на множестве исходов. В ряде работ используются понятия детерминированного и вероятностного эквивалентов, на которые опирается большинство известных методов практического построения функции полезности.

Классификация функций полезности по склонности к риску

Как правило, методы практического построения функции полезности опираются на сравнение простых лотерей. Рассматриваются также вырожденные лотереи, отождествляемые с детерминированными исходами. В связи с этим все методы делятся на два класса: методы, основанные на сопоставлении простой лотереи и детерминированного исхода, и методы, базирующиеся на сопоставлении двух невырожденных простых лотерей. Каждый из этих классов, в свою очередь, распадается на несколько групп. Например, методы простой лотереи предполагают сопоставление лотереи L:$p(A) + (1 - p)(B)$ с детерминированным исходом S. *Методы сравнения по предпочтению* базируются на определении риска для простой лотереи L и детерминированного исхода S. Существуют два подхода к реализации подобных методов. Один из них включает предварительное исследование отношения к риску и проверке согласованности получаемых значений функции полезности. При этом каждое сравнение по предпочтению задает линейное ограничение на функцию полезности. Таким образом, могут быть получены сколь

угодно узкие границы, в которых находится искомая допустимая функция полезности. Второй подход основан на схождении к точке безразличия.

Остальные методы данного класса базируются на определении различного рода эквивалентов. Определение эквивалента заключается в нахождении точки безразличия между лотереей и детерминированным исходом. Существует несколько подходов к оцениванию точки безразличия:

- прямая оценка - ЛПР указывает точное значение точки безразличия;
- схождение - последовательная корректировка до получения точки безразличия;
- метод границ - установление нижних и верхних границ для точки безразличия.

Многомерные функции полезности

В большинстве задач принятия решений, в том числе в задачах анализа рисков, исходы оцениваются не одним, а многими критериями. В условиях вероятностной неопределенности сравнение вариантов многокритериальных решений сводится к сопоставлению по предпочтительности соответствующих распределений вероятностей на множестве векторных оценок (значений векторного критерия). Разумеется, и на такие задачи полностью распространяются основные положения теории полезности, касающиеся, в частности, существования функции полезности. Однако при этом функция полезности оказывается многомерной, то есть имеющей векторный аргумент.

С формальной точки зрения к многокритериальным задачам тоже приложимы методы построения (одномерной) функции полезности, описанные выше (если рассматривать векторную оценку как нечто неделимое). Однако непосредственное использование таких методов обычно невозможно в силу того, что лицо, принимающее решение, не в состоянии сравнивать лотереи с многомерными (многокритериальными) исходами. Основным путем построения многомерной функции полезности является декомпозиция многомерной структуры предпочтений на ряд подструктур меньшей размерности (в частности, одномерных) и, соответственно, представление многомерной функции полезности в виде составной (сложной) функции - «свертки» малоразмерных функций полезности. Структура такой сложной функции зависит от взаимосвязей подструктур структуры предпочтений. При такого рода декомпозиции построение многомерной функции полезности сводится к построению соответствующих маломерных (проще всего, конечно, одномерных) условных функций полезности, а также оцениванию ряда числовых параметров, определяемых конструкцией составной функции свертки.

Декомпозиция многомерной структуры предпочтений ЛПР на множестве вероятностных распределений случайной векторной оценки осуществляется за счет использования специфических особенностей этой структуры. Обычно эти особенности связаны с какими-либо видами независимости одних (групп) критериев от других. Поскольку условия независимости не всегда выполняются в полном объеме, указанный подход стали обобщать за счет «расщепления» шкал (точнее, носителей шкал) критериев и соответствующего разложения структуры предпочтений на подструктуры, для каждой из которых справедливы определенные виды независимости. С другой стороны, в последнее время развивается несколько иной подход к построению многомерной функции полезности, связанный с изучением одних (групп) критериев от других и соответствующих им форм составных функций свертки. Однако этот подход еще не доведен до требуемого практикой уровня развития. Существуют и принципиально иные подходы к моделированию многомерных полезностей. Они включают целенаправленную перестройку самой исходной математической модели ситуации на основе содержательного анализа конкретной проблемы принятия решений. Примером служит подход, предполагающий расщепление исходных критериев, - представление их через некоторые дополнительно вводимые, так чтобы преобразованная структура предпочтений обладала некими свойствами независимости.

Рассмотрим основные результаты декомпозиции структуры предпочтений и методы получения информации о предпочтениях, необходимой для построения соответствующих многомерных функций полезности.

Методы построения многомерных функций полезности

Функция полезности выражает предпочтения ЛПР на множестве случайных исходов и поэтому должна строиться на основе информации о таких предпочтениях. При этом конкретный вид информации определяется допущениями, выдвигаемыми относительно особенностей структуры предпочтений (то есть конкретными видами независимости для различных факторов), и соответствующим функциональным представлением полезности.

Порядок построения многомерной функции полезности

Рекомендуется структурировать систему предпочтений при помощи функции многомерной полезности, придерживаясь последовательно пяти перечисленных ниже стадий:

1) Введение терминологии и основных допущений.
2) Проверка необходимых условий допущений о независимости.
3) Построение условных функций полезности.
4) Нахождение значений констант, задающих масштаб шкалы.
5) Проверка согласованности.

На первой стадии ЛПР знакомится с программным обеспечением, реализующим аналитическую модель, критериями и их шкалами, а также необходимыми понятиями из теории полезности (лотерея, вероятность, функция полезности, ожидаемая полезность и т.п.), причем объяснения должны быть предельно простыми, сформулированными на понятном ЛПР языке и в то же время достаточно четкими и строгими.

Проверка допущений о независимости

Допущение о независимости фактора (критерия) K_i от K_j по полезности проверяется, например, оценкой детерминированных эквивалентов для ряда лотерей, значения которых покрывают достаточно плотно пространство исходов. Если предпочтения оказываются почти одинаковыми для разных фиксированных Kj (о справедливости вывода относительно постоянства можно поинтересоваться у лица, принимающего решение), то проверяемое допущение о независимости можно принять. Прямая проверка взаимонезависимости полезности K_i от K_j затруднена тем, что фактически она включает n факторов разной размерности от их дополнений, и проверить справедливость их всех практически нельзя уже при $n = 5$. Однако эта проблема резко упрощается при уменьшении размерности независимых переменных.

Вычисление значений констант шкал

Общий подход к решению данной задачи состоит в составлении системы необходимого числа уравнений, содержащих эти константы в качестве неизвестных, путем рассмотрения лотерейных детерминированных эквивалентов, а также неслучайных исходов.

Проверка согласованности

Возможны три подхода к решению рассматриваемой проблемы. Первый основан на проведении попарных сравнений различных последствий. Такого рода проверка повторяется несколько раз, чтобы появилась уверенность в ее результатах. При этом рекомендуется начинать с простых сравнений и постепенно переходить к более сложным. Второй подход заключается в предъявлении лицу, принимающему решение, кривых условно равного предпочтения. Третий связан с выяснением склонности лица, принимающего решение, к риску.

Если в процессе анализа согласованности выявляются противоречия, необходимо повторить соответствующие стадии процедуры построения функции полезности до получения некоторой

функции полезности выбранного вида или же перейти к построению функции полезности более общего вида.

Выводы и рекомендации

Основным подходом к построению функций многомерной (многокритериальной) полезности является декомпозиционный - исходная задача большой размерности сводится к ряду задач меньшей размерности, то есть устанавливаются условные (одномерные) функции полезности и шкалирующие константы в функции многомерной полезности, вид которой зависит от принимаемых допущений о независимости определенных факторов (критериев) от всех остальных.

Сложный (с большим числом подлежащих отысканию параметров - условных функций полезности и шкалирующих коэффициентов) вид функции многомерной полезности обеспечивает достаточную свободу и гибкость для аппроксимации структуры предпочтений, однако делает весьма трудоемкой процедуру построения такой функции. Примером служит полилинейная функция полезности. Простой (содержащий небольшое число параметров) вид функции полезности сильно упрощает процедуру ее построения, но он основан на весьма жестких предположениях о независимости, которые редко выполняются на практике, и поэтому такие функции обычно плохо аппроксимируют структуры предпочтений. Пример - аддитивная функция полезности.

Наиболее перспективными являются виды функции полезности, предоставляющие возможность поддерживать разумный компромисс между противоречивыми требованиями к достаточной гибкости функции и к простоте ее построения. Например, к таким функциям относится мультипликативная функция полезности. В литературе описаны многочисленные примеры успешного ее привлечения для решения разнообразных практических многокритериальных задач.

Пример метода оценки рисков

Рассмотрим метод последовательных уступок, который позволяет получить сравнительную оценку возможных последствий реализации угроз с помощью системы критериев.

Прежде всего посредством моделирования или методов экспертных оценок проводится качественный анализ относительной важности показателей эффективности (критериев). Показатели располагаются и нумеруются в порядке убывания важности так, что главным оказывается показатель ω_1, менее существенным - ω_2. затем следуют остальные показатели: ω_3, ω_4, ..., ω_n. Максимизируется первый по важности показатель ω_1 и находится его наибольшее значение W_1. Затем определяется (назначается) величина допустимого снижения (уступки) показателя ω_1 ($\Delta\omega_1 \geq 0$) и наибольшее значение второго показателя ω_2 - W_2 при условии, что значение первого показателя должно быть не меньше ($W_1 - \Delta\omega_1$). Снова определяется (назначается) величина уступки (но уже по второму показателю -($\Delta\omega_2 \geq 0$)), которая служит для нахождения условного максимума W_3 третьего показателя ω_3, и т.д. Наконец, максимизируется последний по важности показатель ω_n при условии, что значения (n - 1) предыдущих должны быть не менее соответствующих величин ($W_i - \Delta\omega_1$). Полученная в результате совокупность показателей эффективности соответствует оптимальной системе или варианту ее построения. Тогда математическое решение задачи описывается совокупностью последовательных шагов:

$$\left.\begin{array}{l} 1.\ W_1 = \sup\omega_1(x); \\ 2.\ W_2 = \sup\omega_2(x), \text{ где } \omega_1(x) \geq W_1 - \Delta\omega_1; \\ \ldots \\ n.\ W_n = \sup\omega_n(x), \text{ где } \omega_{n-1}(x) \geq W_{n-1} - \Delta\omega_{n-1} \end{array}\right\}, \qquad (1)$$

где $x \in X$; X - множество значений технических характеристик, X - значения технических характеристик, обеспечивающих соответствующие значения показателей эффективности.

В результате (n - 1) шагов определяется как совокупность характеристик технических средств, поддерживающих рациональные значения показателей эффективности функционирования системы.

Одна из основных трудностей практического применения *метода последовательных уступок* состоит в необходимости задания величин уступок по всем (кроме последнего по важности) показателям эффективности. Однако если в составе исходной информации отсутствует задание уступки по какому-либо показателю, то ее можно установить на основе анализа взаимосвязей пар смежных по важности показателей эффективности. Вначале решается вопрос о назначении уступки по первому показателю. Для этого находится максимальное значение этого показателя W_1, которое соответствует, например, k-й системе. Предварительно показатели должны быть нормализованы по формулам (6), (7). Затем задается несколько значений уступок по первому показателю, которым будут соответствовать определенные значения второго по важности показателя эффективности $\omega_2'(x)$.

На основе анализа результатов расчетов устанавливается $\Delta\omega_1'(x)$ - рабочий диапазон значений $\omega_1'(x)$, в котором расположены наиболее приемлемые значения $\omega_2'(x)$, или конкретное значение уступки исходя из условия, что минимальному уменьшению показателя $\omega_1'(x)$ относительно его максимального значения W_1 будет отвечать наибольший прирост значения второго показателя $\Delta\omega_2'(x)$. Соответствующая этому условию ; j-я система определяется по формуле:

$$\alpha(j) = \inf\left[\operatorname{arcctg}\frac{\omega'_{j2} - \omega'_{k2}}{\omega'_{k1} - \omega'_{j1}}\right], \qquad (2)$$

где первый индекс характеризует номер системы, а второй - номер показателя эффективности.

Тогда величина уступки по первому показателю рассчитывается так:

$$\Delta\omega'_1 = \omega'_{k1} - \omega'_{j1}. \qquad (3)$$

Далее аналогичным образом анализируется следующая пара смежных показателей $(\omega_2' \mid \omega_3')$ и вычисляется уступка $\Delta\omega_2'$. И так до предпоследнего показателя. Тогда формулы (2) и (3) в общем виде будут выглядеть следующим образом:

$$\alpha(j) = \inf\left[\operatorname{arcctg}\frac{\omega'_{j,i+1} - \omega'_{k,i+1}}{\omega'_{ki} - \omega'_{ji}}\right], \qquad (4)$$

$$\Delta\omega'_i = \omega'_{ki} - \omega'_{ji}. \qquad (5)$$

Описание логики работы и способа формирования результатов решения

В соответствии с математическим описанием метода последовательных уступок возможный алгоритм включает некоторую последовательность шагов. Вначале производится ввод исходных данных (см. табл. П6.1) в виде матрицы.

Таблица П6.1. Исходные данные для метода последовательных уступок

	ω_1	ω_2	...	ω_i	...	ω_{n-1}	ω_n
Система 1	ω_{11}	ω_{12}	...	ω_{1i}	...	ω_{1n-1}	ω_{1n}
Система 2	ω_{21}	ω_{22}	...	ω_{2i}	...	ω_{2n-1}	ω_{2n}
.....	...	...	...	...	...	...	...
Система j	ω_{j1}	ω_{j2}	...	ω_{ji}	...	ω_{jn-1}	ω_{jn}
.....	...	...	...	...	...	...	...
Система l	ω_{l1}	ω_{l2}	...	ω_{li}	...	ω_{ln-1}	ω_{ln}
Индекс предпочтения p_i	p_1	p_2	...	p_i	...	p_{n-1}	p_n
Значения уступок $\Delta\omega_i$	$\Delta\omega_1$	$\Delta\omega_2$	...	$\Delta\omega_i$	...	$\Delta\omega_{n-1}$	$\Delta\omega_n$

В таблице приняты следующие обозначения:

- N - количество оцениваемых показателей эффективности;
- L - количество сравниваемых систем;
- ω_{ji} $(i=1,n; j=1,l)$ - значения показателей эффективности для всех сравниваемых систем;
- $k_i (i=\overline{1,n})$ - индексы предпочтения ($k_i = 0$, если предпочтение отдается максимальному значению i-го показателя, и $k_i = 1$, если предпочтение отдается минимальному значению i-го показателя);
- $\Delta\omega_i (i=\overline{1,n})$ - заданное значение уступки для i-го показателя (если $\Delta\omega_i = 0$, то нормированную уступку для i-го показателя необходимо вычислить в соответствии с формулами (4) и (5)). При этом нельзя составить программу для вычисления уступки по последнему показателю.

После ввода исходных данных элементы матрицы ω_{ji} и $\Delta\omega_1$, нормализуются по следующим правилам:

- для показателей, которые максимизируются:

$$\omega'_{ji} = \frac{\omega_{ji} - \omega_{i\min}}{\omega_{i\max} - \omega_{i\min}}; \qquad (6)$$

- для показателей, которые минимизируются:

$$\omega'_{ji} = \frac{\omega_{i\max} - \omega_{ji}}{\omega_{i\max} - \omega_{i\min}}. \qquad (7)$$

Здесь $\omega_{i\max}, \omega_{i\min}$ - соответственно максимальное и минимальное значения i-го показателя, достигаемые в одной из исследуемых систем.

В результате нормализации значения ω_{ji} лежат в пределах $0 \le \omega_{ji} \le 1$. При этом для всех показателей предпочтительными становятся их наибольшие значения. Нормализованные значения величин уступок вычисляются по формуле:

$$\Delta\omega'_i = \frac{\Delta\omega_i}{\omega_{i\max} - \omega_{i\min}}. \qquad (8)$$

Здесь нормализованная уступка рассчитывается по формулам (4), (5). При этом все показатели должны быть приведены в нормализованный вид (формулы (6), (7)). Затем выбирается режим работы алгоритма. Возможны три варианта:

- с полной расстановкой показателей по важности;

– с неполной расстановкой показателей по важности;
– без расстановки показателей по важности.

Анализ систем начинается с самого важного показателя. При этом последовательно устанавливается оптимальная система по *i*-му показателю. Оптимальная *k*-я система, характеризующаяся максимальным значением очередного по важности *i*-го показателя эффективности, находится из выражения:

$$W_{ki}=sup\omega_{ki}(x) \mid \omega_{ki-1}(x) \geqslant W_{ki-1} - \Delta\omega_{i-1}. \quad (9)$$

Следующий шаг - определение множества эффективных систем путем последовательного исключения неэффективных из общего числа исследуемых. Исключаются из рассмотрения все системы, имеющие меньшее значение *i*-го показателя по сравнению с данной (*k*-й системой) на величину уступки $\Delta\omega_i'$, то есть лежащие в пространстве этих показателей в области, ограниченной осью абсцисс:

$$\omega'_i(x)=W_i-\Delta\omega'_i(x), \quad (10)$$

где W_i - нормированное значение *i*-го показателя *k*-й системы, , $\Delta\omega_i'(x)$ - нормированное значение уступки по *i*-му показателю (см. рис. 2.2). Таким образом, когда

$$\omega_{ji}<W'_i-\Delta\omega'_i(x), \quad (11)$$

система отключается.

Если после вышеописанных действий остаются неисследованные системы, то их начинают сравнивать по следующему по важности $(i + 1)$ -*y* показателю. Такой цикл повторяется *n* раз *(n* - число показателей эффективности) или до исчерпания множества систем и разделения их на эффективные и неэффективные.

После обнаружения эффективной системы метод применяется к оставшимся до полного выявления сравнительной эффективности всех рассматриваемых систем. В режиме работы программы «без экспертов» массив выходной информации представляется в виде таблицы (см. табл. П6.2).

Таблица П6.2. Представление результатов решения в варианте «без экспертов»

	Место 1	Место 2	...	Место *j*	...	Место *l*	Относительная характеристика
Система 1							
Система 2							
.....							
Система *j*							
.....							
Система *l*							

Для вычисления относительных частот попадания исследуемых систем (ε_{ji}) на назначенные места и их относительных характеристик (ξ_i) служит выражение:

$$\varepsilon_{ji} = \frac{E_{ji}}{f!}, \qquad (12)$$

$$\xi_j = \frac{\sum_{j=1}^{n}\left[\varepsilon_{ji} \times (n+1-j)\right]}{n}. \qquad (13)$$

Таким образом, для детализации рассмотренного алгоритма расчета необходимо выбрать некоторый режим.

Первый режим - обработка данных при условии, что все показатели расставлены по важности (пользователь знает их расстановку).

Второй режим - известна важность не всех показателей (возникают затруднения при расстановке менее важных показателей). Задается количество показателей, порядок важности которых известен.

Третий режим («без экспертов») — расстановка показателей по важности неизвестна вообще.

Получаемые результаты показывают не только то, какая из систем (вариантов построения) лучше, но и насколько она лучше. Такая информация является основой для принятия решения руководителем, но не самим решением, поскольку последнее слово всегда остается за лицом, отвечающим за выбор.

Метод анализа иерархий

Метод последовательных уступок хорош в тех случаях, когда имеется возможность расчетным или экспертным путем найти все значения показателей эффективности оцениваемых вариантов построения или реорганизации корпоративной системы защиты информации. В случае затруднений в определении значений показателей эффективности может быть применен *метод анализа иерархий.*

Действительно, данный метод позволяет расставить варианты построения СЗИ в порядке убывания их эффективности в случае многоуровневой (до 10) иерархической структуры показателей, *суждения об относительной значимости каждого из которых вводит эксперт* в области защиты информации.

Приложение 7
Оценка затрат (TCO) на информационную безопасность

Многие руководители служб автоматизации (CIO) и служб информационной безопасности (CISO) отечественных компаний наверняка задавались вопросами: Как оценить эффективность планируемой или существующей корпоративной системы защиты информации? Как оценить эффективность инвестиционного бюджета на информационную безопасность (ИБ) компании? В какие сроки окупятся затраты компании на ИБ? Как экономически эффективно планировать бюджет компании на ИБ и управлять им? Попробуем найти возможные ответы на эти вопросы.

История вопроса

Определение эффективности организации режима ИБ в компании предполагает некоторую оценку затрат на ИБ, а также достигаемого при этом эффекта. Действительно, сравнение этих оценок позволяет получить представление о том, как возвращаются инвестиции на ИБ, а также экономически корректно планировать бюджет предприятия на ИБ и управлять им.

На практике многие решения в области защиты информации часто принимаются на интуитивно-понятийном уровне, без каких-либо экономических расчетов и обоснований. В результате только те начальники служб ИБ, сумевшие заявить и отстоять потребность в защите информации, смогли как-то повлиять на планирование выделения бюджетных средств компании на ИБ. Однако современные требования бизнеса, предъявляемые к организации режима ИБ компании, настоятельно рекомендуют обращаться к более обоснованным технико-экономическим методам и средствам, позволяющим количественно измерять уровень защищенности компании, а также определять экономическую эффективность затрат на ИБ.

Сегодня оценивать эффективности корпоративной системы защиты информации рекомендуется с помощью некоторых критериев эффективности, например показателей *совокупной стоимости владения (TCO), экономической эффективности бизнеса, коэффициентов возврата инвестиций на ИБ (ROI)* и др.

В частности, известная методика совокупной стоимости владения была изначально предложена аналитической компанией Gartner Group в конце 80-х годов (1986-1987 гг.) для оценки затрат на информационные технологии. Методика Gartner Group позволяет рассчитать всю расходную часть корпоративной информационной системы (КИС), включая прямые и косвенные расходы на аппаратно-программные средства, организационные мероприятия, обучение и повышение квалификации сотрудников компании, реорганизацию, реструктуризацию бизнеса и т.д.

На современном этапе методика TCO может быть использована для доказательства экономической эффективности существующих корпоративных систем защиты информации. Она позволяет руководителям служб информационной безопасности обосновывать бюджет на ИБ, а также доказывать эффективность работы сотрудников службы ИБ. Кроме того, поскольку оценка экономической эффективности корпоративной системы защиты информации становится «измеримой», появляется возможность оперативно решать задачи контроля и коррекции показателей экономической эффективности, в частности показателя TCO. Таким образом, этот показатель может послужить инструментом оптимизации расходов на обеспечение требуемого уровня защищенности КИС и обоснование бюджета на ИБ. При этом компании такие работы могут выполнять самостоятельно с привлечением системных интеграторов в области защиты информации или совместно с интегратором.

Отметим, что показатель TCO применим практически на всех основных этапах жизненного цикла корпоративной системы защиты информации и помогает «навести порядок» в существующих и планируемых затратах на ИБ. С такой точки зрения данный показатель

позволяет объективно и независимо обосновать экономическую целесообразность внедрения и использования конкретных организационных и технических мер и средств защиты информации. При этом для объективности решения необходимо дополнительно учитывать состояние внешней и внутренней среды предприятия, например показатели технологического, управленческого, кадрового и финансового развития предприятия, поскольку не всегда наименьший показатель ТСО корпоративной системы защиты информации оказывается оптимальным для предприятия.

Понятно, что при умелом управлении ТСО удается рационально и экономно реализовывать средства бюджета на ИБ, достигая при этом приемлемого уровня защищенности компании, адекватного текущим целям и задачам бизнеса. Существенно, что сравнение определенного показателя ТСО с аналогичными показателями ТСО по отрасли (аналогичными компаниями) и с «лучшими в группе» позволяет объективно и независимо обосновать затраты компании на ИБ. Ведь часто трудно или практически невозможно оценить прямой экономический эффект от затрат на ИБ. Сравнение же «родственных» показателей ТСО дает возможность убедиться, что проект создания или реорганизации корпоративной системы защиты информации компании является оптимальным по сравнению с некоторым среднестатистическим проектом в области защиты информации по отрасли. Указанные сравнения удобно проводить, пользуясь усредненными показателями ТСО по отрасли, рассчитанными экспертами Gartner Group или собственными экспертами компании с помощью методов математической статистики и обработки наблюдений.

Таким образом, методика ТСО Gartner Group позволяет ответить на следующие актуальные вопросы:

- какие ресурсы и денежные средства тратятся на ИБ;
- оптимальны ли затраты на ИБ для бизнеса компании;
- насколько эффективна работа службы ИБ компании по сравнению с другими компаниями;
- как сделать управление инвестированием в защиту информации эффективным;
- какие выбрать направления развития корпоративной системы защиты информации;
- как обосновать бюджет компании на ИБ;
- как доказать эффективность существующей корпоративной системы защиты информации и службы ИБ компании в целом;
- какова оптимальная структура службы ИБ компании;
- как правильно оценить сторонние услуги по сопровождению корпоративной системы защиты информации;
- • как определить эффективность нового проекта в области защиты информации.

Западный опыт - на вооружение

В целом методика ТСО компании Gartner Group дает возможность:

- получить реалистичную информацию об уровне защищенности распределенной вычислительной среды и совокупной стоимости владения корпоративной системы защиты информации;
- сравнить подразделения службы ИБ компании как между собой, так и с аналогичными подразделениями других предприятий в данной отрасли;
- оптимизировать инвестиции на ИБ компании с учетом реального значения показателя ТСО.

Здесь под показателем ТСО понимается сумма прямых и косвенных затрат на организацию (реорганизацию), эксплуатацию и сопровождение корпоративной системы защиты информации в течение года. ТСО может рассматриваться как ключевой количественный показатель

эффективности организации ИБ в компании, так как с его помощью можно не только оценивать совокупные затраты на ИБ, но и управлять этими затратами для достижения требуемого уровня защищенности КИС.

При этом *прямые затраты* включают и капитальные компоненты затрат (ассоциируемые с фиксированными активами или «собственностью»), и трудозатраты, которые учитываются в категориях операций и административного управления. Сюда же относят затраты на услуги удаленных пользователей, сторонние услуги и др., связанные с поддержкой деятельности организации.

В свою очередь *косвенные затраты* показывают влияние КИС и подсистемы защиты информации на сотрудников компании посредством таких измеримых показателей, как простои и «зависания» корпоративной системы защиты информации и КИС в целом, затраты на операции и поддержку (не относящиеся к прямым затратам). Очень часто косвенные затраты играют серьезную роль, так как обычно они не видны в бюджете на ИБ, а выявляются при анализе затрат впоследствии, что в итоге приводит к росту «скрытых» затрат компании на ИБ.

Существенно, что TCO не просто представляет «стоимость владения» отдельными элементами и связями корпоративной системы защиты информации в течение их жизненного цикла. Овладение методикой TCO помогает службе ИБ лучше измерять и снижать затраты, а также управлять ими и/или улучшать уровни сервиса защиты информации с целью адекватности мер защиты бизнесу компании.

Подход к оценке TCO базируется на результатах аудита структуры и поведения корпоративной системы защиты информации и КИС в целом, включая действия сотрудников служб автоматизации, информационной безопасности и просто пользователей КИС. Сбор и анализ статистики по структуре прямых (HW/SW, операции, административное управление) и косвенных затрат (на конечных пользователей и простои) проводится, как правило, в течение 12 месяцев. Полученные данные оцениваются по ряду критериев с учетом сравнения с аналогичными компаниями по отрасли.

Методика TCO позволяет оценить и сравнить состояние защищенности КИС компании с типовым профилем защиты, в том числе показать узкие места в организации защиты, на которые следует обратить внимание. Иными словами, на основе полученных данных можно сформировать понятную с экономической точки зрения стратегию и тактику развития корпоративной системы защиты информации, а именно: «сейчас мы тратим на ИБ столько-то, если будем тратить столько-то по конкретным направлениям ИБ, то получим такой-то эффект».

Известно, что в методике TCO базой для сравнения служат данные и показатели TCO для западных компаний. Однако эта методика способна принимать в расчет специфику российских компаний с помощью поправочных коэффициентов, таких как:

- стоимость основных компонентов корпоративной системы защиты информации и КИС, а также информационных активов компании (Cost Profiles), включая данные о количестве и типах серверов, персональных компьютеров, периферии и сетевого оборудования;
- заработная плата сотрудников (Salary and Asset Scalars) с учетом дохода компании, географического положения, типа производства и местонахождения организации в крупном городе или нет;
- конечные пользователи ИТ (End User Scalars) - их типы и размещение (для каждого типа пользователей требуется различная организация службы поддержки и вычислительной инфраструктуры);
- использование методов так называемой лучшей практики в области управления ИБ (Best Practices) с оценкой реального состояния дел по управлению изменениями, операциями, активами, сервисному обслуживанию, обучению, планированию и управлению процессами;

– уровень сложности организации (Complexity Level), в том числе состояние организации конечных пользователей (процент влияния - 40%), технологии SW (40%), технологии HW (20%).

В целом оценка затрат компании на ИБ подразумевает решение следующих трех задач:

– определение текущего уровня ТСО корпоративной системы защиты информации и КИС в целом;
– аудит ИБ компании на основе сравнения уровня защищенности компании с рекомендуемым (лучшая мировая практика) уровнем ТСО;
– формирование целевой модели ТСО.

Рассмотрим каждую из перечисленных задач.

Оценка текущего уровня ТСО

В ходе работ по оценке ТСО проводится сбор информации и расчет показателей ТСО организации по следующим позициям:

– компоненты КИС (включая систему защиты информации) и информационные активы компании (серверы, клиентские компьютеры, периферийные устройства, сетевые устройства);
– расходы на аппаратные и программные средства защиты информации (расходные материалы, амортизация);
– затраты на организацию ИБ в компании (обслуживание СЗИ и СКЗИ, а также штатных средств защиты периферийных устройств, серверов, сетевых устройств, планирование и управление процессами защиты информации, разработка концепции и политики безопасности и пр.);
– расходы на организационные меры защиты информации;
– косвенные расходы на организацию ИБ в компании, в частности на обеспечение непрерывности или устойчивости бизнеса компании;

Аудит ИБ компании

По результатам собеседования с TOP-менеджерами компании и проведения инструментальных проверок уровня защищенности организации проводится анализ:

– политики безопасности;
– организации защиты;
– классификации информационных ресурсов и управления ими;
– управления персоналом;
– физической безопасности;
– администрирования компьютерных систем и сетей;
– управления доступом к системам;
– разработки и сопровождения систем;
– планирования бесперебойной работы организации;
– проверки системы на соответствие требованиям ИБ.

На основе выполненного анализа выбирается модель ТСО, сравнимая со средними и оптимальными значениями для репрезентативной группы аналогичных организаций, имеющих схожие с рассматриваемой организацией показатели по объему бизнеса. Такая группа берется из

банка данных об эффективности затрат на ИБ и эффективности соответствующих профилей защиты аналогичных компаний.

Сравнение текущего показателя TCO проверяемой компании с модельным значением того же показателя позволяет провести анализ эффективности организации ИБ компании, результатом которого является определение «узких» мест в организации, причин их появления и выработка дальнейших шагов в направлении реорганизации корпоративной системы защиты информации и обеспечения требуемого уровня защищенности КИС.

Формирование целевой модели TCO

По результатам проведенного аудита строится целевая (желаемая) модель, учитывающая перспективы развития бизнеса и корпоративной системы защиты информации (активы, сложность, методы лучшей практики, типы СЗИ и СКЗИ, навыки сотрудников компании и др.).

Кроме того, рассматриваются капитальные расходы и трудозатраты, необходимые для проведения преобразований текущей среды в целевую среду. В трудозатраты на внедрение включаются затраты на планирование, развертывание, обучение и разработку. Сюда же входят возможные временные увеличения затрат на управление и поддержку.

Для обоснования эффекта от внедрения новой корпоративной системы защиты информации (ROI) могут быть использованы модельные характеристики снижения совокупных затрат (TCO), отражающие возможные изменения в корпоративной системе защиты информации.

Пример оценки затрат на ИБ

В качестве примера применения методики TCO для обоснования инвестиций на ИБ рассмотрим проект создания корпоративной системы защиты информации от вирусов и враждебных апплетов, интегрированной с системой контроля и управления доступом на объекте информатизации.

Для этого сначала условно определим три возможных степени готовности такой системы, а именно: *базовую, среднюю* и *высокую.*

Базовая. Стационарные и мобильные рабочие станции обладают локальной защитой от вирусов. Антивирусное программное обеспечение и базы сигнатур регулярно обновляются для успешного распознавания и парирования новых вирусов. Установлена программа автоматического уничтожения наиболее опасных вирусов. Основная цель на этом уровне - организация минимальной защиты от вирусов и враждебных апплетов при небольших затратах.

Средняя. Внедрена сетевая программа обнаружения вирусов. Управление программными обновлениями на сервере автоматизировано. Системный контроль над событиями оповещает о случаях появления вирусов и предоставляет информацию по предотвращению дальнейшего их распространения. Превентивная защита от вирусов предполагает выработку определенной политики защиты информации, передаваемой по открытым каналам связи Internet, и следование этой политике. Дополнительно к техническим мерам активно предлагаются и принимаются организационные меры защиты информации.

Высокая. Антивирусная защита воспринимается как один из основных компонентов КСЗ. Система антивирусной защиты тесно интегрирована с комплексной системой централизованного управления ИБ компании и обладает максимальной степенью автоматизации. При этом организационные меры по защите информации преобладают над техническими. Стратегия защиты информации зависит исключительно от стратегии развития бизнеса компании.

Условно выделим три степени готовности системы контроля и управления доступом: *базовая, средняя, высокая.*

Базовая. Ведется учет серийных номеров как минимум рабочих станций и серверов, инвентаризационные таблички крепятся на соответствующее аппаратное обеспечение. Введена процедура контроля перемещения аппаратных средств КИС. Проходят постоянные и периодические инструктажи персонала компании. Особое внимание уделяется мобильным компонентам КИС.

Средняя. Имеются механические и электронные замки, шлюзовые кабины и турникеты. Организованы контрольно-пропускные пункты и проходные. Осуществляется видеонаблюдение на объекте информатизации. Требования к персоналу выработаны и доведены до сведения сотрудников под расписку. Разработаны инструкции по действию в штатных и внештатных ситуациях. Привлекаются частные и государственные охранные предприятия и структуры.

Высокая. Обеспечение физической безопасности аппаратных средств является частью единой политики безопасности, утвержденной руководством компании. Активно используется весь комплекс мер защиты информации - от организационного до технического уровня.

Проект создания корпоративной системы защиты информации от вирусов предполагает определенное развитие и переход от некоторого базового уровня (уровень 0) к более высокому (уровень 10 в соответствии с лучшей практикой). В табл. П7.1 приведены характеристики процесса развития корпоративной системы защиты информации на выделенных уровнях защиты.

Таблица П7.1. Характеристики базового и повышенного уровней защиты

Процесс	Задача	Базовый уровень (0)	Высокий уровень (10)
Защита от вирусов	Каким образом распространяются обновления механизма антивирусной защиты	Ничего не делается или нет информации	Применяется автоматическое обновление антивирусного обеспечения
Защита от вирусов	Какая степень защиты от вирусов является допустимой	Нет механизма зашиты от вирусов	Защита от вирусов устанавливается службой ИС и недоступна пользователям для изменений
Защита от вирусов	Какой процент клиентских мест поддерживается серверной антивирусной защитой (по отношению к числу вирусных событий)	0%	100%
Защита от вирусов	Как устраняются последствия вирусных атак	Пользователь самостоятельно восстанавливает поврежденные файлы и систему, протокол событий не ведется	Персонал ИС уведомляется об инциденте, проводятся исследования, и принимаются нейтрализующие меры, на местах поддерживается БД вирусных событий
Управление безопасностью	Что делается для гарантии безопасности критичных данных (информация, которая является критичной по отношению к миссии каждого отдельного предприятия)	Ничего не делается	Инструментальные средства шифрования и обеспечения безопасности закупаются у третьей стороны
Управление безопасностью	Что делается для гарантии физической безопасности помещений с целью предотвращения случаев воровства и преступного использования оборудования	Даются сигналы тревоги о нарушении безопасности	Внедряются такие средства безопасности, как смарт-карты или биометрические устройства

В табл. П7.2 представлен список статей и возможный уровень снижения расходов при развитии процессов управления информационной безопасностью и защиты от вирусов (начиная от уровня 0 и заканчивая уровнем 10).

Таблица П7.2. Статьи расходов базового и повышенного уровня защиты

Статья затрат	Защита от вирусов %	Управление *i*, безопасностью, %
Операции (Operations)		
Технические услуги (Technical services)		
Решение проблем уровня II (Tier II problem resolution)	2,600	0,000
Решение проблем уровня III (Tier III problem resolution)	1,300	0,000
Администрирование конечных пользователей (User administration, adds and changes)	0,000	6,500
Установка аппаратного обеспечения (Hardware deployment)	0,000	2,600
Резервное копирование, архивирование и восстановление (Backup, archiving and recovery)	2,600	0,000
Планирование и управление процессами (Planning and process management)		
Управление системными исследованиями, планированием и продуктами (Systems research, planning and product management)	1,300	1,300
Безопасность и защита от вирусов (Security and virus protection)	18,200	2,600
Восстановление деятельности (Business recovery)	19,500	0,000
Решение проблем уровня 0/1 (Service desk, tier 0/1)		
Среднее количество звонков пользователей в месяц (Average number of calls per month)	5,200	2,600
Административные расходы (Administration)		
Финансовые службы и администрация (Finance and administration)		
Супервизорское управление (Supervisory management)	1,268	0,618
Административная поддержка ИС (IS administrative assistance)	0,429	0,169
Управление активами (Asset management)	0,000	5,200
Аудит (Audit)	0,000	1,300
Закупка, снабжение и управление контрактами (Purchasing, procurement and contract management)	0,000	2,600
Затраты конечных пользователей на поддержку ИС (End User IS Costs)		
Время (часов в месяц), затраченное на управление файлами, данными и резервным копированием (Average hours per month spent managing files, data and performing backups)	6,500	0,000
Время (часов в месяц), затраченное на поиск источника поддержки (Average hours per month spent seeking peer support)	6,500	0,000
Время (часов в месяц), затраченное на самоподдержку пользователей (Average hours per month spent helping others)	6,500	0,000
Количество часов в месяц, затраченное на самоподдержку пользователей (Average hours per month spent on self support)	6,500	2,600
Количество незапланированных простоев в месяц (Monthly unplanned downtime hours)	10,400	10,400

В табл. П7.3 и на рис. П7.1 показан уровень снижения расходов при переходе на более высокий уровень защищенности КИС (с уровня 0 на уровень 10). Полученные данные о снижении ТСО (в среднем на 230 тыс. долл. в год) позволяют обосновать инвестиции в размере около 600 тыс. долл. на защиту от вирусов. При этом период окупаемости составляет не более трех лет.

Таблица П7.3. Уровень снижения расходов при внедрении современных методов

Расходы на ИТ, долл. США	Защита от вирусов - 0, безопасность - 0	Защита от вирусов - 10, безопасность - 0	Защита от вирусов - 0, безопасность - 10	Защита от вирусов - 10, безопасность - 10

Совокупная стоимость владения (ТСО)	14 905 090	14 659 236	14 796 746	14 563 990
Расходы на HW/SW	9 183 334	9212787	9 211 699	9 241 232
Расходы на операции ИС	1 402 287	1 376 061	1 394 232	1 368 450
Административные расходы	426 758	425 554	423 952	422 748
Расходы на операции конечных пользователей	2 772 377	2 636 870	2 758 898	2 624 287
Расходы но простои	1 120 334	1 007 965	1 007 965	907 273

Ниже представлен комментарий к указанным расходам.

Расходы на аппаратные средства и программное обеспечение. Эта составляющая модели ТСО включает серверы, компьютеры клиентов (настольные и мобильные), периферийные устройства и сетевые компоненты. Сюда же отнесены расходы на аппаратно-программные средства ИС.

Расходы на операции ИС - прямые затраты на содержание персонала, стоимость работ для поддержки инфраструктуры для пользователей ИС.

Административные расходы - прямые затраты на персонал, обеспечение деятельности и расходы внутренних/внешних поставщиков (вендоров) на поддержку ИС операций, в том числе управление, финансирование, приобретение и обучение.

Расходы на операции конечных пользователей. Это затраты на самоподдержку конечных пользователей, а также на поддержку пользователей друг другом в противовес официальной ИС поддержке. Затраты охватывают самостоятельную поддержку, официальное обучение конечных пользователей, нерегулярное (неофициальное) обучение, самостоятельные прикладные разработки, поддержку локальной файловой системы.

Расходы на простои. Данная составляющая учитывает ежегодные потери производительности конечных пользователей из-за запланированных и незапланированных отключений сетевых ресурсов, в том числе клиентских компьютеров, совместно используемых серверов, принтеров, прикладных программ, коммуникационных ресурсов и ПО для связи. Для анализа фактической стоимости простоев, которые связаны с перебоями в работе сети и оказывают влияние на производительность, исходные данные получают из обзора по конечным пользователям. Рассматриваются только простои, приводящие к потере производительности. Обсудим уровень снижения расходов при внедрении методов лучшей практики (рис. П7.1).

В табл. П7.4 и на рис. П7.2 показан пример расчета ТСО для организаций, обладающих средним уровнем защищенности КИС (уровень 5).

Рис. П7.1. Уровень снижения расходов

Таблица П7.4. Пример расчета ТСО

Расходы на ИТ, долл. США	Защита от вирусов - 0, безопасность - 0	Защита от вирусов - 10, безопасность - 0	Защита от вирусов - 0, безопасность - 0	Защита от вирусов - 10, безопасность - 10
Совокупная стоимость владения (ТСО)	12 326 994	12 234 237	12 302 964	12215093
Расходы на HW/SW	8 884 604	8 912 435	8915619	8 943 557
Расходы на операции ИС	1 016 789	999 693	1 011 027	994 231
Административные расходы	397 553	396 525	395 408	394 398
Расходы на операции конечных пользователей	1 611 683	1 549 384	1 604 710	1 542 839
Расходы на простои	416365	376 201	376 201	340 068

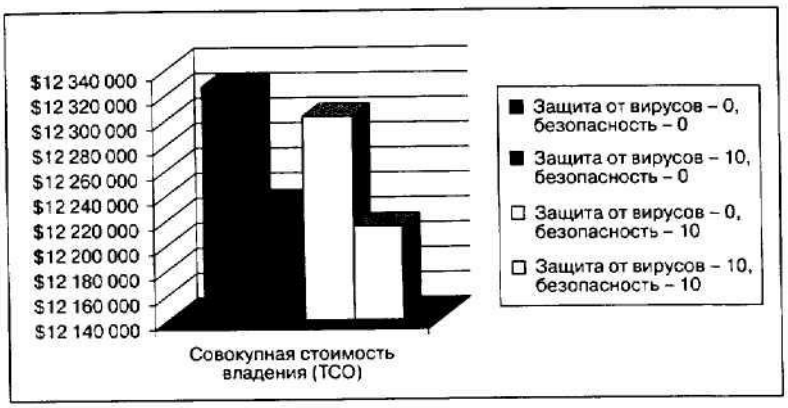


Рис. П7.2. Пример расчета ТСО

Таким образом, применение методики ТСО для обоснования инвестиций в проекты обеспечения ИБ на предприятии вполне обосновано и имеет право на существование. При этом выбор конкретной методики оценки затрат на ИБ относится к сфере ответственности руководителей соответствующих служб и отделов защиты информации.

Специфика расчета ТСО в российских условиях

В настоящее время методика ТСО Gartner Group и модели расчетов затрат на ИБ эволюционно развиваются и постоянно совершенствуются. Посмотрим, как определить прямые (бюджетные) и косвенные затраты на ИБ с учетом специфики российских компаний.

Предположим, что руководство компании внедряет на предприятии системы защиты информации. Уже определены объекты и цели защиты, угрозы информационной безопасности и меры по противодействию им, приобретены и установлены необходимые СЗИ. Чтобы требуемый уровень защиты ресурсов был реально достигнут и соответствовал ожиданиям руководства предприятия, необходимо ответить на основные вопросы, связанные с затратами на информационную безопасность:

- что такое затраты на ИБ;
- неизбежны ли затраты на ИБ;
- какова зависимость между затратами на ИБ и достигаемым уровнем безопасности;

– представляют ли затраты на ИБ существенную часть от оборота компании;
– какую пользу можно извлечь из анализа затрат на ИБ. Приведем возможные ответы на поставленные вопросы.

Что такое затраты на информационную безопасность

Как правило, затраты на ИБ подразделяются на следующие статьи:

– затраты на формирование и поддержание звена управления системой защиты информации (организационные затраты);
– затраты на контроль, то есть на определение и подтверждение достигнутого уровня защищенности ресурсов предприятия;
– внутренние затраты на ликвидацию последствий нарушения политики информационной безопасности (НПБ) - потери денежных средств, понесенные организацией в результате того, что требуемый уровень защищенности не был достигнут;
– внешние затраты на ликвидацию последствий нарушения политики информационной безопасности - компенсация потерь при НПБ в случаях, связанных с утечкой информации, ухудшения имиджа компании, утратой доверия партнеров и потребителей и т.п.;
– затраты на техническое обслуживание СЗИ и мероприятия по предотвращению нарушений политики безопасности предприятия (на предупредительные мероприятия).

При этом обычно разделяют единовременные и систематические затраты. К *единовременным* относят затраты на формирование политики безопасности предприятия: организационные расходы и расходы на приобретение и установку средств защиты. Составляющие *систематических* затрат представлены на рис. П7.3.

Рис. П7.3. Состав систематических затрат

Понятно, что классификация затрат условна, поскольку сбор и анализ затрат на информационную безопасность - это внутренняя деятельность предприятий, и детальная разработка перечня зависит от особенностей конкретной организации. Самое главное при определении затрат на систему безопасности - взаимопонимание и согласие по деталям внутри предприятия. Кроме того, статьи затрат должны быть постоянными и не дублировать друг друга.

Примерный перечень затрат на безопасность

Предположим, что основы политики безопасности на предприятии сформированы. Поэтому рассмотрим подробнее систематические затраты, которые можно разбить на несколько групп.

Первую группу составляют затраты на обслуживание системы безопасности (на предупредительные мероприятия), то есть на:

– управление системой защиты информации:

- планирование СЗИ предприятия;
- изучение возможностей информационной инфраструктуры предприятия по обеспечению безопасности информации ограниченного распространения;
- техническая поддержка производственного персонала при внедрении средств защиты и процедур и планов защиты информации;
- проверка сотрудников на лояльность, выявление угроз безопасности;
- организация системы допуска исполнителей и сотрудников конфиденциального делопроизводства с соответствующими штатами и оргтехникой;

– регламентное обслуживание средств защиты информации:
  - обслуживание и настройка программно-технических средств защиты, операционных систем и установленного сетевого оборудования;
  - организация сетевого взаимодействия и безопасного использования информационных систем;
  - поддержание системы резервного копирования и ведение архива данных;
  - проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, средств вычислительной техники и т.п.;
– аудит системы безопасности:
  - контроль изменений состояния информационной среды предприятия;
  - система контроля за действиями исполнителей;
– поддержание качества технологий:
  - обеспечение соответствия требованиям качества информационных технологий, в том числе анализ возможных негативных аспектов информационных технологий, которые влияют на целостность и доступность информации;
  - доставка (обмен) конфиденциальной информации;
  - удовлетворение субъективных требований пользователей: стиль, удобство интерфейсов и др.;
– поддержание доверия к технологии:
  - обеспечение соответствия принятым стандартам и требованиям, достоверности информации, действенности средств защиты;
– обучение персонала:
  - повышение квалификации сотрудников предприятия в вопросах использо вания имеющихся средств защиты, выявления и предотвращения угроз бе зопасности;
  - развитие нормативной базы службы безопасности;
– другие затраты:
  - заработная плата секретарей и служащих, организационные и прочие расходы, которые непосредственно связаны с предупредительными мероприятиями.

Ко второй группе относятся затраты на контроль, а именно на:

– плановые проверки и испытания:
  - проверки и испытания программно-технических средств защиты информации;
  - проверка навыков эксплуатации средств защиты персоналом предприятия;
  - обеспечение работы лиц, ответственных за реализацию конкретных процедур безопасности по подразделениям;

- оплата работ по контролю правильности ввода данных в прикладные системы;
- оплата инспекторов по контролю соответствия требованиям, предъявляемым к защитным средствам при разработке любых систем (контроль выполняется на стадии проектирования и спецификации требований);

– внеплановые проверки и испытания:
  - оплата работы испытательного персонала специализированных организаций;
  - предоставление испытательному персоналу (внутреннему и внешнему) материально-технических средств;

– соблюдение политики безопасности:
  - затраты на контроль реализации функций управления защитой коммерческой тайны;
  - затраты на организацию временного взаимодействия и координации между подразделениями для решения повседневных конкретных задач;
  - затраты на проведение аудита безопасности по каждой автоматизированной информационной системе, выделенной в информационной среде предприятия;
  - материально-техническое поддержание системы контроля доступа к объектам и ресурсам предприятия;

– внешние контрольные затраты:
  - контрольно-проверочные мероприятия, связанные с лицензионно-разрешительной деятельностью в сфере защиты информации;

– анализ политики безопасности предприятия:
  - идентификация угроз безопасности;
  - поиск уязвимостей системы защиты информации;
  - оплата работы специалистов по определению возможного ущерба и переоценке степени риска.

Третья группа включает внутренние затраты на ликвидацию последствий нарушения политики безопасности, то есть на:

– восстановление системы безопасности до соответствия требованиям политики безопасности:
  - установка обновлений или приобретение последних версий программных средств защиты информации;
  - приобретение технических средств взамен пришедших в негодность;
  - проведение дополнительных испытаний и проверок технологических информационных систем;
  - утилизация скомпрометированных ресурсов;

– восстановление информационных ресурсов предприятия:
  - восстановление баз данных и прочих информационных массивов;
  - проведение мероприятий по контролю достоверности данных, подвергшихся атаке на целостность;

– выявление причин нарушения политики безопасности:
  - расследования нарушений политики безопасности (сбор данных о методах совершения, механизме и способах сокрытия неправомерного деяния; поиск следов, орудий и предметов посягательства; выявление мотивов неправомерных действий и т.д.);
  - обновление планов обеспечения непрерывности деятельности службы безопасности;

– переделки:
  – внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности;
  – повторные проверки и испытания СЗИ.

Внешние затраты на ликвидацию последствий нарушения политики безопасности образуют четвертую группу. Они связаны с:

– обязательствами перед государством и партнерами (восстановление удовлетворенности):
  – восстановление доверия потребителя, партнеров и государства;
  – юридические споры и выплаты компенсаций;
  – разрыв деловых отношений с партнерами;
– тратой лидерства:
  – проведение дополнительных исследований и разработки новой рыночной стратегии;
  – отказ от организационных, научно-технических или коммерческих решений, ставших неэффективными в результате утечки сведений, и расходы на разработку новых средств ведения конкурентной борьбы;
  – снижение приоритетности научных исследований и невозможность патентования и продажи лицензий на научно-технические достижения;
– продвижением продукции:
  – ликвидация «узких мест» в снабжении, производстве и сбыте продукции;
  – компрометация производимой предприятием продукции и падение цен на нее;
  – возникновение трудностей в приобретении оборудования или технологий, в том числе повышение цен на них, ограничение объема поставок;
– экономическим ущербом:
  – невозможность выполнения функциональных задач, определенных уставом, и др.

Неизбежны ли затраты на информационную безопасность Очевидно, что невозможно полностью избежать затрат на безопасность, однако их можно свести к приемлемому уровню. Одни виды затрат на безопасность являются абсолютно необходимыми, другие могут быть существенно уменьшены или исключены и могут исчезнуть при отсутствии нарушений политики безопасности либо сократиться, если количество и разрушающее воздействие нарушений станет меньше.

При соблюдении политики безопасности и проведении профилактики нарушений удается исключить или существенно уменьшить затраты на:

– восстановление системы безопасности до соответствия требованиям политики безопасности;
– восстановление ресурсов информационной среды предприятия;
– переделки внутри системы безопасности;
– восстановление доверия государственных организаций и партнеров;
– юридические споры и выплаты компенсаций;
– выявление причин нарушения политики безопасности.

Необходимые затраты обязательны даже при достаточно низком уровне угроз безопасности. Это затраты на поддержание достигнутого уровня защищенности информационной среды предприятия.

Неизбежными являются *затраты* на:

- обслуживание технических средств защиты;
- конфиденциальное делопроизводство;
- обеспечение функционирования и аудит системы безопасности;
- поддержание минимального уровня проверок и контроля с привлечением специализированных организаций;
- обучение персонала методам информационной безопасности.

Затраты на ИБ и уровень достигаемой защищенности

Общие затраты

Сумма всех затрат на повышение уровня защищенности предприятия от угроз ИБ составляет общие затраты на безопасность.

Взаимосвязь между всеми затратами на безопасность, общими затратами на безопасность и уровнем защищенности информационной среды предприятия может быть представлена так, как это изображено на рис. П7.4.

Общие затраты на безопасность складываются из затрат на предупредительные мероприятия, на контроль и восполнение потерь (внешних и внутренних). С изменением уровня защищенности информационной среды изменяются величины составляющих общих затрат и, соответственно, их сумма - общие затраты на безопасность. Мы не включаем в данном случае единовременные затраты на формирование политики ИБ предприятия, так как на любом действующем предприятии такая политика уже выработана.

Снижение общих затрат

Из примера, представленного на рис. П7.4, видно, что достигаемый уровень защищенности измеряется в категориях «большой риск» и «риск отсутствует» (совершенная защита). Рассматривая левую сторону графика (большой риск),

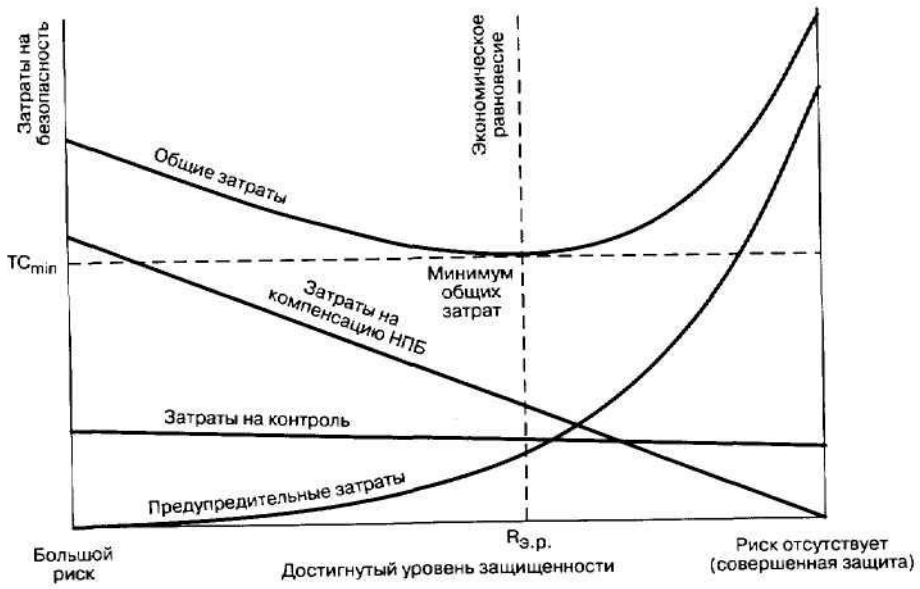


Рис. П7.4. Взаимосвязь между затратами на безопасность и достигаемым уровнем защищенности

мы видим, что общие затраты на безопасность высоки в основном потому, что велики потери на компенсацию при нарушениях политики безопасности. Расходы же на обслуживание системы безопасности очень малы.

При движении по графику вправо достигаемый уровень защищенности возрастает (снижается информационный риск). Это происходит за счет увеличения объема предупредительных мероприятий, связанных с обслуживанием системы защиты. Расходы на компенсацию НПБ уменьшаются в результате предупредительных действий. Как показано на графике, на этой стадии расходы из-за потерь падают быстрее, нежели растут затраты на предупредительные мероприятия. В результате общие затраты на безопасность становятся меньше. Изменения объема затрат на контроль незначительны.

Увеличение общих затрат

Если двигаться по графику вправо, за точку экономического равновесия (то есть в область, где достигаемый уровень защищенности повышается), ситуация начинает меняться. Мы видим, что стремление добиться устойчивого снижения затрат на компенсацию нарушений политики безопасности приводит к более быстрому возрастанию затрат на предупредительные мероприятия. Получается, что ценой расходования значительного объема средств удается достичь сравнительно малого снижения уровня риска.

Экономическое равновесие

График на рис. П7.4 отражает только общий случай, так как построен с учетом некоторых допущений, не всегда отвечающих реальным ситуациям.

Первое допущение заключается в том, что предупредительная деятельность по техническому обслуживанию комплекса программно-технических средств защиты информации и предупреждению нарушений политики безопасности предприятия соответствует правилу Парето: в первую очередь рассматриваются те проблемы, решение которых дает наибольший эффект в части снижения информационного риска. Если не следовать этой модели, то вид графика станет совсем иным.

В соответствии со *вторым допущением* предполагается, что так называемое экономическое равновесие не изменяется во времени. В реальности все обстоит несколько иначе, поскольку на графике не учитываются два важных фактора:

- во-первых, предупредительная (превентивная) деятельность на практике - не просто порча бумаги, она позволяет не повторять допущенные ранее ошибки; но такая деятельность требует больших затрат, и экономический баланс может сдвигаться вправо по диаграмме;
- во-вторых, разработчики средств защиты не успевают за активностью злоумышленников, изыскивающих все новые и новые бреши в системах защиты. Кроме того, информатизация предприятия может породить новые проблемы, решение которых потребует дополнительных предупредительных затрат. Все это в состоянии сместить экономическое равновесие по направлению к левому краю диаграммы.

Опасность ошибочной интерпретации

Многие руководители служб безопасности (СБ) предприятий уверены в том, что они работают на уровне защищенности, отвечающем экономическому равновесию. Однако, как показывает практика, очень часто они не имеют веских доказательств для подтверждения этого предположения.

Рассматриваемый график - идеализированный, на нем уровень защищенности информационной среды предприятия от угроз безопасности представлен в терминах «высокий» и «низкий» и не соотносится с процентом возможного ущерба.

Руководитель службы безопасности, который не сомневается, что у него обеспечен базовый уровень защищенности, склонен считать, что это и есть экономическое равновесие, тогда как руководитель СБ, полагающий, что он поддерживает максимальный уровень защищенности, верит, что экономическое равновесие находится именно на этом уровне.

Приведенный график может внушить таким руководителям СБ уверенность в том, что повышение защищенности информационной среды на их предприятиях будет сопровождаться лишь увеличением затрат. В результате никакой дополнительной предупредительной деятельности вестись не будет.

Нет совершенства

Если предупредительные мероприятия проводятся должным образом и являются эффективными, то достаточно трудно доказать, что на каком-либо предприятии общие затраты на безопасность выросли из-за увеличения расходов на эти нужды.

С другой стороны, если мы имеем дело с режимным объектом, обладающим очень низким уровнем риска, то есть теоретически возможны ситуации, при которых событие наступает, но случается это редко, а потенциальный ущерб сравнительно невелик, то на таком объекте общие затраты на безопасность незначительны.

Оба факта, взятые вместе, могут привести к заключению, что концепция экономического равновесия не подтверждается. Однако многие руководители предприятий уверены в правомочности этой концепции, но рассматривают ее как основание для того, чтобы не повышать уровень защищенности информационной среды.

Доля затрат на ИБ в обороте компании

Эта доля действительно существенна? Самый простой ответ: «Да, конечно!». Там, где затраты на безопасность должным образом учтены, они могут составлять оТ2 до 20% и более от объема продаж (оборота). Эта оценка получена из опыта работы авторов на основе анализа состояния защищенности информационной среды предприятий металлургической отрасли и связи. Типичное разделение затрат на информационную безопасность представлено в табл. П7.5.

Таблица П7.5. Распределение затрат на ИБ

Виды затрат		Расходы на безопасность
Затраты на потери (внешние и внутренние)	=	70% от общих затрат на безопасность
Затраты на контроль	=	25% от общих затрат на безопасность
Затраты на предупредительные мероприятия	=	5% от общих затрат на безопасность

Допустим, указанные затраты на безопасность составляюТ10% оборота. Далее предположим, что за счет увеличения объема предупредительных мероприятий и, следовательно, возрастания предупредительных затрат удалось снизить общие расходы на безопасность до 6% от оборота. Теперь распределение общих затрат на безопасность может быть таким, как описано в табл. П7.6.

Таблица П7.6. Распределение общих затрат на ИБ

Виды затрат		Расходы на безопасность
Затраты на потери (внешние и внутренние)	=	50% от новой величины общих затрат на безопасность
Затраты на контроль	=	25% от новой величины общих затрат на безопасность
Затраты на предупредительные мероприятия	=	25% от новой величины общих затрат на безопасность

Однако общие затраты на безопасность составили только 60% от их первоначальной величины.

Как новое их распределение выглядит по отношению к первоначальным общим затратам на безопасность, показано в табл. П7.7.

Таблица П7.7. Распределение затрат на ИБ

Виды затрат		Расходы на безопасность
Затраты на потери (внешние и внутренние)	$\frac{50\times60}{100}=$	30% от начальной величины общих затрат на безопасность

Затраты на контроль	25×60= 100	25% от начальной величины общих затрат но безопасность
Затраты на предупредительные мероприятия	25×60= 100	25% от начальной величины общих затрат на безопасность
Экономия	=	40% от начальной величины общих затрат на безопасность

Важным следствием рассуждений является вывод о том, что экономия расходов на безопасность невозможна без совершенствования системы защиты информации предприятия.

При оценке затрат на систему безопасности любого предприятия необходимо учитывать соотношение общих затрат на безопасность и общего объема продаж.

Определение объема затрат

Как идентифицировать затраты на безопасность

Первая задача - определить перечень затрат, которые относятся к деятельности предприятия, и распределить их по категориям.

Вторая - составить перечень таким образом, чтобы смысл каждой позиции (каждого элемента) был ясен персоналу предприятия.

Третья - назначить кодовые символы для каждой позиции перечня. Это может быть, например, цифра, буква или их комбинация.

Общий смысл сбора данных по затратам на безопасность - обеспечить руководство предприятия инструментом управления.

Особенно важно, чтобы позиции перечня затрат были определимы в том виде, как они названы и распределены для различных категорий, в том числе для:

- подразделения или какого-либо участка;
- защищаемого ресурса (по всем типам ресурсов);
- какого-либо рабочего места пользователя информационной среды предприятия;
- рисков по каждой категории информации.

Требования устанавливаются самим предприятием для собственного (внутреннего) пользования. Однако при этом не следует забывать, что собранной информации должно быть достаточно для проведения последующего анализа.

Система защиты информации, а следовательно, и система учета и анализа затрат на безопасность, которая не учитывает особенности предприятия, имеет слишком мало шансов на успех. Такая система должна быть встроена в организацию, как бы «сшита по мерке», ее нельзя взять в готовом виде.

Как определить затраты на безопасность

После того как будет установлена система классификации и кодирования различных элементов затрат на безопасность, необходимо выявить источники данных о затратах. Такая информация уже может существовать, часть ее достаточно легко получить, в то время как другие данные определить значительно труднее, а некоторые могут оказаться недоступными.

Затраты на контроль

Посмотрим еще раз на элементы затрат на контроль. Очевидно, что основной объем затрат составляет оплата труда персонала службы безопасности и прочего персонала предприятия, занятого проверками и испытаниями. Эти затраты могут быть установлены весьма точно. Оставшиеся затраты в основном связаны со стоимостью конкретных специальных работ и услуг внешних организаций и материально-техническим обеспечением системы безопасности. Их можно определить напрямую.

Итак, мы видим, что получить точную картину по затратам на контроль достаточно просто.

Внутренние затраты на компенсацию нарушений политики безопасности Определить элементы затрат этой группы намного сложнее, но большую часть оценить достаточно легко:

- установку патчей или приобретение последних версий программных средств защиты информации;
- приобретение технических средств взамен пришедших в негодность;
- восстановление баз данных и прочих информационных массивов;
- обновление планов обеспечения непрерывности деятельности службы безопасности;
- внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности.

Труднее выявить объемы заработной платы и накладных расходов на:

- проведение дополнительных испытаний и проверок технологических информационных систем;
- утилизацию скомпрометированных ресурсов;
- повторные проверки и испытания системы защиты информации;
- мероприятия по контролю достоверности данных, подвергшихся атаке на целостность;
- расследование нарушений политики безопасности.

Выяснение затрат на эти виды деятельности связаны с различными службами:

- отделом информационных технологий;
- контрольно-ревизионным и финансовым отделами;
- отделом безопасности.

Поскольку каждый вовлеченный сотрудник вряд ли в течение всего рабочего дня решает проблемы, связанные лишь с внутренними потерями от нарушений политики безопасности, рассчитывать потери следует с учетом реально затраченного на эту деятельность времени. Таким образом, мы опять убеждаемся, что основные виды затрат в этой категории могут быть определены с достаточной степенью точности.

Внешние затраты на компенсацию нарушений политики безопасности

Часть внешних затрат на компенсацию нарушений политики безопасности обусловлена тем, что были скомпрометированы коммерческие данные партнеров и персональные данные пользователей услуг предприятия. Затраты, необходимые для восстановления доверия, находятся таким же образом, как и в случае внутренних потерь.

Однако существуют и другие расходы, которые не так просто оценить. В их числе:

- затраты на проведение дополнительных исследований и разработку новой рыночной стратегии;
- потери от снижения приоритетности научных исследований и невозможности патентования и продажи лицензий на научно-технические достижения;
- расходы, связанные с ликвидацией «узких мест» в снабжении, производстве и сбыте продукции;
- потери от компрометации производимой предприятием продукции и снижения цен на нее;
- трудности в приобретении оборудования или технологий, в том числе повышение цен на них, ограничение объема поставок.

Необходимость в перечисленных расходах может быть вызвана действиями персонала различных отделов, например проектного, технологического, планово-экономического, юридического, хозяйственного, отделов маркетинга, тарифной политики и ценообразования.

Поскольку сотрудники всех этих отделов едва ли посвящают полный рабочий день вопросам внешних потерь, при установлении объема затрат, опять-таки, следует брать в расчет реально израсходованное время.

И все же, один из элементов внешних потерь действительно невозможно точно вычислить - это потери, связанные с подрывом имиджа предприятия, снижением доверия потребителя к продукции и услугам предприятия. Именно по этой причине 85% корпораций Великобритании скрывают, что их сервис небезопасен. Корпорации боятся обнародования такой информации даже больше, чем атаки в той или иной форме. Однако многие предприятия игнорируют эти затраты на основании того, что их нельзя оценить с какой-либо степенью точности, - их объем только предположителен.

Затраты на предупредительные мероприятия

Эти затраты подсчитать, вероятно, сложнее всего, поскольку предупредительные мероприятия проводятся в разных отделах и затрагивают многие службы. Они могут появляться на любом из этапов жизненного цикла ресурсов информационной среды предприятия, а именно:

- планирования и организации;
- приобретения и ввода в действие;
- доставки и поддержки;
- мониторинга процессов, составляющих информационную технологию.

В добавление к этому большинство затрат данной категории связано с работой персонала службы безопасности. Затраты на предупредительные мероприятия в основном включают заработную плату и накладные расходы. Однако точность их определения в большей степени зависит от точности установления времени, израсходованного каждым сотрудником в отдельности.

Некоторые предупредительные затраты легко выявить напрямую. К ним, в частности, может относиться оплата различных работ сторонних организаций, например:

- обслуживание и настройка программно-технических средств защиты, операционных систем и используемого сетевого оборудования;
- проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, средств вычислительной техники и т.п.;
- доставка конфиденциальной информации;
- консультации;
- курсы обучения.

Источники сведений о затратах

При определении затрат на обеспечение информационной безопасности необходимо помнить, что:

- затраты на приобретение и ввод в действие программно-технических средств могут быть найдены путем анализа накладных, записей в складской документации и т.п.;
- выплаты персоналу легко проверить по ведомостям;
- объемы выплат заработной платы должны быть взяты с учетом реально затраченного времени на проведение работ по обеспечению информационной безопасности; если только часть времени сотрудника уходит на деятельность по обеспечению информационной безопасности, то целесообразность оценки каждой из составляющих затрат его времени не должна подвергаться сомнению;
- классификацию затрат на безопасность и распределение их по элементам следует сделать частью повседневной работы внутри предприятия. С этой целью персоналу нужно хорошо знать различные элементы затрат и соответствующие им коды.

Если все элементы собраны и распределены с достаточной точностью, то последующий анализ затрат на безопасность может свестись лишь к интерпретации данных.

Ответственность за сбор и анализ информации

Кто должен заниматься сбором и анализом данных, составлением отчета о затратах на безопасность? Недопустимо, чтобы это происходило от случая к случаю, тут требуется система. К тому же необходима уверенность в том, что все данные согласуются с финансовыми материалами, счетами и т.д. Кажется логичным привлечение экономистов к подобной работе. Однако они будут нуждаться в помощи по вопросам классификации и анализа элементов затрат, а это уже задача начальника службы безопасности.

Возможное распределение деятельности и ответственности за нее представлено в табл. П7.8.

Таблица П7.8. Распределение деятельности по сбору и анализу данных о затратах на ИБ

Вид деятельности	Исполнитель
Определение категорий затрат	Экономический отдел и служба безопасности
Сбор данных о затратах	Экономический отдел
Распределение данных по категориям	Экономический отдел
Предоставление данных о затратах в службу безопасности	Экономический отдел
Анализ затрат	Служба безопасности
Исследование причин	Служба безопасности
Разработка рекомендаций по снижению затрат	Служба безопасности
Составление отчета о затратах на безопасность и его рассылка	Служба безопасности
Координация деятельности по управлению затратами внутри всего предприятия	Служба безопасности
Наблюдение за выполнением рекомендаций и корректирующих мероприятий	Служба безопасности

Необязательно, чтобы все было именно так. Каждая организация устанавливает свою собственную систему контроля и анализа затрат на безопасность.

База измерений

Если изучать затраты на безопасность, взятые сами по себе в абсолютном (стоимостном) выражении, можно сделать неверные выводы. Для иллюстрации сказанного рассмотрим пример. Предположим, что в какой-либо организации общие затраты на безопасность за четыре периода подряд составили (в относительных единицах):

11 12 13.

Эти данные, рассмотренные изолированно, позволяют сделать вывод, что увеличение затрат на безопасность выходит из-под контроля.

Тем не менее, если посмотреть объем производства за те же самые периоды времени, обнаружатся следующие величины:

100 120 140.

Если теперь сравнить отношение *общих затрат на безопасность* к *объему производства* за тот же период, можно получить следующие данные:

12,5% 11% 10% 9,3%.

Очевидно, что управление затратами на безопасность не только не ухудшалось по периодам, как это предполагалось первоначально, а скорее улучшалось. Хотя общие затраты на безопасность возросли, объем производства увеличился в большей степени. Таким образом, *необходимо соотносить затраты на безопасность с какой-либо другой характеристикой деятельности, которая чувствительна к изменению производства.*

В рассмотренном выше примере объем производства отражает так называемую *базу измерений.*

При определении отношения затрат на безопасность к какой-либо подходящей базе измерений необходима уверенность, что все эти характеристики определялись для одного и того же периода.

Типовые базы измерений

Для многих организаций вполне приемлемо соотносить затраты на безопасность с объемом проданной продукции, причем имеется в виду продукция, которая уже оплачена.

Однако в случаях, когда объем продаж зависит от сезонных факторов или каких-то других циклических изменений, объем проданной продукции не может считаться достоверной базой, поскольку он будет слишком изменчивым, в то время как объем производства и затраты на безопасность могут оставаться относительно постоянными. Заметим, что объем проданной продукции отличается от объема поставленной продукции, так как возможно, чтобы поставленная потребителю продукция еще не была оплачена. Точно так же и объем произведенной продукции не обязательно совпадает с объемом реально проданной или поставленной. Конечно же, решение о том, с какой базой измерений соотносить затраты на безопасность - стоимостью произведенной продукции, числом произведенных единиц продукта, объемом проданной продукции, стоимостью поставленной продукции, следует принимать самому предприятию. Руководство при этом должно быть уверено, что полученные результаты действительно отражают реальную и объективную картину затрат на безопасность.

Другие базы измерений

Ниже рассмотрены некоторые базы измерений и приведены пояснения, почему их рекомендуется применять.

Трудоемкость

Трудоемкость может быть представлена как величина оплаты труда, непосредственно затраченного на производство продукции. Это часто встречающаяся в практике финансовая категория, и поэтому данные для использования в такой базе измерений должны быть доступными. Однако работать с трудоемкостью следует осторожно, поскольку она меняется по разным причинам, например вследствие:

- улучшения технологии;
- автоматизации технологических процессов;
- смены обслуживающего персонала.

Таким образом, трудоемкость может служить базой измерений только для коротких промежутков времени.

Важно помнить следующее:

- трудоемкость не может выступать в качестве измерительной базы в том случае, когда не учитывается эффект инфляции;
- сравнивать величины всегда надо в их стоимостном выражении.

Характерный пример обращения к данной базе: нахождение отношения внутренних затрат на компенсацию последствий нарушений политики безопасности к трудоемкости.

Объем ресурсов информационной среды предприятия

Объем ресурсов информационной среды предприятия - это совокупная стоимость собственных ресурсов, выделяемых в информационной среде предприятия. Ресурсы обычно подразделяются на несколько классов, например физические, программные и информационные (данные). Для каждого класса требуется своя методика оценки ценности.

Оценка ценности ресурсов проводится специализированными организациями во время выполнения анализа рисков безопасности предприятия. Как правило, ценность физических

ресурсов оценивается с точки зрения стоимости их замены или восстановления работоспособности. Программные ресурсы оцениваются тем же способом, что и физические, на основе определения затрат на их приобретение или восстановление. Если для информационного ресурса существуют особенные требования к конфиденциальности или целостности (например, исходный текст имеет высокую коммерческую ценность), то этот ресурс оценивается по той же схеме, то есть в стоимостном выражении.

Результаты измерений на этой базе не зависят от неравномерности продажи продукции. Кроме того, на той же базе может быть определен уровень ущерба, что позволит предприятию принять решение о более эффективной защите собственных экономических интересов. Анализ проводится с помощью определения отношения затрат на несоответствие политике безопасности к объему собственных ресурсов.

Таблица П7.9. Пример анализа затрат

Данные измерений	Вывод
0,0-0,1	Надежность защиты высокая
0,1-0,25	Проблемы в системе защиты
0,25-0,5	Следует усилить систему защиты информации
0,5-0,75	Необходимо менять политику безопасности

Альтернативные соотношения

Не следует ограничиваться только представленными выше соотношениями. Допускается использовать любые соотношения, которые помогут рассортировать интересующую нас информацию.

Использование соотношений

Целью введения всех рассмотренных соотношений является сравнение эффективности деятельности в различные периоды времени. Поэтому необходимо:

- быть последовательным в применении базы измерений;
- вводить в соотношения величины, выраженные в денежных единицах, а не в единицах времени или количества продукции.
- следить, чтобы в каждом соотношении числитель и знаменатель соответствовали одному и тому же периоду времени.

Анализ затрат на ИБ

Отчет по затратам на безопасность

Результаты анализа затрат на безопасность и итоговый отчет должны показать объективную картину, отражающую состояние безопасности.

Анализ затрат на безопасность - инструмент управления, предназначенный для определения достигнутой степени защищенности информационной среды и обнаружения проблем при постановке задач поддержания требуемого уровня безопасности.

Представленный в финансовых терминах и составленный простым языком отчет о затратах на безопасность имеет значительные преимущества перед другими видами отчетов по исследованию безопасности информационной среды предприятия и анализу рисков.

Содержание такого отчета в большей степени зависит от того, какую роль игра-ет в рамках предприятия то лицо, которому он предназначен.

Руководству следует предоставить отчет в виде общих форм. В отчете должна быть представлена общая картина состояния системы безопасности предприятия, изложенная обычно в

финансовых терминах. Другими словами, в этом случае требуется доступно написанный отчет, содержащий только объективную информацию.

Руководители подразделений информатизации и защиты информации нуждаются в более детальных сведениях о достигнутом уровне защищенности тех ресурсов информационной среды предприятия, за которые оно отвечает. Отчет должен быть очень подробным и включать данные о типах ресурсов, видах угроз и т.д.

Целью проведения анализа затрат на безопасность является получение результатов в форме, наиболее полезной и удобной для тех, кто в нем заинтересован.

Читающий отчет должен получить информацию, которая позволит:

- сравнить текущий уровень защищенности с уровнем прошлого периода, то есть определить тенденции в этом направлении;
- сравнить текущий уровень с поставленными целями;
- выявить наиболее значительные области затрат;
- выбрать области для улучшения;
- оценить эффективность программ по улучшению.

Руководитель ожидает получить отчет по затратам на безопасность, который:

- проинформирует его лишь о вещах, относящихся к сфере его компетенции, и ни о чем более;
- написан легким для понимания языком и не напичкан специальными терминами;
- изложен четко и кратко и содержит всю необходимую информацию;
- позволит определить первоочередные задачи и направления деятельности.

Отчет для руководителей подразделений информатизации и защиты информации можно построить в виде таблицы. Предположим, что составляется отчет по трем информационным ресурсам, например *A, B* и *C.* Допустим также, что эти ресурсы различаются между собой только видом содержащейся информации. При этом оценки стоимости ресурсов близки, а технологии защиты схожи друг с другом. Отчет о затратах на безопасность может быть оформлен, например, в виде табл. П7.10.

Таблица П7.10. Фрагмент отчета о затратах на безопасность

Затраты	Периоды			
	I	II	III	IV
РЕСУРС «А»				
Предупредительные	227	198	209	251
На контроль	593	616	606	614
На внутренние потери	985	1016	758	744
На внешние потери	503	528	482	427
Общие затраты на безопасность	2308	2358	2065	2036
Общие затраты на безопасность, отнесенные к объему продаж	1,0%	1,05%	0,9%	0,85%
Общие затраты но безопасность, отнесенные к трудоемкости	1,9%	2%	1,5%	1,4%
РЕСУРС «В»				
Предупредительные	206	229	340	397
На контроль	894	949	916	925
На внутренние потери	1903	1935	1034	948
На внешние потери	620	598	613	632
Общие затраты на безопасность	3623	3711	2903	2902
Общие затраты на безопасность, отнесенные к объему продаж	1,1%	1,15%	0,9%	0,9%

Общие затраты на безопасность, отнесенные к трудоемкости	2,5%	2,55%	1,4%	1,3%
РЕСУРС «С»				
Предупредительные	184	242	299	347
На контроль	815	859	831	802
На внутренние потери	1187	1191	910	893
На внешние потери	1101	1066	72	568
Общие затраты на безопасность	3287	3358	2762	261
Общие затраты на безопасность, отнесенные к объему продаж	1,2%	1,2%	1,0%	0,9%
Общие затраты на безопасность, отнесенные к трудоемкости	1,9%	1,9%	1,5%	1,4%

Анализ затрат

Если проанализировать приведенные данные по первому (I) и второму (И) периодам, можно обнаружить, что внутренние потери на компенсацию нарушений политики безопасности для ресурса *B,* а также внешние потери на НПБ для ресурса *C* чрезвычайно велики.

Руководитель отдела защиты информации предпринял по этому поводу ряд шагов. Он увеличил после второго периода объем предупредительных мероприятий для ресурса *B* и этим эффективно снизил внутренние потери на НПБ к концу третьего (III) периода.

После второго периода он усилил предупредительную деятельность для ресурса *C,* и после третьего периода внешние затраты на НПБ также уменьшились. Хотя предупредительные действия для этого ресурса не дали столь быстрого результата, как для ресурса *B,* тем не менее затраты сократились, а к концу четвертого (IV) периода - даже в большей степени.

Однако, прежде чем проводить какие-либо мероприятия по усилению защищенности информационной среды предприятия, следует ответить на два вопроса: С чего надо начинать? В чем причина происходящего? Начальнику отдела защиты информации необходима значительно большая информация, чем представленная в суммирующей таблице. Он знает, что у него возникли проблемы, но ему неизвестно, какими причинами они вызваны. Он нуждается в более детальном дроблении на составляющие суммарных затрат на безопасность.

Итак, к концу второго периода начальник отдела защиты информации получил следующие сведения, конкретизирующие внутренние затраты на НПБ по ресурсу *B* в зависимости от угроз безопасности ресурса (см. табл. П7.11).

Таблица П7.11. Составляющие затрат на внутренние потери

Код	Источник затрат	Угроза случайного или умышленного изменения информации		Угроза временной недоступности информации		Сумма (усл. ед.)	Доля (%)
		сумма	доля (%)	сумма	доля (%)		
W1	Восстановление системы защиты ресурса до соответствия требованиям ПБ	1001	89,3	120	10,7	1121	57,9
W2	Восстановление ресурса	133	100	-	-	133	6,9
W3	Выявление причин нарушения ПБ	97	87,4	14	12,6	111	5,7
W4	Переделки	440	77,2	130	32,8	570	29,5
	ИТОГО:	1671		264		1935	100

Приведенные данные показывают, что максимальные потери связаны с воздействием угрозы случайного или умышленного изменения информации и возникающей необходимостью восстановления системы защиты ресурса до соответствия требованиям политики безопасности.

Более детальная информация показывает механизмы защиты, которые были использованы для усиления системы защиты ресурса (см. табл. П7.12).

Таблица П7.12. Составляющие затрат на внутренние потери из-за реализации угрозы целостности информации

Механизмы защиты	Сумма (усл. ед.)	Доля (%)
Затраты на введение дополнительных мер, связанных с учетом подключений пользователей к ресурсу	133	13,29
Затраты на введение дополнительных мер, связанных с контролем прав доступа сотрудников и учетом изменений их состояния (увольнение, перевод, отпуск, продолжительная болезнь)	88	8,79
Затраты на установку системы передачи файлов отчетов на сервер протоколирования	280	27,97
Приобретение дополнительных модулей удаленных запросов администратором безопасности	500	49,95
ИТОГО:	1001	100

Анализ этих сведений помогает установить, что предупредительные мероприятия должны быть направлены в первую очередь на обеспечение соответствия требованиям качества информационных технологий, а во вторую - на решение проблемы аудита системы безопасности и т.д.

Продолжим анализ. Начальник отдела защиты информации, прежде чем тратить средства на предупредительные мероприятия в области поддержания качества информационной технологии, подробно и досконально рассматривает возможные причины нанесения ущерба (уязвимости технологии защиты ресурса), например такие:

- недостаточные возможности по архивированию данных;
- бессистемность в части архивирования данных;
- непригодность механизма учета и контроля носителей резервных копий;
- слабость нормативной базы;
- пренебрежение практикой проведения тестовых испытаний системы защиты ресурса;
- недостаточность технических систем охлаждения и питания серверных комнат;
- отсутствие регламента программно-технических средств «типовой рабочей станции» и т.д.

Как оказалось в нашем примере, ни на одну из перечисленных причин не приходится более чем 8% от общей величины потерь в рассматриваемый период. Но затраты на минимизацию таких потерь будут существенно разными в зависимости от решаемой проблемы: наименьшие в случае совершенствования нормативной базы и, возможно, весьма значительные при оборудовании серверных комнат техническими системами охлаждения и питания.

Принятие решений

Все выявленные причины нанесения ущерба заслуживают проведения корректирующих мероприятий, однако руководитель ищет те области, которые дадут наибольшую отдачу в ответ на затраченные усилия. Именно поэтому он может рассмотреть в первую очередь область своих затрат, связанную с внедрением системы передачи отчетов на сервер протоколирования.

Тщательный анализ может привести начальника отдела защиты информации к выводу о том, что лучше начать предупредительные мероприятия с механизмов защиты, имеющих не самую большую затратную часть.

Без доступной детальной информации борьба за повышение уровня защищенности информационной среды предприятия будет равносильна «тушению огня» вместо «предупреждения пожаров».

Итак, необходимо отметить следующее: *затраты на безопасность могут быть сокращены в значительной степени, если удастся выявить специфические причины потерь и предложить программы уменьшения рисков. Во все рекомендации по улучшениям следует включать данные о стоимости реализации предложенных программ. Меры снижения уровня риска должны преследовать следующую цель -с наименьшими затратами получить наилучшие результаты.*

Внедрение системы учета затрат на ИБ

Все вышеизложенное может показаться сложным и трудоемким для реализации. Вероятно, в связи с этим на практике редко встречаются организации, внедрившие систему сбора и анализа затрат на безопасность.

Руководители системы безопасности должны быть уверены в полезности этого мероприятия. Следовательно, нужно убедить их. Приведем некоторые «секреты» успешного внедрения системы:

1) Возьмитесь за простое, не пытайтесь сразу же охватить все ресурсы, требующие защиты; выберите один вид ресурса - по собственному желанию -и стройте систему, которую сможете наполнить фактическими экономическими данными.

2) Начните с тех затрат на безопасность, для которых данные уже известны; при необходимости определите иные необходимые затраты «экспертным» способом.

3) Работая над построением системы, вы можете обнаружить какое-нибудь неожиданное препятствие; не бойтесь этого и не откладывайте задачу - решив ее один раз, вы облегчите себе жизнь в будущем.

4) Упростите систему так, чтобы она соответствовала вашим потребностям.

5) Если затраты определены с точностью ±5%, то работа сделана хорошо. Директор предприятия теперь будет иметь более точную картину затрат на безопасность, а следовательно, и оценку уровня риска.

6) Начинайте с малого и наращивайте постепенно.

7) Создайте образец, чтобы показать, как это может быть сделано.

8) Подтвердите документами ценность анализа затрат на ИБ.

Резюме

Методику TCO можно успешно сочетать с разнообразными методами для расчета возврата инвестиций (ROI). Как правило, при оценке доходной части сначала анализируют те цели, задачи и направления бизнеса, которые необходимо достигнуть с помощью внедрения или реорганизации существующих проектов в области системной интеграции, автоматизации и информационной безопасности. Далее с помощью некоторых измеримых показателей бизнеса оценивают эффект от каждого решения отдельно - допустим, с целью сокращения операционных расходов, обеспечения приемлемой конкурентной способности, улучшения внутреннего контроля и т.д. Перечисленные показатели не надо выдумывать, они существуют в избытке. Далее можно применить методики расчета *коэффициентов возврата инвестиций в инфраструктуру предприятия,* например той же Gartner Group.

По нашему мнению, достаточно результативно принять следующую комбинацию: TCO как расходную часть и ROI как расчетную. Более того, в настоящее время существуют и другие методы и технологии расчета и измерения различных показателей экономической эффективности.

Заключение

Уважаемый читатель, мы надеемся, что настоящая книга оказалась для вас интересной и полезной. Хочется заметить, что своевременно разработанные и утвержденные руководством компании корпоративные методики анализа и управления информационными рисками дают возможность:

- произвести оценку текущего состояния безопасности, задать допустимые уровни остаточных рисков, разработать план мероприятий по обеспечению требуемой степени безопасности в организационно-управленческом, технологическом и техническом аспектах с использованием современных методик и средств;
- рассчитать и экономически обосновать перед руководством или акционерами размер необходимых вложений в поддержание безопасности на основе технологий анализа рисков, соотнести расходы на обеспечение безопасности с потенциальным ущербом и его вероятностью;
- выявить наиболее опасные угрозы и уязвимости и провести первоочередные мероприятия по их нейтрализации до осуществления атак на уязвимые ресурсы;
- определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц, занимающихся информационной безопасностью предприятия, создать необходимый пакет организационно-распорядительной документации;
- разработать и согласовать со службами организации и надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;
- обеспечить поддержание внедренного комплекса защиты в соответствии с изменяющимися условиями функционирования организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

Выполнение приведенных выше мероприятий открывает перед должностными лицами разного уровня новые широкие возможности и позволяет:

- руководителям организаций и предприятий:
  - разработать концепцию и политику безопасности предприятия;
  - рассчитать, согласовать и обосновать необходимые затраты на организацию защиты информационной системы предприятия;
  - объективно и независимо оценить текущей уровень информационной безопасности предприятия;
  - обеспечить требуемый уровень безопасности и в целом повысить экономическую эффективность предприятия;
  - создавать и эффективно использовать профили защиты конкретного предприятия на основе неоднократно апробированных и адаптированных качественных и количественных методик оценки информационной безопасности компании;
- начальникам служб автоматизации (СЮ) и информационной безопасности (CISO):
  - получить оперативную и объективную качественную и количественную оценку состояния информационной безопасности предприятия на всех основных уровнях рассмотрения вопросов безопасности (организационно-управленческом, технологическом и техническом);
  - выработать и обосновать необходимые меры организационного характера (состав и структуру службы информационной безопасности, положение о коммерческой

тайне, пакет должностных инструкций и инструкции действия в нештатных ситуациях);

- составить экономическое обоснование необходимых инвестиций в защиту информации, грамотно выбрать те или иные аппаратно-программные средства защиты информации в рамках единой концепции безопасности в соответствии с требованиями документов Гостехкомиссии России, ФАПСИ, а также международных стандартов ISO 17799, 9001, 15408;
- адаптировать и применять в своей работе предложенные количественные показатели оценки информационной безопасности, методики оценки безопасности и управления ею с привязкой к экономической составляющей эффективности предприятия;

– системным, сетевым администраторам и администраторам безопасности предприятия:

- объективно оценить безопасность всех основных компонентов и сервисов корпоративной информационной системы компании, техническое состояние аппаратно-программных средств защиты информации (межсетевых экранов, маршрутизаторов, хостов, серверов, корпоративных БД и приложений);
- успешно внедрять в практику рекомендации, полученные в ходе решения задач анализа информационных рисков и управления ими, для нейтрализации и локализации выявленных уязвимостей и обеспечения режима информационной безопасности;

– сотрудникам предприятий и организаций:

- определить основные функциональные отношения и, что особенно важно, зоны ответственности, в том числе финансовой, за надлежащее использование информационных ресурсов и состояние политики безопасности компании.

Сегодня практика разработки и применения внутренних корпоративных методик анализа информационных рисков компании и управления ими находится на начальном этапе своего становления и развития. Таким образом, настоящая книга - это прежде всего попытка поделиться уже имеющимся опытом работы в данной области и предложить некоторые практические рекомендации. У нас есть большое желание продолжить работу в этом направлении, и без обратной связи с вами, уважаемые читатели, нам не обойтись. Будем весьма признательны за любые комментарии и предложения по расширению и улучшению качества книги. С нами можно связаться по адресам: s.petrenko@rambler.ru и svsim@bk.ru.

Литература

1. Абрамов А.В., Панасенко СП., Петренко С.А. VPN-решения для российских компаний // Конфидент. Защита информации. - № 1. - 2001. - С. 62-67.

2. Алексенцев А.И. О концепции защиты информации (к постановке вопроса) // Безопасность информационных технологий. - № 4. - 1998. - С. 10-14.

3. Алексенцев А.И. Защита информации. Сводный словарь основных понятий и терминов // Безопасность информационных технологий. - № 4. - 1998. -С.101-108.

4. Астахов А. Общее описание процедуры аттестации автоматизированных систем по требованиям информационной безопасности //Jet Info. - № 11(90). -2000.

5. Бабин С.А. Аудит сетей как фактор обеспечения безопасности сетей // Антонюк-Консалтинг. Сети и системы связи. - № 3. - 1998.

6. Баранов А.В., Петренко С.А. Системная интеграция и безопасность компьютерных сетей // Конфидент. Защита информации. - № 2. - 2001. - С. 34-39.

7. Батурин Ю.М. Проблемы компьютерного права. - М.: Юридическая литература, 1991.

8. Беляев А.В., Петренко С.А. Криптографические стандарты третьего тысячелетия // Chip-Россия. - № 7. - 2001. - С. 146-151.

9. Беляев А.В., Панасенко СП., Петренко С.А. Перспективы прикладной криптографии // Конфидент. Защита информации. - № 6. - 2001. - С. 70-79.

10. Березин А.С., Петренко С.А. Сейф для бизнеса // Конфидент. Защита информации. - № 4- 5. - 2002. - С. 132-135.

11. Березин А.С., Петренко С.А. Построение корпоративных защищенных виртуальных частных сетей//Конфидент. Защита информации. -№ 1. -2001. -С 54-61.

12. Березин А.С., Петренко С.А. Безопасность корпоративной информационной системы глазами бизнеса// Экспресс-электроника. - № 9. - 2002. - С. 84-87.

13. Березин А.С., Зима В.М., Петренко С.А. VPN-технологии: организация защищенного обмена конфиденциальной информацией // Конфидент. Защита информации. - № 6. - 2000. - С. 90-94.

14. Вихорев С.В., Кобцев Р.Ю. Как узнать - откуда напасть, или Откуда исходит угроза безопасности информации // Конфидент. - № 2. - 2002.

15. Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. - СПб.: Издательство Университета МВД РФ, 1997.

16. Вуе М.А., Морозов В.П. Информационно-коммерческая безопасность: защита коммерческой тайны. - СПб.: АО «Безопасность бизнеса», 1993.

17. Гайкович В.Ю. Комплексные проблемы комплексного подхода // Системы безопасности связи и телекоммуникаций. - № 6. - 1998.

18. Гайкович В.Ю., Першин А.Ю. Безопасность электронных банковских систем. - М.: Единая Европа, 1994.

19. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. - М.: МИФИ, 1995.

20. Герасименко В.А., Малюк А.А. Сущность и пути перевода процессов защиты информации на интенсивные способы. - М.: Безопасность информационных технологий. - № 4. - 1998. - С. 15-23.

21. Геррити Т. П. Проблема управления. - М.: Наука, 1971.

22. Гостехкомиссия России. Руководящий документ. Аттестационные испытания АС по требованиям безопасности информации. Типовая методика испытаний объектов информатики по требованиям безопасности информации (Аттестация АС), 1995.

23. Гостехкомиссия России. Руководящий документ. Автоматизированные системы, защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации, 1997.

24. Гришина Н.В. Вопросы планирования деятельности комплексной системы защиты информации. - М.: Безопасность информационных технологий -№ 4. - 1998. - С. 76-80.

25. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. - № 10. - 1997.

26. Гусев В.С. О некоторых подходах к обеспечению комплексной безопасности хозяйствующих субъектов // Приложение к журналу «Жизнь и безопасность», 1998.

27. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000.

28. Доценко СМ. Диплом не отходя от компьютера // Конфидент. Защита информации. - № 2. - 2001. - С. 56-60.

29. Доценко СМ. Аналитические компьютерные технологии и обеспечение безопасности компьютерных сетей // Конфидент. Защита информации. - № 2 -2000. - С. 45-52.

30. Жельников В.А. Криптография от папируса до компьютера. - М.: ABF, 1996.

31. Захарцев С.В. Сборник методических материалов // Конфидент. Защита информации. - № 2. - 2001.

32. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. -М.: Горячая линия - Телеком, 2000.

33. Зубик В.Б. и др. Экономическая безопасность предприятия (фирмы). -Минск: Высшая школа, 1998.

34. Иванов А.А., Шарлот В.В. Чрезвычайные ситуации в системе защиты информации // Конфидент. Защита информации. - № 5. - 2000. - С. 10-22.

Интеллектуальная собственность: Сборник типовых договоров. - М.: ИНФ-РА-М, 1995.

36 Информационная безопасность в учебных планах вузов: Материалы межвузовского семинара. - СПб.: Издательство СПбГУ, 1997.

37. Карпов Е.А. и др. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей. - СПб: Издательство Военного университета связи, 2000.

38. Карр Ч., Хоув Ч. Количественные методы принятия решения в управлении и экономике. - М.: Мир, 1966.

39. Каторин Ю.Ф., Куренков Е.В. и др. Большая энциклопедия промышленного шпионажа. - СПб.: Полигон, 2000.

40. Катрич С.Ф. Процесс принятия решения и АСУ. - М.: Наука, 1980.

41. Кобзарь М.Т, Калайда И.А. Общие критерии оценки безопасности информационных технологий и перспективы их использования //Jet Info. - № 1. - 1998.

42. Кобзарь М.Т., Трубачев А.П. Концептуальные основы совершенствования нормативной базы оценки безопасности информационных технологий в России // Безопасность информационных технологий. - № 4. - 2000.

43. Коваленко В. Защищайтесь, а то хуже будет // Открытые системы. - № 5-6. -1999.

44. Козьминых С.И., Десятов Д.Б., Забияко СВ. Основы проектирования систем безопасности предпринимательской деятельности // Системы безопасности. - № 39. - 2001. - С 84-85.

45. Комментарий к Уголовному кодексу Российской Федерации / Под ред. А.В. Наумова. - М.: Юристъ, 1997.

46. Кононов А.А. Страхование нового века. Как повысить безопасность информационной инфраструктуры // Connect. - № 12. - 2001.

47. Конявский В.А., Хованов В.Н. Система страхования информационных рисков как экономический механизм компенсации ущерба при воздействии угроз информационной безопасности // Системы безопасности. - № 36. - 2001.

48. Коул Э. Руководство по защите от хакеров: Пер. с англ. - М.: Издательский дом «Вильямс», 2002.

49. Курило А.П. О защите банковской тайны // Конфидент. Защита информации. - № 3. - 2001. - С. 18-23.

50. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. - М.: Новый юрист, 1999.

51. Ларичев О.И. Проблемы построения эффективных систем поддержки принятия решений. - М.: ВНИИ СИ, 1988.

52. Липаев В.В. Стандарты на страже безопасности информационных систем // PC WEEC/RE. - № 30. - 2000.

53. Лобанов А.Ф. Основная модель оценки защиты продуктов и систем информационных технологий в стандарте ISO/IEC 15408 // Безопасность информационных технологий. - № 4. - 1998. - С. 71-75.

54. Лукацкий А.В. Обнаружение атак. - СПб.: BHV-Петербург, 2001.

55. Мамаев М., Петренко С. Технологии защиты информации в Интернете -СПб.: Питер, 2002.

56. Мамаев М.А., Петренко С.А. Особенности «сторожевых собак» // Chip-Россия. - № И. - 2001. - С. 68-74.

57. Мамаев М.А., Петренко С.А. World Wild Web, или Дикая паутина // Chip-Россия. - № 1. - 2002. - С. 144-150.

58. Мамаев М.А., Петренко С.А. Что в имени тебе моем? // Chip-Россия - № 3 -2002. - С. 70-75.

59. Материалы семинара Университета МВД РФ. - СПб.: Издательство Университета МВД РФ, 1997.

60. Медведовский И.Д., Петренко С.А., Нестеров С.А. CD «Руководство по управлению информационными рисками корпоративных информационных систем Internet/Intranet». - Domina Security, 2002.

61. Медведовский И.Д, Семьянов П.В., Леонов Д.Г., Лукацкий А.В. Атака из Internet. - М.: Издательство «Солон-Р», 2002.

62. Мещеряков В.А. Криминалистическая классификация преступлений в сфере компьютерной информации // Конфидент. Защита информации - № 5 -1999. - С. 48-52.

63. Минаев В.А., Скрыль С.В., Дворянкин С.В., Потанин В.С. Безопасность информационно-телекоммуникационных систем: основные тенденции развития // Системы безопасности. - № 39. - 2001. - С. 74-77.

64. Минаев В.А., Дмитриев Ю.В., Пеньшин И.В. Все или ничего // Экспресс-электроника. - № 1. - 2001.

65. Немет Э., Снайдер Г., Сибасс С, Хейн Т.Р. UNIX: руководство системного администратора. - Киев: BHV, 2000.

66. Нестеров С.А., Петренко С.А. Программные средства анализа информационных рисков компании // Экспресс-электроника. - № 10. - 2002. - С. 84-86.

67. Никифоров Г.К. Азнакаев Г.Н. Защита коммерческой тайны. - Киев: Юринформ, 1994.

68. Норткат С, Купер М., Фирноу М., Фредерик К. Анализ типовых нарушений безопасности в сетях: Пер. с англ. - М.: Издательский дом «Вильямс», 2001.

69. Общие критерии оценки безопасности информационных технологий: Учебное пособие / Под ред. М.Т. Кобзаря, А.А. Сидака. - М.: МГУЛ, 2001.

70. Олифер В.Г. Направления развития средств безопасности предприятия // Экспресс-электроника. - № 1. - 2001.

71. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей. -СПб.: BHV-Санкт-Петербург, 2000.

72. Панасенко СП., Петренко С.А. Криптографические методы защиты для российских корпоративных систем // Конфидент. Защита информации -2001. - № 5. - С. 64-71.

73. Перечень средств защиты информации, подлежащих сертификации в Системе сертификации Гостехкомиссии России. - Гостехкомиссия России, 1995.

74. Петренко С.А., Симонов С.В. Новые инициативы российских компаний в области защиты конфиденциальной информации // Конфидент. Защита информации. - № 1. - 2003. - С. 34-41.

75. Петренко С.А., Попов Ю.И. Оценка затрат на информационную безопасность // Конфидент. Защита информации. - № 1. - 2003. - С. 45-52.

76. Петренко С.А., Симонов С.В. Как на практике создать корпоративную систему защиты информации // Экспресс-электроника. - № 12. - 2002. -С. 81-83.

77. Петренко С.А. Централизованное управление безопасностью корпоративных систем Internet/Intranet // Read.me. - № 9. - 2000. - С 24-27.

78. Петренко С.А. Технология распределенных межсетевых экранов: Эффективная защита корпоративных серверов от несанкционированного доступа // Read.me. - № 10. - 2000. - С. 14-17.

79. Петренко С.А. Защита корпоративных сетей Internet/Intranet от несанкционированного доступа // Read.me. - № 3. - 2001. - С. 34-37.

80. Петренко С.А. Защитите ваш Интернет-сервер // Data Communications. Сетевой журнал. - № 4. - 2001. - С. 73-75.

81. Петренко С.А. Безопасный доступ корпоративных сетей к Internet // Мир связи. Connect. - № 11/2. - 2000. - С. 80-82.

82. Петренко А.А., Петренко С.А. Аудит информационной безопасности // Связьинвест. - № 10. - 2002. - С. 36-38.

83. Петренко С.А. Защищенная виртуальная частная сеть (VPN): Современный взгляд на защиту конфиденциальных данных // Мир Internet. - № 1. - 2001. -С. 62-65.

84. Петренко С.А. Защищенная виртуальная частная сеть (VPN): Построение корпоративных VPN в российских условиях // Мир Internet. - № 2. -2001.-С. 56-60.

85. Петренко С.А. Защитите ваш Интернет-сервер // Мир Internet. - № 3. -2001. - С. 76-80.

86. Петренко С.А. Безопасность на высшем уровне // Chip-Россия. - № 5. - 2001. -С. 144-147.

87. Петренко С.А. Защита корпоративной сети в Internet или от Internet? // Chip-Россия. - № 6. - 2001. - С. 143-147.

88. Петренко С.А. Неприступная сеть // Chip-Россия. - № 8. - 2001. - С. 148-153.

89. Петренко С.А., Мамаев М.А. Осторожно: вас атакуют // Chip-Россия. - № 10. -2001.- С. 146-151.

90. Петренко С.А. Аудит информационной безопасности корпоративных систем Internet/Intranet"// Системы безопасности. - № 10-11(41). - 2002. - С. 85-87.

91. Петренко С.А. Подготовка предприятия к аудиту информационной безопасности // Системы безопасности. - № 2(44). - 2002. - С. 82-83.

92. Петренко С.А. Особенности организации защиты информации в корпоративных системах Internet/Intranet // Экспресс-электроника. - № 12. - 2001. -С.50-83.

93. Петренко С.А., Панасенко СП. Криптографические методы защиты информации для корпоративных систем // Экспресс-электроника. - № 2-3. - 2002. -С. 60-67.

94. Петренко С.А., Шпак В.Ф. Аудит безопасности корпоративных систем // Экспресс-электроника. - № 2-3. - 2002. - С. 68-73.

95. Петренко С.А. Управление информационными рисками компании // Экспресс-электроника. - № 2-3. - 2002. - С. 106-113.

96. Петренко С.А. Антивирусная защита компании // Экспресс-электроника. -№ 4. - 2002.- С. 60-65.

97. Петренко С.А., Богдель Д.Е., Панасенко СП. Защита информации от нелегалов Интернета // Экспресс-электроника. - № 5. - 2002. - С. 50-57.

98. Петренко С.А. Служба IT-Security: кадры решают все // Экспресс-электроника. - № 5. - 2002. - С. 96-102.

99. Петренко С.А. Российская практика построения виртуальных частных сетей // Экспресс-электроника. - № 6. - 2002. - С. 66-69.

100. Петренко А.А., Петренко С.А. Оцени свой риск // IT Manager. - № 6. - 2002. -С. 42-48.

101. Петренко С.А. Современная концепция безопасности корпоративных компьютерных систем // Конфидент. Защита информации. - № 6. - 2000. - С. 79-83.

102. Петренко С.А. Безопасное подключение к Интернету // Конфидент. Защита информации. - № 4- 5. - 2000. - С. 34-41.

103. Петренко С.А. Централизованное управление антивирусной защитой корпоративных систем Internet/Intranet // Конфидент. Защита информации. - № 2. -2001. - С. 44-47.

104. Петренко С.А. Построение эффективной системы антивирусной защиты // Конфидент. Защита информации. - № 6. - 2001. - С. 54-57.

105. Петренко С.А. Аудит безопасности корпоративных информационных систем // Конфидент. Защита информации. - № 2. - 2002. - С. 30-37.

106. Петренко С.А., Петренко А.А. Аудит безопасности Intranet. - М.: ДМК Пресс, 2002.

107. Петренко С.А. Опыт проведения аналитических работ в подразделениях холдинга «Связьинвест» // Семинар руководителей подразделений безопасности открытых акционерных обществ электросвязи «Комплексное обеспечение безопасности: Теория и практика». - 1-5 апреля 2002. Подмосковный пансионат «Поляны» Администрации Президента Российской Федерации.

108. Петренко С.А. Проектирование системы комплексной защиты информации в Internet/Intranet-системах // Межрегиональный семинар-совещание «Организация и проведение работ по информационной безопасности автоматизированных систем используемых в органах федерального казначейства». - 4-6 сентября 2001. г. Волгоград. Управление федерального казначейства по Волгоградской области. Пилотный центр.

109. Петров А.А. Компьютерная безопасность: криптографические методы защиты. - М.: ДМК, 2000.

ПО. Положение о государственном лицензировании деятельности в области защиты информации. - Гостехкомиссия России, ФАПСИ, 1997.

111. Положение по аттестации объектов информатизации по требованиям безопасности информации. - Гостехкомиссия России, 1994.

112. Положение об аккредитации органов по аттестации объектов информатики, испытательных центров и органов по сертификации продукции по требованиям безопасности информации. - Гостехкомиссия России, 1994.

113. Положение о сертификации средств защиты информации по требованиям безопасности информации. - Гостехкомиссия России, 1996.

114. Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации. - Гостехкомиссия России, 1994.

115. Положение об аккредитации органов по аттестации объектов информатики, испытательных центров и органов по сертификации продукции по требованиям безопасности информации. — Гостехкомиссия России, 1994.

116. Расторгуев С.П. Об обеспечении защиты АИС от недокументированных возможностей программного обеспечения // Конфидент. Защита информации. - № 2. - 2001. - С. 26-29.

117. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 1999.

118. Саати Т., Кернс К. Аналитическое планирование. Организация систем. - М.: Радио и связь, 1991.

119. Саати Т. Принятие решений: метод анализа иерархий. - М: Радио и связь, 1993.

120. Сабынин В.Н. Давайте говорить на одном языке // Системы безопасности. -№ 1. - 2001.

121. Сардак И.Г. Борьба с экономическими преступлениями выходит на новый уровень // Системы безопасности связи и телекоммуникаций. - № 3. - 1998.

122. Свиридов И.В. Информационная война: определения, подходы, взгляды // Безопасность информационных технологий. - № 4. - 1998. - С. 24-38.

123. Симонов С.В. Анализ рисков, управление рисками //Jet Info. - № 1. - 1999.

124. Симонов С.В. Аудит безопасности информационных систем //Jet Info. -№ 9. - 1999.

125. Симонов С.В. Методология анализа рисков в информационных системах // Конфидент. Защита информации. - № 1. - 2001. - С. 72-76.

126. Симонов С.В. Анализ рисков в информационных системах. Практические аспекты // Конфидент. Защита информации. - № 2. - 2001. - С. 48-53.

127. Симонов С.В. Технологии аудита информационной безопасности // Конфидент. Защита информации. - № 2. - 2002. — С. 36-41.

128. Симонов С.В. Технологии и инструментарий для управления рисками //Jet Info.-№ 1.-2003.

129. Спецификации сервисов базового уровня ИБ X/Open Baseline Security Services Specification (XBSS). C529 - X/Open company, 1996.

130. Староверов Д. Оценка угроз воздействия конкурента на ресурсы организации // Конфидент. Защита информации. - № 2. - 2000. - С. 58-62.

131. Староверов Д. Конфликты в сфере безопасности. Социально-психологические аспекты защиты // Системы безопасности связи и телекоммуникаций. -№ 6. - 1998.

132. Сырков Б. Компьютерная преступность в России. Современное состояние // Системы безопасности связи и телекоммуникаций. - № 4. - 1998.

133. Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. - Гостехкомиссия России, 1994.

134. Трахтенгерц Э.А. Компьютерная поддержка принятия решений. - М.: Синтег, 1998.

135. Трубачев А.П., Долинин М.Ю., Кобзарь М.Т., Сидак А.А., Сороковиков В.И. Оценка безопасности информационных технологий / Под общ. ред. В.А. Галатенко. - М.: Издательство СИП РИА, 2001.

136. Турская Е. VPN как средство неотложной помощи // Data Communications. -№ 11.-2000.-С. 31-33.

137. Турский А., Панов С. Защита информации при взаимодействии корпоративных сетей в Internet // Конфидент. Защита информации. - № 5. - 1998. -С. 38-43.

138. Устинов Г.Н., Алгулиев Р.М., Сердюк В.А. Автоматизация процесса восстановления работоспособности сетей передачи данных // Системы безопасности. - № 39. - 2001. - С. 78-81.

139. Шпак В.Ф. Методологические основы обеспечения информационной безопасности объекта // Конфидент. Защита информации. - № 1. - 2000. - С. 75-86.

140. Шпак В.Ф. Сборник методических материалов // Конфидент. Защита информации. - № 1. - 2001.

141. Ярочкин В.И., Халяпин Д.Б. Основы защиты информации. Служба безопасности предприятия. - М.: ИПКИР, 1993.

142. H. Abelson, R. Anderson, S.M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P.G. Neumann, R.L. Rivest, J.I. Schiller, and B. Schneier. The risks of key recovery, key escrow, and trusted third-party encryption. *World Wide Web Journal (Web Security: A Matter of Trust),* 2(3) 241-257, Summer 1997. This report was first distributed via the Internet on May 27, 1997.

143. H. Abelson, R. Anderson, S.M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P.G. Neumann, R.L. Rivest, J.I. Schiller, and B. Schneier. The risks of key recovery, key escrow, and trusted third-party encryption, http://www.cdt.org/ crypto/risks98/. June 1998. This is a reissue of the May 27, 1997 report, with a new preface evaluating what happened in the intervening year.

144. E. Amoroso. *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response.* Intrusion. Net Books, 1999.

145. T. Anderson and PA Lee. *Fault-Tolerance: Principles and Practice.* Prentice-Hall International, Englewood Cliffs, New Jersey, 1981.

146. Are you ready for a BS 7799 audit? DISC PD 3003, 1998.

147. A Arora and S.S. Kulkarni. Detectors and correctors: A theory of fault-tolerance components. In *Proceedings of the Eighteenth International Conference on Distributed Computing Systems.* IEEE Computer Society, May 1998.

148. Automated Information Systems Security Policy Manual, NIST, CIS HB 1400-14.

149. Bundesamt fur Sicherheit in der Informationstechnik. IT Baseline Protection Manual, 2001 (http://www.bsi.bund.deV

150. J. Bararello and W. Kasian. United States Army Commercial Off-The-Shelf (COTS) experience: The promises and realities. In *Proceedings of the NATO Conference on Commercial Off-The-Shelf Products in Defence Applications: The Ruthless Pursuit of COTS,* Brussels, Belgium, April 2000. NATO.

151. A Barnes, A Hollway, and P.G. Neumann. Survivable computer-communication systems: The problem and working group recommendations. VAL-CE-TR-92-22 (revision 1). Technical report, U.S. Army Research Laboratory, AMSRL-SL-E, White Sands Missile Range, NM 88002-5513, May 1993. For Official Use Only.

152. D.E. Bell and L.J. La Padula Secure computer systems: A mathematical model. Technical Report MTR-2547, Vol. II, Mitre Corporation, Bedford, Massachusetts, May 1973.

153. D.E. Bell and L.J. La Padula. Secure computer systems: A refinement of the mathematical model. Technical Report MTR-2547, Vol. III, Mitre Corporation, Bedford, Massachusetts, December 1973.

154. D.E. Bell and L.J. La Padula Secure computer systems: Mathematical foundations. Technical Report MTR-2547, Vol. I, Mitre Corporation, Bedford, Massachusetts, March 1973.

155. D.E. Bell and L.J. La Padula Secure computer systems: Mathematical foundations and model. Technical Report M74-244, The Mitre Corporation, Bedford, Massachusetts, May 1973.

156. D.E. Bell and L.J. La Padula. Secure computer system: Unified exposition and Multics interpretation. Technical Report ESD-TR-75-306, The Mitre Corporation, Bedford Massachusetts, March 1976.

157. S.M. Bellovin. *Verifiably Correct Code Generation Using Predicate Transformers.* PhD thesis, Department of Computer Science, University of North Carolina at Chapel Hill, December 1982. http://www.research.att.com/~smb/dissabstract.html.

158. L.A Benzinger, G.W. Dinolt, and M.G. Yatabe. Final report: A distributed system multiple security policy model. Technical report, Loral Western Development Laboratories, report WDL-TR00777, San Jose, California, October 1994.

159. P.L. Bernstein. Against the Gods: The Remarkable Story of Risk. New York: John Wiley&Sons Inc., 1996.

160. K.J. Biba Integrity considerations for secure computer systems. Technical Report MTR 3153, The Mitre Corporation, Bedford, Massachusetts, June 1975. Also available from USAF Electronic Systems Division, Bedford, Massachusetts, as ESD-TR-76-372, April 1977.

161. M. Blume. *Hierarchical Modularity and Intermodule Optimization.* PhD thesis, Computer Science Department, Princeton University, November 1997.

162. AD. Blumenstiel. Guidelines for National Airspace System electronic security. Technical report, U.S. Department of Transportation/RSPA/Volpe Centre, Cambridge, Massachusetts, 1987.

163. AD. Blumenstiel. Federal Aviation Administration computer security plans. Technical report, U.S. Department of Transportation/RSPA/Volpe Centre, produced by Science Resources Associates, Cambridge, Massachusetts, 1988.

164. AD. Blumenstiel. National Airspace System electronic security. Technical report, U.S. Department of Transportation/RSPA/Volpe Center, Cambridge, Massachusetts, 1988.

165. AD. Blumenstiel. Federal Aviation Administration AIS security accreditation guidelines. Technical report, National Institute on Standards and Technology, Gaithersburg, Maryland, 1990.

166. AD. Blumenstiel. Federal Aviation Administration AIS security accreditation application design. Technical report, U.S. Department of Transportation/RSPA/ Volpe Centre, Cambridge, Massachusetts, 1991.

167. AD. Blumenstiel. Federal Aviation Administration AIS security accreditation program instructions. Technical report, U.S. Department of Transportation/ RSPA/Volpe Centre, Cambridge, Massachusetts, 1992.

168. AD. Blumenstiel. Federal Aviation Administration sensitive application security accreditation guideline. Technical report, U.S. Department of Transportation/ RSPA/Volpe Centre, Cambridge, Massachusetts, 1992.

169. AD. Blumenstiel. Briefing on electronic security in the Communications, Navigation and Surveillance (CNS) environment. Technical report, U.S. Department of Transportation/RSPA/Volpe Centre, Cambridge, Massachusetts, 1994.

170. AD. Blumenstiel and J. Itz. National Airspace System Data Interchange Network electronic security. Technical report, U.S. Department of Transportation/RSPA/ Volpe Centre, Cambridge, Massachusetts, 1988.

171. AD. Blumenstiel and P.E. Manning. Advanced Automation System vulnerabilities to electronic attack. Technical report, U.S. Department of Transportation/RSPA/ Volpe Centre, Cambridge, Massachusetts, July 1986.

172. AD. Blumenstiel et al. Federal Aviation Administration report to Congress on air traffic control data and communications vulnerabilities and security. Technical report, U.S. Department of Transportation/RSPA/Volpe Centre, Cambridge, Massachusetts, 1993.

173. A Boswell. Specification and validation of a security policy model. *IEEE Transactions on Software Engineering*, 21(2) 63-69, February 1995. Special section on Formal Methods Europe '93.

174. J.P. Bowen and M.G. Hinchey. *High-Integrity System Specification and Design.* Springer Verlag, Berlin, 1999.

175. K.A Bradley, B. Mukherjee, R.A Olsson, and N. Puketza Detecting disruptive routers: A distributed network monitoring approach. In *Proceedings of the 1998 Symposium on Security and Privacy*, Oakland, California, May 1998. IEEE Computer Society.

176. EP. Brooks. *The Mythical Man-Month: Essays on Software Engineering.* Addison-Wesley, Reading, Massachusetts, Second edition, 1995.

177. Canadian Systems Security Centre, Communications Security Establishment, Government of Canada. *Canadian Trusted Computer Product Evaluation Criteria, Version 3.0e*, January 1993.

178. D.J. Carney. Quotations from Chairman David: A Little Red Book of truths to enlighten and guide on the long march toward the COTS revolution. Technical report, Carnegie-Mellon University Software Engineering Institute, Pittsburgh, Pennsylvania, 1998.

179. J.M. Carroll. Managing Risk: A Computer-Aided Strategy. Boston: Butterworth Publishers, 1984.

180. R. Charpentier and M. Salois. MaliCOTS: detecting malicious code in COTS software. In *Proceedings of the NATO Conference on Commercial Off-The-Shelf Products in Defence Applications: The Ruthless Pursuit of COTS*, Brussels, Belgium, April 2000. NATO.

181. D.D. Clark et al. *Computers at Risk: Safe Computing in the Information Age.* National Research Council, National Academy Press, 2101 Constitution Ave., Washington, D.C. 20418, 5 December 1990. Final report of the System Security Study Committee.

182. W.J. Clinton. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. Technical report, U.S. Government White Paper, 22 May 1998.

183. CobiT: Executive Summary. - ISACA 3rd Edition, 2000.

184. CobiT: Executive Summary. - ISACA 3rd Edition, 2000.

185. CobiT: Framework. - ISACA 3rd Edition, 2000.

186. CobiT: Control Objectives. - ISACA 3rd Edition, 2000.

187. Code of practice for Information security management. British Standard BS7799, 2001.

188. Code of practice for IT management. DISC PD 0005, 1998.

189. Code of practice for legal admissibility of information stored on electronic document management systems. DISC PD 0008, 1995.

190. Code of Professional Ethics for Information Systems Control Professionals. -ISACA Guidelines, 2000.

191. F. Cohen. Managing Network Security: Balancing Risk (http://all.net/journal/netsec/9812.html). December 1998.

192. E.W. Dijkstra *A Discipline of Programming.* Prentice-Hall, Englewood Cliffs, New Jersey, 1976.

193. S. Dolev. *Self-Stabilisation.* MIT Press, Cambridge, Massachusetts, 2000.

194. C.M. Ellison et al. SPKI certificate theory. Technical report, Internet Engineering Task Force, September 1999. http://www.ietf.org/rfc/rfc2693.txt.

195. E.A Feustel and T. Mayfield. The DGSA Unmet information security challenges for operating system designers. *Operating Systems Review,* 32(1) 3-22, January 1998.

196. General Accounting Office (GAO), Information Security Risk Assessment: Practices of Leading Organisations (http://www.gao.gov/monthlv.list/aug99/ aug991.htm).

197. I. Greenberg, P. Boucher, R. Clark, E.D. Jensen, T.F. Lunt, P.G. Neumann, and D. Wells. The multilevel secure real-time distributed operating system study. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California, June 1992. Issued as Rome Laboratory report RL-TR-93-101, Rome Laboratory C3AB, Griffiss AFB NY 13441-5700. Contact Emilie Siarkiewicz, Internet: SiarkiewiczE@CS.RL.AF.MIL, phone 315-330-3241. For Official Use Only.

198. Guide to BS 7799 auditing. DISC PD 3004, 1998.

199. Guide for developing security plans for information technology systems. — NIST Special Publication, 800-18, 2000.

200. Guide to the Code of practice for Information Security Management. DISC PD 0007, 1995.

201. S. Harris (Hardcover). CISSP All-in-One Exam Guide. McGraw-Hill Osborne Media; Book and CD-ROM edition (December 26, 2001). ISBN: 0072193530.

202. J.R. Heath, P.J. Kuekes, and R.S. Williams. A defect tolerant architecture for chemically assembled computers: The lessons of Teramac for the aspiring nanotechnologist. Technical report, UCLA 1997. http://neon.chem.ucla.edu/~schung/Hgrp/teramac.html.

203. H.M. Hinton. *Composable Safety and Progress Properties.* PhD thesis, University of Toronto, 1995.

204. C.M. Holloway, editor. *Third NASA Langley Formal Methods Workshop,* Hampton, Virginia, May 10-12 1995. NASA Langley Research Center. NASA Conference Publication 10176, June 1995.

205. G.J. Holzmann. *Design and Validation of Computer Protocols.* Prentice-Hall, Englewood Cliffs, New Jersey, 1991.

206. Information Technology Security (ITS). Minimum Baseline Protective Resuirements. http: //esdis.dsfo.nasa.gov/security/req/basereq/basereqlist.htm.

207. IEEE. Standard specifications for public key cryptography. Technical report, IEEE Standards Department, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, 2000 and ongoing. http://grouper.ieee.org/groups/1363/.

208. Information security management. Part 2. Specification for information security management systems. British Standard BS7799, Part 2, 2000.

209. Information technology - Code of practice for Information security management. International Standard ISO/IEC 17799:2000(E).

210. Information security management: an introduction. DISC PD 3000, 1998ISO/ IEC.

211. 15408-1. Information technology. Security techniques - Evaluation criteria for IT security, Part 1: Introduction and general model, 1999.

212. IS Auditing Guideline: Corporate Governance of Information Systems. - ISACA Guidelines, 2000.

213. IS Auditing Guideline: Planning the IS Audit. - ISACA Guidelines, 2000.

214. IS Auditing Guideline: Using the Work of Other Auditors and Experts. - ISACA Guidelines, 2000

215. ISO/IEC 15408-2: Information technology. Security techniques - Evaluation criteria for IT security, Part 2: Security functional requirements, 1999.

216. ISO/IEC 15408-3: Information technology. Security techniques - Evaluation criteria for IT security, Part 3: Security assurance requirements, 1999.

217. R. Jagannathan, T.F. Lunt, D. Anderson, C Dodd, F. Gilham, C Jalali, H.S. Javitz, P.G. Neumann, A. Tamaru, and A Valdes. System Design Document: Next-generation Intrusion-Detection Expert System (NIDES). Technical report, Computer Science Laboratory, SRI International, Menlo Park, California 9 March

1993.

218. S.Jantsch. Risks by using COTS products and commercial ICT services. In *Proceedings of the NATO Conference on Commercial Off-The -Shelf Products in Defence Applications: The Ruthless Pursuit of COTS,* Brussels, Belgium, April 2000. NATO.

219. R.Y. Kain and C.E. Landwehr. On access checking in capability-based systems. In *Proceedings of the 1986 IEEE Symposium on Security and Privacy,* April 1986.

220. Kaeo M. Designing Network Security. A practical guide to creating a secure network infrastructure. 98-84218. Cisco Press. Cisco Systems, Indianapolis, Indiana 46290 USA, 1999.

221. PA Karger. *Improving Security and Performance for Capability Systems.* PhD thesis, Computer Laboratory University of Cambridge, Cambridge, England, October 1988. Technical Report No. 149.

222. C. Ko. *Execution Monitoring of Security-Critical Programs in a Distributed System: A Specification-Based Approach.* PhD thesis, Computer Science Department, University of California at Davis, 1996.

223. P.C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA DSS, and other systems. In *Springer- Verlag, Berlin, Lecture Notes in Computer Science, Advances in Cryptology, Proceedings of Crypto '96,* pages 104 -113, Santa Barbara, California, August 1996.

224. L. Lamport, W.H. Kautz, P.G. Neumann, R.L. Schwartz, and P.M. Melliar-Smith. Formal techniques for fault tolerance in distributed data processing. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California April 1981. For Rome Air Development Centre.

225. C.E. Landwehr, AR. Bull, J.P. McDermott, and W.S. Choi. A taxonomy of computer program security flaws, with examples. Technical report, Centre for Secure Information Technology, Information Technology Division, Naval Research Laboratory, Washington, D.C., November 1993.

226. N.G. Leveson. Using COTS components in safety-critical systems. In *Proceedings of the NATO Conference on Commercial Off-The- Shelf Products in Defence Applications: The Ruthless Pursuit of COTS,* Brussels, Belgium, April 2000. NATO.

227. P.D. Lincoln and J.M. Rushby. Formally verified algorithms for diagnosis of manifest, symmetric, link, and Byzantine faults. Technical Report SRI-CSL-95-14, Computer Science Laboratory, SRI International, Menlo Park, California, October 1995.

228. U. Lindqvist and P.A Porras. Detecting computer and network misuse through the Production-Based Expert System Toolset (P-BEST). In *Proceedings of the 1999 Symposium on Security and Privacy,* Oakland, California, May 1999. IEEE Computer Society.

229. M. Lubaszewski and B. Courtois. A reliable fail-safe system. *IEEE Transactions on Computers,* C-47(2) 236-241, February 1998.

230. T.F. Lunt. Aggregation and inference: Facts and fallacies. In *Proceedings of the 1989 IEEE Symposium on Research in Security and Privacy,* May 1989.

231. T.F. Lunt, A Tamaru, F. Gilham, R. Jagannathan, C. Jalali, P.G. Neumann, H.S. Javitz, and A Valdes. A Real-Time Intrusion-Detection Expert System (IDES). Technical report, Computer Science Laboratory, SRI International, Menlo Park, California 28 February 1992.

232. T.F. Lunt and R.A Whitehurst. The SeaView formal top-level specifications and proofs. Final report, Computer Science Laboratory, SRI International, Menlo Park, California January/February 1989. Volumes 3A and 3B of «Secure Distributed Data Views», SRI Project 1143.

233. A.R Maneki. Algebraic properties of system composition in the Loral, Ulysses and McLean trace models. In *Proceedings of the 8th IEEE Computer Security Foundations Workshop,* Kenmore, County Kerry, Ireland, June 1995.

234. T. Marsh (ed.). Critical Foundations: Protecting America's Infrastructures. Technical report, President's Commission on Critical Infrastructure Protection, October 1997.

235. D. McCullough. Ulysses security properties modelling environment: The theory of security. Technical report, Odyssey Research Associates, Ithaca, New York, July 1988.

236. D. McCullough. A hook-up theorem for multilevel security. *IEEE Transactions on Software Engineering,* 16(6), June 1990.

237. G. McGraw and E.W. Felten./аш *Security: Hostile Applets, Holes, and Antidotes.* John Wiley and Sons, New York, 1997.

238. G. McGraw and E.W. Felten. *SecuringJava: Getting Down to Business with Mobile Code.* John Wiley and Sons, New York, 1999. This is the second edition of

239. P.M. Melliar-Smith and L.E. Moser. Surviving network partitioning. *Computer,* 31(3) 62-68, March 1998.

240. J. Meseguer. A logical theory of concurrent objects and its realisation in the Maude language. In *Research Directions on Concurrent Object-Oriented Programming.* MIT Press, Cambridge, Massachusetts, 1993.

241. J. Millen. 20 years of covert channel modelling and analysis. In *Proceedings of the*

1999 Symposium on Security and Privacy, pageS113-114, Oakland, California May 1999. IEEE Computer Society, http://www.csl.sri.com/~millen/paper/20yrcc.ps.

242. J. Millen. Efficient fault-tolerant certificate revocation. In *Seventh ACM Conference on Computer and Communications Security.* ACM SIGSAC, 2000. Submitted.

243. J.K. Millen. Survivability measure. Technical report, SRI International Computer Science Laboratory, Menlo Park, California, January 1999.

244. J.K. Millen. Survivability measure. Technical report, SRI International Computer Science Laboratory, Menlo Park, California, June 2000. http://www.csl.sri.com/ -millen/papers/measure.ps.

245. J.K. Millen and R. Wright. Certificate revocation the responsible way. In *Proceedings of a workshop on Computer Security, Dependability, and Assurance (CSDA '98): From Needs to Solutions workshop,* 1998. http://www.csl.sri.com/~millen/papers/needs.ps.

246. J.K. Millen and R. Wright. Reasoning about trust and insurance in a public-key infrastructure. In *Proceedings of the Computer Security Foundations Workshop,* Cambridge, England, July 2000. http://www.csl.sri.com/~millen/papers/insurance.ps.

247. Model Curricula for Information Systems Auditing at the Undergraduate and Graduate Level. - ISACA 2000.

248. R. Morris and K. Thompson. Password security: A case history. *Communications of the ACM,* 22(11) 594-597, November 1979.

249. R.T. Morris. Computer science technical report 117. Technical report, AT&T Bell Laboratories, Murray Hill, New Jersey, 25 February 1985.

250. L. Moser, P.M. Melliar-Smith, and R. Schwartz. Design verification of SIFT Contractor Report 4097, NASA Langley Research Centre, Hampton, VA, September 1987.

251. NASA Langley Research Centre. *Formal Methods Specification and Verification, Vol.1.* NASA, June 1995.

252. NASA Langley Research Centre. *Formal Methods Specification and Verification, Vol. II.* NASA Fall 1995.

253. NATO. *Proceedings of the NATO Conference on Commercial Off-The-Shelf Products in Defence Applications: The Ruthless Pursuit of COTS,* Brussels, Belgium, April 2000.

254. NCSC. *Trusted Network Interpretation Environments Guideline.* National Computer Security Centre, 1 August 1990. NCSC-TG-011 Version-1.

255. NCSC. *Trusted Network Interpretation (TNI).* National Computer Security Centre, 31 July 1987. NCSC-TG-005, Version-1, Red Book.

256. NCSC. *Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria (TDI).* National Computer Security Centre April 1991. NCSC-TG-021, Version-2, Lavender Book.

257. NCSC. *Department of Defense Trusted Computer System Evaluation Criteria (TCSEC).* National Computer Security Centre, December 1985. DOD-5200.28-STD, Orange Book.

258. NCSC. *Guidance for Applying the Trusted Computer System Evaluation Criteria in Specific Environments.* National Computer Security Centre, June 1985. CSC-STD-003-85, Yellow Book.

259. G.C. Necula *Compiling with Proofs.* PhD thesis, Computer Science Department, Carnegie-Mellon University, 1998.

260. P.G. Neumann. On hierarchical design of computer systems for critical applications. *IEEE Transactions on Software Engineering,* SE-12(9), September 1986. Reprinted in Rein Turn (ed.), Advances in Computer System Security, Vol. 3, Artech House, Dedham, Massachusetts, 1988.

261. P.G. Neumann. On the design of dependable computer systems for critical applications. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California October 1990. CSL Technical Report CSL-90-10.

262. P.G. Neumann. Can systems be trustworthy with software-implemented crypto? Technical report, Final Report, Project 6402, SRI International, Menlo Park, California October 1994. For Official Use Only, NOFORN.

263. P.G. Neumann. *Computer-Related Risks.* ACM Press, New York, and Addison-Wesley, Reading, Massachusetts, 1994. ISBN 0-201-55805-X.

264. P.G. Neumann. Architectures and formal representations for secure systems. Technical report, Final Report, Project 6401, SRI International, Menlo Park, California October 1995. CSL report 96-05.

265. P.G. Neumann. Illustrative risks to the public in the use of computer systems and related technology, index to RISKS cases. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California 2000. The most recent version is available on-line at ftp://ftp.csl.sri.com/pub/users/neumann/illustrative.ps, ftp://ftp.csl.sri.com/pub/users/neumann/illustrative.pdf. and in html form for browsing at http://www.csl.sri.com/neumann/illustrative.html.

266. P.G. Neumann, R.S. Boyer, R.J. Feiertag, K.N. Levitt, and L. Robinson. A Provably Secure Operating System: The system, its applications, and proofs. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California May 1980. 2nd ed., Report CSL-116.

267. P.G. Neumann, J. Goldberg, K.N. Levitt, and J.H. Wensley. A study of fault-tolerant computing. Final report for ARPA, AD 766 974, Stanford Research Institute, Menlo Park, CA July 1973.

268. P.G. Neumann and L. Lamport. Highly dependable distributed systems. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California June 1983. Final Report, Contract No. DAEA18-81-G-0062, for U.S. Army CECOM.

269. P.G. Neumann, N.E. Proctor, and T.F. Lunt. Preventing security misuse in distributed systems. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California June 1992.

270. P.G. Neumann. Practical Architectures for Survivable Systems and Networks (Phase-Two Final Report), Computer Science Laboratory, SRI International, Menlo Park, California June 2000.

271. D.B. Parker. *Fighting Computer Crime.* John Wiley & Sons, New York, 1998.

272. J. Paul. Bugs in the program. Technical report, Report by the Subcommittee on Investigations and Oversight of the Committee on Science, Space and Technology, U.S. House of Representatives, 1990.

273. R. Perlman. *Network Layer Protocols with Byzantine Robustness.* PhD thesis, MIT, Cambridge, Massachusetts, 1988.

274. S.A Petrenko. Audit information security // International Workshop. Information Management. Mathematical Models of business processes. School of Management, St. Petersburg State University, Russia, June 28-29, 2001, pp. 150-172.

275. H. Petroski. *To Engineer is Human: The Role of Failure in Successful Design.* St. Martin's Press, New York, 1985.

276. H. Petroski. *Design Paradigms: Case Histories of Error and Judgement in Engineering.* Cambridge University Press, Cambridge, England, 1994.

277. C.P. Pfleeger. *Security in Computing.* Prentice-Hall, Englewood Cliffs, New Jersey, 1996. Second edition.

278. S.L. Pfleeger. *Software Engineering: Theory and Practice.* Prentice-Hall, Englewood Cliffs, New Jersey, 1998.

279. P.A Porras. STAT: A State Transition Analysis Tool for intrusion detection. Master's thesis, Computer Science Department, University of California, Santa Barbara, July 1992.

280. P.A Porras and P.G. Neumann. EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances. In *Proceedings of the Nineteenth National Computer Security Conference,* pages 353-365, Baltimore, Maryland, 22-25 October 1997. NIST/NCSC.

281. P.A Porras and A Valdes. Live traffic analysis of TCP/IP gateways. In *Proceedings of the Symposium on Network and Distributed System Security.* Internet Society, March 1998.

282. D. Prasad. *Dependable Systems Integration Using the Theories of Measurement and Decision Analysis.* PhD thesis, Department of Computer Science, University of York, August 1998.

283. D. Prasad and J. McDermid. Dependability evaluation using a multi-criteria decision analysis procedure. In *To appear,* 1999.

284. Preparing for BS 7799 certification. DISC PD 3001, 1998.

285. Principles of good practice for information management. DISC PD 0010, 1995.

286. N.E. Proctor. The restricted access processor: An example of formal verification. In *Proceedings of the 1985 Symposium on Security and Privacy,* pages 49-55, Oakland, CA April 1985. IEEE Computer Society.

287. B. Randell. System design and structuring. *Computer Journal,* 29(4):300-306, 1986.

288. B. Randell and J.E. Dobson. Reliability and security issues in distributed computing systems. In *Proceedings of the Fifth Symposium on Reliability in Distributed Software and Database Systems,* Los Angeles, California, January 1986.

289. B. Randell, J.-C. Laprie, H. Kopetz, and B. Littlewood, editors. *Predictably Dependable Computing Systems.* Basic Research Series. Springer-Verlag, Berlin, 1995.

290. T.R.N. Rao. *Error-Control Coding for Computer Systems.* Prentice-Hall, Englewood Cliffs, New Jersey, 1989.

291. Risk Management Guide for Information Technology Systems, NIST, Special Publication 800-30.

292. Risk Matrix http://www.mitre.org/resources/centers/sepo/risk/risk_matrix.htlm

293. R. Rowlingson. The convergence of military and civil approaches to information security. In *Proceedings of the NATO Conference on Commercial Off-The-Shelf Products in Defence Applications: The Ruthless Pursuit of COTS,* Brussels, Belgium, April 2000. NATO.

294. M. Salois and R. Charpentier. Dynamic detection of malicious code in COTS software. In *Proceedings of the NATO Conference on Commercial Off-The-Shelf Products in Defence Applications: The Ruthless Pursuit of COTS,* Brussels, Belgium, April 2000. NATO.

295. C. Salter, O.S. Saydjari, B. Schneier, and J. Wallner. Toward a secure system engineering methodology. In *New Security Paradigms Workshop,* September 1998. http://www.counterpane.com/secure-methodology.html.

296. F.B. Schneider. Open source in security: Visiting the bizarre. In *Proceedings of the 2000 Symposium on Security and Privacy,* pageS126-127, Oakland, California, May 2000. IEEE Computer Society.

297. F.B. Schneider and M. Blumenthal, editor. *Trust in Cyberspace*. National Research Council, National Academy Press, 2101 Constitution Ave., Washington, D.C. 20418, 1998. Final report of the National Research Council Committee on Information Trustworthiness.

298. N. Schneidewind. The ruthless pursuit of the truth about COTS. In *Proceedings of the NATO Conference on Commercial Off-The-Shelf Products in Defence Applications: The Ruthless Pursuit of COTS,* Brussels, Belgium, April 2000. NATO.

299. B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C: Second Edition.* John Wiley & Sons, New York, 1996.

300. B. Schneier. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, New York, 2000.

301. M.D. Schroeder and J.H. Saltzer. A hardware architecture for implementing protection risks. *Communications of the ACM,* 15(3), March 1972.

302. Kevin J. Soo Hoo. How Much Is Enough? A Risk-Management Approach to Computer Security. Consortium for Research on Information Security and Policy (CRISP), School of Engineering, Stanford University, June 2000. Working Paper.

303. Standards for Information Systems Auditing. - ISACA Standards, 2000.

304. Standards for Information Systems Control Professionals. - ISACA Standards, 2000.

305. D.E. Stevenson. Validation and verification methodologies for large-scale simulations: There are no silver hammers, either. *IEEE Computational Science and Engineering,* 1998.

306. D.W.J. Stringer-Calvert. *Mechanical Verification of Compiler Correctness.* PhD thesis, Department of Computer Science, University of York, 1998.

307. K. Sullivan, J.C. Knight, X. Du, and S. Geist. Information survivability control systems. In *Proceedings of the 1999 International Conference on Software Engineering (ICSE),* 1999.

308. J.T. Trostle. Timing attacks against trusted path. *In Proceedings of the 1998 Symposium on Security and Privacy,* Oakland, California, May 1998. IEEE Computer Society.

309. UK-MoD. *Interim Defence Standard 00-55, The Procurement of Safety-Critical Software in Defence Equipment.* U.K. Ministry of Defence, 5 April 1991. DefStan 00-55; Part 1, Issue 1: Requirements; Part 2, Issue 1: Guidance.

310. UK-MoD. *Interim Defence Standard 00-56, Hazard Analysis and Safety Classification of the Computer and Programmable Electronic System Elements of Defence Equipment.* U.K. Ministry of Defence, 5 April 1991. DefStan 00-56.

311. US-Senate. *Security in Cyberspace.* U.S. Senate Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs, Hearings, S. Hrg. 104-701, June 1996. ISBN 0-16-053913-7.

312. M. Vidger and J. Dean. Maintaining COTS-based systems. In *Proceedings of the NATO Conference on Commercial Off-The-Shelf Products in Defence Applications: The Ruthless Pursuit of COTS,* Brussels, Belgium, April 2000. NATO.

313. J.M. Voas and G. McGraw. *Software Fault Injection: Inoculating Programs Against Errors.* John Wiley & Sons, New York, 1998.

314. D.S. Wallach. *A New Approach to Mobile Code Security.* PhD thesis, Computer Science Department, Princeton University, January 1999. http://www.cs.rice.edu/~dwallach/.

315. D.S. Wallach and E.W. Felten. Understanding Java stack inspection. In *Proceedings of the 1998 Symposium on Security and Privacy,* Oakland, California, May 1998. IEEE Computer Society.

316. W.H. Ware. Security controls for computer systems. Technical report, RAND report for the Defence Science Board, 1970. Now on-line at http://cryptome.org/ sccs.htm.

317. W.H. Ware. A retrospective of the criteria movement. In *Proceedings of the Eighteenth National Information Systems Security Conference,* pages 582-588, Baltimore, Maryland, 10-13 October 1995. NIST/NCSC.

318. J.H. Wensley et al. Design study of software-implemented fault-tolerance (SIFT) computer. NASA contractor report 3011, Computer Science Laboratory, SRI International, Menlo Park, California, June 1982.

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

320. R. Witty. The Role of the Chief Information Security Officer. Research Note, Gartner Research, Strategic Planning, SPA-13-2933, April 2001.

321. R. Witty, J. Dubiel, J. Girard, J. Graff, A. Hallawell, B. Hildreth, N. MacDonald, W. Malik, J. Pescatore, M. Reynolds, K. Russell, A Weintraub, V. Wheatman. The Price of Information Security. Gartner Research, Strategic Analysis Report, K-l1-6534, June 2001.

322. I. White. Wrapping the COTS dilemma In *Proceedings of the NATO Conference on Commercial Off-The-Shelf Products in Defence Applications: The Ruthless Pursuit of COTS,* Brussels, Belgium, April 2000. NATO.

323. C.C. Wood. Information Security Policies Made Easy [a book of 1000+ already-written policies provided in both hardcopy and CD-ROM], AND in it's 7th edition, 1999; Publisher: Pentasafe Security Technologies, Inc., Sausalito, CA USA ISBN#l-881585-06-9.

324. C.C. Wood. Best Practices in Internet Commerce Security [derived from a survey of Internet merchants, Internet service providers (ISPs), Internet commerce hosting firms, Internet Trusted Third Parties (TTPs), and Internet commerce software vendors], 1998; Publisher: Pentasafe Security Technologies, Inc., Sausalito, CA USA; ISBN#1-881585-05-0.

325. C.C. Wood. How to Handle Internet Electronic Commerce Security: Risks, Controls & Product Guide [a guide for the design and specification of Internet security measures], released in 1996; Publisher: Pentasafe Security Technologies, Inc., Sausalito, CA, USA ISBN#l-881585-03-4.

326. C.C. Wood Effective Information Security Management [a book of tools and techniques for dealing with information security problems], 1991; Publisher: Elsevier Advanced Technology, Oxford, England; ISBN#l-85617-070-5.

327. C.C. Wood. Computer Security: A Comprehensive Controls Checklist [a book detailing standard control practices — particularly useful for audits and reviews], 1987; Publisher: John Wiley & Sons, New York, NY, USA ISBN#0-471-84795-X.

Ресурсы Internet

328. http://www.bsi-global.com - Британский институт стандартов.

329. http://www.cert.org/ - Координационный центр CERT университета Карнеги-Меллона: бюллетени по вопросам сетевой безопасности, рекомендации.

330. http://www.securityfocus.com/ - портал: материалы по безопасности (общие и применительно к ОС Windows, Linux, Solaris); ссылки на программные средства и литературу; колонка новостей; подписка на Bugtraq и другие списки рассылки.

331. http://www.sans.org/ - институт SANS (System Administration, Networking, and Security): статьи по безопасности, бюллетени, новости, проекты.

332. http://xforce.iss.net/ - раздел сайта компании Internet Secure Systems: новости, база данных уязвимостей, руководства, ссылки.

333. http://www.packetfactory.net/ - сайт разработчиков библиотеки libnet, программ Nemesis и Pandora и другого инструментария.

334. http://www.garlic.com/~lynn/secure.htm - глоссарий по информационной безопасности.

335. http://www.insecure.org/ - сайт разработчиков сканера nmap; программы для злоумышленников, статьи по безопасности.

336. http://blacksun.box.sk/tutorials.html - статьи по различным аспектам сетевой безопасности и работы сетевых сервисов.

337. http://www.phrack.com/ - журнал Phrack.

338. http://www.cerias.purdue.edu/ - Центр информационной безопасности университета Пурду: архив программного обеспечения, публикации.

339. http://www.rootshell.com/ - программы для злоумышленников (этим термином мы обозначаем программы, именуемые по-английски *exploit*, то есть программы, использующие какую-либо уязвимость системы для выполнения атаки или для демонстрации возможности атаки), документация.

340. http://www.mitre.org/resources/centers/sepo/risk/risk_matrix.html - сайт Risk Matrix.

341. http:/Avww.iso_17799software.com - библиотека The ISO 17799 Service & Software Directory.

342. http://www.methodware.com - сайт компании MethodWare.

343. http://www.riskwatch.com - сайт компании Risk Watch.

344. http://krylov_lib_ru/maturity_man.html - частная библиотека.

345. http://www.bsi.bund.de/gshb/english/menue.htm - IT Baseline Protection Manual. Standard security safeguards.

346. http://www.bsi.bund.de/fehler/index.htm - сайт Германского института стандартов в области информационных технологий.

347. http://icat.nist.gov - база данных по уязвимостям института стандартов США (NIST).

348. http://www.pcorp.u-net.com/risk.htm - сайт компании C&A Systems Security Ltd, разработчика ПО для сертификации на требования ISO 17799 под названием «Кобра».

349. http://www.aexis.de/RA%20ToolPage.htm - RA Software Tool, демонстрационная версия метода.

350. http://www.insight.co.uk/cramm/index.htm - сайт компании «Инсайт консалтинг», распространяющей метод CRAMM.

Статьи, новости, документация

351. http://www.isacaru.

352. http://www.bcp.ru.

353. http://www.confident.ru.

354. http://www.infosec.ru.
355. http://www.jet.msk.su.
356. http://www.kpmg.ru.
357. http://www.ey.com/global/content.nsf/Russia_E/Home.
358. http://www.cisco.com/global/RU/win.
359. http://www.microsoft.com/rus.
360. http://www.void.ru.
361. http://www.hackzone.rii.
362. http://www.security.nnov.ru.
http://www.xakep.ru.