ВЫСШЕЕ ОБРАЗОВАНИЕ
серия основана в 1996 г.

Е.К. БАРАНОВА
А.В. БАБАШ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

УЧЕБНОЕ ПОСОБИЕ

Четвертое издание, переработанное и дополненное

Допущено Учебно-методическим объединением по образованию в области прикладной информатики в качестве учебного пособия для студентов, обучающихся по направлению «Прикладная информатика»

Москва
РИОР
ИНФРА-М

УДК 621.391(075.8)
ББК 32.81я73
Б24

ФЗ
№ 436-ФЗ
Издание не подлежит маркировке в соответствии с п. 1 ч. 4 ст. 11

Авторы:
Баранова Е.К. — доцент, Национальный исследовательский университет «Высшая школа экономики» (Москва);
Бабаш А.В. — д-р физ.-мат. наук, профессор, Национальный исследовательский университет «Высшая школа экономики» (Москва)

Рецензенты:
Баяндин Н.И. — доцент, кафедра прикладной информатики и информационной безопасности, Российский экономический университет им. Г.В. Плеханова;
Дмитриев М.Г. — д-р физ.-мат. наук, профессор, главный научный сотрудник, Федеральный исследовательский центр «Информатика и управление» РАН

Баранова Е.К., Бабаш А.В.

Б24 Информационная безопасность и защита информации : учеб. пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — М. : РИОР : ИНФРА-М, 2019. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6

ISBN 978-5-369-01761-6 (РИОР)
ISBN 978-5-16-013849-7 (ИНФРА-М, print)
ISBN 978-5-16-106532-7 (ИНФРА-М, online)

Учебное пособие посвящено рассмотрению базовых вопросов информационной безопасности и защиты информации и может быть рекомендовано бакалаврам и магистрам, изучающим курсы «Информационная безопасность» и «Управление информационной безопасностью», а также смежные с ними дисциплины.

Книга может быть также полезна аспирантам и специалистам, интересующимся вопросами защиты информации.

УДК 621.391(075.8)
ББК 32.81я73

ISBN 978-5-369-01761-6 (РИОР)
ISBN 978-5-16-013849-7 (ИНФРА-М, print)
ISBN 978-5-16-106532-7 (ИНФРА-М, online)

ПРЕДИСЛОВИЕ

В эпоху информационных технологий проблема обеспечения защиты информационных систем от внутренних и внешних воздействий приобретает первостепенное значение. От ее успешного решения зависит безопасность граждан и будущее страны. В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, прямо указывается: «Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации».

В России в последние годы принят ряд стандартов, регламентирующих деятельность в области информационной безопасности (ИБ), — это семейство ГОСТ Р ИСО/МЭК 27000, основанное и соответствующее семейству международных стандартов на системы управления информационной безопасностью ISO/IEC 27000. Эти стандарты определяют требования к системам управления информационной безопасностью, управлению рисками, метрики и измерения, а также являются руководством по их внедрению.

В связи с крупными изменениями в нормативно-правовой базе в области ИБ в четвертом издании книги авторы постарались учесть основные требования новых стандартов, поэтому перед вами фактически новое учебное пособие по информационной безопасности и защите информации, где рассматриваются проблемы уязвимости информации в современных информационных системах, анализируются и классифицируются угрозы безопасности информации, конкретизируются задачи систем ее обеспечения, дан обзор методов и технических приемов защиты информации. Основное внимание уделено многоуровневому подходу к обеспечению режима информационной безопасности, методам защиты от вредоносного программного обеспечения, защите информации в распределенных вычислительных сетях, организационно-правовому обеспечению безопасности информации. Излагаются методы анализа и оценки информационных рисков, угроз и уязвимостей системы, методы принятия решений в разработке си-

стемы информационной безопасности, а также перспективы создания изначально защищенных информационных технологий.

В первой главе книги рассматриваются нормативно-правовые основы обеспечения информационной безопасности с учетом основных положений семейства стандартов ГОСТ Р ИСО/МЭК 27000, существенное внимание уделено основополагающим нормативным документам, определяющим порядок использования различной информации, а также ответственность за связанные с этим нарушения. Кроме того, в этой главе изложены общие подходы к обеспечению информационной безопасности на административном уровне, раскрыто понятие политики безопасности, проанализированы основные угрозы информационной безопасности в контексте ее составляющих.

Во второй главе рассмотрена проблема защиты информационных систем от вредоносных программ. В соответствии с современной классификацией таких программ изложены основные способы противодействия проникновению вредоносных программ в компьютеры пользователей. Здесь же рассматриваются угрозы для мобильных устройств и способы противодействия этим угрозам.

Отдельная глава книги посвящена рассмотрению актуальных в настоящее время вопросов анализа и оценки информационных рисков, угроз и уязвимостей системы с учетом требований стандарта ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Рассматриваются методики и программный инструментарий для оценки рисков в сфере информационной безопасности, в частности процедура применения методологии анализа рисков OCTAVE в соответствии со стандартом ГОСТ Р ИСО/МЭК 27005-2010, а также приводятся примеры использования программного пакета методологии CORAS. Отдельный подраздел, включенный в четвертое издание книги, посвящен управлению инцидентами информационной безопасности, поскольку конечным результатом обеспечения ИБ является предотвращение или минимизация ущерба от вероятных угроз или инцидентов ИБ и, таким образом, получение выигрыша для всего бизнес-процесса организации. Здесь описываются особенности организации центра управления событиями информационной безопасности (Security Operations Center, SOC) и одно из наиболее популярных решений последних лет для контроля и выявления инцидентов — SIEM-система (Security Information and Event Management). В приложениях к этой главе рассматриваются примеры реализации методик по анализу рисков для организаций малого и среднего бизнеса.

С появлением сетевых информационных систем проблема обеспечения информационной безопасности стала приобретать новые черты, поскольку наряду с локальными угрозами, осуществляемыми в пределах одного узла, к сетевым информационным системам применим специфический вид угроз, обусловленных распределенностью сетевых и информационных ресурсов в пространстве. Это так называемые сетевые, или удаленные, угрозы. Они характеризуются, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого узла, и, во-вторых, тем, что атаке может подвергаться не конкретный узел, а информация, передаваемая по сетевым каналам. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по числу попыток, так и по успешности их реализации. Соответственно, обеспечение безопасности вычислительных сетей с позиции противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных вычислительных систем состоит в том, что, если в локальных вычислительных сетях наиболее часты угрозы конфиденциальности и целостности информации, то в территориально распределенных сетях на первое место выходит угроза нарушения доступности информации. Все эти вопросы рассмотрены в четвертой главе. Там же описаны наиболее значимые механизмы защиты вычислительных систем от несанкционированных воздействий как преднамеренного, так и непреднамеренного характера, такие как идентификация и аутентификация, регистрацияи аудит, межсетевое экранирование, VPN и др. Отдельное внимание уделено угрозам информационной безопасности и методам защиты в облачных сервисах.

Разработка и эксплуатация сложных информационных систем выявили проблемы, которые можно решить лишь на основании комплексной оценки и учета различных по своей природе факторов, разнородных связей и внешних условий. Все более важным в современных быстро изменяющихся условиях становится вопрос качественного и эффективного принятия решений в различных ситуациях, поэтому пятая глава книги посвящена рассмотрению методов принятия решений, которые могут быть рекомендованы при разработке систем информационной безопасности.

При подготовке четвертого издания книги авторы сочли необходимым дополнить главу, посвященную рассмотрению экономических аспектов эффективности систем защиты информации, поскольку очевидно, что ни один проект в современном мире не может быть принят к исполнению без экономического обоснования инвестиций в него.

Сложность задач экономического анализа практически во всех областях деятельности обусловлена тем, что многие ключевые параметры экономических моделей невозможно оценить с высокой степенью достоверности, поскольку они носят вероятностный характер. Особенно это касается информационной безопасности, где формализации поддаются далеко не все параметры, вероятностный характер носят не только потенциальные угрозы и уязвимости системы, но и стоимость ущерба от реализации этих угроз, и оценка риска может проводиться не на количественном, а на качественном уровне.

Книга может быть полезна бакалаврам и магистрам высших учебных заведений, изучающим курс «Информационная безопасность и защита информации», а также аспирантам и специалистам, интересующимся вопросами защиты информации.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Проблема обеспечения информационной безопасности

1.1.1. Определение понятия «информационная безопасность»

Информационная безопасность является одной из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств обработки информации.

«Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества. Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации»[1]. Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты общества информационного.

С понятием «информационная безопасность» в различных контекстах связаны различные определения. Так, в принятом в 1996 г. Законе РФ «Об участии в международном информационном обмене» информационная безопасность определялась как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. Подобное же определение дается и в Доктрине информационной безопасности Российской Федерации, где указывается, что информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

Оба эти определения рассматривают информационную безопасность в национальных масштабах и поэтому имеют очень широкое понятие.

[1] Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

Характерно, что применительно к различным сферам деятельности, так или иначе связанным с информацией, понятие «информационная безопасность» принимает более конкретные очертания. Так, например, в «Концепции информационной безопасности сетей связи общего пользования Российской Федерации» даны два определения этого понятия.

1. *Информационная безопасность* — это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности.

2. *Информационная безопасность* — свойство сетей связи общего пользования сохранять неизменными характеристики информационной безопасности в условиях возможных воздействий нарушителя.

Необходимо иметь в виду, что при рассмотрении проблемы информационной безопасности нарушитель необязательно является злоумышленником. Им может быть сотрудник, нарушивший режим информационной безопасности, или внешняя среда, например высокая температура может привести к сбоям в работе технических средств хранения информации и т.д.

Сформулируем следующее определение информационной безопасности.

Информационная безопасность — это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

Рассматривая информацию как товар, можно утверждать, что нанесение ущерба информации в целом приводит к материальным затратам. Например, раскрытие технологии изготовления оригинального продукта приведет к появлению аналогичного продукта, но от другого производителя и, как следствие, владелец технологии, а может быть и автор, потеряют часть рынка и т.д.

С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и т.д.), логично утверждать, что изменение ее может привести к катастрофическим последствиям в объекте управления — производстве, транспорте и др.

Именно поэтому при определении понятия «информационная безопасность» на первое место ставится защита информации от различных воздействий. А под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности.

Согласно ст. 16 Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: «Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации».

Решение проблемы информационной безопасности, как правило, начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Это обусловлено тем, что для разных категорий субъектов характер решаемых задач может существенно различаться. Например, задачи, решаемые администратором локальной сети по обеспечению информационной безопасности, в значительной степени отличаются от задач, решаемых пользователем на домашнем компьютере, не связанном сетью.

Исходя из этого можно сделать следующие важные выводы:

- задачи по обеспечению информационной безопасности для разных категорий субъектов могут существенно различаться;
- информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации — это принципиально более широкое понятие.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику конкретного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий — области, развивающейся беспрецедентно высокими темпами. В сфере информационной безопасности важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие, как минимум, адекватно реагировать на угрозы информационной безопасности или предвидеть новые угрозы и уметь им противостоять.

Иногда понятие «информационная безопасность» подменяется терминами «компьютерная безопасность» или «кибербезопасность».

В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры – только одна из составляющих информационных систем. Несмотря на это, в рамках данной книги основное внимание будет уделяться вопросам, связанным с обеспечением режима информационной безопасности применительно к вычислительным системам, в которых информация хранится, обрабатывается и передается с помощью компьютеров.

Согласно определению компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

1.1.2. Составляющие информационной безопасности

Как уже было отмечено ранее, информационная безопасность — многогранная область деятельности, в которой успех может принести только систематический, комплексный подход.

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трех задач, обеспечивающих:

1) доступность информации;
2) целостность информации;
3) конфиденциальность информации.

Именно доступность, целостность и конфиденциальность являются равнозначными составляющими информационной безопасности.

Доступность информации

Информационные системы создаются для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям невозможно, то это, очевидно, наносит ущерб всем пользователям.

Роль доступности информации особенно проявляется в разного рода системах управления — производством, транспортом и т.п. Менее драматичные, но также весьма неприятные последствия — и материальные, и моральные — может иметь длительная недоступность информационных услуг, которыми пользуется большое число людей, например, продажа железнодорожных и авиабилетов, банковские услуги, доступ в информационную сеть Интернет.

Доступность — это гарантия получения требуемой информации или информационной услуги пользователем за определенное время.

Фактор времени в определении доступности информации в ряде случаев является очень важным, поскольку некоторые виды информации и информационных услуг имеют смысл только в определенный промежуток времени. Например, получение заранее заказанного билета на самолет после его вылета теряет всякий смысл. Точно так же получение прогноза погоды на вчерашний день не имеет никакого смысла, поскольку это событие уже наступило. В этом контексте весьма уместна поговорка: «Дорога ложка к обеду».

Целостность информации

Целостность информации условно подразделяется на статическую и динамическую. Статическая целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации. Динамическая целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например, техническими, социальными.

Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно так же неточный перевод инструкции по применению лекарственного препарата чреват нанесением вреда здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

Целостность — гарантия того, что информация сейчас существует в ее исходном виде, т.е. при ее хранении или передаче не было осуществлено несанкционированных изменений.

Конфиденциальность информации

Конфиденциальность — самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с серьезными трудностями. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишены возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии, как основного средства обеспечения конфиденциальности, стоят многочисленные законодательные и технические проблемы.

Конфиденциальная информация есть практически во всех организациях. Это может быть технология производства, программный продукт, персональные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальными данными являются пароли для доступа к системе.

Конфиденциальность — гарантия доступности конкретной информации только тому кругу лиц, для кого она предназначена.

Нарушение каждой из трех рассмотренных категорий приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности — к фальсификации информации и, наконец, нарушение конфиденциальности — к раскрытию информации. Базовые составляющие информационной безопасности приведены на рис. 1.1.

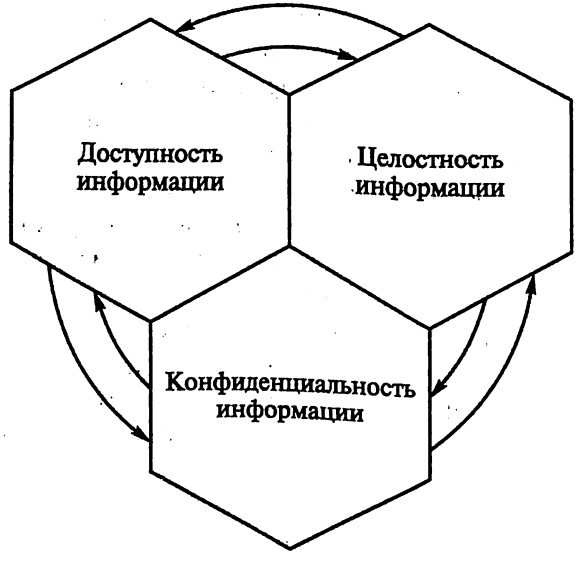


Рис. 1.1. Базовые составляющие информационной безопасности

Как уже отмечалось, выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности. Кроме того, нарушение одной из этих категорий может привести к нарушению или полной бесполезности двух других. Например, хищение пароля для доступа к компьютеру (нарушение конфиденциальности) может привести к его блокировке,

уничтожению данных (нарушение доступности информации) или фальсификации информации, содержащейся в памяти компьютера (нарушение целостности информации).

1.2. Уровни формирования режима информационной безопасности

1.2.1. Задачи информационной безопасности общества

Анализ основ информационной безопасности показал, что обеспечение режима информационной безопасности является задачей комплексной. С одной стороны, информационная безопасность предполагает, как минимум, обеспечение трех ее составляющих — доступность, целостность и конфиденциальность данных. И уже с учетом этого проблему информационной безопасности следует рассматривать комплексно. С другой стороны, информацией и информационными системами в буквальном смысле «пронизаны» все сферы общественной деятельности, и влияние информации на общество все нарастает, поэтому обеспечение информационной безопасности также требует комплексного подхода.

В этой связи закономерным является рассмотрение проблемы обеспечения информационной безопасности на нескольких уровнях, которые в совокупности обеспечивали бы защиту информации и информационных систем от вредных воздействий, наносящих ущерб субъектам информационных отношений.

Рассматривая проблему информационной безопасности в широком смысле, можно отметить, что в этом случае речь идет об информационной безопасности всего общества и его жизнедеятельности, при этом на информационную безопасность возлагается задача минимизации всех отрицательных последствий всеобщей информатизации и содействия развитию всего общества при использовании информации как ресурса его развития.

В этой связи основными задачами информационной безопасности в широком смысле являются:

- защита государственной тайны, т.е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;
- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
- защита прав предпринимателей при осуществлении ими коммерческой деятельности;

- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

Рассматривая проблему информационной безопасности в узком смысле, отметим, что в этом случае речь идет о совокупности методов и средств защиты информации и материальных носителей, направленных на обеспечение целостности, конфиденциальности и доступности информации.

Исходя из этого выделим следующие задачи информационной безопасности:

- защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;
- защита технических и программных средств информатизации от преднамеренных воздействий.

1.2.2. Уровни формирования режима информационной безопасности

С учетом изложенного выделим три уровня формирования режима информационной безопасности:

- законодательно-правовой;
- административный (организационный);
- программно-технический.

Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус. Кроме того, к этому уровню относятся стандарты и спецификации в области информационной безопасности. Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений. К этому уровню можно отнести и морально-этические нормы поведения, которые сложились традиционно или складываются по мере распространения вычислительных средств в обществе. Морально-этические нормы могут быть регламентированными в законодательном порядке, т.е. в виде свода правил и предписаний. Наиболее характерным примером таких норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ

США. Тем не менее, эти нормы большей частью не являются обязательными как законодательные меры.

Административный (организационный) уровень включает комплекс взаимосвязанных мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации. Организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Программно-технический уровень включает три подуровня: физический, технический (аппаратный) и программный. Физический подуровень решает задачи с ограничением физического доступа к информации и информационным системам, соответственно, к нему относятся технические средства, реализуемые в виде автономных устройств и систем, не связанных с обработкой, хранением и передачей информации: система охранной сигнализации, система наблюдения, средства физического воспрепятствования доступу (замки, ограждения, решетки и т.д.).

Средства защиты аппаратного и программного подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу. К аппаратным средствам относятся схемы контроля информации по четности, схемы доступа по ключу и т.д. К программным средствам защиты, образующим программный подуровень, относятся специальное программное обеспечение, используемое для защиты информации, например, антивирусный пакет. Программы защиты могут быть как отдельные, так и встроенные. Так для шифрования данных может использоваться Encrypting System (EFS) – система шифрования данных, реализующая шифрование на уровне файлов в операционных системах Microsoft Windows, или специальная программа шифрования.

Подчеркнем, что формирование режима информационной безопасности является сложной системной задачей, решение которой в разных странах специфично по содержанию и зависит от таких факторов, как научный потенциал страны, степень внедрения средств информатизации в жизнь общества и в экономику, развитие производственной базы, общей культуры общества и, наконец, традиций и норм поведения.

1.3. Нормативно-правовые основы информационной безопасности в РФ

1.3.1. Правовые основы информационной безопасности общества

Законодательные меры в сфере информационной безопасности направлены на создание в стране законодательной базы, упорядочивающей и регламентирующей поведение субъектов и объектов информационных отношений, а также определяющей ответственность за нарушение установленных норм.

Работа по созданию нормативной базы предусматривает разработку новых или корректировку существующих законов, положений, постановлений и инструкций, а также создание действенной системы контроля за исполнением указанных документов. Необходимо отметить, что такая работа в последнее время ведется практически непрерывно, поскольку сфера информационных технологий развивается стремительно, соответственно появляются новые формы информационных отношений, существование которых должно быть определено законодательно.

В Российской Федерации иерархия законодательной и нормативной правовой базы в области информационной безопасности может быть представлена следующим образом.

Акты федерального законодательства:

- Конституция РФ;
- Законы федерального уровня (включая федеральные конституционные законы, кодексы);
- Указы Президента РФ;
- Постановления правительства РФ;
- Нормативные правовые акты федеральных министерств и ведомств;
- Нормативные правовые акты субъектов РФ, органов местного самоуправления.

Нормативно-методические документы:

- Методические документы государственных органов России;
- Доктрина информационной безопасности РФ;
- Руководящие документы ФСТЭК (Гостехкомиссии России);
- Приказы ФСБ.

Стандарты информационной безопасности, из которых выделяют:

- Международные стандарты;
- Государственные (национальные) стандарты РФ;

- Рекомендации по стандартизации;
- Методические указания.

Основополагающими документами по информационной безопасности в Российской Федерации являются Конституция РФ и Доктрина информационной безопасности РФ.

В Конституции РФ гарантируется «тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» (ст. 23, ч. 2), а также «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (ст. 29, ч. 4). Кроме этого, Конституцией РФ «гарантируется свобода массовой информации» (ст. 29, ч. 5), т.е. массовая информация должна быть доступна гражданам.

Доктрина информационной безопасности РФ определяет важнейшие задачи обеспечения информационной безопасности РФ.

Доктрина информационной безопасности представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ и служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности РФ;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности РФ;
- разработки целевых программ обеспечения информационной безопасности РФ.

Доктрина информационной безопасности развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

1.3.2. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации

1. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» с изменениями и дополнениями, внесенными после его принятия, регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

В Законе определены следующие основные понятия:

- *государственная тайна* — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;
- *носители сведений, составляющих государственную тайну*, — материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов;
- *система защиты государственной тайны* — совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях;
- *доступ к сведениям, составляющим государственную тайну*, — санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;
- *гриф секретности* — реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;
- *средства защиты информации* — технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Законом определено, что средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Организация сертификации средств защиты информации возлагается на Федеральную службу по техническому и экспортному контролю (ФСТЭК), Федеральную службу безопасности (ФСБ) Российской Федерации, Министерство обороны (МО) Российской Федерации в соответствии с функциями, возложенными на них законодательством Российской Федерации.

2. Закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» является одним из базовых законов в области защиты информации,

который регламентирует отношения, возникающие при формировании и использовании информационных ресурсов Российской Федерации на основе сбора, накопления, хранения, распространения и предоставления потребителям документированной информации, а также при создании и использовании информационных технологий, при защите информации и прав субъектов, участвующих в информационных процессах и информатизации.

Этот закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

В соответствии с указанным законом ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе[1].

[1] Статья 9 Федерального закона РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Следует отметить, что процесс законотворчества идет достаточно сложно. Если в вопросах защиты государственной тайны создана более или менее надежная законодательная система, то в вопросах защиты служебной, коммерческой и частной информации существует достаточно много противоречий и «нестыковок».

При разработке и использовании законодательных и других правовых и нормативных документов, а также при организации защиты информации важно правильно ориентироваться во всем блоке действующей законодательной базы в этой области.

Проблемы, связанные с правильной трактовкой и применением законодательства Российской Федерации, периодически возникают в практической работе по организации защиты информации от ее утечки по техническим каналам, от несанкционированного доступа к информации и от воздействий на нее при обработке в технических средствах информатизации, а также в ходе контроля эффективности принимаемых мер защиты.

1.3.3. Ответственность за нарушения в сфере информационной безопасности

Немаловажная роль в системе правового регулирования информационных отношений отводится ответственности субъектов за нарушения в сфере информационной безопасности.

Основными документами в этом направлении являются:

- Уголовный кодекс Российской Федерации;
- Кодекс Российской Федерации об административных правонарушениях.

В принятом в 1996 г. *Уголовном кодексе* Российской Федерации как наиболее сильно действующем законодательном акте по предупреждению преступлений и привлечению преступников и нарушителей к уголовной ответственности, вопросам безопасности информации посвящены следующие главы и статьи:

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

Статья 140. Отказ в предоставлении гражданину информации.

Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Статья 237. Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей.

Статья 283. Разглашение государственной тайны.

Статья 284. Утрата документов, содержащих государственную тайну.

Особое внимание уделяется компьютерным преступлениям, ответственность за которые предусмотрена в специальной 28 главе кодекса «Преступления в сфере компьютерной информации». Глава 28 включает следующие статьи:

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, — наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, — наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо арестом на срок до шести месяцев, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, — наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, — наказываются лишением свободы на срок до семи лет.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предна-

значенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, — наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, — наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, — наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, — наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного

года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, — наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

1.4. Стандарты информационной безопасности

1.4.1. Требования безопасности к информационным системам

Стандарт ISO/IEC 15408 «*Критерии оценки безопасности информационных технологий*» (в последней редакции 2009 года) относится к оценочным стандартам. Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран. Он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. Именно поэтому данный стандарт очень часто называют «Общими критериями».

«*Общие критерии*» являются метастандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.

Как и «Оранжевая книга»[1], «Общие критерии» содержат два основных вида требований безопасности:

1) *функциональные требования* — соответствуют активному аспекту защиты: предъявляются к функциям безопасности и реализующим их механизмам;

2) *требования доверия* — соответствуют пассивному аспекту: предъявляются к технологии и процессу разработки и эксплуатации.

В отличие от «Оранжевой книги», «Общие критерии» не содержат предопределенных «классов безопасности». Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.

---

[1] Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации в области информационной безопасности во многих странах, стал стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем». Этот труд, называемый чаще всего по цвету обложки «Оранжевой книгой», был впервые опубликован в августе 1983 г.

Очень важно, что безопасность в «Общих критериях» рассматривается не статично, а в привязке к жизненному циклу объекта оценки.

Угрозы безопасности в стандарте характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

1.4.2. Принцип иерархии: класс – семейство – компонент – элемент

Для структуризации пространства требований в «Общих критериях» введена иерархия *класс – семейство – компонент – элемент*.

Классы определяют наиболее общую, «предметную» группировку требований (например, функциональные требования подотчетности).

Семейства в пределах класса различаются по строгости и другим тонкостям требований.

Компонент — минимальный набор требований, фигурирующий как целое.

Элемент — неделимое требование.

Между компонентами могут существовать зависимости, которые возникают, когда компонент сам по себе недостаточен для достижения цели безопасности.

Подобный принцип организации защиты напоминает принцип программирования с использованием библиотек, в которых содержатся стандартные (часто используемые) функции, из комбинаций которых формируется алгоритм решения.

«Общие критерии» позволяют с помощью подобных библиотек (компонент) формировать два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Функциональный пакет — это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового добавлением необходимых пакетов расширения, т.е. подобно тому как создаются производные классы в объектно-ориентированных языках программирования.

1.4.3. Функциональные требования

Все функциональные требования объединены в группы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в «Общих критериях» представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это гораздо больше, чем число аналогичных понятий в «Оранжевой книге». «Общие критерии» включают следующие классы *функциональных требований*:

- идентификация и аутентификация;
- защита данных пользователя;
- защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
- управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- доступ к объекту оценки;
- приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- использование ресурсов (требования к доступности информации);
- криптографическая поддержка (управление ключами);
- связь (аутентификация сторон, участвующих в обмене данными);
- доверенный маршрут/канал (для связи с сервисами безопасности).

Рассмотрим содержание одного из классов.

Класс функциональных требований «*Использование ресурсов*» включает три семейства.

1. *Отказоустойчивость*. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В стандарте различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя.

Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

2. *Обслуживание по приоритетам.* Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.
3. *Распределение ресурсов.* Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

Аналогично и другие классы включают наборы семейств требований, которые используются для их формулировки к системе безопасности.

«Общие критерии» — достаточно продуманный и полный документ в отношении функциональных требований, и именно на этот стандарт безопасности ориентируются соответствующие организации в нашей стране, и в первую очередь Федеральная служба по техническому и экспортному контролю (ФСТЭК).

1.4.4. Требования доверия

Вторая форма требований безопасности в «Общих критериях» — *требования доверия безопасности.*

Установление доверия безопасности основывается на активном исследовании объекта оценки.

Форма представления требований доверия та же, что и для функциональных требований (класс — семейство — компонент).

Всего в «Общих критериях» 10 классов, 44 семейства, 93 компонента требований доверия безопасности.

Классы требований доверия безопасности:

- разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
- поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
- тестирование;
- оценка уязвимостей (включая оценку стойкости функций безопасности);
- поставка и эксплуатация;
- управление конфигурацией;
- руководства (требования к эксплуатационной документации);

- поддержка доверия (для поддержки этапов жизненного цикла после сертификации);
- оценка профиля защиты;
- оценка задания по безопасности.

Применительно к требованиям доверия (для функциональных требований не предусмотрены) в «Общих критериях» введены оценочные уровни доверия (их 7), содержащие осмысленные комбинации компонентов.

Степень доверия возрастает от 1-го к 7-му уровню. Так, оценочный уровень доверия 1-го (начальный) применяется, когда угрозы не рассматриваются как серьезные, а оценочный уровень 7 применяется к ситуациям чрезвычайно высокого риска.

1.5. Стандарты информационной безопасности распределенных систем

1.5.1. Сервисы безопасности в вычислительных сетях

В последнее время с развитием вычислительных сетей и, в особенности, глобальной сети Интернет вопросы безопасности распределенных систем приобрели особую значимость. Важность этого вопроса косвенно подчеркивается появлением чуть позже «Оранжевой книги» стандарта, получившего название «Рекомендации X.800», который достаточно полно трактовал вопросы информационной безопасности распределенных систем, т.е. вычислительных сетей.

Рекомендации X.800 выделяют следующие сервисы (функции) безопасности и исполняемые ими роли.

Аутентификация. Этот сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. Аутентификация партнеров по общению используется при установлении соединения и периодически во время сеанса. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

Управление доступом. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

Конфиденциальность данных обеспечивает защиту от несанкционированного получения информации. Отдельно выделяется *конфиденциальность трафика* — это защита информации, которую можно получить, анализируя сетевые потоки данных.

Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры — с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки.

1.5.2. Механизмы безопасности

В X.800 определены следующие сетевые *механизмы безопасности*:

- шифрование;
- электронная подпись;
- механизм управления доступом;
- механизм контроля целостности данных;
- механизм аутентификации;
- механизм дополнения трафика;
- механизм управления маршрутизацией;
- механизм нотаризации (заверения).

Таблица 1.1 иллюстрирует механизмы (по отдельности или в комбинации с другими), которые могут использоваться для реализации той или иной функции. Так, например, «Конфиденциальность трафика» обеспечивается «Шифрованием», «Дополнением трафика» и «Управлением маршрутизацией».

1.5.3. Администрирование средств безопасности

В рекомендациях X.800 рассматривается понятие *администрирование средств безопасности*, которое включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Примером может служить распространение криптографических ключей.

Согласно рекомендациям X.800 усилия *администратора средств безопасности* должны распределяться по трем направлениям:

- администрирование информационной системы в целом;
- администрирование сервисов безопасности;
- администрирование механизмов безопасности.

Администрирование информационной системы в целом включает обеспечение актуальности политики безопасности, взаимодействие с другими административными службами, реагирование на происходящие события, аудит и безопасное восстановление.

Таблица 1.1

Взаимосвязь функций и механизмов безопасности

Функция	*Механизм*							
	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация партнеров	+	+	–	+	–	–	–	–
Аутентификация источника	+	+	–	–	–	–	–	–
Управление доступом	–	–	+	–	–	–	–	–
Конфиденциальность	+	–	+	–	–	–	+	–
Избирательная конфиденциальность	+	–	–	–	–	–	–	–
Конфиденциальность трафика	+	–	–	–	–	+	+	–
Целостность соединения	+	–	–	+	–	–	–	–
Целостность вне соединения	+	+	–	+	–	–	–	–
Неотказуемость	–	+	–	+	–	–	–	+

Администрирование сервисов безопасности предусматривает определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Администрирование механизмов безопасности включает:

- управление криптографическими ключами (генерация и распределение);
- управление шифрованием (установка и синхронизация криптографических параметров);

- администрирование управления доступом (распределение информации, необходимой для управления, — паролей, списков доступа и т.п.);
- управление аутентификацией (распределение информации, необходимой для аутентификации, — паролей, ключей и т.п.);
- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений — частоту отправки, размер и т.п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

В 1987 г. Национальным центром компьютерной безопасности США (англ. National Computer Security Center) была опубликована интерпретация «Оранжевой книги» для сетевых конфигураций. Этот документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

Интерпретация отличается от самой «Оранжевой книги» учетом динамичности сетевых конфигураций. В интерпретациях предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети.

Среди защитных механизмов в сетевых конфигурациях на первое место выдвигается *криптография*, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость реализации механизмов управления ключами.

В интерпретациях «Оранжевой книги» впервые систематически рассматривается вопрос обеспечения доступности информации.

Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

- внесение в конфигурацию той или иной формы избыточности (резервное оборудование, запасные каналы связи и т.п.);

- наличие средств реконфигурирования для изоляции и/или замены узлов либо коммуникационных каналов, отказавших или подвергшихся атаке на доступность;
- рассредоточенность сетевого управления, отсутствие единой точки отказа;
- наличие средств нейтрализации отказов (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);
- выделение подсетей и изоляция групп пользователей друг от друга.

1.6. Федеральная служба по техническому и экспортному контролю (ФСТЭК)

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю», *Федеральная служба по техническому и экспортному контролю* (ФСТЭК) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;

2) противодействия иностранным техническим разведкам на территории Российской Федерации;

3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;

4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

5) осуществления экспортного контроля.

Таким образом, в Российской Федерации информационная безопасность обеспечивается соблюдением указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов ФСТЭК (до 16 августа 2004 г. ФСТЭК носила название — Государственная техническая комиссия при Президенте РФ) и других нормативных документов.

В Российской Федерации в отношении стандартизации положений в сфере информационной безопасности первостепенное значение имеют руководящие документы Федеральной службы по техническому и экспортному контролю, одной из задач которой является «проведение единой государственной политики в области технической защиты информации».

ФСТЭК России является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну. ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею.

1.7. Административный уровень обеспечения информационной безопасности

1.7.1. Цели, задачи и содержание административного уровня

Административный уровень является промежуточным между законодательно-правовым и программно-техническим уровнями формирования режима информационной безопасности. Законы и стандарты в области информационной безопасности служат лишь отправным нормативным базисом информационной безопасности. Основой практического построения комплексной системы безопасности является административный уровень, определяющий главные направления работ по защите информационных систем.

Задача административного уровня — разработка и реализация практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем.

Кроме того, что немаловажно, именно на административном уровне определяются механизмы защиты, которые составляют третий уровень информационной безопасности — программно-технический.

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения в конкретных условиях функционирования информационной системы.

Содержанием административного уровня являются следующие мероприятия:

1) разработка политики безопасности;

2) проведение анализа угроз и расчета рисков;

3) выбор механизмов и средств обеспечения информационной безопасности.

1.7.2. Разработка политики информационной безопасности

Разработка политики безопасности ведется для конкретных условий функционирования информационной системы. Как правило, речь идет о политике безопасности организации, предприятия или учебного заведения. С учетом этого рассмотрим следующее определение политики безопасности.

Политика безопасности — это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме того, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Основные направления разработки политики безопасности:

- определение объема и требуемого уровня защиты данных;
- определение ролей субъектов информационных отношений.

В «Оранжевой книге» политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

Результатом разработки политики безопасности является комплексный документ, представляющий собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Этот документ выступает методологической основой практических мер по обеспечению информационной безопасности и включает следующие группы сведений:

- основные положения информационной безопасности организации;
- область применения политики безопасности;
- цели и задачи обеспечения информационной безопасности организации;
- распределение ролей и ответственности субъектов информационных отношений организации и их общие обязанности.

Основные положения определяют важность обеспечения информационной безопасности, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

При описании области применения политики безопасности перечисляются компоненты автоматизированной системы обработки, хранения и передачи информации, подлежащие защите.

В состав автоматизированной информационной системы входят следующие компоненты:

- *аппаратные средства* — компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства — дисководы, принтеры, контроллеры), кабели, линии связи и т.п.;
- *программное обеспечение* — приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;
- *данные* — хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
- *персонал* — обслуживающий персонал и пользователи.

Цели, задачи, критерии оценки информационной безопасности определяются функциональным назначением организации. Например, для режимных организаций на первое место ставится соблюдение конфиденциальности. Для сервисных информационных служб реального времени важным является обеспечение доступности подсистем. Для информационных хранилищ актуальным может быть обеспечение целостности данных.

Политика безопасности затрагивает всех субъектов информационных отношений в организации, поэтому на этапе разработки политики безопасности очень важно разграничить их права и обязанности, связанные с их непосредственной деятельностью.

С позиции обеспечения информационной безопасности разграничение прав и обязанностей целесообразно провести по следующим группам (ролям):

- специалист по информационной безопасности;
- владелец информации;
- поставщики аппаратного и программного обеспечения;
- менеджер отдела;
- операторы;
- аудиторы.

В зависимости от размеров организации, степени развитости ее информационной системы некоторые из перечисленных ролей могут отсутствовать вообще, а некоторые могут совмещаться одним и тем же физическим лицом.

Специалист по информационной безопасности (начальник службы безопасности, администратор по безопасности) играет основную роль в разработке и соблюдении политики безопасности предприятия. Он проводит расчет и перерасчет рисков, выявляет уязвимости системы безопасности по всем направлениям (аппаратные средства, программное обеспечение и т.д.).

Владелец информации — лицо, непосредственно владеющее информацией и работающее с ней. В большинстве случаев именно владелец информации может определить ее ценность и конфиденциальность.

Поставщики аппаратного и программного обеспечения обычно являются сторонними лицами, которые несут ответственность за поддержание должного уровня информационной безопасности в поставляемых им продуктах.

Администратор сети — лицо, занимающееся обеспечением функционирования информационной сети организации, поддержанием сетевых сервисов, разграничением прав доступа к ресурсам сети на основании соответствующей политики безопасности.

Менеджер отдела является промежуточным звеном между операторами и специалистами по информационной безопасности. Его задача — своевременно и качественно инструктировать подчиненный ему персонал обо всех требованиях службы безопасности и следить за их выполнением на рабочих местах. Менеджеры должны доводить до подчиненных все аспекты политики безопасности, которые непосредственно их касаются.

Операторы обрабатывают информацию, поэтому должны знать класс конфиденциальности информации и характер ущерба, который будет нанесен организации при ее раскрытии.

Аудиторы — внешние специалисты по безопасности, нанимаемые организацией для периодической проверки функционирования всей системы безопасности организации.

1.8. Классификация угроз информационной безопасности

1.8.1. Классы угроз информационной безопасности

Анализ и выявление угроз информационной безопасности является второй важной функцией административного уровня обеспечения информационной безопасности. Во многом облик разрабатываемой системы защиты и состав механизмов ее реализации определяется потенци-

альными угрозами, выявленными на этом этапе. Например, если пользователи вычислительной сети организации имеют доступ в Интернет, то количество угроз информационной безопасности резко возрастает, соответственно, это отражается на методах и средствах защиты.

Угроза информационной безопасности — это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются *злоумышленниками*.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем, например неконтролируемого доступа к персональным компьютерам или нелицензионного программного обеспечения (к сожалению, даже лицензионное программное обеспечение не лишено уязвимостей).

История развития информационных систем показывает, что новые уязвимые места возникают постоянно. С такой же регулярностью, но с небольшим отставанием появляются и средства защиты. В большинстве своем средства защиты есть реакция в ответ на выявленные угрозы, так, например, постоянно распространяются исправления к программному обеспечению фирмы Microsoft, устраняющие очередные его уязвимые места, и др. Такой подход к обеспечению безопасности малоэффективен, поскольку всегда имеет место промежуток времени между моментом выявления угрозы и ее устранением. Именно в этот период злоумышленник может нанести непоправимый вред информации.

Вследствие изложенного, более приемлем другой способ — упреждающая защита, предусматривающая разработку механизмов защиты от возможных, предполагаемых и потенциальных угроз.

Отметим, что некоторые угрозы нельзя считать следствием целенаправленных действий вредного характера. Существуют угрозы, вызванные случайными ошибками или техногенными явлениями.

Знание возможных угроз информационной безопасности, а также уязвимых мест системы защиты необходимо для того, чтобы выбрать наиболее экономичные и эффективные средства обеспечения безопасности.

Угрозы информационной безопасности классифицируются по нескольким признакам:

- *по составляющим информационной безопасности* (доступность, целостность, конфиденциальность), против которых в первую очередь направлены угрозы;
- *по компонентам информационных систем*, на которые угрозы нацелены (данные, программы, аппаратура, персонал);

- *по характеру воздействия* (случайные или преднамеренные, действия природного или техногенного характера);
- *по расположению источника угроз* (внутри или вне рассматриваемой информационной системы).

Отправной точкой при анализе угроз информационной безопасности является определение составляющей информационной безопасности, которая может быть нарушена той или иной угрозой: конфиденциальность, целостность или доступность.

На рис. 1.2 показано, что все виды угроз, классифицируемые по другим признакам, могут воздействовать на все составляющие информационной безопасности.

Рис. 1.2. Классификация угроз информационной безопасности

Рассмотрим угрозы по характеру воздействия.

Опыт проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы.

Причинами *случайных воздействий* при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания (природные и техногенные воздействия);
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия — это целенаправленные действия злоумышленника. В качестве злоумышленника могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами, например:

- недовольством служащего служебным положением;
- любопытством;
- конкурентной борьбой;
- уязвленным самолюбием и т.д.

Угрозы, классифицируемые по расположению их источника, бывают внутренними и внешними.

Внешние угрозы обусловлены применением вычислительных сетей и созданием на их основе информационных систем.

Основная особенность любой вычислительной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно — с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Особенность данного вида угроз заключается в том, что местоположение злоумышленника изначально неизвестно.

1.8.2. Каналы несанкционированного доступа к информации

Одним из наиболее распространенных и многообразных способов воздействия на информационную систему, позволяющих нанести ущерб любой из составляющих информационной безопасности, является *несанкционированный доступ* (НСД). Он возможен из-за ошибок в системе защиты, нерационального выбора средств защиты, их некорректной установки и настройки.

Каналы НСД классифицируются по компонентам автоматизированных информационных систем:

1) через человека:
   - хищение носителей информации;
   - чтение информации с экрана или клавиатуры;
   - чтение информации из распечатки;
2) через программу:
   - перехват паролей;
   - расшифровка зашифрованной информации;
   - копирование информации с носителя;
3) через аппаратуру:
   - подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
   - перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

1.8.3. Технические каналы утечки информации

Под *техническим каналом утечки информации* (ТКУИ) понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал. По сути, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте, причем под последней обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.

Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве побочные излучения, которые в той или иной степени связаны с обрабатываемой информацией. Физические явления, лежащие в основе появления этих излучений, имеют различный характер, тем не менее, они могут рассматриваться как непреднамеренная передача конфиденциальной информации по некоторым побочным каналам, образованным источником излучения, средой распространения и, возможно, приемной стороной (злоумышленником). Такие побочные каналы принято называть *техническим каналом утечки информации*.

Основными источниками образования технических каналов утечки любой, в том числе конфиденциальной, информации являются:

- преобразователи физических величин;
- излучатели электромагнитных колебаний;
- паразитные связи и наводки на провода и элементы электронных устройств.

Примером реализации системы преобразователей является звукоусилительная система, в которой микрофон (входной преобразователь)

превращает звук в электрический сигнал. Последний передается и усиливается усилителем низкой (звуковой) частоты (преобразователь по мощности), а затем поступает на громкоговоритель (выходной преобразователь), воспроизводящий звук, существенно более громкий, нежели тот, который воспринимается микрофоном.

Образованию каналов утечки информации способствуют определенные обстоятельства и причины технического характера, такие как несовершенство схемных решений (конструктивных и технологических), принятых для данной категории технических средств, эксплуатационный износ элементов изделия (изменение параметров элементов, аварийный выход/вывод из строя) и другие.

При выявлении технических каналов утечки информации применительно к средствам вычислительной техники необходимо рассматривать все оборудование как систему, включающую основное (стационарное) оборудование, например компьютеры, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными компьютерами и элементами вычислительной сети), распределительные и коммутационные устройства, системы электропитания, системы заземления.

В указанной системе следует различать устройства, непосредственно участвующие в обработке, хранении, передаче конфиденциальной информации, и устройства, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся совместно с основным оборудованием, обеспечивая его работу (система электропитании, заземление и т.д.) или условия для работы пользователей (система кондиционирования и т.д.).

В качестве потенциальных каналов утечки информации следует рассматривать элементы вспомогательного оборудования, имеющих выход за пределы контролируемой зоны, т.е. зоны, в пределах которой исключено несанкционированное пребывание посторонних лиц, например в пределах аудитории или отдельного здания.

Кроме соединительных линий основного и вспомогательного оборудования, за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются посторонними проводниками и тоже являются потенциальными каналами утечки информации.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов

перехвата, технические каналы утечки информации бывают электромагнитные, электрические и параметрические (рис. 1.3).

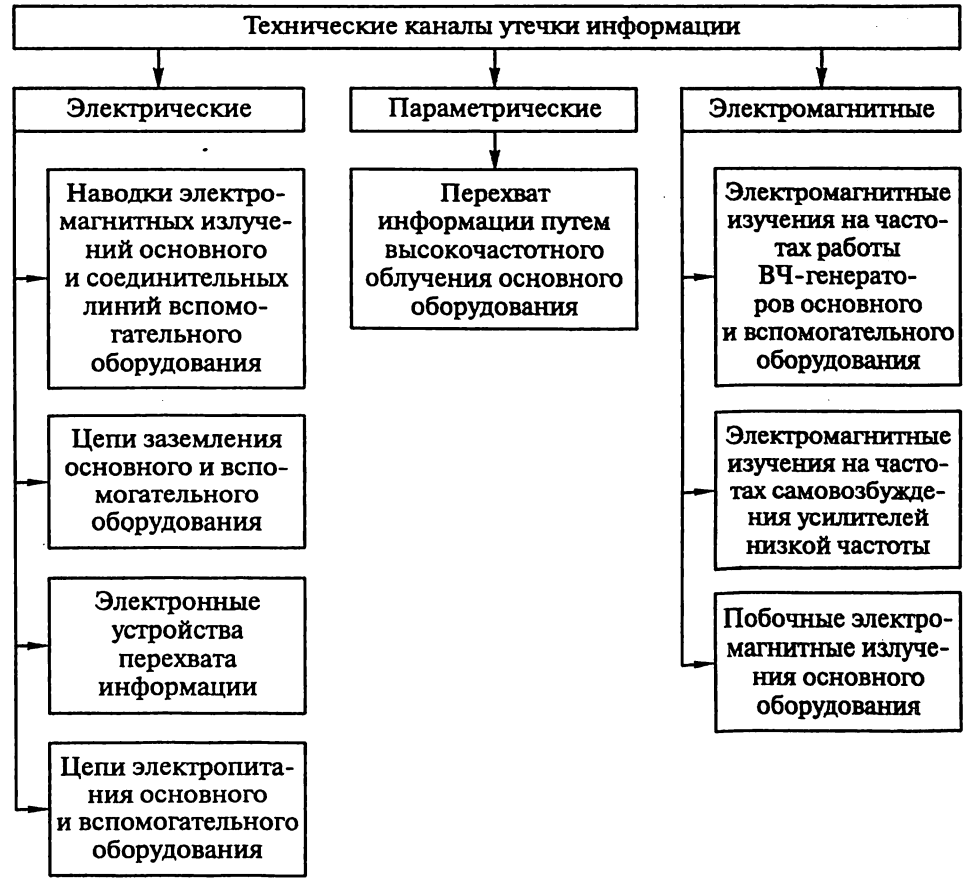


Рис. 1.3. Технические каналы утечки информации

Электромагнитные каналы утечки информации охватывают каналы утечки информации, возникающие за счет:

- различного вида побочных электромагнитных излучений (ПЭМИ) основного и вспомогательного оборудования;
- излучений на частотах работы высокочастотных (ВЧ) генераторов основного и вспомогательного оборудования;
- излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) основного оборудования.

Электромагнитные излучения элементов основного и вспомогательного оборудования. Носителем информации в технических средствах является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по токоведущим элементам основного и вспомогательного оборудования вокруг них (в окружающем пространстве) возникает электрическое и магнитное поле. В силу этого элементы основного и вспомогательного оборудования можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

Электромагнитные излучения на частотах работы ВЧ-генераторов основного и вспомогательного оборудования, в состав которого входят различного рода ВЧ-генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов и т.д.

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах ВЧ-генераторов наводятся электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т.д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных ВЧ-колебаний генераторов. Эти промодулированные ВЧ-колебания излучаются в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения УНЧ *основного и вспомогательного оборудования.* Самовозбуждение УНЧ основного и вспомогательного оборудования (например, усилителей систем звукоусиления и звукового сопровождения) возможно за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения лежит в пределах рабочих частот нелинейных элементов УНЧ (например, полупроводниковых приборов). Сигнал на частотах самовозбуждения, как правило, оказывается модулированным информационным сигналом. Самовозбуждение наблюдается в основном при переводе УНЧ в нелинейный режим работы, т.е. в режим перегрузки.

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными вне контролируемой зоны.

Электрические каналы утечки информации. Причинами возникновения электрических каналов утечки информации являются:

- наводки электромагнитных излучений основного оборудования на соединительные линии вспомогательного оборудования и посторонние проводники, выходящие за пределы контролируемой зоны;
- прохождение информационных сигналов в цепи электропитания основного и вспомогательного оборудования;
- прохождение информационных сигналов в цепи заземления основного и вспомогательного оборудования.

Наводки электромагнитных излучений возникают при излучении элементами основного и вспомогательного оборудования (в том числе и их соединительными линиями) информационных сигналов, а также при наличии гальванической связи соединительных линий основного оборудования и посторонних проводников или линий вспомогательного оборудования. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий основного оборудования и посторонних проводников.

Пространство вокруг основного оборудования, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется опасной зоной.

Случайной антенной в данном случае может стать цепь вспомогательного оборудования или посторонние проводники, способные принимать побочные электромагнитные излучения.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенная случайная антенна представляет собой компактное техническое средство, например телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д. К распределенным случайным антеннам относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

Прохождение информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя (например, УНЧ) и трансформатором выпрямительного устройства. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания. Информационный сигнал

может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Прохождение информационных сигналов в цепи заземления. Кроме заземляющих проводников, служащих для непосредственного соединения основного оборудования с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны подключения к соединительным линиям вспомогательного оборудования и посторонним проводникам, проходящим через помещения, где установлено основное оборудование, а также к его система электропитания и заземления. Для этих целей используются специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

Электронные устройства перехвата информации, устанавливаемые в основное оборудование, иногда называют аппаратными закладками. Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Наиболее часто закладки устанавливаются в основное оборудование иностранного производства.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а уже затем по команде передается на запросивший ее объект.

Параметрический канал утечки информации. Перехват обрабатываемой в технических средствах информации возможен также путем их «высокочастотного облучения». При взаимодействии облучающего электромагнитного поля с элементами основного оборудования происходит переизлучение электромагнитного поля. В ряде случаев это вторичное излучение модулируется информационным сигналом. При съеме информации для исключения взаимного влияния, облучающего и переизлученного сигналов, может использоваться их временная или частотная развязка. Например, для облучения основного оборудования могут использовать импульсные сигналы. При переизлучении параметры сигналов изменяются. Поэтому данный канал утечки информации часто называют параметрическим.

Для перехвата информации по данному каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности и специальные радиоприемные устройства.

1.9. Анализ угроз информационной безопасности

1.9.1. Наиболее распространенные угрозы нарушения доступности информации

Самыми частыми и самыми опасными (в отношении размера ущерба) являются *непреднамеренные ошибки* штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (обычные ошибки администрирования).

Самый эффективный способ борьбы с непреднамеренными случайными ошибками — максимальная автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам автоматизированной информационной системы, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;

- выход системы из штатного режима эксплуатации в силу случайных либо преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рассматриваются следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности.

Опасными являются и *стихийные бедствия* — пожары, наводнения, землетрясения, ураганы. По статистике, на долю этих источников угроз с учетом перебоев электропитания приходится 13 % потерь, понесенных информационными системами.

Угрозы доступности могут выглядеть грубо — как повреждение или даже разрушение оборудования (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего — грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов.

Одним из способов нарушения доступности является загрузка информационной системы (загрузка полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению источника такие угрозы подразделяется на *внутренние* и *внешние*. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Известны случаи вывода из строя сервисов глобальной сети Интернет, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание.

Одним из опаснейших способов нарушения доступности и в целом информационной безопасности является внедрение в атакуемые системы *вредоносного программного обеспечения*.

Целями такого программного обеспечения являются:

- внедрение другого вредоносного программного обеспечения;
- получение контроля над атакуемой системой;
- агрессивное потребление ресурсов;
- изменение или разрушение программ и/или данных.

К сожалению, количество «вредного» программного обеспечения постоянно увеличивается. Вирусы и троянские программы считают уже на десятки тысяч, а базы данных антивирусных программ обновляются практически ежедневно, несмотря на постоянно внедряемые методы «универсального» детектирования (т.е. детектирования не конкретных вариантов отдельно взятого вируса, а всего «семейства» или даже целого класса вредоносных программ).

Причины роста указанного вида угроз связаны с тем, что к компьютерам получают доступ всё большее и большее число кибер-хулиганов (по мере расширения глобальных информационных сетей). Какое-то число из них начинает самоутверждаться описанным способом.

Подробный анализ этого класса угроз и методы их предотвращения рассмотрены в отдельной главе.

1.9.2. Основные угрозы нарушения целостности информации

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят *кражи* и *подлоги*.

В большинстве случаев виновниками оказываются штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные, например, время создания или получения документа.

Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. С этой угрозой связано понятие «аутентичность», т.е. возможность подтверждения (доказательства) авторства того или иного документа или действия.

Потенциально уязвимы с позиции нарушения целостности не только данные, но и программы. Внедрение уже рассмотренного ранее вредоносного программного обеспечения — пример подобного нарушения.

Угрозами динамической целостности являются дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

1.9.3. Основные угрозы нарушения конфиденциальности информации

Конфиденциальную информацию условно можно разделить на *предметную* и *служебную*. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный, и вообще нетехнический, характер, например, при работе с несколькими информационными системами возникает необходимость запоминания нескольких паролей. В таких случаях чаще всего пользуются записными книжками, листками, которые зачастую находятся рядом с компьютером, и т.д. Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (зачастую — и не может быть обеспечена) необходимая защита. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным *перехват данных*. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна — получить доступ к данным в тот момент, когда они наименее защищены.

Перехват данных — очень серьезная угроза, и если конфиденциальность действительно критична, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например, на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных.

К неприятным угрозам, от которых трудно защищаться, можно отнести *злоупотребление полномочиями*. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример — нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Литература к главе 1

1. *Башлы П.Н.* Информационная безопасность: Учебник. — Ростов-на-Дону: Фолиант, 2005.
2. *Башлы П.Н., Бабаш А.В., Баранова Е.К.* Информационная безопасность. — М.: Изд. центр ЕАОИ, 2010.
3. *Галатенко В.А.* Основы информационной безопасности. — М.: Интернет-Университет Информационных Технологий — ИНТУИТ. РУ, 2003.
4. *Галатенко В.А.* Стандарты информационной безопасности. — М.: Интернет-Университет Информационных Технологий — ИНТУИТ. РУ, 2004.
5. *Завгородний В.И.* Комплексная защита в компьютерных системах: Учебное пособие. — М.: Логос; ПБОЮЛ Н.А.Егоров, 2001.
6. *Карпов Е.А., Котенко И.В., Котухов М.М.* и др. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под ред. И.В. Котенко. — СПб.: ВУС, 2000.
7. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. — М.: Горячая линия — Телеком, 2004 .
8. *Щербаков А.Ю.* Введение в теорию и практику компьютерной безопасности. — М.: Издательство Молгачева С.В., 2001.
9. Руководящие документы ФСТЭК и ГОСТы Российской Федерации по защите информации, а также другая литература по анализу требований к информационной безопасности, размещенные на сайте: http://fstec.ru/. Сборник нормативных документов по информационной безопасности.

ГЛАВА 2. ВРЕДОНОСНЫЕ ПРОГРАММЫ И ЗАЩИТА ОТ НИХ

2.1. Вредоносные программы как угроза информационной безопасности

2.1.1. Вредоносное программное обеспечение (ПО) и информационная безопасность

Вредоносные программы — одна из главных угроз информационной безопасности, что связано с масштабностью распространения этого явления и, как следствие, огромным ущербом, наносимым информационным системам.

Вредоносные программы создаются специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К указанной категории относятся вирусы и черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников.

Современное вредоносное ПО — это практически незаметный для обычного пользователя «враг», который постоянно совершенствуется, находя все новые и более изощренные способы проникновения на компьютеры пользователей. Необходимость борьбы с вредоносными программами обусловлена возможностью нарушения ими всех составляющих информационной безопасности.

Е. Касперский в своей книге «Компьютерное зловредство»[1] отмечает, что «Компьютерные вирусы, черви, троянские программы, спам, сетевые атаки и прочие нежелательные компьютерные явления давно перестали быть чем-то необычным, приводящим пользователя или системного администратора в шоковое состояние. Заражение вирусом или троянской программой — вполне частая ситуация как для тех, кто небрежно относится к элементарным правилам компьютерной гигиены, так и для профессиональных системных администраторов, отвечающих за бесперебойную работу корпоративных сетей. Обыденным также стал электронный спам, давно количественно перекрывший поток «легальных» писем».

[1] *Касперский Е.* Компьютерное зловредство. — СПб.: Питер, 2009.

2.1.2. Хронология развития вредоносных программ

Термин «*компьютерный вирус*» появился в середине 80-х гг. на одной из конференций по безопасности информации, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла. Согласно современной классификации Лаборатории Касперского в настоящее время используется более широкое понятие — «*вредоносные программы*», включающее компьютерные вирусы, сетевых червей, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников.

Трудность, возникающая при попытках сформулировать строгое определение вируса, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и др.) либо присущи другим программам, которые никакого отношения к вирусам не имеют, либо существуют вирусы, которые не содержат указанных отличительных черт (за исключением возможности распространения).

«*Программный вирус*» — это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах[1].

Невозможность четкой формулировки определения компьютерного вируса сама по себе не является проблемой. Главная проблема, которая следует из этого, заключается в том, что нет четких (однозначных) признаков, по которым можно отличить различные файлы от «вирусов», что не позволяет в полной мере устранить их влияние.

Несмотря на все усилия разработчиков антивирусного программного обеспечения, до сегодняшнего дня нет достаточно надежных антивирусных средств и, скорее всего, противостояние «вирусописателей» и их оппонентов будет постоянным.

Исходя из этого необходимо понимать, что нет достаточных программных и аппаратных средств защиты от вирусов, а надежная защита от вирусов может быть обеспечена комплексным применением этих средств и, что немаловажно, соблюдением элементарной «компьютерной гигиены».

Появление первых компьютерных вирусов, способных дописывать себя к файлам, связывают с инцидентом, который произошел в первой

[1] *Башлы П.Н.* Информационная безопасность: Учебник. — Ростов-на-Дону: Фолиант, 2005.

половине 70-х гг. на системе Univax 1108. Вирус, получивший название «Pervading Animal», дописывал себя к выполняемым файлам — делал практически то же самое, что тысячи современных компьютерных вирусов.

Можно отметить, что в те времена значимые события, связанные с компьютерными вирусами, происходили один раз в несколько лет. С началом 80-х компьютеры становятся все более и более популярными. Растет число программ, начинают развиваться глобальные сети. Результатом этого становится появление большого числа разнообразных «троянских коней» — программ, которые при их запуске наносят системе какой-либо вред. В 1986 г. произошла первая эпидемия IBM-PC-вируса «Brain». Вирус, заражающий 360 Кб дискеты, практически мгновенно разошелся по всему миру. Причиной такого «успеха» стала, скорее всего, неготовность компьютерного общества к встрече с таким явлением как компьютерный вирус.

В 1987 г. произошло событие, которое популяризировало «компьютерные вирусы». Код вируса «Vienna» впервые публикуется в книге Ральфа Бюргера «Computer Viruses: A High Tech Desease». Сразу же в 1987 г. появляются несколько вирусов для IBM-PC.

В пятницу 13 мая 1988 г. сразу несколько фирм и университетов ряда стран мира «познакомились» с вирусом «Jerusalem» — в этот день вирус уничтожал файлы при их запуске. Вместе с несколькими другими вирус «Jerusalem» распространился по тысячам компьютеров, оставаясь незамеченным — антивирусные программы еще не были распространены в то время так же широко, как сегодня, а многие пользователи и даже профессионалы еще не верили в существование компьютерных вирусов. Не прошло и полугода, как в ноябре повальная эпидемия сетевого вируса Морриса (другое название — Internet Worm) заразила более 6000 компьютерных систем в США и практически парализовала их работу. По причине ошибки в коде вируса он неограниченно рассылал свои копии по другим компьютерам сети и таким образом полностью забрал под себя ее ресурсы. Общие убытки от вируса Морриса были оценены в 96 млн долл. США.

В 1992 г. появились первые конструкторы вирусов VCL и PS-MPC, которые увеличили и без того немалый поток новых вирусов. В конце этого года первый вирус для Windows, заражающий выполняемые файлы этой операционной системы, открыл новую страницу компьютерных вирусов.

В дальнейшем развитие компьютерных вирусов напоминает сводку с полей сражений. Создатели вирусов становятся все более изощренными, число антивирусных программ растет, но ни одна из них не защищает в полной мере. В компьютерном обществе появляется синдром «компьютерного вируса».

К борьбе с вирусами подключаются правоохранительные органы: летом 1994 г. автор вируса SMEG был арестован. Примерно в то же самое время в той же Великобритании арестована целая группа вирусописателей, называвшая себя ARCV (Assotiation for Really Cruel Viruses). Некоторое время спустя еще один автор вирусов был арестован в Норвегии.

Август 1995 г. — один из поворотных моментов в истории вирусов и антивирусов: обнаружен первый вирус для Microsoft Word («Concept»). Так начиналось время макровирусов.

В 1998 г. появились первые полиморфные Windows32-вирусы — «Win95. HPS» и «Win95. Marburg». Разработчикам антивирусных программ пришлось спешно адаптировать к новым условиям методики детектирования полиморфных вирусов, рассчитанных до того только на DOS-вирусы.

Наиболее заметной в 1998 г. была эпидемия вируса «Win95. CIH», ставшая сначала массовой, затем глобальной, а затем повальной — сообщения о заражении компьютерных сетей и домашних персональных компьютеров исчислялись сотнями, если не тысячами. Начало эпидемии было зарегистрировано на Тайване, где неизвестный злоумышленник заслал зараженные файлы в местные интернет-конференции.

С середины 90-х гг. основным источником вирусов становится глобальная сеть Интернет.

С 1999 г. макровирусы начинают постепенно терять свое господство. Это связано со многими факторами. Во-первых, пользователи осознали опасность, таящуюся в простых doc- и xls-файлах. Люди стали более внимательными, научились пользоваться стандартными механизмами защиты от макровирусов, встроенными в MS Office.

В 2000 г. происходят очень важные изменения на мировой «вирусной арене». На свет появляется новый тип вредоносных программ — сетевые черви. А одновременно с ним — супервирус «Чернобыль». Это исполняемый вирус под Windows, имеющий ряд особенностей. Во-первых, зараженный файл не меняет своего размера по сравнению с первоначальным вариантом. Такой эффект достигается благодаря структуре исполняемых файлов Windows: каждый exe-файл разбит на секции, выровненные по строго определенным границам. В результате между секциями почти всегда образуется небольшой зазор. Хотя такая структура приводит к увеличению места, занимаемого файлом

на диске, она же позволяет существенно повысить скорость работы операционной системы с таким файлом. «Чернобыль» либо записывает свое тело в один такой зазор, либо дробит свой код на кусочки и копирует каждый из них в пустое место между границами. В результате антивирусу сложнее определить, заражен файл или нет, и еще сложнее вылечить инфицированный объект. Во-вторых, «Чернобыль» стал первопроходцем среди программ, умеющих «портить» аппаратные средства. Некоторые микросхемы позволяют перезаписывать данные, хранящиеся в их мини-ПЗУ. Этим и занимается данный вирус.

2000 г. еще можно назвать годом «Любовных Писем». Вирус «LoveLetter», обнаруженный 5 мая, мгновенно разлетелся по всему миру, поразив десятки миллионов компьютеров практически во всех уголках планеты. Причины этой глобальной эпидемии кроются в чрезвычайно высокой скорости распространения. Вирус немедленно после заражения системы рассылал свои копии по всем адресам электронной почты, найденным в адресной книге почтовой программы Microsoft Outlook. Подобно обнаруженному весной 1999 г. вирусу «Melissa», «LoveLetter» это делал, якобы, от имени владельца зараженного компьютера, о чем тот, естественно, даже не догадывался. Немаловажную роль при распространении вируса сыграл и психологический аспект: мало кто сможет удержаться, чтобы не прочитать любовное письмо от своего знакомого. Именно на это была сделана основная ставка в процессе разработки вируса. О масштабах заражения вирусами в начале XXI в. свидетельствует тот факт, что только в мае атаке вируса «LoveLetter» подверглись более 40 млн компьютеров. Уже за первые 5 дней эпидемии вирус нанес мировой экономике убытки в размере 6,7 млрд долл. США.

С 2000 г. сетевые черви начинают полностью преобладать на вирусной арене мира. Сегодня, по данным Лаборатории Касперского, на их долю приходится 89,1% всех заражений. В структуре распространенности сетевых червей традиционно преобладают почтовые, использующие e-mail в качестве основного транспорта для доставки на целевые компьютеры.

В 2001 г. был обнаружен новый тип вредоносных программ, способных активно распространяться и работать на зараженных компьютерах без использования файлов, — «бесфайловые черви». В процессе работы такие вирусы существуют исключительно в системной памяти, а при передаче на другие компьютеры — в виде специальных пакетов данных.

Такой поворот событий поставил сложные задачи перед разработчиками антивирусных пакетов. Традиционные технологии (антивирусный сканер и монитор) проявили неспособность эффективно противостоять новой угрозе, поскольку их алгоритм борьбы с вредоносными программами основан именно на перехвате файловых операций. Решением проблемы стал специальный антивирусный фильтр, который в фоновом режиме проверяет все поступающие на компьютер пакеты данных и удаляет «бесфайловых» червей. Глобальная эпидемия сетевого червя CodeRed, начавшаяся 20 июля 2001 г., подтвердила действенность технологии «бефайловых» червей. Но еще серьезнее оказалась эпидемия вируса «Helkern'» 25 января 2003 г.

В 2004 г. и в последующие 2005 и 2006 гг. «громких» инцидентов практически не происходило, но зато двукратно возросло число разнообразных троянских программ, которые распространялись самыми разными способами: через интернет-пейджеры, веб-сайты, при помощи сетевых червей или традиционной электронной почты. При этом возросла «популярность» именно сетевых непочтовых червей, которые проникают на компьютеры, используя различные дыры в программном обеспечении, например, черви Mytob и Zotob (Bozori), авторы которых были арестованы в августе 2005 г.

Продолжали появляться новые вирусы и троянские программы для мобильных платформ, особенно часто — для операционной системы Symbian. Помимо ставшего уже обычным метода заражения через Bluetooth-соединения, они использовали и принципиально новые методы. 10 января 2005 г.: Lasco — первый пример вируса, не только рассылавшего себя на другие телефоны, но и заражавшего исполняемые файлы Symbian. 4 марта 2005 г.: Comwar рассылает себя в MMS-сообщениях по контактам из адресной книги (аналогично первым компьютерным почтовым червям). 13 сентября 2005 г.: Cardtrap — троянская программа, пытавшаяся установить другие вредоносные файлы для Windows, т.е. попытка использовать кросс-платформенное заражение.

В 2005 г. происходят изменения и в антивирусной индустрии. Корпорация Microsoft активно готовится к выходу на антивирусный рынок и покупает сразу две антивирусные компании. 8 февраля 2005 г. объявляется о покупке компании Sybari, специализирующейся на технологиях защиты электронной почты для Microsoft Exchange, а 20 июля объявлено о покупке Front Bridge Technologies, разрабатывавшей технологии фильтрации сетевого трафика. Также в 2005 г. разворачивается скандал с очередной уязвимостью в приложениях Windows. На этот раз «дыра» была обнаружена в обработчике графического формата Windows Meta Files (WMF). Ситуация осложнилась тем, что информация об этой уязвимости была опубликована до выхода соответствую-

щего обновления Windows — пользователи оказались беззащитными перед сотнями троянских программ, которые тут же начали использовать эту «дыру» для проникновения в компьютеры.

Год 2006 характерен выходом корпорации Microsoft на антивирусный рынок. В ноябре 2006 г. появляется очередная версия ОС Microsoft Vista, которая позиционируется как система повышенной безопасности, но и в данном случае решить проблему защиты от вредоносных программ удалось лишь частично.

Червь Conficker, атаковавший компьютеры под управлением операционной системы Microsoft Windows, впервые был обнаружен в 2008 г. Это была самая крупномасштабная эпидемия со времен распространения вируса SQL Slammer 2003 г. Для проникновения в компьютер Conficker использовал некоторые уязвимости ОС Windows, а чтобы получить привилегии администратора, подбирал пароль администратора по словарю и связывал пораженные компьютеры в единую виртуальную сеть, готовую выполнять любые команды и задачи, поставленные создателем вируса.

Вредоносный червь WannaCry атаковал компьютеры по всему миру в мае 2017 г. Программа, проникая в операционную систему, блокировала все данные и требовала выкуп за расшифровку. Интересно, что авторы вымогателя требовали выкуп в биткоинах, которые невозможно отследить в системе по финансовым расчетам. На основе WannaCry уже созданы более совершенные приложения, которые сложно обнаружить и блокировать.

В июне 2017 г. сеть подверглась атаке нового вируса-вымогателя Petya, первые модификации которого были обнаружены еще в 2016 г. Как и WannaCry, вирус блокирует данные, а за расшифровку и доступ к компьютеру требует выкуп в биткоинах. Но новые модификации не только блокируют данные, но и поражают операционную систему запуска. Многие специалисты сходятся во мнении, что это приложение создано не с целью выкупа, а для нанесения крупномасштабного ущерба. Возможно, первые атаки в июне 2017 г. были пробными и за ними последуют более мощные атаки.

К сожалению, следует отметить, что этот экскурс может быть продолжен, так как год за годом мы становимся свидетелями увеличения не только числа вредоносных программ, но и разнообразия их применения. Поэтому заинтересованный читатель может обратиться к информации сайтов Лаборатории Касперского[1].

[1] https://securelist.ru.

2.1.3. Классификация вредоносного программного обеспечения

К вредоносному ПО относятся *сетевые черви*, *классические файловые вирусы*, *троянские программы*, *хакерские утилиты* и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам сети.

Сетевые черви представляют собой программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- проникновения на удаленные устройства (компьютеры, мобильные телефоны);
- запуска своей копии на удаленном устройстве;
- дальнейшего перехода на другие устройства в сети[1].

Путями распространения большинства известных червей являются:

- вложение в электронное письмо;
- ссылка в ICQ- и IRC-сообщениях на зараженный файл, расположенный на каком-либо веб- или FTP-ресурсе;
- файл в каталоге обмена P2P и пр.

Некоторые черви распространяются в виде сетевых пакетов и проникают непосредственно в память компьютера и там самостоятельно активизируют свой код — это так называемые «бесфайловые», или «пакетные» черви (например, CodeRed и Slammer).

Классические компьютерные вирусы — это программы, распространяющие свои копии по ресурсам локального компьютера с целью:

- последующего запуска своего кода при каких-либо действиях пользователя;
- дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевые сервисы для проникновения в другие компьютеры. Копия вируса попадает на удаленные компьютеры только в тех случаях, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

- при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
- вирус скопировал себя на съемный носитель или заразил файлы на нем;
- пользователь отослал электронное письмо с зараженным вложением.

[1] *Касперский Е.* Указ. соч.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например шпионскую процедуру или троянский компонент уничтожения информации на диске (например, вирус CIH).

Следует отметить, что в последнее время классические вирусы встречаются крайне редко. Однако заражение файлов вирусными методами периодически встречается в современных сетевых червях и троянских программах, написанных в криминальных целях. Такие черви и троянские программы при заражении компьютера внедряют свой код в файлы операционной системы и/или приложений для того, чтобы этот код было сложнее обнаружить и удалить из системы. В этих случаях используются технологии классических компьютерных вирусов.

Троянские программы — это вредоносные программы, созданные для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей. В отличие от вирусов и червей, представители данной категории не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения. Основным признаком, по которому различают типы троянских программ, являются их несанкционированные пользователем действия — те, которые они производят на зараженном компьютере.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособности зараженного компьютера: например, троянские программы, разработанные для массированных распределенных атак на удаленные ресурсы сети или для рассылки спама.

Хакерские утилиты и прочие вредоносные программы включают:

- утилиты, автоматизирующие создание вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносных программ;
- хакерские утилиты, скрывающие код зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному компьютеру или удаленным компьютерам сети.

Компьютерные вирусы, черви, троянские программы существуют для десятков операционных систем и приложений. В то же время имеется огромное число других операционных систем и приложений, для которых вредоносные программы пока не обнаружены. Что же является причиной существования вредных программ в одних системах и отсутствия их в других?

Причиной появления подобных программ, как указывают эксперты Лаборатории Касперского[1], в конкретной операционной системе или приложении является одновременное выполнение следующих условий:

- *популярность*, широкое распространение данной системы;
- *документированность* — наличие разнообразной и достаточно полной документации по системе;
- *незащищенность* системы или существование известных уязвимостей в ее безопасности и приложениях.

Каждое из перечисленных условий является необходимым, а выполнение всех условий одновременно служит достаточным для разнообразных вредоносных программ.

Условие популярности системы необходимо для того, чтобы она попалась на глаза хотя бы одному компьютерному хулигану или хакеру. Если система существует в единичных экземплярах, то вероятность ее злонамеренного использования близка к нулю. Если же производитель системы добился ее массового распространения, то очевидно, что раньше или позже хакеры и вирусописатели попытаются воспользоваться ей в своих интересах.

Напрашивается естественный вывод: чем популярнее операционная система или приложение, тем чаще она будет выступать жертвой вирусной атаки. Практика это подтверждает — распределение количества вредоносного программного обеспечения для Windows, Linux и MacOS практически совпадает с долями рынка, которые занимают эти операционные системы.

Наличие полной документации необходимо для существования вирусов по естественной причине: создание программ (включая вирусные) невозможно без технического описания использования сервисов операционной системы и правил написания приложений. Например, у обычных мобильных телефонов конца прошлого и начала нынешнего столетия подобная информация была закрыта — ни компании — производители программных продуктов, ни хакеры не имели возможности разрабатывать программы для данных устройств. У телефонов с под-

[1] https://securelist.ru

держкой Java и у «умных» телефонов есть документация по разработке приложений — и, как следствие, появляются и вредоносные программы, разработанные специально для телефонов данных типов.

Уязвимостями называют «дыры» в программном обеспечении, как программистские (ошибки в коде программы, позволяющие вирусу «пролезть в дыру» и захватить контроль над системой), так и логические (возможность проникновения в систему легальными, иногда даже документированными методами). Если в операционной системе или в ее приложениях существуют известные уязвимости, то такая система открыта для вирусов, какой бы защищенной она ни была.

Под защищенностью системы понимаются архитектурные решения, которые не позволяют новому (неизвестному) приложению получить полный или достаточно широкий доступ к файлам на диске (включая другие приложения) и потенциально опасным сервисам системы. Подобное ограничение фактически блокирует любую вирусную активность, но при этом, естественно, накладывает существенные ограничения на возможности обычных программ.

2.2. Антивирусные программы

2.2.1. Особенности работы антивирусных программ

Одним из наиболее эффективных способов борьбы с вредоносными программами является использование антивирусного ПО.

Антивирусная программа предназначена для поиска, обнаружения, классификации и удаления вредоносных программ.

Вместе с тем необходимо признать, что не существует антивирусов, гарантирующих стопроцентную защиту, поскольку на любой алгоритм антивируса всегда можно предложить новый алгоритм вируса, невидимого для этого антивируса.

При использовании антивирусных программ необходимо иметь представление об особенностях их работы.

- «*Ложное срабатывание*» — это детектирование вируса в незараженном объекте (файле, секторе или системной памяти).
- «*Пропуск вируса*» — недетектирование вируса в зараженном объекте.
- «*Сканирование по запросу*» — это поиск вирусов по запросу пользователя. В данном режиме антивирусная программа неактивна до тех пор, пока не будет вызвана пользователем из командной строки, командного файла или программы-расписания.
- «*Сканирование на лету*» — постоянная проверка на вирусы объектов, к которым происходит обращение (запуск, открытие, создание и т.п.). В этом режиме антивирус постоянно активен, он присутствует в памяти «резидентно» и проверяет объекты без запроса пользователя.

2.2.2. Методы защиты от вредоносных программ

Основной метод борьбы с вредоносными программами, как и в медицине, — своевременная профилактика. Компьютерная профилактика предполагает соблюдение правил «компьютерной гигиены», позволяющих значительно снизить вероятность заражения и потери каких-либо данных. Уяснение и строгое следование основным правилам поведения при использовании индивидуального компьютера и в сети является важным методом защиты от компьютерных злоумышленников. Всего есть три основных правила, которые верны как для индивидуальных, так и для корпоративных пользователей.

1. *Обязательное использование антивирусной защиты.* Если вы не являетесь экспертом в области компьютерной безопасности, то лучше воспользуйтесь надежной антивирусной защитой и защитой от сетевых атак (сетевой экран) — доверьте свою безопасность профессионалам. Большинство современных антивирусных программ защищают от самых разнообразных компьютерных угроз — от вирусов, червей, троянских программ и рекламных систем. Интегрированные решения по безопасности также ставят фильтр против спама, сетевых атак, посещения нежелательных и опасных интернет-ресурсов.

2. *Не следует доверять всей поступающей на компьютер информации* — электронным письмам, ссылкам на веб-сайты, сообщениям на интернет-пейджеры. Категорически не следует открывать файлы и ссылки, приходящие из неизвестного источника. Риск заражения снижается также при помощи организационных мер. К таким мерам относятся различные ограничения в работе пользователей, как индивидуальных, так и корпоративных, например:
   - запрет на использование интернет-пейджеров;
   - доступ только к ограниченному числу веб-страниц;
   - физическое отключение внутренней сети предприятия от Интернета и использование для выхода в Интернет выделенных компьютеров и т.д.

К сожалению, жесткие ограничительные меры могут конфликтовать с пожеланиями каждого конкретного пользователя или с бизнес-процессами предприятия. В таких случаях необходимо искать баланс, причем в каждом отдельно взятом случае этот баланс может быть различным.

3. *Следует обращать достаточно внимания* на информацию от антивирусных компаний и от экспертов по компьютерной безопасности. Обычно они своевременно сообщают о новых видах интернет-мошенничества, новых вирусных угрозах, эпидемиях и т.п. — уделяйте больше внимания подобной информации.

2.2.3. Факторы, определяющие качество антивирусных программ

Качество антивирусной программы определяется несколькими факторами; перечислим их по степени важности.

1. Надежность и удобство работы — отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки.
2. Качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц, упакованных и архивированных файлов. Отсутствие «ложных срабатываний». Возможность лечения зараженных объектов.
3. Существование версий антивируса под основные популярные платформы (DOS, Windows, Linux и т.д.).
4. Возможность сканирования «на лету».
5. Существование серверных версий с возможностью администрирования сети.
6. Скорость работы.

2.3. Угрозы для мобильных устройств

2.3.1. Классификация угроз для мобильных устройств

Популярность мобильных телефонов и смартфонов, все более активное их использование в рабочих целях, для доступа к Интернету, к банковскому счету, для оплаты товаров и услуг — все это приводит к появлению нового типа угроз и вредоносного ПО.

Классификация таких вредоносных программ практически идентична компьютерным «вредителям», в число которых входят:

- черви, распространяющиеся через специфические для смартфонов протоколы и сервисы;
- троянцы-вандалы, использующие ошибки Symbian для установки в систему;
- троянцы, ориентированные на нанесение финансового ущерба пользователю.

По данным экспертов Лаборатории Касперского[1] каталог вредоносных программ для мобильных телефонов насчитывает следующие шесть платформ, подверженных заражению (табл. 2.1).

Практически все современные мобильные телефоны и смартфоны, имеют поддержку Java и позволяют запускать Java-приложения, которые могут быть загружены из интернета. Освоив создание вредоносных Java-приложений, вирусописатели не только вырвались за пределы какой-то одной платформы, но и смогли значительно увеличить «зону поражения» — ведь под угрозой оказались не только пользователи смартфонов, но и практически каждый владелец обычного мобильного телефона.

Таблица 2.1

Каталог вредоносных программ для мобильных телефонов

Платформа	*Число семейств*	*Число модификаций*
Symbian	62	253
J2ME	31	182
WinCE	5	26
Python	3	45
SGold	3	4
MSIL	2	4

Что касается iPhone, в настоящее время это 4% мирового рынка мобильных телефонов и 20% американского, и Android — для этих платформ потенциальная возможность вредоносной атаки различна. Для iPhone заражение наиболее вероятно только в том случае, когда пользователь взломал свое устройство и устанавливает на него приложения из неофициальных источников. Android, по прогнозам, не будет иметь столь жесткой привязки к официальным источникам файлов, и пользователи «легальных» телефонов смогут ставить на свои устройства все что угодно.

Список вредоносных влияний для мобильных устройств достаточно широк и быстро пополняется; перечислим основные их них:

- распространение через Bluetooth, MMS;
- отправка SMS;
- заражение файлов;
- возможность удаленно управлять смартфоном;

[1] При написании этой главы использованы материалы сайта: https://securelist.ru.

- изменение или подмена иконок, системных приложений;
- установка «ложных» или некорректных шрифтов, приложений;
- борьба с антивирусами;
- блокирование работы карт памяти;
- кража информации;
- порча пользовательских данных;
- отключение систем защиты, встроенных в операционную систему;
- загрузка других файлов из Интернета;
- звонки на платные номера.

Рассмотрим перечень некоторых вредоносных программы для мобильных устройств.

Trojan-SMS

Лидером в этом перечне являются Trojan-SMS, чье вредонсное поведение сводится к отправке SMS на дорогие премиум-номера без ведома хозяев телефонов. Основная платформа существования Trojan-SMS — это Java 2 MicroEdition. SMS-троянцы, написанные для J2ME, опасны еще и тем, что они являются кроссплатформенными программами. В России использование Trojan-SMS было поставлено вирусописателями на поток. Самый популярный способ распространения таких вредоносных программ — через WAP-порталы, на которых посетителю предлагают загрузить различные мелодии, картинки, игры и приложения для мобильного телефона. Абсолютное большинство троянских программ маскируется либо под приложения, которые могут отправлять бесплатные SMS или предоставлять возможность использования бесплатного мобильного Интернета, либо под приложения эротического или порнографического характера.

Мобильные угрозы in-the-wild

Cabir и ComWar до недавнего времени — одни из наиболее распространенных мобильных угроз, каждая из которых была обнаружена более чем в тридцати странах мира . ComWar — это первый червь, распространяющийся через MMS. Как и Cabir, он способен рассылаться через Bluetooth, однако именно MMS является его основным способом размножения и, если учитывать его масштаб, наиболее опасным из всех возможных.

Однако повышенное внимание мобильных операторов к появившимся червям и внедрение средств антивирусной проверки MMS-трафика, позволили остановить распространение этих червей. Другими причинами исчезновения локальных эпидемий стало появление и распространение антивирусных продуктов для телефонов, новые средства защиты, реализованные в операционных системах (запуск только подписанных приложений) и постепенное исчезновение моделей телефонов, на которых Cabir и ComWar могли функционировать.

Worm.SymbOS.Beselo

Принцип действия червя, классифицированного как Worm.SymbOS.Beselo.a (чуть позже был обнаружен еще один вариант — Beselo.b), очень схож с ComWar и является классическим для червей такого типа. Распространение происходит через рассылку инфицированных SIS-файлов по MMS и через Bluetooth. После запуска на атакуемом устройстве червь начинает рассылать себя по адресной книге смартфона, а также на все доступные устройства в радиусе действия Bluetooth.

Skuller

Skuller представляет самое многочисленное семейство мобильных троянцев, поскольку это представитель самого примитивного из всех возможных symbian malware. Создать подобного троянца под силу любому человеку, умеющему пользоваться утилитой для создания sis-файлов. Все остальное сделают уязвимости Symbian: возможность перезаписи любых файлов, включая системные, и крайняя неустойчивость системы при ее столкновении с неожиданными (нестандартными для данного дистрибутива либо поврежденными) файлами. В основе большинства вариантов Skuller лежат два файла:

- файл с именем подменяемого приложения и расширением «aif» — это файл-иконка с изображением черепа (файл также содержит в себе текстовую строку «Skulls Skulls»);
- файл с именем подменяемого приложения и расширением «app» — это приложение EPOC, файл — «пустышка», который не содержит никакого функционала.

Важнейшим фактором распространения вредоносных программ на мобильных устройствах являются уязвимости в используемом программном обеспечении и в самих мобильных операционных системах. У злоумышленников существует всего два способа для проникновения в систему: человеческий фактор (социальная инженерия) и ошибки в программном обеспечении (уязвимости). В настоящее время для мобильных устройств следует рассматривать, как минимум, три основных источника уязвимостей: операционные системы Windows CE и Symbian; беспроводные протоколы (Bluetooth, WiFi, инфракрасные порты).

Мобильные угрозы продолжают распространяться по миру[1], однако в настоящее время вместо глобальных эпидемий червей наблюдаем локальные вспышки заражений, ориентированные на жителей одной конкретной страны или одного региона. По данным экспертов, регионами, для которых проблема мобильных вирусов является наиболее актуальной, являются Россия, Китай, Индонезия и страны Западной Европы.

2.3.2. Защита мобильных устройств

Мобильный телефон как маленький компьютер снабжен множеством механизмов связи с внешним миром, такими как Bluetooth, WiFi, GPRS, SMS, MMS и многое другое. Есть возможность передачи данных по кабелю или расширения памяти телефона с помощью карт памяти.

Основа безопасности мобильных устройств — это установка лицензионного программного обеспечения. Не следует устанавливать неподписанное ПО, но даже если оно подписано, то всегда нужно читать лицензионное соглашение. Антивирусная защита мобильного устройства важна не менее, чем защита компьютера.

Важнейшей частью антивируса является «сканер» — специальная программа, проверяющая все файлы один за другим на наличие в нем вируса. При анализе каждого файла осуществляется поиск вхождения сигнатуры — короткого, уникального для вируса участка кода. Если сигнатура не обнаруживается, то файл считается незараженным, а если сигнатура обнаруживается, то файл удаляется или отправляется в карантин.

Одного «сканера» для полноценной защиты мобильного телефона от вирусов недостаточно, так как «сканер» ищет уже зараженные файлы на мобильном телефоне и картах памяти, а многие вирусы наносят ощутимый вред при попадании на мобильный телефон. Для защиты телефона от инфицирования используется «монитор». Он анализирует данные по любым каналам связи, а у телефона их множество, и ищет в этих данных вирусы.

Передача данных по любому каналу связи осуществляется следующим образом. Сначала открывается соединение, затем происходит передача данных, после окончания передачи данных соединение разрывается, и полученные данные сохраняются в виде файла на мобильный телефон. Задачей «монитора» является проверка данных на присутствие в них вирусов перед их сохранением на телефон. Если вирус не найден, то данные сохраняются, а если вирус обнаружен, то данные удаляются.

Описанная проверка происходит в режиме «на лету», и со стороны ее заметить невозможно. Однако есть ситуации, когда нет возможности проверить данные в режиме «на лету». Например, при попадании новой карты памяти в телефон, нет возможности быстро проверить большие объемы памяти и единственный способ — проверить эти данные «сканером». Сочетание «сканера» и «монитора» обеспечивает комплексную защиту мобильного телефона от попадания вирусов.

Примером антивирусной защиты мобильного телефона может служить Kaspersky Internet Security для Android – мобильный антивирус для смартфонов и планшетов, обеспечивающий комплексную защиту от вредоносных приложений, спама, кражи и вредоносных веб-сайтов на мобильном устройстве.

[1] https://securelist.ru/ksb-threat-predictions-for-2018/88032.

Литература к главе 2

1. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. — М.: ДиаСофт, 2002.
2. *Касперский Е.* Компьютерное зловредство. — СПб.: Питер, 2009.
3. *Мельников В.В.* Безопасность информации в автоматизированных системах. — М.: Финансы и статистика, 2003.
4. *Хорев П.Б.* Методы и средства защиты информации в компьютерных системах. — М.: Академия, 2006.
5. Энциклопедия Securelist. URL:https://securelist.ru/encyclopedia/

ГЛАВА 3. АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННЫХ РИСКОВ, УГРОЗ И УЯЗВИМОСТЕЙ СИСТЕМЫ

3.1. Методики оценки рисков в сфере информационной безопасности

3.1.1. Общие понятия и терминология

В общем случае под риском понимают возможность наступления некоторого неблагоприятного события, влекущего за собой различного рода потери. Поскольку информация перестала быть просто необходимым для производства вспомогательным ресурсом или побочным проявлением всякого рода деятельности, а приобрела ощутимый стоимостной вес, который четко определяется реальной прибылью, получаемой при ее использовании, или размерами ущерба, с разной степенью вероятности наносимого владельцу информации в случае ее искажения или утраты, проблема обеспечения информационной безопасности приобрела в настоящее время исключительное значение.

Введем ряд понятий, используемых в сфере информационной безопасности и защиты информации, а также в современных методиках управления рисками ИБ.

В соответствии с ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» защита информации *(information security)* — это сохранение конфиденциальности, целостности и доступности информации; кроме того, также могут быть включены другие свойства, такие как аутентичность, подотчетность, неотрекаемость и надежность.

Важным этапом в сфере обеспечения информационной безопасности является процесс управления рисками ИБ. Процесс управления рисками представляет собой скоординированные действия по управлению и контролю организации в отношении риска. Управление рисками включает в себя оценку риска, обработку риска, принятие риска и сообщение о риске.

Цель процесса оценивания рисков состоит в определении характеристик рисков по отношению к информационной системе и ее ресурсам (активам). На основе полученных данных могут быть выбраны необходимые средства защиты. При оценивании рисков учитываются многие факторы: ценность ресурсов, оценки значимости угроз, уязвимостей, эффективность существующих и планируемых средств защиты и многое другое.

Угроза (*Threat*) — совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.

Уязвимость (*Vulnerability*) — слабость в системе защиты, которая делает возможным реализацию угрозы.

Анализ рисков (*Risk Analysis*) — процесс определения угроз, уязвимостей, возможного ущерба, а также контрмер.

Базовый уровень безопасности (*Baseline Security*) — обязательный минимальный уровень защищенности для информационных систем. В ряде стран существуют критерии для определения этого уровня. В качестве примера приведем критерии Великобритании — *CCTA Baseline Security Survey*, определяющие минимальные требования в области ИБ для государственных учреждений этой страны. В Германии эти критерии изложены в стандарте *BSI*. Существуют критерии ряда организаций — *NASA*, *X/Open*, *ISACA* и др. В нашей стране это может быть класс защищенности в соответствии с требованиями ФСТЭК России, профиль защиты, разработанный в соответствии со стандартом *ISO-15408*, или какой-либо другой набор требований. Тогда критерий достижения базового уровня безопасности — это выполнение заданного набора требований.

Базовый (Baseline) анализ рисков — 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 предъявляются повышенные требования в области ИБ.

Полный (*Full*) ***анализ рисков*** — анализ рисков для информационных систем, предъявляющих повышенные требования в области ИБ; включает в себя определение ценности информационных ресурсов, оценку угроз и уязвимостей, выбор адекватных контрмер, оценку их эффективности.

Риск информационной безопасности *(Information Security Risk)* — возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации (см. ГОСТ Р ИСО/МЭК 27005-2010. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»).

Количественная оценка риска (*Risk Estimation*) — процесс присвоения значений вероятности и последствий риска (см. ГОСТ Р ИСО/МЭК 27005-

2010. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»).

Управление рисками (*Risk Management*) — процесс определения контрмер в соответствии с оценкой рисков.

Система управления ИБ (*Information Security Management System*) — комплекс мер, направленных на обеспечение режима ИБ на всех стадиях жизненного цикла информационной системы (ИС).

Ресурсы (***активы***) — объекты, имеющие ценность для организации и оказывающие влияние на непрерывность осуществления деятельности. Все ресурсы должны быть идентифицированы и учтены, также должны быть определены владельцы ресурсов.

В *BS ISO/IEC 17799-2005* «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью» (в настоящее время в РФ используется новый стандарт: ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности») были выделяются следующие типы ресурсов (рис. 3.1):

Рис. 3.1. Типы ресурсов

- *информация*: базы данных и файлы данных, договоры и соглашения, системная документация, руководства пользователей, планы обеспечения непрерывности бизнеса, процедуры восстановления, журналы аудита и архивная информация;
- *программные ресурсы*: прикладное программное обеспечение, системное программное обеспечение, средства разработки и утилиты;
- *физические ресурсы*: компьютерное оборудование, коммуникационное оборудование, переносные носители и другое оборудование;
- *сервисы*: вычислительные и телекоммуникационные сервисы, основные коммунальные услуги, например отопление, освещение, электроэнергия и кондиционирование;
- *люди*, а также их квалификации, навыки и опыт;
- *нематериальные ресурсы*, такие как репутация и имидж организации.

На рис. 3.2 представлен процесс менеджмента риска информационной безопасности (ГОСТ Р ИСО/МЭК 27005-2010).

Менеджмент риска ИБ должен быть непрерывным процессом. В рамках данного процесса следует устанавливать контекст, оценивать и обрабатывать риски, используя для реализации рекомендации и решения плана обработки рисков. До принятия решения о том, что и когда должно быть сделано для снижения риска до приемлемого уровня, в рамках менеджмента риска анализируется, что может произойти и какими могут быть возможные последствия.

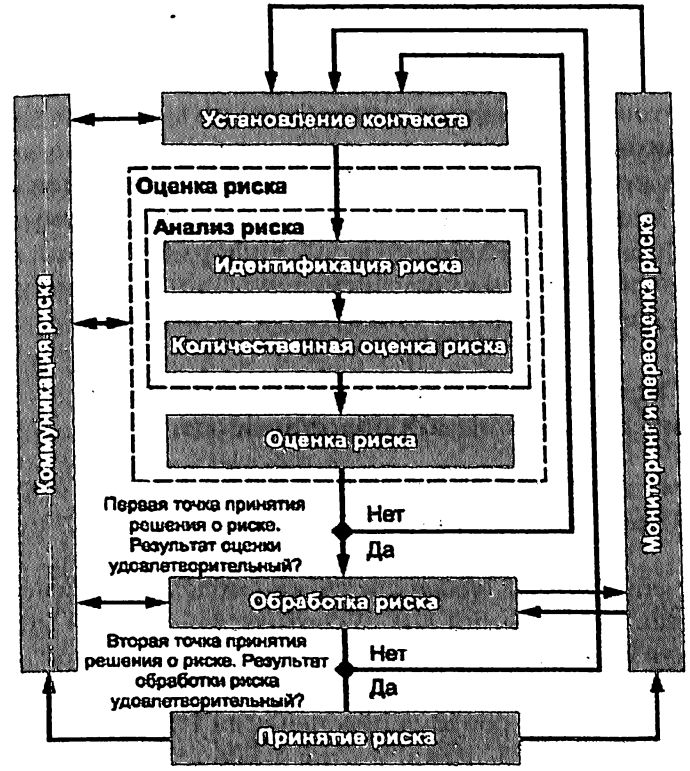


Рис. 3.2. Процесс менеджмента риска информационной безопасности (ГОСТ Р ИСО/МЭК 27005-2010)

Менеджмент риска ИБ должен способствовать:

- идентификации рисков;
- оценке рисков, исходя из последствий их реализации для бизнеса и вероятности их возникновения;
- осознанию и информированию о вероятности и последствиях рисков;

- установлению приоритетов в рамках обработки рисков;
- установлению приоритетов мероприятий по снижению имеющих место рисков;
- привлечению причастных сторон к принятию решений о менеджменте риска и поддержанию их информированности о состоянии менеджмента риска;
- эффективности проводимого мониторинга обработки рисков;
- проведению регулярного мониторинга и пересмотра процесса менеджмента риска;
- сбору информации для совершенствования менеджмента риска;
- подготовке менеджеров и персонала по вопросам рисков и необходимых действий, предпринимаемых для их уменьшения.

Процесс менеджмента риска ИБ может быть применен ко всей организации, к любой отдельной части организации (например, подразделению, филиалу, службе), к любой информационной системе, к имеющимся, планируемым или специфическим аспектам управления (например, к планированию непрерывности бизнеса)[1].

3.1.2. Описание процесса оценки рисков информационной безопасности

Основным фактором, от которого зависит отношение организации к вопросам информационной безопасности, является степень ее зрелости.

Университет *Carnegie Mellon* предложил модель определения зрелости организации с позиции ИБ. В соответствии с этой моделью выделяется пять уровней зрелости, которым можно поставить в соответствие различное понимание проблем ИБ в организации.

На первом уровне проблема обеспечения ИБ руководством формально не выдвигается. С точки зрения руководства организации, находящейся на первом уровне зрелости, задачи обеспечения режима ИБ неактуальны.

На втором уровне проблема обеспечения ИБ решается неформально, существуют стихийно сложившиеся процедуры обеспечения ИБ, их полнота и эффективность не анализируются. На уровне руководства существует определенное понимание задач обеспечения ИБ.

[1] ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

На третьем уровне руководство организации осознает задачи в области ИБ и заинтересовано в использовании стандартов в области ИБ. В организации принято следовать в той или иной мере стандартам и рекомендациям, обеспечивающим базовый уровень ИБ.

На четвертом уровне для руководства организации актуальны вопросы измерения параметров, характеризующих режим ИБ. В организации имеется полный комплект документов в области ИБ, действующие инструкции соблюдаются. Регулярно проводится внутренний аудит в области ИБ.

На пятом уровне ставятся и решаются различные варианты оптимизационных задач в области обеспечения режима ИБ[1].

Используя модель зрелости, руководство может определить:

- текущее положение организации;
- средний показатель для отрасли;
- цель организации.

Для простоты интерпретации результатов далее (рис. 3.3) приведено графическое изображение модели зрелости[2].

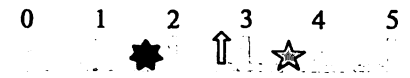


Рис. 3.3. Графическое изображение модели зрелости: ✸ — текущее положение организации; ⇧ — средний показатель для отрасли; ☆ — цель организации

По данным исследований большинство российских компаний находятся ниже третьего уровня зрелости[3]. Однако наблюдается стремление к повышению уровня зрелости с позиции ИБ. Инструментом, позволяющим принимать эффективные решения по минимизации последствий нарушения безопасности информации и вероятности их наступления, а также выбору защитных мер, является управление рисками.

В процессе оценки риска устанавливается ценность информационных активов, выявляются потенциальные угрозы и уязвимости, которые существуют или могут существовать, определяются существующие меры, средства контроля и управления, а также их воздействие на идентифицированные риски, определяются возможные последствия и, наконец, назначаются приоритеты установленным рискам, а также осу-

[1] *Петренко С.А., Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. — М.: ДМК Пресс, 2005.

[2] COBIT 4.1 Российское издание. — М.: Аудит и контроль информационных систем, 2008.

[3] *Петренко С.А., Симонов С.В.* Указ. соч.

ществляется их ранжирование по критериям оценки риска, зафиксированным при установлении контекста.

Оценка риска часто проводится за две или более итерации. Сначала проводится высокоуровневая оценка для идентификации потенциально высоких рисков, служащих основанием для дальнейшей оценки. Следующая итерация может включать дальнейшее углубленное рассмотрение потенциально высоких рисков. В тех случаях, когда полученная информация недостаточна для оценки риска, проводится более детальный анализ, возможно, по отдельным частям сферы действия или с использованием иного метода.

Выбор подхода к оценке риска в зависимости от задач и целей оценки риска осуществляет руководство организации[1].

На рис. 3.4 схематично изображен процесс оценки рисков ИБ.

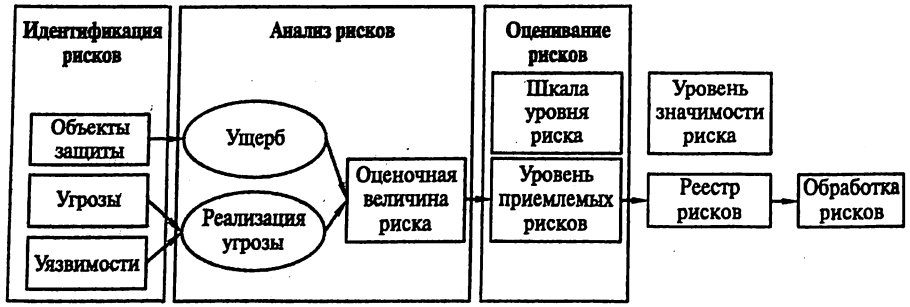


Рис. 3.4. Процесс оценки рисков информационной безопасности

Идентификация риска заключается в составлении перечня и описании элементов риска: объектов защиты, угроз, уязвимостей.

Выделяются следующие типы объектов защиты:

- информационные активы;
- программное обеспечение;
- физические активы;
- сервисы;
- люди, а также их квалификации, навыки и опыт;
- нематериальные ресурсы, такие как репутация и имидж организации.

Как правило, на практике рассматривают первые три группы. Остальные объекты защиты не рассматриваются в силу сложности их оценки.

[1] ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

На этапе идентификации рисков также выполняется идентификация угроз и уязвимостей. В качестве исходных данных для этого используют результаты аудитов, данные об инцидентах информационной безопасности, экспертные оценки пользователей, специалистов по информационной безопасности, ИТ-специалистов и внешних консультантов.

Информация, полученная на этапе идентификации рисков, используется в процессе анализа рисков для определения:

- возможного ущерба, наносимого организации в результате нарушений безопасности активов[1];
- вероятности наступления такого нарушения;
- величины риска.

Величина возможного ущерба формируется с учетом стоимости активов и тяжести последствий нарушения их безопасности.

Выделяют три подхода к оценке стоимости активов:

- затратный (затраты, необходимые для создания актива);
- доходный (ожидаемые доходы от использования активов);
- сравнительный (сравнение актива с аналогами, в отношении которых имеется информация о стоимости).

Затем полученные различными подходами результаты обобщают, получая интегрированную оценку стоимости.

Второй составляющей, формирующей значение возможного ущерба, является тяжесть последствий нарушения безопасности активов. Учитываются все возможные последствия и степень их негативного влияния на организацию, ее партнеров и сотрудников.

Необходимо определить степень тяжести последствий от нарушения конфиденциальности, целостности, доступности и других важных свойств информационного актива, а затем найти общую оценку.

Следующим этапом анализа рисков является оценка вероятности реализации угроз.

После того как были определены величина возможного ущерба и вероятность реализации угроз, определяют величину риска. Риск вычисляют комбинированием возможного ущерба, выражающего вероятные последствия нарушения безопасности активов, и вероятности реализации угроз. Такое комбинирование часто проводят при помощи матрицы, где в строках размещаются возможные значения ущерба, в столбцах — вероятности реализации угрозы, а на пересечении — величина риска.

Далее сравнивают вычисленные уровни риска со шкалой уровня риска. Это необходимо для того, чтобы реалистично оценивать влияние,

[1] Федеральный стандарт оценки № 1 (ФСО № 1) «Общие понятия оценки, подходы к оценке и требования к проведению оценки».

которое вычисленные риски оказывают на бизнес организации, и доносить смысл уровней риска до руководства. Оценивание рисков должно также идентифицировать приемлемые уровни риска, при которых дальнейшие действия не требуются. Все остальные риски требуют принятия дополнительных мер.

Для обработки риска информационной безопасности входными данными являются сведения о перечне рисков с назначенными приоритетами в соответствии с критериями оценки рисков, касающимися сценариев инцидентов, которые приводят к этим рискам. Для обработки риска имеется четыре варианта: *снижение риска*, *сохранение риска*, *предотвращение риска* и *перенос риска* (рис. 3.5).

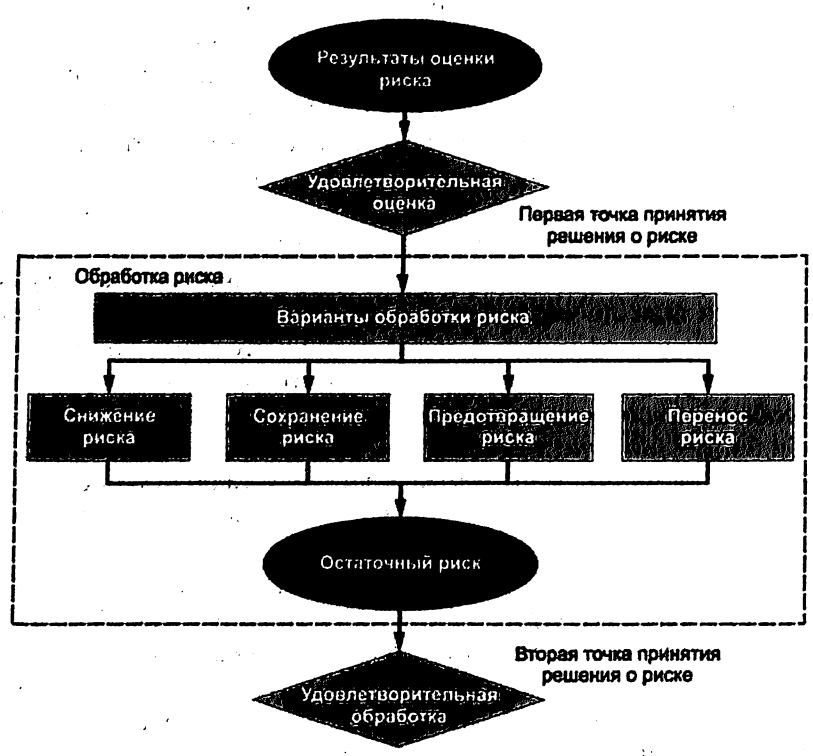


Рис. 3.5. Деятельность по обработке риска (ГОСТ Р ИСО/МЭК 27005-2010)

При *снижении риска* уровень риска должен быть снижен путем выбора меры и средства контроля и управления так, чтобы остаточный риск мог быть повторно оценен как допустимый.

Решение *сохранить риск*, не предпринимая дальнейшего действия, следует принимать в зависимости от оценки риска.

Предотвращение риска — отказ от деятельности или условия, вызывающего конкретный риск.

Перенос риска — разделение с другой стороной бремени потерь или выгод от риска.

В процессе обработки должны быть выбраны меры и средства контроля и управления для снижения, сохранения, предотвращения или переноса рисков, а также определен план обработки рисков.

Варианты обработки риска должны выбираться исходя из результатов оценки риска, предполагаемой стоимости реализации этих вариантов и их ожидаемой эффективности. Должны реализовываться такие варианты, при которых значительное снижение риска может быть достигнуто при относительно небольших затратах. Дополнительные варианты повышения эффективности могут быть неэкономичными, и необходимо принимать решение о целесообразности их применения.

Неблагоприятные последствия рисков необходимо снижать до разумных пределов независимо от каких-либо абсолютных критериев. Редкие, но серьезные риски должны рассматриваться руководством. В таких случаях может возникнуть необходимость реализации мер и средств контроля и управления, которые являются необоснованными по причинам затратности (например, меры и средства контроля и управления непрерывности бизнеса для охвата высоких специфических рисков).

Четыре варианта обработки риска не являются взаимоисключающими. В отдельных случаях организация может получить значительную выгоду от объединения вариантов, таких как снижение риска, уменьшение последствий и перенос или сохранение любого остаточного риска.

Некоторые варианты обработки риска могут быть эффективными для более чем одного риска (например, обучение и осведомленность в части ИБ). План обработки риска должен четко определять порядок приоритетов, при соблюдении которого должна реализовываться обработка отдельного риска. Порядок приоритетов может устанавливаться с использованием различных методов, включая ранжирование рисков и анализ «затраты — выгоды». В обязанности руководства входит принятие решения о балансе между затратами на реализацию мер и средств контроля и управления и бюджетными отчислениями.

При определении существующих мер и средств контроля и управления может быть установлено, что существующие меры и средства контроля и управления превышают текущую потребность в показателях сравнения затрат, включая поддержку. В случае удаления избыточных или ненужных мер и средств контроля и управления (особенно, если расходы на их поддержку велики) должны учитываться факторы ИБ и стоимости. Поскольку меры и средства контроля и управления оказывают влияние друг на друга, удаление избыточных мер и средств контроля и управления может в итоге снизить эффективность использования всех оставшихся мер и средств обеспечения безопасности. Кроме того, может быть менее затратным оставить избыточные или ненужные средства контроля, чем удалить их.

3.1.3. Обзор существующих стандартов и методик оценки рисков информационной безопасности[1]

Международный стандарт ISO/IEC 27005

До недавнего времени не существовало международного стандарта по управлению рисками информационной безопасности. В 2008 г. международной организацией по стандартизации и международной электротехнической комиссией был принят ISO/IEC 27005:2008 «Информационные технологии — Методы обеспечения безопасности — Управление рисками информационной безопасности». Указанный стандарт заменил сразу два морально устаревших стандарта ISO/IEC 13335-3 и ISO/IEC 13335-4, на базе которых он в основном и был разработан. ISO 27005 также опирается на следующие стандарты управления рисками, перечисленные в его библиографическом списке: ISO Guide 73, AS/NZS 4360 и NIST SP 800-30.

На рис. 3.6 показан порядок управления рисками информационной безопасности в соответствии с ISO/IEC 27005:2008.

Стандарт США NIST SP 800-30

Стандарт NIST SP 800-30:2002 «Risk Management Guide for Information Technology Systems» подробно рассматривает вопросы управления информационными рисками. Основные стадии, которые согласно стандарту NIST 800-30 должен включать процесс управления рисками, показаны на рис. 3.7.

[1] В разделе использованы материалы работы: *Гулякина В.В.* Разработка методики оценки рисков информационной безопасности. Дипломная работа (научный руководитель Е.К. Баранова). — М.: РГСУ, 2009.

На стадии «Описание системы» определяются цели создания информационной системы, ее границы, информационные ресурсы, требования в области ИБ и компонентов управления ИС и режимом ИБ.

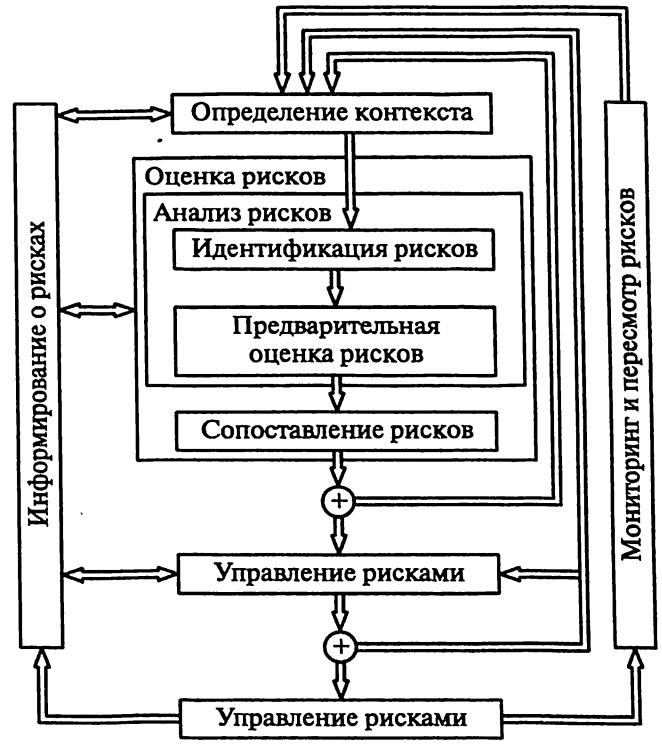


Рис. 3.6. Порядок управления рисками по ISO/IEC 27005:2008

Описание рекомендуется вести в соответствии со следующим планом:

- аппаратные средства ИС, их конфигурация;
- используемое ПО;
- интерфейсы системы, т.е. 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;

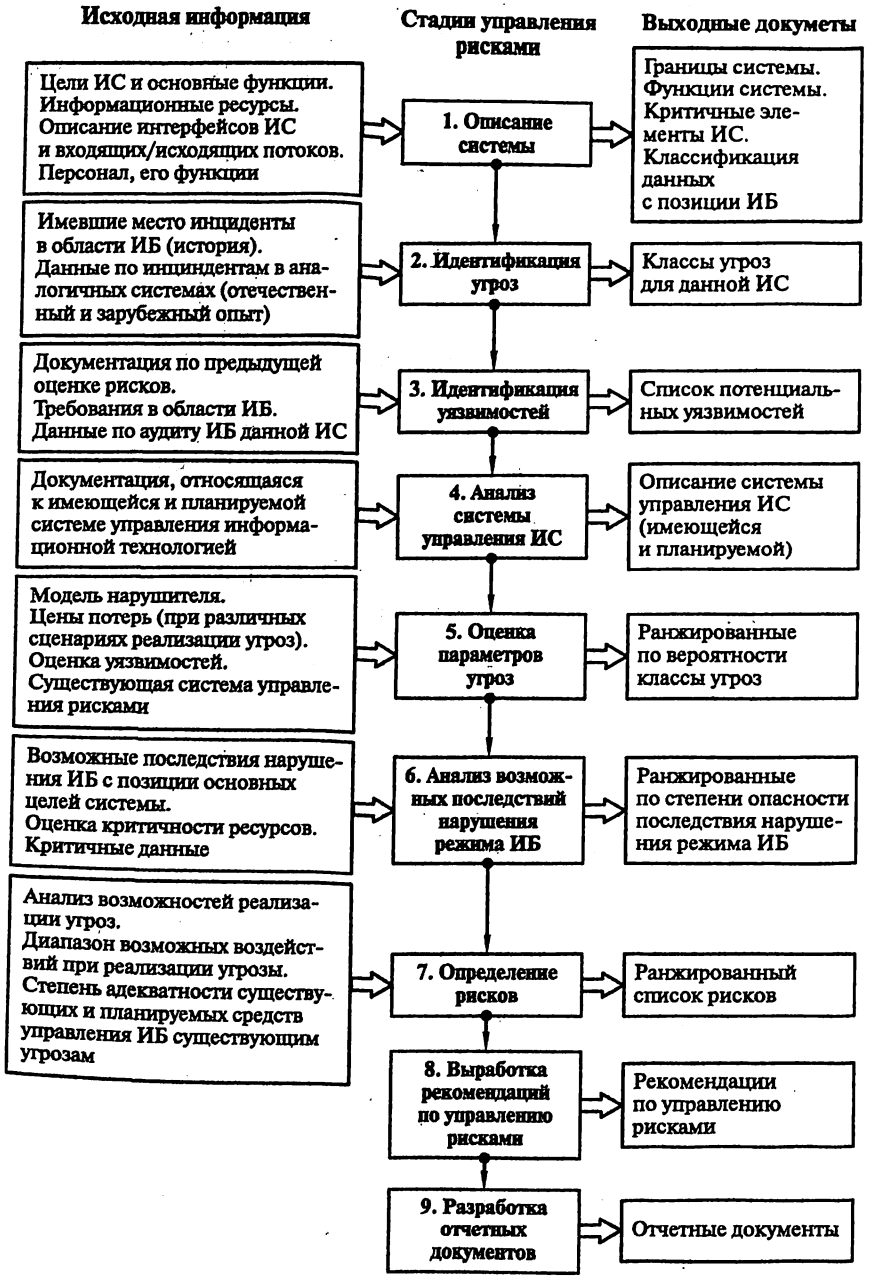


Рис. 3.7. Процесс управления рисками NIST SP 80-30

- 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 получения информации по перечисленным пунктам на практике рекомендуется использовать:

- разнообразные вопросники (check-листы), которые могут быть адресованы различным группам управленческого и обслуживающего персонала;
- интервью аналитиков, которые проводят неформальные беседы с персоналом и затем готовят формализованное описание;
- анализ документов предприятия;
- специализированный инструментарий (ПО) — сканеры, дающие возможность составить схему информационной системы, программы для структурированного описания информационных систем, позволяющие создать необходимые отчетные формы.

На стадии «Идентификация угроз» осуществляется построение модели нарушителя, где описывается, кто может выступать в качестве нарушителя, возможности и мотивы нарушителя, сценарий реализации угрозы. Итогом этого является перечень актуальных для информационной системы угроз.

В результате выполнения идентификации уязвимостей составляется список потенциальных уязвимостей информационной системы. Для существующей ИС при составлении списков прибегают к ряду источников: сетевые сканеры уязвимостей, каталоги уязвимостей разных организаций. При оценке уровня уязвимости принимают во внимание существующие процедуры и методы обеспечения режима информационной безопасности, данные внутреннего аудита и результаты анализа имевших место инцидентов.

Затем выбирают шкалы для оценки параметров рисков. Наиболее распространенной является качественная шкала с несколькими градациями. Оценка производится экспертно.

С использованием шкал оценивают тяжесть последствия нарушения ИБ и вероятности реализации угроз. Затем измеряют уровень рисков, комбинируя вероятности реализации угрозы и тяжести последствий ее реализации. Уровень риска зависит от уровней угроз, уязвимостей и цены возможных последствий. Риски должны быть ранжированы по степени их опасности.

Следующим шагом является выработка рекомендаций по управлению рисками. Рекомендации по уменьшению рисков до допустимого уровня необходимы. Они должны быть комплексными и учитывать возможные меры различных уровней.

Результаты оценки рисков оформляются в виде отчетных документов[1].

Руководство по управлению рисками в области безопасности от компании Microsoft

В этом руководстве риск определяется как вероятность того, что вследствие использования уязвимости в текущей среде пострадают конфиденциальность, целостность или доступность актива. Взаимосвязь компонентов риска показана на рис. 3.8.

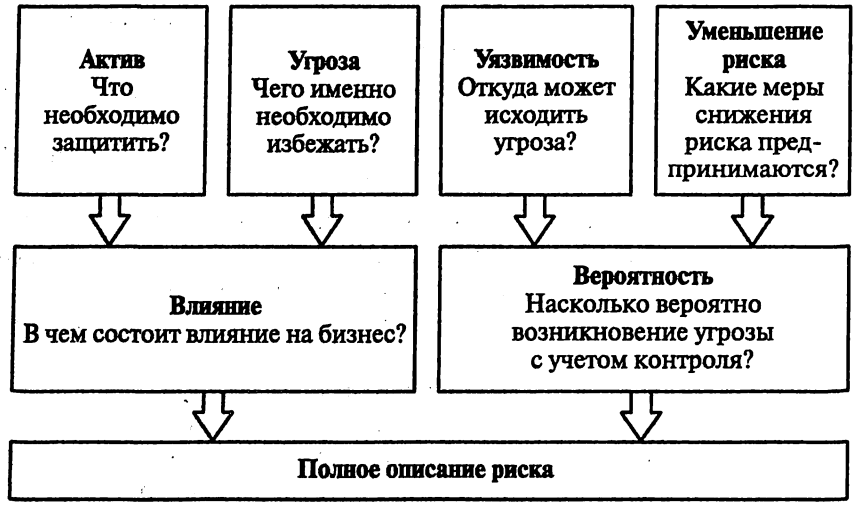


Рис. 3.8. Взаимосвязь компонентов риска

[1] *Петренко С.А., Симонов С.В.* Указ. соч.

Управление рисками представляет собой непрерывный процесс, включающий четыре этапа (рис. 3.9).

1. *Оценка рисков* — выявление и приоритизация рисков для бизнеса.
2. *Поддержка принятия решений* — поиск и оценка решений для контроля.
3. *Реализация контроля* — внедрение решений для контроля, снижающих риск.
4. *Оценка эффективности программы* — анализ эффективности процесса управления рисками и проверка того, обеспечивают ли элементы контроля надлежащий уровень безопасности.

Рис. 3.9. Этапы процесса управления рисками безопасности

Каждый этап этого цикла включает несколько шагов.

В этап оценки рисков входят:
- планирование;
- сбор данных о рисках;
- приоритизация рисков

Этап поддержки принятия решений включает:
- определение функциональных требований для снижения рисков;
- выбор возможных решений для контроля;
- проверку предложенных элементов контроля на соответствие функциональным требованиям;
- оценку снижения риска;
- оценку стоимости решения;
- определение экономически наиболее эффективного решения по нейтрализации риска путем анализа выгод и затрат

В этап реализации контроля входят:
- включение персонала, процессов и технологий в решение по нейтрализации риска;
- упорядочение решений по нейтрализации риска в рамках предприятия.

Этап оценки эффективности программы управления рисками содержит:
- разработку системы показателей рисков, их уровня и изменения;
- оценку эффективности программы управления рисками для выявления возможностей усовершенствования.

Итак, оценка рисков представляет собой процесс определения и упорядочения рисков в рамках организации.

Планирование является важным шагом, основные задачи которого состоят в точном определении сферы действия оценки и в получении поддержки со стороны руководства.

После завершения планирования необходимо получить сведения о рисках у сотрудников организации. Поскольку риск включает несколько компонентов (активы, угрозы, уязвимости и элементы контроля), собирают данные по каждому из них.

Для каждого риска определяют вероятность его возникновения и размер связанных с ним потерь. Далее используется одна из разновидностей табличной оценки рисков.

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

- высокий риск;
- средний риск;
- незначительный риск.

Риски разных групп в отчетной таблице выделяются разным цветом: высокий риск — красным, средний — желтым, низкий — зеленым.

С учетом уровня допустимых рисков выявленным рискам назначают приоритеты, которые служат для того, чтобы определить те риски, которые в первую очередь требуют нейтрализации. Эти риски в дальнейшем подвергаются подробному анализу с применением количественных методик, что дает возможность сформировать перечень наиболее опасных рисков с указанием числовых характеристик.

Области, включенные в оценку угроз безопасности в отчете Microsoft Security Assessment Tool (MSAT), приведены в табл. 3.1.

Таблица 3.1

Области, включенные в оценку угроз безопасности в отчете MSAT

Инфраструктура	Важность для безопасности
Защита периметра	Защита периметра касается безопасности на границах сети, где внутренняя сеть соединяется с внешним миром. Она составляет первую линию обороны против нарушителей
Проверка подлинности	Строгие процедуры проверки подлинности для пользователей, администраторов и удаленных пользователей предотвращают получение доступа к сети чужаками путем использования локальных и удаленных атак
Управление и наблюдение	Управление, наблюдение и правильное ведение журнала имеют ключевое значение для поддержки и анализа ИТ-сред. Эти средства еще более важны после того, как атака произошла и требуется анализ инцидента

Инфраструктура	Важность для безопасности
Рабочие станции	Защита отдельных рабочих станций является ключевым фактором в защите любой среды, особенно когда разрешен удаленный доступ. Рабочие станции должны обладать мерами безопасности для защиты от распространенных атак
Приложения	**Важность для безопасности**
Развертывание и использование	Когда ключевые для бизнеса приложения развертываются в производственной среде, необходимо защитить безопасность и доступность этих приложений и серверов. Постоянное обслуживание важно для надежного исправления ошибок безопасности и избежания внесения в среду новых ошибок
Проектирование приложений	Проектирование, которое не в должной мере решает вопросы с такими механизмами безопасности, как проверка подлинности, авторизация и проверка данных, может позволить взломщикам воспользоваться уязвимостями безопасности и таким образом получить доступ к важной информации. Безопасные методологии разработки приложений являются ключом к обеспечению того, что разработанные самостоятельно или подрядчиком приложения решают проблемы с моделью угроз, способной создать уязвимости в защите организации. Целостность и конфиденциальность данных являются одними из крупнейших забот для любого бизнеса. Потеря или кража данных может отрицательно сказаться на прибыли организации, равно как и на ее репутации. Важно понимать, как приложения обрабатывают ключевые для бизнеса данные и как эти данные защищены
Эксплуатация	**Важность для безопасности**
Среда	Безопасность компании зависит от рабочих процедур, процессов и рекомендаций, примененных к среде. Они повышают безопасность организации, включая в себя больше, чем просто технологии. Точное документирование среды и наличие руководств имеют ключевое значения для способности рабочей группы управлять, поддерживать и обслуживать безопасность среды
Политика безопасности	Корпоративной политикой безопасности именуется коллекция отдельных политик и рекомендаций, существующих для управления безопасным и верным использованием технологии и процессов внутри организации. Эта область охватывает политики, касающиеся всех типов безопасности, таких как безопасность пользователя, системы и данных

Окончание табл. 3.1

Эксплуатация	Важность для безопасности
Резервное копирование и восстановление	Резервное копирование и восстановление имеют ключевое значение для поддержания бесперебойности бизнес-операций в случае несчастья или сбоя оборудования/программного обеспечения. Отсутствие должных процедур резервного копирования и восстановления может привести к значительным потерям данных и продуктивности. Под угрозой может оказаться репутация компании и торговой марки
Управление исправлениями и обновлениями	Хорошее управление исправлениями и обновлениями важно в обеспечении безопасности ИТ-среды организации. Своевременное применение обновлений и исправлений необходимо, чтобы помочь в защите от известных и потенциальных уязвимостей
Персонал	**Важность для безопасности**
Требования и оценки	Требования безопасности должны быть понятны всем, кто принимает решения, чтобы их технические и бизнес-решения улучшали безопасность, а не конфликтовали с ней. Регулярные оценки сторонними консультантами могут помочь компании в обозрении, оценке и определении областей для улучшений
Политики и процедуры	Четкие, практичные процедуры по управлению отношениями с поставщиками и партнерами могут помочь в предотвращении создания угроз компании. Процедуры, охватывающие наем и увольнение сотрудников, могут помочь защитить компанию от беспринципных или обозленных сотрудников
Подготовка и осведомленность	Сотрудники должны быть обучены и осведомлены о политиках безопасности и о том, как безопасность касается их обязанностей, чтобы они случайно не подвергли компанию большей угрозе

В России в последние годы принят ряд стандартов, регламентирующих деятельность по управлению рисками информационной безопасности, перечислим лишь некоторые (часть стандартов находится в процессе доработки):

- ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий». Данный документ представляет собой руководство по управлению безопасностью информационных и телекоммуникационных технологий (ИТТ), устанавливает концепцию и модели, лежащие в основе базового понимания безопасности ИТТ, и раскрывает общие вопросы управления, которые важны для успешного планирования, реализации и поддержки безопасности ИТТ;
- ГОСТ Р 51897-2011 «Менеджмент риска. Термины и определения». Содержит определения основных терминов в области менеджмента риска;
- семейство ГОСТ Р ИСО/МЭК 27000, основанное и соответствующее семейству международных стандартов на системы управления информационной безопасностью ISO/IEC 27000. Эти стандарты определяют требования к системам управления информационной безопасностью, управлению рисками, метрики и измерения, а также руководство по внедрению.

В семействе ISO 27000 четыре вида групп стандартов:

- стандарты для обзора и введения в терминологию;
- стандарты, которые определяют обязательные требования к СУИБ
- (система управления информационной безопасностью);
- стандарты, определяющие требования и рекомендации для аудита СУИБ;
- стандарты, предлагающие лучшие практики внедрения, развития и совершенствования СУИБ.

Перечислим наиболее значимые стандарты семейства ISO 27000:

Стандарты для обзора и введения в терминологию

- ISO/IEC 27000:2016 «Информационные технологии. Средства обеспечения безопасности. Системы менеджмента информационной безопасности. Обзор и словарь»;

Стандарты, которые определяют обязательные требования к СУИБ

- ISO/IEC 27001:2005 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». Это основной стандарт пакета. Он определяет требования к разработке, внедрению, поддержке и улучшению систем менеджмента информационной безопасности;

Стандарты, определяющие требования и рекомендации для аудита СУИБ

- ISO/IEC 27006:2011 «Информационные технологии. Средства обеспечения безопасности. Требования для органов, выполняющих аудит и сертификацию систем менеджмента информационной безопасности». Этот стандарт расширяет требования стандарта ISO 17021 специально для органов, проводящих аудит и сертификацию СУИБ;

- ISO/IEC 27007:2011 «Информационные технологии. Средства обеспечения безопасности. Руководящие указания для аудита систем менеджмента информационной безопасности». Стандарт ISO 27007 предлагает рекомендации по проведению аудитов СУИБ со стороны сертификационных организаций. Он полезен для аудиторов этих организаций;
- ISO/IEC TR 27008:2011 «Информационные технологии. Методы обеспечения безопасности — Руководство для аудиторов по мерам и средствам обеспечения информационной безопасности». Данный стандарт, как и ISO 27007, является дополнительным стандартом к ISO 19011:2011 специально для СУИБ. Он специализирован для аудита средств управления информационной безопасностью в организации;

Стандарты, предлагающие лучшие практики внедрения, развития и совершенствования СУИБ

- ISO/IEC 27002:2005 «Информационные технологии. Средства обеспечения. Свод практики для менеджмента информационной безопасности». Он дает указания для разработки, внедрения, поддержки и совершенствования СУИБ;
- ISO/IEC 27003:2010 «Информационные технологии. Руководство по осуществлению системы менеджмента информационной безопасности». Стандарт дает указания и методику для процессов разработки и внедрения СУИБ;
- ISO/IEC 27004:2009 «Информационные технологии. Средства обеспечения безопасности. Измерения менеджмента информационной безопасности». Стандарт является руководством для выбора, проектирования, управления и улучшения средств и методов измерения эффективности и результативности системы;
- ISO/IEC 27005:2011 «Информационные технологии. Методы защиты. Менеджмент рисков информационной безопасности». Этот стандарт является одним из самых важных в группе;
- ISO/IEC 27011:2016 «Информационная технология. Методы и средства обеспечения безопасности. Практическое руководство по контролю за информационной безопасностью организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002». Это специализированное руководство по СУИБ в телекоммуникационных организациях;
- ISO/IEC 27035:2016 «Информационные технологии — Методы обеспечения защиты. Управление инцидентами по информационной безопасности».

Стандарты и методики оценки рисков разных стран мира

Помимо рассмотренных документов по управлению рисками, существует множество других, среди которых:

- немецкий стандарт BSI 100-3 «Risk Analysis based on IT-Grundschutz»;
- австралийский стандарт AS/NZS 4360-2004 «Australian/New Zealand Standard Risk management»;
- руководство по оценке рисков ИБ, разработанное в Швейцарии, SOMAP «Open Information Security Risk Assessment Guide»;
- французские разработки EBIOS «Expression of Needs and Identification of Security Objectives» и MARION «Risk Analysis Guide»;
- испанский документ MAGERIT «Methodology for Information Systems Risk Analysis and Management».

Все упомянутые документы распространяются бесплатно на английском языке. Перечисленные разработки представляют собой так называемые лучшие практики в данной области. Однако не следует воспринимать зарубежные разработки как панацею от всех бед, следует помнить, что они в обязательном порядке требуют адаптации.

3.1.4. Подходы к оценке рисков информационной безопасности

Реактивный и проактивный подходы

Рассмотрим подходы к оценке рисков информационной безопасности с использованием следующей аналогии. Грипп — это смертельно опасное заболевание, которым ежегодно заболевают миллионы человек. Очень часто лечение связано со значительными затратами, а также невозможностью из-за болезни выполнять свою работу. Чтобы справиться с этой угрозой, человек может или ничего не предпринимать, пока не заболеет, а затем обращаться к врачам и лечиться, или же пройти предварительную вакцинацию до начала эпидемии.

То же и с отношением к вопросам информационной безопасности. Организация может не вкладывать средства в проведение оценки рисков информационной безопасности, внедрение защитных мер, разработку планов обеспечения непрерывности, а в случае нарушения безопасности нести убытки, расходовать ресурсы на ликвидацию последствий. Такой подход называется реактивным.

Если подобное «тушение пожаров» организацию не устраивает, то выбирают проактивный подход. Вместо того чтобы начинать что-то делать лишь после возникновения проблем, организация уменьшает

вероятность их появления — для этого выполняют оценку и обработку рисков информационной безопасности, разрабатывают планы проведения профилактических мероприятий.

Организации, которые выбирают проактивный подход и реагируют на инциденты с использованием взвешенных и рациональных методик, определяя причины, которые привели к возникновению инцидента, лучше защищены и могут быстрее реагировать на инциденты.

Качественная и количественная оценка рисков информационной безопасности

До начала работ по оценке рисков ИБ необходимо определить, в качественных или количественных показателях выражать риски.

Качественная оценка рисков позволяет выявить существующие риски, определить степень их воздействия на организацию.

Существуют несколько моделей качественной оценки. Все они достаточно просты, варианты различаются лишь числом градаций шкал. Одна из самых распространенных моделей — трехуровневая. Каждый фактор оценивается по шкале «низкий — средний — высокий». Во многих случаях трехуровневая шкала является достаточной, но в некоторых случаях может потребоваться более детальная шкала, например пятиуровневая: «незначительный — низкий — средний — высокий — очень высокий». Однако следует помнить: какой бы уровень детализации ни был выбран, необходимо позаботиться о том, чтобы интерпретация уровней могла отражать различия между уровнями.

Трехуровневые качественные шкалы для оценки возможного ущерба, вероятности реализации угроз, величины рисков предлагают использовать большинство международных стандартов.

Основное преимущество качественного подхода состоит в том, что данный подход позволяет отказаться от сложных процедур определения точной стоимости актива, затрат на защитные меры, вероятности реализации угроз, что значительно сокращает время на проведение работ по оценке рисков. Однако полученные результаты субъективны, не имеют однозначной интерпретации.

Итоговые результаты качественной оценки рисков могут служить исходной информацией для проведения количественной оценки.

Методы количественного характера выражают риски численно, т.е. ожидаемые потери в числовом эквиваленте и вероятность или частоту этих потерь.

В результате количественной оценки каждому риску ставится в соответствие величина возможных финансовых потерь в случае его реализации, что может использоваться для обоснования необходимости внедрения защитных мер, а также рассчитывается вероятность реализации угроз, что позволяет оценить их реальную опасность.

Количественные оценки позволяют оценить соотношение возможных финансовых потерь и расходов на приобретение и эксплуатацию защитных мер, а затем рассчитывать экономический эффект мероприятий. Наличие численных оценок, подтвержденных выкладками, в отчетах для руководства повышает уровень доверия к отчетным документам.

Однако у описанного подхода есть несколько существенных недостатков. Во-первых, не существует эффективного формализованного метода, позволяющего точно определить стоимости активов. Как, например, точно определить влияние нарушения ИБ, получившего широкую огласку, на имидж организации? Во-вторых, скрупулезная реализация всех аспектов количественного подхода требует больших затрат.

Количественная оценка точнее, позволяет получить конкретные значения рисков, но требует заметно больше времени и ресурсов, что не всегда оправданно, так как организации постоянно развиваются, изменяются, следовательно, за то время, пока выполняется оценка, фактические значения рисков могут оказаться другими.

Какой метод оценки рисков ИБ выбрать, зависит от того, насколько точно можно рассчитать стоимость объектов защиты, оценить вероятность реализации угрозы и степень уязвимости. Если эти данные точны и достаточны, то целесообразно использовать количественную оценку, в противном случае — качественную.

Как уже было отмечено ранее, для количественной оценки рисков нужна достоверная, полная исходная информация, которую, как правило, сложно получить. Например, для оценки вероятности угроз необходима накопленная статистика, отражающая факты и частоту реализации угроз.

К сожалению, отсутствие исходной информации и эффективного инструментария ее обработки делает использование количественных методов оценки в настоящее время неэффективным.

Базовая и детальная оценка рисков информационной безопасности

Выбор глубины проводимой оценки будет зависеть от множества факторов: область деятельности, размеры организации, степень автоматизации бизнес-процессов, уровень зрелости организации, наличие

квалифицированного персонала, средств, выделяемых на обеспечение ИБ, и т.д. Анализ перечисленных факторов позволяет выбрать подходящий в каждой конкретной ситуации подход к оценке рисков.

Сегодня существует три подхода к оценке рисков информационной безопасности:

- базовый;
- детальный;
- комбинированный.

Рассмотрим каждый из них подробнее.

Первый подход предполагает обеспечение базового уровня защищенности путем выбора минимального набора защитных мер. В данном случае оценивают вероятности нарушения безопасности и тяжести возможных последствий такого нарушения. При этом риск тем больше, чем выше вероятность нарушения безопасности и тяжесть возможных последствий.

Основное преимущество использования базового подхода — это возможность обойтись минимальным количеством ресурсов при проведении оценки и дальнейшей обработки рисков ИБ.

Рассматриваемый подход экономически эффективен при условии, что выбранный базовый уровень защищенности соответствует уровню, необходимому для большинства объектов защиты организации. Если выбранный базовый уровень завышен, то защитные меры окажутся излишними, в случае же если базовый уровень защищенности занижен, то для ряда объектов защиты выбранные меры будут недостаточны.

Если базовых оценок недостаточно, используют детальную оценку рисков. В этом случае для каждого объекта защиты или группы объектов защиты определяют перечень актуальных угроз и оценивают вероятность их реализации, а также степень легкости, с которой угрозы могут реализоваться, т.е. уровень уязвимости.

Описываемый подход позволяет определить необходимые и достаточные защитные меры, однако связан со значительными затратами времени и средств, а также с необходимостью привлечения квалифицированных специалистов. Поскольку оценка проводится одинаково тщательно для всех объектов защиты организации, определение и реализация необходимых защитных мер для какого-либо критичного объекта защиты может произойти слишком поздно, когда безопасность уже нарушена и организация несет убытки. Таким образом, проводить детальную оценку рисков применительно ко всем объектам защиты не рекомендуется.

У каждого из перечисленных подходов есть достоинства и недостатки, в связи с чем в каждом конкретном случае важно найти между

ними баланс. В качестве такого баланса выступает третий подход — комбинированный, который предполагает проведение предварительной оценки для всех объектов защиты, с тем чтобы установить, какой из подходов (базовый или детальный) лучше подходит для конкретного объекта защиты (или группы объектов защиты).

Исходные данные для принятия решения о применимости базового или детального подходов могут быть получены в результате анализа следующих факторов:

- требования нормативно-правовых актов РФ по информационной безопасности;
- цели, для достижения которых используется объект защиты (если в организации выделены и описаны бизнес-процессы, то указываются бизнес-процессы, в реализации которых задействован объект защиты);
- степень зависимости деятельности организации от объекта защиты;
- стоимость создания, приобретения объекта защиты, затраты на поддержание в рабочем состоянии, ремонт и т.д.;
- наличие потенциальных нарушителей (конкуренты, обиженные сотрудники и т.п.);
- возможность возникновения экстремальных погодных условий, близость к источникам опасности и т.д.

Если нарушение безопасности объекта защиты может причинить организации ущерб, отрицательно повлиять на ее деятельность, репутацию, то принимается решение проводить детальную оценку рисков, во всех остальных случаях достаточно применение базового подхода.

Использование быстрой и простой предварительной оценки рисков в значительной мере способствует успешному планированию работ по оценке рисков, ресурсы и средства могут быть вложены туда, где они принесут максимальный эффект, так как они в первую очередь будут направлены на критичные объекты защиты, в наибольшей степени нуждающиеся в защите.

Единственный потенциальный недостаток такого подхода состоит в следующем: отдельные объекты защиты могут быть ошибочно отнесены к объектам защиты, не требующим проведения детальной оценки рисков, и к этим объектам защиты в дальнейшем будут применены базовые защитные меры[1].

[1] ГОСТ Р ИСО/МЭК 13335-3–2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий».

Подобный подход наиболее предпочтителен для большинства организаций, так как сочетает лучшие свойства базового и детального подходов и позволяет при сведении к минимуму времени и усилий, затраченных на оценку рисков, обеспечить необходимую защиту критичных объектов защиты.

Экспертная оценка рисков информационной безопасности

Определение величин, формирующих значение рисков, как правило, осуществляется методом экспертных оценок, который предусматривает формирование мнения группы экспертов, являющихся специалистами в рассматриваемой предметной области, путем их опроса.

На качество полученных оценок существенно влияют полнота и достоверность предоставляемой эксперту исходной информации. Для этих целей в организации создается экспертная комиссия, в состав которой могут входить как сотрудники организации, так и сторонние эксперты. В организации разрабатывается положение, регламентирующее деятельность экспертной комиссии.

Такой подход не требует значительных средств или времени, однако оценки субъективны, основаны на практическом опыте конкретного эксперта, и это влечет за собой трудности при обосновании перед высшим руководством необходимости реализации выбранных защитных мер.

3.2. Программное обеспечение для оценки рисков информационной безопасности

Проблема оценки рисков ИБ представляет собой многофакторную задачу, что требует привлечения достаточно сложного вычислительного аппарата и программного инструментария для получения надежных оценок. При этом современное программное обеспечение для оценки рисков ИБ дает возможность получения как качественных, так и количественных значений оценок. На рис. 3.10 приведены наиболее популярные современные методики анализа и оценки рисков.

Методики, использующие оценку риска на качественном уровне (например по шкале «высокий», «средний», «низкий»). К таким методикам, в частности, относится FRAP	Количественные методики (риск оценивается через числовое значение, например, размер ожидаемых годовых потерь). К этому классу относится методика Risk Watch	Методики, использующие смешанные оценки. Такой подход используется в методике CRAMM

Рис. 3.10. Методики и программные продукты для оценки рисков ИБ

Методика FRAP (Facilitated Risk Analysis Process), предлагаемая компанией *Peltier and Associates*, разработана Томасом Пелтиером (*Thomas R. Peltier*) и опубликована в 2001 г. Методика FRAP использует оценку риска на качественном уровне, в ней обеспечение ИБ информационной системы предлагается рассматривать в рамках процесса управления рисками. Заметим, что управление рисками в сфере ИБ — процесс, позволяющий компаниям найти баланс между затратами на средства защиты и получаемым эффектом.

Основные этапы оценки рисков методики FRAP могут быть сформулированы следующим образом.

1. Определение защищаемых ресурсов — производится с использованием опросных листов, изучения документации на систему, инструментов автоматизированного анализа активов.

2. Идентификация и составление списка угроз. При составлении списка угроз могут использоваться различные подходы:
   - заранее подготовленные экспертами перечни угроз (*checklists*), из которых выбирают наиболее вероятные для данной системы;
   - анализ статистики происшествий, связанных с ИБ данной ИС или подобных ей; по возможности оценивается их частота за избранный для оценивания период времени.

3. Установление вероятности возникновения угроз и оценка ущерба, который может быть нанесен данной угрозой. Исходя из полученных значений, оценивают уровень угрозы. Оценка ведется для вероятности возникновения угрозы и ущерба от нее по качественным шкалам («высокий», «средний», «низкий») с использованием матрицы рисков (рис. 3.11).

При проведении анализа, как правило, принимают, что на начальном этапе в системе отсутствуют средства и механизмы защиты. Таким образом оценивается уровень риска для незащищенной ИС, что в последствии позволяет показать эффект от внедрения средств защиты информации (СЗИ).

4. После того как угрозы идентифицированы и дана оценка риска, определяются контрмеры, позволяющие устранить риск или снизить его до приемлемого уровня. При этом должны приниматься во внимание законодательные ограничения, делающие невозможным или, наоборот, предписывающие в обязательном порядке, использование тех или иных средств и механизмов защиты. Чтобы определить ожидаемый эффект, можно провести оценку того же риска, но при условии внедрения предлагаемого СЗИ. Вместе с определением средства защиты необходимо учитывать, какие затраты повлечет его приобретение и внедрение. Кроме того, необходимо оценить, безопасно ли само это средство, не создает ли оно новых уязвимостей в системе.

PROBABILITY

IMPACT

	High	Medium	Low
High	A	B	C
Medium	B	B	C
Low	B	C	D

A — Corrective action must be implemented
B — Corrective action should be implemented
C — Requires monitor
D — No action required at this time

- уровень A — связанные с риском действия (например, внедрение СЗИ) должны быть выполнены немедленно и в обязательном порядке;
- уровень B — связанные с риском действия должны быть предприняты;
- уровень C — требуется мониторинг ситуации (но непосредственных мер по противодействию угрозе принимать, возможно, не надо);
- уровень D — никаких действий в данный момент предпринимать не требуется

Рис. 3.11. Пример матрицы оценки рисков методики FRAP

Чтобы использовать экономически эффективные средства защиты, необходимо проводить анализ соотношения затрат и получаемого эффекта. При этом оценивается не только стоимость приобретения СЗИ, но и стоимость эксплуатации.

5. Документирование. Когда оценка рисков закончена, ее результаты подробно документируются в стандартизованном формате. Полученный отчет может быть использован при определении политик, процедур или бюджета безопасности.

Заметим, что последовательность и содержание этапов методики FRAP во многом повторяет аналогичный перечень методик, рассматриваемых далее, но в ней более подробно раскрываются пути получения данных о системе и ее уязвимостях.

Методика Risk Watch компании *Risk Watch* представляет собой семейство программных средств для анализа рисков:

- *Risk Watch for Physical Security* — для анализа физической защиты ИС;
- *Risk Watch for Information Systems* — для информационных рис-ков;
- *HIPAA-WATCH for Healthcare Industry* — для оценки соответствия требованиям стандарта *HIPAA* (*US Healthcare Insurance Portability and Accountability Act*), актуальных в основном для медицинских учреждений, расположенных на территории США;

- *Risk Watch RW17799for ISO 17799* — для оценки соответствия ИС требованиям международного стандарта *ISO 17799*.

В методе *Risk Watch* в качестве критериев для оценки и управления рисками, используются ожидаемые годовые потери (*Annual Loss Expectancy, ALE*) и оценка возврата инвестиций (*Return on Investment, ROI*). *Risk Watch* ориентирована на точную количественную оценку соотношения потерь от реализации угроз безопасности и затрат на создание системы защиты.

В основе продукта *Risk Watch* лежит методика анализа рисков, которая состоит из четырех этапов.

Первый этап — определение предмета исследования. Здесь описываются такие параметры, как тип организации, состав исследуемой системы, базовые требования в области безопасности.

Второй этап — ввод данных, описывающих конкретные характеристики системы. Эти данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимостей информационных систем. Для выявления возможных уязвимостей используется вопросник, база которого содержит более 600 опросов. Вопросы связаны с категориями ресурсов (рис. 3.12).

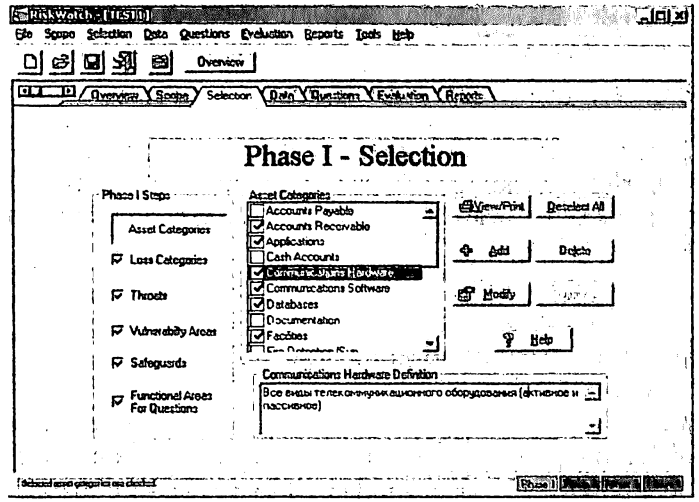


Рис. 3.12. Определение категорий защищаемых ресурсов

Также задаются частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Если для выбранного класса угроз в системе есть среднегодовые оценки возникновения: *LAFE* (*Local Annual Frequency Estimate*), показывают, сколько раз в год в сред-

нем данная угроза реализуется в данном месте, и *SAFE* (*Standard Annual Frequency Estimate*) — сколько раз в год в среднем данная угроза реализуется в этой «части мира», то используются они (рис. 3.13). Такая детализация при описании угроз делает оценку более точной.

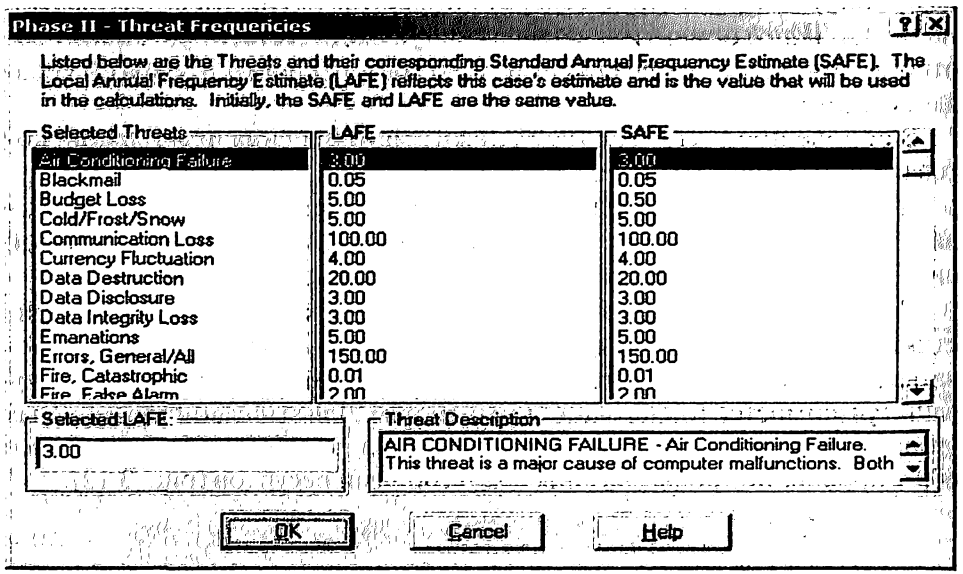


Рис. 3.13. Пример оценок LAFE и SAFE для одной из угроз

Третий этап — количественная оценка риска. На этом этапе рассчитывают профиль рисков и выбирают меры обеспечения безопасности.

По сути, риск оценивается с помощью математического ожидания потерь за год:

$$M = PV,$$

где M — математическое ожидание;

P — вероятность возникновения угрозы;

V — стоимость ресурса.

В связи с тем что *Risk Watch* использует определенные американским институтом стандартов *NIST* оценки *LAFE* и *SAFE*, базовая формула уточняется с использованием поправочных коэффициентов. Вводится также поправочный коэффициент, который позволяет учесть, что в результате реализации угрозы защищаемый ресурс может быть уничтожен не полностью, а только частично.

Четвертый этап — генерация отчетов, которые могут быть следующих видов:

- краткие итоги;

- полные и краткие отчеты об элементах, описанных на первом и втором этапах;
- отчет от стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз;
- отчет об угрозах и мерах противодействия;
- отчет по оценке возврата инвестиций, *ROI* (фрагмент на рис. 3.14);
- отчет о результатах аудита безопасности.

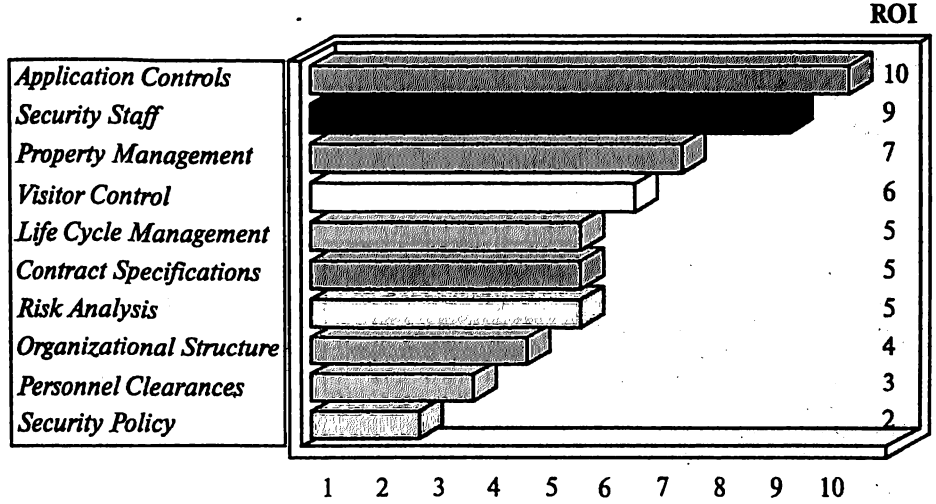


Рис. 3.14. Пример графика показателя ROI для различных мер защиты

Заметим, что методика *Risk Watch* позволяет оценить не только те риски, которые существуют у предприятия в настоящий момент, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты.

Эффект от внедрения средств защиты количественно описывается с помощью показателя *ROI*, который показывает отдачу от сделанных инвестиций за определенный период времени.

Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия.

Методика CRAMM (*CCTA Risk Analysisand Management Method*) — одна из первых методик анализа рисков в сфере ИБ [1].

[1] *Петренко С.А., Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. — М.: Академия АйТи: ДМК Пресс, 2004.

Работа над CRAMM была начата в середине 80-х гг. в *Central Computing and Telecommunication Agency (CCTA)*, Великобритания.

В основе метода CRAMM лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит как для крупных, так и для мелких организаций как государственного, так и коммерческого сектора. Версии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами данных (*profiles*).

CRAMM — пример методики расчета, где первоначальные оценки даются на качественном уровне, а затем переходят к количественной оценке (в баллах). Анализ и оценка рисков ИБ с помощью CRAMM проводится в три стадии (рис. 3.15).

На первой стадии	**На второй стадии**	**На третьей стадии**
анализируется все, что касается идентификации и определений ценности ресурсов системы. Она начинается с решения задачи определения границ исследуемой системы: собираются сведения о конфигурации системы и о том, кто отвечает за физические и программные ресурсы, кто входит в число пользователей системы, как они ее применяют или будут применять	рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. В конце стадии заказчик получает идентифицированные и оцененные уровни рисков для своей системы. На этой стадии оцениваются зависимость пользовательских сервисов от определенных групп ресурсов и существующий уровень угроз и уязвимостей, вычисляются уровни рисков и анализируются результаты	обеспечивается поиск адекватных контрмер. По существу, это поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика. На этой стадии CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Контрмеры можно объединить в три категории: около 300 рекомендации общего плана: более 1000 конкретных рекомендаций: около 900 примеров организации защиты

Рис. 3.15. Методика CRAMM

Пример идентификации ресурсов и построения модели с позиции ИБ системы на первой стадии CRAMM приведен на рис. 3.16.

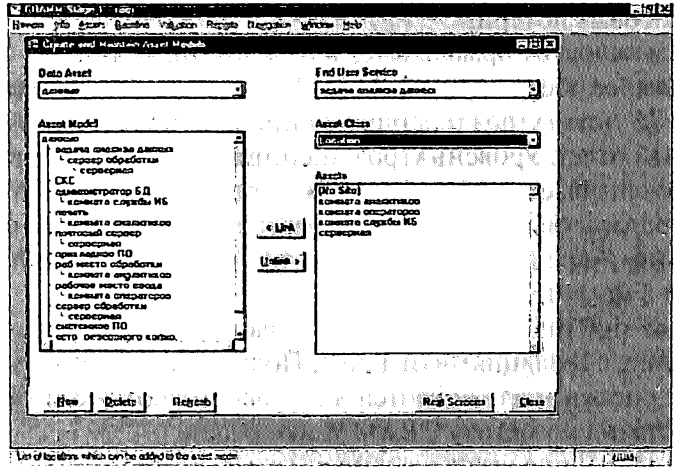


Рис. 3.16. Идентификация ресурсов и построение модели с позиции ИБ

Пример оценки ценности информационных ресурсов на первой стадии анализа по методу CRAMM приведен на рис. 3.17.

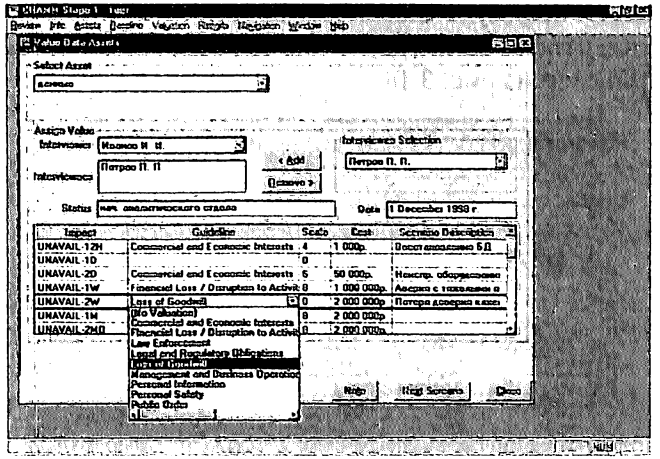


Рис. 3.17. Оценка ценности информационных ресурсов

Критериями оценки ценности ресурсов являются:

- ущерб для репутации организации;
- безопасность персонала;
- разглашение персональных сведений;
- разглашение коммерческих сведений;
- неприятности со стороны правоохранительных органов;

• финансовые потери;
• невозможность нормальной работы организации.

Программное обеспечение CRAMM для каждой группы ресурсов и каждого из 36 типов угроз генерирует список вопросов, допускающих однозначный ответ. Уровень угроз оценивается в зависимости от ответов как «очень высокий», «высокий», «средний», «низкий» и «очень низкий». Уровень уязвимостей оценивается, в зависимости от ответов как «высокий», «средний» и «низкий». CRAMM объединяет угрозы и уязвимости в матрице риска.

На основе этой информации рассчитываются уровни рисков по дискретной шкале с градациями от 1 до 7. Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком.

Вторая стадия по методу CRAMM включает:
• идентификацию угроз и возможных уязвимостей;
• группировку по угрозам или воздействиям с целью минимизации объема работы по анализу рисков;
• измерение рисков;
• получение отчета и обсуждение результатов с заказчиками;
• коррекция по результатам обсуждения.

Пример идентификации угроз и возможных уязвимостей по методу CRAMM приведен на рис. 3.18.

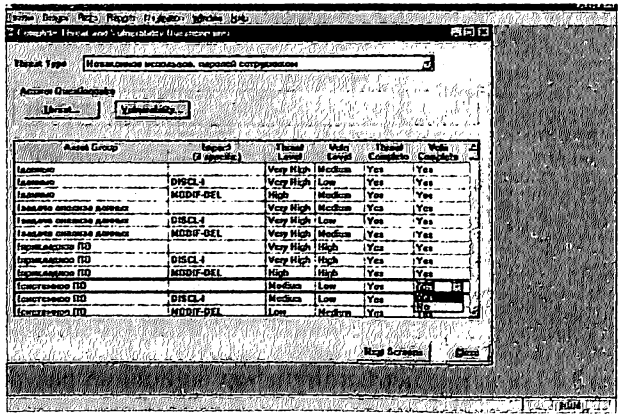


Рис. 3.18. Угрозы и уязвимости

На третьей стадии выполняются следующие шаги:
• генерация вариантов контрмер;
• выбор подходящих вариантов и анализ их эффективности;
• сравнительный анализ различных вариантов (*What if*);

• получение отчета и обсуждение результатов с заказчиками;
• коррекция по результатам обсуждения.

Достоинства методики CRAMM могут быть сформулированы следующим образом:
– метод достаточно хорошо апробирован;
– удачная система моделирования информационной системы;
– обширная база данных для оценки рисков и выбора контрмер;
– предполагается возможность использования как средства аудита.

В качестве недостатков следует отметить достаточно большой объем результирующих отчетов и сравнительно высокую трудоемкость использования.

Система ГРИФ — комплексная система оценки и управления рисками информационной безопасности.

Основная задача системы ГРИФ — дать возможность самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в ИС и эффективность существующей практики по обеспечению безопасности, а также предоставить возможность доказательно (в цифрах) убедить руководство в необходимости инвестиций в сферу ее ИБ.

Система содержит модуль управления рисками, который позволяет проанализировать все причины того значения риска, который получается после обработки алгоритмом занесенных данных. Благодаря расчету эффективности каждой возможной контрмеры, а также определению значения остаточного риска можно выбрать оптимальные контрмеры, которые позволят снизить риск до необходимого уровня с наименьшими затратами.

На первом этапе метода ГРИФ проводится опрос ИТ-специалистов с целью определения полного списка информационных ресурсов, представляющих ценность для организации.

На втором этапе проводится опрос ИТ-специалистов с целью ввода в систему ГРИФ всех видов информации, представляющей ценность для организации. Введенные группы ценной информации должны быть размещены пользователем на указанных на предыдущем этапе объектах хранения информации (серверах, рабочих станциях и т.д.). Заключительная фаза — указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

На третьем этапе определяют все виды пользовательских групп с указанием числа пользователей в каждой группе. Затем фиксируют, к каким группам информации на ресурсах имеет доступ каждая из групп

пользователей. В заключение определяют виды (локальный и/или удаленный) и права доступа пользователей ко всем ресурсам, содержащим ценную информацию.

На четвертом этапе проводится опрос ИТ-специалистов для определения имеющихся средств защиты ценной информации. Кроме того, в систему вводится информация о разовых затратах на приобретение всех применяющихся средств защиты информации и ежегодные затраты на их техническую поддержку, а также ежегодные затраты на сопровождение системы ИБ организации.

На завершающем этапе необходимо ответить на вопросы по политике безопасности, реализованной в системе, что позволит оценить реальный уровень защищенности системы и детализировать оценки рисков.

Анализ рисков информационной безопасности осуществляется с помощью построения модели информационной системы организации. Рассматривая средства защиты ресурсов, взаимосвязь ресурсов между собой, влияние прав доступа групп пользователей, организационные меры, модель исследует защищенность каждого вида информации. На рис. 3.19 приведено основное окно программы ГРИФ для анализа угроз и уязвимостей.

Для того, чтобы оценить информационные риски, необходимо проанализировать архитектуру и защищенность информационной системы.

Владельцу ИС требуется первоначально описать архитектуру сети:

- все ресурсы, на которых хранится ценная информация;
- сетевые группы, в которых находятся ресурсы системы (физические связи ресурсов друг с другом);
- отделы, к которым относятся ресурсы;
- виды ценной информации;
- ущерб для каждого вида ценной информации по трем видам угроз (угрозы конфиденциальности, целостности и доступности);
- бизнес-процессы, в которых обрабатывается информация;
- группы пользователей, имеющих доступ к ценной информации;
- класс группы пользователей;
- доступ группы пользователей к информации;
- характеристики этого доступа (вид и права);
- средства защиты информации;
- средства защиты рабочего места группы пользователей.

Исходя из перечисленных данных можно построить полную модель информационной системы компании, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе.

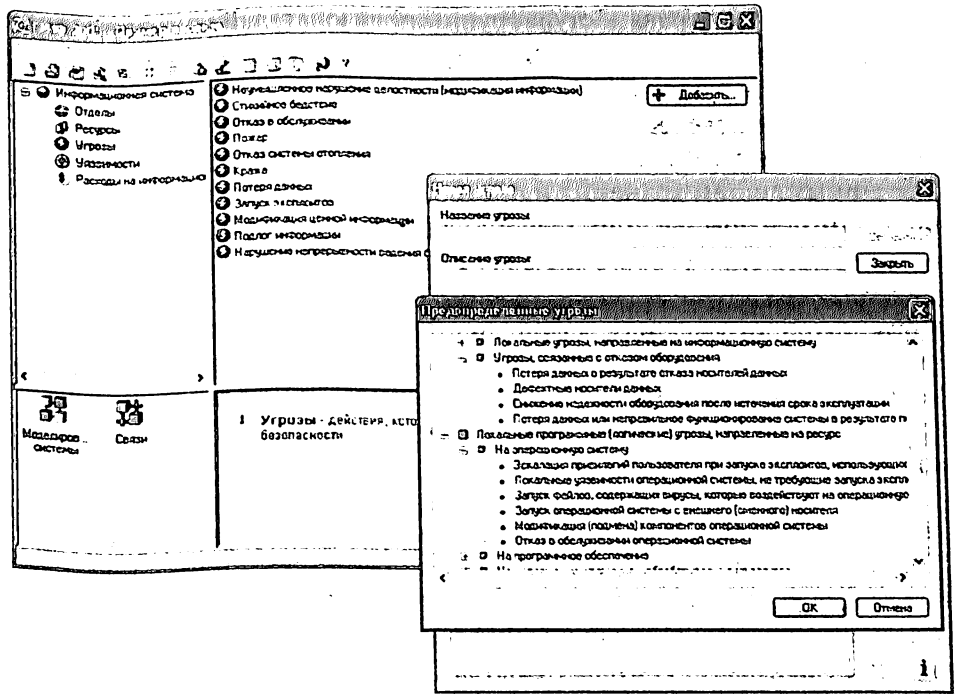


Рис. 3.19. Анализ угроз и уязвимостей с использованием системы ГРИФ

Риск оценивается отдельно по каждой связи «пользователь — информация», т.е. в модели рассматривается взаимосвязь «субъект — объект» с учетом всех характеристик.

Риск реализации угрозы информационной безопасности для каждого вида информации рассчитывается по трем основным угрозам: конфиденциальность, целостность и доступность. Владелец информации задает ущерб отдельно по трем угрозам — это проще и понятнее, так как оценить ущерб в целом не всегда возможно.

Алгоритм работы системы

1. Расчет рисков для угроз конфиденциальности и целостности (алгоритмы расчета для угроз целостности и конфиденциальности похожи, поэтому здесь мы их объединили)

Определяется вид доступа для группы пользователей к информации. От этого будет зависеть количество средств защиты, так как для локального и удаленного доступа применяются разные средства защиты.

Определяются права доступа группы пользователей к информации. Это важно для целостности (при доступе «только чтение» целостность информации нарушить нельзя) и для доступности.

Особым видом средства защиты является антивирусное программное обеспечение. В условиях современного функционирования компьютерных систем хранения и обработки информации вредоносное программное обеспечение представляет собой наиболее опасную и разрушительную угрозу. Учитывая значительность потенциального ущерба от вредоносного программного обеспечения, отсутствие антивирусного программного обеспечения на ресурсе (или клиентском месте пользователя) необходимо принимать во внимание отдельно. Если на ресурсе не установлено антивирусное ПО, то вероятность реализации угроз конфиденциальности, целостности и доступности резко возрастает.

Теперь у нас есть все необходимые данные, чтобы определить средства защиты информации и рабочего места группы пользователей. Просуммировав веса средств защиты, получим суммарный коэффициент. Для угрозы целостность учитываются специфические средства защиты — средства резервирования и контроля целостности информации. Если к ресурсу осуществляется локальный и удаленный доступ, то на данном этапе будут определены три коэффициента: коэффициент локальной защищенности информации на ресурсе, коэффициент удаленной защищенности информации на ресурсе и коэффициент локальной защищенности рабочего места группы пользователей. Из полученных коэффициентов выбираем минимальный. Чем меньше коэффициент защищенности, тем слабее защита, т.е. важно учесть наименее защищенное (наиболее уязвимое) место в информационной системе. Отдельно учитывается наличие криптографической защиты данных при удаленном доступе. Если пользователи могут получить удаленный доступ к ценным данным, не используя систему шифрования, это может значительно повлиять на целостность и конфиденциальность данных.

На последнем этапе перед получением итогового коэффициента защищенности связи «информация — группа пользователей» анализируется количество участников в группе пользователей и наличие у группы пользователей выхода в Интернет. Все эти параметры сказываются на защищенности информации. Таким образом, получаем конечный, итоговый коэффициент защищенности для связки «информация — группа пользователей».

Полученный итоговый коэффициент нужно умножить на базовую вероятность реализации угрозы информационной безопасности. Базовая вероятность определяется на основе метода экспертных оценок. Группа экспертов, исходя из классов групп пользователей, получающих доступ к ресурсу, видов и прав их доступа к информации, рассчитывает базовую вероятность для каждой информации. Владелец информационной системы при желании может задать этот параметр самостоятельно. Перемножив базовую вероятность и итоговый коэффициент защищенности, получаем итоговую вероятность реализации угрозы. Напомним, что для каждой из трех угроз информационной безопасности мы отдельно рассчитываем вероятность реализации.

На завершающем этапе значение полученной итоговой вероятности умножаем на ущерб от реализации угрозы и получаем риск угрозы информационной безопасности для связи «вид информации — группа пользователей».

Чтобы получить риск для вида информации (с учетом всех групп пользователей, имеющих к ней доступ), необходимо сначала учесть итоговые вероятности реализации угрозы по следующей формуле

$$P_{inf} = 1 - \prod_{i=1}^{n} (1 - P_{ug,n}).$$

А затем полученную итоговую вероятность для информации необходимо умножить на ущерб от реализации угрозы, получая таким образом риск от реализации угрозы для данной информации.

2. Расчет рисков по угрозе отказ в обслуживании

Если для целостности и конфиденциальности вероятность реализации угрозы рассчитывается в процентах, то для доступности аналогом вероятности является время простоя ресурса, содержащего информацию. Однако риск по угрозе отказ в обслуживании все равно считается для связки «информация — группа пользователей», так как существует ряд параметров, которые влияют не на ресурс в целом, а на отдельный вид информации.

На первом этапе определяется базовое время простоя для информации.

Далее необходимо рассчитать коэффициент защищенности связки «информация — группы пользователей». Для угрозы отказ в обслуживании коэффициент защищенности определяется с учетом права доступа группы пользователей к информации и средств резервирования.

Так же, как для угроз нарушения конфиденциальности и доступности, при расчете рисков по угрозе «отказ в обслуживании», наличие антивирусного программного обеспечения учитывается отдельно.

Накладывая коэффициент защищенности на время простоя информации, получим время простоя информации, учитывая средства защиты информации. Оно рассчитывается в часах простоя в год.

Специфичный параметр для связки «информация — группа пользователей» — время простоя сетевого оборудования. Доступ к ресурсу может осуществляться разными группами пользователей с использованием разного сетевого оборудования. Для сетевого оборудования время простоя задает владелец информационной системы. Время простоя сетевого оборудования суммируется со временем простоя информации, полученным в результате работы алгоритма, таким образом, мы получаем итоговое время простоя для связи «информация — группа пользователей».

Значение времени простоя для информации (T_{inf}), учитывая все группы пользователей, имеющих к ней доступ, вычисляется по следующей формуле:

$$T_{inf} = (1 - \prod_{i=1}^{n} (1 - \frac{T_{ug,n}}{T_{max}})) \times T_{max},$$

где T_{max} — максимальное критичное время простоя;

$T_{ug,n}$ — время простоя для связи «информация — группа пользователей».

3. Задание контрмер

Для расчета эффективности введенной контрмеры необходимо пройти последовательно по всему алгоритму с учетом заданной контрмеры. То есть на выходе пользователь получает значение двух рисков — риска без учета контрмеры (R_{old}) и риска с учетом заданной контрмеры (R_{new}) или с учетом того, что уязвимость закрыта.

Эффективность введения контрмеры рассчитывается по следующей формуле:

$$E = \frac{R_{old} - R_{new}}{R_{old}}.$$

Окончательные результаты:

- риск реализации по трем базовым угрозам для вида информации;
- риск реализации по трем базовым угрозам для ресурса;
- риск реализации суммарно по всем угрозам для ресурса;

- риск реализации по трем базовым угрозам для информационной системы;
- риск реализации по всем угрозам для информационной системы;
- риск реализации по всем угрозам для информационной системы после задания контрмер;
- эффективность контрмеры;
- эффективность комплекса контрмер.

Благодаря новому расширенному алгоритму программа ГРИФ из состава Digital Security Office позволяет анализировать не только информационные потоки, но и конкретные угрозы и уязвимости информационной системы.

В результате выполнения всех действий по данным этапам на выходе будет сформирована полная модель ИС в отношении ИБ с учетом реального выполнения требований комплексной политики безопасности, что позволит перейти к программному анализу введенных данных для получения комплексной оценки рисков и формирования итогового отчета.

К недостаткам ГРИФ можно отнести отсутствие возможности добавления специфичных для организации требований политики безопасности.

Методика компании MethodWare. Компания MethodWare разработала собственную методику оценки и управления рисками и выпустила ряд соответствующих инструментальных средств. К этим средствам относятся:

1. ПО оценки и управления рисками Operational Risk Builder и Risk Advisor. Методика соответствует австралийскому стандарту Australian/New Zealand Risk Management Standard (AS/NZS 4360:1999) и стандарту ISO/IEC 17799.

2. ПО управления жизненным циклом информационной технологии в соответствии с CobiT Advisor 3rd Edition (Audit) и CobiT 3rd Edition Management Advisor. В руководствах CobiT существенное место уделяется оценке и управлению рисками.

3. ПО для автоматизации построения разнообразных опросных листов Questionnaire Builder.

В Risk Advisor реализована методика, позволяющая задать модель ИС с позиции ИБ, идентифицировать риски, угрозы, потери в результате инцидентов. Основными этапами работы являются: описание контекста, определение рисков, оценка угроз и возможного ущерба, выработка управляющих воздействий и разработка плана восстановления и действий в чрезвычайных ситуациях.

На этапе *описания контекста* характеризуется модель взаимодействия организации с внешним миром в нескольких аспектах: стратегическом, организационном, бизнес-цели, управление рисками, кри-

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

Организационный контекст описывает отношения внутри организации: стратегию, цели на организационном уровне, внутреннюю политику. Контекст управления рисками излагает концепцию ИБ. Контекст бизнес-целей — основные бизнес-цели, критерии оценки используются при управлении рисками.

Описание рисков. Задается матрица рисков на основе некоторого шаблона. Риски оценивают по качественной шкале и разделяют на приемлемые и неприемлемые. Затем выбирают управляющие воздействия (контрмеры) с учетом зафиксированной ранее системы критериев, эффективности контрмер и их стоимости. Стоимость и эффективность также оценивают в качественных шкалах.

Описание угроз. В начале формируют список угроз. Угрозы определенным образом классифицируют, затем описывают связь между рисками и угрозами. Описание также делают на качественном уровне и позволяют зафиксировать их взаимосвязи.

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

Анализ результатов. В результате построения модели можно сформировать подробный отчет (около 100 разделов), посмотреть на экране агрегированные описания в виде графа рисков.

Risk Advisor позволяет автоматизировать различные аспекты управления рисками компании. При этом оценки рисков дают в качественных шкалах. Подробный анализ факторов рисков не предусмотрен. Сильной стороной рассмотренной методики является возможность описания различных связей, адекватный учет многих факторов риска и существенно меньшая трудоемкость по сравнению с CRAMM.

Сравнительный анализ инструментальных средств оценки рисков информационной безопасности

Рассмотренные методики анализа и оценки рисков полностью применимы и в российских условиях, несмотря на то, что показатели защищенности от несанкционированного доступа (НСД) к информации и требования по защите информации различаются в российских руководящих документах и зарубежных стандартах.

В табл. 3.2 приведено сравнение рассмотренных средств оценки рисков информационной безопасности.

Таблица 3.2

Сравнение средств оценки рисков информационной безопасности

Критерий сравнения	CRAMM	ГРИФ 2006	*RiskAdvisor*	*RiskWatch*
Стандарты	BS 7799	ISO 17799, ISO 27001	AS/NZS 4360:1999, ISO 17799	ISO 17799
Возможность изменения базы данных	нет	ограничена	да	да
Качественная оценка рисков	да	да	да	нет
Количественная оценка рисков	нет	да	нет	да
Достоинства	Объемная база знаний. Основан на универсальном методе CRAMM. Наиболее «мощный» продукт для детальной оценки рисков	Невысокая трудоемкость. Интеграция с ActiveDirectory для описания архитектуры ИС	Невысокая трудоемкость. Возможность описания разноплановых взаимосвязей	Невысокая трудоемкость. Совместный анализ информационных и физических рисков. Высокая гибкость метода
Недостатки	Высокая трудоемкость. Высокая стоимость. Больше подходит для аудита уже существующих ИС. Большое количество бумажной документации, не всегда полезной на практике. Нельзя вносить изменения в базу знаний	Невозможность изменения требований политики безопасности	Подробный анализ факторов рисков не предусмотрен. Ориентирован на документацию более организационных и административных факторов, чем программно-технических	Ориентирован на документацию более программно-технических факторов, чем организационных и административных. Высокая стоимость. Необходимость наличия достоверной статистики по инцидентам

Следует отметить, что при выборе той или иной методики и программного обеспечения для оценки рисков в сфере информационной безопасности пользователь в первую очередь руководствуется следующими критериями: насколько предлагаемая методика соответствует конкретным требованиям к принятию решений; получает ли пользователь корректные ответы на свои вопросы; насколько логична методика; оценивает ли частоту угроз, размер ущерба и вероятность их возникновения; измеряет ли методика именно риски или уязвимости; предлагает ли соответствующие меры защиты.

Особенно полезным представляется использование инструментальных средств типа метода CRAMM при проведении анализа рисков ИС с повышенными требованиями в области ИБ. Это позволяет получать обоснованные оценки рисков, уязвимостей, эффективности защиты. Существенным достоинством таких методов является возможность проведения исследования в сжатые сроки, с документированием результатов. Грамотное использование метода CRAMM позволяет получать очень хорошие результаты, наиболее важным из которых является возможность экономического обоснования расходов организации на обеспечение ИБ и непрерывности бизнеса. Экономически обоснованная стратегия управления рисками позволяет, в конечном счете, экономить средства, избегая неоправданных расходов.

Использование описанного инструментария позволяет унифицировать и упростить работу с моделью ресурсов, профилями угроз, перечнями уязвимостей и рисками, использование результатов для переоценки рисков, даже если она выполнялась другими специалистами.

Программный инструментарий полезен тем, что содержит алгоритм процесса оценки рисков, что упрощает работу неопытному специалисту, однако это является основным недостатком подобных программ, так как указанный алгоритм «зашит» в программу и изменению не подлежит, т.е. не может быть адаптирован под цели конкретной организации.

Резюмируя изложенное, перечислим те преимущества, которые дает анализ и оценка рисков в сфере ИБ.

1. Возможность выявления проблем в сфере ИБ, причем не только уязвимостей компонентов системы, но и недостатков, например, политик безопасности.

2. Грамотно проведенный анализ и оценка рисков позволяют руководству организации оценить выгоды от внедрения средств и механизмов защиты и принять участие в процессе определения требуемого уровня защищенности ИС.

3. Проведение анализа и оценки рисков добавляет обоснованность рекомендациям по ИБ.

4. Ранжирование рисков позволяет выделить наиболее приоритетные направления для внедрения новых средств защиты и мероприятий по обеспечению ИБ.

5. Хорошо разработанные методики и программное обеспечение для анализа и оценки рисков позволяет специалистам, не являющимся экспертами в данной области, воспользоваться аккумулированными в методике знаниями, чтобы получить заслуживающие доверия результаты анализа.

3.3. Базовый подход к обоснованию проекта подсистемы обеспечения информационной безопасности

3.3.1. Оценка потерь от реализации потенциальных угроз и затрат на защиту информации

Первый подход к оценке потерь от реализации потенциальных угроз основан на проверке соответствия уровня защищенности ИС требованиям одного из стандартов в области ИБ. Это может быть класс защищенности в соответствии с требованиями ФСТЭК России, профиль защиты, разработанный в соответствии со стандартом ISO-15408, или какой-либо другой набор требований. Тогда критерий достижения цели в области безопасности — это выполнение заданного набора требований.

В этом случае *критерий эффективности* — минимальные суммарные затраты на выполнение поставленных функциональных требований:

$$\sum c_i \rightarrow \min,$$

где c_i — затраты на i-е средство защиты.

Основной недостаток такого подхода заключается в том, что в случае, когда требуемый уровень защищенности жестко не задан, например, через законодательные требования, определить «наиболее эффективный» уровень защищенности ИС достаточно сложно.

Второй подход к построению системы обеспечения ИБ связан с оценкой и управлением рисками. Изначально он исходит из принципа «разумной достаточности» примененного к сфере обеспечения ИБ. Этот принцип может быть описан следующим набором утверждений:

- абсолютно непреодолимую защиту создать невозможно;

- необходимо соблюдать баланс между затратами на защиту и получаемым эффектом, в том числе и экономическим, заключающимся в снижении потерь от нарушений безопасности;
- стоимость средств защиты не должна превышать стоимость защищаемой информации (или других ресурсов — аппаратных, программных);
- затраты нарушителя на НСД к информации должны превышать тот эффект, который он получит, осуществив подобный доступ.

Рассматривая ИС в ее исходном состоянии, мы оцениваем размер ожидаемых потерь от инцидентов, связанных с нарушением ИБ (как правило, берется определенный период времени, например год). После этого оцениваем влияние предлагаемых средств и мер обеспечения безопасности на снижение рисков, и их стоимость. Если представить некоторую идеальную ситуацию, то идею подхода отображает график на рис. 3.19.

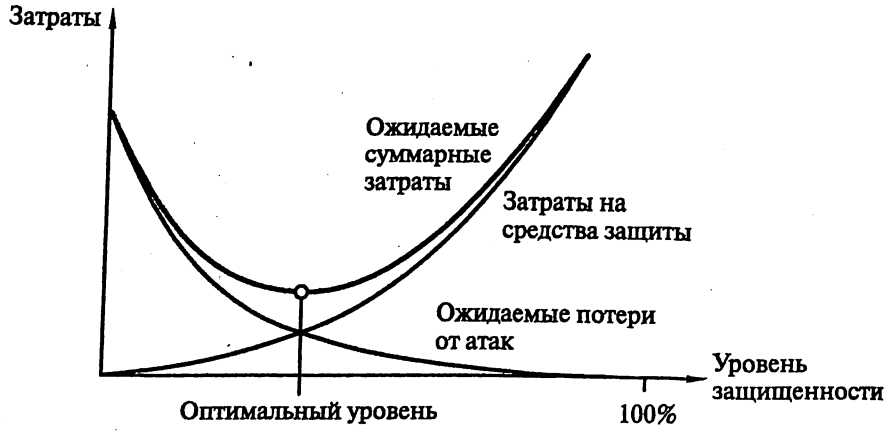


Рис. 3.19. График соотношения «затраты на защиту — ожидаемые потери»

По мере того как затраты на защиту растут, размер ожидаемых потерь падает, и если обе функции имеют вид, представленный на рисунке, то можно определить минимум функции «Ожидаемые суммарные затраты», который нам и требуется.

К сожалению, точные зависимости между затратами и уровнем защищенности определить достаточно трудно, поэтому аналитический метод определения минимальных затрат в представленном виде неприменим на практике.

3.3.2. Идентификация риска

Риск может быть идентифицирован следующим набором параметров:

- *угроза*, возможной реализацией которой вызван данный риск;
- *ресурс*, в отношении которого может быть реализована данная угроза (например, ресурс может быть информационный, аппаратный, программный);
- *уязвимость*, через которую может быть реализована данная угроза в отношении данного ресурса.

Размер ущерба от реализации угрозы в отношении ресурса зависит:

— от стоимости ресурса, который подвергается риску;

— от степени разрушительности воздействия на ресурс, выражаемой в виде коэффициента разрушительности; как правило, указанный коэффициент лежит в диапазоне от 0 до 1.

Таким образом, получаем оценку, представимую в виде произведения:

<Стоимость ресурса> × <Коэффициент разрушительности>

Далее необходимо оценить частоту возникновения рассматриваемого нежелательного события за фиксированный период и вероятность успешной реализации угрозы. В результате, стоимость риска может быть вычислена по формуле:

<Вероятность угрозы> × <Вероятность использования уязвимости для реализации угрозы> × <Стоимость ресурса> × × <Коэффициент разрушительности>

3.3.3. Модель безопасности с полным перекрытием

Модель системы безопасности с полным перекрытием строится исходя из постулата, что система безопасности должна иметь по крайней мере одно средство для обеспечения безопасности на каждом возможном пути воздействия нарушителя в отношении ИС. В модели точно определяется каждый объект, требующий защиты, оцениваются средства обеспечения безопасности в отношении их эффективности и их вклад в обеспечение безопасности всей ИС.

С каждым объектом, требующим защиты, связывается некоторое множество действий, к которым может прибегнуть нарушитель для получения несанкционированного доступа к объекту.

Множество отношений «*объект — угроза*» образуют *двудольный граф*, в котором ребро (y_i, o_j) существует тогда и только тогда, когда y_i является средством получения доступа к объекту o_j. Пример модели процесса защиты информации в виде двудольного графа приведен на рис. 3.20.

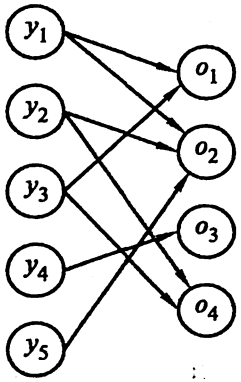


Рис. 3.20. Пример модели процесса защиты информации в виде двудольного графа

Следует отметить, что связь между угрозами и объектами не является связью типа «один к одному» — угроза может распространяться на любое число объектов, а объект может быть уязвим со стороны более чем одной угрозы. Цель защиты состоит в том, чтобы «перекрыть» каждое ребро данного графа и воздвигнуть барьер для доступа по этому пути.

В идеальном случае каждое средство защиты $m_k \in M$ должно устранять некоторое ребро (y_i, o_j). В действительности m_k выполняет функцию «барьера», обеспечивая некоторую степень сопротивления попыткам проникновения.

Набор M средств обеспечения безопасности преобразует двудольный в *трехдольный граф*. На рис. 3.21 приведен пример модели процесса защиты информации в виде трехдольного графа.

Ребра указывают на соответствующие связи между угрозами, средствами защиты и множеством объектов защиты.

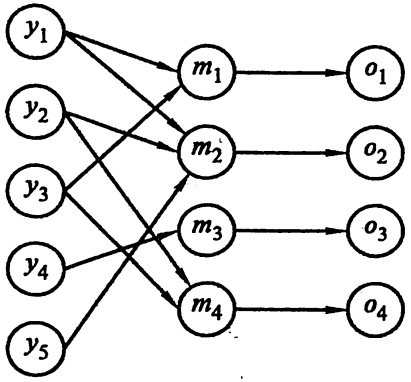


Рис. 3.21. Пример модели процесса защиты информации в виде трехдольного графа

Система обеспечения безопасности описывается в виде пятикортежного набора

$$S = \{O, Y, M, V, B\},$$

где O — набор защищаемых объектов;

Y — набор угроз;

M — набор средств обеспечения безопасности;

V — набор уязвимых мест — отображение TO на набор упорядоченных пар $V_i = (y_i, o_j)$, представляющих собой пути проникновения в систему;

B — набор барьеров — отображение $V \times M$ или $T \times O \times M$ на набор упорядоченных троек $b_i = (y_i, o_j, m_k)$, представляющих собой точки, в которых требуется осуществлять защиту в системе.

Модель системы безопасности с полным перекрытием описывает требования к составу подсистемы защиты ИС. Но в ней не рассматривается вопрос стоимости внедряемых средств защиты и соотношения затрат на защиту и получаемого эффекта. Кроме того, определить полное множество «путей проникновения» в систему на практике может оказаться достаточно сложно.

Анализ графа дает возможность оценить, все ли возможные пути реализации угроз перекрыты, и выработать рекомендации в случае отсутствия защиты каких-либо объектов. Заметим, что математический аппарат для анализа графовых структур достаточно хорошо разработан, что дает возможность проводить анализ существенно разветвленных графов. Кроме того, процесс построения и модернизации графа легко выполняется с использованием ПО.

Отметим, что рассмотренная модель безопасности с полным перекрытием применима, в основном, как инструментарий при разработке определенных политик безопасности, либо в случае построения комплексной системы защиты информации для малого предприятия, так как при большом объеме множеств Y, M и O анализ модели становится затруднительным.

Применение модели с полным перекрытием для анализа рисков информационной безопасности малого предприятия приводится в Приложении 3.1.

3.4. Пакет методологии Coras как программное обеспечение для анализа рисков информационной безопасности предприятия

Методология *Coras*, предназначенная для анализа рисков безопасности, представляет собой инструмент для моделирования рисков и угроз, используемый на протяжении всей работы. ПО использует язык *UML* (от англ. *Unified Modeling Language* — унифицированный язык моделирования) — язык графического описания для объектного моделирования в области разработки ПО. *UML* является языком широкого профиля, это открытый стандарт, использующий графические обозначения для создания абстрактной модели системы, называемой *UML*-моделью. *UML* был создан для определения, визуализации, проектирования и документирования, в основном, ПО.

В ПО используются следующие элементы, представленные в табл. 3.2.

На рис. 3.22 представлено главное окно программы.

Окно программы можно разделить на четыре области: меню (1), панель инструментов (2), области проводника (3) и построения диаграммы (4).

Меню, расположенное в верхней части главного окна программы, имеет стандартный набор команд.

Таблица 3.2

Вид	*Название на английском языке*	*Название на русском языке*
	Asset	Ценность, информация, подлежащая защите
	Stakeholder	Владелец информации
	Threat Human Accidental	Угроза непреднамеренная, человеческого происхождения
	Threat Human Deliberate	Угроза преднамеренная, человеческого происхождения
	Threat Non Human	Угроза нечеловеческого происхождения
	Threat Scenario	Сценарий угрозы
	Vulnerability	Уязвимость
	Unwanted Incident	Нежелательный инцидент
	Risk	Риск
	Treatment	Противодействие угрозе

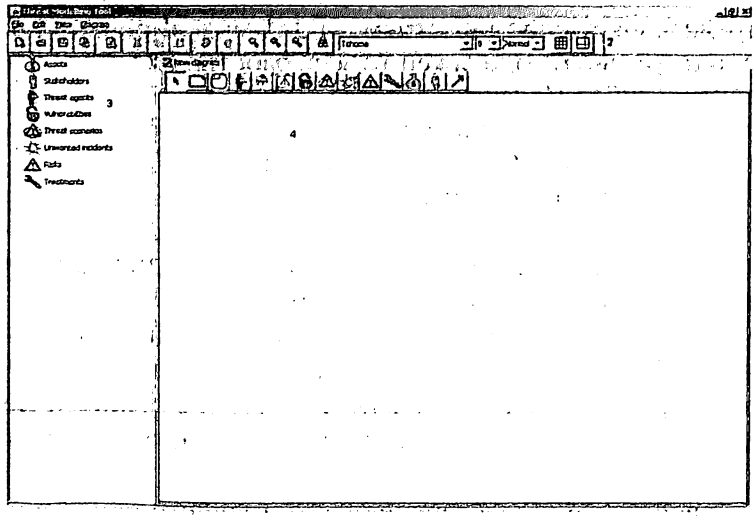


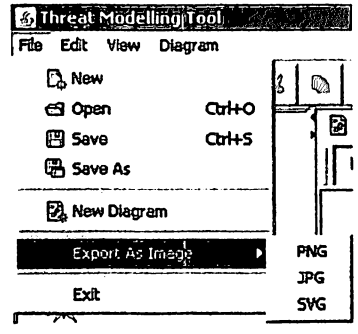
Рис. 3.22. Главное окно программы Coras

Первая половина кнопок, расположенных на панели, — дублирование действий главного меню. Далее расположена кнопка, реализующая поиск.

Поиск элемента осуществляется по его имени и типу. Также можно указать имя диаграммы. После нажатия на кнопку *Search* (Искать) в таблице, расположенной под введенными данными для поиска, отобразятся подходящие записи.

Под меню расположена панель инструментов, представленная на рис. 3.27, 3.28.

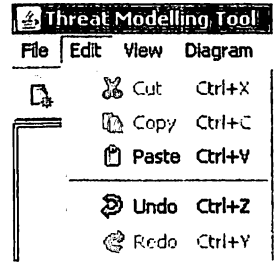
1) File/Файл



1. Создать
2. Открыть
3. Сохранить
4. Сохранить как
5. Новая диаграмма
6. Экспорт в:
   - 6.1.1. Png
   - 6.1.2. Jpg
   - 6.1.3. Svg
7. Выход

Рис. 3.23. Подменю файл

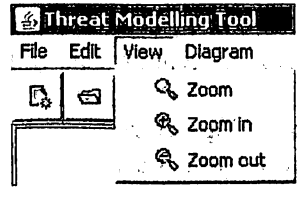
2) Edit/Редактирование



1. Удалить
2. Копировать
3. Вставить
4. Отменить
5. Повторить

Рис. 3.24. Подменю редактирование

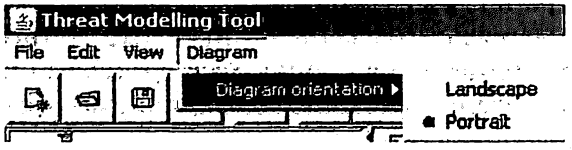
3) View/Вид



1. Масштаб 100%
2. Приблизить
3. Отдалить

Рис. 3.25. Подменю вид

4) Diagram/Диаграмма



1. Ориентация
   1.1. Альбомная
   1.2. Книжная

Рис. 3.26. Подменю диаграмма

Рис. 3.27. Кнопки главного меню и поиска

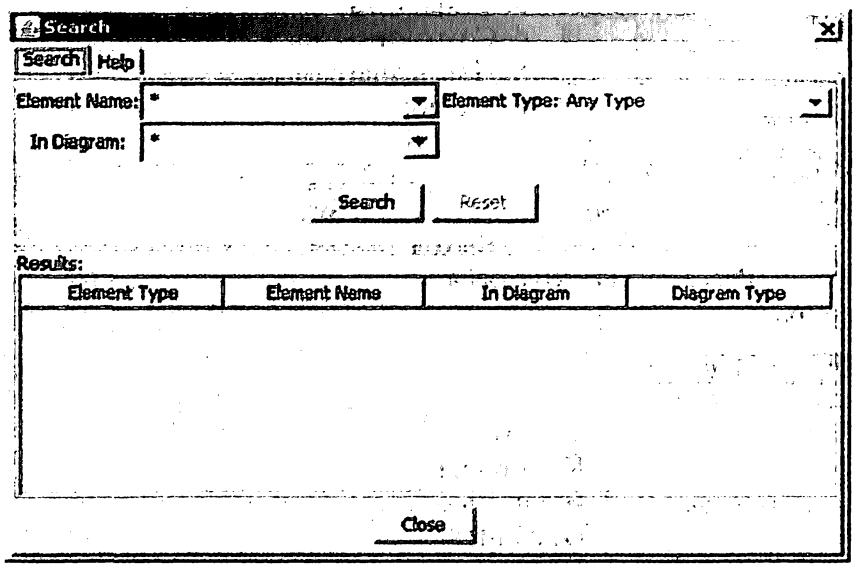


Рис. 3.28. Окно поиска

Поиск элемента осуществляется по его имени и типу. Также можно указать имя диаграммы. После нажатия на кнопку *Search* (Искать) в таблице, расположенной под введенными данными для поиска, отобразятся подходящие записи.

Шапка таблицы — условия поиска: тип элемента, его имя, название диаграммы, ее тип.

После того как поиск завершен, кнопка *Reset* (Сброс) становится активной. Нажатие на нее сбросит все введенные и найденные данные.

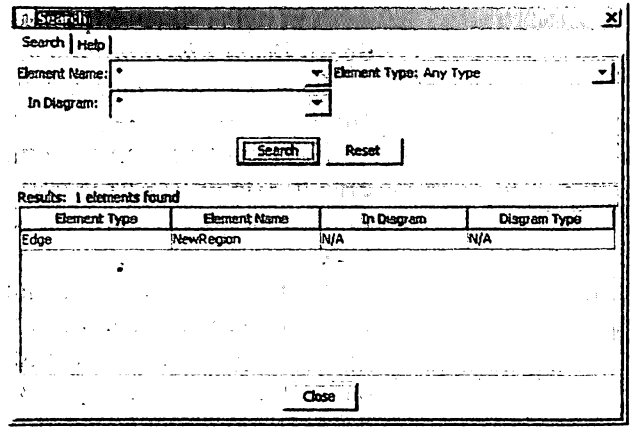


Рис. 3.29. Результаты поиска

После кнопки поиска располагается панель редактирования шрифта текста. Здесь для пользователя реализована возможность изменения шрифта, его размера и выделения: обычный (*Normal*), жирный (*Bold*), курсив (*Italic*).

Две последние кнопки, расположенные на панели инструментов (рис. 3.30), позволяют добавлять сетку на область построения диаграмм, а также отметить лист размером А4.

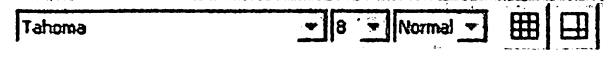


Рис. 3.30. Редактирование шрифта и страницы

Слева расположены все объекты, используемые в данной модели угроз для анализа рисков ИБ. При этом в случае добавления на лист моделирования какого-либо объекта он сразу отображается в этой схеме, представленной в виде дерева, что удобно для понимания связей, которые были установлены между объектами.

Проводник скрывается и отображается путем нажатия на стрелки, нанесенные на границу между областью построения диаграммы и самим проводником (рис. 3.32).

При создании новой диаграммы (*File/New* или кнопка *New* на панели инструментов) на области построения диаграмм появляется новая вкладка с именем по умолчанию *New diagram*.

Для изменения имени диаграммы необходимо щелкнуть правой кнопкой мыши на заголовке вкладки и выбрать *Edit diagram name* (рис. 3.33). В появившемся диалоговом окне ввести имя.

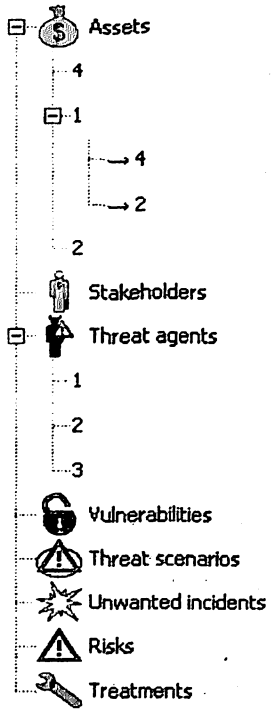


Рис. 3.31. Проводник объектов, используемых в диаграмме

Для удаления диаграммы следует выбрать *Delete diagram*.

Generate risk diagram генерирует картину рисков для данного проекта.

Панель объектов, которые непосредственно используются при моделировании, расположена на вкладке диаграммы (рис. 3.31).

Кроме перечисленных в табл. 3.2 объектов, на этой панели инструментов есть кнопка примечания (comment) для добавления подписей, разъяснений, область (region) для выделения объектов в отдельные области (например, в пределах охраняемой территории и за ее пределами). Первая стрелка служит для выделения, перемещения объектов, последняя (рис. 3.35) — для установления связей между объектами. Для того чтобы установить связь, необходимо выполнить следующие действия:

1) выбрать последнюю кнопку (стрелка) на панели инструментов диаграммы (см. рис. 3.35);

2) навести курсор на объект, являющийся началом связи. Нажать левую кнопку мыши;

3) объект начинает выделяться синим цветом;

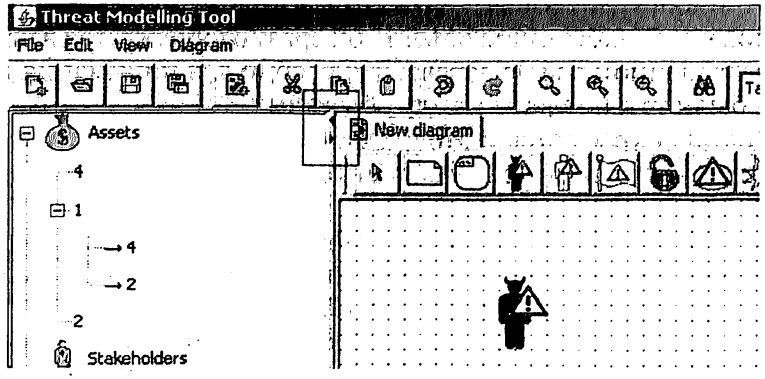


Рис. 3.32. Скрыть/отобразить проводник

4) не отпуская кнопку мыши, переводим ее на объект, являющийся окончанием связи;

5) после того как начальный объект прекратит выделяться, начнет конечный. После окончания выделения установится связь между объектами.

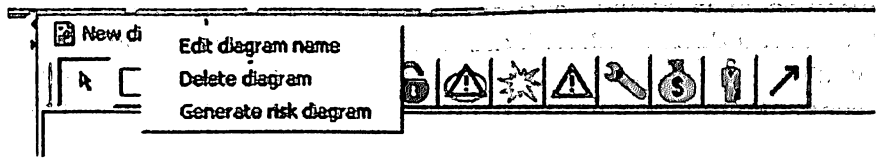


Рис. 3.33. Вкладка для работы с диаграммой

Установление связей необходимо для генерирования модели рисков.

Для того чтобы изменить имя объекта, нужно выбрать его и щелкнуть мышью, появится строка для ввода.

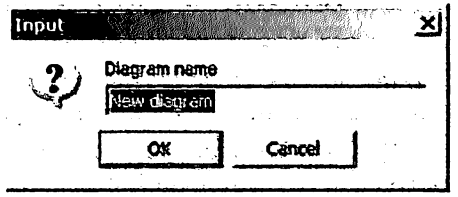


Рис. 3.34. Изменение имени диаграммы

Рис. 3.35. Панель объектов

Методология анализа безопасности Coras включает в себя семь этапов.

1. Вводная встреча. Цель — полное понимание того, что подлежит анализу (что будет анализироваться). Во время этой встречи аналитики собирают информацию, основанную на представлениях заказчика

2. Отдельная встреча с представителями заказчика. Аналитики знакомят со своим пониманием полученной на первом этапе информацией и документами, к которым заказчик открыл доступ для аналитиков. На этом этапа идентифицируются первые угрозы, уязвимости, сценарии угроз и нежелательные инциденты.

3. Третий этап включает усовершенствованное описание той ситуации, которую необходимо проанализировать, все предположения и другие сделанные предварительные условия. Он заканчивается, как только вся документация была одобрена заказчиком.

4. Четвертый этап включает в себя идентификацию всех возможных потенциальных нежелательных инцидентов, а также угроз и уязвимостей.

5. На этом этапе оцениваются последствия, которые возможны в случае осуществления нежелательных инцидентов, а также вероятность этих инцидентов.

6. Первичная полная картина рисков, которую редактируют.

7. Обоснование и описание действий, предотвращающих угрозы.

В приложении 3.2 для малого предприятия проведен анализ рисков информационной безопасности по методологии Coras с применением программного обеспечения[1].

3.5. Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартом ГОСТ Р ИСО/МЭК 27005-2010

В последние годы активно ведется работа по внедрению в систему ИБ организаций международных стандартов серии 27000, определяющих требования к системе менеджмента информационной безопасности (СМИБ). Большой популярностью в настоящее время пользуется методология анализа рисков информационной безопасности OCTAVE, разработанная институтом Software Engineering Institute (SEI) при университете Карнеги Меллона (Carnegie Mellon University).

Методика OCTAVE — это оперативная оценка критических угроз, активов и уязвимостей. Методика предполагает создание группы анализа рисков ИБ, которая включает сотрудников бизнес-подразделений, эксплуатирующих систему и сотрудников информационного отдела.

Однако данная методика не лишена некоторых недостатков. Так, методология не предусматривает интеграции анализа риска в СМИБ организации, имеются проблемы с организацией мониторинга рисков и проведением повторных оценок рисков, не предполагает механизмов управления остаточными рисками, не позволяет исключить риски.

Для анализа рисков в методике OCTAVE предлагается подход из восьми шагов, объединенных в четыре фазы (рис. 3.36).

Рабочие листы и опросные анкеты, применяемые в процессе анализа рисков, содержатся в англоязычном описании методики «Introducing OCTAVE Allegro: Improving the Information Risk Assessment Process» .

Рассмотрим обобщенный алгоритм действий группы анализа рисков, основанный на методике OCTAVE, а также рекомендации по

[1] *Bjorn, A.G.* (January 2002). CORAS, A Platform for Risk Analysis on Security Critical Systems — Model-based Risk Analysis Targeting Security (www.nr.no/coras).

внедрению в СМИБ организации оценки рисков на постоянной основе и мониторингу рисков ИБ.

На шаге 1 необходимо определить критерии оценки рисков ИБ, т.е. совокупность качественных показателей, которая позволит установить значения оценки риска и последствия реализации риска. Без введения таких критериев невозможно оценить зависимость организации от тех или иных рисков.

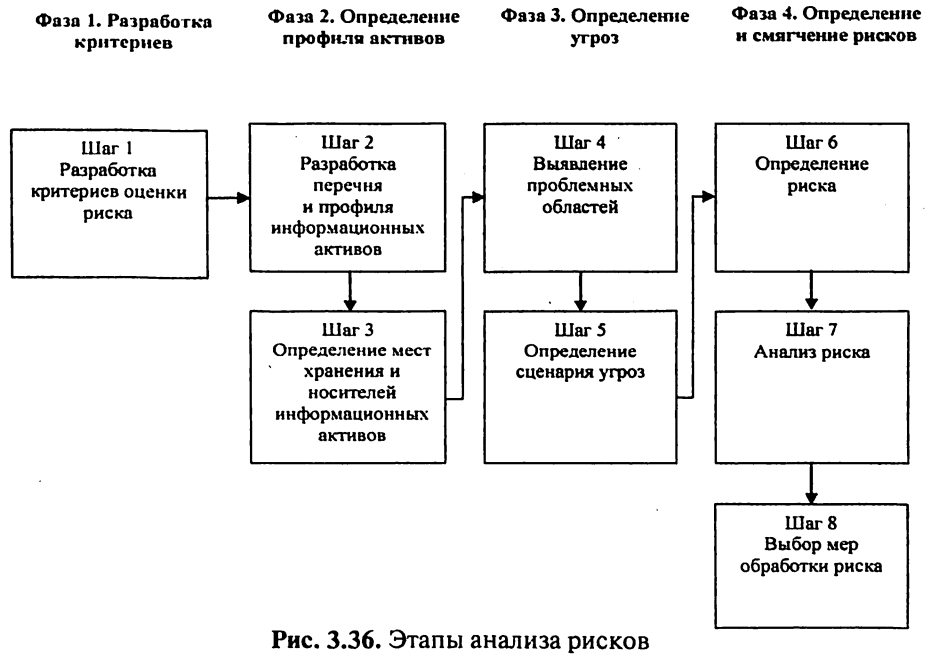


Рис. 3.36. Этапы анализа рисков по методике OCTAVE

В качестве таких критериев могут быть использованы требования безопасности, применяемые в организации, уровень инвестиций и затрат на ИБ, стратегическая ценность и критичность затронутых информационных активов и т.п. На первом шаге необходимо установить те воздействия на ИБ, которые наиболее приоритетны и критичны для организации (например, утечка конфиденциальной информации, подрыв авторитета на рынке, дискредитация фирмы среди партнеров и клиентов, угроза здоровью и физической безопасности сотрудников). Критерии оценки рисков должны отражать осознание информационных рисков, существующих в сфере деятельности организации. Критерии устанавливают диапазон последствий реализации риска: «низкие», «средние» и «высокие».

Шаг 2 начинается с составления перечня информационных активов и определения их профиля. Профиль — это информация, описывающая актив его уникальными особенностями, качествами, характеристиками, стоимостью. Профилирование позволяет четко определить «границы» актива и требования безопасности к нему. Профиль создается для каждого актива и описывается на отдельном листе. Профиль актива представляет собой входные данные для следующих шагов и служит основой для выявления угроз и рисков.

Далее выполняется шаг 3. Информационные активы могут храниться не только в самой организации, но и вне ее пределов. Например, организация может допускать к обслуживанию своей инфраструктуры другие организации — поставщики услуг. Если такой поставщик услуг не выполняет требования безопасности активов, к обслуживанию которых он допущен, то это несет риск. Риск может содержаться в самом факте хранения, передачи или обработки актива в постороннем месте. Это нарушает защиту информационного актива. Еще большую угрозу несет привлечение таким поставщиком услуг субподрядчиков, о которых владелец актива может и не знать. Таким образом, для получения адекватного профиля актива важно определить все места хранения, передачи и обработки актива, а также установить, находится ли он в зоне прямого управления организацией.

На шаге 3 группа анализа составляет карту актива, где указываются все места его хранения, передачи и обработки, которые могут стать точками уязвимости или, наоборот, точками, которые можно полностью контролировать, гарантируя защищенность актива.

Местом хранения актива может являться техническое средство, программное обеспечение, бумажный носитель или сотрудник организации. Причем люди здесь особенно важны, так как при получении защищаемой информации они становятся «контейнерами» актива. Такие риски необходимо своевременно выявлять.

На шаге 4 выявляются проблемные области в ИБ организации. Целью шага 4 является не составление полного перечня всех возможных угроз, а оперативное определение тех угроз, которые сразу очевидны для аналитика.

На шаге 5 на основе выявленных проблемных областей составляются сценарии угроз, которые визуально эффективно представлять в виде дерева, где с целью более надежного рассмотрения угроз каждая ветвь рассматривается для каждого информационного актива. Для облегчения определения сценария угроз по каждой ветви необходимо использовать опросные анкеты. Этот шаг также позволяет учесть ве-

роятности реализации угроз, что помогает на более поздних шагах разработать мероприятия по снижению риска. Как правило, в этом случае используется качественная шкала и вводятся три уровня вероятности реализации угрозы: «низкая», «средняя» и «высокая».

На шаге 6 после определения угроз и выявления последствий их реализации определяют риски ИБ. Необходимо определить, как именно риск будет воздействовать на организацию или актив, при этом риск определяется для каждого актива, чтобы оценить его критичность для организации или самого актива.

На шаге 7 определяется количественная мера ущерба, который будет нанесен организации при реализации угрозы. Это относительная оценка, которая позволяет расставить риски по их приоритету. Например, если для компании наиболее важна ее репутация на рынке, то в первую очередь надо смягчать риски именно в этой проблемной области.

На заключительном шаге выбираются меры обработки определенных рисков с учетом их приоритета для организации.

Решение о принятии, уменьшении или отложении риска основывается на ряде факторов, основными из которых являются величина воздействия риска и вероятность его реализации. Если риск может серьезно воздействовать на организацию, но при этом маловероятен, то, возможно, его не нужно смягчать. Решение о том, какие риски смягчать, а какие нет, должны принимать аналитики и/или руководство организации.

Выбор стратегии смягчения риска — сложная задача, и ее решение может потребовать взаимодействия с другими специалистами организации. Выбранная стратегия должна гарантировать защиту активов в соответствии с критериями безопасности. Необходимо учитывать затраты на смягчение риска, так как они, как минимум, не должны превышать стоимость актива.

Кроме того, не все риски могут быть устранены полностью. Выбранная стратегия может привести к остаточному риску, который необходимо либо принять, либо смягчить.

Оценку рисков ИБ необходимо проводить на постоянной основе, при этом проводить ее рекомендуется не менее чем раз в год. Это связано с быстрым развитием информационных технологий и как следствие — с возникновением новых рисков ИБ, возможным устареванием и исключением некоторых ранее принятых рисков или потерей эффективности мер, принятых ранее. Риски ИБ необходимо регулярно отслеживать, для чего целесообразно внедрять систему мониторинга рисков. Для этого, помимо ежегодного повторного анализа рисков, необходимы следующие мероприятия:

1. На постоянной основе проводить с работниками разъяснительную работу по угрозам ИБ, которые могут нести те или иные уязвимости, привлекать их к процессу ежегодной оценки рисков, анализировать информацию, полученную от них.

2. Установить единые правила поведения сотрудников на рабочих местах, требовать их выполнения, прививать работникам культуру ИБ. К данному вопросу следует подойти с особым вниманием, чтобы при внедрении таких правил не нарушить права работников.

3. Сравнивать результаты работы, фигурирующие в отчетах и докладах, с текущим положением дел, а также с информацией, поступающей от других источников, проводить дополнительные проверки в случае несоответствия.

4. Обмениваться информацией с регулирующими государственными органами по вопросам соблюдения законодательства и прочим вопросам, которые отражают функционирование процесса управления рисками.

5. Обмениваться информацией с заказчиками и клиентами по вопросам защиты конфиденциальных данных.

6. К процессу оценки рисков привлекать сотрудников организации.

7. При ежегодном анализе рисков частично менять состав группы анализа из числа работников организации, что позволит взглянуть на риски «свежим взглядом», а также усилит культуру ИБ среди сотрудников.

8. Тщательно документировать каждый процесс анализа рисков.

Предлагаемые меры позволят своевременно реагировать на вновь возникающие угрозы, а также отсеивать из рассмотрения те угрозы, которые по тем или иным причинам потеряли свою актуальность.

Далее рассмотрим на сколько предлагаемая процедура анализа рисков соответствует требованиям линейки международных стандартов ИСО/МЭК серии 27000.

В общем виде соответствие предлагаемой процедуры применения методологии OCTAVE стандартам серии ИСО/МЭК 27000–27005 отображено в табл. 3.3[1].

Стандарты серии ИСО/МЭК 27000–27005 устанавливают четкие требования к оценке рисков как к процессу в целом, так и к его этапам по отдельности. Предложенные процедуры методологии OCTAVE позволяют соблюсти данные требования.

[1] *Баранова Е. К., Забродоцкий А.С.* Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии ИСО/МЭК 27000-27005 // Вестник Московского университета им. С.Ю. Витте. Серия 3: Образовательные ресурсы и технологии. — 2015. — № 3(11). — С. 73–77.

Таблица 3.3

Соответствие стандартам серии ИСО/МЭК 27000-27005

Требование	Ссылка на стандарт		Соответствие в процедуре
	стандарт	пункт	
Определение критериев приемлемости или неприемлемости рисков	27001	4.2.1	Шаг 1
	27002	4.1	
	27003	8.1	
	27005	7.2	
Определение активов	27001	4.2.1	Шаги 2 и 3
	27005	8.2.1.2	
Определение угроз и их источников	27001	4.2.1	Шаг 4
	27003	8.1	
	27005	8.2.1.3	
Определение уязвимостей	27001	4.2.1	Шаг 5
	27003	8.1	
	27005	8.2.1.5	
Оценка вероятности сценариев	27001	4.2.1	Шаг 5
	27003	8.1	
	27005	8.2.2.3	
Определение последствий	27001	4.2.1	Шаг 5
	27003	8.1	
	27005	8.2.1.6	
Оценка влияния инцидентов ИБ	27001	4.2.1	Шаг 6
	27003	8.1	
Оценка уровня риска	27001	4.2.1	Шаг 7
	27005	8.2.2.5	
Обработка риска	27001	4.2.1	Шаг 8
	27002	4.2	
	27003	8.1	
	27005	8.2.2	
Мониторинг рисков ИБ	27001	4.2.3	Мониторинг
	27005	12	

3.6. Управление инцидентами информационной безопасности

3.6.1. Процесс управления инцидентами информационной безопасности

Информационная безопасность любой организации в первую очередь направлена на уменьшение рисков, связанных с информационными ресурсами. Конечным результатом обеспечения ИБ является предотвращение или минимизация ущерба от вероятных угроз или инцидентов ИБ и, таким образом, получение выигрыша для всего бизнес-процесса организации. Для достижения данного результата в организациях, как правило, созданы подразделения информационной безопасности, которые занимаются защитой информационных ресурсов. Однако не стоит забывать о том, что вероятность возникновения инцидентов ИБ существует всегда, и даже самый совершенный комплекс мер по защите информации не может гарантировать возникновение в информационной среде событий, потенциально несущих угрозу всему бизнес-процессу. Неготовность организации к пониманию этого вопроса и своевременному его решению может сильно «ударить» по бизнесу и существенно повысить величину причиненного ущерба. У организаций, которые понимают степень важности этой проблемы, возникают вопросы, связанные с ИБ, а именно:

- с чего стоит начинать процесс управления инцидентами?
- как обеспечить взаимодействие между структурными подразделениями организации и оценивать эффективность их работы?

Для решения этих вопросов руководителям организаций или специалистам по обеспечению ИБ разумно реализовать комплексный подход к решению следующих задач:

1) определение, оповещение и регистрация инцидентов ИБ;

2) реагирование на инциденты ИБ и применение превентивных мер защиты для устранения причин потенциального ущерба;

3) расследование или анализ инцидентов с целью предотвращения повторного их проявления.

Решить эти задачи можно путем разработки и реализации эффективного процесса управления инцидентами.

Тема управления инцидентами информационной безопасности на сегодняшний день является одной из наиболее обсуждаемых и актуальных для организаций. Это связанно с тем, что управление инцидентами ИБ является важнейшим процессом развития и совершенствования всей системы управления информационной безопасности (СУИБ).

Именно процесс управления инцидентами ИБ позволяет определить конкретные уязвимости ИБ организации, обнаружить следы атак и вторжений в информационную среду компании, что, в свою очередь, дает информацию о слабостях в системе защиты информации. Таким образом, управление инцидентами ИБ позволяет оценить эффективность СУИБ, определить ключевые роли персонала в результате возникновения нештатных ситуаций и, главное, за минимальный промежуток времени принять необходимые меры для восстановления полноценной работы компании.

Как показывает практика, необходимость своевременного выявления инцидентов и реагирования на них обусловлена тем, что на карту поставлены не только конфиденциальность, целостность и доступность информации, а прежде всего репутация и финансы, которых может лишиться компания, не идентифицировав инцидент, о котором сигнализировали средства защиты.

В рамках управления инцидентами ИБ различают два взаимосвязанных понятия — это *событие ИБ* и собственно сам *инцидент ИБ*.

Событие ИБ — это идентифицированный случай состояния системы или сети, который указывает на возможное нарушение политики информационной безопасности или отказ средств защиты либо ранее неизвестная ситуация, которая может быть существенной для безопасности (см. ГОСТ Р ИСО/МЭК ТО 18044-2007 «Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»).

Событие ИБ характеризуется рядом параметров, которые определяют его возникновение (рис. 3.37).

Событие представляет собой логическую связь между действием и объектом, на который направленно данное действие, и результатом действия. Иногда возникающие события являются частью шагов, предпринимаемых злоумышленником для получения какого-либо несанкционированного результата. Эти события можно рассматривать как часть инцидента ИБ. Если событие возникает вновь и может нанести ущерб организации, то такое событие нужно считать инцидентом ИБ.

Инцидент ИБ — это возникновение одного или нескольких нежелательных или непредвиденных событий ИБ, в результате которых велика вероятность компрометации бизнес-процессов и угрозы ИБ для организации (см. ГОСТ Р ИСО/МЭК ТО 18044-2007).

Принимая во внимание тот факт, что событие может являться частью инцидента ИБ, схема его возникновения будет выглядеть следующим

образом (рис. 3.38). Инцидент включает в себя такие элементы, как злоумышленник; цели, на достижение которых направлена его деятельность; используемые методы и средства; действия и объекты, на которые направлены эти действия.

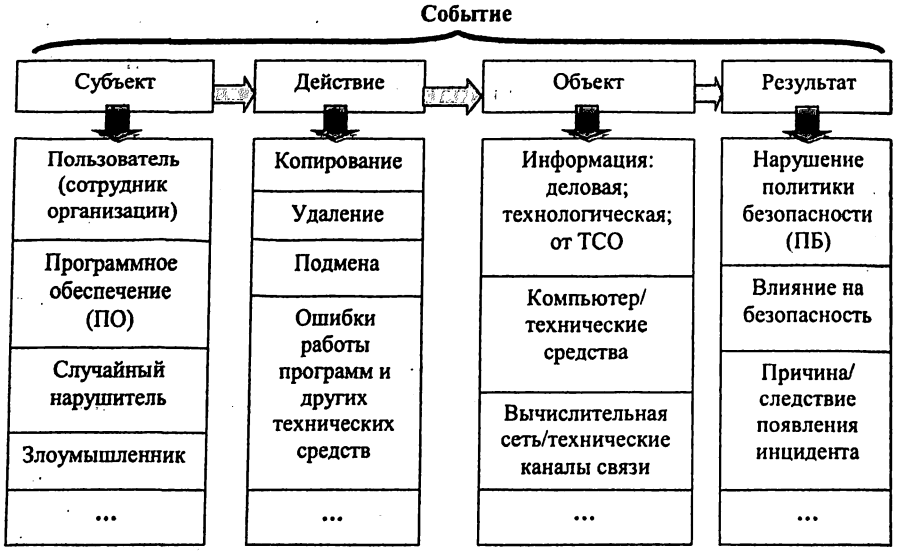


Рис. 3.37. Событие информационной безопасности

Возникновение инцидентов ИБ может быть преднамеренным (осуществляет злоумышленник) или случайным (ошибки программного обеспечения, ошибки персонала, природные явления и т.д.) и может вызываться как техническими, так и физическими средствами. Несмотря на тот факт, что случайные инциденты менее опасны, чем преднамеренные управлять ими нужно в одинаковой степени, так как даже из-за случайных ошибок возможно нарушение непрерывности основных бизнес-процессов.

На рис. 3.38 видно, что субъект, преднамеренно совершающий инцидент ИБ, преследует определенные цели, на достижение которой направлены все его действия. В процессе совершения инцидента субъект использует определенные методы и средства, которые при успешном выполнении позволяют ему добиться желаемых результатов. При случайном возникновении инцидента не подразумеваются никакие определенные цели, методы и средства, поэтому применение этой схемы целесообразно только для преднамеренного возникновения инцидента ИБ. Для описания случайного возникновения инцидент стоит рассматривать как совокупность событий ИБ.

На сегодняшний день в организациях обычно выделяют только компьютерные инциденты, однако, как мы уже сумели убедиться, понятие инцидента очень многогранное. В связи с этим целесообразнопривести классификацию инцидентов ИБ:

- *компьютерные* — связаны с обработкой информации в автоматизированных системах;
- *технические* — здесь подразумевается выход/вывод из строя аппаратных средств;
- *организационные* — связанные с деятельностью всего персонала компании;
- *технологические* — процессы производства, нарушение работоспособности технологических элементов и т.п.

Рис. 3.38. Инцидент информационной безопасности

Технологические инциденты наиболее критичны на предприятиях топливно-энергетического комплекса (например, в нефтяных компаниях) или предприятиях технологического производства. Для всех остальных организаций можно ограничиться анализом первых трех групп.

Примерами компьютерных инцидентов являются отказ в обслуживании системы; заражение вирусами; несанкционированный доступ к информации и т.д.

Под организационными инцидентами подразумеваются халатность работников фирмы; несоблюдение правил политики информационной безопасности; нарушение правил трудового распорядка и др.

В качестве примеров технических инцидентов можно выделить следующие: выход из строя жесткого диска (HDD); неработоспособность флэш-накопителей и т.д.

Управление инцидентами — это процесс, который отвечает за управление жизненным циклом всех инцидентов. Основная цель управления инцидентами — это скорейшее возобновление прерванной работы для пользователей. Кроме того, процесс управления инцидентами должен осуществлять точную регистрацию всех инцидентов для оценки и совершенствования процесса управления и предоставления необходимой информации для других процессов.

В общем виде процесс управления инцидентами может быть представлен следующим образом (рис. 3.39).

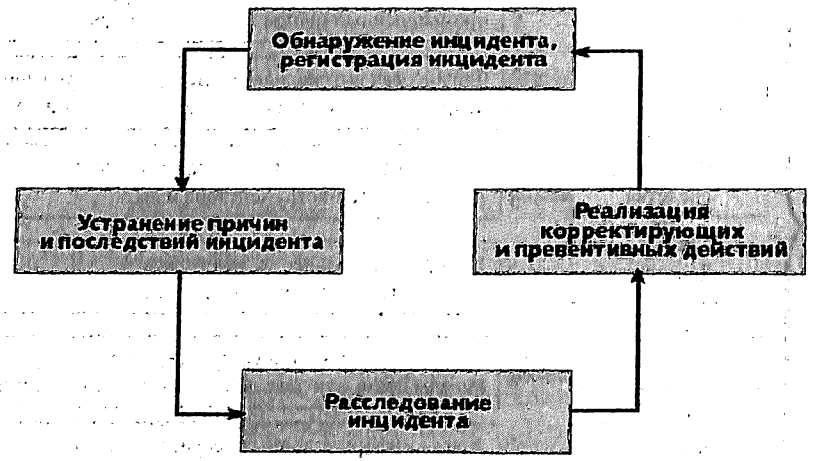


Рис. 3.39. Процесс управления инцидентами ИБ

В зависимости от вида инцидента необходимо выставить приоритет по степени реагирования на него. Логично предположить, что в первую очередь должны устраняться технологические инциденты, затем компьютерные, организационные и технические инциденты, но эта последовательность не всегда такова. Стоит отметить, что технологические инциденты решаются не IT-службой компании, поэтому для объективного определения приоритета вводятся следующие критерии:

- степень воздействия инцидента на бизнес-процесс, т.е. степень отклонения от нормального уровня работоспособности;

- срочность инцидента, т.е. приемлемая задержка разрешения инцидента для пользователя или бизнес-процесса.

Для каждого приоритета определяются количество специалистов и объем ресурсов, которые могут быть направлены на разрешение инцидента. Порядок разрешения инцидентов, имеющих одинаковый приоритет, может быть определен в соответствии с усилиями, необходимыми для его устранения. Например, легко устраняемый инцидент может быть разрешен прежде инцидента, который требует больших усилий для устранения.

Рассмотрим этапы процесса управления инцидентами в соответствии с ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».

1. Планирование и подготовка управления инцидентами ИБ

Очевидно, что данный этап является подготовительным и предназначен для организации и регламентирования деятельности по реагированию на инциденты. На данном этапе необходимо:

- обеспечить людские и материальные ресурсы для восстановления работы;
- создать схему реагирования на инциденты;
- составить и утвердить ряд организационно-регламентирующих документов в области управления инцидентами;
- ознакомить персонал с нормативными документами, обозначить ответственность за несоблюдение и провести обучение согласно разработанной схеме реагирования на инциденты;
- провести тестирование схемы реагирования на инциденты ИБ;
- назначить группу людей ответственных в расследовании и устранении инцидентов;
- составить перечень возможных инцидентов;
- создать единую базу данных (БД) всех возникающих инцидентов.

2. Использование или эксплуатация

Данный этап должен выполнять функции схемы по реагированию на инциденты:

- обнаружение инцидента;
- регистрация инцидента — запись в базу данных и составление отчета, который должен включать в себя идентификатор инцидента, время обнаружения, влияние инцидента на бизнес-процесс, приоритет инцидента, имя сотрудника, обнаружившего инцидент и его обязанности, описание возникшей проблемы, метод обратной связи;

- оповещение службы реагирования о возникновении инцидента на предприятии;
- предварительный анализ инцидента (выполняется сопоставление возникшего инцидента с уже случившимися ранее инцидентами, проверяется наличие возможного решения или обходного пути, также выявляются причины возникновения инцидента);
- обновление базы данных (приоритет инцидента, его статус, необходимое время на его устранение, контактные данные группы поддержки, которая приняла уведомление об инциденте, действия, осуществленные для разрешения инцидента, время и дата его закрытия);
- реагирование на инцидент (устранение последствий и причин возникновения инцидента).

3. Анализ

На данном этапе проводится углубленный анализ инцидента, на основе которого выдаются рекомендации по улучшению всего процесса обеспечения информационной безопасности и процесса управления инцидентами. Составляется отчет, содержащий в себе всю информацию об инциденте.

4. Улучшение

- реализация составленных рекомендаций по улучшению процесса обеспечения ИБ;
- тестирование модернизированной системы.

На первый взгляд может показаться, что управление инцидентами весьма сложный процесс, с точки зрения его разработки, так как требуется выполнить множество действий для его реализации. В свою очередь, точное следование данным этапам позволяет выстроить эффективный процесс, который позволит в кратчайшие сроки разрешить возникшие трудности и восстановить процесс работы (рис. 3.40).

На рис. 3.40 реагирование и устранение инцидентов представляет собой слаженное взаимодействие процессов, необходимых для эффективного управления инцидентами в компании. Схема детально отражает структуру разумной организации системы по управлению инцидентами ИБ.

Ведение эффективного процесса управления инцидентами возможно только в том случае, если в организации четко определены роли и обязанности сотрудников, связанных с реализацией данного процесса.

В таких случаях лучше всего применять ролевой подход для назначения обязанностей (табл. 3.4).

Таблица 3.4

Определение должностных обязанностей

№	Должность	Роль	Обязанности
1	Менеджер по ИБ	Руководитель группы по управлению инцидентами и связующее звено с отделом по ИБ	1. Разработка плана управления инцидентами на предприятии. 2. Координация действий персонала для эффективного реагирования на инциденты. 3. Реализация комплекса мер по устранению инцидентов.
2	Служба реагирования на инциденты ИБ	Служба, занимающаяся вопросами ликвидации инцидента	1. Реагирование на инцидент. 2. Выполнение комплексного анализа возникающих инцидентов. 3. Осуществление процесса устранения инцидентов.
3	Специалист по обеспечению информационной безопасности	Сотрудник отдела информационной безопасности	1. Выявление причин возникновения инцидента ИБ. 2. Выдача рекомендаций по улучшению системы обеспечения ИБ (СУИБ). 3. Модернизация СУИБ.

Процесс управления инцидентами требует от персонала и службы по обеспечению информационной безопасности четкой и слаженной работы. Не стоит забывать о том, что успешное функционирование любого процесса на предприятии на 90% зависит от персонала. Поэтому в обязательном порядке нужно проводить обучение персонала в области реагирования на инциденты, тестировать разработанную схему реагирования и восстановления. Это необходимо для того, чтобы ни один возникающий инцидент не остался незамеченным и не превращался в катастрофу для сотрудников организации. Также стоит внимательно расследовать и применять меры по устранению для каждого возникшего инцидента за минимальный период времени. Эффективное управление инцидентами ИБ снижает вероятность их повторного возникновения и, как следствие, минимизирует ущерб, причиненный ими.

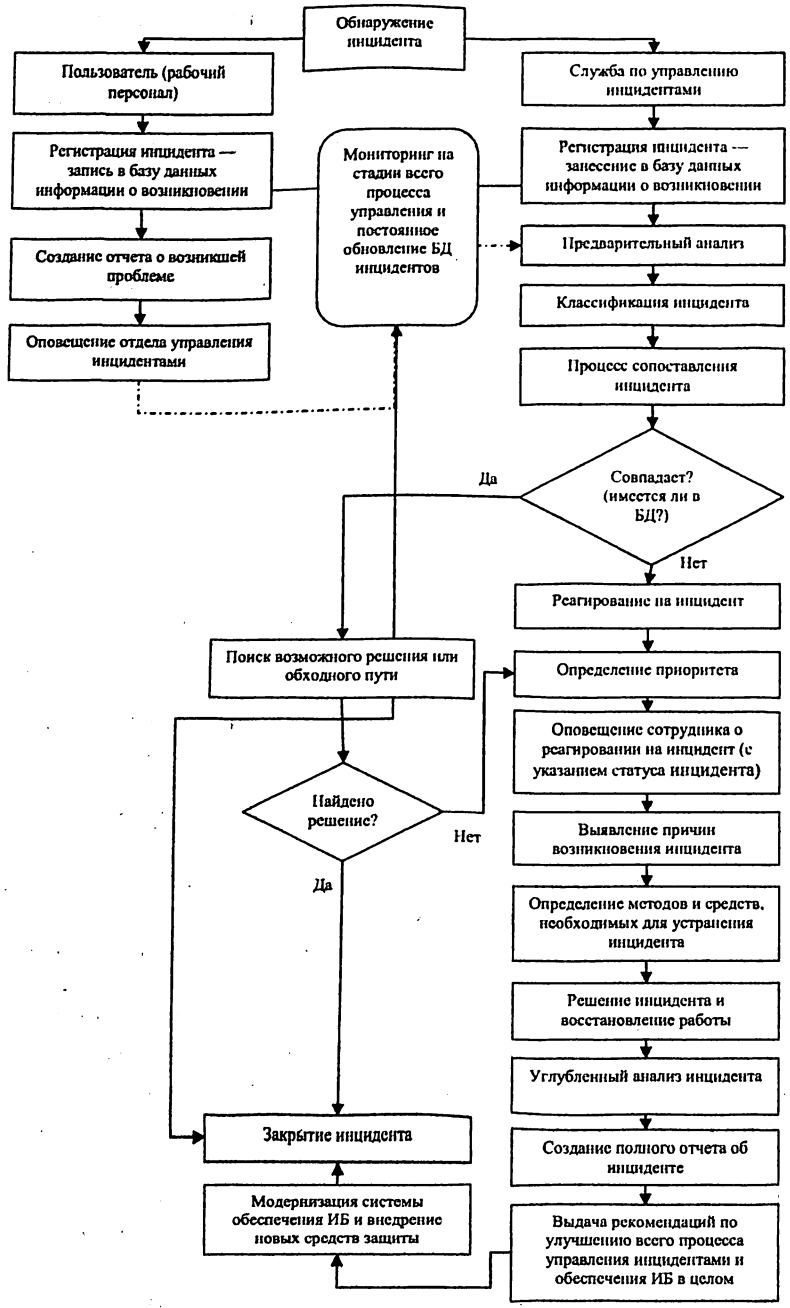


Рис. 3.40. Реагирование и устранение инцидентов

3.6.2. Организация центра управления событиями информационной безопасности

Центр управления событиями информационной безопасности (Security Operations Center, SOC) представляет собой комплекс процессов и программно-аппаратных средств, предназначенных для централизованного сбора и анализа информации о событиях и инцидентах ИБ, поступающих из различных источников IT-инфраструктуры, и своевременное реагирование на них.

Мониторинг событий информационной безопасности — процесс постоянного наблюдения за событиями ИБ с целью своевременного выявления действий в информационных системах, которые привели либо могут привести к реализации угроз информационной безопасности, и реагирования на них[1].

Одним из наиболее популярных решений последних лет для контроля и выявления инцидентов является SIEM-система (Security Information and Event Management). Популярность SIEM прежде всего обусловлена значительным объемом задач, которые можно решить с помощью SIEM-системы:

- сконцентрировать инциденты, фиксируемые другими системами самостоятельно, в рамках единого ядра инцидент-менеджмента;
- получить удобный инструмент для поиска необходимых событий, разбора инцидентов, хранения собранных данных о событиях и инцидентах ИБ;
- выявлять статистические отклонения и медленно развивающиеся инциденты за счет анализа больших интервалов и объемов информации с конкретных средств защиты;
- сопоставлять и коррелировать данные из разных систем и как следствие строить сложные цепочки сценариев по обнаружению инцидентов, «обогащать» информацию в логах одних систем данными из других.
- SIEM-системы появились в результате эволюционного развития и последующего слияния систем SEM и SIM. *SEM* (*Security Event Management*) — системы, действующие в режиме, приближенном к реальному времени. Для этого им требуются автоматический мониторинг событий, их сбор, корреляция, генерация предупреждающих сообщений. *SIM* (*Security Information Management*) анали-

[1] Организация SECURITY OPERATION CENTER (SOC) // ЗАО НИП «ИНФОРМЗАЩИТА». URL: http://docplayer.ru/46349479-Organizaciya-security-operation-center-soc.html.

зируют накопленную статистическую информацию о различных отклонениях от «нормального поведения» системы и т.д. Когда же возможности *SIM* и *SEM* объединяются в рамках одного продукта, говорят о SIEM-системах.

Принцип работы SIEM заключается в том, что система собирает информацию, анализирует «на лету» и генерирует предупреждающее сообщение, записывает информацию в базы данных, анализирует поведение на основании предыдущих наблюдений и также генерирует предупреждающее сообщение.

Основной целью построения и функционирования *SIEM*-систем является значительное повышение уровня информационной безопасности в информационно-телекоммуникационной инфраструктуре за счет обеспечения возможности в режиме, близком к реальному времени, манипулировать информацией о безопасности и осуществлять проактивное управление инцидентами и событиями безопасности. «Проактивный» означает «действующий до того, как ситуация станет критической». Предполагается, что проактивное управление инцидентами и событиями безопасности основывается на автоматических механизмах, которые используют информацию о предыстории анализируемых сетевых событий и прогнозе будущих событий, а также на автоматической подстройке параметров мониторинга событий к текущему состоянию защищаемой системы.

Для достижения заявленной цели SIEM-система должна обладать возможностью успешного решения следующего комплекса задач[1]:

- сбора, обработки и анализа событий безопасности, поступающих в систему из множества гетерогенных источников;
- обнаружения в режиме реального времени атак и нарушений критериев и политик безопасности;
- оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов;
- анализа и управления рисками информационной безопасности;
- проведения расследований инцидентов;
- обнаружения расхождения критически важных ресурсов и бизнес-процессов с внутренними политиками безопасности и приведение их в соответствие друг с другом;
- принятия эффективных решений по защите информации;

[1] *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН). — СПб.: 2012. Вып. 20, С. 27–56.

- формирования отчетных документов.

Содержание основных механизмов функционирования SIEM-системы можно представить в виде трех уровней иерархии: *сбор данных*; *управление данными*; *анализ данных* о событиях и инцидентах информационной безопасности.

На уровне сбора данных выполняется их нормализация. *Нормализация* означает приведение форматов записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки.

На уровне управления данными осуществляется фильтрация, классификация, агрегация, корреляция и приоритизация. *Фильтрация* событий безопасности заключается в удалении избыточных событий из поступающих в систему потоков. *Классификация* позволяет для атрибутов событий безопасности определить их принадлежность определенным классам. *Агрегация* объединяет события, схожие по определенным признакам. *Корреляция* выявляет взаимосвязи между разнородными событиями, что позволяет обнаруживать атаки, а также нарушения критериев и политик безопасности. *Приоритизация* определяет значимость и критичность событий безопасности на основании правил, определенных в системе.

На уровне анализа данных выполняется анализ событий и инцидентов, генерация отчетов и предупреждений, принятие решений и визуализация. *Анализ событий, инцидентов и их последствий* включает процедуры моделирования событий, атак и их последствий, анализа уязвимостей и защищенности системы, определения параметров нарушителей, оценки риска, прогнозирования событий и инцидентов. *Генерация отчетов и предупреждений* означает формирование, передачу, отображение и/или печать результатов функционирования. *Принятие решений* определяет выработку мер по реконфигурированию средств защиты с целью предотвращения атак или восстановления безопасности инфраструктуры. *Визуализация* предполагает представление в графическом виде данных, характеризующих результаты анализа событий безопасности и состояние защищаемой системы и ее элементов.

Представленная на рис. 3.41 схема реализации SIEM включает следующие компоненты: агенты (обеспечивают сбор данных из различных источников); серверы-коллекторы (аккумулируют информацию, поступающую от агентов); сервер баз данных (обеспечивает хранение информации); сервер корреляции (анализирует информацию).

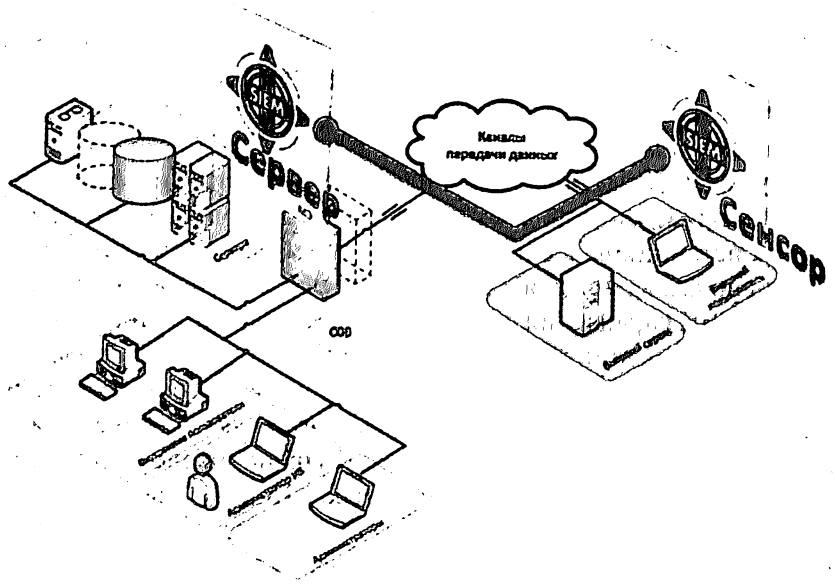


Рис. 3.41. Схема реализации SIEM

Входной информацией для *SIEM*-систем могут служить практически любые данные о функционировании системы. Как указывалось выше, сбор данных может осуществляться с помощью специальных программных агентов, которые локально собирают журналы событий и, по возможности, передают их на сервер. Для «вычитки» того или иного источника данных агент использует коллекторы — библиотеки, играющие важную роль, так как разные источники могут именовать одно и то же событие по-разному («проблема синонимов»). Коллекторы помогают привести все эти события к однозначному толкованию.

SIEM-системы могут использовать для сбора входной информации следующие источники:

- *Access Control Authentication* — применяются для мониторинга контроля доступа к информационным системам и использования привилегий;
- *DLP-системы* — поставляют сведения о попытках инсайдерских утечек, нарушении прав доступа;
- *IDS/IPS-системы* — несут данные о сетевых атаках, изменениях конфигурации и доступа к устройствам;

- *Антивирусные приложения* — генерируют события о работоспособности ПО, базах данных, изменении конфигураций и политик, вредоносном коде;
- *Журналы событий серверов и рабочих станций* — применяются для контроля доступа, обеспечения непрерывности, соблюдения политик информационной безопасности;
- *Межсетевые экраны* — содержат сведения об атаках, вредоносном ПО и пр.;
- *Сетевое активное оборудование* — используется для контроля доступа, учета сетевого трафика;
- *Сканеры уязвимостей* — предоставляют данные об инвентаризации активов, сервисов, программного обеспечения, уязвимостях и топологической структуре;
- *Системы инвентаризации и asset-management* — поставляют данные для контроля активов в инфраструктуре и выявления новых активов;
- *Системы веб-фильтрации* — предоставляют данные о посещении сотрудниками подозрительных или запрещенных веб-сайтов.

SIEM-системы способны выявлять сетевые атаки во внутреннем и внешнем периметрах; вирусные эпидемии или отдельные вирусные заражения; попытки несанкционированного доступа к конфиденциальной информации; мошенничество; ошибки и сбои в работе информационных систем; уязвимости; ошибки конфигураций в средствах защиты и информационных системах; целевые атаки (APT, Advanced Persistent Threat — «развитая устойчивая угроза»).

В компаниях с развитой IT-инфраструктурой и большим количеством разнообразных средств защиты без специализированных технических средств выстроить полную картину нарушений в системе ИБ весьма проблематично. Кроме того, внедряемые средства защиты направлены лишь на снижение вероятности возникновения инцидентов ИБ. В случае если инцидент произошел, без оперативного вмешательства в процесс ликвидации его последствий ущерб может быть весьма серьезным. Поэтому важно своевременно реагировать на выявляемые в ходе мониторинга инциденты.

Без постоянного мониторинга состояния ИБ, оперативного реагирования на инциденты, управления уязвимостями и контроля выполнения требований законодательства, нормативных актов и внутренних корпоративных политик, компаниям довольно сложно быстро и качественно проверять состояние требуемого уровня безопасности, а также поддерживать ИБ на должном уровне.

Можно выделить несколько предпосылок для создания *SOC* — центра управления событиями информационной безопасности:

- постоянно развивающаяся IT-инфраструктура;
- большое количество активных средств защиты информации;
- отсутствие единой картины происходящего в IT-инфраструктуре;
- невозможность оценить эффективность текущих мер защиты информации;
- невозможность своевременного реагирования на инциденты ИБ;
- отсутствие сквозного процесса между IT, ИБ и бизнесом;
- необходимость выполнения требований стандартов.

SIEM-система является ядром любого SOC. Система управления (мониторинга) событиями ИБ реализует комплексный подход к решению задач сбора, анализа, корреляции и контроля событий ИБ, поступающих от различных средств защиты. На рынке систем управления событиями ИБ представлены технические решения различных производителей. Они отличаются по функционалу, спектру решаемых задач, сфере применения[1]. Базовые компоненты SOC представлены на рис. 3.42.

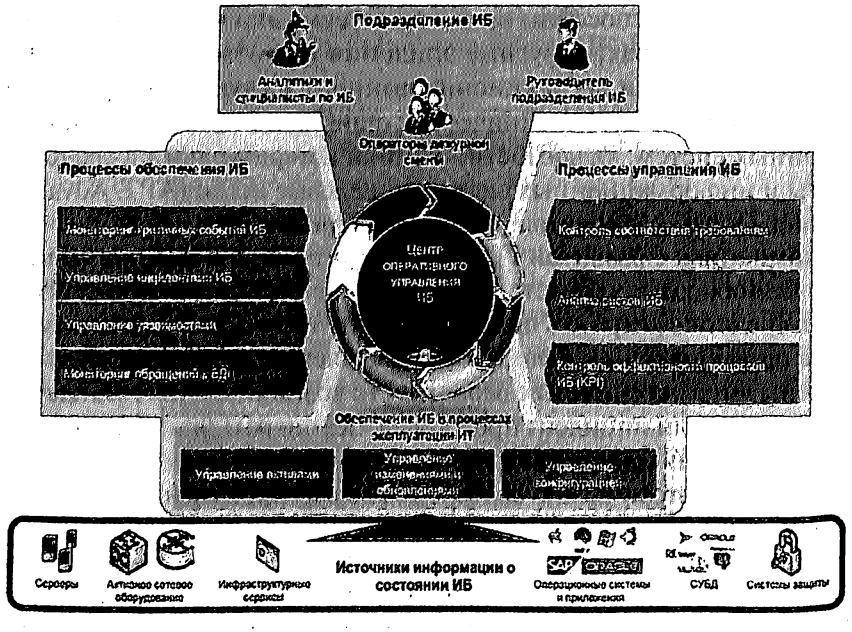


Рис. 3.42. Базовые компоненты SOC

[1] Самый безопасный SOC / Артем Медведев // Jet Info № 3. URL: http://www.jetinfo.ru/stati/samyj-bezopasnyj-soc.

Security Operation Center — это не только и не столько технические средства, это прежде всего команда, задача которой обнаруживать, анализировать, реагировать, уведомлять о возникновении и предотвращать инциденты ИБ. Чтобы персонал, вооруженный техническими средствами, понимал свои задачи, имел четкие инструкции и *KPI* (*Key Performance Indicators* — ключевые показатели эффективности), мог эффективно взаимодействовать внутри SOC и со смежными подразделениями, необходимо выстроить целый ряд процессов в зоне ответственности SOC, направленных на повышение защищенности IT-инфраструктуры. Таким образом, формула работающего SOC выглядит так:

SOC = ПЕРСОНАЛ + ПРОЦЕССЫ + ТЕХНИЧЕСКИЕ ИНСТРУМЕНТЫ

Структура и порядок функционирования *SOC* в первую очередь определяются целями его создания. Эти цели должны быть определены в соответствии с бизнес-задачами организации и зафиксированы документально. Например, к целям SOC можно отнести:

- регламентирование и систематизацию деятельности по выявлению и реагированию на инциденты;
- минимизацию рисков, таких как: несвоевременное обнаружение и оповещение об инциденте, неверная корреляция событий или инцидентов ИБ между собой, выбор недействительных процедур по блокировке распространения инцидента ИБ, утрата свидетельств инцидента и возможности его расследования в будущем;
- снижение количества инцидентов ИБ и связанных с ними финансовых потерь;
- снижение совокупных затрат на управление инцидентами ИБ;
- повышение корпоративной дисциплины.

Эффективность внедрения и использования технических средств максимальна, если компания четко понимает задачи, которые предстоит решать при помощи инструментов *SOC*.

Во-первых, при помощи SOC возможно организовать процесс непрерывного совершенствования защитных мер для обеспечения безопасности. Постоянный анализ текущих событий и инцидентов ИБ, выяснение причин их возникновения с привлечением различных подразделений позволяют оценить эффективность текущих мер защиты, понять их недостатки и выработать предложения по их замене или корректировке.

Во-вторых, внедрение SOC позволяет снизить прямые и косвенные затраты. При небольшом штате сотрудников, когда «не хватает рук», SOC позволяет сократить ресурсы, необходимые для ручной обработки событий ИБ при увеличении количества контролируемых средств защиты. При этом SOC не требует увеличения штата, а напротив, позволяет оптимизировать работу сотрудников путем сведения данных на одну консоль и автоматизации проводимого анализа событий ИБ.

В-третьих, средствами центра управления событиями ИБ можно разделить полномочия контроля за IT-системами. Средства защиты, их администрирование и эксплуатация, как правило, находятся в ведении подразделения IT, в то время как подразделениям ИБ отводятся только функции контроля. *SOC* — это, пожалуй, единственный инструмент контроля в руках у подразделений ИБ, позволяющий им отслеживать действия в IT-системах, что объективно снижает влияние человеческого фактора и повышает уровень информационной безопасности компании.

И наконец, данные, предоставляемые *SOC*, существенно уточняют оценку рисков, которая является основой в выборе тех или иных мер защиты. Кроме того, формализация процедур снижает косвенные затраты компании, так как вопросы согласований без качественного обоснования занимают значительное количество рабочего времени сотрудников.

Внедрение и системное использование СМИИБ позволяет уменьшить негативное воздействие инцидентов ИБ на бизнес, усилить акцент на их предупреждение, улучшить качество результатов оценки и управления рисками ИБ, что в итоге позволяет повысить общий уровень ИБ компании.

Помимо повышения защиты бизнеса построение процесса управления инцидентами зачастую преследует цель соответствия различным отраслевым и международным стандартам, большинство из которых содержат требования, касающиеся не только мониторинга обращений к критичным данным, но и процедуры работы с инцидентами ИБ.

ПРИЛОЖЕНИЕ 3.1

Применение модели с полным перекрытием для анализа рисков информационной безопасности малого предприятия

Постановка задачи: Построить модель защиты информации с полным перекрытием для малого предприятия, схема которого приведена на рис. П3.1[1].

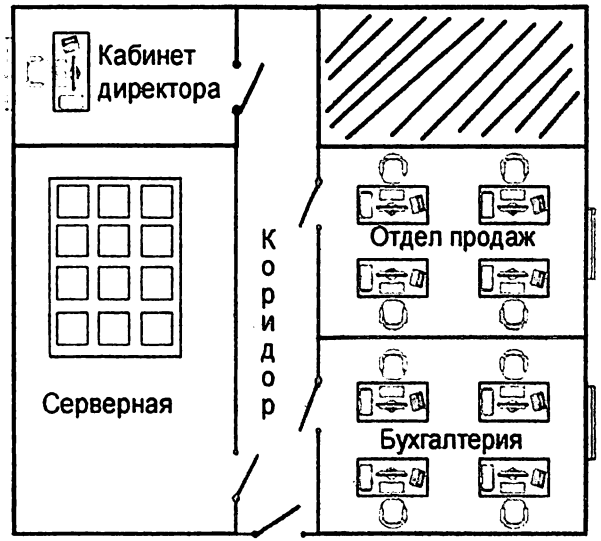


Рис. П3.1. Структурная схема предприятия

В табл. П3.1 дано описание объектов защиты.

Помещения предприятия располагаются на первом этаже, на входе — охрана. Локальная сеть предприятия реализована на витой паре. Интернет-кабель — оптоволокно. Выход в Интернет доступен любому сотруднику.

Сфера деятельности предприятия

Создание и ведение информационных порталов. Разработка и внедрение учетно-управленческих систем.

[1] В приложении 3.1 использованы материалы работы: *Баранова Е.К., Чежин А.А.* Анализ и управление рисками в сфере информационной безопасности малого предприятия / Сб. студ. научных работ кафедры информационной безопасности. — М.: РГСУ, 2009.

Таблица П3.1

Описание объектов защиты

Кабинет директора	окно; компьютер; телефон.
Серверная	почтовый сервер; файловый сервер.
Отдел продаж	окно; четыре телефона; четыре компьютера; принтер.
Бухгалтерия	окно; четыре телефона; четыре компьютера; сейф; принтер.
Коридор	

Статус обрабатываемой информации

Информация, составляющая коммерческую тайну; финансовая документация.

Определение и описание множества угроз дано в табл. П3.2.

Таблица П3.2

Определение и описание множества угроз

У1 — пожар	Угрожает всей информации, хранимой в помещениях. Приводит к нарушению работоспособности оборудования ИС, безвозвратной утрате информационных и других активов. Предотвращается организационными мерами, наличием поста охраны и противопожарной сигнализации
У2 — несанкционированный доступ	НСД злоумышленника Угрожает всей хранимой в помещении информации (вскрытие сейфа, хищение бумаг, удаление информации и т.д.). Обнаруживается при срабатывании сигнализации, визуальном осмотре помещения. Приводит к нарушению конфиденциальности целостности и доступности информации. Предотвращается установкой инженерных средств защиты (решетки, двери, сигнализация) или поста охраны
У3 — неправомерные действия персонала	Угрожает всей обрабатываемой информации. Обнаруживается при раскрытии факта утечки информации, нарушении целостности, доступности. Предотвращается организационными мерами (пункт в договоре о конфиденциальности информации, контроль доступа, санкции за нарушение законодательства)

Окончание табл. П3.2

У4 — потеря информации вследствии заражения вирусами	Угрожает всей информации, обрабатываемой и хранимой на компьютерах. Обнаруживается при наличии антивирусного пакета, нестандартным «поведением» ПО. Приводит к нарушению конфиденциальности целостности и доступности информации. Предотвращается организационными мерами, установкой спецоборудования и антивирусного ПО
У5 — утечка информации, в результате использования общедоступной сети Интернет	Угрожает всей информации, обрабатываемой и хранимой на компьютерах. Обнаруживается при раскрытии факта утечки информации, нарушении целостности, доступности. Предотвращается организационными мерами
У6 — съем информации через окна	Угрожает информации, выведенной на монитор (съем злоумышленником визуальной информации); утечка речевой информации. Обнаруживается при раскрытии факта утечки информации, при визуальном осмотре прилегающей к помещению территории. Приводит к нарушению конфиденциальности информации. Предотвращается с помощью жалюзи на окнах и рекомендации отвернуть мониторы от окон
У7 — съем с телефонной линии	Угрожает конфиденциальности речевой информации, передающейся по телефону, а также конфиденциальности речевой информации вне разговора, при положенной трубке. Обнаруживается путем визуального осмотра аппарата и линии, наличию подозрительных шумов в трубке, проведением мониторинга. Проявляется практически все рабочее время. Приводит к нарушению конфиденциальности информации. Предотвращается организационными мерами, проведением мониторинга

Определение и описание объектов защиты (см. рис. П3.2)

О1. Непосредственно помещение, в котором располагается организация.

О2. Рабочие станции пользователей.

О3. Почтовый сервер организации.

О4. Файловый сервер организации.

О5. Финансовая документация.

О6. Окно.

О7. Телефон.

Определение и описание средств защиты

М.1.1. Дверь с замком.

М.1.2. Охрана на входе.

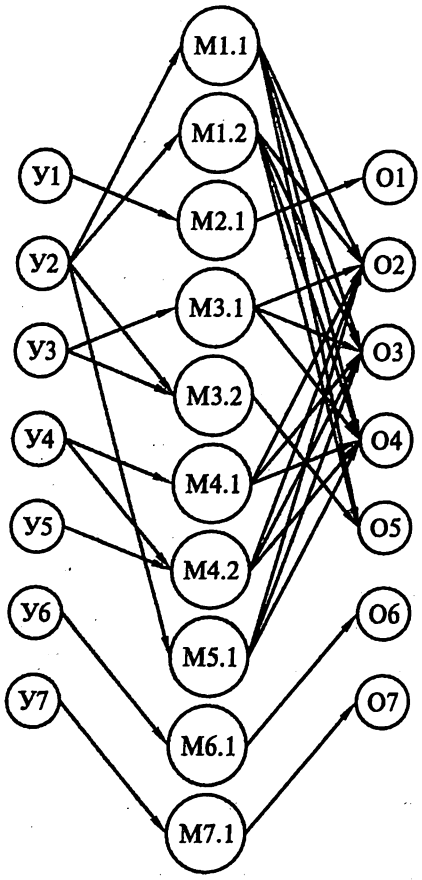


Рис. П3.2. Модель процесса защиты в виде трехдольного графа

М.2.1. Противопожарная сигнализация.

М.3.1. Построение сетевой инфраструктуры на основе Microsoft Active Directory.

М.3.2. Использование сейфа для хранения конфиденциальной документации.

М.4.1. Использование лицензионного ПО.

М.4.2. Использование антивирусного пакета NOD32.

М.5.1. Использование аппаратного средства Cisco Pix FireWall.

М.6.1. Жалюзи.

М.7.1. Использование телефонных аппаратов, сертифицированых по требованиям защиты речевой информации.

Средства защиты подсистем организации даны в табл. П3.3. Приведенные здесь обозначения использованы на рис. П3.2.

Таблица П3.3

Средства защиты подсистем организации

Функциональная подсистема	*Элементарные альтернативы*	
Защита от НСД злоумышленника	М 1.1	М 1.2
Защита от угрозы пожара	М 2.1	—
Защита от неправомерных действий персонала	М 3.1	М 3.2
Защита от вирусов	М 4.1	М 4.2
Защита от утечек при использовании общедоступной сети Интернет	М 5.1	—
Защита окон	М 6.1	—
Защита телефонной линии	М 7.1	—

ПРИЛОЖЕНИЕ 3.2

Использование программного обеспечения Coras для анализа рисков филиала МВА[1]

Магистр делового администрирования, MBA (от англ. Master of Business Administration, используется также калька с английского магистр бизнес-администрирования) — квалификационная степень в менеджменте.

Квалификация MBA подразумевает способность выполнять работу руководителя среднего и высшего звена. Период обучения в зависимости от начальной подготовки и конкретной программы занимает от двух до пяти лет.

Учебные заведения, которые предоставляют степень MBA, называются бизнес-школы. Чаще всего бизнес-школы создаются при университетах.

В настоящее время бизнес-школы есть во многих высших учебных заведениях. Проанализируем риски ИБ для одной из них, используя методологию Coras и соответствующее ПО.

ШАГ 1

Задача этого этапа: общее представление об объекте анализа.

Бизнес-школа, которая представляет собой помещение из шести комнат: приемная, преподавательская, совмещающая функции кабинета руководства и серверной, три идентичные аудиторные класса и мультимедийная лекционная аудитория. Комнаты расположены на первом (цокольном) этаже государственного университета постройки конца XIX в.

Возникает проблема защиты коммерческой информации, персональных данных обучающихся в этом отделении MBA, а также авторской информации (лекционных курсов преподавателей).

Для обработки защищаемой информации используются несколько компьютеров, все они находятся в помещении с окнами. Рядом с каждым компьютером есть внутренний телефон. Помимо этого, у приемной и преподавательской имеется «выход в городскую АТС», хранилище бумажных документов находится в приемной, серверная нахо-

[1] В приложении 3.2 использованы материалы работы: *Жукова Ю.Н.* Программное обеспечение для анализа рисков информационной безопасности малого предприятия. Дипломная работа (научный руководитель Е.К. Баранова). — М.: РГСУ, 2009.

дится в соседнем с ней помещении — преподавательской. Проводная сеть основана на оптоволокне, что исключает возможность снятия информации с кабеля. Выхода в Интернет нет.

На рис. П3.3 показана схема бизнес-школы.

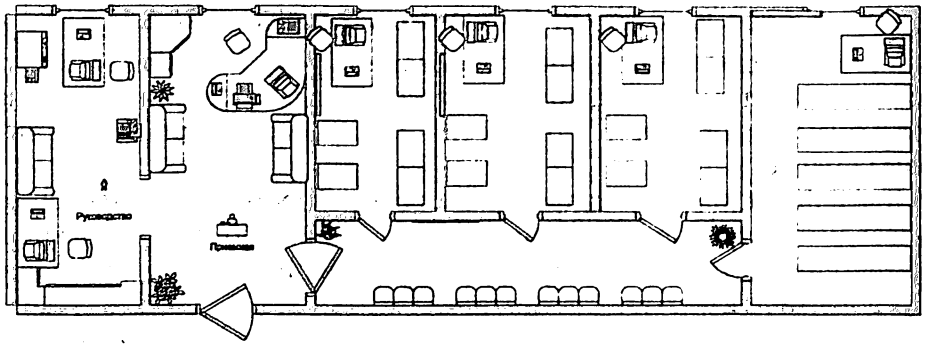


Рис. П3.3. Схема бизнес-школы

Каждому студенту этой бизнес-школы выдаются как электронные материалы, так и бумажные носители информации, являющиеся объектом авторских прав MBA, за распространение которых каждый студент предупрежден об ответственности.

На объекте используются следующие меры по защите информации:

1. Окна и двери тщательно герметизированы монтажной пеной.
2. Окна защищены от лазерной прослушки рифлением.
3. Весь персонал нанят по договору с применением пункта, гарантирующего сохранение коммерческой тайны.
4. Парольная защита на ресурсы.
5. Помещения оборудованы системами охранной сигнализации, ИБП.
6. Действует система видеонаблюдения.
7. Между помещениями стоят деревянные двери, во внешние помещения ведет стальная дверь.
8. Все компьютеры оснащены антивирусом Касперского.
9. Используется лицензионное ПО.
10. Документация хранится в приемной комнате в несгораемом сейфе.
11. Все помещения оборудованы системами противопожарной сигнализации.
12. Предусмотрены средства пожарной безопасности.
13. Стоит программа обнаружения закладок.

ШАГ 2

Целью его является более подробное изучение объекта, определение информации, подлежащей защите.

Персонал состоит из постоянного и переменного:

1) Постоянный состав:

зав.кафедрой;

преподаватели — 5 чел.;

секретарь;

администратор сети и безопасности;

сотрудники — 3 чел.;

уборщицы — 2 чел.

2) Переменный состав:

учащиеся.

Используя программный продукт, составим схему активов (ценной информации, подлежащей защите).

На рис. П3.4 дана диаграмма активов.

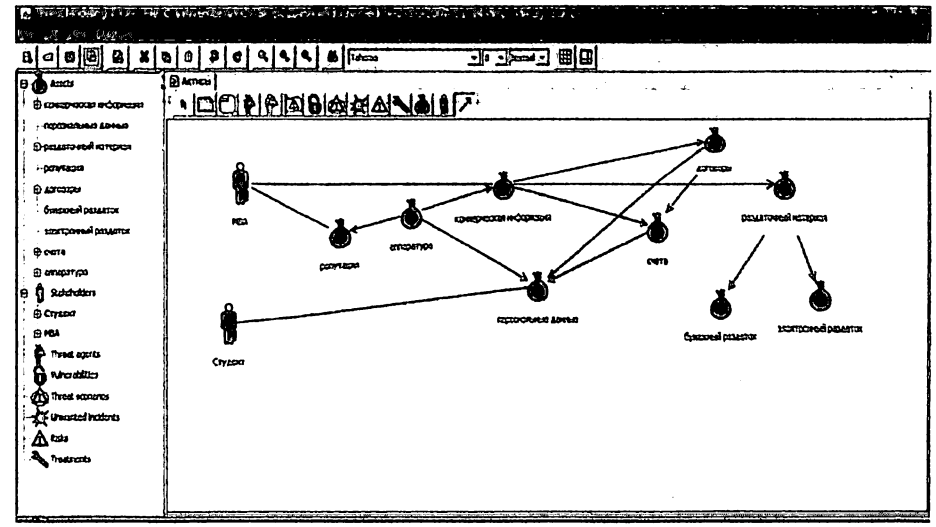


Рис. П3.4. Диаграмма активов

Элементы анализа можно представить в виде схемы на рис. П3.5.

Составим табл. П3.4 для полного описания модели рисков с использованием информации по защите объекта, отображенной в шаге 1. В ней также приведена параллель между объектами программного обеспечения и традиционными вопросами для анализа рисков.

Таблица П3.4

Риски

Кто/что причина?	*Как? Какой инцидент? Чему угрожает?*	*Благодаря чему стала возможной — уязвимость*
Нарушитель	Хищение информации с сервера	Отсутствие шифрования
	Несанкционированное копирование информации	Ошибки в разграничении доступа
	Хищение аппаратуры	Возможность доступа к системам видеонаблюдения
	Запись речевой информации	Диктофон
Системные сбои	Потеря информации	Отсутствие копии
Вирус, закладки	Потеря информации	Ошибки пользователей
Персонал	Установка своего ПО	Политика безопасности
	Копирование информации на носители	Простой пароль
	Доступ к защищаемой информации	Ошибки администратора

ШАГ 3

Последний «подготовительный» шаг

Составим матрицу рисков, в которой столбцы являются шкалой последствий нежелательных инцидентов, а строки — вероятностью происхождения данного инцидента, или его частоты (табл. П3.5).

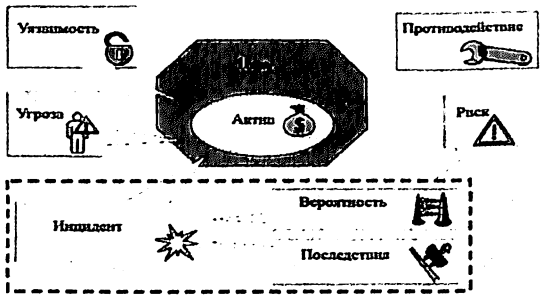


Рис. П3.5. Схема элементов

Желательно для каждого актива по каждой шкале составить описание: что значит редко, иногда, регулярно и часто в количественном отношении за определенный период времени и т.п.

Далее в таблицу матрицы рисков (табл. П3.5) вносятся данные по тому, каким является риск: приемлемый или нет.

Итогом этого этапа являются вероятность и вес последствий, объединенные в матрицу рисков, по которой становится понятно, какой риск является приемлемым, а какой — нет.

Таблица П3.5

Матрица рисков

		Шкала последствий нежелательных инцидентов			
		Незначительные	*Минимальные*	*Средние*	*Катастрофические*
Вероятностная шкала	*Редко*	Приемлемый	Приемлемый	Приемлемый	Неприемлемый
	Иногда	Приемлемый	Приемлемый	Неприемлемый	Неприемлемый
	Регулярно	Приемлемый	Неприемлемый	Неприемлемый	Неприемлемый
	Часто	Неприемлемый	Неприемлемый	Неприемлемый	Неприемлемый

ШАГ 4

Этот шаг называется идентификацией рисков. С помощью описанных в предыдущем параграфе объектов строим диаграмму рисков.

Генерируем диаграмму угроз. В новой вкладке отображаются все отмеченные ранее активы. Для того чтобы не было загроможденности, оставляем только те активы, которые включают в себя разъяснения по подчиненным активам. В нашем случае остаются: раздаточный материал, коммерческая информация, аппаратура и репутация.

Используя табл. П3.4, строим модель угроз, изображенную на рис. П3.6.

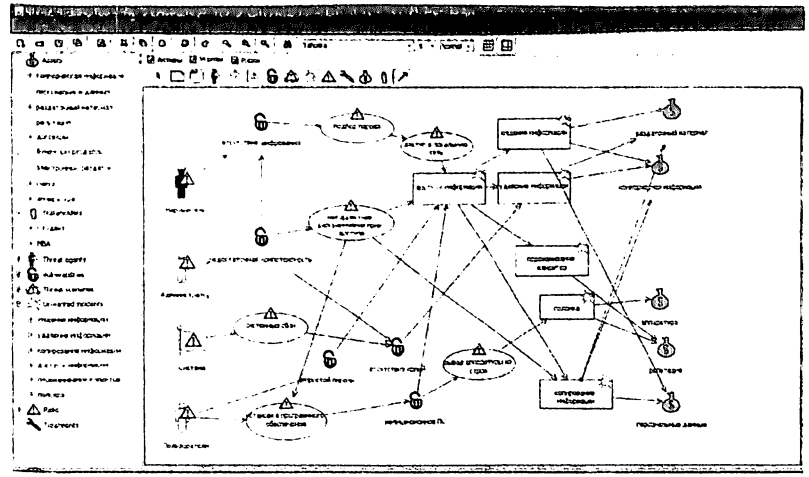


Рис. П3.6. Модель угроз

ШАГ 5

На полученную в предыдущем шаге модель наносим вероятность осуществления сценария нежелательного инцидента.

В результате получаем полную модель угроз. Для нашего примера эта модель угроз представлена на рис. П3.7.

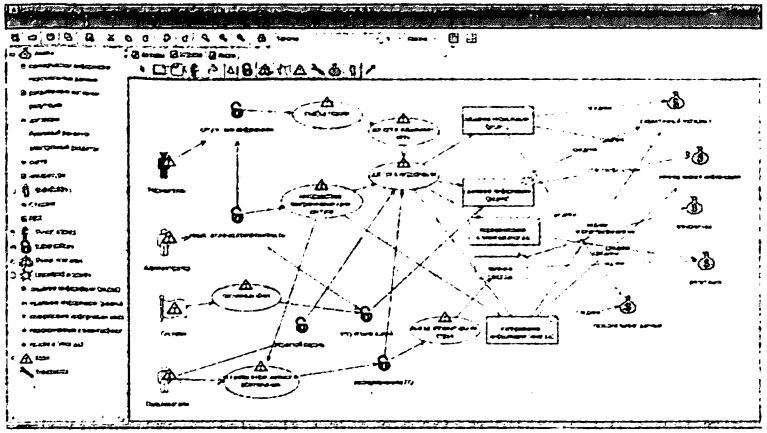


Рис. П3.7. Модель угроз с вероятностными характеристиками

ШАГ 6

Генерируем диаграмму рисков (щелкаем правой кнопкой мыши по вкладке *Угрозы* и выбираем *Generate risk diagram*). Полученная диаграмма представлена на рис. П3.8.

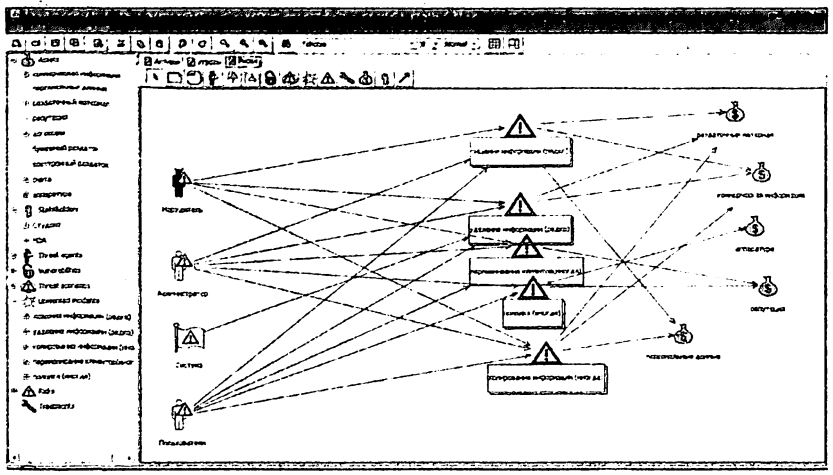


Рис. П3.8. Диаграмма рисков

Теперь по каждому риску для каждого актива определяем последствия в случае осуществления этого риска (рис. П3.9).

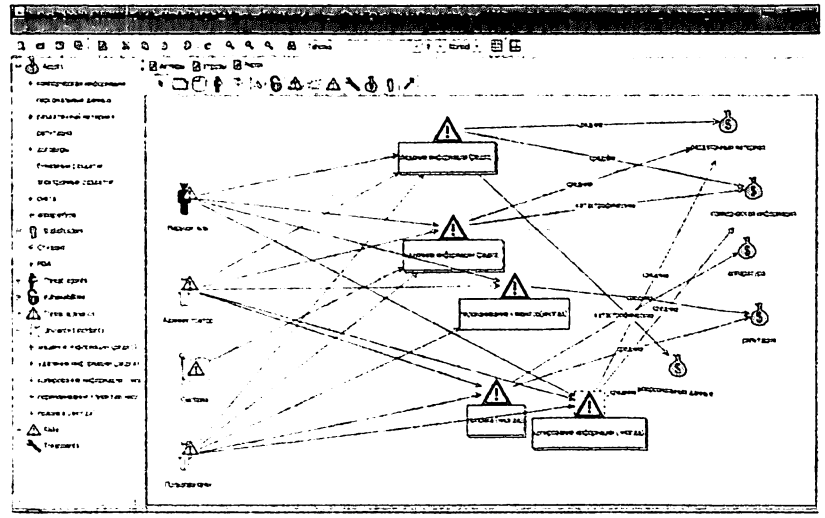


Рис. П3.9. Диаграмма рисков с характеристикой последствий осуществления угрозы

На диаграмме угроз для каждой уязвимости ставим противодействие (рис. П3.10).

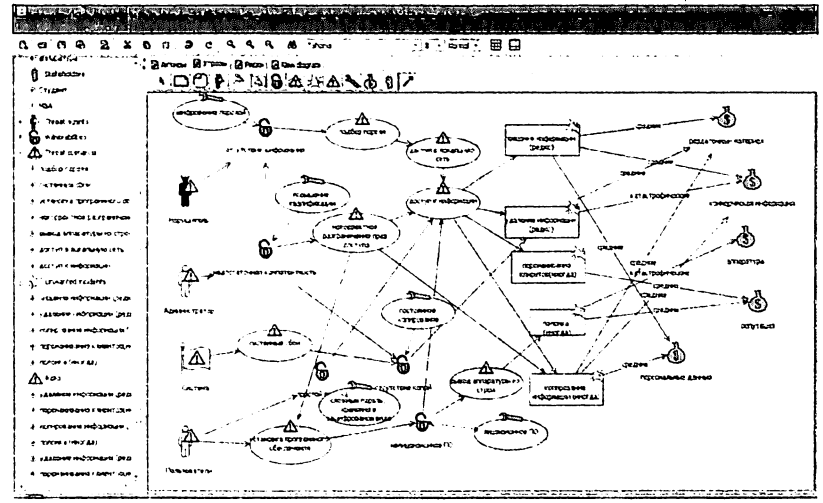


Рис. П3.10. Диаграмма угроз после добавления противодействий

ШАГ 7

В соответствии с рис. П3.9 занесем полученную информацию в матрицу рисков, получим следующую таблицу (табл. П3.6).

Таблица П3.6

Матрица рисков по диаграмме

		Шкала последствий нежелательных инцидентов			
		Незначительные	Минимальные	Средние	Катастрофические
Вероятностная шкала	Редко	—	—	Хищение раздаточного материала. Хищение коммерческой информации. Хищение персональных данных. Удаление раздаточного материала	Удаление коммерческой информации
	Иногда	—	—	Переманивание клиентов. Копирование персональных данных. Копирование раздаточного материала	Поломка аппаратуры. Копирование коммерческой информации
	Регулярно	—	—	—	—
	Часто	—	—	—	—

Внося поправки в соответствии с табл. П3.6, получаем диаграмму неприемлемых рисков (рис. П3.11).

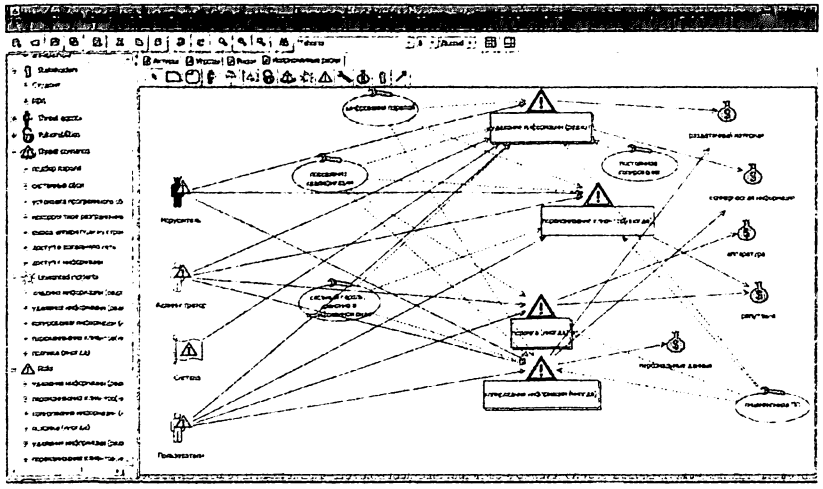


Рис. П3.11. Диаграмма неприемлемых рисков

На основании диаграммы неприемлемых рисков можно предложить следующие противодействия в порядке влияния на риски:

1. Повышение квалификации администратора.
2. Установка только лицензионного программного обеспечения.
3. Создание сложных паролей и их хранение в зашифрованном виде.
4. Постоянное копирование информации.

ПРИЛОЖЕНИЕ 3.3

Алгоритм оценки рисков информационной безопасности для организаций малого и среднего бизнеса

На первом этапе рассчитывается уровень угрозы по уязвимости T_h на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации.

Для режима с одной базовой угрозой

$$T_h = \frac{ER}{100} \times \frac{P(V)}{100},$$

где T_h — уровень угрозы по уязвимости;

ER — критичность реализации угрозы, %;

$P(V)$ — вероятность реализации угрозы через данную уязвимость, %.

Для режима с тремя базовыми угрозами используются следующие формулы:

$$T_{hc} = \frac{ER_c}{100} \times \frac{P(V)_c}{100},$$

где T_{hc} — уровень угрозы по уязвимости конфиденциальности;

ER_c — критичность реализации угрозы конфиденциальности, %;

$P(V)_c$ — вероятность реализации угрозы конфиденциальности, %;

$$T_{hi} = \frac{ER_i}{100} \times \frac{P(V)_i}{100},$$

где T_{hi} — уровень угрозы по уязвимости целостности;

ER_i — критичность реализации угрозы целостности, %;

$P(V)_i$ — вероятность реализации угрозы целостности, %.

$$T_{ha} = \frac{ER_a}{100} \times \frac{P(V)_a}{100},$$

где T_{ha} — уровень угрозы по уязвимости доступности;

ER_a — критичность реализации угрозы доступности, %;

$P(V)_a$ — вероятность реализации угрозы доступности, %;

значения уровня угрозы по уязвимости находятся в интервале от 0 до 1.

Чтобы рассчитать уровень угрозы по нескольким уязвимостям, через которые возможна реализация данной угрозы на ресурсе, нужно просуммировать полученные уровни угроз через конкретные уязвимости.

Для режима с одной базовой угрозой используется формула

$$CT_h = 1 - \prod_{i=1}^{n} (1 - T_{hi}),$$

где T_{hi} — уровень угрозы по конкретной уязвимости;

CT_h — уровень угрозы по нескольким уязвимостям;

значения уровня угрозы по нескольким уязвимостям находятся в интервале от 0 до 1.

Для режима с тремя базовыми угрозами

$$CT_{hc} = 1 - \prod_{j=1}^{n} (1 - T_{hc,j}),$$

где CT_{hc} — уровень угрозы по нескольким уязвимостям по критерию угрозы конфиденциальности;

$T_{hc,j}$ — уровень угрозы по уязвимости конфиденциальности;

$$CT_{hi} = 1 - \prod_{j=1}^{n} (1 - T_{hi,j}),$$

где $CT_{hi,j}$ — уровень угрозы по нескольким уязвимостям по критерию угрозы целостности;

$T_{hi,j}$ — уровень угрозы по уязвимости целостности;

$$CT_{ha} = 1 - \prod_{j=1}^{n} (1 - T_{ha,j}),$$

где CT_{ha} — уровень угрозы по нескольким уязвимостям по критерию угрозы доступности;

$T_{ha,j}$ — уровень угрозы по уязвимости доступности;

значения уровня угрозы по всем уязвимостям находятся в интервале от 0 до 1.

Аналогично рассчитывается общий уровень угроз по ресурсу R (учитывая все угрозы, действующие на ресурс).

Для режима с одной базовой угрозой

$$CT_hR = 1 - \prod_{i=1}^{n} (1 - T_{hi}),$$

где CT_hR — уровень угрозы по ресурсу;

T_{hi} — уровень угрозы по уязвимости;

значение общего уровня угрозы находятся в интервале от 0 до 1.

Для режима с тремя базовыми угрозами используются следующие формулы:

$$CT_hR_c = 1 - \prod_{j=1}^{n} (1 - T_{hc,j}),$$

где $T_{hc,j}$ — уровень угрозы по уязвимости конфиденциальности;

CT_hR_c — уровень угрозы конфиденциальности по всем угрозам ресурса;

$$CT_hR_i = 1 - \prod_{j=1}^{n} (1 - T_{hi,j}),$$

где $T_{hi,j}$ — уровень угрозы по уязвимости целостности;

CT_hR_i — уровень угрозы целостности по всем угрозам ресурса.

$$CT_hR_a = 1 - \prod_{j=1}^{n} (1 - T_{ha,j}),$$

где $T_{ha,j}$ — уровень угрозы по уязвимости доступности;

CT_hR_a — уровень угрозы доступности по всем угрозам ресурса;

значение общего уровня угрозы находится в интервале от 0 до 1.

Риск по ресурсу R рассчитывается следующим образом.

Для режима с одной базовой угрозой

$$R = CT_hR \times D,$$

где D — критичность ресурса (задается в финансовых единицах или уровнях);

CT_hR — общий уровень угроз по ресурсу.

Если риск задается в уровнях, то в качестве значения критичности берется оценка уровня.

В случае угрозы доступности (отказ в обслуживании) критичность ресурса в год вычисляется по следующей формуле:

$$D_{a/год} = D_{a/час} \times T_{max},$$

где $D_{a/год}$ — критичность ресурса по угрозе доступности в год;

$D_{a/час}$ — критичность ресурса по угрозе доступности в час;

T_{max} — максимальное критическое время простоя ресурса в год.

Для остальных угроз критичность ресурса задается в год.

В результате работы алгоритма пользователь системы получает следующие данные:

- риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса;
- риск реализации суммарно по всем угрозам для ресурса;
- риск реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы;
- риск реализации по всем угрозам для информационной системы;
- риск реализации по всем угрозам для информационной системы после задания контрмер;
- эффективность контрмер;
- эффективность комплекса контрмер.

Литература к главе 3

1. *Александрович Г.Я., Нестеров С.А., Петренко С.А.* Автоматизация оценки информационных рисков компании // Защита информации. — Конфидент, 2003. — № 2. — С. 78–81.
2. *Бабаш А.В., Баранова Е.К.* Актуальные вопросы защиты информации: монография. – М.: РИОР:ИНФРА-М, 2017.
3. *Баранова Е.К.* Методики анализа и оценки рисков информационной безопасности. Моделирование и анализ безопасности и риска в сложных системах // Труды Международной научной школы МА БР 2014 (Санкт-Петербург, 18–20 ноября 2014 г.). — СПб., 2014. — С. 132–138.
4. *Баранова Е.К.* Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. — 2009. — № 1(49). — С. 15–26.
5. *Баранова Е.К., Зубровский Г.Б.* Управление инцидентами информационной безопасности. Проблемы информационной безопасности // Труды I Международной научно-практической конференции «Проблемы информационной безопасности». Гурзуф: Крымский федеральный университет им. В.И. Вернадского, 26–28 февраля 2015 г. — Гурзуф, 2015. — С. 27–33.

6. *Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН). СПб.: 2012. Вып. 20, С. 27–56.
7. *Петренко С.А., Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. — М.: Академия АйТи: ДМК Пресс, 2004.
8. *Симонов С.* Современные технологии анализа рисков в информационных системах // PCWEEK. 2001. №37. — URL: http://info-sec.edu.nw.ru/arch/analiz.htm.
9. The logic behind CRAMM's assessment of measures of risk and determination of appropriate countermeasures. — URL: http://www.cramm.com/downloads/techpapers.htm.
10. *Peltier T.R.* Information security risk analysis / Auerbach 2001. ISBN 0-8493-0880-1.
11. Risk Watchusers manual. URL: http://www.riskwatch.com.
12. *Taylor L.* Risk analysis tools & how they work. — URL: http://www.riskwatch.com.

ГЛАВА 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОМПЬЮТЕРНЫХ СЕТЯХ

4.1. Особенности обеспечения информационной безопасности в компьютерных сетях

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве, и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что наряду с локальными угрозами, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид угроз, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые, или удаленные угрозы. Они характерны, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям. С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по числу попыток, так и по успешности их применения и, соответственно, обеспечение безопасности вычислительных сетей с позиции противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных вычислительных систем состоит в том, что если в локальных вычислительных сетях наиболее частыми являются угрозы раскрытия и целостности, то в сетевых системах на первое место выходит угроза отказа в обслуживании.

Удаленная угроза — потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи. Это определение охватывает обе особенности сетевых систем — распределенность компьютеров и распределенность информации. Поэтому при рассмотрении вопросов ИБ вычислительных сетей рассматриваются два подвида удаленных угроз — это удаленные угрозы на инфраструктуру и протоколы сети и

удаленные угрозы на телекоммуникационные службы. Первые используют уязвимости в сетевых протоколах и инфраструктуре сети, а вторые — уязвимости в телекоммуникационных службах.

Цели сетевой безопасности могут меняться в зависимости от ситуации, но обычно связаны с обеспечением следующих составляющих ИБ:

- целостность данных;
- конфиденциальность данных;
- доступность данных.

Целостность данных — одна из основных целей ИБ сетей — предполагает, что данные не были изменены, подменены или уничтожены в процессе их передачи по линиям связи, между узлами вычислительной сети. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Конфиденциальность данных — вторая главная цель сетевой безопасности. При информационном обмене в вычислительных сетях большое количество информации относится к конфиденциальной, например, личная информация пользователей, учетные записи (имена и пароли), данные о кредитных картах и др.

Доступность данных — третья цель безопасности данных в вычислительных сетях. Функциями вычислительных сетей являются совместный доступ к аппаратным и программным средствам сети и совместный доступ к данным. Нарушение ИБ как раз и связано с невозможностью реализации этих функций.

В локальной сети должны быть доступны принтеры, серверы, рабочие станции, данные пользователей и др.

В глобальных вычислительных сетях должны быть доступны информационные ресурсы и различные сервисы, например почтовый сервер, сервер доменных имен, web-сервер и др.

При рассмотрении вопросов, связанных с ИБ, в современных вычислительных сетях необходимо учитывать следующие факторы:

- глобальная связанность;
- разнородность корпоративных информационных систем;
- распространение технологии «клиент/сервер».

Применительно к системам связи глобальная связанность означает, что речь идет о защите сетей, пользующихся внешними сервисами, основанными на протоколах TCP/IP и предоставляющих аналогичные

сервисы вовне. Весьма вероятно, что внешние сервисы находятся в других странах, поэтому от средств защиты в данном случае требуется следование стандартам, признанным на международном уровне. Национальные границы, законы, стандарты не должны препятствовать защите потоков данных между клиентами и серверами.

Из факта глобальной связанности вытекает также меньшая эффективность мер физической защиты, общее усложнение проблем, связанных с защитой от несанкционированного доступа, необходимость привлечения для их решения новых программно-технических средств, например, межсетевых экранов.

Разнородность аппаратных и программных платформ требует от изготовителей средств защиты соблюдения определенной технологической дисциплины. Важны не только чисто защитные характеристики, но и возможность встраивания этих систем в современные корпоративные информационные структуры. Если, например, продукт, предназначенный для криптографической защиты, способен функционировать исключительно на платформе Wintel (Windows+Intel), то его практическая применимость вызывает серьезные сомнения.

Корпоративные ИС оказываются разнородными еще в одном важном отношении — в разных частях этих систем хранятся и обрабатываются данные разной степени важности и секретности.

Использования технологии «клиент/сервер» с позиции ИБ имеет следующие особенности:

- каждый сервис имеет свою трактовку главных аспектов ИБ (доступности, целостности, конфиденциальности);
- каждый сервис имеет свою трактовку понятий субъекта и объекта;
- каждый сервис имеет специфические угрозы;
- каждый сервис нужно по-своему администрировать;
- средства безопасности в каждый сервис нужно встраивать по-особому.

Особенности вычислительных сетей, и в первую очередь глобальных, предопределяют необходимость использования специфических методов и средств защиты, например:

- защита подключений к внешним сетям;
- защита корпоративных потоков данных, передаваемых по открытым сетям;
- защита потоков данных между клиентами и серверами;
- обеспечение безопасности распределенной программной среды;

• защита важнейших сервисов (в первую очередь — web-сервиса);
• аутентификация в открытых сетях.

Вопросы реализации таких методов защиты будут рассмотрены далее.

В последнее время все четче просматривается незащищенность вычислительных сетей от глобальных атак. Успешные глобальные сетевые атаки, безусловно, являются самым разрушительным явлением, которое может произойти в современных сетях.

4.2. Сетевые модели передачи данных

4.2.1. Понятие протокола передачи данных

Обмен информацией между ЭВМ на больших расстояниях всегда казался более важной задачей, чем локальный обмен. Поэтому ему уделялось больше внимания и, соответственно, велось большее финансирование во многих странах. Один из немногих открытых проектов по исследованию вычислительных сетей, финансировавшийся военным ведомством США, известен под названием сеть ARPA — Advanced Research Projects Agency. С самого начала в рамках этого проекта велись работы по объединению ресурсов многих вычислительных машин различного типа. В 1960–70-е гг. многие результаты, полученные при эксплуатации сети ARPA, были опубликованы в открытой печати. Это обстоятельство, а также тот факт, что почти все страны занялись практически слепым копированием не только аппаратной архитектуры американских машин, но и базового программного обеспечения, обусловили сильное влияние сети ARPA на многие другие сети, именно поэтому принято считать, что сеть ARPA является предшественницей всемирной компьютерной сети Интернет.

Основной задачей сетевой общественности явилась разработка протоколов обмена информацией. Эта задача совершенно справедливо представлялась важнейшей, поскольку настоятельно требовалось заставить «понимать» друг друга компьютеры, обладавшие различной архитектурой и программным обеспечением. Первоначально разработчики многочисленных корпоративных сетей договаривались о внутренних протоколах информационного обмена в своих сетях. Никакой стандартизации не было. Но уже в 70-е гг. специалистам стало совершенно ясно, что стандартизация необходима и неизбежна. В эти годы шел бурный процесс создания многочисленных национальных и международных комитетов и комиссий по стандартизации программных и аппаратных средств в области вычислительной техники и информационного обмена.

В общем случае протокол сетевого обмена информацией можно определить как перечень форматов передаваемых блоков данных, а также правил их обработки и соответствующих действий. Другими словами, протокол обмена данными — это подробная инструкция о том, какого типа информация передается по сети, в каком порядке обрабатываются данные, а также набор правил обработки этих данных.

Человек — оператор компьютера, включенного в сеть, тем или иным способом, например с помощью программ-приложений, формирует и передает по сети сообщения, предназначенные для других людей или компьютеров. В ответ он также ожидает поступления сообщения. В этом смысле сообщение представляет собой логически законченную порцию информации, предназначенную для потребления конечными пользователями — человеком или прикладной программой. Например, это может быть набор алфавитно-цифровой и графической информации на экране или файл целиком. Сейчас сообщения неразрывно связывают с прикладным уровнем или, как его еще называют, уровнем приложений сетевых протоколов.

Сообщения могут проходить довольно сложный путь по сетям, стоять в очередях на передачу или обработку, в том числе не доходить до адресата, о чем отправитель также должен быть уведомлен специальным сообщением.

Первоначально вычислительные сети были сетями коммутации сообщений. Это было оправдано, пока сообщения были сравнительно короткими. Но параллельно с этим всегда существовали задачи передачи на расстояние больших массивов информации. Решение этой задачи в сетях с коммутацией сообщений является неэффективным, поскольку длины сообщений имеют большой разброс — от очень коротких до очень длинных, что характерно для компьютерных сетей.

В связи с этим было предложено разбивать длинные сообщения на части — пакеты — и передавать сообщения не целиком, а пакетами, вставляя в промежутках пакеты других сообщений. На месте назначения сообщения собираются из пакетов. Короткие сообщения при этом были вырожденным случаем пакета, равного сообщению.

В настоящее время почти все сети в мире являются сетями коммутации пакетов.

4.2.2. Принципы организации обмена данными в вычислительных сетях

Существуют два принципа организации обмена данными:

- установление виртуального соединения с подтверждением приема каждого пакета;
- передача датаграмм.

Установление виртуального соединения, или создание виртуального канала является более надежным способом обмена информацией. Поэтому он более предпочтителен при передаче данных на большие расстояния и (или) по физическим каналам, в которых возможны помехи. При виртуальном соединении пункт приема информации уведомляет отправителя о правильном или неправильном приеме каждого пакета. Если какой-то пакет принят неправильно, отправитель повторяет его передачу. Так длится до тех пор, пока все сообщение не будет успешно передано. На время передачи информации между двумя пунктами коммутируется канал, подобный каналу при телефонном разговоре. Виртуальным его называют потому, что в отличие от телефонного коммутированного канала обмен информацией может идти по различным физическим путям даже в процессе передачи одного сообщения.

Термин «*датаграмма*» образован по аналогии с термином «телеграмма». Аналогия заключается том, что короткие пакеты — собственно датаграммы — пересылаются адресату без подтверждения получения каждой из них. О получении всего сообщения целиком должна уведомить целевая программа.

4.2.3. Транспортный протокол TCP и модель TCP/IP

За время развития вычислительных сетей было предложено и реализовано много протоколов обмена данными, самыми удачными из которых явились семейство протоколов TCP/IP (Transmission Control Protocol/Internet Protocol — протокол управления передачей/межсетевой протокол).

TCP/IP — это стек протоколов, состоящий из следующих основных компонентов:

- межсетевой протокол (Internet Protocol), обеспечивающий адресацию в сетях (IP-адресацию);
- межсетевой протокол управления сообщениями (Internet Control Message Protocol — ICMP), который обеспечивает низкоуровневую поддержку протокола IP, включая такие функции, как сообщения об ошибках, квитанции, содействие в маршрутизации и т.п.;

- протокол разрешения адресов (Address Resolution Protocol — ARP), выполняющий преобразование логических сетевых адресов в аппаратные, а также обратный ему RARP (Reverse ARP);
- протокол пользовательских датаграмм (User Datagramm Protocol — UDP);
- протокол управления передачей (Transmission Control Protocol — TCP).

Протокол UDP обеспечивает передачу пакетов без проверки доставки, в то время как протокол TCP требует установления виртуального канала и, соответственно, подтверждения доставки пакета с повтором в случае ошибки.

Этот набор протоколов образует самую распространенную модель сетевого обмена данными, получившую название TCP/IP. Модель TCP/IP иерархическая и включает четыре уровня (табл. 4.1).

Таблица 4.1

Уровни модели TCP/IP

Уровень	*Название*	*Функция*
4	Прикладной	Приложения пользователей, создание сообщений
3	Транспортный	Доставка данных между программами в сети
2	Межсетевой	Адресация и маршрутизация
1	Доступа к среде передачи данных	Сетевые аппаратные средства и их драйверы

Прикладной уровень определяет способ общения пользовательских приложений. В системах «клиент — сервер» приложение-клиент должно знать, как посылать запрос, а приложение-сервер должно знать, как ответить на запрос. Этот уровень обеспечивает такие протоколы, как HTTP, FTP, Telnet.

Транспортный уровень позволяет сетевым приложениям получать сообщения по строго определенным каналам с конкретными параметрами.

На сетевом уровне определяются адреса включенных в сеть компьютеров, выделяются логические сети и подсети, реализуется маршрутизация между ними.

На канальном уровне определяется адресация физических интерфейсов сетевых устройств, например сетевых плат. К этому уровню относятся программы управления физическими сетевыми устройствами, так называемые драйверы.

Как уже отмечалось ранее, в сетях с коммутацией пакетов, а модель TCP/IP относится к таким сетям, для передачи по сети сообщение

(сформированное на прикладном уровне) разбивается на пакеты или датаграммы. *Пакет или датаграмма* — это часть сообщения с добавленным заголовком пакета или датаграммы.

На транспортном уровне к полезной информации добавляется заголовок — служебная информация. Для сетевого уровня полезной информацией является уже пакет или датаграмма транспортного уровня. К ним добавляется заголовок сетевого уровня.

Полученный блок данных называется IP-пакетом. Полезной нагрузкой для канального уровня является уже IP-пакет. Здесь перед передачей по каналу к нему добавляются собственный заголовок и еще завершитель. Получившийся блок называется кадром. Он и передается по сети.

Переданный по сети кадр в пункте назначения преобразуется в обратном порядке, проходя по уровням модели снизу вверх.

4.3. Модель взаимодействия открытых систем OSI/ISO

4.3.1. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO

В конце 80-х гг. наблюдался подлинный бум, вызванный разработкой Международной организации по стандартизации (International Standard Organization) коммуникационных протоколов. Разработанная ISO спецификация, названная моделью взаимодействия открытых систем (OSI — Open Systems Interconnection) заполонила научные публикации. Казалось, что эта модель займет первое место и оттеснит широко распространившийся TCP/IP. Но этого не произошло. Одной из причин стала тщательная проработка протоколов TCP/IP, их функциональность и открытость к наращиванию функциональных возможностей, хотя к настоящему времени достаточно очевидно, что они имеют и множество недостатков.

Приведем сравнительную схему уровневых моделей протоколов OSI и TCP/IP (рис. 4.1). Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что в процессе обмена сообщениями участвуют две стороны, т.е. в данном случае необходимо организовать согласованную работу двух «иерархий», работающих на разных компьютерах. Оба участника сетевого обмена должны принять множество соглашений. Например, они должны согласовать уровни и форму электрических сигналов, способ определения длины сообщений, договориться о методах контроля достоверности

и т.п. Другими словами, соглашения должны быть приняты для всех уровней, начиная от самого низкого — уровня передачи битов — до самого высокого, реализующего сервис для пользователей сети.

Рис. 4.1. Сравнительная схема уровневых моделей протоколов OSI и TCP/IP

4.3.2. Распределение функций безопасности по уровням модели OSI/ISO

Модель взаимодействия открытых систем OSI/ISO определяет различные уровни взаимодействия систем в сетях с коммутацией пакетов, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень.

В модели OSI средства взаимодействия делятся на семь уровней: прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический. Каждый уровень имеет дело с определенным аспектом взаимодействия сетевых устройств.

Физический уровень имеет дело с передачей *битов* по физическим каналам связи, таким как коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал. К этому уровню имеют отношение характеристики физических сред передачи данных, такие как полоса пропускания, помехозащищенность, волновое сопротивление и др.

Одной из задач *канального уровня* является проверка *доступности среды передачи*. Другая задача канального уровня — *реализация механизмов обнаружения и коррекции ошибок*. Для этого на канальном уровне биты группируются в наборы, называемые кадрами (frames). Канальный уровень обеспечивает корректность передачи каждого кадра.

Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать различные принципы передачи сообщений между конечными

узлами и обладать произвольной структурой связей. Внутри одной сети доставка данных обеспечивается канальным уровнем, а вот доставкой данных между различными сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора *маршрута* передачи сообщения даже в том случае, когда структура связей между составляющими сетями имеет характер, отличный от принятого в протоколах канального уровня.

Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. *Маршрутизатор* — это устройство, которое собирает информацию о топологии межсетевых соединений и пересылает пакеты сетевого уровня в сеть назначения. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями.

Транспортный уровень обеспечивает приложениям или верхним уровням стека — прикладному и сеансовому — передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное — способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Сеансовый уровень обеспечивает *управление диалогом*: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации. Последние позволяют вставлять *контрольные точки* в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все сначала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

Представительный уровень имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например, в кодах ASCII и EBCDIC. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол Secure Socket Layer (SSL), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

Прикладной уровень — это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют совместную работу, например, с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется сообщением.

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня — физический, канальный и сетевой — являются сетезависимыми, т.е. протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием.

Три верхних уровня — прикладной, представительный и сеансовый — ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было изменения в топологии сети, замена оборудования или переход на другую сетевую технологию.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений.

В «Общих критериях» приводится распределение функций безопасности по уровням эталонной семиуровневой модели OSI, как показано в табл. 4.2.

4.4. Адресация в глобальных сетях

4.4.1. Основы построения IP-протокола

Одной из главных проблем построения глобальных сетей является проблема адресации. С одной стороны, постоянное расширение глобальной сети Интернет привело к нехватке уникальных адресов для вновь подключаемых узлов. С другой стороны, система адресации в таких сетях должна быть защищена от возможного вмешательства злоумышленников, связанного с подменой адресов и реализацией обход-

ных маршрутов передачи сообщений. Адресация современного Интернета основана на протоколе IP (Internet Protocol), история которого неразрывно связана с транспортным протоколом TCP.

Таблица 4.2

Распределение функций безопасности по уровням OSI/ISO

Функция безопасности	*Уровень OSI*						
	1	2	3	4	5	6	7
Аутентификация	–	–	+	+	–	–	+
Управление доступом	–	–	+	+	–	–	+
Конфиденциальность соединения	+	+	+	+	–	+	+
Конфиденциальность вне соединения	–	+	+	+	–	+	+
Избирательная конфиденциальность	–	–	–	–	–	+	+
Конфиденциальность трафика	+	–	+	–	–	–	+
Целостность с восстановлением	–	–	–	+	–	–	+
Целостность без восстановления	–	–	+	+	–	–	+
Избирательная целостность	–	–	–	–	–	–	+
Целостность вне соединения	–	–	+	+	–	–	+
Неотказуемость	–	–	–	–	–	–	+

«+» данный уровень может предоставить функцию безопасности;
«–» данный уровень не подходит для предоставления функции безопасности.

Концепция протокола IP представляет сеть как множество компьютеров (хостов), подключенных к некоторой интерсети. Интерсеть, в свою очередь, рассматривается как совокупность физических сетей, связанных маршрутизаторами. Физические объекты (хосты, маршрутизаторы, подсети) идентифицируются при помощи специальных IP-адресов. Каждый IP-адрес представляет собой 32-битовый идентификатор. Принято записывать IP-адреса в виде 4 десятичных чисел, разделенных точками.

Для этого 32-битовый IP-адрес разбивается на четыре группы по 8 бит (1 байт), после чего каждый байт двоичного слова преобразовывается в десятичное число по известным правилам. Например, IP-адрес:

10010011 10000111 00001110 11100101

преобразуется указанным способом к следующему виду:

147.135.014.229

4.4.2. Классы адресов вычислительных сетей

Каждый адрес является совокупностью двух идентификаторов: сети — Net ID, и хоста — Host ID. Все возможные адреса разделены на 5 классов, схема которых приведена на рис. 4.2.

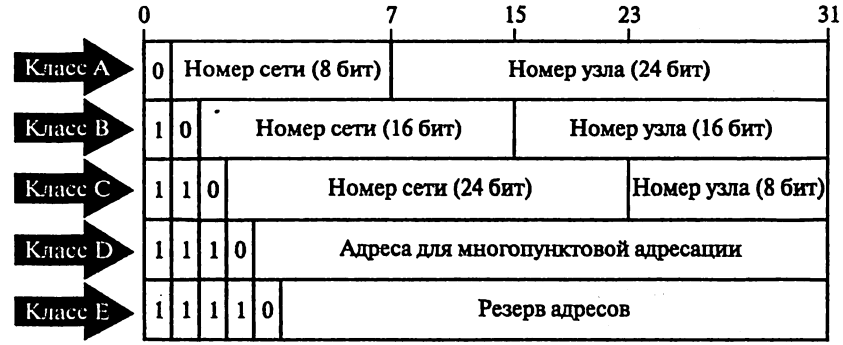


Рис. 4.2. Классы адресов вычислительных сетей

Из рис. 4.2 видно, что классы сетей определяют как возможное число этих сетей, так и число хостов в них. Практически используются только первые три класса:

Класс A определен для сетей с числом хостов до 16 777 216. Под поле Net ID отведено 7 бит, под поле Host ID — 24 бита.

Класс B используется для среднемасштабных сетей (Net ID — 14 бит, Host ID — 16 бит). В каждой такой сети может быть до 65 536 хостов.

Класс C применяется для небольших сетей (Net ID — 21 бит, Host ID — 8 бит) с числом хостов до 255.

4.5. Классификация удаленных угроз в вычислительных сетях

При изложении данного материала в некоторых случаях корректнее говорить об удаленных атаках, нежели об удаленных угрозах объектам вычислительных сетей. Тем не менее, все возможные удаленные атаки являются, в принципе, удаленными угрозами информационной безопасности.

Удаленные угрозы можно классифицировать по следующим признакам[1].

- По характеру воздействия:
  - пассивные (класс 1.1);
  - активные (класс 1.2).

[1] *Медведовский И.Д., Семьянов П.В., Платонов В.В.* Атака через Internet / Под ред. проф. П.Д. Зегжды. —М.: НПО «Мир и семья-95», 1997.

Пассивным воздействием на распределенную вычислительную систему называется такое, которое не оказывает непосредственное влияние на работу системы, но может нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на работу сети приводит к тому, что пассивное удаленное воздействие практически невозможно обнаружить. Примером пассивного типового удаленного воздействия в вычислительных сетях является прослушивание канала связи в сети.

Под активным воздействием на вычислительную сеть понимается воздействие, оказывающее непосредственное влияние на работу сети (например, изменение конфигурации, нарушение работоспособности) и нарушающее принятую в ней политику безопасности. Практически все типы удаленных угроз являются активными воздействиями. Это связано с тем, что в самой природе разрушающего воздействия содержится активное начало. Очевидной особенностью активного воздействия по сравнению с пассивным является принципиальная возможность его обнаружения, так как в результате его осуществления в системе происходят определенные изменения. В отличие от активного, при пассивном воздействии не остается никаких следов (просмотр чужого сообщения ничего не меняет).

- По цели воздействия:

– нарушение конфиденциальности информации (класс 2.1);
– нарушение целостности информации (класс 2.2);
– нарушение доступности информации, работоспособности системы (класс 2.3).

Этот классификационный признак является прямой проекцией трех основных типов угроз — раскрытия, целостности и отказа в обслуживании.

Одна из основных целей злоумышленников — получение несанкционированного доступа к информации. Существуют две принципиальные возможности доступа к информации: перехват и искажение. Возможность перехвата информации означает получение к ней доступа, но невозможность ее модификации. Следовательно, перехват информации ведет к нарушению ее конфиденциальности. Примером перехвата информации может служить прослушивание канала в сети. В этом случае имеется несанкционированный доступ к информации без возможности ее искажения. Очевидно также, что нарушение конфиденциальности информации является пассивным воздействием.

Возможность искажения информации означает либо полный контроль над информационным потоком между объектами системы, либо возможность передачи сообщений от имени другого объекта. Таким образом, очевидно, что искажение информации ведет к нарушению ее целостности. Описанное информационное разрушающее воздействие представляет собой яркий пример активного воздействия. Примером удаленной угрозы, цель которой — нарушение целостности информации, может служить типовая удаленная атака «ложный объект распределенной вычислительной сети».

Принципиально другая цель преследуется злоумышленником при реализации угрозы для нарушения работоспособности сети. В этом случае не предполагается получение несанкционированного доступа к информации. Его основная цель — добиться, чтобы узел сети или какой-то из сервисов, поддерживаемый им, вышел из строя и для всех остальных объектов сети доступ к ресурсам атакованного объекта был бы невозможен. Примером удаленной атаки, целью которой является нарушение работоспособности системы, может служить типовая удаленная атака «отказ в обслуживании».

- По условию начала осуществления воздействия. Удаленное воздействие, так же как и любое другое, может начать осуществляться только при определенных условиях. В вычислительных сетях можно выделить три вида условий начала осуществления удаленной атаки:

– атака по запросу от атакуемого объекта (класс 3.1);
– атака по наступлению ожидаемого события на атакуемом объекте (класс 3.2);
– безусловная атака (класс 3.3).

В первом случае злоумышленик ожидает передачи от потенциальной цели атаки запроса определенного типа, который и будет условием начала осуществления воздействия. Примером подобных запросов в сети Интернет служат DNS-запросы. Отметим, что данный тип удаленных атак наиболее характерен для распределенных вычислительных сетей.

Во втором случае злоумышленник осуществляет постоянное наблюдение за состоянием операционной системы удаленной цели атаки и при возникновении определенного события в этой системе начинает воздействие. Как и в предыдущем случае, инициатором осуществления начала атаки выступает сам атакуемый объект.

Реализация третьего вида атаки не связана ни с какими событиями и реализуется безусловно по отношению к цели атаки, т.е. атака осуществляется немедленно.

- По наличию обратной связи с атакуемым объектом:

– с обратной связью (класс 4.1);

– без обратной связи (однонаправленная атака) (класс 4.2).

Удаленная атака, осуществляемая при наличии обратной связи с атакуемым объектом, характеризуется тем, что на некоторые запросы, переданные на атакуемый объект, атакующему требуется получить ответ, а следовательно, между атакующим и целью атаки существует обратная связь, которая позволяет атакующему адекватно реагировать на все изменения, происходящие на атакуемом объекте.

В отличие от атак с обратной связью удаленным атакам без обратной связи не требуется реагировать на какие-либо изменения, происходящие на атакуемом объекте. Атаки данного вида обычно осуществляются передачей на атакуемый объект одиночных запросов, ответы на которые атакующему не нужны. Подобную удаленную атаку можно называть однонаправленной удаленной атакой. Примером однонаправленных атак является типовая удаленная атака «отказ в обслуживании».

- По расположению субъекта атаки относительно атакуемого объекта:

– внутрисегментное (класс 5.1);
– межсегментное (класс 5.2).

Напомним ряд определений.

Субъект атаки (или источник атаки) — это атакующая программа или злоумышленник, непосредственно осуществляющие воздействие.

Маршрутизатор (router) — устройство, обеспечивающее маршрутизацию пакетов обмена в глобальной сети.

Подсеть (subnetwork) (в терминологии Интернет) — совокупность хостов, являющихся частью глобальной сети, для которых маршрутизатором выделен одинаковый номер подсети. Хосты внутри одной подсети могут взаимодействовать между собой непосредственно, минуя маршрутизатор.

Сегмент сети — физическое объединение хостов. Например, сегмент сети образуют совокупность хостов, подключенных к серверу по схеме «общая шина». При такой схеме подключения каждый хост имеет возможность подвергать анализу любой пакет в своем сегменте.

С позиции удаленной атаки чрезвычайно важно, как по отношению друг к другу располагаются субъект и объект атаки, т.е. в одном или в разных сегментах они находятся. В случае внутрисегментной атаки, как следует из названия, субъект и объект атаки находятся в одном сегменте. При межсегментной атаке субъект и объект атаки находятся в разных сегментах.

Данный классификационный признак позволяет судить о так называемой «степени удаленности» атаки.

Важно отметить, что межсегментная удаленная атака представляет гораздо большую опасность, чем внутрисегментная. Это связано с тем, что в случае межсегментной атаки объект ее и непосредственно атакующий могут находиться на расстоянии многих тысяч километров друг от друга, что может существенно воспрепятствовать мерам по локализации субъекта атаки.

- По уровню модели ISO/OSI, на котором осуществляется воздействие:

– физический (класс 6.1);
– канальный (класс 6.2);
– сетевой (класс 6.3);
– транспортный (класс 6.4);
– сеансовый (класс 6.5);
– представительный (класс 6.6);
– прикладной (класс 6.7).

Классификация удаленных угроз приведена в табл. 4.3.

4.6. Типовые удаленные атаки и их характеристика

Как уже было показано ранее, распределенные вычислительные сети проектируются на основе одних и тех же принципов, а следовательно, имеют практически одинаковые проблемы безопасности, причем в большинстве случаев — независимо от используемых сетевых протоколов, топологии и инфраструктуры вычислительной сети.

С учетом этого специалисты в области информационной безопасности используют понятие типовой удаленной угрозы (атаки)[1], характерной для любых распределенных вычислительных сетей. Введение этого понятия в совокупности с описанием механизмов реализации типовых удаленных угроз позволяет выработать методику исследования безопасности вычислительных сетей, заключающуюся в последовательной умышленной реализации всех типовых удаленных угроз и наблюдению за поведением системы.

Типовая удаленная атака — это удаленное информационное разрушающее воздействие, программно осуществляемое по каналам связи и характерное для любой распределенной вычислительной сети.

[1] *Медведовский И.Д., Семьянов П.В., Платонов В.В.* Указ. соч.

Таблица 4.3

Классификация удаленных атак

Типовая удаленная атака	Характер воздействия		Цель воздействия			Условие начала			Наличие обратной связи		Расположение субъекта атаки		Уровень модели OSI						
	1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	5.1	5.2	6.1	6.2	6.3	6.4	6.5	6.6	6.7
Класс воздействия	+	–	+	–	–	–	–	+	–	+	+	–	–	+	–	–	–	–	–
Анализ сетевого трафика	–	+	+	+	+	+	+	+	+	+	+	+	+	–	+	+	+	+	+
Подмена доверенного объекта сети	–	+	+	+	+	+	+	–	+	+	+	+	+	–	+	+	+	+	–
Ложный объект сети	–	+	+	+	+	+	–	+	+	+	+	+	+	–	+	–	–	–	–
Отказ в обслуживании	–	+	–	–	+	–	–	+	–	+	+	+	–	+	+	+	+	+	+

Основной особенностью распределенной вычислительной сети является распределенность ее объектов в пространстве и связь между ними по физическим линиям связи. При этом все управляющие сообщения и данные, пересылаемые между объектами вычислительной сети, передаются по сетевым соединениям в виде пакетов обмена. Эта особенность привела к появлению специфичного для распределенных вычислительных сетей типового удаленного воздействия, заключающегося в прослушивании канала связи, называемого *анализом сетевого трафика*.

Анализ сетевого трафика позволяет:

- изучить логику работы распределенной вычислительной сети, что достигается перехватом и анализом пакетов обмена на канальном уровне (знание логики работы сети позволяет на практике моделировать и осуществлять другие типовые удаленные атаки);
- перехватить поток данных, которыми обмениваются объекты сети, т.е. удаленная атака данного типа заключается в получении несанкционированного доступа к информации, которой обмениваются пользователи (примером перехваченной при помощи данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети).

Одной из проблем безопасности распределенной сети является недостаточная идентификация и аутентификация (определение подлинности) удаленных друг от друга объектов. Основная трудность заключается в осуществлении однозначной идентификации сообщений, передаваемых между субъектами и объектами взаимодействия. Обычно в вычислительных сетях эта проблема решается использованием виртуального канала, по которому объекты обмениваются определенной информацией, уникально идентифицирующей данный канал. Для адресации сообщений в распределенных вычислительных сетях используется сетевой адрес, который уникален для каждого объекта системы (на канальном уровне модели OSI — это аппаратный адрес сетевого адаптера, на сетевом уровне — адрес определяется протоколом сетевого уровня, например, IP-адрес). Сетевой адрес также может использоваться для идентификации объектов сети.

В том случае, когда в вычислительной сети использует нестойкие алгоритмы идентификации удаленных объектов, оказывается возможной типовая удаленная атака, заключающаяся в передаче по каналам связи сообщений от имени произвольного объекта или субъекта сети, т.е. *подмена объекта* или *субъекта сети*.

Недостаточно надежная идентификация сетевых управляющих устройств (например, маршрутизаторов) является причиной возмож-

ного *внедрения в сеть ложного объекта* путем изменения маршрутизации пакетов, передаваемых в сети.

Современные глобальные сети представляют собой совокупность сегментов сети, связанных между собой через сетевые узлы. При этом маршрутом называется последовательность узлов сети, по которой данные передаются от источника к приемнику. Каждый маршрутизатор имеет специальную таблицу, называемую таблицей маршрутизации, в которой для каждого адресата указывается оптимальный маршрут. Таблицы маршрутизации существуют не только у маршрутизаторов, но и у любых хостов (узлов) в глобальной сети. Для обеспечения эффективной и оптимальной маршрутизации в распределенных сетях применяются специальные управляющие протоколы, позволяющие маршрутизаторам обмениваться информацией друг с другом (RIP (Routing Internet Protocol), OSPF (Open Shortest Path First)), уведомлять хосты о новом маршруте — ICMP (Internet Control Message Protocol), удаленно управлять маршрутизаторами — SNMP (Simple Network Management Protocol). Эти протоколы позволяют удаленно изменять маршрутизацию в сети Интернет, т.е. являются протоколами управления сетью.

Реализация данной типовой удаленной атаки заключается в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются объекты сети, и атака перейдет во вторую стадию, связанную с приемом, анализом и передачей сообщений, получаемых от дезинформированных объектов вычислительной сети.

Получив контроль над проходящим потоком информации между объектами, ложный объект вычислительной сети может применять различные методы воздействия на перехваченную информацию, например:

1) селекция потока информации и сохранение ее на ложном объекте (нарушение конфиденциальности);

2) модификация информации: модификация данных (нарушение целостности); модификация исполняемого кода и внедрение разрушающих программных средств — программных вирусов (нарушение доступности, целостности);

3) подмена информации (нарушение целостности).

Одной из основных задач, возлагаемых на сетевую операционную систему, функционирующую на каждом из объектов распределенной

вычислительной сети, является обеспечение надежного удаленного доступа с любого объекта сети к данному объекту. В общем случае в сети каждый субъект системы должен иметь возможность подключиться к любому объекту сети и получить в соответствии со своими правами удаленный доступ к его ресурсам. Обычно в вычислительных сетях возможность предоставления удаленного доступа реализуется следующим образом: на объекте в сетевой операционной системе запускаются на выполнение ряд программ-серверов (например, FTP-сервер, WWW-сервер и т.п.), предоставляющих удаленный доступ к ресурсам данного объекта. Указанные программы-серверы входят в состав телекоммуникационных служб предоставления удаленного доступа. Задача сервера состоит в том, чтобы постоянно ожидать получения запроса на подключение от удаленного объекта и, получив такой запрос, передать на запросивший объект ответ, в котором либо разрешить подключение, либо нет. По аналогичной схеме происходит создание виртуального канала связи, по которому обычно взаимодействуют объекты сети. В этом случае непосредственно операционная система обрабатывает приходящие извне запросы на создание виртуального канала и передает их в соответствии с идентификатором запроса (номер порта) прикладному процессу, которым служит соответствующий сервер. В зависимости от различных параметров объектов вычислительной сети, основными из которых являются быстродействие узлов, объем оперативной памяти и пропускная способность канала связи — число одновременно устанавливаемых виртуальных подключений ограничено, соответственно, ограничено и число запросов, обрабатываемых в единицу времени. С этой особенностью работы вычислительных сетей связана типовая удаленная атака *«отказ в обслуживании»*.

Результат применения этой удаленной атаки — нарушение на атакованном объекте работоспособности соответствующей службы предоставления удаленного доступа, т.е. невозможность получения удаленного доступа с других объектов вычислительной сети — отказ в обслуживании. Одна из разновидностей этой типовой удаленной атаки состоит в передаче с одного адреса такого числа запросов на атакуемый объект, которое позволяет трафик. В этом случае если в системе не предусмотрены правила, ограничивающие число принимаемых запросов с одного объекта (адреса) в единицу времени, то результатом такой атаки может быть как переполнение очереди запросов и отказ одной из телекоммуникационных служб, так и полная остановка компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов. И последней, третьей, разновидностью атаки «отказ в обслу-

живании» является передача на атакуемый объект некорректного, специально подобранного запроса. В этом случае при наличии ошибок в удаленной системе возможно зацикливание процедуры обработки запроса, переполнение буфера с последующим зависанием системы.

Основными причинами успеха удаленных угроз в вычислительных сетях являются следующие:

1. Отсутствие выделенного канала связи между объектами сети.
2. Недостаточная идентификация объектов и субъектов сети.
3. Взаимодействие объектов без установления виртуального канала.
4. Отсутствие в распределенных вычислительных сетях полной информации о ее объектах.
5. Отсутствие в распределенных вычислительных сетях криптозащиты сообщений.

4.7. Механизмы обеспечения информационной безопасности в информационных системах

4.7.1. Идентификация и аутентификация

Идентификация и аутентификация применяются для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

Общий алгоритм работы таких систем заключается в том, чтобы получить от субъекта (например, пользователя) информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

Наличие процедур аутентификации и/или идентификации пользователей является обязательным условием любой защищенной системы, поскольку все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами информационных систем.

Дадим определения этих понятий.

Идентификация — присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

Аутентификация (установление подлинности) — проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке, является ли подключающийся субъект тем, за кого он себя выдает.

При построении систем идентификации и аутентификации возникает проблема выбора идентификатора, на основе которого осуществляются процедуры идентификации и аутентификации пользователя. В качестве идентификаторов обычно используют:

- набор символов (пароль, секретный ключ, персональный идентификатор и т.п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи);
- физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т.п.) или особенности поведения (особенности работы на клавиатуре и т.п.).

Наиболее распространенными, простыми и привычными являются методы аутентификации, основанные *на паролях* — конфиденциальных идентификаторах субъектов. В этом случае при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам системы.

Парольные методы аутентификации по степени изменяемости паролей делятся на:

- методы, использующие постоянные (многократно используемые) пароли;
- методы, использующие одноразовые (динамично изменяющиеся) пароли.

Использование одноразовых или динамически меняющихся паролей является более надежным методом парольной защиты.

В последнее время получили распространение комбинированные методы идентификации и аутентификации, требующие помимо знания пароля наличие карточки (token) — специального устройства, подтверждающего подлинность субъекта.

Карточки разделяют на два типа:

- пассивные (карточки с памятью);
- активные (интеллектуальные карточки).

Самыми распространенными являются пассивные карточки с магнитной полосой, которые считываются специальным устройством, имеющим клавиатуру и процессор. При использовании указанной карточки пользователь вводит свой идентификационный номер. В случае его совпадения с электронным вариантом, закодированным в карточке, пользователь получает доступ в систему. Это позволяет достоверно установить лицо, получившее доступ к системе, и исключить несанкционированное использование карточки злоумышленником (например, при ее утере). Такой способ часто называют двухкомпонентной аутентификацией.

Интеллектуальные карточки имеют кроме памяти собственный микропроцессор. Это позволяет реализовать различные варианты парольных методов защиты, например многоразовые пароли, динамически меняющиеся пароли.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100%-ную идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако эти методы нельзя использовать при идентификации процессов или данных (объектов данных), они только начинают развиваться, требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, по почерку, по тембру голоса и др.

Новейшим направлением аутентификации является доказательство подлинности удаленного пользователя по его местонахождению. Данный защитный механизм основан на использовании системы космической навигации типа GPS (Global Positioning System). Пользователь, имеющий аппаратуру GPS, многократно посылает координаты заданных спутников, находящихся в зоне прямой видимости. Подсистема аутентификации, зная орбиты спутников, может с точностью до метра определить местоположение пользователя. Высокая надежность аутентификации определяется тем, что орбиты спутников подвержены колебаниям, предсказать которые достаточно трудно. Кроме того, координаты постоянно меняются, что исключает их перехват. Такой метод аутентификации может быть использован в случаях, когда авторизованный удаленный пользователь должен находиться в нужном месте.

Общая процедура идентификации и аутентификации пользователя при его доступе в защищенную информационную систему заключается в следующем. Пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предъявляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами. Если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий. В случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор. В тех случаях, когда пользователь превышает лимит возможных повторов ввода информации (ограничение на число повторов является обязательным условием для защищенных систем) система временно блокируется и выдает сообщение о несанкционированных действиях (причем, может быть, и незаметно для пользователя).

Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

В целом аутентификация по уровню ИБ делится на три категории:

1) статическая;
2) устойчивая;
3) постоянная.

Первая категория обеспечивает защиту только от несанкционированных действий в системах, где нарушитель не может во время сеанса работы прочитать аутентификационную информацию. Примером средства статической аутентификации являются традиционные постоянные пароли. Их эффективность преимущественно зависит от сложности угадывания паролей и, собственно, от того, насколько хорошо они защищены.

Устойчивая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Реализациями устойчивой аутентификации являются системы, использующие одноразовые пароли и электронные подписи. Устойчивая аутентификация обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и использовать ее в следующих сеансах работы.

Однако устойчивая аутентификация не обеспечивает защиту от активных атак, в ходе которых маскирующийся злоумышленник может оперативно (в течение сеанса аутентификации) перехватить, модифицировать и вставить информацию в поток передаваемых данных.

Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.

4.7.2. Методы разграничения доступа

После выполнения идентификации и аутентификации подсистема защиты устанавливает полномочия (совокупность прав) субъекта для последующего контроля санкционированного использования объектов ИС.

Обычно полномочия субъекта представляются: списком ресурсов, доступным пользователю, и *правами по доступу* к каждому ресурсу из списка.

Существуют следующие методы разграничения доступа:

1) разграничение по спискам;
2) использование матрицы установления полномочий;
3) разграничение по уровням секретности и категориям;
4) парольное разграничение.

При разграничении доступа по спискам задаются соответствия: каждому пользователю — список ресурсов и прав доступа к ним или каждому ресурсу — список пользователей и их прав доступа к данному ресурсу.

Списки позволяют установить права с точностью до пользователя. Здесь нетрудно добавить права или явным образом запретить доступ. Списки используются в подсистемах безопасности операционных систем и систем управления базами данных.

Использование матрицы установления полномочий подразумевает применение матрицы доступа (таблицы полномочий). В указанной матрице строками являются идентификаторы субъектов, имеющих доступ в ИС, а столбцами — объекты (ресурсы) ИС. Каждый элемент матрицы может содержать имя и размер предоставляемого ресурса, право доступа (чтение, запись и др.), ссылку на другую информационную структуру, уточняющую права доступа, ссылку на программу, управляющую правами доступа и др.

Данный метод предоставляет более унифицированный и удобный подход, так как вся информация о полномочиях хранится в виде единой таблицы, а не в виде разнотипных списков. Недостатками матрицы являются ее возможная громоздкость и неоптимальность (большинство клеток — пустые). Фрагмент матрицы установления полномочий показан в табл. 4.4.

Таблица 4.4

Матрица полномочий

Субъект	*Диск c:*	*Файл d:\prog. exe*	*Принтер*
Пользователь 1	Чтение Запись Удаление	Выполнение Удаление	Печать Настройка параметров
Пользователь 2	Чтение	Выполнение	Печать с 17:00 до 9:00
Пользователь 3	Чтение Запись	Выполнение	Печать с 17:00 до 9:00

Разграничение доступа по уровням секретности и категориям заключается в разделении ресурсов ИС по уровням секретности и категориям.

При разграничении по степени секретности выделяют несколько уровней, например: общий доступ, конфиденциально, секретно, совершенно секретно. Полномочия каждого пользователя задаются в соответствии с максимальным уровнем секретности, к которому он допущен. Пользователь имеет доступ ко всем данным, имеющим уровень конфиденциальности не выше, чем ему определен. Например, пользователь имеющий доступ к данным «секретно», также имеет доступ к данным «конфиденциально» и «общий доступ».

При разграничении по категориям задается и контролируется ранг категории пользователей. Соответственно, все ресурсы ИС разделяются по уровням важности, причем определенному уровню соответствует категория пользователей.

Парольное разграничение, очевидно, представляет использование методов доступа субъектов к объектам по паролю. При этом используются все методы парольной защиты. Очевидно, что постоянное использование паролей создает неудобства пользователям и временные задержки. Поэтому указанные методы используют в исключительных ситуациях.

На практике обычно сочетают различные методы разграничения доступа. Например, первые три метода усиливают парольной защитой.

Разграничение прав доступа является обязательным элементом защищенной ИС.

В ГОСТе Р 50739–95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации» и в документах ФСТЭК определены два вида (принципа) управления доступом:

- дискретное;
- мандатное.

Дискретное управление доступом представляет собой разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту. Данный вид организуется на базе методов разграничения по спискам или с помощью матрицы.

Мандатное управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах (файлы, папки, рисунки) и официального разрешения (допуска) субъекта к информации соответствующего уровня конфиденциальности.

4.7.3. Регистрация и аудит

Регистрация является еще одним механизмом обеспечения защищенности ИС. Этот механизм основан на подотчетности системы обе-

спечения безопасности, фиксирует все события, касающиеся безопасности, такие как:

- вход и выход субъектов доступа;
- запуск и завершение программ;
- выдача печатных документов;
- попытки доступа к защищаемым ресурсам;
- изменение полномочий субъектов доступа;
- изменение статуса объектов доступа и т.д.

Эффективность системы безопасности принципиально повышается в случае дополнения механизма регистрации механизмом аудита. Это позволяет оперативно выявлять нарушения, определять слабые места в системе защиты, анализировать закономерности системы, оценивать работу пользователей.

Аудит — это анализ накопленной информации, проводимый оперативно в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация механизмов регистрации и аудита позволяет решать следующие задачи обеспечения ИБ:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений ИБ;
- предоставление информации для выявления и анализа проблем.

Рассматриваемые механизмы регистрации и аудита являются сильным психологическим средством, напоминающим потенциальным нарушителям о неотвратимости наказания за несанкционированные действия, а пользователям — за возможные критические ошибки.

Практическими средствами регистрации и аудита являются:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный) журнал.

Первое средство является обычно дополнением к мониторингу, осуществляемому администратором системы. Комплексный подход к протоколированию и аудиту обеспечивается при использовании регистрационного журнала.

Регистрационный журнал — это хронологически упорядоченная совокупность записей результатов деятельности субъектов системы, достаточная для восстановления, просмотра и анализа последовательности действий, окружающих или приводящих к выполнению операций, процедур или совершению событий при транзакции с целью контроля конечного результата.

Фрагмент журнала безопасности подсистемы регистрации и аудита операционной системы показан на рис. 4.5

Безопасность 13 событий

Тип	Дата	Время	Источник	Категория	Событие	Пользователь	Компьютер
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	админ	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	562	админ	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Учетные записи	643	админ	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	админ	GHJ
Аудит успехов	26.04.2004	5:35:02	Security	Доступ к объектам	560	админ	GHJ
Аудит успехов	26.04.2004	5:34:49	Security	Доступ к объектам	562	админ	GHJ

Рис. 4.5. Фрагмент журнала безопасности подсистемы регистрации и аудита операционной системы

Обнаружение попыток нарушений ИБ входит в функции активного аудита, задачами которого являются оперативное выявление подозрительной активности и предоставление средств для автоматического реагирования на нее.

Под *подозрительной активностью* понимается поведение пользователя или компонента ИС, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям). Например, подсистема аудита, отслеживая процедуру входа (регистрации) пользователя в систему, подсчитывает число неудачных попыток входа. В случае превышения установленного порога таких попыток подсистема аудита формирует сигнал о блокировке учетной записи данного пользователя.

Организация регистрации событий, связанных с безопасностью ИС, включает, как минимум, три этапа:

1) сбор и хранение информации о событиях;
2) защита содержимого журнала регистрации;
3) анализ содержимого журнала регистрации.

На первом этапе определяются данные, подлежащие сбору и хранению, период чистки и архивации журнала, степень централизации управления, место и средства хранения журнала, возможность регистрации шифрованной информации и др. Регистрируемые данные должны быть защищены в первую очередь от несанкционированной модификации и, возможно, раскрытия. Самым важным этапом является анализ регистрационной информации. Известны несколько методов анализа информации с целью выявления несанкционированных действий.

Статистические методы основаны на накоплении среднестатистических параметров функционирования подсистем и сравнении текущих параметров с ними. Наличие определенных отклонений может сигнализировать о возможности появления некоторых угроз.

Эвристические методы используют модели сценариев несанкционированных действий, которые описываются логическими правилами, или модели действий, по совокупности приводящие к несанкционированным действиям.

4.7.4. Межсетевое экранирование

Одним из эффективных механизмов обеспечения ИБ в распределенных вычислительных сетях является экранирование, выполняющее функции разграничения информационных потоков на границе защищаемой сети.

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым обеспечивая все составляющие ИБ. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет *межсетевой экран*, или *брандмауэр* (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в ИС и/или выходящих из нее, и обеспечивает защиту ИС посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны классифицируются по следующим признакам:

- по месту расположения в сети — на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;
- по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет. Внутренние сетевые экраны могут поддерживать несколько протоколов. Например, при использовании сетевой операционной системы Novell Netware следует принимать во внимание протокол SPX/IPX.

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI. Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Межсетевые экраны разделяют на четыре типа:

- межсетевые экраны с фильтрацией пакетов;

- шлюзы сеансового уровня;
- шлюзы прикладного уровня;
- межсетевые экраны экспертного уровня.

Типы межсетевых экранов для соответствующих уровней модели ISO/OSI приведены в табл. 4.5.

Таблица 4.5

Типы межсетевых экранов и уровни модели ISO/OSI

№ п/п	Уровень модели OSI	*Протокол*	*Тип межсетевого экрана*
1	Прикладной	Telnet, FTP, DNS, NFS, SMTP, HTTP	Шлюз прикладного уровня. Межсетевой экран экспертного уровня.
2	Представления данных	–	–
3	Сеансовый	TCP, UDP	Шлюз сеансового уровня
4	Транспортный	TCP, UDP	–
5	Сетевой	IP, ICMP	Межсетевой экран с фильтрацией пакетов
6	Канальный	ARP, RAP	–
7	Физический	Ethernet	–

Межсетевые экраны с фильтрацией пакетов представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их со сконфигурированной таблицей правил. Эти межсетевые экраны просты в использовании, дешевы, оказывают минимальное влияние на производительность вычислительной системы. Основным недостатком является их уязвимость при подмене IP-адресов. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

Шлюзы сеансового уровня контролируют допустимость сеанса связи. Они следят за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т.е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функцию трансляции сетевых адресов, которая скрывает внутренние IP-адреса, тем самым исключая подмену IP-адреса.

Однако в таких межсетевых экранах отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

Шлюзы прикладного уровня проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип межсетевого экрана, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб сети Интернет (HTTP, FTP, Telnet и т.д.) и служат для проверки сетевых пакетов на наличие достоверных данных.

Описываемые шлюзы снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно при работе в Интернет при работе по низкоскоростным каналам, но существенно при работе во внутренней сети.

Межсетевые экраны экспертного уровня сочетают в себе элементы всех трех описанных ранее категорий. Как и межсетевые экраны с фильтрацией пакетов, они работают на сетевом уровне модели OSI, фильтруя входящие и исходящие пакеты на основе проверки IP-адресов и номеров портов. Рассматриваемые экраны также выполняют функции шлюза сеансового уровня, определяя, относятся ли пакеты к соответствующему сеансу. И, наконец, брандмауэры экспертного уровня берут на себя функции шлюза прикладного уровня, оценивая содержимое каждого пакета в соответствии с политикой безопасности, выработанной в конкретной организации.

Вместо применения связанных с приложениями программ-посредников брандмауэры экспертного уровня используют специальные алгоритмы распознавания и обработки данных на уровне приложений. С помощью этих алгоритмов пакеты сравниваются с известными шаблонами данных, что теоретически должно обеспечить более эффективную фильтрацию пакетов.

4.7.5. Технология виртуальных частных сетей

Технология виртуальных частных сетей (VPN — Virtual Private Network) является одним из эффективных механизмов обеспечения ИБ при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети являются комбинацией нескольких самостоятельных сервисов (механизмов) безопасности:

- шифрования (с использование инфраструктуры криптосистем) на выделенных шлюзах (шлюз обеспечивает обмен данными между вычислительными сетями, функционирующими по разным протоколам);
- экранирования (с использованием межсетевых экранов);
- туннелирования.

Сущность технологии VPN представлена на рис. 4.6.

На все компьютеры, имеющие выход в Интернет (вместо Интернета может быть и любая другая сеть общего пользования), устанавливаются VPN-агенты, которые обрабатывают IP-пакеты, передаваемые по вычислительным сетям. Перед отправкой IP-пакета VPN-агентом выполняются следующие операции:

1) анализируется IP-адрес получателя пакета, в зависимости от этого адреса выбирается алгоритм защиты данного пакета (VPN-агенты могут поддерживать одновременно несколько алгоритмов шифрования и контроля целостности), кроме того, пакет может и вовсе быть отброшен, если в настройках VPN-агента такой получатель не значится;
2) вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;
3) пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);
4) формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета).

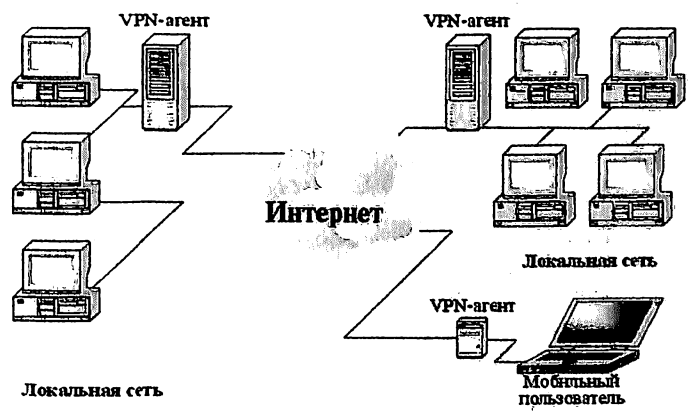


Рис. 4.6. Технология VPN

В результате этого обмен данными между двумя локальными сетями снаружи представляется как обмен между двумя компьютерами, на которых

установлены VPN-агенты. Всякая полезная для внешней атаки информация, например внутренние IP-адреса сети, в этом случае недоступна.

При получении IP-пакета выполняются обратные действия:

1) из заголовка пакета извлекается информация о VPN-агенте отправителя пакета, если такой отправитель не входит в число разрешенных, то пакет отбрасывается (то же самое происходит при приеме пакета с намеренно или случайно поврежденным заголовком);
2) согласно настройкам выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);
3) после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов является незаметной для пользователей. Сложной является только настройка VPN-агентов, которая может быть выполнена только очень опытным пользователем. VPN-агент может находиться непосредственно на защищаемом компьютере (что особенно полезно для мобильных пользователей). В этом случае он защищает обмен данными только одного компьютера, на котором он установлен.

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами. Такой канал называется туннелем, а технология его создания называется туннелированием (рис. 4.7). Вся информация передается по туннелю в зашифрованном виде.

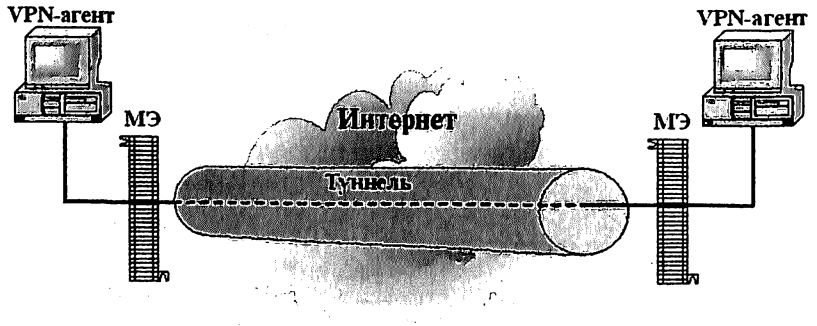


Рис. 4.7. Пример расположения межсетевых экранов

Одной из обязательных функций VPN-агентов является фильтрация пакетов. Она реализуется в соответствии с настройками VPN-агента, совокупность которых образует политику безопасности виртуальной частной сети. Для повышения защищенности виртуальных частных сетей на концах туннелей целесообразно располагать межсетевые экраны.

4.8. Современные DDoS-атаки как угроза для бизнеса в Интернете

4.8.1. Основные виды DDoS-атак

В настоящее время наблюдается массовый выход бизнеса в Интернет: системы онлайн-банкинга, всевозможные порталы (игровые, медиа, образовательные), интернет-магазины и пр. Практически каждая организация имеет собственный сайт, даже фрилансеры стараются завести себе страничку-визитку в Интернете, чтобы привлечь наибольшее количество клиентов, обрести популярность, эффективно заработать.

DoS-атака (от англ. Denial of Service) — атака, направленная на отказ в обслуживании ресурса или канала.

DDoS-атака (от англ. Distributed Denial of Service) — множественная *DoS*-атака, осуществляемая из нескольких источников.

DDoS — распределенные атаки типа «отказ в обслуживании» направлены в первую очередь на доступность ресурса, поэтому наиболее подвержены таким атакам те сферы бизнеса, которые напрямую зависят от доступности ресурса пользователям, например: туристические фирмы, системы онлайн-банкинга, игровые порталы, интернет-магазины, порталы государственных услуг, облачные сервисы, и даже онлайн-ресурсы образовательных организаций (электронные дневники, системы дистанционного обучения) и др.

Причины таких атак могут быть различны: конкуренция, вымогательство, протест, личная неприязнь или просто ради развлечения, но самая распространенная причина, по мнению экспертов, для серьезных атак на крупный и средний бизнес — это сокрытие факта другой атаки, т.е. попросту отвлечение внимания.

Цель DDoS-атаки — заблокировать на некоторое время доступ к онлайн-ресурсу путем перегрузки канала «мусорными» запросами, в результате чего бизнес несет существенные финансовые и репутационные потери. Ситуация усугубляется тем, что DDoS-атаку сегодня может организовать практически любой желающий — стоимость ее невелика, контакты исполнителей можно найти при помощи поисковых сервисов. Доступность и простота организации DDoS-атаки ставят под угрозу практически любую компанию, у которой есть недоброжелатели. Количество пострадавших варьируется в зависимости от географической принадлежности и сферы деятельности фирмы.

Даже если злоумышленникам не удается полностью лишить пользователя доступа к информационным ресурсам компании, их частичная недоступность также является серьезной проблемой. Многие организации по-прежнему не считают DDoS-атаки серьезной угрозой. В то же время недоступность сайта и неудавшиеся транзакции — это только вершина айсберга. Если в случае взлома системы злоумышленники крадут данные клиентов и конфиденциальную информацию, то DDoS-атака может стать причиной потери репутации, оттока существующих клиентов или исков за непредоставленные услуги.

DDoS-атаки можно разделить на три обширные группы:

атаки на канал — данная категория атак направлена на насыщение полосы пропускания;

атаки на уровне протоколов — эта категория направлена на ограничение оборудования или уязвимости различных протоколов;

атаки на уровне приложений — такие атаки направлены на уязвимости в приложениях и операционных системах, они приводят к неработоспособности какого-либо приложения или ОС в целом.

Рассмотрим основные виды DDoS-атак:

ICMP-флуд (Smurf-атака). В этом случае по широковещательному адресу злоумышленник отправляет поддельный ICMP-пакет, в котором адрес атакующего меняется на адрес жертвы. Все узлы присылают ответ на данный *ping*-запрос.

UDP-флуд. Этот вид атак использует UDP-протокол. Его характерные особенности — отсутствие необходимости в установлении сессии и отправки какого-либо ответа. На случайные порты хост-машины приходит бесчисленное количество пакетов, принуждая постоянно проверять, слушает ли данный порт какое-то приложение, и в случае ошибки возвращать пакет «ICMP Destination Unreachable». Естественно, такая активность поглощает ресурсы хост-машины, приводя к ее недоступности.

SYN-флуд. Данный вид атаки основан на попытке запуска большого числа одновременных TCP-соединений через посылку SYN-пакета с несуществующим обратным адресом. После нескольких попыток отослать в ответ ACK-пакет на недоступный адрес большинство операционных систем ставят неустановленное соединение в очередь. И только после n-ой попытки закрывают соединение. Поскольку поток ACK-пакетов очень большой, вскоре очередь оказывается заполненной, и ядро отказывает в попытках открыть новое соединение.

HTTP-флуд. В этом случае атакующий отсылает небольшие HTTP-пакеты, которые заставляют в свою очередь отвечать сервер пакетами, размеры которых значительно больше. Тем самым злоумышленник

имеет большой шанс насытить полосу пропускания жертвы и вызвать отказ в работе сервисов.

Отраженная DDoS-атака с усилением. Эта атака основана на транспортном протоколе *UDP*, который активно используется многими важными интернет-сервисами, в частности DNS (всем известный Domain Name Service) и NTP (менее известный Network Time Protocol), хотя сегодня уже ведутся атаки и с помощью сервисов потокового вещания. Самое главное в этом случае, что нет «рукопожатия», т.е. сервис «не проверяет» адрес отправителя. Другими словами, кто угодно может послать UDP-пакет от чьего угодно имени (IP-адреса). Соответственно, атакующий посылает UDP-пакет на сервис (обычно DNS или NTP) от имени жертвы (с ее IP-адреса) и сервис отвечает не на IP-адрес атакующего, а на IP-адрес жертвы. Вот почему и название у атаки — «отражение». Но этого недостаточно для успешной DDoS-атаки. В названии присутствует еще слово «усиление». В данном случае у DNS- и NTP-служб есть приятная для атакующего особенность — множитель. Это выглядит следующим образом: атакующий от имени жертвы отправляет на DNS- или NTP-сервер пакет размером 1 кбайт, а DNS- или NTP-сервер отвечает на адрес жертвы пакетом в n-раз больше. Вот это и есть то самое усиление, о котором было сказано в самом начале. Отсюда и название «усиленная отраженная DDoS-атака».

Slow HTTP Post. Атака заключается в отправке серверу большого HTTP POST-запроса маленькими частями (по 1 байту). По стандарту HTTP-сервер должен дождаться полной передачи данных (получив содержимое размером 1 байт) и может закрывать соединение только по таймауту. Таким образом, в случае подобной DDoS-атаки медленными соединениями атакуемый сервер открывает огромное количество соединений, катастрофически расходуя свои ресурсы.

Slow HTTP headers. Эта атака аналогична методу Slow HTTP Post, только вместо пост-запроса используется медленная отправка заголовка HTTP. Как и при атаке методом Slow Post, сервер ждет окончания заголовков, прежде чем закрыть соединение, что приводит к большому количеству открытых соединений и как следствие — к перегрузке сервера. Подобные DDoS-атаки сложно отличить от обычных запросов с медленным соединением.

Фальшивые Googlebots. Это сравнительно новая технология совершения DDoS-атак. Ее особенностью является использование ботов, маскирующихся под Googlebots — роботов поисковой системы Google, которые отслеживают появление и обновление web-страниц для индексации сайтов в поисковых системах.

Существует множество других типов атак и зачастую кажется, что возможности злоумышленников безграничны, но это утверждение верно, только если ничего не предпринимать.

4.8.2. Способы защиты от DDoS-атак

Способ защиты, к которому обычно прибегают первоначально, — это организация самостоятельной защиты, но подобный вид мер безопасности способен нейтрализовать лишь самые простые атаки: запрет протоколов ICMP и UDP могут значительно облегчить жизнь, но только до определенного уровня. Также защиту может предоставлять хостинг-провайдер или оператор связи, но их возможности ограничены доступным для них каналом и ни один, ни другой не будут разбирать высокоуровневые протоколы HTTP / HTTPS.

Лучшей практикой будет использование облачного решения. Однако облако, которое действительно защищает от DDoS-атак, должно обладать следующими свойствами:

- *Распределенность*. В облаке должно быть несколько географически разнесенных узлов, чтобы вывод из строя любого из них не оказывал влияния на сервис.
- *Собственная автономная система и собственные адресные блоки*, из которых для защищаемого сервиса выделяется новый IP-адрес, скрывающий истинное его расположение в сети.
- *Глобальная связность автономной системы с Интернетом*. Только магистральные операторы в качестве провайдеров облачных сервисов дадут уверенность клиентам, находящимся под защитой облачного решения, в том, что их трафик не будет теряться вне зависимости от того, какие атаки осуществляются.
- *Полная автоматизация процесса фильтрации*. У хорошей системы защиты от DDoS-атак — тысячи клиентов и сотни инцидентов в день. Этот объем невозможно обработать вручную. Ручное вмешательство порождает ошибки, так как человек должен оперативно решать, какие фильтры подключать и пр., что не всегда приводит к нужному результату.
- *Постоянная фильтрация* должна быть приоритетной услугой, поскольку любое переключение по протоколу BGP или DNS означает время простоя сайта, измеряемое десятками минут, и раскрытие истинного местоположения сервера.
- *Использование технологии MPLS (Multiprotocol Label Switching) VPN* в качестве резервной связности системы защиты и сервера. Это позволит даже при полностью забитых «мусором» каналах датацентра сохранить полную работоспособность сервера.
- *Использование статического контента на CDN* (от англ. Content Delivery Network — сеть доставки контента, географически распределенная сетевая инфраструктура, позволяющая оптимизировать доставку и дистрибуцию контента конечным пользователям в сети Интернет).

Сам сервер должен обладать рядом качеств, которые позволят ему быть всегда доступным для клиента. Среди них: возможность выдерживать рост легитимной нагрузки; поддерживать структуру «один сервер — один сервис» (Web должен быть на своем сервере единственным приложением), иначе атакующая сторона узнает его IP, например, из записи MX (Mail Exchanger), указывающей способ маршрутизации электронной почты, или Web-сервер может быть выведен из строя исчерпанием ресурсов процессора за счет другого сервиса. Очень желательно использовать устойчивый распределенный DNS.

Какой бы метод защиты от DDoS ни выбрала компания, главное помнить, что к атакам нужно быть готовым заранее. Кроме того, построенная IT-инфраструктура должна полностью соответствовать объемам бизнеса компании, что поможет минимизировать ущерб и не потерять лояльность клиентов.

DDoS-атакам подвержены организации любых масштабов — от малых до крупных, однако, по данным Лаборатории Касперского[1], в прошедшем году активнее всего атакам подвергались предприятия среднего и малого бизнеса (рис. 4.8).

На финансовые сервисы напрямую пришлось лишь 12% от всех атак, но данный вид атак не направлен на прямой вывод средств, а осуществляется в первую очередь на те ресурсы, доступность которых важнее всего для функционирования компании. Интересен тот факт, что зачастую такие атаки проводятся, чтобы отвлечь внимание от других, более серьезных атак.

Длительность атак может быть от нескольких минут до нескольких часов и даже дней, все зависит от атакуемого ресурса, его системы защиты, скорости реагирования на инциденты, мощностей атакующего, метода, выбранного для атаки. По мнению экспертов, число DDoS-атак уверенно росло в течение всего прошедшего года, что в условиях кризиса связано с обострившейся конкурентной борьбой.

[1] Отчет Лаборатории Касперского. DDoS-атаки за 2017 год. URL:https://securelist.ru.

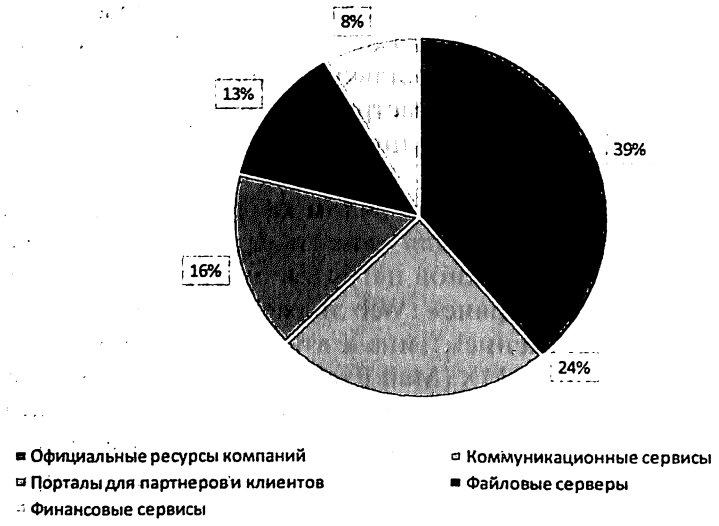


Рис. 4.8. Соотношение сервисов, подвергшихся DDoS-атакам за 2017 г.

Таблица 4.6, в которой рассматриваются различные сервисы и сферы бизнеса в Интернете, а также вероятные причины DDoS-атак на них, наглядно демонстрирует, что атакован может быть ресурс любой направленности и любых масштабов[1]. Например, такое явление, как хактивизм (синтез социальной активности и хакерства), сейчас встречается повсеместно в сводках по информационной безопасности, и довольно сложно понять истинные мотивы людей, которые им занимаются. От таких злоумышленников не застрахован никто.

Строя грамотную стратегию защиты от DDoS-атак, важно помнить о том, что перекрытие всей подсети несет риск блокировки доступа к ресурсу для легальных клиентов. Однако этот способ отлично подойдет для защиты внутренних серверов организации. Следует отметить, что нет универсального средства борьбы.

Для защиты от DDoS-атак помимо привлечения средств защиты и третьих лиц необходимо провести ряд превентивных мер, перечисленных ниже.

[1] Бабаш А.В., Баранова Е.К. Актуальные вопросы защиты информации: монография / А.В.Бабаш, Е.К. Баранова. — М.: РИОР:ИНФРА-М, 2017.

Таблица 4.6

Соотношение сервисов и причин DDoS-атак на них

Целевые ресурсы	Мотивы	шантаж	хактивизм	онлайн-протест	манипулирование рынком	конкурентное преимущество	вымогательство	политические взгляды	ведение информационной войны	получение политической выгоды	недовольство сотрудников
Финансовые сервисы	стоки и обменники	+	+	+	+						
	транснациональные банки	+	+	+	+						
	региональные банки	+	+	+	+						
	системы денежных переводов и платежные системы	+	+	+	+						
Интернет-торговля	транснациональные организации		+			+	+				
	интернет-магазины		+			+	+				
	онлайн-казино		+			+	+				
	игровые порталы		+			+	+				
Облачные сервисы	поставщики услуг		+			+		+			
	новостные и другие порталы		+			+		+	+		
Государственные сервисы	порталы предоставления государственных услуг		+	+				+	+	+	
	сайты политических организаций		+	+				+	+	+	
	сайты местного правительства (управы районов, городов и др.)		+	+				+	+	+	
Образовательные ресурсы	сайты университетов и школ		+	+							+
	системы дистанционного образования		+	+							+
	личные кабинеты		+	+							+
	другие образовательные порталы		+	+							+

Проведение анализа сети. Изучение объемов трафика в различные периоды времени необходимо для того, чтобы в самом начале обнаружить признаки аномального поведения и принять меры. Также на этом этапе следует провести анализ рисков и выявить наиболее критичные ресурсы, просчитать бюджет, который организация готова вложить в защиту от DDoS-атак, а также проанализировать уже осуществлявшиеся атаки (если они были) и последствия от них.

Назначение ответственных лиц и составление плана действий в случае чрезвычайной ситуации.

Проведение регулярного обучения сотрудников, задействованных в работе с защищаемым ресурсом.

Грамотная настройка межсетевого экрана, а также усовершенствование имеющихся ресурсов, если это возможно. Например, необходимо грамотно задать ограничения на ресурсы, соединения и таймауты, а также обратить внимание на настройки сетевой части (ядра) по ранее перечисленным параметрам.

После проведения перечисленных мер можно принимать решение о привлечении внешних организаций к защите от DDoS-атак.

Рассмотрим основные шаги по защите от DDoS-атак.

Идентифицирование типа трафика

Исходя из описанных ранее вариантов атак можно сделать вывод, что в большинстве случаев на ресурс посылается определенный тип трафика. Также верным признаком DDoS-атаки является наличие поддельных IP-адресов. Однако тут стоит помнить про DDoS-нападения, направленные против определенных служб типа HTTP, которые используют допустимый трафик и запросы. Для идентификации «вредного» трафика нужно анализировать весь трафик путем его записи в файл, последующего анализа и выделения преобладающего трафика. Контролировать входящий трафик можно и посредством маршрутизатора совместно со списками ограничения доступа.

Отслеживание источников атаки

На данном этапе основная проблема заключается в том, что DDoS-атаки распределены.

Ограничение допустимого предела определенного типа трафика

Здесь возникает глобальная проблема: с «вредным» трафиком есть шанс (и не маленький) отсечь и легальный трафик.

Последующий мониторинг

Помимо перечисленных методов защиты от DDoS-атак можно просто приобрести уже готовый продукт, который не предполагает активного участия администратора ресурса и основную часть работы выполняет самостоятельно. Так, проведенный опрос среди администраторов нескольких организаций выявил наиболее популярные продукты:

- *CloudFlare* — фильтрует трафик прежде, чем он попадает на сайт, имеет инструментарий для экстренной защиты от DDoS-атак, имеет бесплатную версию;
- *Kaspersky DDoS Prevention* — использует методы статистического, поведенческого и экспертного анализа;
- *Arbor* — позволяет конфигурировать систему защиты в зависимости от потребностей, обеспечивая тем самым комплексный подход к защите от атак. Позволяет работать в режиме «всегда включен», что обеспечивает защиту 24/7. Кроме того, система имеет дружественный интерфейс, что позволяет комфортно и продуктивно работать администратору безопасности.

Ведя бизнес, в Интернете стоит помнить, что DDoS-атака — это первый признак того, что злоумышленники параллельно ведут более серьезную и опасную атаку.

Большинство из предлагаемых на рынке программ, направленных на предотвращение атак типа «отказ в обслуживании», не подходят для небольших сетей или провайдеров, таким образом, необходимо уметь идентифицировать и фильтровать трафик. Также необходимо быть готовым к атаке и заранее спланировать стратегию защиты.

Несмотря на наличие предлагаемых «коробочных» средств для защиты от DDoS-атак, невозможно просто доверить им критически значимый ресурс для ведения бизнеса в Интернете, так как современные средства все равно предполагают в той или иной степени участие администратора. Также не стоит забывать о превентивных мерах, которые описаны выше и регулярном проведении мониторинга, так как технологии с каждым днем развиваются все стремительнее, а это значит, что злоумышленник получает все больше ресурсов, совершенствует навыки, использует эти технологии для реализации атак.

Принимая во внимание вышесказанное, следует помнить, что подход к защите информации бизнеса любых масштабов должен быть комплексным. Только так можно максимально оптимизировать расход ресурсов (финансовых, технических и человеческих) и добиться успеха в защите от подобного рода атак и всего того, что они могут за собой повлечь.

4.9. Угрозы информационной безопасности и методы защиты в облачных сервисах

4.9.1. Основные характеристики и модели облачных сервисов

Облачный сервис — это Интернет-сервис, предполагающий передачу части объектов IT-инфраструктуры на обслуживание сторонней организации (так называемый аутсорсинг). То есть по сути облачный сервис — это сервис на основе сложной компьютерной системы, которая требует довольно высоких вычислительных мощностей и затрат на техобслуживание. Самое лучшее определение понятию «облачные вычисления» дали американские специалисты Питер Мелл (Peter Mell) и Тим Грэнс (Tim Grance) из Лаборатории информационных технологий Национального института стандартов и технологий (*NIST*) в своей работе «The NIST Definition of Cloud Computing»[1]. Итак, облачные вычисления, по их версии, — это «модель предоставления удобного сетевого доступа в режиме "по требованию" к коллективно используемому набору настраиваемых ресурсов (например, сетей, серверов, хранилищ данных, приложений и/или сервисов), которые пользователь может оперативно задействовать под свои задачи и высвобождать при сведении к минимуму числа взаимодействий с поставщиком услуги или собственных управленческих усилий».

Работа в облаках обладает огромным потенциалом для компаний. Зачастую применение облачных вычислений — наилучший способ решения корпоративных задач, на которые не хватает мощности собственной IT-инфраструктуры. Помимо существенной экономической выгоды, важным аргументом использования этой технологии для многих компаний может стать возможность доступа к данным из любой точки планеты. Несмотря на все плюсы облачных сервисов, большинство компаний боятся их использовать по причине недоработки в области информационной безопасности. Информация, находящаяся в облачных сервисах, может подвергнуться атаке посредством уязвимостей как непосредственно облачной системы, так и решений, нацеленных на управление сервисами. Таким образом, актуальной является задача идентификации угроз информационной безопасности для облачных систем, анализа этих угроз и методов обеспечения информационной безопасности в облачных сервисах.

[1] Ссылка на оригинальный текст: https://csrc.nist.gov/publications/detail/sp/800-145/final.

Характеристики облачных вычислений, которые делают их столь привлекательными для бизнеса, следующие:

- *самообслуживание по требованию потребителя* — это возможность потребителя услуги не привлекать сотрудника вендора к решению повседневных задач бизнеса. Потребитель может сам в любое время получить доступ к хранилищу данных или воспользоваться серверным временем;
- *доступность через всемирную сеть Интернет* — это возможность взаимодействия потребителя услуги с потребляемыми ресурсами (программным обеспечением, базами данных, операционными системами) через сеть Интернет, посредством возможностей тонкого или толстого клиента;
- *объединение ресурсов* (хранилищ данных, вычислительной мощности, оперативной памяти, пропускной способности, виртуальных машин) в единый пул — это централизация поставщиком услуг вычислительных ресурсов для обслуживания большого числа клиентов (технология Multi-tenancy);
- *быстрая адаптация и оперативное масштабирование* — быстрое и гибкое резервирование вычислительных возможностей в соответствии с требованиями заказчика (потребителя ресурсов);
- *измеримая услуга* — автоматический контроль и оптимизация использованных ресурсов через измерение некоторых параметров (размер хранилища данных, пропускная способность канала передачи и ряд других).

В настоящее время выделяют следующие модели облачных сервисов.

Software-as-a-Service (*SaaS*) — модель продажи программного обеспечения, при которой поставщик разрабатывает веб-приложение и самостоятельно управляет им, предоставляя заказчикам доступ к программному обеспечению через Интернет.

Database-as-a-service (*DBaaS, «база данных как сервис»*) — облачный подход к хранению и управлению структурированными данными. Это одна из наиболее востребованных технологий в области управления информационными ресурсами. Суть концепции *DBaaS* в том, что пользователю не нужно устанавливать и поддерживать базу данных, ему достаточно произвести запрос и получить по нему базу данных. Для ее создания используются ресурсы частного, публичного или гибридного облака.

Desktop-as-a-Service (DaaS) — модель распространения и эксплуатации программного обеспечения, получившая известность в начале 2000-х гг. и являющаяся логическим продолжением *SaaS*. При предоставлении услуги *DaaS* клиенты получают полностью готовое к работе («под ключ»)

стандартизированное виртуальное рабочее место, которое каждый пользователь имеет возможность дополнительно настраивать под свои задачи. Таким образом, пользователь получает доступ не к отдельной программе, а к необходимому для полноценной работы программному комплексу. Физически доступ к рабочему месту пользователь может получить через локальную сеть или Интернет. В качестве терминала может использоваться персональный компьютер или ноутбук, нетбук и даже смартфон.

Platform-as-a-Service (PaaS, «платформа как услуга») — это модель предоставления облачных вычислений, при которой потребитель получает доступ к использованию информационно-технологических платформ, таких как ОС, СУБД, связующему ПО, средствам тестирования и разработки, размещенным у облачного провайдера.

Infrastructure-as-a-Service (IaaS) — инфраструктура, как услуга предоставляет возможность использования облачной инфраструктуры для самостоятельного управления ресурсами обработки, хранения, сетями и другими фундаментальными вычислительными ресурсами. Например, потребитель может устанавливать и запускать произвольное программное обеспечение, которое может включать в себя операционные системы, платформенное и прикладное программное обеспечение.

Особенности каждой из разновидностей облачных сервисов можно продемонстрировать на распределении зон ответственности между клиентом и облачным провайдером (табл. 4.7).

С точки зрения принадлежности различают четыре разновидности облачной инфраструктуры.

Частное облако (private cloud) — облачная инфраструктура, которая принадлежит непосредственно одной организации. Это не просто набор виртуальных машин, но и система мониторинга и управления. Она служит для анализа эффективности, корректности и оптимальности процессов, протекающих в частном облаке.

Преимущества: увеличенная возможность контроля; высокий уровень безопасности; высокая скорость трансфера данных внутри облаков данного типа.

Публичное облако (public cloud) — облачная инфраструктура, которая принадлежит множеству компаний. Наибольшее количество вопросов по информационной безопасности возникает именно в нем. Проверка безопасности устройств конечных пользователей становится одной из приоритетных задач в обеспечении ИБ публичного облака. Такая структура обладает неограниченными возможностями в плане масштабирования.

Таблица 4.7

Распределение зон ответственности между клиентом и облачным провайдером

Клиент	Облачный провайдер SaaS
Офис, электричество, рабочее место	Мониторинг, резервное копирование
ПК, ноутбуки, каналы связи	Администрирование приложений
	Администрирование баз данных
	Администрирование ОС
	Виртуализация
	Оборудование
	Системные инженеры
	Инфраструктура дата-центра

Клиент	Облачный провайдер PaaS
Офис, электричество, рабочее место	Администрирование баз данных
ПК, ноутбуки, каналы связи	Администрирование ОС
Мониторинг, резервное копирование	Виртуализация
Администрирование приложений	Оборудование
	Системные инженеры
	Инфраструктура дата-центра

Клиент	Облачный провайдер IaaS
Офис, электричество, рабочее место	Виртуализация
ПК, ноутбуки, каналы связи	Оборудование
Мониторинг, резервное копирование	Системные инженеры
Администрирование приложений баз данных и ОС	Инфраструктура дата-центра

Преимущества: простота и эффективность использования; экономия средств за счет отсутствия расходов на программное обеспечение и электронные компоненты; минимальный риск простоя бизнес-про-

цессов, за счёт миграции серверной части (серверов приложений) в облако; гибкость и масштабируемость.

Гибридное облако (hybrid cloud) — это сочетание двух и более видов облаков (частного, публичного, общественного). Эта разновидность облачных вычислений позволяет не только заказчику переносить часть своей инфраструктуры на обслуживание к облачному провайдеру в дата-центр, но и облачному провайдеру включать свои внешние ресурсы и сервисы в инфраструктуру заказчика.

Преимущества: уменьшение капитальных затрат; оптимизация расходов на инфраструктуру; средства управления, доступные в частном облаке, наряду с быстрым масштабированием общественного; уменьшение распределения ресурсов для временных проектов.

Общественное облако (community cloud) — облачная инфраструктура с общими серверами, которые открыты доступу по общедоступной сети. К примеру, общественным облаком является iCloud Apple или Google Drive.

Преимущества: масштабируемость (доступность по требованию); экономичность; независимое местоположение.

Наиболее уязвимыми, с точки зрения информационной безопасности, считаются модели *PaaS* и *IaaS*, где пользователям предоставляется больший контроль над инфраструктурой облака, а также больший набор предоставляемых услуг. Группы угроз безопасности для моделей *PaaS* и *IaaS* представлены, соответственно, на рис. 4.9 и 4.10.

На рис. 4.11. представлены основные риски потребителей при использовании облачных сервисов.

4.9.2. Методы защиты данных в облачных сервисах

Существуют различные методы защиты от угроз информационной безопасности в облачных сервисах. Традиционные методы защиты в виртуальной среде теряют свою эффективность как с точки зрения экономической целесообразности, так и с точки зрения обеспечения должного уровня защищенности.

Как указывалось ранее, наиболее трудными и уязвленными с точки зрения обеспечения информационной безопасности сервисами, являются PaaS и IaaS. Их выделяют в виду предоставления пользователям большего контроля над инфраструктурой облака, а также большего набора услуг по сравнению с другими сервисами. В табл. 4.8 приведена классификация атак и методов защиты PaaS и IaaS сервисов.

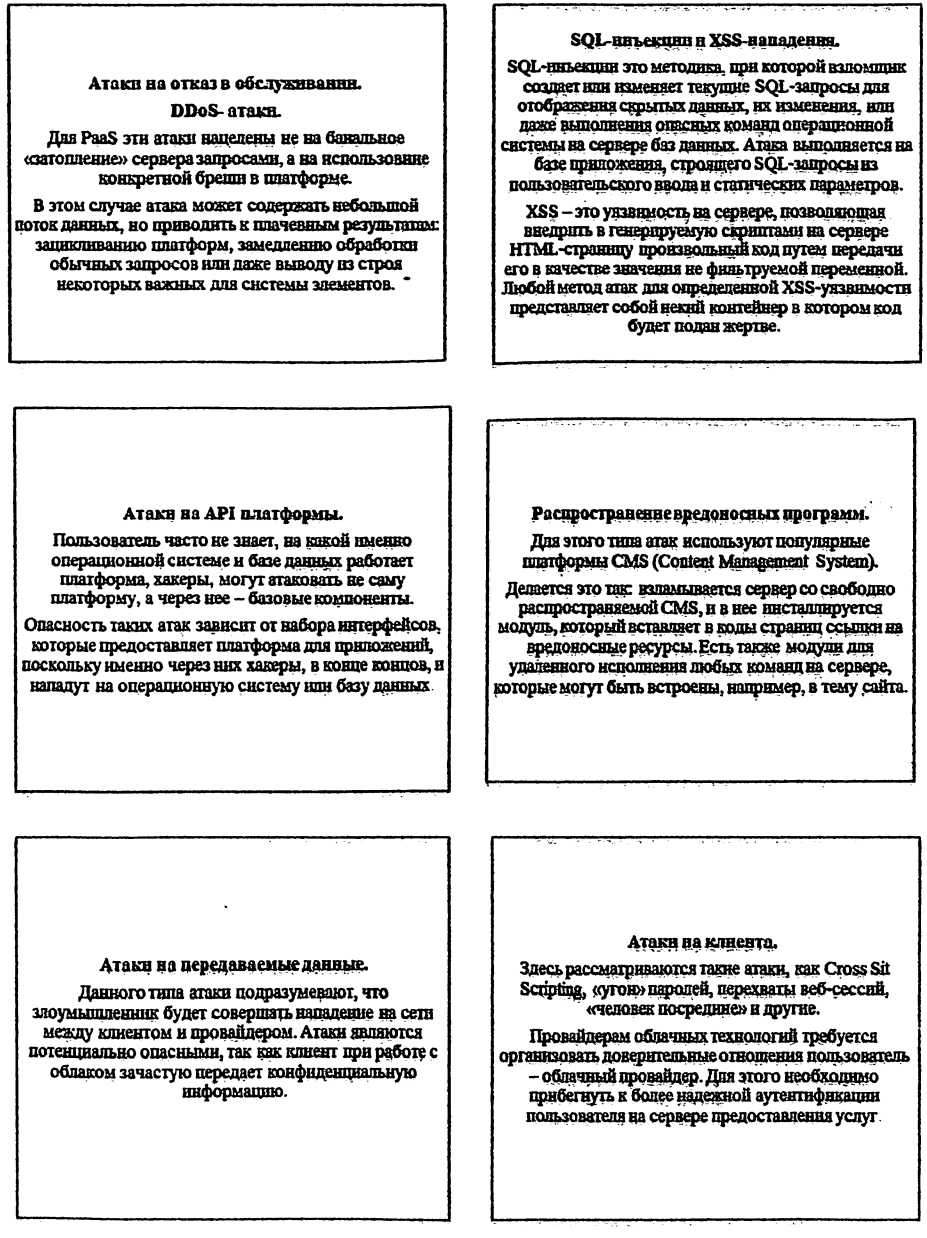


Рис. 4.9. Группы угроз безопасности модели PaaS

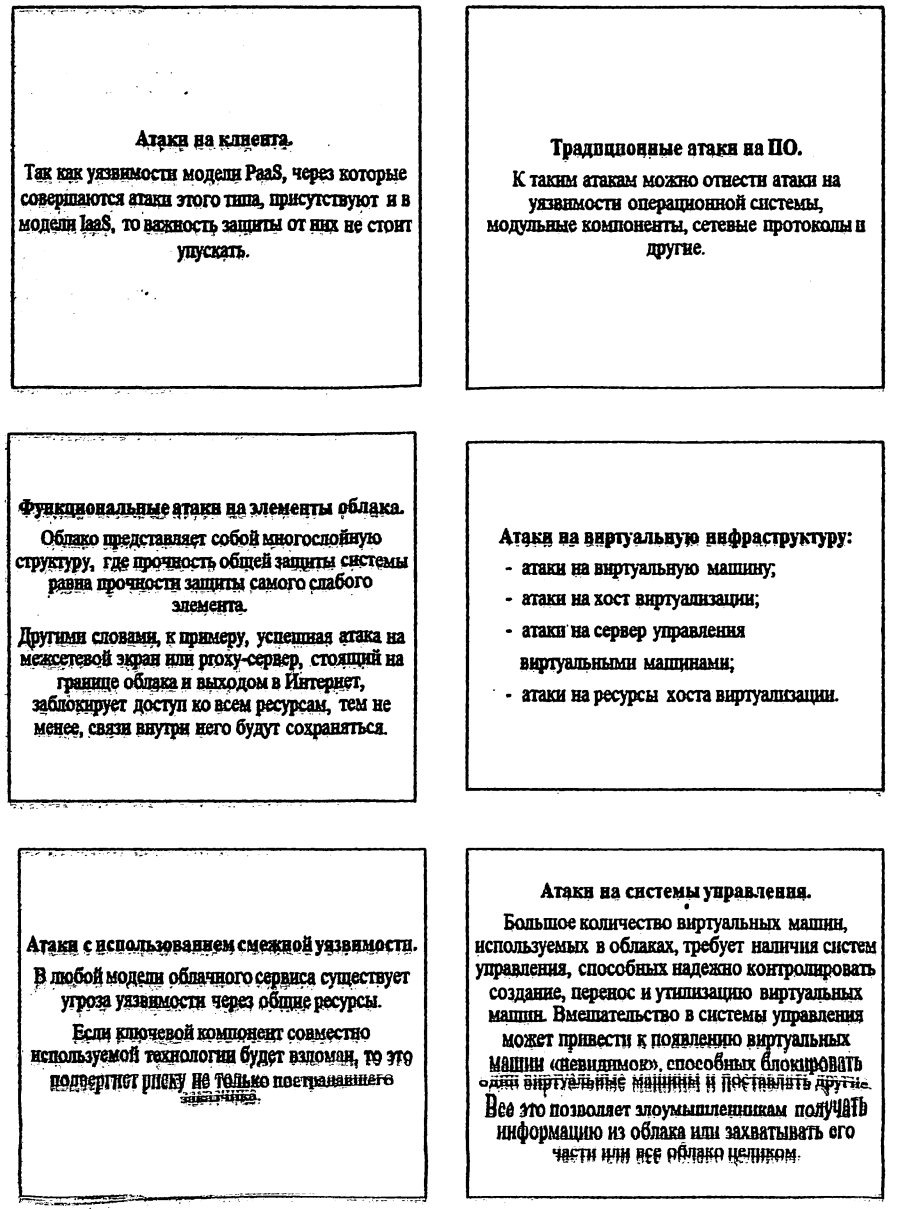


Рис. 4.10. Группы угроз безопасности модели IaaS

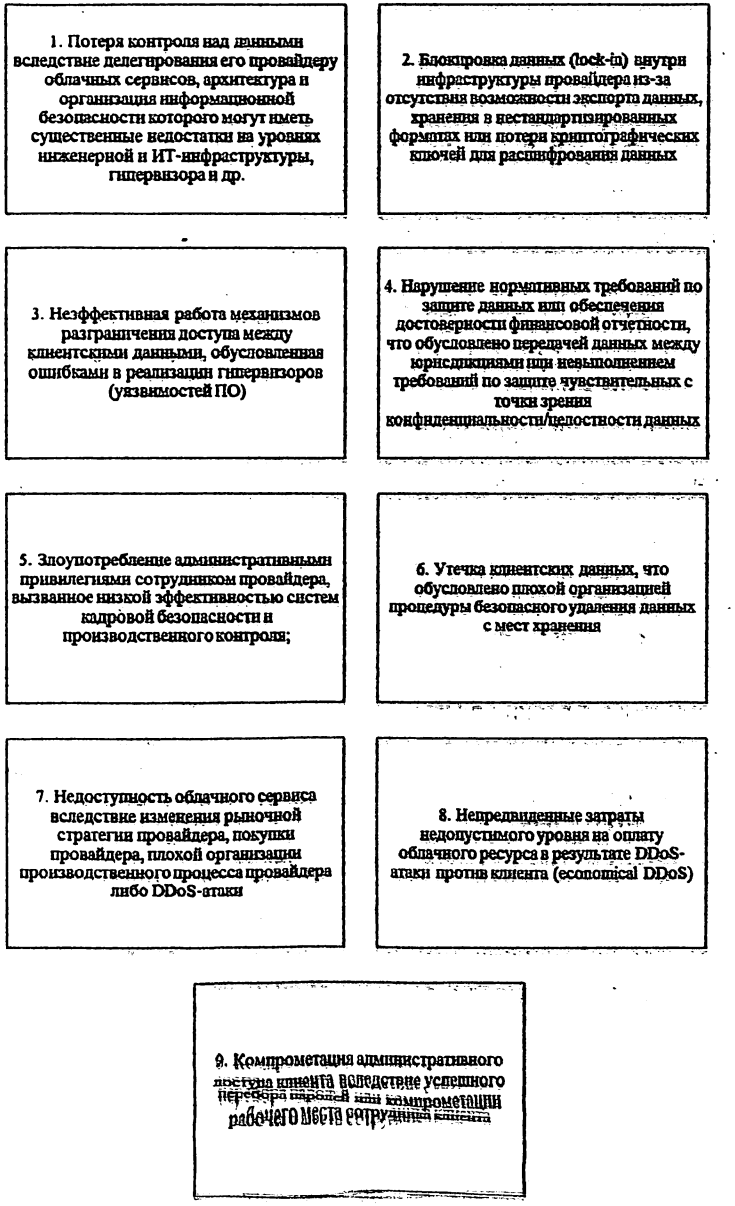


Рис. 4.11. Основные риски потребителей при использовании облачных сервисов

Таблица 4.8

Классификация атак и методов защиты в облачных сервисах

Атака	Методы защиты
PaaS	
Атаки на отказ в обслуживании	Proxy-сервер с защитой от DDoS
SQL-инъекции и XSS-нападения	Экран уровня приложений Анализаторы сценариев
Распространение вредоносных программ	Облачные антивирусы Сканеры кодов сайта
Атаки на API платформы	Безопасный набор интерфейсов для работы с приложениями
Атаки на передаваемые данные	SSL, TLS, IPSec и т.д.
Атаки на клиента	SSL, TLS, IPSec и т.д. LDAP, SAML
IaaS	
Атаки на клиента	SSL, TLS, IPSec и т.д. LDAP, SAML
Традиционные атаки на ПО	Межсетевой экран (NGFW) Антивирус IPS
Функциональные атаки на элементы облака	Эффективная организация резервного копирования и разграничения доступа для службы хранения данных
Атаки на виртуальную инфраструктуру	Программные продукты для анализа трафика и предотвращения вторжений для виртуальной среды. Программное обеспечение для разграничения прав доступа в виртуальной инфраструктуре. Программное обеспечение для проведения аудита виртуальной среды на предмет наличия ошибок в конфигурации безопасности
Атаки с использованием смежных уязвимостей	VPN, VLAN, VPLS Изменение кода в единой программной среде
Атаки на системы управления	Отслеживание лог-файлов и их анализ. Анализ событий для обнаружения вредоносной активности

Как видно из табл. 4.8, существует множество современных методы защиты от атак на сервисы PaaS и IaaS. Рассмотрим некоторые наиболее популярные из них.

Next Generation Firewall (NGFW) — межсетевой экран нового поколения. В него входят функции защиты каналов связи, обнаружения вторжений, глубокого анализа и фильтрации веб-трафика, трафика электронной почты, а также детального разграничения прав пользователей. По мнению специалистов в области ИБ, наиболее признанными межсетевыми экранами нового поколения, являются межсетевые экраны компаний Palo Alto, Check Point, Fortinet и Cisco.

Экран уровня приложений или Web Application Firewall — защитный экран для приложений, осуществляющих передачу информации по протоколам HTTP и HTTPS. Исследовательская и консалтинговая компания Gartner, специализирующаяся на рынках информационных технологий, выделяет следующих производителей экранов уровня приложений как лучших: Imperva, F5, Akamai, Citrix, Fortinet, Barracuda Networks, CloudFlare.

Virtual Private LAN Service (VPLS) — сервис виртуальной частной сети. Это способ организации связи на основе IP / MPLS-сетей, который позволяет объединять в единую сеть географически распределенные объекты.

Облачные антивирусы состоят из двух частей: клиентской части (приложения) и веб-сервиса, который располагается на одном или нескольких серверах поставщика. Подобного рода антивирусы практически не нагружают систему и имеют высокую скорость работы по сравнению с обычными клиентскими антивирусами. По мнению специалистов в области ИБ, наиболее эффективными облачными антивирусами, являются антивирусы компаний: Лаборатория Касперского, Avira, Panda Security и ряд других. Многие эксперты и специалисты по безопасности недоверчиво относятся к облачным антивирусам из-за того, что часть ресурсов является «общей» для всех потребителей — это не только вычислительные мощности серверов, но и центральная база данных, содержащая информацию о вредоносном коде.

Virtual Local Area Network (VLAN) представляет собой виртуальную локальную компьютерную сеть, позволяющую сконфигурировать несколько виртуальных широковещательных доменов в рамках одного физического. Эта технология имеет ряд преимуществ:

- возможность территориального разнесения разных отделов организации;

- низкая вероятность прослушивания трафика сторонними сотрудниками (другого VLAN);
- уменьшение количества широковещательных запросов (снижение пропускной способности сети).

Для того чтобы обеспечить полную и грамотную защиту от угроз информационной безопасности в облачных сервисах, следует использовать комплексный подход построения системы обеспечения информационной безопасности (СОИБ).

При построении комплексной системы обеспечения информационной безопасности необходимо последовательно решать следующие задачи:

- оценка текущего состояния информационной безопасности;
- определение желаемого (целевого) состояния информационной безопасности;
- формирование дорожной карты мероприятий, направленных на преодоление существующего разрыва и достижение желаемого (целевого) состояния информационной безопасности.

Очень важно, чтобы обеспечивалась комплексная защита, которая в первую очередь должна включать системы раннего предупреждения о начале атаки, отображение подозрительных входящих запросов, подробную непрерывную аналитику входящих данных и т.п. Также необходимо обеспечить шифрование данных, однако тут важно не упустить из виду слабые места: ключи шифрования, контроль доступа, мониторинг и доступ к данным. Если ключи шифрования недостаточно защищены, то они уязвимы для кражи, если же ключи защищены хорошо, но контроль доступа не достаточно надежен, возможность получить доступ к конфиденциальным данным, «представившись» авторизированным пользователем. Шифрование должно реализовываться на базе надежных ключевых решений по управлению доступом, чтобы обеспечить гарантированную защиту ключей. Криптографические методы защиты работают совместно с другими технологиями защиты данных и позволяют получить дополнительную информацию по обеспечению безопасности для построения всестороннего многоуровневого подхода к защите и конфиденциальности данных и снижения рисков взлома в облаке и за его пределами.

Многие компании также внедряют аудит баз данных, контроль доступа к каталогу (DAP — Directory Access Protocol) и системы для анализа входящей информации от сторонних систем (SIEM — Security Information and Event Management) для сбора информации о выполняемых операциях и процессах, но мониторинг и корреляция событий сами по себе не обеспечивают информационную безопасность данных.

Сегодня облачные технологии занимают далеко не последнее место в инфраструктуре современных компаний. Совокупный объем рынка в сфере облачных технологий растет из года в год. Некоторые исследователи прогнозируют, что к 2020 г. показатель достигнет рекордных 240 млрд долл. Проблема информационной безопасности облачных сервисов чрезвычайно важна не только для поставщиков услуг, но и для их заказчиков. На сегодняшний день созданы различные международные европейские и американские коммерческие и некоммерческие организации, цель которых — обеспечить безопасность ресурсов облака любого вида и масштаба. Грамотный подход к выбору поставщика услуг, мер защиты от актуальных угроз безопасности на всех уровнях облачной инфраструктуры, дает компании преимущество перед злоумышленниками и используемыми ими средствами.

Литература к главе 4

1. *Бабаш А.В.*, *Баранова Е.К.* Актуальные вопросы защиты информации: монография / *А.В.Бабаш*, *Е.К. Баранова*. – М.: РИОР:ИНФРА-М, 2017.
2. *Баранова Е. К.*, *Забродоцкий А. С.* Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии ИСО/МЭК 27000-27005 // Вестник Московского университета им. С.Ю. Витте. Серия 3: Образовательные ресурсы и технологии. – 2015. – № 3(11). – С. 73–77. 2.
3. *Башлы П.Н.* Современные сетевые технологии. Учеб. пособие. — М.: Горячая линия — Телеком, 2006.
4. *Башлы П.Н.*, *Бабаш А.В.*, *Баранова Е.К.* Информационная безопасность: учебно-практ. пособие. — М.: Изд. центр ЕАОИ, 2010.
5. *Карпов Е.А.*, *Котенко И.В.*, *Котухов М.М.* и др. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под ред. И.В.Котенко. — СПб.: ВУС, 2000.
6. *Медведовский И.Д.*, *Семьянов П.В.*, *Леонов Д.Г.* и др. Атака из Internet. — М.: Солон-Р, 2002.
7. *Мэйволд Э.* Безопасность сетей: Пер. с англ. — М.: ЭКОМ, 2002.
8. *Новиков Ю.В.*, *Кондратенко С.В.* Локальные сети: архитектура, алгоритмы, проектирование. — М.: ЭКОМ, 2001.

9. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер, 2002.
10. *Прохода А.Н.* Обеспечение Интернет-безопасности. Практикум: Учеб. пособие для вузов. — М.: Горячая линия — Телеком, 2007.
11. *Спортак М., Паппас Ф.* Компьютерные сети и сетевые технологий. — М.: ТИД «ДС», 2002.
12. *Щербаков А.Ю.* Введение в теорию и практику компьютерной безопасности. — М.: Издательство Молгачева С.В., 2001.

ГЛАВА 5. МЕТОДЫ ПРИНЯТИЯ РЕШЕНИЙ В РАЗРАБОТКЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

5.1. Основные понятия и определения

5.1.1. Принятие решений как особый вид человеческой деятельности

Принятие решений — каждодневная деятельность человека, часть его повседневной жизни. Простые решения принимаются легко, часто автоматически, не очень задумываясь; в сложных и ответственных случаях человек обращается за помощью к друзьям, родственникам, опытным людям, книгам для подтверждения своего решения, несогласия с ним или за советом. Решения разрабатываются и реализуются с разной степенью профессионализма, поэтому их диапазон практически неограничен — от необдуманных до детально разработанных.

Техническая революция середины XX в. изменила круг задач, решаемых человеком, в различных сферах его деятельности. Возникли новые сложные и непривычные для него проблемы. В течение столетий люди могли принимать решения, ориентируясь на один-два фактора. Сейчас положение изменилось. Большое число задач являются многокритериальными. Человеку приходится оценивать множество сил, влияний, последствий и интересов, характеризующих варианты решения.

Принятие решения в большинстве случаев заключается в генерации возможных альтернатив решений, их оценке и выборе лучшей. Для подавляющего большинства человеческих решений нельзя точно рассчитать и оценить последствия. Можно лишь предполагать, что определенный вариант решения приведет к наилучшему результату. Однако такое предположение может оказаться ошибочным.

Что же такое «наилучшее» решение? В исследованиях операций «наилучшим» считается решение, доставляющее оптимум функции, выражающей цель системы. Более общее определение «правильного», или «наилучшего» решения в смысле принятия решений будем считать

[1] В гл. 5 использованы материалы учебно-методического пособия: *Тимашков П.С.* Математические методы принятия решений. — М.: МЭСИ, 2003.

выбор такой альтернативы из числа возможных, в которой с учетом всех разнообразных факторов и противоречивых требований будет оптимизирована общая ценность, т.е. она будет в максимальной степени соответствовать достижению поставленной цели. Отметим, что в отличие от исследования операций, в теории принятия решений не существует абсолютно лучшего решения. Решение является лучшим лишь для конкретного лица, принимающего решение (ЛПР) в отношении поставленных им целей, при заданных условиях. Эта субъективная оценка оказывается в настоящее время единственно возможной основой объединения разнородных физических параметров решаемой проблемы в единую модель, позволяющую оценивать варианты решений. В этой субъективности нет ничего плохого. Опытные руководители хорошо осознают, сколько личного и субъективного они вносят в принимаемые решения. С другой стороны, об успехах и неудачах большинства человеческих решений люди могут судить исходя только из своих субъективных предпочтений.

5.1.2. Люди, принимающие решения, и их роль в процессе принятия решений

В процессе принятия решений люди могут играть разные роли. Под ЛПР будем понимать субъекта, который всерьез намерен устранить стоящую перед ним проблему, выделить на ее разрешение и реально задействовать имеющиеся у него активные ресурсы, суверенно воспользоваться положительными результатами от решения проблемы или взять на себя всю ответственность за неуспех, неудачу, за напрасные расходы[1].

В качестве ЛПР может выступать группа, принимающая решения (ГПР). Примером ГПР могут быть судьи в фигурном катании, бальных танцах и других подобных видах спорта, комиссии на выделение грантов ученым, аттестационные комиссии в учебных заведениях и пр. Главное в деятельности ГПР — достижение согласия при выработке совместных решений.

Иногда наряду с ЛПР выделяют владельца проблемы, если таковыми являются различные люди. В таком случае владелец проблемы — человек, решающий проблему и ответственный за принятые решения, а ЛПР — человек, фактически осуществляющий выбор наилучшего варианта действия.

Активная группа — группа людей, имеющих общие интересы и старающихся оказать влияние на процесс выбора и его результат. Примерами таких групп являются политические фракции, которые стараются повлиять определенным образом на политическую, экономическую, социальную жизнь страны. Даже небольшие группы людей могут при активных действиях влиять как на процедуры, так и на результат процесса принятия решений. В связи с этим ЛПР уже на первых этапах изучения проблемы выделяет активные группы, оценивает по их критериям имеющиеся альтернативы и пытается найти решение, удовлетворяющее все стороны. Учет интересов активных групп не должен приводить ЛПР к отказу от собственных целей и предпочтений. Часто ЛПР идет на дополнительные расходы, чтобы получить вариант решения, приемлемый для всех участников выбора.

В процессе принятие решений человек может выступать в качестве эксперта. Эксперт — это тот, кто лично работает в рассматриваемой области деятельности, является признанным специалистом по решаемой проблеме, может и имеет возможность высказать суждения по ней в доступной для ЛПР форме. Установлено, что процесс становления эксперта довольно длительный, и при благоприятных условиях человек формируется как эксперт в определенной области не менее чем за 10 лет. Этот универсальный факт справедлив для различных областей науки, искусства и спорта. Большую роль в становлении эксперта играют постоянные упражнения и, как показывают исследования, время упражнений и руководство опытного учителя, особенно на начальных этапах, являются основными факторами становления эксперта.

В литературе можно встретить и другие оценки: например, в работе[1] указывается, что в технических системах человек может самостоятельно стать хорошим специалистом через 2–4 года; в биологических системах — через 6–8 лет; и лишь в социальных системах — через 10–12 лет. В связи с этим будем отличать специалиста от эксперта. Существенными признаками, отличающими эксперта от специалиста, будут признание его заслуг, умение высказываться на языке, понятном ЛПР, наличие у него разрешения на высказывание своего мнения, личная заинтересованность в сотрудничестве с ЛПР по рассматриваемой проблеме[2].

В современном мире резко возросла сложность принятия разумных решений. При принятии сложных решений в их подготовке иногда принимает участие консультант по принятию решений. Консультант обычно не вносит свои предпочтения, оценки в принятии решений. Он помогает ЛПР в формулировании проблемы; выявляет позиции

[1] *Варфоломеев В.И., Воробьев С.Н.* Принятие управленческих решений: Учеб. пособие для вузов. — М.: КУДИЦ-ОБРАЗ, 2001.

[1] *Смирнов Э.А.* Управленческие решения. — М.: ИНФРА-М, 2001.

[2] *Варфоломеев В.И., Воробьев С.Н.* Принятие управленческих решений: Учеб. пособие для вузов. — М.: КУДИЦ-ОБРАЗ, 2001.

активных групп, сильные и слабые стороны предлагаемых ими критериев и альтернатив; обеспечивает работу с экспертами и экспертными группами; помогает выработать разумное компромиссное решение.

5.1.3. Альтернативы

Альтернатива — это один из возможных способов достижения цели или один из конечных вариантов решений. Альтернативы различаются между собой последовательностью и приемами использования активных ресурсов. Для любой задачи принятия решений должна существовать тройка: цель, критерии, альтернативы. Если отсутствует один из компонентов, то проблема не поставлена. При наличии менее двух альтернатив выбор отсутствует.

Задача формирования исходного множества альтернатив — составная часть процесса принятия решений. Даже если выбор ограничен плохими, очень плохими и абсолютно неудовлетворительными альтернативами, всегда существует наиболее благоприятное решение.

Альтернативы могут быть зависимыми и независимыми. Если действие над какой-либо альтернативой не влияет на качество других, то такая альтернатива является независимой. При зависимых альтернативах оценки одних из них оказывают влияние на качество других.

Задачи принятия решений существенно различаются в зависимости от наличия альтернатив на момент выработки политики и принятия решений. В некоторых задачах все возможные альтернативы известны, и из них производится выбор наилучшей. Например, можно выбирать лучший университет, наиболее надежный банк или же банк с оптимальным соотношением выгода–риск, наиболее благоприятный район для покупки квартиры и т.д. Существует множество задач, в которых все альтернативы или их часть появляются после принятия решений. Например, требуется разработать правила отбора лиц на предоставление грантов на конкурсной основе. Альтернативы в такой задаче появляются после разработки и декларации правил отбора.

Существуют также задачи, когда на основе рассмотрения имеющихся альтернатив возникают новые альтернативы. Первичные альтернативы не всегда удовлетворяют участников процесса выбора. Рассматривая их, участники понимают, чего же все-таки не хватает, что реализуемо при данной ситуации, а что — нет. Этот класс задач можно назвать задачами с конструируемыми альтернативами.

5.1.4. Критерии

В современной науке о принятии решений считается, что варианты решений (альтернативы) характеризуются различными показателями

их привлекательности для ЛПР. Эти показатели называют признаками, факторами, атрибутами, критериями.

Пусть задано некоторое конечное множество альтернатив A. Из множества A или любого его подмножества X необходимо выделить одно или несколько вариантов решений, в некотором смысле лучших или более соответствующих каким-либо заранее оговоренным условиям. Для решения этой задачи обычно используется следующий подход[1].

Множество вариантов A проецируется на числовую ось так, что каждому варианту соответствует конкретная точка числовой оси. В одну и ту же точку может либо не может проецироваться более одного варианта. Числовая ось, на которую спроецировано множество вариантов A, называется шкалой. Сам процесс проецирования, т.е. приписывания элементам из A числовых значений, соответствующих точкам числовой оси, в которые они проецируются — шкалированием. Если после такого проецирования упорядочить все варианты из A по величине приписанных им числовых оценок и сохранить за каждым вариантом лишь его порядковый номер, то образованная таким образом шкала называется порядковой, или ранговой.

Если вариант считается тем «лучше» или тем более соответствующим заранее фиксированной цели выбора, чем большая (или меньшая) числовая или ранговая оценка приписывается варианту, то шкала называется критерием для выбора или критериальной шкалой.

Рассмотрим вариант $x \in A$ и выразим его критериальную оценку, т.е. числовое значение той точки шкалы, в которую вариант спроецирован через $f(x)$. Обозначим через $f(x)$ функцию, заданную на всех вариантах из A и имеющую числовые значения, определяемые критериальной шкалой. Такая функция и называется критерием.

Критерий — это способ выражения различий в оценке альтернативных вариантов с точки зрения участников процесса выбора, т.е. показатель привлекательности вариантов решений. Именно с помощью критерия ЛПР будет судить о предпочтительности исходов, а значит, и способов проведения операции по решению проблемы. Значимость того или иного из выбранных критериев определяется именно тем, что ЛПР не считает возможным выносить суждения о предпочтительности исхода операции, если именно того или иного критерия оценки недостает.

В профессиональной деятельности выбор критериев часто определяется многолетней практикой, опытом. В подавляющем большинстве задач выбора имеется достаточно много критериев оценок вариантов

[1] *Смирнов Э.А.* Управленческие решения. — М.: ИНФРА-М, 2001.

решений. Существует ряд свойств или требований, которым должен (по возможности) удовлетворять набор критериев. Набор критериев должен быть полным, действенным, разложимым, неизбыточным и минимальным.

Полнота набора означает, что он должен охватывать все важные аспекты проблемы. Набор критериев является полным, если с его помощью можно показать степень достижения общей цели, т.е. набор из критериев полон, если, зная значения n-мерного критерия, связанного с общей целью, ЛПР имеет полное представление о степени достижения общей цели.

Действенность критериев. ЛПР должен понимать смысл критериев и влияние их действий на обсуждаемую проблему. Критерии должны быть такими, чтобы их можно было объяснять другим, особенно в тех случаях, когда важнейшей целью работы является выработка и защита определенной позиции. Поскольку смысл анализа решений — помочь ЛПР выбрать лучший курс действий, то и критерии должны служить этой цели.

Разложимость. При использовании n критериев необходимо построить n-мерную функцию предпочтений. Для задач с большим числом критериев полезно произвести декомпозицию задачи и разложить ее на подзадачи, каждая из которых содержит меньшее число критериев, т.е. желательно, чтобы набор критериев был разложим.

Неизбыточность. Критерии должны быть определены так, чтобы не дублировался учет одних и тех же аспектов решаемой проблемы.

Минимальная размерность. Желательно, чтобы набор критериев оставался настолько малым, насколько это возможно. Увеличение числа критериев, с одной стороны, приводит к анализу решаемой задачи в более широком плане, с другой стороны, может сильно усложнить и запутать анализ, что приведет к ошибочности результатов.

Формальные методы формирования набора критериев предложить трудно. Они очень сильно зависят от опыта и способности экспертов и, что крайне важно, характера лица, принимающего решения.

5.1.5. Оценка важности критериев

Оценка значимости критерия (его «веса») играет большую роль в формализованных процедурах формирования решения.

Существует много методов оценки важности критериев, связанных главным образом с оценкой «весов» критериев экспертами или ЛПР. Методы работы с экспертами — специальная проблема, которой касаться не будем.

Рассмотрим возможный подход, опирающийся на оценку существующего и желательного состояния. Достаточно условно методы определения «весов» приоритетов можно подразделить на три категории.

1. В первом случае используются опыт и знания ЛПР. Составляется список критериев, и ЛПР вычеркивает из списка критерии, которые с его точки зрения не имеют большого значения. При отсутствии в списке необходимых критериев ЛПР может его дополнить. Определение «веса» каждого критерия не формализуется.

2. Во втором случае значимость критериев определяется на основе оценок текущего и желательного состояния объекта по каждому критерию, опыта и знаний. Введем в рассмотрение два подпространства S и D в пространстве критериев. $S \subseteq R^m$ — это подмножество m-мерного Евклидова пространства (m — число критериев), в котором желательно иметь значения критериев, характеризующих объект, т.е. S — это подмножество, в котором может быть найдено решение. В тех случаях, когда желаемое состояние задается координатами, а не интервалами, подмножество S может состоять из одной точки s_0.

D — это множество точек в этом же пространстве, определяющих по оценкам ЛПР текущее состояние объекта, относительно которого принимается решение. Множество D может состоять из одной точки d_0, если текущее состояние задается координатами, а не интервалами. При таком подходе значимость j-го критерия K_j будет некоторой функцией от значений j-го критерия в областях D и S, обозначим их соответственно K_j^D и K_j^S.

$$K_j = \gamma_j f\left(K_j^D, K_j^S\right).$$

Возможны конкретные виды функции f — это может быть разность K_j^S и K_j^D, показывающая, насколько надо улучшить положение или их частное, показывающее, во сколько раз надо улучшить положение.

3. В третьем случае значимость критериев определяется на основе оценок текущего и желательного состояния объекта по каждому критерию, динамики объекта при нулевых управляющих воздействиях по каждому критерию, опыта и знаний. Введем еще одно подпространство $H(t)$ в том же критериальном пространстве R^m. Это подпространство, к которому могут принадлежать значения критериев, характеризующих объект по оценкам ЛПР через время t, если на объект не подавать управляющие воздействия.

Если через $K_j^{H(t)}$ обозначить значение, которое j-й критерий примет через время t, то

$$K_j = \gamma_j f\left(K_j^D, K_j^S, K_j^{H(t)}\right).$$

Возможны различные конкретные виды этой функции, например:

$$K_j = \gamma_j\left[\alpha_j\left(K_j^S - K_j^D\right) + \beta_j\left(K_j^D - K_j^{H(t)}\right)\right]$$

или

$$K_j = \gamma_j\left[\alpha_j \frac{K_j^S}{K_j^D} + \beta_j \frac{K_j^D}{K_j^{H(t)}}\right],$$

где α_j и β_j — коэффициенты, характеризующие относительную важность разности (частного) K_j^S, K_j^D и K_j^D, $K_j^{H(t)}$.

Во многих случаях целесообразно сосредоточить основное внимание на наиболее важных критериях, установив некоторый порог $K_j \geq \text{const}$, где $j = \overline{1, m}$. Такой подход иногда имеет место в кризисных ситуациях или когда критериев оказывается слишком много.

Коэффициенты α_j и β_j трудно определить на основе какой-либо формальной процедуры, исключая опрос экспертов. Однако они могут быть определены ЛПР в качестве лингвистических переменных: «α_j существенно больше β_j» или «α_j незначительно больше β_j» и т.д., что во многих случаях может быть сделано ЛПР исходя из его субъективных представлений о важности динамической составляющей в оценке критериев.

Для того чтобы выразить коэффициент γ_j, можно использовать следующие подходы:

- выразить непосредственно в баллах;
- сравнить с некоторым базовым критерием;
- попарно сравнить важности критериев (подход метода аналитической иерархии).

5.1.6. Многодисциплинарный характер науки о принятии решений

Термин «принятие решений» встречается в различных научных дисциплинах. Прежде всего следует назвать экономику. Она определяет правила рационального поведения людей в задачах выбора.

Поведение человека в задачах принятия решений имеет специфические особенности, которые определяются характеристиками человеческой системы переработки информации. Такие особенности исследуются в рамках когнитивной психологии.

В политологии одним из главных объектов изучения является механизм принятия лидерами политических решений. Принятие решений широко используется в исследовании операций. Теории активных систем и искусственного интеллекта, зоология, информатика и многие другие научные направления затрагивают проблемы принятия решений. Центральным для этих проблем является сам акт выбора человеком одного из вариантов решений. В отличие от других научных дисциплин в науке о принятии решений основным предметом является исследование процесса выбора. Эта наука изучает, как человек принимает решения и как следует ему в этом помогать, создавая специальные методы и компьютерные системы. Управление, принятие решений в любой предметной области требуют от ЛПР знания инструментов, которые помогают определить оптимальную допустимую политику.

Принятие решений — это прикладная научная дисциплина. В развитии принятия решений как научного направления принимают участие математики, психологи, политологи, специалисты по искусственному интеллекту, теории организации, информатике, вычислительной технике.

5.2. Анализ задач и методов принятия решений

5.2.1. Схема процесса принятия решений

В классической книге лауреата нобелевской премии профессора Г. Саймона «*The New Science of Management Decision*» (1960) процесс принятия решений разбит на четыре фазы: сбор информации (*intelligence*); поиск и построение альтернатив (*design*); выбор альтернатив (*choice*); оценка результатов (*review*). Первая фаза — сбор информации — сконцентрирована на идентификации проблемы принятия решения и сборе всей доступной информации о ней. При поиске и построении альтернатив (вторая фаза) центральным вопросом становится определение относительно небольшого числа альтернатив, которые следует изучить в деталях. На третьей фазе происходит выбор одного из вариантов решений из множества альтернатив, подготовленных на второй фазе. Последний шаг в процессе принятия решений — это реализация выбранной альтернативы и обобщение опыта, полученного в процессе решения проблемы.

Таким образом, само решение принимается в рамках второй и третьей фаз:

- конструирование относительно небольшого множества альтернатив;
- окончательный выбор варианта решения из сформированного множества.

Схематически две эти фазы представлены на рис. 5.1. Фазы существенным образом различаются как целями и информацией, так и методами. На фазе, в которой одним из вопросов является выбор относительно небольшого числа альтернатив (эту фазу часто называют earlyscreening), ЛПР должен принять во внимание все возможные пути достижения цели. В процессе же детального анализа и окончательного выбора альтернативы ЛПР ограничивает себя малым числом подготовленных вариантов решений. Выбору альтернативы из этого числа предшествует их детальное изучение.

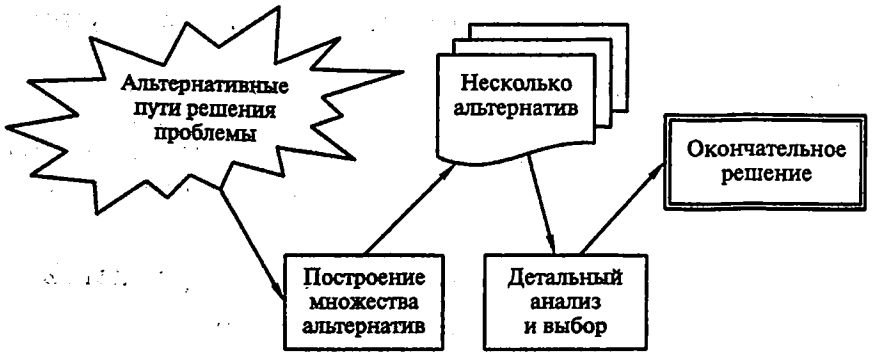


Рис. 5.1. Фазы процесса принятия решений

Рассмотрим схему процесса принятия решений, приведенную на рис. 5.2.

Основу принятия всех решений на всех этапах процесса выработки решений составляют предпочтения ЛПР. Несомненно, целесообразным началом процесса принятия решений должна стать формализация предпочтений. После того как предпочтения ЛПР формализованы с требуемым качеством, а также получена необходимая информация о предпочтениях, переходят к следующему важному шагу принятия решений — к построению функции выбора.

Функция выбора в теории принятия решений имеет фундаментальное значение. Именно на ее построение, в конечном счете, ориентированы решение задач формирования исходного множества альтернатив, анализ условий проведения операций, выявление и измерение предпочтений ЛПР.

Задача формирования исходного множества альтернатив не поддается полной формализации. Решение этой задачи — творческий процесс, в котором главная роль принадлежит ЛПР.

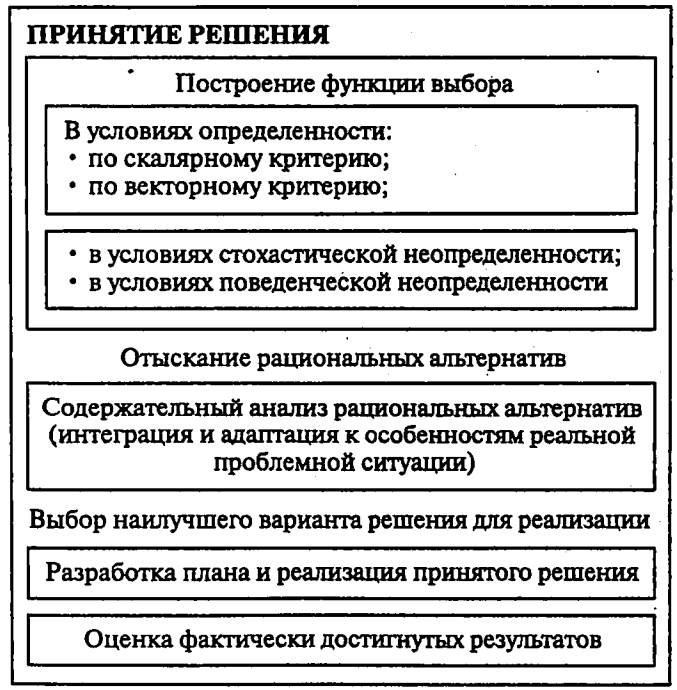


Рис. 5.2. Схема процесса принятия решений

Множеству альтернатив предъявляются определенные требования. Во-первых, оно должно быть по возможности более широким. Это обеспечит в дальнейшем необходимую свободу выбора решений ЛПР и сведет к минимуму возможность упустить «лучшее» решение. Однако это первое принципиальное требование входит в противоречие со вторым, вытекающим из принципа соответствия решения времени, месту и возможностям ЛПР. Следовательно, во-вторых, исходное множество альтернатив должно быть обозримым, достаточно узким, чтобы у ЛПР было достаточно времени для оценки последствий и предпочтительности альтернатив при сложившихся ограничениях на ресурсы.

Для удовлетворения двух указанных противоречий сначала формируют множество альтернатив, все элементы которого потенциально,

по их облику, по скрытым в них возможностям обеспечивают достижение целевого результата в сложившейся обстановке. Полученное таким образом множество претендентов на способ решения проблемы называют множеством целевых альтернатив.

Затем из множества целевых альтернатив отбирают те, которые являются логически непротиворечивыми и могут быть реализованы в отпущенные на операцию сроки. Кроме того, отбираемые альтернативы должны быть удовлетворены необходимыми активными ресурсами и отвечать общей системе предпочтений ЛПР.

Эти отобранные из целевых альтернатив варианты назовем физическими альтернативами из числа целевых. Остальные варианты, потенциально приводящие к цели, но физически нереализуемые, отбрасываем.

Полученные в результате подобных манипуляций варианты дополняют способами действий, придающими альтернативам необходимую гибкость и устойчивость по отношению к изменяющимся или неизвестным на данный момент компонентам условий проведения операции. В итоге получается исходное множество альтернатив.

Осознанный выбор должен вестись на основе сравнения результатов оценки альтернатив. Поэтому задача оценки альтернатив имеет главной целью получение для каждой альтернативы значений результатов, характеризующих интенсивность существенных свойств исходов операции, планируемой к проведению в заданных условиях. При решении таких задач строятся модели желаний, предпочтений, политики человека, принимающего решения.

Оценка фактических результатов есть итог проведенной ЛПР операции. Целью этой операции является накопление опыта и пополнение базы данных и знаний о причинах успехов и неудач. В будущем такой опыт и знания помогут избежать серьезных ошибок в управлении при решении сходных проблем, повысить эффективность будущих решений.

5.2.2. Классификация задач принятия решений

Задачи принятия решений отличаются большим многообразием, классифицировать их можно по различным признакам, характеризующим количество и качество доступной информации. В общем случае задачи принятия решений можно представить следующим набором информации:

$$(T, A, K, X, F, G, D),$$

где T — постановка задачи;

A — множество допустимых альтернативных вариантов;

K — множество методов измерения предпочтений;

X — множество методов измерения предпочтений (например, использование различных шкал);

F — отображение множества допустимых альтернатив в множество критериальных оценок;

G — системы предпочтений эксперта;

D — решающее правило, отражающее систему предпочтений.

Любой из элементов этого набора может служить классификационным признаком принятия решений. Рассматриваются различные классификационные признаки.

По виду отображения F. Попытки применения исследования операций для решения различного класса задач выявили большие различия в природе изучаемых систем. В связи с этим Г. Саймоном и А. Ньюэллом была предложена следующая классификация.

1. Хорошо структурированные или количественно сформулированные проблемы, в которых существенные зависимости выяснены настолько хорошо, что они могут быть выражены в числах или символах, принимающих в конце концов численные оценки.

2. Слабоструктурированные или смешанные проблемы, которые содержат как качественные, так и количественные элементы, причем качественные, малоизвестные и неопределенные стороны имеют тенденцию доминировать.

3. Неструктурированные или качественно выраженные проблемы, содержащие лишь описание важнейших ресурсов, признаков и характеристик, количественные зависимости между которыми совершенно неизвестны.

Согласно этой классификации проблемы исследования операций можно назвать хорошо структурированными. В типичных задачах исследования операций объективно существует реальность, допускающая строгое количественное описание и определяющая существование единственного очевидного критерия качества. Этот класс задач широко применяется при оценке и выборе элементов технических устройств, например: оптимизация форм корпуса самолетов или кораблей, управление электростанцией, расчет радиоактивного заражения местности, минимизация затрат на перевозки и т.д. Для этих задач существуют адекватные математические модели процессов и/или устройств и существуют данные, позволяющие априорно определить параметры моделей.

Характерными особенностями проблем третьего класса являются:

- уникальность выбора в том смысле, что каждый раз проблема является новой для ЛПР, либо обладает новыми особенностями по сравнению со встречавшейся ранее подобной;
- неопределенность в оценках альтернативных вариантов решений проблемы;
- качественный характер оценки вариантов решения проблемы, чаще всего формулируемой в словесной форме;
- оценка альтернатив может быть получена лишь на основе субъективных предпочтений ЛПР или ГПР;
- критериальные оценки могут быть получены только от экспертов.

К этому классу проблем относятся, например, проблемы планирования научных исследований, конкурсного отбора проектов, планирования развития города и т.д.

Ко второму классу проблем относят многие смешанные задачи, использующие как эвристические предпочтения, так и аналитические модели. Сюда относятся многие проблемы, связанные с экономическими и политическими решениями, проблемы медицинской диагностики и т.п.

По постановке задачи T. Задачи принятия решений можно разбить на две группы:

— Задачи первой группы.

Дано: группа из n-альтернатив-вариантов решения проблемы и N критериев, предназначенных для оценки альтернатив; каждая из альтернатив имеет оценку по каждому из критериев.

Требуется: построить решающие правила на основе предпочтений ЛПР, позволяющие выделить лучшую альтернативу; упорядочить альтернативы по качеству; отнести альтернативы к упорядоченным по качеству классам решений.

— Задачи второй группы.

Дано: группа из N критериев, предназначенных для оценки любых возможных альтернатив; альтернативы либо заданы частично, либо появляются после построения решающего правила.

Требуется: на основании предпочтений ЛПР построить решающие правила, позволяющие упорядочить по качеству все возможные альтернативы; отнести все возможные альтернативы к одному из нескольких (указанных ЛПР) классов решений.

Примером задач первой группы является многокритериальная оценка имеющихся на рынке провайдеров сотовой связи, имеющихся в продаже товаров и т.д. Здесь все возможные альтернативы заданы, критерии определены ЛПР. От ЛПР требуется построить правило сравнения объектов, имеющих оценки по многим критериям.

Примером задач второй группы является построение правила принятия решений для фонда, распределяющего ресурсы на научные исследования. Проекты проведения исследований еще не поступили, но критерии оценки и решающее правило должны быть определены заранее. Критерии и решающее правило определяет ЛПР.

По типу системы предпочтений эксперта G. Предпочтения могут формироваться одним лицом или коллективом, в зависимости от этого задачи принятия решений можно классифицировать на задачи индивидуального принятия решений и задачи коллективного принятия решений.

По мощности множества критериев выбора K. Множество критериев выбора может содержать один элемент или несколько. В соответствии с этим задачи принятия решений можно разделить на задачи со скалярным критерием и задачи с векторным критерием.

По обстановке, в которой принимается решение. Обстановку, в которой принимается решение, можно подразделить на стабильную и экстремальную.

При принятии решений в стабильной обстановке ЛПР, как правило, имеет больше времени для сбора и анализа данных и оценки принимаемых решений.

Принятие решений в экстремальной ситуации характеризуется острым дефицитом времени и, в большинстве случаев, быстро меняющейся обстановкой. Эти два фактора сильно усложняют процесс принятия решений для ЛПР.

5.2.3. Классификация методов принятия решений

Существует множество классификаций методов принятия решений, основанных на применении различных признаков.

В табл. 5.1 приведена одна из возможных классификаций, признаками которой являются содержание и тип получаемой экспертной информации.

Используемый принцип классификации позволяет достаточно четко выделить четыре большие группы методов, причем три группы относятся к принятию решений в условиях определенности, а четвертая — к принятию решений в условиях неопределенности. Из множества известных методов и подходов к принятию решений наибольший интерес представляют те, которые дают возможность учитывать многокритериальность и неопределенность, а также позволяют осуществлять

Таблица 5.1

Классификация методов принятия решений

№	*Содержание информации*	*Тип информации*	*Метод принятия решений*
1	Экспертная информация не требуется	—	*а* — метод доминирования; *б* — метод на основе глобальных критериев.
2	Информация о предпочтениях на множестве критериев	Качественная информация	*а* — лексикографическое упорядочивание; *б* — сравнение разностей критериальных оценок; *в* — метод припасовывания.
		Количественная оценка предпочтительности критериев	*а* — метод «эффективность–стоимость»; *б* — методы свертки на иерархии критериев; *в* — методы порогов; *г* — методы идеальной точки.
		Количественная информация о замещениях	*а* — метод кривых безразличия; *б* — методы теории ценности.
3	Информация о предпочтительности альтернатив	Оценка предпочтительности парных сравнений	*а* — методы математического программирования; *б* — линейная и нелинейная свертка при интерактивном способе определения ее параметров.
4	Информация о предпочтениях на множестве критериев и о последствиях альтернатив	Отсутствие информации о предпочтениях; количественная и/или интервальная информация о последствиях	*а* — методы с дискретизацией неопределенности;
		Качественная информация о предпочтениях и количественная о последствиях	*а* — стохастическое доминирование; *б* — методы принятия решений в условиях риска и неопределенности на основе глобальных критериев; *в* — метод анализа иерархий; *г* — методы теории нечетких множеств.
		Качественная информация о предпочтениях и последствиях	*а* — методы практического принятия решений; *б* — методы выбора статистически ненадежных решений.
		Количественная информация о предпочтениях и последствиях	*а* — методы кривых безразличия для принятия решений в условиях риска и неопределенности; *б* — методы деревьев решений; *в* — декомпозиционные методы теории ожидаемой полезности.

выбор решений из множества альтернатив различного типа при наличии критериев, имеющих разные типы шкал.

В свою очередь, среди методов, образующих четвертую группу, наиболее перспективными являются декомпозиционные методы теории ожидаемой полезности, методы анализа иерархий и теории нечетких множеств. Эти методы в наибольшей степени удовлетворяют требованиям универсальности, учета многокритериальности выбора в условиях неопределенности из дискретного или непрерывного множества альтернатив, простоты подготовки и переработки экспертной информации.

5.2.4. Системы поддержки принятия решений

Системы поддержки принятия решений существуют очень давно: это военные советы, коллегии министров, всевозможные совещания, аналитические центры и т.д. Хотя они никогда не назывались системами поддержки принятия решений, но выполняли именно их задачи.

Увеличение объема информации, поступающей в органы управления и непосредственно к руководителям, усложнение решаемых задач, необходимость учета большого числа взаимосвязанных факторов и быстро меняющаяся обстановка настоятельно требуют использовать вычислительную технику в процессе принятия решений. В связи с этим появился новый класс вычислительных систем — системы поддержки принятия решений.

Термин «система поддержки принятия решений» появился в начале 70-х гг., и за это время было дано большое число определений этого понятия, в том числе следующие:

1. Системы поддержки принятия решений являются человеко-машинными объектами, которые позволяют лицам, принимающим решения, использовать данные, знания, объективные и субъективные модели для анализа и решения слабоструктурированных и неструктурированных проблем.

2. Система поддержки принятия решений — это компьютерная система, позволяющая ЛПР сочетать собственные субъективные предпочтения с компьютерным анализом ситуации при выборе рекомендаций в процессе принятия решения.

3. Система поддержки принятия решений — компьютерная информационная система, используемая для различных видов деятельности при принятии решений в ситуациях, где невозможно или нежелательно иметь автоматическую систему, полностью выполняющую весь процесс.

Все три определения не противоречат, а дополняют друг друга и достаточно полно характеризуют систему поддержки принятия решений.

Человеко-машинная процедура принятия решений с помощью систем поддержки представляет собой циклический процесс взаимодействия человека и компьютера. Цикл состоит из фазы анализа и постановки задачи для компьютера, выполняемой ЛПР, и фазы оптимизации (поиска решения), реализуемой компьютером.

Системы поддержки принятия решений:

- помогают произвести оценку обстановки, осуществить выбор критериев и оценить их относительную важность;
- генерируют возможные решения;
- осуществляют оценку решений и выбирают лучшее;
- обеспечивают постоянный обмен информацией об обстановке принимаемых решений и помогают согласовать групповые решения;
- моделируют принимаемые решения;
- осуществляют динамический компьютерный анализ возможных последствий принимаемых решений;
- производят сбор данных о результатах реализации принятых решений и осуществляют оценку результатов.

5.3. Принятие решений на основе метода анализа иерархий

5.3.1. Иерархическое представление проблемы

Метод анализа иерархий (*Analytic Hierarchy Process* — AHP), или подход аналитической иерархии предполагает декомпозицию проблемы на простые составляющие части и обработку суждений ЛПР. В результате определяется относительная значимость исследуемых альтернатив для всех критериев, находящихся в иерархии. Относительная значимость выражается численно в виде векторов приоритетов. Полученные таким образом значения векторов являются оценками в шкале отношений и соответствуют так называемым жестким оценкам.

Постановка задачи, решаемой с помощью метода AHP, заключается обычно в следующем.

Дано: общая цель решения задачи; критерии оценки альтернатив; альтернативы.

Требуется: выбрать наилучшую альтернативу.

Подход AHP состоит из совокупности этапов:

1. Структуризация задачи в виде иерархической структуры с несколькими уровнями: цели — критерии — альтернативы.
2. Попарное сравнение элементов каждого уровня лицом, принимающим решения. Результаты сравнения имеют числовой характер.
3. Вычисление коэффициентов важности для элементов каждого уровня. Проверка согласованности суждений ЛПР.
4. Подсчет количественной оценки качества альтернатив. Выбор лучшей альтернативы.

5.3.2. Структуризация задачи в виде иерархии

Построение иерархии начинается с очерчивания проблемы исследования. Далее строится иерархия, включающая цель на верхнем уровне, промежуточные уровни (например, критерии) и альтернативы, формирующие самый нижний иерархический уровень (рис. 5.3).

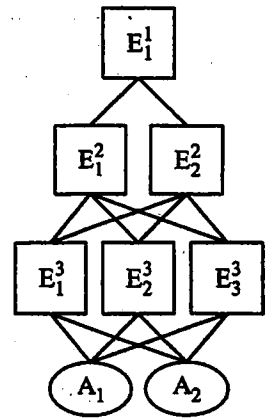


Рис. 5.3. Иерархическое представление проблемы

Верхний индекс у элементов указывает уровень иерархии, а нижний — их порядковый номер.

Рассмотрим процесс построения иерархической структуры на примере.

Пример. В современном мире для эффективного руководства необходимо иметь максимум информации, причем оперативной и постоянно обновляемой, также необходимо быстро принимать решения и с оптимальной скоростью притворять их в жизнь, доводить до подчиненных. В связи с этим современный бизнес просто немыслим без передовых средств связи, в частности мобильного телефона. Телефон стал неотъемлемым атрибутом делового человека.

Для эффективного использования сотовой связи необходимо правильно выбрать оператора связи. При выборе оператора нужно учесть ряд критериев:

- доступность в любое время, в любом месте;
- средняя стоимость услуг;
- удобство оплаты;
- спектр предоставляемых дополнительных услуг;

и пр.

Учитывая все это, структура решаемой проблемы: выбор оператора связи из имеющихся на рынке, может быть представлена в виде иерархической структуры, представленной на рис. 5.4.

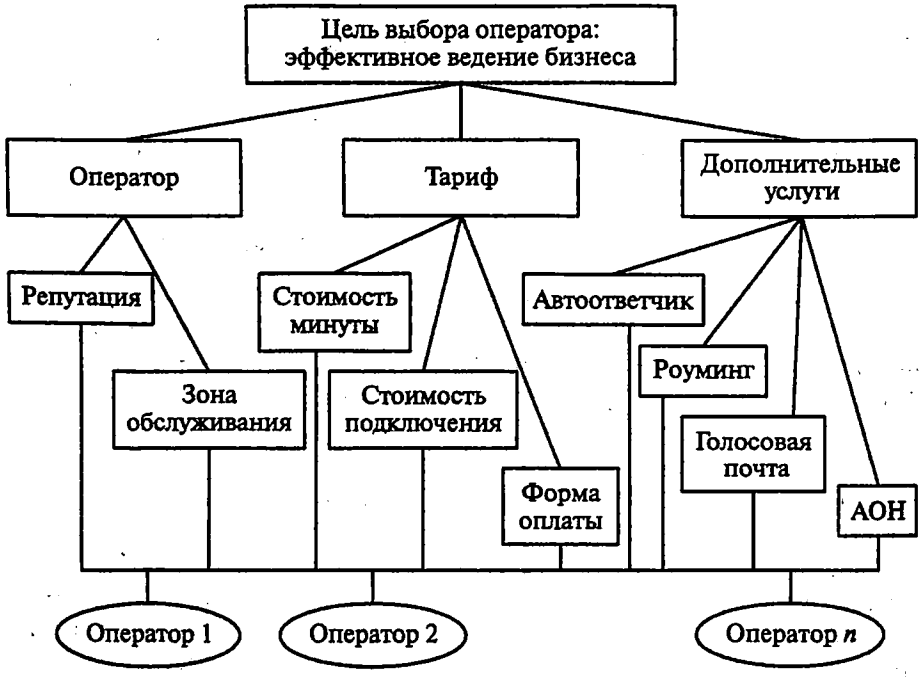


Рис. 5.4. Иерархическая схема проблемы выбора оператора сотовой связи

Во многих случаях на уровне альтернатив должны быть указаны цифры. Необходимо сопоставить эти зачастую совершенно разнородные величины так, чтобы выявить предпочтения ЛПР. После построения иерархии устанавливается метод сравнения ее элементов. Существует несколько методов сравнения элементов, выбор которых обусловлен характером связей альтернатив с уровнем критериев, количеством альтернатив, временем поступления альтернатив и прочими соображениями ЛПР.

5.3.3. Парное сравнение альтернатив (метод парных сравнений)

Для установления относительной важности элементов иерархии используется шкала отношений. Данная шкала позволяет ЛПР ставить в соответствие степеням предпочтения одного сравниваемого объекта перед другим некоторые числа (табл. 5.2).

Таблица 5.2

Шкала отношений

Степень значимости	*Определение*	*Объяснение*
1	Одинаковая значимость	Два действия вносят одинаковый вклад в достижение цели
3	Некоторое преобладание значимости одного действия над другим	Существуют соображения в пользу предпочтения одного из действий, однако эти соображения недостаточно убедительны
5	Существенная или сильная значимость	Имеются надежные данные или логические суждения для того, чтобы показать предпочтительность одного из действий
7	Очевидная или очень сильная значимость	Убедительное свидетельство в пользу одного действия перед другим
9	Абсолютная значимость	Свидетельства в пользу предпочтения одного действия перед другим в высшей степени убедительны
2, 4, 6, 8	Промежуточные значения между двумя соседними суждениями	Ситуация, когда необходимо компромиссное решение
Обратные величины приведенных выше величин	Если действию *i* при сравнении с действием *j* приписывается одно из определенных выше чисел, то действию *j* при сравнении с действием *i* приписывается обратное значение	Если согласованность была постулирована при получении *N* числовых значений для образования матрицы

При использовании указанной шкалы ЛПР, сравнивая два объекта в смысле достижения цели, расположенной на вышележащем уровне иерархии, должен поставить число в интервале от 1 до 9 или обратное значение.

Для этого в иерархии выделяют элементы двух типов: элементы-родители и элементы-потомки. Элементы-потомки воздействуют на соответствующие элементы вышестоящего уровня иерархии, являющиеся по отношению к первым элементами-родителями. Матрицы парных сравнений строятся для всех элементов-потомков, относящихся к определенному родителю. Парные сравнения производятся в терминах доминирования одного элемента над другим в соответствии со шкалой отношений.

Если элемент E_1 доминирует над элементом E_2, то клетка матрицы, соответствующая строке E_1 и столбцу E_2, заполняется целым числом, а клетка, соответствующая строке E_2 и столбцу E_1, заполняется обратным к нему числом.

При проведении парных сравнений следует отвечать на вопросы: какой из двух сравниваемых элементов важнее или имеет большее воздействие, какой более вероятен и какой предпочтительнее.

При сравнении критериев обычно спрашивают, какой из критериев более важен; при сравнении альтернатив по отношению к критерию — какая из альтернатив более предпочтительна или более вероятна.

Рассмотрим процесс построения матрицы парных сравнений на примере.

Пример. Провести анализ провайдеров на предмет их желательности с точки зрения определенного человека. Этот человек, руководствуется пятью независимыми (будем считать, что это так) характеристиками: тарифы, скорость сети, доступность сети, удобство оплаты, дополнительные услуги. В качестве альтернатив человек рассматривает следующие компании: *Comstar*, Зебра Телеком, РОЛ и МТУ.

Иерархическая схема может быть представлена согласно рис. 5.5.

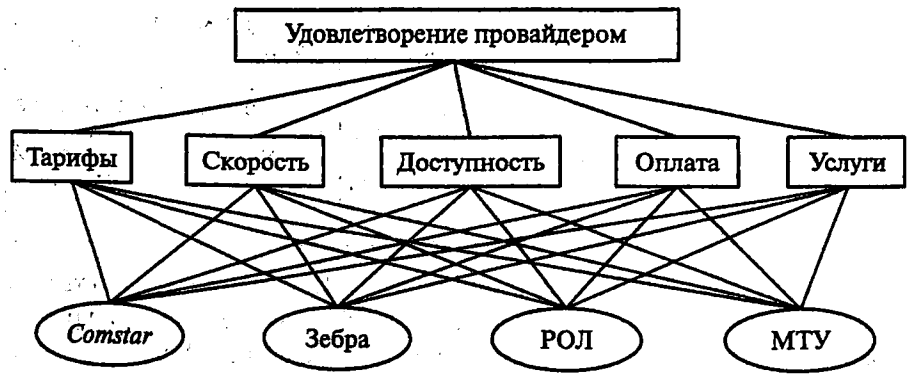


Рис. 5.5. Иерархическая схема проблемы выбора провайдера

После построения иерархии строятся матрицы парных сравнений. При сравнении элементов, принадлежащих одному уровню иерархии, ЛПР выражает свое мнение, используя одно из приведенных в табл. 5.2 определений. В матрицу сравнений заносится соответствующее число.

Начнем построение матриц парных сравнений с матрицы «Удовлетворение провайдером», которая покажет относительную важность характеристик при выборе компании:

[Удовлетворение провайдером] =

	Т	С	Д	О	У
Т	1	1/7	5	1/3	1/9
С	7	1	7	4	8
Д	1/5	1/7	1	1/6	1/3
О	3	1/4	6	1	4
У	9	1/8	3	1/4	1

При построении матрицы человек задавался вопросом, какая характеристика для него наиболее важна при выборе провайдера.

При сравнении любого критерия с самим собой не возникает вопросов о доминирующем воздействии одного из критериев, т.е. соответствующая позиция в матрице заполняется единицей, что соответствует одинаковой степени значимости критериев (см. табл. 5.2 — шкала отношений).

Рассмотрим первую строку матрицы. В позиции один–два, при сравнении важности тарифов и скорости, ЛПР поставил значение, равное $^1/_7$. Это означает, что скорость доминирует по предпочтению над тарифами. «При выборе провайдера для меня скорость во много крат важнее, чем тарифы» — говорит ЛПР. Семерка отвечает очевидной или очень сильной значимости одного сравниваемого объекта по сравнению с другим, согласно шкале отношений.

Цифра пять в позиции один–три говорит о том, что для ЛПР тарифы важней доступности сети, в то время $^1/_3$ на пересечении строки тарифов и столбца оплаты отвечает случаю, когда удобство оплаты для ЛПР немного важнее расценок провайдера.

Иерархию в какой-либо рассматриваемой проблеме можно выявить посредством анкетирования, синтезировать результат и продолжить дело с помощью анкеты для выявления суждений.

Рассмотрим, как могут быть получены матрицы суждения для одной матрицы. Тот же метод может быть применен для иерархии. В качестве примера возьмем иерархическую структуру, представленную на рис. 5.6.

Обозначим значения шкалы, располагая их в ряд от одного крайнего значения к равенству и затем вновь повышая до второго крайнего значения (табл. 5.3). В левом столбце перечислим все альтернативы, которые нужно сравнивать по степени превосходства с другими альтернативами из правого столбца. Эксперты должны отметить суждения, которые выражают превосходство элемента из левого столбца над соответствующим элементом из правого столбца, расположенным в той

же строке. Если такое превосходство в действительности имеет место, то одна из позиций левее равенства будет отмечена. В противном случае будет отмечено равенство или некоторая позиция справа.

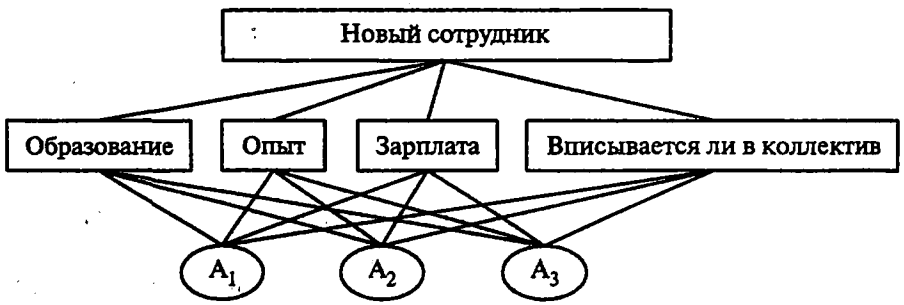


Рис. 5.6. Иерархическая схема задачи выбора нового сотрудника

Такая таблица составляется и заполняется для каждого критерия (четыре анкеты для сравнения альтернатив по каждому из критериев) и для сравнения критериев относительно цели (одна анкета, в которой ЛПР решает, какие критерии для него наиболее значимые).

После заполнения экспертами анкет по ним составляются матрицы парных сравнений. Например, анкета имеет вид, представленный в табл. 5.4.

Таблица 5.3

Сравнение альтернатив относительно критерия «образование»

Альтернативы	Абсолютное	Очень сильное	Сильное	Слабое	Равенство	Слабое	Сильное	Очень сильное	Абсолютное	Альтернативы
A_1	–	–	–	–	–	–	–	–	–	A_2
A_1	–	–	–	–	–	–	–	–	–	A_3
A_2	–	–	–	–	–	–	–	–	–	A_3

Матрица парных сравнений для анкеты из табл. 5.4 имеет вид:

$$[\text{образование}]_1 = \begin{array}{c|ccc} & A_1 & A_2 & A_3 \\ \hline A_1 & 1 & 7 & 3 \\ A_2 & \frac{1}{7} & 1 & \frac{1}{5} \\ A_3 & \frac{1}{3} & 5 & 1 \end{array}$$

Таблица 5.4

Сравнение альтернатив относительно критерия «образование», составленное первым экспертом по резюме кандидатов

Альтернативы	Абсолютное	Очень сильное	Сильное	Слабое	Равенство	Слабое	Сильное	Очень сильное	Абсолютное	Альтернативы
A_1	–	x	–	–	–	–	–	–	–	A_2
A_1	–	–	–	x	–	–	–	–	–	A_3
A_2	–	–	–	–	–	–	–	x	–	A_3

Для агрегирования мнений экспертов принимается среднегеометрическое, вычисляемое по формуле

$$a_{ij}^{\text{агр}} = \sqrt[n]{a_{ij}^{(1)} \cdot a_{ij}^{(2)} \cdot \ldots \cdot a_{ij}^{(n)}},$$

где $a_{ij}^{\text{агр}}$ — оценка элемента, принадлежащего i-й строке и j-му столбцу матрицы парных сравнений k-го эксперта.

Логичность критерия становится очевидной, если два равноценных эксперта указывают при сравнении объектов одинаковые оценки, что при вычислении агрегированной оценки дает единицу и свидетельствует об эквивалентности сравниваемых объектов.

В достаточно ответственных задачах на экспертизу осреднение суждений экспертов проводится с учетом их квалификации. Для определения весовых коэффициентов экспертов используют иерархическую структуру критериев, представленную на рис. 5.7.

Расчет агрегированной оценки в случае привлечения экспертов, имеющих различную значимость, ведется по формуле

$$a_{ij}^{\text{агр}} = a_{ij}^{\alpha_1} \cdot a_{ij}^{\alpha_2} \cdot \ldots \cdot a_{ij}^{\alpha_n},$$

где $a_{ij}^{\alpha_k}$ — оценка объекта, проведенная k-м экспертом с весовым коэффициентом α_k. При этом $\sum_{k=1}^{n} \alpha_k = 1$.

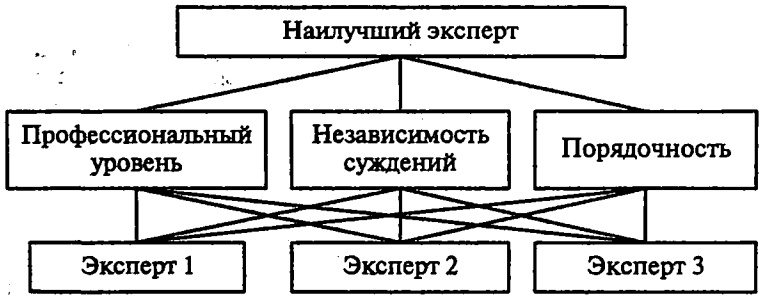


Рис. 5.7. Иерархия для ранжирования экспертов

Пример. Предположим, что в случае с выбором нового кандидата на работу первый эксперт, которым мог быть начальник отдела управления кадрами, по результатам резюме заполнил анкету, которая приведена в табл. 5.4. Во время проведения собеседования с каждым из претендентов второй эксперт, например один из директоров, заключил, что по уровню образования кандидатам соответствует анкета, заполнённая в виде табл. 5.5.

Таблица 5.5

Сравнение альтернатив относительно критерия «образование», составленное вторым экспертом по результатам собеседования с кандидатами

Альтернативы	Абсолютное	Очень сильное	Сильное	Слабое	Равенство	Слабое	Сильное	Очень сильное	Абсолютное	Альтернативы
A_1	–	x	–	–	–	–	–	–	–	A_2
A_1	–	–	x	–	–	–	–	–	–	A_3
A_2	–	–	–	–	–	x	–	–	–	A_3

Матрица парных сравнений для анкеты в табл. 5.5 имеет вид

$$[\text{образование}]_2 = \begin{array}{c|ccc} & A_1 & A_2 & A_3 \\ \hline A_1 & 1 & 7 & 5 \\ A_2 & \frac{1}{7} & 1 & \frac{1}{3} \\ A_3 & \frac{1}{5} & 3 & 1 \end{array}$$

Для объединения оценок суждений двух экспертов строится матрица со средним геометрическим оценок. В рассматриваемой задаче такой подход не совсем правомерен. Однако будем считать, что суждения двух экспертов обладают одинаковой степенью значимости. Результирующая матрица имеет вид

$$[\text{образование}] = \begin{array}{c|ccc} & A_1 & A_2 & A_3 \\ \hline A_1 & 1 & \sqrt{7\cdot 7} & \sqrt{3\cdot 5} \\ A_2 & \sqrt{\frac{1}{7}\cdot\frac{1}{7}} & 1 & \sqrt{\frac{1}{5}\cdot\frac{1}{3}} \\ A_3 & \sqrt{\frac{1}{3}\cdot\frac{1}{5}} & \sqrt{5\cdot 3} & 1 \end{array}$$

При построении матриц парных сравнений важным вопросом является согласованность, или однородность матрицы. Согласованность — это следование логике при высказывании суждений экспертом. Для более наглядной иллюстрации понятия согласованности приведем пример.

Пример. Предположим, что имеются три фрукта: яблоко, апельсин и ананас. Некто, предположим, ребенок, говорит: «Ананас в три раза вкуснее апельсина, а апельсин в два раза вкуснее яблока». Следующим высказыванием ребенка на вопрос о его любви к яблокам и ананасам, он говорит, что ананас в пять раз лучше яблока. В таких высказываниях ребенка несогласованности практически нет, несмотря на то, что исходя из его первого предложения, ананас в шесть раз предпочтительнее яблока. Однако нарушения логики могло быть гораздо более серьезным и даже привести к нетранзитивности. Так, второе высказывание могло звучать: «Мне яблоки нравятся больше, чем ананасы».

В практических задачах количественная и транзитивная (порядковая) однородность нарушается, поскольку человеческие ощущения нельзя выразить точной формулой. Для улучшения однородности в числовых суждениях, какая бы величина a_{ij} ни была взята для сравнения i-го элемента с j-м, a_{ij} приписывается значение обратной величины, т.е. $a_{ji} = \frac{1}{a_{ij}}$.

Определение. Квадратную матрицу $A_{n\times n}$ в которой все элементы $a_{ji} = \frac{1}{a_{ij}}$; $i, j = \overline{1, n}$, называют обратносимметрической.

При построении матриц парных сравнений не следует искусственно выстраивать матрицу исходя из условий согласованности. Такой подход может исказить предпочтения ЛПР. Однако во многих задачах однородность матриц должна быть высокой. Для оценки однородности используют то свойство, что при нарушении однородности ранг матрицы отличен от единицы и она имеет несколько собственных значений. При небольших отклонениях суждения от однородности одно из собственных значений будет существенно большие остальных и приблизительно равно порядку матрицы. Это свойство вытекает из следующих двух теорем.

Теорема 1. В положительной обратносимметрической квадратной матрице $\lambda_{max} \geq n$.

Теорема 2. Положительная обратносимметрическая квадратная матрица А согласованна тогда и только тогда, когда $\lambda_{max} = n$.

Таким образом, для оценки однородности суждений эксперта можно использовать отклонение величины максимального собственного значения λ_{max} от порядка матрицы n.

Согласованность суждения оценивается индексом однородности (индексом согласованности) или отношением однородности (отношением согласованности) в соответствии со следующими формулами:

$$\text{ИО} = \text{ИС} = \frac{\lambda_{max} - n}{n-1}, \quad \text{ОО} = \text{ОС} = \frac{\text{ИО}}{\text{М(ио)}},$$

где M(ио) — среднее значение индекса однородности случайным образом составленной матрицы парных сравнений, которое основано на экспериментальных данных. Значение есть табличная величина, входным параметром выступает размерность матрицы (табл. 5.6).

Таблица 5.6

Среднее значение индекса однородности в зависимости от порядка матрицы

n	1	2	3	4	5	6	7	8	9	10	11
M(ио)	0	0	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51

В качестве допустимого используется значение ОО ≤ 0,10. Если для матрицы парных сравнений ОО > 0,10, то это свидетельствует о существенном нарушении логики суждений, допущенном экспертом при заполнении матрицы, поэтому эксперту предлагается пересмотреть данные, использованные для построения матрицы, чтобы улучшить однородность.

5.3.4. Вычисление коэффициентов важности для элементов каждого уровня

Ранжирование элементов, анализируемых с помощью матрицы парных сравнений, осуществляется на основании главных собственных векторов, получаемых в результате обработки матриц.

Определение. Пусть задана квадратная матрица $A_{n\times n}$. Число λ называется собственным значением, а ненулевой вектор W — собственным вектором квадратной матрицы A, если они связаны между собой соотношением $AW = \lambda W$.

Собственные значения квадратной матрицы $A_{n\times n}$ могут быть вычислены как корни уравнения $\det(A - \lambda E) = 0$, а собственные векторы — как решение соответствующих однородных систем $(A - \lambda E)W = 0$.

Определение. Собственный вектор, отвечающий максимальному собственному значению, называется главным собственным вектором.

Пример. Рассмотрим следующую матрицу парных сравнений:

$$[A] = \begin{array}{c|ccc} & A_1 & A_2 & A_3 \\ \hline A_1 & 1 & \frac{1}{3} & \frac{1}{2} \\ A_2 & 3 & 1 & 3 \\ A_3 & 2 & \frac{1}{3} & 1 \end{array}$$

Вычислим для данной матрицы главный собственный вектор.

$\det(A - \lambda E) = 0$,

$$\begin{vmatrix} 1-\lambda & \frac{1}{3} & \frac{1}{2} \\ 3 & 1-\lambda & 3 \\ 2 & \frac{1}{3} & 1-\lambda \end{vmatrix} = 0,$$

$$(1-\lambda)\cdot\begin{vmatrix} 1-\lambda & 3 \\ \frac{1}{3} & 1-\lambda \end{vmatrix} - 3\cdot\begin{vmatrix} \frac{1}{3} & \frac{1}{2} \\ \frac{1}{3} & 1-\lambda \end{vmatrix} + 2\cdot\begin{vmatrix} \frac{1}{3} & \frac{1}{2} \\ 1-\lambda & 3 \end{vmatrix} = 0,$$

$$(1-\lambda)\cdot\left[(1-\lambda)^2-1\right]-3\cdot\left(\frac{1-\lambda}{3}-\frac{1}{6}\right)+2\cdot\left(1-\frac{1-\lambda}{2}\right)=0.$$

При решении данного уравнения получено максимальное собственное значение $\lambda_{max} = 3{,}05$. Для вычисления главного собственного вектора необходимо решить систему линейных уравнений:

$$\begin{pmatrix} 1 & \frac{1}{3} & \frac{1}{2} \\ 3 & 1 & 3 \\ 2 & \frac{1}{3} & 1 \end{pmatrix}\cdot\begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = 3{,}05\cdot\begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} W = \begin{pmatrix} 0{,}157 \\ 0{,}594 \\ 0{,}249 \end{pmatrix}.$$

Полученный главный собственный вектор ранжирует альтернативы и назначает им веса. Таким образом, вторая альтернатива наиболее предпочтительная, затем идет третья и первая. Заметим, что сумма координат полученного вектора равна единице. Таким образом, можно говорить об относительной важности того или иного сравниваемого критерия или альтернативы.

Квадратная матрица имеет не более n различных собственных значений. Вычислить главный собственный вектор положительной квадратной матрицы A с точностью до некоторого постоянного сомножителя C можно по формуле

$$\lim_{k\to\infty}\frac{A^k e}{e^{\mathrm{T}} A^k e} = CW,$$

где $e = (1, 1, ..., 1)^{\mathrm{T}}$ — вектор составленный из n единиц.

Максимальное собственное значение вычисляется по формуле: $\lambda_{max} = e^{\mathrm{T}} AW$.

Как видно из рассмотренного примера, вычисление собственных векторов и собственных значений «в лоб» не является тривиальной задачей. При вычислении максимального собственного значения матриц порядка больше двух практически всегда требуется прибегать к приближенным методам. Такой подход существенно усложняет задачу, так как в случае одной иерархии число матриц парных сравнений может быть очень велико. В случае, когда человек не владеет численными методами, метод иерархической иерархии вообще может быть им отклонен.

Для вычисления собственных векторов и собственных значений матриц целесообразно использовать вычислительные средства и современные программные продукты. Однако при отсутствии вычислительных мощностей приближенное значение главного собственного вектора можно получить суммированием элементов каждой строки и последующим делением каждой суммы на сумму элементов всей матрицы.

Пример. Рассмотрим матрицу парных сравнений и вычислим приближенное значение главного собственного вектора:

$$[A] = \begin{array}{c|ccc} & A_1 & A_2 & A_3 \\ \hline A_1 & 1 & \frac{1}{3} & \frac{1}{2} \\ A_2 & 3 & 1 & 3 \\ A_3 & 2 & \frac{1}{3} & 1 \end{array}.$$

Просуммируем элементы каждой строки и найдем сумму всех элементов матрицы:

$$W_S = \begin{pmatrix} 1\frac{5}{6} \\ 7 \\ 3\frac{1}{3} \end{pmatrix}, \qquad S = 1\frac{5}{6}+7+3\frac{1}{3} = 12\frac{1}{6}.$$

Нормализуя вектор W_S делением каждой координаты на величину S, получаем приближенное значение главного собственного вектора

$$\hat{W} = \begin{pmatrix} 0{,}151 \\ 0{,}575 \\ 0{,}274 \end{pmatrix}.$$

Приближенное значение максимального собственного значения можно найти по формуле $\lambda_{max} = e^{\mathrm{T}} AW$, рассмотренной выше:

$$\lambda_{max} = (1\ 1\ 1)\cdot\begin{pmatrix} 1 & \frac{1}{3} & \frac{1}{2} \\ 3 & 1 & 3 \\ 2 & \frac{1}{3} & 1 \end{pmatrix}\cdot\begin{pmatrix} 0{,}151 \\ 0{,}575 \\ 0{,}274 \end{pmatrix} \approx 3{,}10.$$

При таком вычислении главного собственного вектора и максимального собственного значения может оказаться, что согласованная в действительности матрица является несогласованной по вычислениям, и наоборот.

Пример. Вычислим отношение согласованности рассмотренной матрицы, взяв в качестве максимального собственного значения его точное и приближенное число:

$$\text{ИС} = \frac{3{,}05-3}{3-1} = 0{,}025;\ \text{ОС} = \frac{0{,}025}{0{,}58} \approx 0{,}04;$$

$$\text{ИС}_{\approx} = \frac{3{,}10-3}{2} = 0{,}05;\ \text{ОС}_{\approx} = \frac{0{,}05}{0{,}58} \approx 0{,}09.$$

При большей погрешности метода вычисления главного собственного вектора отношение согласованности матрицы парных сравнений могло оказаться больше 0,10.

Желательно использовать процедуры точного нахождения собственных значений и векторов матриц. Такое пожелание превращается в требование в особо ответственных задачах.

Вычисление собственных векторов и значений в пакете Mathematica

Для вычисления собственных векторов и значений первым шагом является определение матрицы. Для определения введем в пустом документе название матрицы *M* и поставим знак равенства. Зададим трехмерную матрицу с единицами на главной диагонали. Для этого выберем в меню опцию *Input Create Table/Matrix/Palette...* или используем комбинацию клавиш <*Shift*>+<*Ctrl*>+<*C*> (рис. 5.8 и 5.9). В открывшемся окне определим размерность матрицы и отметим необходимость заполнить главную диагональ единицами. Поля, которые необходимо заполнять, выделены на рис. 5.9.

После вставки матрицы и заполнения всех ее элементов необходимо нажать клавиши <*Shift*>+<*Enter*> — пакет произведет назначение матрице соответствующих числовых характеристик.

Вычисление собственных значений выполняется функцией *Eigenvalues*[*M*], а собственных векторов — функцией *Eigenvectors*[*M*]. При вычислении желательно сопроводить функции последующим символом *N* через две косые черты (//*N*), в противном случае Mathematica проведет вычисления символьно. После ввода строки *Eigenvalues*[*M*]//*N* и нажатия клавиш <*Shift*>+<*Enter*>, Mathematica выдаст результат, представленный на рис. 5.10.

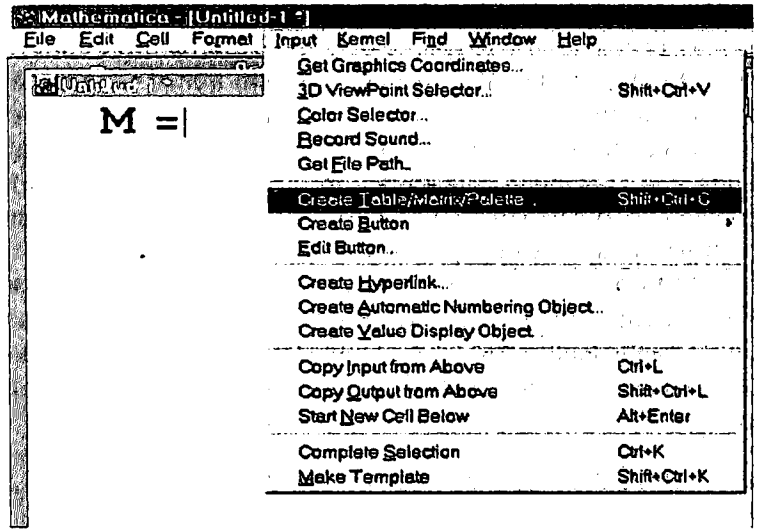


Рис. 5.8. Меню вставки пакета Mathematica

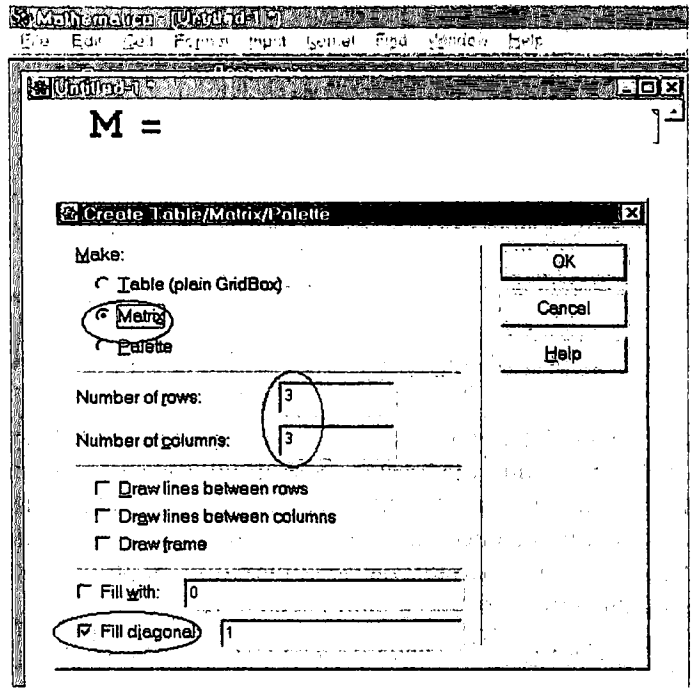


Рис. 5.9. Определение размерности матрицы в пакете Mathematica

На рис. 5.10 приведены вычисления и векторов, и значений. При выполнении вычислений получено одно действительное собственное значение. Это значение нас и интересует, оно несколько превышает размерность матрицы, тройку, что свидетельствует о неполной согласованности матрицы. На приведенном рисунке интересующий нас вектор обведен. Вектор не является нормированным. Для его нормализации необходимо найти сумму элементов вектора, а затем разделить все координаты на получившуюся сумму.

При использовании пакета Mathematica необходимо помнить, что строчные и заглавные буквы различаются. Так, например, названия функций должны начинаться с заглавной буквы, в противном случае они не распознаются. Аргументы функций обязаны стоять в квадратных скобках.

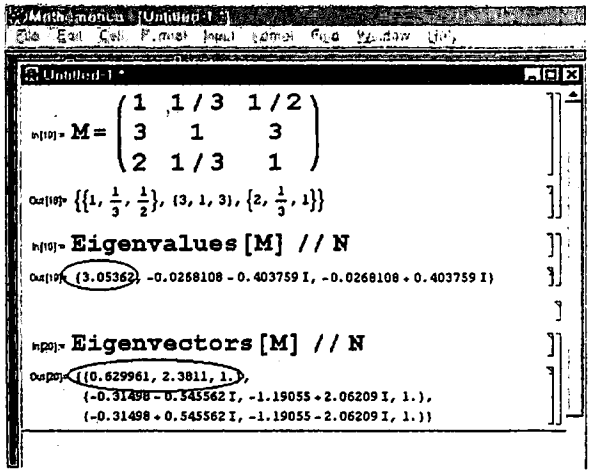


Рис. 5.10. Вычисление собственных значений и векторов матрицы в пакете Mathematica

Вычисление необходимых величин даже при помощи пакета является задачей, требующей времени. В Mathematica можно создавать собственные процедуры и функции, писать мультимедийные учебники. Процедуру поиска собственных значений и векторов можно закодировать, что в дальнейшем сведет операцию вычисления лишь к вводу новых значений матрицы парных сравнений.

Вычисление собственных векторов и значений в Mathcad

Вычислим собственные векторы и значения с использованием Mathcad. Определим и введем в рабочий документ матрицу парных

сравнений. В Mathcad операция присваивание выполняется посредством оператора :=. Для того чтобы определить матрицу, введем с клавиатуры ее имя и знак присваивания. Для присваивания необходимо нажать на клавиатуре комбинацию клавиш <*Shift*>+<:>, в результате чего появится знак присваивания (рис. 5.11). Для ввода матрицы воспользуемся одной из опций. Большинство вычислений с матрицами, и другие вычисления в Mathcad, можно выполнить тремя способами — с помощью панелей инструментов, выбором операции в меню или обращением к соответствующей функции.

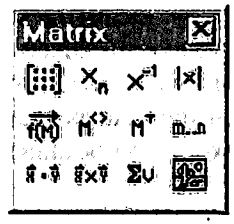


Рис. 5.11. Панель операций с матрицами в пакете Mathcad

Воспользуемся первым вариантом. После того как имя матрицы и оператор присваивания введены, откроем панель операций с матрицами, щелкнув по кнопке (см. рис. 5.11). После этого на появившейся панели щелкнем по кнопке и зададим размерность матрицы (рис. 5.12).

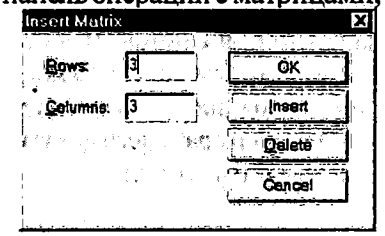


Рис. 5.12. Окно определения размеров матрицы в Mathcad

После ввода матрицы присвоим некоторой переменной значение функции *eigenvals(A)*. Эта функция вычисляет собственные значения квадратной матрицы *A*. Присвоение должно быть выполнено правее или ниже определения матрицы *A*, в противном случае матрица *A* для функции будет неизвестна. После выполнения такого присваивания введем с клавиатуры C=. Фрагмент рабочего стола после выполнения всех описанных процедур имеет вид

$$A := \begin{pmatrix} 1 & \frac{1}{3} & \frac{1}{2} \\ 3 & 1 & 3 \\ 2 & \frac{1}{3} & 1 \end{pmatrix} \qquad C := \text{eigenvals}(A)$$

$$C = \begin{pmatrix} 3.054 \\ -0.027 + 0.404i \\ -0.027 - 0.404i \end{pmatrix}.$$

Для вычисления главного собственного вектора воспользуемся функцией *eigenvec(A, z)* — вычисление собственного вектора матрицы *A*, отвечающего собственному значению *z*. Чтобы обратиться к функции, введем с клавиатуры ее имя, затем перечислим в скобках ее аргу-

менты: название матрицы и название вектора собственных значений с индексом, задающим номер интересующего нас собственного значения. Индексы координат векторов в Mathcad начинаются с нулевого (данная настройка может быть изменена). После ввода функции необходимо поставить знак равенства:

$$\text{eigenvec}(A, C_0) = \begin{pmatrix} 0.237 \\ 0.896 \\ 0.376 \end{pmatrix}.$$

Вектор не нормирован. Нормируем его. Для удобства расчетов присвоим главный собственный вектор некоторой переменной *P*. Сумму *S* координат вектора *P* вычислим при помощи кнопки $\sum$ на панели операций с матрицами (рис. 5.11, кнопка вторая слева внизу). При ее нажатии появляется знак суммы. Под знаком суммы поставим вектор *P*, координаты которого мы собираемся суммировать. После нахождения суммы произведем деление вектора *P* на сумму *S*.

Фрагмент рабочего документа Mathcad, содержащий перечисленные действия, имеет вид:

$$P := \text{eigenvec}(A, C_0)$$

$$S := \sum P \quad S = 1.509$$

$$\frac{P}{S} = \begin{pmatrix} 0.157 \\ 0.594 \\ 0.249 \end{pmatrix}.$$

Для того чтобы вычислить собственные значения и главный собственный вектор новой матрицы, достаточно изменить числа в исходной матрице A. При этом необходимо следить, чтобы индекс интересующего нас собственного значения был соответствующим. Рабочий стол удобно дополнить формулами индекса согласованности и отношения согласованности матрицы парных сравнений:

$$A := \begin{pmatrix} 1 & \frac{1}{4} & \frac{1}{2} \\ 4 & 1 & 3 \\ 2 & \frac{1}{3} & 1 \end{pmatrix} \quad C := \text{eigenvals}(A) \quad C = \begin{pmatrix} 3.018 \\ -9.147 \times 10^{-3} + 0.235i \\ -9.147 \times 10^{-3} + 0.235i \end{pmatrix}$$

$$\text{eigenvec}(A, C_0) = \begin{pmatrix} 0.2 \\ 0.915 \\ 0.349 \end{pmatrix} \quad P := \text{eigenvec}(A, C_0)$$

$$S := \sum P \quad S = 1.465 \quad \frac{P}{S} = \begin{pmatrix} 0.136 \\ 0.625 \\ 0.238 \end{pmatrix}$$

$$IS := \frac{C_0 - 3}{2} \quad IS = 9.147 \times 10^{-3} \quad OS := \frac{IS}{0.58} \quad OS = 0.016.$$

Ввод нижнего индекса можно произвести при помощи кнопки x_n панели операций с матрицами (см. рис. 5.11, кнопка вторая справа сверху).

Вычисление собственных векторов и значений по формулам

Для вычисления главного собственного вектора и наибольшего собственного значения *обратносимметрической* квадратной матрицы второго, третьего и четвертого порядка существуют точные формулы. Использование формул весьма сомнительно в силу большого числа вычислений, за исключением матрицы второго порядка:

Матрица 2×2:

$\begin{bmatrix} 1 & a \\ 1/a & 1 \end{bmatrix}$. Для этого случая $\lambda_{max} = 2$, $W = \left(\frac{a}{a+1}; \frac{1}{a+1}\right)$.

Матрица 3×3

$$\begin{bmatrix} 1 & a_{12} & a_{13} \\ 1/a_{12} & 1 & a_{23} \\ 1/a_{13} & 1/a_{23} & 1 \end{bmatrix}; \quad \lambda_{max} = \sqrt[3]{\frac{a_{13}}{a_{12} \cdot a_{23}}} + \sqrt[3]{\frac{a_{12} \cdot a_{23}}{a_{13}}} + 1.$$

$$D = a_{12} \cdot a_{23} + (a_{13} + a_{23}) \cdot (\lambda - 1) + a_{13}/a_{12} - 1 + (1 - \lambda)^2.$$

$$\Delta = a_{12} \cdot a_{23} + a_{13} \cdot (\lambda - 1).$$

$$W=\begin{bmatrix} \frac{\Delta}{D} \\ \frac{(\lambda-1)\cdot a_{23}+a_{13}/a_{12}}{D} \\ \frac{-1+(1-\lambda)^2}{D} \end{bmatrix}.$$

Матрица 4×4

$$\begin{bmatrix} 1 & a & b & c \\ 1/a & 1 & d & e \\ 1/b & 1/d & 1 & f \\ 1/c & 1/e & 1/f & 1 \end{bmatrix}$$

$$B=\left(\frac{df}{e}+\frac{e}{df}\right)+\left(\frac{ae}{c}+\frac{c}{ae}\right)+\left(\frac{ad}{b}+\frac{b}{ad}\right)+\left(\frac{bf}{c}+\frac{c}{bf}\right)$$

$$r=\sqrt[3]{\left(-8+\frac{B^2}{2}+8C\right)+\sqrt{\left[-\frac{4}{3}\cdot(C+3)\right]^3+\left(8-\frac{B^2}{2}-8C\right)^2}}+$$

$$+\sqrt[3]{\left(-8+\frac{B^2}{2}+8C\right)-\sqrt{\left[-\frac{4}{3}\cdot(C+3)\right]^3+\left(8-\frac{B^2}{2}-8C\right)^2}}.$$

$$\lambda_{max}=\frac{2+\sqrt{r+4}}{2}+\sqrt{\frac{8-r}{4}+\frac{B}{2\cdot\sqrt{r+4}}}$$

$$Q=(\lambda-1)^3+(c+f+e)\cdot(\lambda-1)^2+\left[(a\cdot e-3)+(b+d)\cdot f+\left(\frac{1}{a}+\frac{1}{b}\right)\cdot c+\frac{e}{d}\right]\cdot$$

$$\cdot(\lambda-1)+\left[(adf-c-e-f)+\left(\frac{be}{d}+\frac{bf}{a}\right)+\frac{cd+ae-ad}{b}+\frac{c-b}{ad}\right].$$

$$W=\begin{bmatrix} \frac{c(\lambda-1)^2+(ae+bf)\cdot(\lambda-1)+\left(adf+\frac{be}{d}-c\right)}{Q} \\ \frac{e(\lambda-1)^2+\left(df+\frac{c}{a}\right)\cdot(\lambda-1)+\left(\frac{bf}{a}+\frac{cd}{b}-e\right)}{Q} \\ \frac{f(\lambda-1)^2+\left(\frac{e}{d}+\frac{c}{b}\right)\cdot(\lambda-1)+\left(\frac{c}{ad}+\frac{ae}{b}-f\right)}{Q} \\ \frac{(\lambda-1)^3-3(\lambda-1)-\left(\frac{ad}{b}+\frac{b}{ad}\right)}{Q} \end{bmatrix}.$$

Вычисление собственных векторов и значений в MS Excel

Довольно просто, используя определение собственного значения и формулу $\lambda_{max}=e^{T}AW$, а также теорему о величине максимального собственного значения обратносимметрической квадратной матрицы, средствами MS Excel можно получать наибольшее собственное значение и нормированный главный собственный вектор. Для этого можно создать макрос или же воспользоваться возможностями инструмента *Поиск решения*. Реализовать такой подход студентам предлагается самостоятельно — как индивидуальное задание, групповое или в виде дискуссии на семинаре.

5.3.5. Подсчет количественной оценки качества альтернатив (иерархический синтез)

Иерархический синтез используется для общего ранжирования альтернатив относительно цели, т.е. для подсчета количественной оценки качества альтернатив. Рассмотрим иерархию на рис. 5.13.

Алгоритм иерархического синтеза для приведенного примера следующий.

1. Определим векторы приоритетов $W_{E_1^3}, W_{E_2^3}, W_{E_3^3}$ относительно последнего уровня иерархии. Для этого строим матрицы парных сравнений $[E_1^3], [E_2^3], [E_3^3]$ и вычисляем для каждой из матриц максимальные собственные значения (для оценки однородности суждений) и главные собственные вектора (приоритеты):

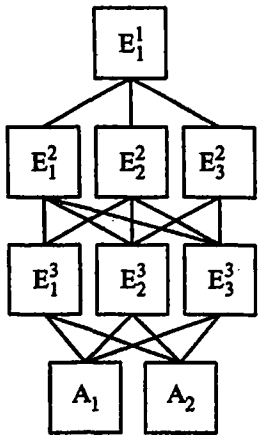


Рис. 5.13. Пример трехуровневой иерархической структуры

$$[E_1^3]=\begin{array}{c|cc} & A_1 & A_2 \\ \hline A_1 & 1 & a_{12} \\ A_2 & 1/a_{12} & 1 \end{array} \Rightarrow \lambda_{\max}, W_{E_1^3}$$

$$[E_2^3]=\begin{array}{c|cc} & A_1 & A_2 \\ \hline A_1 & 1 & * \\ A_2 & 1/* & 1 \end{array} \Rightarrow \lambda_{\max}, W_{E_2^3}$$

$$[E_3^3]=\begin{array}{c|cc} & A_1 & A_2 \\ \hline A_1 & 1 & \times \\ A_2 & 1/\times & 1 \end{array} \Rightarrow \lambda_{\max}, W_{E_3^3}$$

2. Аналогичным образом обрабатываем матрицы парных сравнений для вышележащих уровней. Эти матрицы построены для того, чтобы определить предпочтительность элементов определенного иерархического уровня относительно элементов вышележащего уровня.

$$[E_1^2]=\begin{array}{c|ccc} & E_1^3 & E_2^3 & E_3^3 \\ \hline E_1^3 & & & \\ E_2^3 & & & \\ E_3^3 & & & \end{array} \Rightarrow \lambda_{\max}, W_{E_1^2}$$

$$[E_2^2]=\begin{array}{c|ccc} & E_1^3 & E_2^3 & E_3^3 \\ \hline E_1^3 & & & \\ E_2^3 & & & \\ E_3^3 & & & \end{array} \Rightarrow \lambda_{\max}, W_{E_2^2}$$

$$[E_3^2]=\begin{array}{c|cc} & E_2^3 & E_3^3 \\ \hline E_2^3 & & \\ E_3^3 & & \end{array} \Rightarrow \lambda_{\max}, W_{E_3^2}$$

3. Осуществляем иерархический синтез. Последовательно определяем векторы приоритетов альтернатив $W_{E_j^i}^A$ относительно элементов E_j^i, находящихся на всех иерархических уровнях. Для предпоследнего уровня $W_{E_1^3}^A = W_{E_1^3}$, $W_{E_2^3}^A = W_{E_2^3}$, $W_{E_3^3}^A = W_{E_3^3}$. Вычисление векторов приоритетов проводится в направлении от нижних уровней к верхним с учетом конкретных связей между элементами, принадлежащими различным уровням. Вычисление производится перемножением соответствующих векторов и матриц.

$$W_{E_1^2}^A = [\underbrace{W_{E_1^3}^A \quad W_{E_2^3}^A \quad W_{E_3^3}^A}_{\text{матрица}}] \cdot W_{E_1^2} \qquad W_{E_2^2}^A = [W_{E_1^3}^A \quad W_{E_2^3}^A \quad W_{E_3^3}^A] \cdot W_{E_2^2}$$

$$W_{E_3^2}^A = [W_{E_2^3}^A \quad W_{E_3^3}^A] \cdot W_{E_3^2}.$$

Результирующий вектор приоритетов альтернатив относительно основной цели $W_{E_1^1}^A = [W_{E_1^2}^A \quad W_{E_2^2}^A \quad W_{E_3^2}^A] \cdot W_{E_1^1}$.

Пример (из книги Т. Саати[1]). Рассмотрим общее благополучие индивидуума — высший уровень иерархии. На этот уровень в основном влияют детские, юношеские и взрослые впечатления. Факторы развития и зрелости, отражающиеся в благополучии, могут включать как влияние отца и матери в отдельности, так и их совместное влияние как родителей, социоэкономический фон, отношения с братьями и сестрами, группа ровесников, школьное обучение, религиозный статус и т.д.

На перечисленные факторы, которые составляют второй уровень иерархии, влияют соответствующие критерии. Например, влияние отца может быть разбито на категории, включающие его темперамент, строгость, заботу и привязанность. Отношение с братьями и сестрами можно дальше характеризовать их количеством, разницей в возрасте, полом; моделирование воздействия и роли ровесников обеспечивает более яркую картину влияния друзей, обучения в школе и учителей.

В качестве альтернативной основы описания для второго уровня можно включить чувство собственного достоинства, уверенность в будущем, адаптируемость к новым людям и новым обстоятельствам и т.д., влияющим или находящимся под влиянием расположенных выше элементов.

[1] *Саати Т.* Принятие решений. Метод анализа иерархий: Пер. с англ. — М.: Радио и связь, 1989.

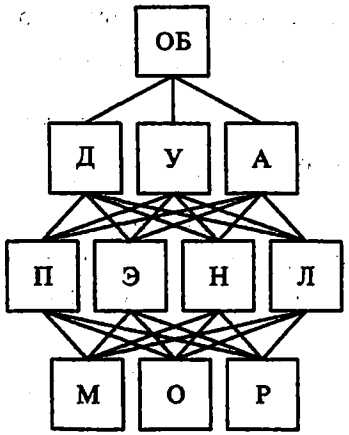


Рис. 5.14. Иерархическая схема общего благополучия индивидуума

Более полная основа психологической предыстории может включать несколько сотен элементов на каждом уровне, выбранных экспертами и расположенных таким образом, чтобы получить максимальное понимание рассматриваемого индивидуума.

Рассмотрим ограниченный случай, где испытуемый чувствует, что уверенность в его силах подорвана и его социальная приспособляемость ослаблена запретами в детстве. Ему задают вопросы только о детских впечатлениях и просят попарно установить связь между следующими элементами на каждом уровне.

Построим иерархию, в которой: ОБ — общее благополучие; Д — чувство собственного достоинства; У — чувство уверенности в будущем; А — способность адаптироваться к другим; П — явная привязанность, проявленная по отношению к субъекту; Э — идеи строгости, этики; Н — действительное наказание ребенка; Л — подчеркивание личной приспособляемости к другим; М — влияние матери; О — влияние отца; Р — влияние обоих родителей.

Выполним расчеты по иерархической схеме, приведенной на рис. 5.14.

[ОБ] =

	Д	У	А
Д	1	6	4
У	1/6	1	3
А	1/4	1/3	1

$W_{ОБ}$=(0,701; 0,193; 0,106)

λ_{max} = 3,26; ИС = 0,07; ОС = 0,12

[Д] =

	П	Э	Н	Л
П	1	6	6	3
Э	1/6	1	4	3
Н	1/6	1/4	1	1/2
Л	1/3	1/3	2	1

$W_{Д}$ = (0,604; 0,213; 0,064; 0,119)

λ_{max} = 4,35; ИС = 0,12; ОС = 0,13

[У] =

	П	Э	Н	Л
П	1	6	6	3
Э	1/6	1	4	3
Н	1/6	1/4	1	1/2
Л	1/3	1/3	2	1

$W_{Д}$ = (0,604; 0,213; 0,064; 0,119)

λ_{max} = 4,35; ИС = 0,12; ОС = 0,13

[А] =

	П	Э	Н	Л
П	1	1/5	1/3	1
Э	5	1	4	1/5
Н	3	1/4	1	1/4
Л	1	5	4	1

$W_{ОБ}$ = (0,127; 0,281; 0,120; 0,463)

λ_{max} = 5,42; ИС = 0,47; ОС = 0,52

[П] =

	М	О	Р
М	1	9	4
О	1/9	1	8
Р	1/4	1/8	1

$W_{П}$ = (0,721; 0,210; 0,069)

λ_{max} = 4; ИС = 0,33; ОС = 0,57

[Э] =

	М	О	Р
М	1	1	1
О	1	1	1
Р	1	1	1

$W_{Э}$ = (0,333; 0,333; 0,333)

λ_{max} = 0; ИС = 0,0; ОС = 0,0

[Н] =

	М	О	Р
М	1	9	6
О	1/9	1	1/4
Р	1/6	4	1

$W_{Н}$ = (0,713; 0,061; 0,176)

λ_{max} = 3,11; ИС = 0,06; ОС = 0,10

[Л] =

	М	О	Р
М	1	5	5
О	1/5	1	1/3
Р	1/5	3	1

$W_{Н}$ = (0,701; 0,097; 0,202)

λ_{max} = 3,14; ИС = 0,07; ОС = 0,12

Осуществим иерархический синтез:

$$\begin{bmatrix} 0{,}721 & 0{,}333 & 0{,}713 & 0{,}701 \\ 0{,}210 & 0{,}333 & 0{,}061 & 0{,}097 \\ 0{,}069 & 0{,}333 & 0{,}176 & 0{,}202 \end{bmatrix} \cdot \begin{bmatrix} 0{,}604 & 0{,}604 & 0{,}127 \\ 0{,}213 & 0{,}213 & 0{,}281 \\ 0{,}064 & 0{,}064 & 0{,}120 \\ 0{,}119 & 0{,}119 & 0{,}463 \end{bmatrix} \cdot \begin{bmatrix} 0{,}701 \\ 0{,}193 \\ 0{,}106 \end{bmatrix} = \begin{bmatrix} 0{,}635 \\ 0{,}208 \\ 0{,}156 \end{bmatrix}.$$

Индивидууму посоветовали больше общаться с отцом с целью уравновешивания влияния родителей.

В приведенном примере некоторые матрицы несогласованные. Однако следует понимать, что человеку в данной ситуации нельзя было повторно задавать одни и те же вопросы до тех пор, пока все матрицы не стали бы однородными.

После решения задачи синтеза иерархии, оценивается однородность всей иерархии с помощью суммирования показателей однородности всех уровней, приведенных путем взвешивания к первому иерархическому уровню.

Пример. Рассмотрим иерархию из предыдущего примера. Пусть $ИО_1$ — индекс согласованности первого уровня; $ИО_{21}$, $ИО_{22}$ и $ИО_{23}$ — индексы согласованности второго уровня; $ИО_{31}$, $ИО_{32}$, $ИО_{33}$ и $ИО_{34}$ — индексы согласованности третьего уровня. Тогда индекс однородности иерархии можно определить следующим образом:

$$ИО_И = ИО_1 + W_{ОБ}^{Т} \cdot \begin{bmatrix} ИО_{21} \\ ИО_{22} \\ ИО_{23} \end{bmatrix} + W_{ОБ}^{Т} \cdot [W_Д \;\; W_У \;\; W_А]^{Т} \begin{bmatrix} ИО_{31} \\ ИО_{32} \\ ИО_{33} \\ ИО_{34} \end{bmatrix}.$$

$$ИО_И = 0{,}07 + (0{,}701; 0{,}193; 0{,}106) \cdot \begin{bmatrix} 0{,}12 \\ 0{,}12 \\ 0{,}47 \end{bmatrix} + (0{,}701; 0{,}193; 0{,}106) \times$$

$$\times \begin{bmatrix} 0{,}604 & 0{,}213 & 0{,}064 & 0{,}119 \\ 0{,}604 & 0{,}213 & 0{,}064 & 0{,}119 \\ 0{,}127 & 0{,}281 & 0{,}120 & 0{,}463 \end{bmatrix} \cdot \begin{bmatrix} 0{,}33 \\ 0{,}00 \\ 0{,}06 \\ 0{,}07 \end{bmatrix} = 0{,}42.$$

Для оценки отношения однородности используют выражение

$$ОО_И = \frac{ИО_И}{М(ИО_И)},$$

где

$$М(ИО_И) = М(ИО_1) + W_{ОБ}^{Т} \cdot \begin{bmatrix} М(ИО_{21}) \\ М(ИО_{22}) \\ М(ИО_{23}) \end{bmatrix} + W_{ОБ}^{Т} \cdot [W_Д \; W_У \; W_А]^{Т} \begin{bmatrix} М(ИО_{31}) \\ М(ИО_{32}) \\ М(ИО_{33}) \\ М(ИО_{34}) \end{bmatrix}.$$

$$М(ИО_И) = 0{,}58 + (0{,}701; 0{,}193; 0{,}106) \cdot \begin{bmatrix} 0{,}9 \\ 0{,}9 \\ 0{,}9 \end{bmatrix} + (0{,}701; 0{,}193; 0{,}106) \times$$

$$\times \begin{bmatrix} 0{,}604 & 0{,}213 & 0{,}064 & 0{,}119 \\ 0{,}604 & 0{,}213 & 0{,}064 & 0{,}119 \\ 0{,}127 & 0{,}281 & 0{,}120 & 0{,}463 \end{bmatrix} \cdot \begin{bmatrix} 0{,}58 \\ 0{,}58 \\ 0{,}58 \\ 0{,}58 \end{bmatrix} = 2{,}06.$$

$$ОО_И = \frac{ИО_И}{М(ИО_И)} = \frac{0{,}42}{2{,}06} = 0{,}20.$$

Однородность иерархии считается удовлетворительной при значениях $ОО_И \le 0{,}10$.

5.3.6. Метод сравнения объектов относительно стандартов

Метод парного сравнения альтернатив не всегда может быть эффективно применен в некоторых практических ситуациях[1].

1. Эксперту может быть предложено для анализа более девяти альтернатив, что существенно усложняет построение согласованных матриц парных сравнений.

2. При добавлении новых альтернатив изменяется порядок ранее прошедших альтернатив относительно критериев качества.

[1] *Трахтенгерц Э.А.* Компьютерная поддержка принятия решений: Научно-практич. изд. — М.: СИНТЕГ, 1998. — Серия «Информатизация России на пороге XXI века».

3. Альтернативы могут поступать эксперту для сравнения не одновременно, а через определенные промежутки времени. Поэтому невозможно попарно сравнивать объекты.

Для решения проблемы сравнения и оценки альтернатив в указанных ситуациях наиболее целесообразен метод сравнения альтернатив относительно стандартов. Стандарт устанавливает уровень качества объекта относительно критерия качества. Например, критерию «ликвидность» для объекта «экономические выгоды обеспечения банковского кредита» может быть назначено три стандарта, характеризующих соответственно высокий (H), средний (M) и низкий (L) уровни ликвидности. Каждый стандарт отождествляется, как правило, с некоторым существующим на практике эталоном качества; так высокий, средний и низкий стандарты по критерию «ликвидность» могут быть отождествлены с драгоценными металлами, ценными бумагами и недвижимостью. В иерархии стандарты присваиваются элементам, имеющим непосредственную связь с альтернативами (рис. 5.15). Число стандартов по каждому такому элементу может быть различно и определяется экспертом.

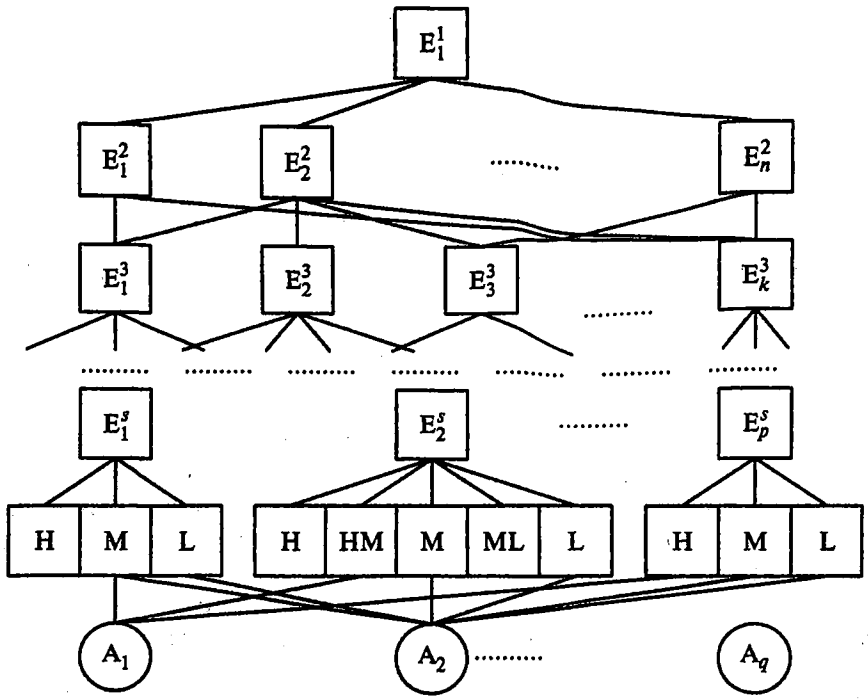


Рис. 5.15. Иерархическая структура с учетом стандартов

По каждому стандарту эксперт устанавливает относительную степень предпочтения, которая указывает значимость стандарта для эксперта. Численное значение каждого стандарта определяется их попарным сравнением по шкале отношений и вычислением главного собственного вектора.

Введем следующие обозначения:

$C\{C_0, C_g\}$ — множество стандартов, включающее два подмножества, устанавливающие, соответственно, основную $\{C_0\}$и дополнительную $\{C_g\}$ шкалы. Основная шкала включает градации $C_0 = \{H, M, L\}$. Дополнительная шкала может включать градации $C_g = \{HH, HM, ML, LL\}$, где HH, HM, ML, LL — соответственно очень высокое, промежуточное между высоким и средним, промежуточное между средним и низким, очень низкое значение стандартов.

Для каждого элемента E_j^s иерархии, непосредственно связанного со стандартами, устанавливается подмножество $C_j \subset C$. Стандарты, входящие в подмножества C_j, сформированные относительно E_j^s, попарно сравниваются по 9-балльной шкале и вычисляются векторы W_j^s.

ЛПР присваивает каждой альтернативе значение одного стандарта. Процедура идентификации проводится по всем элементам E_j^s. В результате идентификации строится матрица A вида

$$A = \begin{array}{c|cccc} & E_1^s & E_2^s & \dots & E_p^s \\ \hline A_1 & w_{11} & w_{12} & \dots & w_{1p} \\ A_2 & w_{21} & w_{22} & \dots & w_{2p} \\ \vdots & \dots & \dots & \dots & \dots \\ A_r & w_{r1} & w_{r2} & \dots & w_{rp} \end{array}$$

Элементы матрицы представляют собой численные значения стандартов, соответствующие определенной альтернативе и элементу E_j^s. Таким образом, столбцы в матрице A представляют собой ненормированные векторы приоритетов альтернатив по соответствующим элементам E_j^s.

Для получения нормированным векторов W_j^A приоритетов альтернатив необходимо все элементы каждого столбца разделить на сумму элементов соответствующего столбца или, что то же самое, умножить матрицу A на диагональную матрицу S вида

$$S = \begin{array}{c|cccc} & E_1^s & E_2^s & \dots & E_p^s \\ A_1 & \left(\sum_{i=1}^{n} w_{i1}\right)^{-1} & 0 & \dots & 0 \\ A_2 & 0 & \left(\sum_{i=1}^{r} w_{i2}\right)^{-1} & \dots & 0 \\ \vdots & \dots & \dots & \dots & \dots \\ A_r & 0 & 0 & \dots & \left(\sum_{i=1}^{r} w_{ip}\right)^{-1} \end{array}$$

Множество нормированных векторов приоритетов альтернатив относительно всех элементов нижнего уровня определяется соотношением $[W^A] = [A] \cdot [S]$.

Далее алгоритм иерархического синтеза такой же, как и в методе парных сравнений.

В методе сравнения альтернатив относительно стандартов добавление новой альтернативы не нарушает порядок ранее проранжированных альтернатив.

Пример. Пусть задана иерархия, представленная на рис. 5.16.

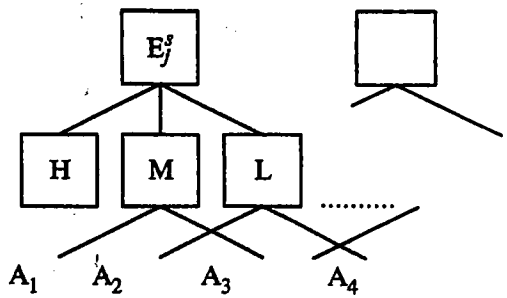


Рис. 5.16. Одна из ветвей иерархии с учетом стандартов

Пусть матрица предпочтений стандартов для элемента E_j^s имеет вид

$$\begin{array}{c|ccc} & H & M & L \\ H & 1 & 5 & 7 \\ M & 1/5 & 1 & 3 \\ L & 1/7 & 1/3 & 1 \end{array} \qquad W_j^S = \begin{pmatrix} 0{,}696 \\ 0{,}225 \\ 0{,}079 \end{pmatrix}.$$

Вектор $W_j^A = \begin{pmatrix} 0{,}225 \\ 0{,}079 \\ 0{,}225 \\ 0{,}079 \end{pmatrix}$, т.е. первая и третья альтернативы отвечают среднему стандарту по рассматриваемому критерию, а вторая и четвертая — низкому стандарту. Добавим еще одну альтернативу и присвоим ей значение, соответствующее высокому стандарту:

$$W_j^A = \begin{pmatrix} 0{,}225 \\ 0{,}079 \\ 0{,}225 \\ 0{,}079 \\ 0{,}696 \end{pmatrix}, \text{ или нормированный } W_{j\,(\text{норм})}^A = \begin{pmatrix} 0{,}173 \\ 0{,}061 \\ 0{,}173 \\ 0{,}061 \\ 0{,}534 \end{pmatrix}.$$

5.3.7. Многокритериальный выбор в иерархиях с различным числом и составом альтернатив под критериями

В практике встречаются задачи, когда ранжируемые по множеству критериев альтернативы оцениваются экспертом не по всем критериям[1]. Задача характерна для ситуаций, когда множество критериев, выделенных для всех рассматриваемых альтернатив, является избыточным относительно одной или нескольких альтернатив. В таком случае эксперт имеет разное число альтернатив под каждым критерием или под их частью.

Рассмотрим методику определения вектора приоритета альтернатив для случая, когда иерархия имеет один уровень критериев, объединенных фокусом (целью), и разное количество альтернатив у каждого критерия. Методика предполагает выполнение ряда процедур по структурированию информации и проведению вычислительных операций.

Процедура 1. Исходная проблема структурируется в виде иерархии.

Процедура 2. Осуществляется экспертная оценка альтернатив по соответствующим критериям, с использованием метода парного сравнения или метода сравнения альтернатив относительно стандартов. На основе экспертных оценок строится матрица A следующего вида:

[1] *Варфоломеев В.И., Воробьев С.Н.* Принятие управленческих решений: Учеб. пособие для вузов. — М.: КУДИЦ-ОБРАЗ, 2001.

$$A = \begin{array}{c|cccc} & E_1 & E_2 & \dots & E_p \\ \hline A_1 & a_{11} & a_{12} & \dots & a_{1p} \\ A_2 & a_{21} & a_{22} & \dots & a_{2p} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ A_r & a_{r1} & a_{r2} & \dots & a_{rp} \end{array}$$

В матрице A экспертные оценки a_{ij} представляют векторы приоритетов альтернатив относительно критериев E_j. При этом если альтернатива A_i не оценивается по критерию E_j, то в матрице A соответствующее значение $a_{ij} = 0$. Векторы в матрице имеют различное число значений a_{ij} и могут быть нормированными или нет в зависимости от используемого метода сравнения альтернатив.

Процедура 3. В результате обработки матрицы попарных сравнений критериев относительно фокуса определяется вектор приоритетов критериев относительно цели.

Процедура 4. Формируются следующие диагональные матрицы S и L:

$$S = \begin{array}{c|cccc} & E_1 & E_2 & \dots & E_p \\ \hline & \left(\sum_{i=1}^{r} a_{i1}\right)^{-1} & 0 & \dots & 0 \\ & 0 & \left(\sum_{i=1}^{r} a_{i2}\right)^{-1} & \dots & 0 \\ & \vdots & \vdots & \dots & \vdots \\ & 0 & 0 & \dots & \left(\sum_{i=1}^{r} a_{ip}\right)^{-1} \end{array}$$

$$L = \begin{array}{c|cccc} & E_1 & E_2 & \dots & E_p \\ \hline & R_1/N & 0 & \dots & 0 \\ & 0 & R_2/N & \dots & 0 \\ & \vdots & \vdots & \dots & \vdots \\ & 0 & 0 & \dots & R_p/N \end{array}$$

где R_j — число альтернатив, находящихся под критерием E_j;

$N = \sum_{j=1}^{p} R_j$ — суммарное число альтернатив, находящихся под всеми критериями.

С помощью матрицы S нормируются векторы приоритетов альтернатив, образующих матрицу A, умножением последней на S справа. Использование критерия L позволяет эксперту или ЛПР изменять при необходимости вес альтернатив, связанных с соответствующими критериями пропорционально отношению R_j/N. Этим обеспечивается повышение приоритета альтернатив, образующих большие группы, и снижение приоритета альтернатив в группах с их относительно небольшим числом. Необходимость приведенной вычислительной процедуры обусловлена тем, что у критериев с высоким приоритетом в иерархии может находиться большое число альтернатив, а у критериев с низким приоритетом — значительно меньшее число альтернатив. В этой ситуации желательно повышение приоритетов альтернатив в большой группе, поскольку, если альтернатив много, каждая из них получит меньший составной приоритет, чем каждая альтернатива, входящая в меньшую группу с низким приоритетом критерия.

Процедура 5. Определяется вектор приоритетов альтернатив относительно W относительно критериев перемножением матриц слева направо следующих матриц и векторов:

$W = [A] \cdot [S] \cdot [L] \cdot \overline{X} \cdot [B]$ — случай ненормированных оценок в матрице A;

$W = [A] \cdot [L] \cdot \overline{X} \cdot [B]$ — случай нормированных оценок в матрице A.

Матрица B предназначена для окончательного нормирования значений вектора приоритетов альтернатив.

$$B = \begin{array}{c|cccc} & E_1 & E_2 & \dots & E_p \\ \hline & \left(\sum_{i=1}^{r} x_i\right)^{-1} & 0 & \dots & 0 \\ & 0 & \left(\sum_{i=1}^{r} x_i\right)^{-1} & \dots & 0 \\ & \vdots & \vdots & \dots & \vdots \\ & 0 & 0 & \dots & \left(\sum_{i=1}^{r} x_i\right)^{-1} \end{array}$$

где x_i — значение ненормированного вектора приоритетов альтернатив, полученное после последовательного перемножения матриц $[A] \cdot [S] \cdot [L] \cdot \overline{X}$;

r — число альтернатив.

Существуют иерархии, у которых альтернативы сгруппированы в подмножества $\{A_1, A_2, ..., A_m\}$, $\{A'_1, A'_2, ..., A'_s\}$, $\{A''_1, A''_2, ..., A''_l\}$, а элементы каждого из таких подмножеств связаны, в свою очередь, с определенными группами критериев $\{K_{11}, K_{12}, ..., K_{1t}\}$, $\{K_{21}, K_{22}, ..., K_{2r}\}$, $\{K_{n1}, K_{n2}, ..., K_{np}\}$ (рис. 5.17).

Дерево состоит из ряда самостоятельных иерархических ветвей.

Алгоритм синтеза для иерархии с несколькими ветвями

Шаг 1. Вычисляют векторы приоритетов альтернатив относительно критериев K_{ij}.

$$\left\{W^A_{K_{11}}, W^A_{K_{12}}, ..., W^A_{K_{1m}}\right\}$$

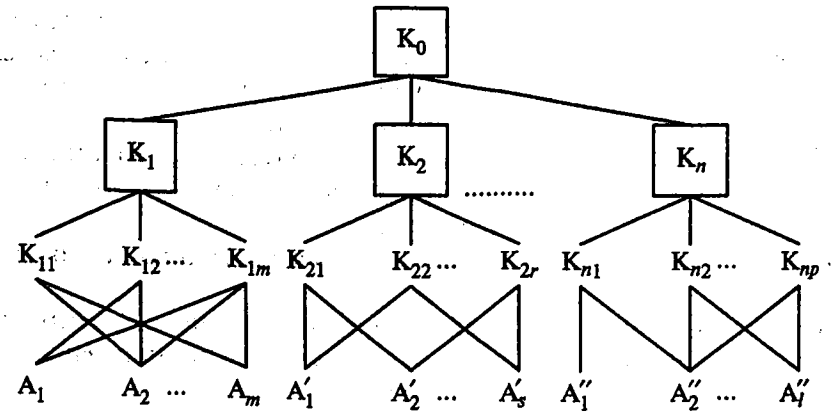


Рис. 5.17. Иерархия с несколькими ветвями

$$\left\{W^{A'}_{K_{21}}, W^{A'}_{K_{22}}, ..., W^{A'}_{K_{2r}}\right\}$$

$$\left\{W^{A''}_{K_{n1}}, W^{A''}_{K_{n2}}, ..., W^{A''}_{K_{np}}\right\}$$

Шаг 2. Строят матрицы A_i, у которых наименованиями строк являются альтернативы, а наименованиями столбцов — критерии K_{ij}. При этом если альтернатива не связана с критерием K_{ij}, то в матрице A_i на пересечении соответствующих строки и столбца ставится ноль.

Шаг 3. Вычисляются векторы приоритетов альтернатив W_i^A, $i = \overline{1, n}$ относительно критериев K_i по выражениям:

$$W_1^A = [A_1][S_1][L_1]\overline{X}_1[B_1]$$
$$W_2^A = [A_2][S_2][L_2]\overline{X}_2[B_2]$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$W_n^A = [A_n][S_n][L_n]\overline{X}_n[B_n]$$

Матрицы $[S_i]$ — для нормирования матриц $[A_i]$;

$[L_i]$ — матрица изменения веса альтернатив пропорционально соотношению R/N, где R — число альтернатив под критерием, а N — суммарное число альтернатив.

X_i — вектор приоритетов критериев K_{ij} относительно критериев K_i;

B_i — диагональная матрица для получения нормированного вектора W_i^A, $i = \overline{1, n}$.

Шаг 4. Вычисляют вектор приоритетов критериев X_0 относительно фокуса иерархии K_0.

Шаг 5. Строят результирующую матрицу A_0, у которой наименованиями строк являются все рассматриваемые альтернативы, а наименованиями столбцов — критерии K_i. При этом результирующая матрица имеет вид

$A_0 =$

	K_1	K_2	...	K_n
A_1				
A_2	W_1^A	0	...	0
...				
A_m				
A'_1				
A'_2	0	W_2^A	...	0
...				
A'_r				
A''_1				
A''_2	0	0	...	W_n^A
...				
A''_p				

Шаг 6. Определяют результирующий нормированный вектор приоритетов W_0^A всех рассматриваемых альтернатив относительно фокуса иерархии K_0 на основании выражения

$$W_0^A = [A_0][S_0][L_0]\bar{X}_0[B_0].$$

Достоинством метода является нацеленность на сравнение реальных альтернатив. Метод может применяться и в случаях, когда эксперты или ЛПР не могут дать абсолютные оценки альтернатив по критериям, а пользуются более слабыми сравнительными измерениями.

Недостатки метода неоднократно обсуждались в статьях различных авторов. Весьма существенной проблемой, на взгляд многих ученых, является необоснованный переход к числам при проведении измерений, оторванность метода объединения оценок от предпочтений ЛПР.

5.4. Методы принятия решений, основанные на исследовании операций

5.4.1. Отличительные черты подхода исследования операций

Модели, описывающие поведение людей, активно используются в исследовании операций. Под исследованием операций будем понимать применение математических, количественных методов для обоснования решений во всех областях целенаправленной человеческой деятельности.

Основными этапами решения любой задачи в исследовании операций являются:

- построение модели;
- выбор критерия оптимальности;
- нахождение оптимального решения.

Для подхода исследования операций характерны следующие особенности.

Используемые модели носят объективный характер. Построение моделей рассматривается в рамках исследования операций как средство отражения объективно существующей реальности. Когда модель, правильно отражающая действительность, найдена, критерий оптимальности установлен, оптимальное решение может быть получено единственно возможным образом. Другими словами, опираясь на одни и те же данные, различные специалисты должны получать одинаковые результаты. Это требование определяет, что деятельность людей, описываемая моделью, подчинена требованиям целесообразности.

Руководитель получает научно обоснованное решение. По заказу руководителя аналитик исследует организацию, внешнюю среду и пытается построить адекватную модель. В этой работе сам ЛПР чаще всего не нужен. В описании многочисленных случаев применения методов исследования операций подчеркивается, что группа аналитиков самостоятельно находит удачное решение. Конечно, иногда руководитель дает дополнительную информацию, но его роль не отличается от роли любого сотрудника организации. Можно сказать, что руководитель дает заказ и получает готовое решение. Все остальное делают специалисты-аналитики по исследованию операций. В общем случае заказ руководителя может быть сформулирован в следующем виде: найти оптимальное, единственно верное и научно обоснованное решение. Давая такой заказ, руководитель находится в достаточно удобном положении: он полагается на силу научного подхода.

Существует объективный критерий успехов в применении методов исследования операций. Если проблема, требующая решения, ясна и критерий определен, то аналитический метод сразу показывает, насколько новое решение лучше старого. Оптимальное решение проблемы бессмысленно оспаривать.

5.4.2. Динамическое программирование

Динамическое программирование есть особый метод оптимизации решений, специально приспособленный к так называемым «многошаговым», или «многоэтапным» операциям.

Постановка задачи

Представим себе некоторую операцию Q, распадающуюся на ряд последовательных шагов; например, деятельность предприятия в течении нескольких хозяйственных лет; поэтапное планирование инвестиций; управление производственными мощностями в течение длительного срока, или же преодоление группой самолетов нескольких полос противовоздушной обороны; или же распределения весов многоступенчатой ракеты между ее ступенями с целью оптимизации скорости. Некоторые операции расчленяются на шаги естественно; в некоторых членение приходится вводить искусственно: скажем, процесс наведения ракеты на цель можно условно разбить на этапы, каждый из которых занимает какое-то время Δt.

Рассмотрим управляемый процесс. Предположим, что управление можно разбить на n шагов, т.е. решение принимается последовательно на каждом шаге, а управление, переводящее систему из начального состояния в конечное, представляет собой совокупность n пошаговых управлений. В результате управления система переходит из состояния x_0 в x_n.

Обозначим через $u_k \in U_k$ управление на k-м шаге ($k = 1, 2, ..., n$). U_k — множество допустимых управлений на k-м шаге.

Пусть $u = (u_1, u_2, ..., u_n)$ — управление, переводящее систему из состояния x_0 в состояние x_n. Обозначим через x_k состояние системы после k-го шага управления. Получаем последовательность состояний x_0, $x_1, ... x_{k-1}, x_k, x_{k+1}, ..., x_n$ (рис. 5.18).

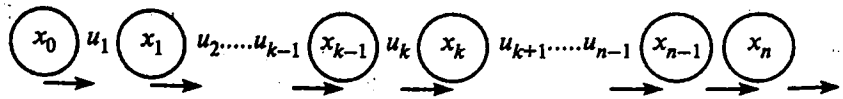


Рис. 5.18. Переход системы из одного состояния в другое в результате управляющих сигналов

Показатель эффективности рассматриваемой управляемой операции зависит от начального состояния и управления:

$$Z = F(x_0, u), \tag{5.1}$$

где $u \in U$ — множество возможных управлений.

Сделаем несколько предположений.

1. Состояние x_k системы на k-м шаге зависит только от предшествующего состояния x_{k-1} и управления на k-м шаге u_k и не зависит от предшествующих состояний и управлений (свойство отсутствия последействия):

$$x_k = \varphi_k(x_{k-1}, u_k),\ k = \overline{1, n} \text{ уравнения состояний;} \tag{5.2}$$

φ_k — оператор перехода.

2. Целевая функция (5.1) является аддитивной от показателя эффективности каждого шага, т.е. выигрыш за всю операцию складывается из выигрышей на отдельных шагах:

$$Z = F(x_0, u) = \sum_{k=1}^{n} f_k(x_{k-1}, u_k), \tag{5.3}$$

где $f_k(x_{k-1}, u_k) = Z_k$ — показатель эффективности шага k. (5.4)

Общая постановка задачи ДП. Определить такое допустимое управление $u \in U$, переводящее систему из состояния x_0 в состояние x_n, при котором целевая функция (5.3) принимает максимальное значение.

Принцип решения задач динамического программирования

Любую многошаговую задачу можно решать по-разному: либо искать сразу все элементы решения на всех шагах, либо же строить оптимальное управление шаг за шагом, на каждом этапе расчета оптимизируя только один шаг. Обычно второй способ оказывается проще, чем первый, особенно при большом числе шагов.

Такая идея постепенной, пошаговой оптимизации и лежит в основе метода динамического программирования. Оптимизация одного шага, как правило, проще оптимизации всего процесса: лучше, оказывается, много раз решить сравнительно простую задачу, чем один раз — сложную.

С первого взгляда идея может показаться довольно тривиальной. В самом деле, чего, казалось бы, проще: если трудно оптимизировать операцию в целом, разбить ее на ряд шагов. Каждый шаг будет отдельной, маленькой операцией, оптимизировать которую уже нетрудно. Надо выбрать на этом шаге такое управление, чтобы эффективность этого шага была максимальна. Не так ли?

Нет! Принцип динамического программирования отнюдь не предполагает, что каждый шаг оптимизируется отдельно, независимо от других. Напротив, шаговое управление должно выбираться дальновидно, с учетом всех его последствий в будущем. Что толку выбрать на данном шаге управление, при котором эффективность этого шага максимальна, если этот шаг лишит нас возможности хорошо выиграть на последующих шагах?

Пусть, например, планируется работа группы промышленных предприятий, из которых часть занята выпуском предметов потребления, а остальные производят для них машины. Задача операции — получить за n лет максимальный объем выпуска предметов потребления. Допустим, планируются капиталовложения на первый год. Исходя из узких интересов этого шага, мы должны были бы все наличные средства вложить в производство предметов потребления. Но правильно ли будет такое решение с позиции эффективности операции в целом? Очевидно, нет. Это решение недальновидное. Имея в виду будущее, надо выделить какую-то часть средств и на производство машин. От этого объем продукции за первый год, конечно, уменьшится, зато будут созданы условия для его увеличения в последующие годы.

Планируя многошаговую операцию, надо выбирать управление на каждом шаге с учетом всех его будущих последствий на еще предстоя-

щих шагах. Управление на i-м шаге выбирается не так, чтобы выигрыш именно на данном шаге был максимален, а так, чтобы была максимальна сумма выигрышей на всех оставшихся до конца шагах плюс данный.

Принцип динамического программирования не предполагает, что каждый шаг оптимизируется отдельно, независимо от других. Напротив, шаговое управление должно выбираться дальновидно, с учетом всех его последствий в будущем.

Однако из этого правила есть исключение. Среди всех шагов есть один, который может планироваться попросту, без оглядки на будущее. Какой это шаг? Очевидно, последний! Этот шаг, единственный из всех, можно планировать так, чтобы он сам, как таковой, принес наибольшую выгоду.

Поэтому процесс динамического программирования обычно разворачивается от конца к началу: прежде всего планируется последний, n-й шаг. А как его спланировать, если неизвестно, чем закончился предпоследний?

Планируя последний шаг, нужно сделать разные предположения о том, чем кончился предпоследний, $(n-1)$-й шаг, и для каждого из этих предположений найти условное оптимальное управление на n-м шаге. «Условное» потому, что оно выбирается исходя из условия, что предпоследний шаг кончился определенным образом.

Предположим, что это сделано, и для каждого их возможных исходов предпоследнего шага известно условное оптимальное управление и соответствующий ему условный оптимальный выигрыш на n-м шаге. Теперь можно оптимизировать управление на предпоследнем, $(n-1)$-м шаге. Снова сделаем все возможные предположения о том, чем кончился предыдущий, $(n-2)$-й шаг, и для каждого из этих предположений найдем такое управление на $(n-1)$-м шаге, при котором выигрыш за последние два шага максимален. Так найдем для каждого исхода $(n-2)$-го шага условное оптимальное управление на $(n-1)$-м шаге и условный оптимальный выигрыш на двух последних шагах. Далее, «пятясь» назад, оптимизируем управление на $(n-2)$-м шаге и т.д., пока не дойдем да первого.

Предположим, что все условные оптимальные управления и условные оптимальные выигрыши за весь «хвост» процесса известны. Это значит: известно, что надо делать, как управлять на данном шаге и что мы за это получим на «хвосте», в каком бы состоянии ни был процесс к началу шага. Теперь можно построить уже не условно оптимальное, а просто оптимальное управление u^* и найти не условно оптимальный, а просто оптимальный выигрыш Z^*.

В самом деле, пусть известно, в каком состоянии x_0 была управляемая система в начале первого шага. Тогда можно выбрать оптимальное управление u_1^* на первом шаге. Применив его, изменим состояние системы на некоторое новое x_1^*; в этом состоянии мы подошли ко второму шагу. Тогда тоже известно уловное оптимальное управление u_2^*, которое к концу второго шага переводит систему в состояние x_2^*, и т.д. Что касается оптимального выигрыша Z^* за всю операцию, то он уже известен: ведь именно на основе его максимальности выбирали управление на первом шаге.

Таким образом, в процессе оптимизации управления методом динамического программирования многошаговый процесс «проходится» дважды: первый раз — от конца к началу, в результате чего находят условные оптимальные управления и условные оптимальные выигрыши за оставшийся «хвост» процесса; второй раз — от начала к концу, когда остается только «прочитать» уже готовое управления u^*, состоящее из оптимальных шаговых управлений $u_1^2, u_2^*, \ldots, u_n^*$.

Первый этап — условная оптимизации — несравненно сложнее второго. Второй этап почти не требует дополнительных вычислений.

Принцип оптимальности Беллмана. Уравнения Беллмана

Предположим, что задача

$$Z = F(x_0, u) = \sum_{k=1}^{n} f_k(x_{k-1}, u_k) \to \max,$$

$$x_k = \varphi_k(x_{k-1}, u_k),\ k = \overline{1, n},$$

$$u_k \in U_k,\ k = \overline{1, n},$$

$$x_k \in X_k,\ k = \overline{0, n}$$

имеет решение.

Тогда справедлив *принцип оптимальности Беллмана*: оптимальное управление $u^* = (u_1^*, u_2^*, \ldots, u_n^*)$ обладает тем свойством, что каковы бы ни были состояния системы x_{k-1}^* на любом шаге и управление u_k^*, принимаемое в этом состоянии, последующие управляющие решения $u_{k+1}^*, \ldots, u_n^*$ должны составлять оптимальную стратегию относительно состояния x_k^*, полученного в результате управляющего решения u_k^*, т.е. состояния, к которому придет система в конце данного шага.

Другими словами: управление на каждом шаге необходимо выбирать так, чтобы оптимальной была сумма выигрышей на всех оставшихся до конца процесса шагах, включая выигрыш на данном шаге.

На основании принципа оптимальности Беллмана можно получить основное уравнение динамического программирования, или уравнение Беллмана.

Рассмотрим последовательность задач, используя принцип оптимальности. На каждом шаге любого состояния системы x_{k-1} управление u_k нужно выбирать «с оглядкой», так как этот выбор влияет на последующее состояние x_k и на дальнейший процесс управления, зависящий от x_k. Это следует из принципа оптимальности.

Как отмечалось ранее, среди всех шагов есть одно исключение, он может планироваться попросту, без оглядки на будущее — это последний шаг. Данный шаг — единственный, который можно планировать так, чтобы он сам, как таковой, принес наибольшую выгоду.

Рассмотрим n-й шаг: x_{n-1} — состояние системы к началу n-го шага, x_n — конечное состояние, u_n — управление на шаге n, а $f_n(x_{n-1}, u_n)$ — целевая функция шага n.

Согласно принципу оптимальности u_n нужно выбирать так, чтобы для любых состояний x_{n-1} получить максимум целевой функции на этом шаге.

Обозначим через $Z_n^*(x_{n-1})$ максимум показателя эффективности шага n при условии, что к началу последнего шага система была в произвольном состоянии x_{n-1}, а на последнем шаге управление было оптимальным.

$$Z_n^*(x_{n-1}) = \max_{u_n} f_n(x_{n-1}, u_n). \qquad (5.5)$$

Управление u_n, при котором достигается максимум (5.5) также зависит от x_{n-1}, называется условным оптимальным управлением шага n и обозначается $u_n^*(x_{n-1})$.

Решив задачу (5.5), найдем для всех возможных состояний x_{n-1} две функции: $u_n^*(x_{n-1})$ и $Z_n^*(x_{n-1})$.

Рассмотрим двухшаговую задачу: присоединим к n-му шагу $(n-1)$-й (рис. 5.19).

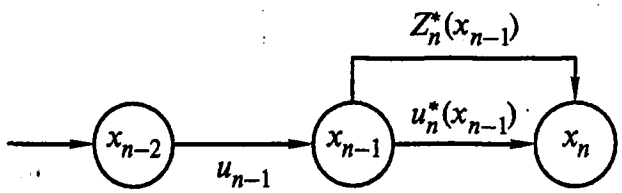


Рис. 5.19. Оптимальное управление на двух последних шагах

Для любых состояний x_{n-2}, произвольных управлений u_{n-1} и оптимального управления на шаге n значение целевой функции на двух последних шагах равно

$$f_{n-1}(x_{n-2}, u_{n-1}) + Z_n^*(x_{n-1}). \qquad (5.6)$$

Согласно принципу оптимальности для любых состояний x_{n-2} управление нужно выбирать так, чтобы оно вместе с оптимальным управлением на последнем шаге приводило бы к максимальному эффекту на двух последних шагах. Следовательно, необходимо искать максимум (6) по всем допустимым u_{n-1}.

$$Z_{n-1}^*(x_{n-2}) = \max_{u_{n-1}} \{f_{n-1}(x_{n-2}, u_{n-1}) + Z_n^*(x_{n-1})\}. \qquad (5.7)$$

В результате максимизации получаем две функции: $u_{n-1}^*(x_{n-2})$ и $Z_{n-1}^*(x_{n-2})$.

Далее рассматривается трехшаговая задача: к двум последним добавляется $(n-2)$-й и т.д.

Обозначим через $Z_k^*(x_{k-1})$ условный максимум целевой функции, полученный при оптимальном управлении на $n-k+1$ шагах, начиная с k-го до конца, при условии, что к началу k-го шага система находится в состоянии x_{k-1}.

$$Z_k^*(x_{k-1}) = \max_{\{u_k, \ldots, u_n\}} \sum_{i=k}^{n} f_i(x_{i-1}, u_i),$$

$$Z_{k+1}^*(x_k) = \max_{\{u_{k+1}, \ldots, u_n\}} \sum_{i=k+1}^{n} f_i(x_{i-1}, u_i).$$

Целевая функция на $n-k$ последних шагах при произвольном управлении u_k на k-м шаге и оптимальном управлении на последующих $n-k$ шагах равна $f_k(x_{k-1}, u_k) + Z_{k+1}^*(x_k)$.

Согласно принципу оптимальности u_k выбирается из условия максимума этой суммы, т.е.

$$Z_k^*(x_{k-1}) = \max_{u_k} \{f_k(x_{k-1}, u_k) + Z_{k+1}^*(\varphi(x_{k-1}, u_k))\}, k = \overline{n-1, 1}. \qquad (5.8)$$

Уравнения (5.8) называются *уравнениями Беллмана*. Это рекуррентные соотношения, позволяющие найти предыдущие значения функции, зная последующие. Процесс решения уравнений (5.5) и (5.8) называется условной оптимизацией.

В результате условной оптимизации получаем две последовательности: $Z_n^*(x_{n-1}), Z_{n-1}^*(x_{n-2}), \ldots, Z_1^*(x_0)$ и $u_n^*(x_{n-1}), u_{n-1}^*(x_{n-2}), \ldots, u_1^*(x_0)$.

Используя эти последовательности, можно найти решение задачи динамического программирования при данных n и x_0: $Z_{\max} = Z_1^*(x_0)$,

$$u_1^* = u_1^*(x_0) \to x_1^* = \varphi_1(x_0, u_1^*) \to u_2^* = u_2^*(x_1^*) \to \ldots \to u_n^* = u_n^*(u_{n-1}^*).$$

Отметим в заключение, что рассмотренные здесь методы принятия решений могут активно использоваться при аудите информационной безопасности, что является сегодня одним из наиболее эффективных инструментов для получения независимой и объективной оценки текущего уровня защищенности предприятий от угроз информационной безопасности. Кроме того, результаты аудита используются для формирования стратегии развития системы защиты информации в организации. Необходимо помнить, что аудит безопасности не является однократной процедурой, а должен проводиться на регулярной основе. Только в этом случае аудит будет приносить реальную пользу и способствовать повышению уровня ИБ компании.

В приложении 5.1 рассматриваются конкретные примеры использования методов принятия решений в разработке комплексной системы защиты информации.

Задания к главе 5

Задание 1. Является ли матрица A матрицей парных сравнений? Для матрицы A найти приближенное $\overline{W}$ и точное W значения главного собственного вектора. Оценить погрешность $\Delta\overline{W} = |W - \overline{W}|$. Определить, является ли матрица парных сравнений согласованной.

1.1. $A = \begin{pmatrix} 1 & & & \\ 1 & & 1 & \\ 1 & 1 & & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$

1.2. $A = \begin{pmatrix} 1 & 1 & & & \\ & & 1 & 1 & 2 \\ 1 & & & 1 & \\ 1 & 1 & 2 & 1 & 1 \end{pmatrix}$

1.3. $A = \begin{pmatrix} 1 & 3 & & & \\ 1 & 3 & 1 & 1 & 2 \\ 1 & & & 1 & 3 \\ 1 & 1 & 2 & 1 & 3 & 1 \end{pmatrix}$

1.4. $A = \begin{pmatrix} 1 & & & & \\ 1 & & 1 & 3 & 3 \\ 1 & & 1 & 3 & 1 & 1 & 2 \\ 1 & & 1 & 3 & 2 & 1 \end{pmatrix}$

1.5. $A = \begin{pmatrix} 1 & & & \\ 1 & & 1 & \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$

1.6. $A = \begin{pmatrix} 1 & & & 1 & \\ 1 & & 1 & 6 & \\ 1 & 1 & 6 & 1 & \\ 1 & 1 & 1 & & 1 \end{pmatrix}$

1.7. $A = \begin{pmatrix} 1 & & & 6 & 1 \\ 1 & & 1 & & \\ 1 & 6 & 1 & 1 & \\ 1 & 1 & 1 & & 1 \end{pmatrix}$

1.8. $A = \begin{pmatrix} 1 & 6 & 1 & & 8 \\ 1 & 6 & 1 & 1 & 8 \\ & & 8 & 1 & \\ 1 & 8 & 1 & 1 & 1 \end{pmatrix}$

1.9. $A = \begin{pmatrix} 1 & & & 1 & 9 & 8 \\ 1 & & 1 & 1 & & \\ 9 & & 1 & 1 & & \\ 1 & 8 & 1 & 1 & & 1 \end{pmatrix}$

1.10. $A = \begin{pmatrix} 1 & & & 6 & 8 \\ 1 & & 1 & 8 & 1 & 7 \\ 1 & 6 & 1 & 8 & 1 & \\ 1 & 8 & 7 & 1 & & 1 \end{pmatrix}$

Задание 2. Преобразовать матрицу парных сравнений A из задания 1 таким образом, чтобы она стала абсолютно согласованной (ОС = 0). При этом:

а) оставить первую строку матрицы без изменений;

б) оставить последнюю строку матрицы без изменения.

Задание 3. Найти агрегированную оценку двух экспертов, если матрица парных сравнений первого эксперта имеет вид, представленный в задании 1, а матрица парных сравнений второго имеет вид:

3.1. $A = \begin{pmatrix} 1 & 3 & 6 & 8 \\ 1 & 3 & 1 & 5 \\ 1 & 6 & 1 & 3 \\ 1 & 8 & 1 & 5 & 1 & 3 & 1 \end{pmatrix}$

3.2. $A = \begin{pmatrix} 1 & & & 7 & 8 \\ 1 & & 1 & 1 & 3 & 2 \\ 1 & 7 & 3 & & 1 & 2 \\ 1 & 8 & 1 & 2 & 1 & 2 & 1 \end{pmatrix}$

3.3. $A = \begin{pmatrix} 1 & 3 & 2 & & 8 \\ 1 & 3 & 1 & 1 & & 1 & 2 \\ 1 & 2 & & 1 & & 3 \\ 1 & 8 & 2 & 1 & 3 & & 1 \end{pmatrix}$

3.4. $A = \begin{pmatrix} 1 & 6 & 4 & 8 \\ 1 & 6 & 1 & 3 & 5 \\ 1 & 4 & 1 & 3 & 1 & 4 \\ 1 & 8 & 1 & 5 & 1 & 4 & 1 \end{pmatrix}$

3.5. $A=\begin{pmatrix} & & 3 & 5 \\ & & 3 & \\ 3 & 3 & & 3 \\ 5 & & 3 & \end{pmatrix}$ 3.6. $A=\begin{pmatrix} & & & 6 \\ & & 5 & \\ & 5 & & 3 \\ 6 & & 3 & \end{pmatrix}$

3.7. $A=\begin{pmatrix} & & 6 & 5 \\ & & & \\ 6 & & & 3 \\ 5 & & 3 & \end{pmatrix}$ 3.8. $A=\begin{pmatrix} & 7 & & 8 \\ 7 & & 8 & 3 \\ & 8 & & 5 \\ 8 & 3 & 5 & \end{pmatrix}$

3.9. $A=\begin{pmatrix} & & 6 & 8 \\ & & 8 & 7 \\ 6 & 8 & & 3 \\ 8 & 7 & 3 & \end{pmatrix}$ 3.10. $A=\begin{pmatrix} 1 & & & 1 & 9 & 8 \\ 1 & & 1 & & 1 & \\ 9 & & 1 & & 1 & 3 \\ 1 & 8 & 1 & & 1 & 3 & 1 \end{pmatrix}$

Задание 4. Найти агрегированную оценку экспертов из задания 3 при условии, что квалификация первого эксперта имеет вес 3 (первый эксперт более квалифицированный), а второго — 1.

Задание 5. Для иерархической структуры, представленной на рис. 5.5, определить приоритет провайдера, выполнив иерархический синтез. Матрица сравнения критериев относительно цели имеет вид:

5.1. $=\begin{pmatrix} 1 & & & 6 & & 7 \\ 1 & & 1 & 3 & & \\ 1 & 6 & 1 & 3 & 1 & & 1 \\ 1 & & 1 & & 1 & 1 & 1 & 3 \\ 1 & 7 & 1 & & 1 & 3 & 1 \end{pmatrix}$ 5.2. $=\begin{pmatrix} 1 & & 5 & & 8 & 2 & 7 \\ 1 & 8 & & 1 & 3 & & 1 & 2 \\ 1 & 8 & 1 & 3 & 1 & 2 & 1 \\ 1 & 2 & 1 & & 1 & 2 & 1 & 1 & 3 \\ 1 & 7 & & 2 & 1 & 3 & 1 \end{pmatrix}$

5.3. $=\begin{pmatrix} 1 & & & 2 & 2 & 7 \\ 1 & & 1 & 3 & 2 & 2 \\ 1 & 2 & 1 & 3 & 1 & 2 & 1 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 \\ 1 & 7 & 1 & 2 & 1 & 1 & 1 \end{pmatrix}$ 5.4. $=\begin{pmatrix} 1 & & 5 & & 1 & 2 & 3 \\ 1 & 8 & & 1 & 1 & 4 & 4 & 1 & 2 \\ & 1 & & 4 & & 1 & 2 & 1 \\ 1 & 2 & 1 & 4 & 1 & 2 & 1 & 1 & 3 \\ 1 & 3 & & 2 & 1 & 3 & 1 \end{pmatrix}$

5.5. $A=\begin{pmatrix} & & & & & \\ & & & & & \\ & & & & 5 & \\ & & & 5 & & \\ & & & & & \end{pmatrix}$ 5.6. $A=\begin{pmatrix} & & 5 & & & \\ & 5 & & & & \\ & & & & & \\ & & & & & \\ & & & & & \end{pmatrix}$

5.7. $A=\begin{pmatrix} & & 6 & & 7 \\ & & 5 & & 5 \\ 6 & 5 & & & \\ & & & & 6 \\ 7 & 5 & & 6 & \end{pmatrix}$ 5.8. $A=\begin{pmatrix} & & 5 & 8 & & \\ & 8 & & & & \\ & 8 & & & & 7 \\ & & & 7 & & \\ & & & & & \end{pmatrix}$

5.9. $A=\begin{pmatrix} & & & & & 5 \\ & & & & & \\ & & & & & \\ & & & & & \\ 5 & & & & & \end{pmatrix}$ 5.10. $A=\begin{pmatrix} 1 & & 5 & 1 & & & 7 \\ 1 & 8 & 1 & & & 1 & 1 \\ & & 1 & & 1 & & 1 \\ 1 & & & 1 & & 1 & 8 \\ 1 & 7 & 1 & & 1 & 1 & 8 & 1 \end{pmatrix}$

Матрицы сравнения альтернатив относительно критериев необходимо принять из предыдущих заданий по следующему правилу:

Задание	*Тарифы*	*Скорость*	*Доступность*	*Оплата*	*Услуги*
5.1	1.1	1.3	1.5	1.7	3.1
5.2	1.2	1.4	1.4	1.8	3.3
5.3	1.3	1.5	1.3	1.9	3.4
5.4	1.4	1.6	1.2	1.10	3.5
5.5	1.5	1.7	1.1	1.1	3.6
5.6	1.6	1.8	1.6	1.2	3.7
5.7	1.7	1.9	1.7	1.3	3.8
5.8	1.8	1.10	1.8	1.4	3.9
5.9	1.9	1.1	1.9	1.5	3.10
5.10	1.10	1.2	1.10	1.6	

Задание 6. Построить трехуровневую иерархическую структуру (пример — на рис. 5.14). Используя мнения двух экспертов, произвести синтез иерархии, оценить ее согласованность, сделать соответствующие выводы.

ПРИЛОЖЕНИЕ 5.1

Использование методов принятия решений в разработке комплексной системы защиты информации

Разработка и эксплуатация сложных ИС, каковыми являются *комплексные системы защиты информации* (КСЗИ) выявили проблемы, которые можно решить лишь на основании комплексной оценки и учета различных по своей природе факторов, разнородных связей, внешних условий и прочих показателей. Поэтому все более важным в современных быстро изменяющихся условиях становится вопрос качественного и эффективного *принятия решений* в различных ситуациях.

Напомним, что под термином «принятие решений» подразумевается действие над множеством альтернатив (систем, ситуаций, факторов и т.д.), в результате которого получается подмножество выбранных альтернатив.

Постановка задачи и применение методов принятия решений зависят от многих факторов; отметим основные из них:

- множество альтернатив может быть конечным или бесконечным;
- оценка может осуществляться по одному или нескольким критериям, которые могут иметь как количественный, так и качественный характер;
- алгоритм выбора может быть однократным или адаптивным и повторяющимся;
- последствия выбора могут быть точно известны или носить вероятностный характер.

Генерирование множества альтернатив с применением экспертных методов

При исследовании сложных информационных систем, при генерировании альтернатив наиболее часто прибегают к услугам экспертов — лиц, обладающих достаточным опытом и знаниями в рассматриваемой предметной области. Заметим, что аппарат обработки экспертных мнений достаточно хорошо проработан и используется во многих практических областях.

Организация работы экспертов включает следующие основные этапы:

- формулировка цели экспертного опроса;
- создание рабочей группы;
- разработка сценария проведения сбора информации и выбор методов обработки мнений;
- подбор экспертов в соответствии с целями опроса;
- проведение сбора экспертной информации;
- анализ экспертной информации;
- интерпретация полученных результатов и подготовка заключения для ЛПР.

Можно сказать, что методы обработки мнений экспертов позволяют структурировать множество альтернатив при различных суждениях экспертов. В ходе формирования набора критериев можно учитывать мнение каждого эксперта, а затем объединить это множество в одно мнение. Для оценки сравнительной значимости критериев применяют компромиссное ранжирование. Каждый эксперт дает свое ранжирование критериев по важности, и на основе индивидуального ранжирования строится, например, *обобщенная матрица сравнений с использованием строчных сумм*.

Метод строчных сумм, предполагающий построение матрицы сравнений, заключается в следующем.

1. Составляется матрица, где наименования строк и столбцов соответствуют именам альтернатив.

2. На пересечении строки и столбца выставляют числа по следующему правилу:

1, если альтернатива с именем строки лучше альтернативы с именем столбца;

0, если альтернатива с именем строки хуже альтернативы с именем столбца;

0,5, если альтернативы равноценны.

Главную диагональ оставляют незаполненной.

3. После заполнения рассчитывают суммы строк.

4. Строится ранжировка альтернатив:

ранг 1 присваивается альтернативе, имеющей максимальную строчную сумму;

ранг 2 — альтернативе, имеющей следующую по величине сумму, и т.д.

Таким образом получается обобщенное мнение экспертов.

Пример. На первом этапе формируются критерии, на основании которых производится сравнение предложенных проектов КСЗИ.

В качестве критериев оценки сравниваемых проектов КСЗИ экспертами были выдвинуты следующие:

- эффективность КСЗИ;
- минимизация расходов на КСЗИ;
- комплексность технологий и решений;
- увеличение срока службы инфраструктуры;
- снижение эксплуатационных расходов.

Обобщенная матрица сравнений с использованием строчных сумм для рассматриваемого примера приведена в табл. П5.1.

Таблица П5.1

Попарное сравнение критериев

Критерий	Эффективность КСЗИ	Минимизация расходов на КСЗИ	Комплексность технологий и решений	Увеличение срока службы инфраструктуры	Снижение эксплуатационных расходов	Сумма строк	Ранг
Эффективность КСЗИ		0	0,5	0,5	0,5	1,5	3
Минимизация расходов на КСЗИ	1		1	1	0,5	3,5	1
Комплексность технологий и решений	0,5	0		0,5	0,5	1,5	3
Увеличение срока службы инфраструктуры	0,5	0	0,5		0,5	1,5	3
Снижение эксплуатационных расходов	0,5	0,5	0,5	0,5		2	2

Морфологический анализ

Основная идея морфологического анализа — систематически находить все мыслимые варианты решения проблемы или реализации системы путем комбинирования выделенных элементов или признаков. Морфологический подход разработан и применен впервые швейцарским астрономом Ф. Цвикки и первоначально был известен как *метод Цвикки*.

Наибольшее распространение получил метод, представляющий собой развитие подхода Цвикки и известный под названием *метод морфологической матрицы*. Идея его состоит в том, чтобы определить все

мыслимые параметры, от которых может зависеть решение проблемы, и представить их в виде матриц-столбцов, а затем определить в морфологической матрице все возможные сочетания параметров по одному из каждой строки. Полученные таким образом варианты могут сноваться подвергаться оценке и анализу в целях выбора наилучшего.

Построение и исследование по методу морфологической матрицы проводится в пять этапов:

1. Точная формулировка поставленной проблемы, цели исследования, существующих ограничений.
2. Выделение показателей P_i, от которых зависит решение проблемы.
3. Сопоставление показателю P_i его значений p_{ik} и сведение этих значений в морфологическую матрицу.

Набор значений различных показателей (по одному из каждой строки) представляет собой возможный вариант решения проблемы (например, p_{11}, p_{23}, ..., p_{kn}). Общее число вариантов, содержащихся в морфологической матрице, равно $N = k_1, k_2, ..., k_n$, где k_1, k_2, ..., k_n — число значений i-го показателя.

4. Оценка всех имеющихся в морфологической матрице вариантов.
5. Выбор из морфологической матрицы наиболее привлекательного варианта решения проблемы.

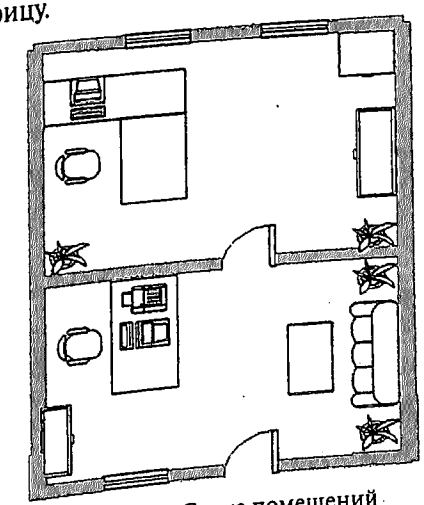


Рис. П5.1. Схема помещений организации

Пример. Рассмотрим объект, который представляет собой помещение из двух комнат: приемная и кабинет директора (рис. П5.1). Организация, расположенная в данном помещении, занимается сбором и анализом коммерческой информации. Следовательно, возникает проблема защиты коммерческой и служебной информации.

Для оптимизации принятия решения будем использовать морфологический метод синтеза альтернатив и принятия рациональных решений.

Анализ угроз

При анализе информационной безопасности обязательным условием является построение полного множества угроз. Каждая конкрет-

ная угроза должна рассматриваться в следующем порядке: чему она угрожает, как обнаруживается, частота ее проявления, последствия, как предотвращается.

В нашем случае множество угроз $У = \{У_1, У_2, ..., У_n\}$ следующее:

1) съем за счет побочных электромагнитных излучений и наводок (ПЭМИН);

2) съем с телефонной линии;

3) съем с окон с использованием лазера;

4) несанкционированный доступ (НСД) с помощью проникновения злоумышленника в помещение;

5) утечки за счет персонала;

6) съем с помощью закладок и диктофонов;

7) потеря информации из-за вирусов;

8) пожар.

Построение морфологической матрицы

В табл. П5.2 приведена морфологическая матрица, соответствующая обследуемому объекту.

Таблица П5.2

Морфологическая матрица

Функциональная подсистема	Элементарные альтернативы		
Защита окон	A_{11}	A_{12}	A_{13}
Защита от ПЭМИН	A_{21}	A_{22}	
Защита телефонной линии	A_{31}	A_{32}	A_{33}
Защита от НСД персонала	A_{41}	A_{42}	A_{43}
Защита от НСД злоумышленника	A_{51}	A_{52}	A_{53}
Съем с помощью закладок и диктофонов	A_{61}	A_{62}	A_{63}
Защита от вирусов	A_{71}	A_{72}	
Защита от пожаров	A_{81}	A_{82}	

Обозначения альтернативных вариантов защиты в таблице следующие:

A_{11} — установка решеток;

A_{12} — установка жалюзи;

A_{13} — установка генератора виброакустических помех;

A_{21} — экранирование;

A_{22} — снижение уровней информационных ПЭМИН и повышение уровней помех;

A_{31} — защита телефонного аппарата и линий фильтрами, диодами, конденсаторами, подключенными в цепь;

A_{32} — изменение напряжения в телефонной линии при разговоре;

A_{33} — генерация высокочастотных помех в телефонной линии;

A_{41} — парольная защита;

A_{42} — система шифрования;

A_{43} — использование сейфа;

A_{51} — система контроля доступа;

A_{52} — система видеонаблюдения;

A_{53} — охрана периметра;

A_{61} — использование принципа сравнения уровня сигнала на антенне внутри контролируемой зоны и вне ее;

A_{62} — постоянный анализ эфира и фиксация вновь появившихся источников излучения;

A_{63} — устройство обнаружения диктофонов;

A_{71} — использование антивирусных программ;

A_{72} — использование лицензионного программного обеспечения;

A_{81} — использование охранно-пожарной сигнализации;

A_{82} — средства пожарной безопасности.

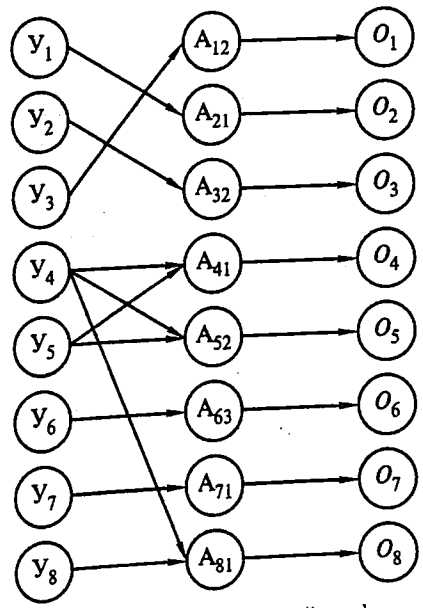


Рис. П5.2. Трехдольный граф для одного из вариантов защиты

Правило генерации вариантов исследуемых систем таково, что каждый целостный вариант отличается от любого другого варианта рассматриваемого морфологического множества хотя бы одной альтернативой.

Построение модели защиты в виде трехдольного графа

Построим модель процесса защиты рассматриваемой организации для одного целостного варианта в виде трехдольного графа, обозначив перечисленные угрозы через $У_i$, объекты — через O_i.

Оценка альтернатив с использованием критериального метода

Наиболее популярным для оценки альтернатив является *критериальный метод*, когда каждая отдельно взятая альтернатива оценивается численно и сравнение альтернатив сводится к сравнению соответствующих чисел.

Для всего множества альтернатив $X = \{x_1, x_2, x_3, ..., x_N\}$ вводится целевая функция $Z = \max f(x)$ или $Z = \min f(x)$. При практическом рассмотрении множества альтернатив выясняется, что для их оценки в большинстве случаев требуется более чем один критерий, т.е. некоторое множество $Z_i = f_i(x)$, где $i = 1, ..., N$. В большинстве случаев невозможно найти альтернативу, являющуюся предпочтительной на всем множестве критериев, в таком случае необходимо применять специальные многокритериальные способы выбора. Примером такого решения является сведение многокритериальной задачи к однокритериальной, т.е. введение суперкритерия $Z_0 = Z_0(f_i(x))$, где $i = 1, ..., N$.

Для определения вклада каждого из критериев обычно используются аддитивные (П5.1) или мультипликативные (П5.2) функции:

$$Z_0 = \sum_{i=1}^{N} \frac{P_i f_i(x)_i}{a_i}, \qquad \text{(П5.1)}$$

$$Z_0 = \prod_{i=1}^{N} \frac{f_i(x)^{P_i}}{a_i}, \qquad \text{(П5. 2)}$$

где a_i — величина, обеспечивающая нормализацию разнородных критериев;

P_i — вес (он должен принадлежать интервалу (0,1)), характеризующий вклад частного критерия в суперкритерий.

К положительным свойствам аддитивного суперкритерия следует отнести его простоту и доступность. Главный же недостаток заключается в том, что такой суперкритерий не вытекает из объективной роли частных критериев в определении качества системы и, как следствие, выступает как математический прием, лишь придающий задаче удобный вид. Кроме того, низкие оценки по одним критериям могут компенсироваться высокими по другим.

Правомочность мультипликативного суперкритерия основывается на принципе справедливой относительной компенсации: справедливым следует считать такой компромисс, при котором суммарный уровень относительного снижения значений одного или нескольких критериев не превышает суммарного уровня относительного увеличения значений

других критериев. Для мультипликативной функции в сравнении с аддитивной фактически действует правило «низкая оценка хотя бы по одному критерию влечет за собой низкое значение суперкритерия».

Выбор между аддитивной и мультипликативной свертками частных критериев определяется степенью важности абсолютных или относительных изменений значений частных критериев соответственно.

При оценивании систем, в частности информационных, выделяют две группы критериев:

— критерии качества систем;

— критерии эффективности систем.

Критерии качества обозначают свойство или совокупность существенных свойств системы, обусловливающих ее пригодность к целевому использованию. При оценивании качества системы признается целесообразным введение нескольких уровней качества. Рассмотрим их в порядке иерархической значимости.

Устойчивость: для сложных систем, какими являются КСЗИ, характерны такие формы устойчивости, как надежность, живучесть и т.д.

Помехоустойчивость, понимаемая как способность системы без искажений воспринимать и передавать информационные потоки. Помехоустойчивость характеризуется такими показателями как надежность систем связи; пропускная способность; возможность эффективного кодирования/декодирования; электромагнитная совместимость электронных средств и т.д.

Управляемость — это способность системы переходить за конечное время в требуемое состояние под влиянием управляющих воздействий. Управляемость включает такие понятия, как гибкость управления системой; оперативность; точность; производительность; инерционность и т.д.

Способность — это качество системы, определяющее ее возможности по достижению требуемого результата на основе имеющихся ресурсов в заданный период времени. Иными словами, способность — это потенциальная эффективность функционирования системы, способность получить требуемый результат при идеальном способе использования ресурсов и в отсутствие воздействий внешней среды.

Самоорганизация является наиболее сложным качеством системы. Самоорганизующаяся система способна изменять свою структуру, параметры, алгоритмы функционирования для повышения эффективности. Принципиально важным свойством этого уровня являются свобода выбора решений, адаптируемость, самообучаемость и способность к распознаванию ситуаций.

При исследовании качества системы для простых систем часто ограничиваются исследованием одного критерия, например устойчивости. Для сложных систем, какими являются КСЗИ, выбор критериев качества зависит от сложности системы; целей исследования; наличия информации; условий применения системы.

Критерии эффективности систем соответствуют комплексному операционному свойству процесса функционирования системы, характеризующему его приспособленность к достижению цели операции (выполнению задачи системы). К этим критериям относятся следующие:

- *результативность операций*, которая обусловливается получаемым целевым эффектом, ради которого функционирует система;
- *ресурсоемкость*, характеризующаяся наличием ресурсов всех видов, используемых для получения целевого эффекта;
- *оперативность*, характеризующаяся расходом времени, необходимого для достижения цели;
- *оценка алгоритма функционирования*, являющаяся ведущей при оценке эффективности, так как наличие хорошего алгоритма функционирования системы повышает уверенность в получении требуемых результатов (это положение наиболее важно для организационно-технических систем, к которым относятся КСЗИ).

В совокупности результативность, ресурсоемкость и оперативность порождают комплексное свойство системы — эффективность как степень приспособленности системы к достижению цели.

Оценка альтернатив с использованием метода парных сравнений

Основные этапы этого метода сводятся к следующему:

- взвешивание целей и определение соответствующих им критериев;
- взвешивание и определение удельных весов критериев;
- проведение парных сравнений альтернатив по каждому критерию;
- составление финальной матрицы для оценки альтернатив и определение относительной общей ценности каждой альтернативы;
- выбор проекта с наивысшей относительной ценностью.

После проведения ранжирования методом строчных сумм, рассмотренным в предыдущем разделе, все цели E_i получат нормированные веса g_i, кроме того, для каждой i-й цели должны быть определены критерии Z_{ij}, где i — порядковый номер цели ($i = 1, ..., m$), а j — номер критерия для i-й цели ($j = 1, ..., m_i$).

В случае если для одной цели определяется более одного критерия, их также необходимо ранжировать методом строчных сумм, получить

нормированные веса c_j, после чего подсчитать суммарные веса критериев q_{ij} по формуле

$$q_{ij} = g_i c_j,$$

где $i = 1, ..., n$ — число целей;

$j = 1, ..., m_i$ — число критериев для i-й цели.

Схема целей и критериев представлена на рис. П5.3.

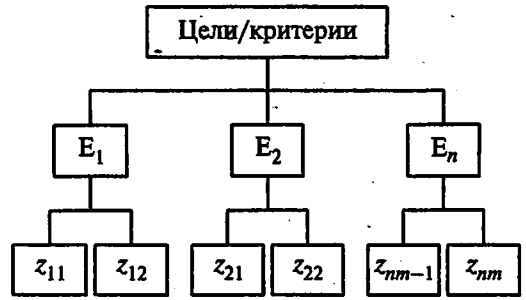


Рис. П5.3. Схема целей и критериев

На следующем этапе проводится попарное сравнение альтернативных проектов A_i по каждому критерию Z_{ij} и на основании полученных результатов строится матрица относительных предпочтений $\{P_{kn}\}$, где $k = \sum m_i$, каждый столбец которой будут представлять результаты сравнения по определенному критерию.

Вид матрицы относительных предпочтений приведен в табл. П5.3.

Таблица П5.3

Матрица относительных предпочтений

Альтернативный проект	Суммарный вес критерия			
	q_{11}	q_{12}	...	q_{nm}
A_1	P_{11}	P_{12}	...	P_{1k}
...	...	...	...	...
A_n	P_{n1}	P_{n2}	...	P_{nk}

Вид финальной матрицы для оценки альтернативных вариантов представлен в табл. П5.4. Элементы матрицы относительных предпочтений перемножаются с суммарными весами критериев, в результате суммирования полученных по каждой строке результатов, получаем финальные оценки F_i, причем большее значение оценки соответствует лучшему проекту.

Таблица П5.4

Финальная матрица оценки альтернатив

Критерий	Z_{11}	Z_{12}	...	Z_{nm}	Финальная оценка
Альтернативные проекты	Суммарные веса критериев				
	q_{11}	q_{12}	...	q_{nm}	
A_1	$P_{11}\, q_{11}$	$P_{12}\, q_{12}$	...	$P_{1k}\, q_{nm}$	F_1
...	...	...	...	...	...
A_n	$P_{n1}\, q_{11}$	$P_{n2}\, q_{12}$	...	$P_{nk}\, q_{nm}$	F_n

Полученная матрица финальных оценок используется для сравнения инновационных проектов и принятия решений об их эффективности.

Пример. Для сравнения альтернативных вариантов построения комплексной системы защиты информации выбирается цель — *Повышение эффективности комплексной системы защиты информации*. На рис. П5.4 показана схема попарного сравнения целей и критериев.

Рис. П5.4. Схема попарного сравн[illegible]ий и критериев

1. Попарное сравнение и ранжирование подцелей E_1, E_2, ..., выполняется с использованием метода строчных сумм.

2. Попарное сравнение и ранжирование критериев Z_{11}, Z_{12}, ...; Z_{21}, Z_{22}, ...; ... также осуществляется методом строчных сумм.

В качестве примера приведем попарное сравнение критериев для подцели E_1 «Совершенствование технологий эксплуатации КСЗИ», табл. П5.5.

Таблица П5.5

Попарное сравнение критериев для подцели E_1 «Совершенствование технологий эксплуатации КСЗИ»

Критерий	Z_{11}	Z_{12}	Z_{13}	Z_{14}	Z_{15}	Сумма строк	Вес критерия C_{ij}
Z_{11}		0	0,5	0,5	0,5	1,5	0,15
Z_{12}	1		1	1	0,5	3,5	0,35
Z_{13}	0,5	0		0,5	0,5	1,5	0,15
Z_{14}	0,5	0	0,5		0,5	1,5	0,15
Z_{15}	0,5	0,5	0,5	0,5		2,0	0,2
						Общая сумма 10	

Аналогичным образом получают веса подцелей g_i на множестве $E\{E_1, E_2, ...\}$.

3. Веса подцелей и критериев размещаются в сводной табл. П5.6.

Таблица П5.6

Сводная таблица весов подцелей и критериев

N_i	Подцели E_{11}, E_{12}, ...	Вес целей g_i	Критерии	Вес критерия c_{ij}	Суммарный вес критерия q_{ij}
1	Совершенствование технологии эксплуатации КСЗИ	0.1	Z_{11} Z_{12} Z_{13} Z_{14} Z_{15}	0,15 0,35 0,15 0,15 0,20	0,015 0,035 0,015 0,015 0,020
2	Внедрение новых алгоритмов функционирования системы	0,3	Z_{21} . .	. . .	. . .
...	...	...	...	...	...

4. Далее формируется матрица относительных предпочтений (см. табл. П5.3)

5. Формируется финальная матрица оценки альтернативных проектов (см. табл. П5.4).

В заключение следует отметить, что для практического применения описанных методов принятия решений при разработке КСЗИ на кафедре информационной безопасности и программной инженерии РГСУ под руководством авторов учебного пособия разработано и используется в рамках учебного процесса программное обеспечение:

MatrixAnalysis — программное обеспечение для морфологического анализа альтернатив и принятия рациональных решений при разработке КСЗИ[1];

TGP — программное обеспечение для моделирование процессов в системе защиты информации с использованием метода трехдольных графов[2].

Литература к главе 5

1. *Андрейчиков А.В., Андрейчикова О.Н.* Анализ, синтез, принятие решений в экономике. — М.: Финансы и статистика, 2000.
2. *Варфоломеев В.И., Воробьев С.Н.* Принятие управленческих решений: Учеб. пособие для вузов. — М.: КУДИЦ-ОБРАЗ, 2001.
3. *Вентцель Е.С.* Исследование операций: задачи, принципы, методология. — М.: Наука, 1988.
4. *Кремер Н.Ш., Путко Б.А., Тришин И.М. и др.* Исследование операций в экономике. — М.: ЮНИТИ, 2000.
5. *Ларичев О.И.* Теория и методы принятия решений, а также Хроника событий в Волшебных странах: Учебник. — М.: Логос, 2000.
6. *Саати Т.* Принятие решений. Метод анализа иерархий: Пер. с англ. — М.: Радио и связь, 1989.
7. *Смирнов Э.А.* Управленческие решения. — М.: ИНФРА-М, 2001.
8. *Трахтенгерц Э.А.* Компьютерная поддержка принятия решений: Научно-практич. изд. — М.: СИНТЕГ, 1998. — Серия «Информатизация России на пороге XXI века».
9. *Эддоус М., Стэнсфилд Р.* Методы принятия решений. — М.: ЮНИТИ, 1997.
10. *Ericson K.A.* The acquisition of expert performance: introduction to some of the issues// K.A. Ericson (Ed.). The road to excellence: the acquisition of expert performance in the arts and sciences, sport and games. — Hillsdale, NJ: Lawrence Erlbaum Associates, 1996.
11. *Lotov A., Bushenkov V., Kamenev G.* Feasible Goals Method Search for Smart Decisions. — Moscow, RAS, 2001.

[1] *Пыжьянова О.* Дипломный проект «Программные средства для морфологического анализа альтернативных вариантов системы защиты объекта информатизации» (руководитель Баранова Е.К.). — М., РГСУ, 2007; *Трифонов Д.* Курсовая работа «Морфологический анализ альтернативных вариантов системы защиты объекта информатизации» (руководитель Баранова Е.К.). — М., РГСУ, 2008.

[2] *Ревин А.* Дипломная работа «Моделирование процессов в системе защиты информации с использованием метода трехдольных графов» (руководитель Баранова Е.К.). — М., РГСУ, 2007.

ГЛАВА 6. ЭКОНОМИЧЕСКИЕ АСПЕКТЫ ЭФФЕКТИВНОСТИ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Методики оценки экономической эффективности системы обеспечения информационной безопасности

Очевидно, что ни один проект в современном мире не может быть принят к исполнению без экономического обоснования инвестиций в него. Сложность задач экономического анализа практически во всех областях деятельности обусловлена тем, что многие ключевые параметры экономических моделей невозможно оценить с высокой степенью достоверности, поскольку они носят вероятностный характер. Особенно это касается информационной безопасности, где формализации поддаются далеко не все параметры, а вероятностный характер носят не только потенциальные угрозы и уязвимости системы, но и стоимость ущерба от реализации этих угроз, а оценка риска может производиться не на количественном, а на качественном уровне. Трудность оценки экономической эффективности систем обеспечения ИБ связана и с такими объективными причинами, как:

- быстрое развитие информационных технологий, методов и средств, используемых как для защиты, так и для атак;
- невозможность достоверно предугадать все возможные сценарии атак на информационные системы и модели поведения атакующих;
- невозможность дать точную оценку стоимости информационных ресурсов, а также оценить последствия различных нарушений в денежном выражении[1].

Оценка экономической эффективности системы обеспечения ИБ компании зависит от следующих основных факторов:

- потребность в том или ином мероприятии по обеспечению ИБ;
- планируемые инвестиции в информационную безопасность.

[1] *Ажмухамедов И.М., Ханжина Т.Б.* Оценка экономической эффективности мер по обеспечению информационной безопасности // Вестник Астраханского государственного технического университета. Серия: Экономика. — 2011. — № 1. — С. 185–190.

Взаимосвязь факторов обусловлена возрастающим характером функции, отражающей потребность в защите информации, и ограничивающим характером инвестиций в ИБ. Первая возрастает с развитием рынка и самой компании (увеличивается число сотрудников, контрагентов, конкурентов, возрастают риски, как внутренние, так и внешние). Инвестиции же, в целях оценки экономической эффективности системы ИБ, играют роль некоего ограничителя, поскольку финансовые ресурсы компании ограничены, и вкладывать их в информационную безопасность компания готова только до определенного уровня – такого, который позволит компании достигать своей первичной цели в основном виде деятельности.

Экономическое обоснование затрат на информационную безопасность во многих методиках проводится с помощью использования совокупных показателей. Наибольшее распространение в практике по обеспечению ИБ получили следующие показатели[1]:

- *PP (Payback Period*, срок окупаемости — период времени, необходимый чтобы доходы, полученные в результате инвестиций, покрыли затраты);
- *TCO (Total Cost of Ownership* — совокупная стоимость владения);
- *ROI (Return on Investment* — отдача от инвестиций и *ROSI* — изменение *ROI* от инвестиций в информационную безопасность);
- *NPV (Net Present Value* — чистый дисконтированный доход).

Рассмотрим значения этих показателей более подробно.

Показатель Payback Period

Показатель Payback Period (срок окупаемости) характеризует период времени, необходимый чтобы доходы, полученные в результате инвестиций, покрыли затраты на эти самые инвестиции. Иначе говоря, если деньги на проект заемные, то отдадим мы их через срок, который и называется Payback Period. Логично, что доход от инвестиций должен быть «чистым», поскольку вкладываем мы конечную и свою «чистую» сумму денег.

Формула расчета показателя выглядит следующим образом:

$$PP = min\ n, \text{ при котором } \sum_{i=1}^{n} CF_i > IC,$$

[1] *Антонова Е.К., Баранова Е.К., Бабаш А.В.* Особенности оценки экономической эффективности системы защиты информации // Материалы 26-й научно-практической конференции «Методы и технические средства обеспечения безопасности информации», 26–29 июня 2017. — СПб.: Изд-во Политехнического университета. — 2017. — С. 68–77.

где *IC (Invest Capital)* — инвестиционный капитал, первоначальные затраты инвестора на объект вложения;

CF (Cash Flow) — денежный поток, который создается объектом инвестиций, при этом здесь подразумевается чистый денежный поток (приход минус расход по проекту);

i — период времени, по которому учитывается денежный поток CF_i;

n — количество периодов времени.

Формула расчета периода окупаемости может иметь и следующий вид:

$$PP = \frac{IC}{CF}$$

Здесь затраты на инвестиции представляют собой все издержки инвестора при вложении в инвестиционный проект. Денежный поток необходимо учитывать за определенные периоды времени (день, неделя, месяц, год). В результате период окупаемости инвестиций будет иметь аналогичную шкалу измерения.

Следует отметить, что показатель окупаемости оценивает риски невозврата инвестиций. То есть чем больше период окупаемости, тем больше риски (например, если окупаемость приближается к времени жизни системы, то риски считаются очень большими). Однако данный показатель не универсален. В целом он не показывает инвестиционную привлекательность проекта с точки зрения дальнейшего дохода (после истечения срока окупаемости). Если окупаемость равна одному году, это не означает, что проект через два года и более будет приносить доход на том же уровне.

Вместе с тем в реальных условиях достаточно сложно прогнозировать устойчивые будущие денежные поступления, поэтому период окупаемости может существенно измениться. Для того чтобы снизить возможные отклонения от плана окупаемости, следует обеспечить надежность источников поступления денежного потока инвестиционного проекта. К тому же показатель не учитывает влияние инфляции на изменение стоимости денег во времени. Срок окупаемости инвестиций может быть использован как критерий отсева на первом этапе оценки и отбора «тяжелых» инвестиционных проектов.

Показатель TCO

Показатель TCO определяется как сумма прямых и косвенных затрат, которые несет владелец системы на протяжении всего жизненного цикла ее эксплуатации. TCO считается для ограниченного периода времени, поскольку для каждой IT-системы существует определенный срок функционирования.

Формула расчета показателя TCO в общем виде выглядит следующим образом:

$$TCO = DE + IDC,$$

где *DE (Direct Expenses)* — прямые расходы;

IDC (Indirect Costs) — косвенные расходы.

На примере внедрения IT-системы суммарная величина TCO включает в себя затраты на:

- проектирование информационной системы (*DE*);
- приобретение аппаратных и программных средств (*DE*);
- разработку программного обеспечения и его документирование, а также на исправление ошибок и доработку в течение периода эксплуатации (*IDC*);
- текущее администрирование информационных систем (*IDC*);
- техническую поддержку и сервисное обслуживание (*IDC*);
- расходные материалы (*IDC*);
- телекоммуникационные услуги (*IDC*);
- затраты на обучение (*IDC*);
- издержки, связанные с потерей времени пользователями в случае сбоев в работе информационных систем (*IDC*).

Также в расчет затрат на повышение уровня ИБ необходимо включать расходы на реорганизацию бизнес-процессов и информационную работу с персоналом. Кроме того, при анализе расходов необходимо учитывать, что в большинстве случаев внедрение средств защиты информации предполагает появление дополнительных обязанностей у персонала компании и необходимости осуществления дополнительных операций при работе с информационными системами. Значение TCO в каждом конкретном случае необходимо определять индивидуально с учетом особенностей проекта, который предстоит реализовать: основной востребованной функциональности, существующей инфраструктуры, количества пользователей и других факторов.

Показатель TCO позволяет руководителям служб безопасности обосновывать бюджет на информационную безопасность. Кроме того, поскольку оценка экономической эффективности системы защиты информации становится «измеримой», возможно оперативно решать задачи контроля и коррекции показателей экономической эффективности деятельности службы безопасности.

Немаловажный аспект состоит в том, что при оценке стоимости внедрения какого-либо решения большое внимание уделяется сто-

имости его приобретения (капитальные затраты), а то, сколько денег позволяет сэкономить его эксплуатация, как правило, остается в тени. Экономия происходит не только за счет снижения прямых затрат (применения новых технологий и алгоритмов, повышающих производительность и позволяющих получить больше требуемых результатов в единицу времени), но и за счет снижения косвенных издержек (например: электроэнергия, аренда, техническое сопровождение, обучение персонала). Очевидно, функциональность продукта сильно влияет на второй тип затрат (косвенные затраты), поэтому такого рода затраты обязательно учитываются при расчете TCO.

Одним из преимуществ показателя TCO является то, что он позволяет сделать выводы о целесообразности реализации проекта в области ИБ на основании оценки одних лишь только затрат.

Другим преимуществом этого показателя является то, что модель расчета TCO предполагает оценку не только первоначальных затрат на создание СЗИ, но и затрат, которые могут иметь место на различных этапах всего жизненного цикла системы. Но, несмотря на это, показатель TCO является статичным и не учитывает изменения ситуации во времени.

Особенность применения этого показателя состоит в сравнении полученной оценки для конкретной компании с рекомендуемой или оцениваемой экспертно оптимальной величиной TCO для данного типа компаний. Если полученная совокупная стоимость владения системы безопасности значительно превышает рекомендованное значение и приближается к предельному, то необходимо принять меры по снижению TCO.

Показатели ROI и ROSI

ROI — это процентное отношение прибыли (или экономического эффекта) от внедрения проекта к инвестициям, необходимым для реализации этого проекта. В общем случае под инвестициями подразумевается показатель TCO.

Формула расчета показателя ROI выглядит следующим образом:

$$ROSI = \frac{\text{Доходы} - \text{Расходы}}{\text{Инвестиции}},$$

где Доходы — фактические доходы компании за отчетный период (год);

Расходы — фактические расходы компании за отчетный период (год);

Инвестиции — инвестиции, необходимые для реализации проекта.

Таким образом, ROI — это интегральный показатель, позволяющий оценить насколько эффективно работают вложенные в компанию деньги, т.е. сколько денег «производит» за год каждый рубль, вложенный в компанию по данному проекту.

Показатель ROI, может быть скорректирован на ставку дисконтирования. Функция дисконтирования используется при анализе инвестиционных вложений для учета влияния фактора времени и приведения разновременных затрат к единому моменту. Ставка дисконтирования в этом случае позволяет учесть изменение стоимости денег с течением времени.

Совместно с показателем ROI рассмотрим показатель *ROSI (Return on Security Investment* – оценка эффективности инвестиций в безопасность). Формула его расчета приведена ниже:

$$ROSI = \frac{\Delta\text{Доходы} - \Delta\text{Расходы}}{\Delta\text{Инвестиции}},$$

где *ROSI* — показатель изменения ROI за счет инвестиций в ИБ;

ΔДоходы — изменение в доходах, обусловленное инвестициями ИБ;

ΔРасходы — изменение в расходах, обусловленное инвестициями ИБ;

ΔИнвестиции — инвестиции, сделанные в ИБ.

Смысл совместного расчета показателей ROI и ROSI сводится к сопоставлению этих показателей для понимания того, влияет ли реализация проекта на деятельность компании и каким образом.

В зависимости от эффективности проекта организации системы информационной безопасности и от отношения размера инвестиций в него к общим инвестициям в компанию, изменяется общая эффективность компании.

Так, ROI может:

- увеличиться (ROSI > ROI);
- уменьшиться (ROSI < ROI);
- остаться прежним (ROSI = ROI).

После расчета ROSI его значение необходимо сравнить со следующими «пороговыми величинами»:

ROSI < 0, т.е. эффективность проекта отрицательна и это, конечно, худший вариант, но он не так редок, как может показаться;

ROI > ROSI > 0, т.е. внедрение проекта приведет к уменьшению общего ROI в компании;

ROSI > ROI, т.е. внедрение проекта приведет к увеличению общего ROI в компании.

Однако, применяя показатель ROI для расчета эффективности вложений в информационную безопасность, следует понимать, что прямого влияния на рост доходов система информационной безопасности не имеет. Поэтому, как правило, не стоит ожидать увеличения выручки компании после инвестиций в сферу информационной защищенности.

Показатель NPV

Чистый дисконтированный доход (чистая текущая стоимость, чистый приведенный доход, текущая стоимость) — показатель, отражающий изменение денежных потоков и разность между дисконтированными денежными доходами и расходами.

Из определения очевидно, что при расчете данного показателя учитываются динамичные факторы изменения денежного потока (например, инфляция). Влияние таких факторов расчетным способом нейтрализуется, и в итоге получается стоимость, приведенная к определенному периоду времени. Общая формула расчета показателя выглядит следующим образом:

$$NPV = \sum_{t=0}^{n} \frac{CF_t}{(1+r)^t},$$

где CF_t – денежный поток в период времени t;

r – ставка дисконтирования;

t – период времени, по которому учитывается CF_t;

n – количество периодов времени.

Отметим, что под периодом $t = 0$ здесь подразумевается «начальная точка», когда были осуществлены инвестиции. При таком подходе стоимость всех дальнейших денежных потоков приводится к их стоимости в период $t = 0$.

Расчет денежного потока сводится к суммированию положительных денежных потоков (потенциальных доходов) и вычитанию из них возникающих отрицательных потоков (расходов).

Критерии оценки показателя *NPV* следующие:

- $NPV < 0$ — результатом реализации инвестиционного проекта будут убытки;
- $NPV = 0$ — инвестиционный проект обеспечит уровень безубыточности, когда все доходы равны расходам;
- $NPV > 0$ — инвестиционный проект принесет прибыль.

Следует отметить, что при расчете показателя *NPV* будущие денежные потоки мы можем скорректировать на риски, умножив тот или иной вид дохода и расхода на соответствующий коэффициент. Также здесь может быть учтена количественная оценка риска.

Одним из немногих способов, который поможет компании определить экономический эффект от осуществления мероприятий в сфере защиты информации, является финансовая оценка того ущерба, который может быть нанесен информационным ресурсам компании и который может быть предотвращен в результате реализации предлагаемых мероприятий. Таким образом, предполагаемый предотвращенный ущерб и будет составлять полученный экономический эффект или дополнительный денежный поток. При таком подходе большинство расчетов могут быть только оценочными и носить приблизительный характер. Это связано с тем, что активность злоумышленников, являющихся источниками угроз ИБ, практически непредсказуема: невозможно достоверно предсказать стратегии нападения, квалификацию нападающих, их конкретные намерения и ресурсы, которые будут задействованы для совершения тех или иных действий, а также намерения в отношении украденной информации. Соответственно, для осуществления всех необходимых расчетов необходимо сделать множество допущений и экспертных оценок в контексте деятельности конкретного предприятия, а также по возможности изучить статистическую информацию, касающуюся атак на информационные ресурсы, аналогичные защищаемым. При таком подходе, экономическая оценка эффективности мер по защите информации предполагает: оценку существующих угроз для информационных активов, которых коснется реализация защитных мер; оценку вероятности реализации каждой из выявленных угроз; экономическую оценку последствий реализации угроз.

Рассмотренные методики оценки экономической эффективности защиты информации и ключевые показатели, положенные в основу применения этих методик, представлены в табл. 6.1.

Таблица 6.1

Методики оценки экономической эффективности системы обеспечения ИБ

Наименование показателя	Формула расчета
Срок окупаемости, PP	$PP = min\ n$, при котором $\sum_{i=1}^{n} CF_i > IC$, $PP = \frac{IC}{CF}$ где *IC* (Invest Capital) — инвестиционный капитал, первоначальные затраты инвестора в объект вложения; *CF* (Cash Flow) — денежный поток, который создается объектом инвестиций, при этом здесь подразумевается чистый денежный поток (приход минус расход по проекту); *i* — период времени, по которому учитывается денежный поток CF_i; *n* — количество периодов времени.
Совокупная стоимость владения, TCO	$TCO = DE + IDC$, где *DE* (Direct Expenses) — прямые расходы; *IDC* (Indirect Costs) — косвенные расходы.
Отдача от инвестиций, *ROI, ROSI*	$ROSI = \frac{\text{Доходы} - \text{Расходы}}{\text{Инвестиции}}$, $ROSI = \frac{\Delta\text{Доходы} - \Delta\text{Расходы}}{\Delta\text{Инвестиции}}$, где ΔДоходы — изменение в доходах, обусловленное инвестициями в ИБ; ΔРасходы — изменение в расходах, обусловленное инвестициями в ИБ; ΔИнвестиции — инвестиции, сделанные в ИБ.
Чистый дисконтированный доход, NPV	$NPV = \sum_{t=0}^{n} \frac{CF_t}{(1+r)^t}$, где CF_t — денежный поток в период времени *t*; *r* — ставка дисконтирования; *t* — период времени, по которому учитывается CF_t; n — количество периодов времени.

Помимо обозначенных выше методик, рассмотрим некоторые качественные методы оценки экономической эффективности системы защиты информации.

Метод *REJ* (*Rapid Economic Justification*) — метод быстрого экономического обоснования, можно отнести к группе методов, направленной на анализ и выработку управленческих решений в области управления информационной безопасностью. Данный метод был разработан компанией *Microsoft*. Он позволяет проводить оценку бизнес-преимуществ в рассматриваемой сфере в сопоставлении с ресурсными и капитальными затратами, направленными на достижение этих преимуществ. Иными словами, данная методика предусматривает конкретизацию модели TCO за счет установления соответствия между расходами на IT и приоритетами бизнеса. Для достижения данной цели предусмотрен следующий пятиступенчатый процесс:

- разработка бизнес-плана, отражающего мнение всех заинтересованных сторон и учитывающего основные факторы успеха и ключевые показатели эффективности бизнеса;
- совместная проработка влияния технологии на факторы успеха бизнеса;
- анализ критериев стоимости и эффективности запланированных мероприятий;
- определение потенциальных рисков с указанием вероятности возникновения и воздействия каждого из них;
- вычисление стандартных финансовых показателей.

Следует отметить, что методология REJ наиболее эффективна в реализации по отношению к отдельным проектам, нежели к их портфелю или бизнесу в целом. Ключевое преимущество методики заключается в базировании на показателе TCO и при этом наличии анализа рисков.

Методика *BSC (Balanced Scorecard)* — методика сбалансированного плана достижения стратегических показателей. Она позволяет взвешенно оценить деятельность предприятия по четырем ключевым сферам: финансы, заказчики, внутренние процессы и персонал. Преимущество данной методики в плане ее применения сотрудниками службы безопасности заключается в уходе от финансовой оценки деятельности предприятия. Следовательно, методика применима в таких областях, которые напрямую не влияют на уровень доходов (каковой и является информационная безопасность). В рамках применения данной методики представляется возможность оценить

нематериальные активы: уровень корпоративных инноваций, степень удовлетворенности сотрудников, эффективность приложений и др. Однако при применении методики BSC в случае игнорирования основополагающего этапа планирования стратегии ведения бизнеса с четкими причинно-следственными связями, ее использование может привести к определению параметров, которые не имеют непосредственного отношения к эффективности бизнеса, а значит не соответствуют цели обеспечения информационной безопасности.

Методика *ROV (Real Options Valuation)* — была разработана на основе удостоенной Нобелевской премии модели опционов Блэка – Шоулза. Данная технология позволяет оценить эффективность аренды, слияние, покупки и производства. Ее можно использовать в качестве альтернативы стандартным процедурам составления бюджета и плана капиталовложений в условиях неопределенного состояния рынка и экономики в целом, т.е. со стороны внешних факторов, когда на передний план выходят параметры гибкости.

И наконец, методика *IE* или *AIE (Applied Information Economics)* — прикладная информационная экономика. Она направлена на анализ конкретного проекта и заключается в ранжировании приоритетов предприятия в области информационной безопасности с учетом материальных и нематериальных факторов (таких как конкурентоспособность, изменение риска). Для данной методики характерен большой объем расчетов ввиду того, что она методологически объединяет элементы теории опционов, современной теории управления портфелем активов, традиционные бухгалтерские подходы и некоторые статистические методы. Учитывая многофакторность подхода, методика IE применяется при анализе рисков в достаточно дорогостоящих проектах информационной безопасности.

Рассмотренные качественные методики оценки экономической эффективности проектов имеют свои сильные и слабые стороны с точки зрения возможности их применения к оценке экономической эффективности системы обеспечения ИБ, ключевые из которых представлены в табл. 6.2.

Таблица 6.2

Ключевые достоинства и недостатки качественных методик оценки экономической эффективности системы обеспечения ИБ

Методика	Достоинства	Недостатки
REJ	Возможность оценить вклад службы защиты информации в бизнес-результат компании	Невозможно комплексно оценить преобразование инфраструктуры информационной безопасности
BS	Учет всех ключевых аспектов ведения бизнеса	Большая трудоемкость ввиду необходимости создания и ведения эффективной системы сбора и обработки информации
ROV	Возможность влиять на оцениваемые параметры по ходу проекта	Весьма трудоемкая с точки зрения проведения анализа
IE	Учет проектных приоритетов в контуре приоритетов бизнеса в целом	Большой объем расчетов

6.2. Сравнительный анализ методов оценки экономической эффективности системы обеспечения информационной безопасности

При проведении сравнительного анализа рассмотрим четыре методики оценки экономической эффективности проектов ИБ: срок окупаемости (*PP*), совокупная стоимость владения (*TCO*), отдача от инвестиций в информационную безопасность (*ROI, ROSI*) и чистый дисконтированный доход (*NPV*).

Критерии для сравнительного анализа методик и их веса определены экспертным путем и обоснованы в работе[1]. В качестве *критериев оценки* используются следующие девять параметров: универсальность методики; объективность показателя; доступность исходных данных; прозрачность расчета; наличие критерия результативности; возможность факторного анализа; количественная оценка инвестиций; учет риска; учет бюджетных ограничений.

[1] *Зубарева Е.В., Васенёва В.А., Николаенко В.Г.* Количественная оценка эффективности инвестиций в информационную безопасность предприятия // Евразийский союз ученых. – М.: Изд-во ООО «Международный образовательный центр». — 2015. — № 5(14). — С. 63–65.

Веса критериев представлены табл. 6.3 значениями от 1 до 5 и численно определены исходя из сопоставления со значимостью остальных критериев. Значимость в данном контексте определена как качественная характеристика методики с позиции ее применения в компании.

Таблица 6.3

Веса критериев сравнения методик оценки экономической эффективности ИБ

Методика	Вес критерия (1–5)
Универсальность методики	5
Объективность показателя	4
Доступность исходных данных	3
Прозрачность расчета	4
Наличие критерия результативности	4
Возможность факторного анализа	5
Количественная оценка инвестиций	4
Учет риска	4
Учет бюджетных ограничений	3

Поясним суть и значимость каждого из критериев. Под универсальностью методики подразумевается возможность ее применения к проектам обеспечения ИБ независимо, прежде всего, от сути самого внедрения (будь то информационная технология, организационный аспект управления информационной безопасностью или физическое средство защиты). Также не менее важным аспектом универсальности методики является возможность ее применения в разного рода компаниях независимо от отрасли, размера, цели компании и т.д. Поскольку обобщенная оценка методик предполагает результат в виде вывода относительно применимости методик в том или ином типе компании, данный критерий имеет максимальный по сравнению с остальными критериями вес 5.

Объективность показателя предполагает полноту отражения данных о системе обеспечения ИБ (в нашем случае стоимостных) в показателе. Чем полнее представлен и учтен объект методики, чем меньше субъективно определяемых критериев ключевого показателя, тем более объективна эта методика. Данному критерию присвоен вес 4.

Доступность исходных данных предполагает возможность доступа субъектов применения методики (чаще всего это сотрудники службы защиты информации или финансовые аналитики по проектам в области ИБ) к исходным данным, необходимым для расчетов. Кроме того, даже при максимальном уровне доступа, не все исходные данные можно получить из-за невозможности их расчета без предварительно обозначенных гипотез (например, в части распределения косвенных затрат по проекту). Ввиду некоторой субъективности самого критерия, ему присвоен вес 3.

Прозрачность расчета как критерий сравнения методик представляет собой возможность увидеть в результате расчета показателя, как формируются те или иные промежуточные итоги, из чего они складываются, как соотносятся с проектом, как их можно оценить в контексте общей управленческой отчетности. Данный критерий важен с позиции принятия решений руководством, так как без понимания того, как обоснована необходимость инвестирования в проект обеспечения ИБ, не возможно принятие корректного решения. Критерию присвоен вес 4.

Наличие критерия результативности предполагает возможность оценки итога путем его сопоставления с некоторой мерой, отражающей результат. Причем чем меньше зависимость этой самой меры от самой компании, тем выше оценка по данному критерию. Вес критерия составляет 4.

Возможность факторного анализа в чем-то пересекается с прозрачностью расчета в части понимания принципа расчета показателя. Если его можно разложить на факторы, на него влияющие, существует возможность понимания влияния на итоговый результат. С точки зрения аналитики, это один из ключевых критериев, поэтому ему присвоен вес 5.

Количественная оценка инвестиций предполагает наличие результата в форме некоторой суммы, которую компания может инвестировать в проект защиты информации. Данный критерий зависит в некотором смысле от финансового положения самой организации, однако факт отражения суммы инвестиций является значительным плюсом для количественной методики, поэтому данному критерию присвоен вес 4.

Учет риска предполагает возможность корректировки показателя планируемых инвестиций на внутренние и внешние риски. Для количественных методик такой риск может быть выражен в виде некоторой процентной ставки, куда закладываются инфляционные ожидания, повышение ставки по кредитам в случае привлечения заемных источников финансирования. Кроме того, риск может быть представлен в

виде различных сценариев, где учитываются наименее или наиболее вероятные ожидаемые денежные потоки. Данному критерию присвоен вес 4.

Критерий учета бюджетных ограничений не является необходимым для методики, но дает ей плюс. Например, сотрудники службы защиты информации при анализе проекта располагают изначально определенным максимумом инвестиций, которые они могут вложить в проект. Если такую функцию можно ввести в расчет, то значительно удобнее анализировать проект. Критерию присвоен вес 3.

По каждому критерию экспертно оценена каждая из четырех выбранных методик (шкала оценивания — от 1 до 10). В отношении каждой методики введена суммарная оценка, рассчитанная исходя из критериальных оценок с учетом весов критериев. Итоговая оценка позволит сделать общие выводы относительно степени разработанности методик, а оценки по каждому критерию позволят сделать выводы относительно того, в какого типа компаниях данная методика наиболее удачно может быть применена.

Как уже указывалось, мы сравниваем четыре количественные методики — срок окупаемости, совокупная стоимость владения, отдача от инвестиций и чистый дисконтированный доход. Критериев для сравнения выбрано девять. Результаты оценивания методик и общие взвешенные оценки представлены в табл. 6.4.

Таблица 6.4

Оценка методик по критериям

Критерий	PP	TCO	ROI, ROSI	NPV
Универсальность методики	9	10	9	9
Объективность показателя	7	8	7	8
Доступность исходных данных	8	9	8	8
Прозрачность расчета	7	8	7	8
Наличие критерия результативности	8	7	9	9
Возможность факторного анализа	8	10	9	9
Количественная оценка инвестиций	8	10	8	9
Учет риска	9	8	9	9
Учет бюджетных ограничений	7	8	7	9
Итоговая оценка	7,94	8,75	8,19	8,69

Для большей наглядности, результаты сравнения методик представлены на диаграмме (рис. 6.1).

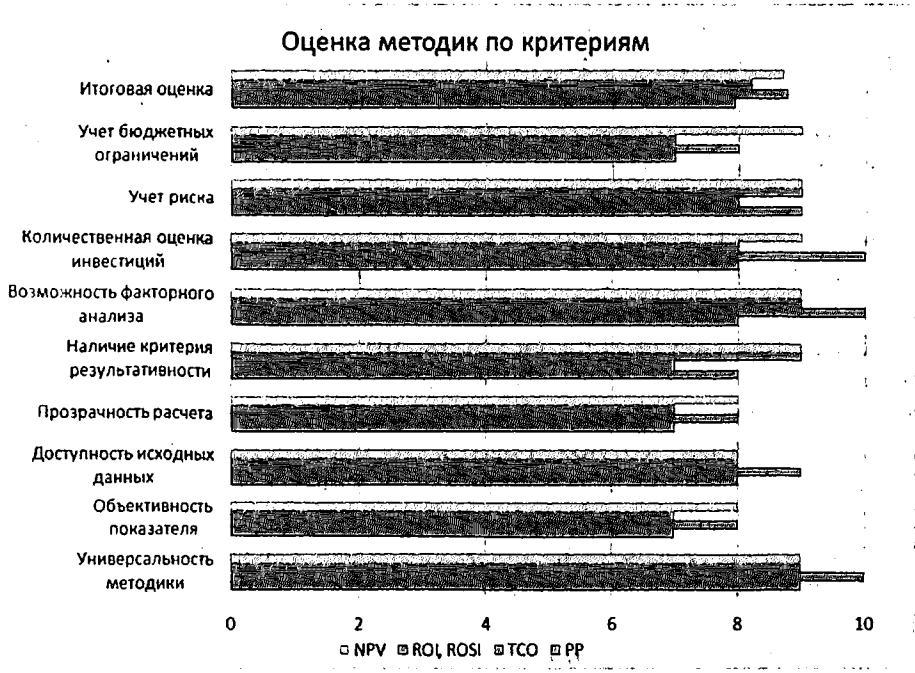


Рис. 6.1. Оценка методик экономического анализа ИБ

Интерпретируя результаты сравнения методик оценки экономической эффективности проектов обеспечения ИБ в компании, можно сделать следующие выводы. Наибольшую по сравнению с остальными оценку получила методика TCO. Действительно, это один из наиболее универсальных показателей не только оценки планируемых инвестиций в ИБ, но и контроля текущей стоимости владения информационными активами. Также данный показатель, согласно оценкам, является наилучшим в плане факторного анализа, что важно для принятия решения об изменении размера инвестиций. Важно и то, что показатель абсолютный и он дает стоимостную оценку.

Следует отметить, что в отношении малого и среднего бизнеса данный показатель может быть применен фактически независимо от отрасли, к которой относится компания: сумма владения информационными активами будет показательна для руководства. Но в отношении малого бизнеса, если это не сектор информационных технологий и не информационный бизнес, стоимость владения не достаточно показа-

тельна без ее сравнения с другими оценками либо сопоставления с доходами (в случае ИБ — с потенциальными потерями)[1].

Что касается особенностей оценки при различных организационно-правовых формах, здесь несколько сложнее и картина зависит от каждого конкретного случая. Тем не менее, в ООО более вероятна и достаточно распространена единоличная форма владения активами компании, т.е. условимся, что инвестор один. В АО же, как правило, таких собственников, держателей акций (инвесторов) больше одного. Следовательно, во втором случае инвесторам сложнее принять решение исключительно по показателю TCO, поскольку у них не возникает понимания, как ситуация в дальнейшем отразится на их доходе (или не отразится на потерях, в связи с незащищенностью бизнеса с позиций ИБ).

Последняя ситуация плавно приводит нас к рассмотрению второго по оценке показателя — NPV. Чистый дисконтированный доход по сути своей представляет разницу положительных и отрицательных денежных потоков, что может быть интерпретировано как прибыль[2] (не будем углубляться в пояснения о разных видах прибыли). Следовательно, для акционерных обществ и держателей акций данный показатель представляется оптимальным. Кроме названного, преимуществом показателя является учет бюджетных ограничений. Наиболее эффективен чистый дисконтированный доход, когда мы говорим о проекте внедрения системы обеспечения ИБ, нежели когда сопоставляем с активами предприятия. NPV можно вычислить как для определенного этапа проекта, так и для всего его жизненного цикла, приведя его стоимость к какому-либо периоду путем дисконтирования.

Следующий показатель — ROI или ROSI. Его преимущество как относительного показателя заключается в возможности сопоставления с доходами или потерями, что делает его эффективным для применения в малом бизнесе.

Идеально, когда при принятии решения в комплексе рассматриваются абсолютные и относительные показатели. Таким показательным сочетанием для СЗИ является пара показателей TCO и ROSI.

[1] *Тихонов Д.В.* Модели оценки эффективности систем информационной безопасности. Диссертация на соискание степени кандидата экономических наук. Шифр специальности: 08.00.13, 08.00.05. СПб.: 2009. — 126 с. URL: http://dlib.rsl.ru/01004359710.

[2] *Aubuchon K.* Applying NPV and ROI to Security Investment Decisions. — Washington, DC: U.S. — 2015. — P. 65–74.

Важным критерием показателя отдачи инвестиций является наличие критерия результативности, что делает его практически применимым независимо от сферы бизнеса и размеров компании.

Говоря о сочетании абсолютного и относительного показателей, нельзя не отметить важность совместного использования и взаимозависимости показателей NPV и PP. Оба эти показателя применимы по отношению к проектам ИБ. Чистый дисконтированный доход по полному циклу учитывает притоки и оттоки денежных средств на каждом этапе этого цикла, а срок окупаемости в случае с проектами обеспечения ИБ и есть количество этих этапов. Кроме названного, срок окупаемости как относительный показатель важен, поскольку в нем можно отразить корректировку на риск.

Таким образом, интерпретировав оценки показателей применительно к типу компаний и сопоставив их друг с другом, можно сделать вывод, что наиболее показательным в любом случае является сочетание использования методик с абсолютными и относительными результатами. Так, TCO и ROSI могут быть использованы как инструменты и принятия решения об инвестировании, и контроля текущей стоимости, а применимы они в большей степени в компаниях с единоличной формой владения. При акционерной форме наиболее показательным для инвесторов является результат применения методики NPV, которая в сочетании с PP дает достаточно полную экономическую оценку эффективности проекта системы защиты информации.

Литература к главе 6

1. *Ажмухамедов И.М., Ханжина Т.Б.* Оценка экономической эффективности мер по обеспечению информационной безопасности // Вестник Астраханского государственного технического университета. Серия: Экономика. — 2011. — № 1. — С. 185–190.

2. *Антонова Е.К., Баранова Е.К., Бабаш А.В.* Особенности оценки экономической эффективности системы защиты информации // Материалы 26-й научно-практической конференции «Методы и технические средства обеспечения безопасности информации», 26–29 июня 2017. — СПб.: Изд-во Политехнического университета. — 2017. — С. 68–77.

3. *Баранова Е.К., Бабаш А.В.* Информационная безопасность и защита информации / Третье издание, переработанное и дополненное. — М.: ИНФРА-М; РИОР, 2016.

4. *Зубарева Е.В., Васенёва В.А., Николаенко В.Г.* Количественная оценка эффективности инвестиций в информационную безопасность предприятия. // Евразийский союз ученых. — М.: Изд-во ООО «Международный образовательный центр». — 2015. — № 5(14). — С. 63–65.

5. *Тихонов Д.В.* Модели оценки эффективности систем информационной безопасности. Диссертация на соискание степени кандидата экономических наук. Шифр специальности: 08.00.13, 08.00.05. СПб., 2009. URL: http://dlib.rsl.ru/01004359710

6. *Aubuchon K.* Applying NPV and ROI to Security Investment Decisions. – Washington, DC: U.S. — 2015. — P. 65–74.

ТЕСТ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ»

1. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
   a) меры обеспечения целостности;
   b) административные меры;
   c) меры обеспечения конфиденциальности.
2. Дублирование сообщений является угрозой:
   a) доступности;
   b) конфиденциальности;
   c) целостности.
3. Вредоносное ПО Melissa подвергает атаке на доступность:
   a) системы электронной коммерции;
   b) геоинформационные системы;
   c) системы электронной почты.
4. Выберите вредоносную программу, которая открыла новый этап в развитии данной области.
   a) Melissa.
   b) Bubble Boy.
   c) ILOVEYOU.
5. Самыми опасными источниками внутренних угроз являются:
   a) некомпетентные руководители;
   b) обиженные сотрудники;
   c) любопытные администраторы.
6. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности.
   a) просчеты при администрировании информационных систем;
   b) необходимость постоянной модификации информационных систем;
   c) сложность современных информационных систем.
7. Агрессивное потребление ресурсов является угрозой:
   a) доступности
   b) конфиденциальности
   c) целостности
8. Программа Melissa — это:
   a) бомба;

b) вирус;
c) червь.

9. Для внедрения бомб чаще всего используются ошибки типа:
a) отсутствие проверок кодов возврата;
b) переполнение буфера;
c) нарушение целостности транзакций.

10. Окно опасности появляется, когда:
a) становится известно о средствах использования уязвимости;
b) появляется возможность использовать уязвимость;
c) устанавливается новое ПО.

11. Среди ниже перечисленных отметьте две троянские программы:
a) ILOVEYOU;
b) Back Orifice;
c) Netbus.

12. Уголовный кодекс РФ не предусматривает наказания за:
a) создание, использование и распространение вредоносных программ;
b) ведение личной корреспонденции на производственной технической базе;
c) нарушение правил эксплуатации информационных систем.

13. Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают:
a) средства выявления злоумышленной активности;
b) средства обеспечения отказоустойчивости;
c) средства контроля эффективности защиты информации.

14. Уровень безопасности B согласно «Оранжевой книге» характеризуется:
a) произвольным управлением доступом;
b) принудительным управлением доступом;
c) верифицируемой безопасностью.

15. В число классов требований доверия безопасности «Общих критериев» входят:
a) разработка;
b) оценка профиля защиты;
c) сертификация.

16. Согласно «Оранжевой книге» политика безопасности включает в себя следующие элементы:
a) периметр безопасности;
b) метки безопасности;
c) сертификаты безопасности.

17. Согласно рекомендациям X.800 выделяются следующие сервисы безопасности:
a) управление квотами;
b) управление доступом;
c) экранирование.

18. Уровень безопасности A согласно «Оранжевой книге» характеризуется:
a) произвольным управлением доступом;
b) принудительным управлением доступом;
c) верифицируемой безопасностью.

19. Согласно рекомендациям X.800 аутентификация может быть реализована на:
a) сетевом уровне;
b) транспортном уровне;
c) прикладном уровне.

20. В число целей политики безопасности верхнего уровня входят:
a) решение сформировать или пересмотреть комплексную программу безопасности;
b) обеспечение базы для соблюдения законов и правил;
c) обеспечение конфиденциальности почтовых сообщений.

21. В число целей политики безопасности верхнего уровня входят:
a) управление рисками;
b) определение ответственных за информационные сервисы;
c) определение мер наказания за нарушения политики безопасности.

22. В рамках политики безопасности нижнего уровня осуществляются:
a) стратегическое планирование;
b) повседневное администрирование;
c) отслеживание слабых мест защиты.

23. Политика безопасности строится на основе:
a) общих представлений об ИС организации;
b) изучения политик родственных организаций;
c) анализа рисков.

24. В число целей политики безопасности верхнего уровня входят:
a) формулировка административных решений по важнейшим аспектам реализации программы безопасности;
b) выбор методов аутентификации пользователей;
c) обеспечение базы для соблюдения законов и правил.

25. Риск является функцией:
    a) размера возможного ущерба;
    b) числа пользователей информационной системы;
    c) уставного капитала организации.
26. В число этапов управления рисками входят:
    a) идентификация активов;
    b) ликвидация пассивов;
    c) выборобъектов оценки.
27. Первый шаг в анализе угроз — это:
    a) идентификация угроз;
    b) аутентификация угроз;
    c) ликвидация угроз.
28. Управление рисками включает в себя следующие виды деятельности:
    a) определение ответственных за анализ рисков;
    b) оценка рисков;
    c) выбор эффективных защитных средств.
29. Оценка рисков позволяет ответить на следующие вопросы:
    a) чем рискует организация, используя информационную систему?
    b) чем рискуют пользователи информационной системы?
    c) чем рискуют системные администраторы?
30. В число классов мер процедурного уровня входят:
    a) поддержание работоспособности;
    b) поддержание физической формы;
    c) физическая защита.
31. В число принципов управления персоналом входят:
    a) минимизация привилегий;
    b) минимизация зарплаты;
    c) максимизация зарплаты.
32. В число этапов процесса планирования восстановительных работ входят:
    a) выявление критически важных функций организации;
    b) определение перечня возможных аварий;
    c) проведение тестовых аварий.
33. В число направлений повседневной деятельности на процедурном уровне входят:
    a) ситуационное управление;
    b) конфигурационное управление;
    c) оптимальное управление.

34. Протоколирование и аудит могут использоваться для:
    a) предупреждения нарушений ИБ;
    b) обнаружения нарушений;
    c) восстановления режима ИБ.
35. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:
    a) выработка и проведение в жизнь единой политики безопасности;
    b) унификация аппаратно-программных платформ;
    c) минимизация числа используемых приложений.
36. Экранирование может использоваться для:
    a) предупреждения нарушений ИБ;
    b) обнаружения нарушений;
    c) локализации последствий нарушений.
37. В число основных принципов архитектурной безопасности входят:
    a) следование признанным стандартам;
    b) применение нестандартных решений, не известных злоумышленникам;
    c) разнообразие защитных средств.
38. В число основных принципов архитектурной безопасности входят:
    a) усиление самого слабого звена;
    b) укрепление наиболее вероятного объекта атаки;
    c) эшелонированность обороны.
39. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:
    a) использование собственных линий связи;
    b) обеспечение конфиденциальности и целостности при сетевых взаимодействиях;
    c) полный анализ сетевого трафика.
40. В число универсальных сервисов безопасности входят:
    a) управление доступом;
    b) управление информационными системами и их компонентами;
    c) управление носителями.
41. Контроль целостности может использоваться для:
    a) предупреждения нарушений ИБ;
    b) обнаружения нарушений;
    c) локализации последствий нарушений.

42. В число универсальных сервисов безопасности входят:
a) средства построения виртуальных локальных сетей;
b) экранирование;
c) протоколирование и аудит.
43. В качестве аутентификатора в сетевой среде могут использоваться:
a) кардиограмма субъекта;
b) номер карточки пенсионного страхования;
c) результат работы генератора одноразовых паролей.
44. Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от:
a) перехвата;
b) воспроизведения;
c) атак на доступность.
45. В число основных понятий ролевого управления доступом входит:
a) роль;
b) исполнитель роли;
c) пользователь роли.
46. В качестве аутентификатора в сетевой среде могут использоваться:
a) год рождения субъекта;
b) фамилия субъекта;
c) секретный криптографический ключ.
47. Ролевое управление доступом использует следующее средство объектно-ориентированного подхода:
a) инкапсуляция;
b) наследование;
c) полиморфизм.
48. В число основных понятий ролевого управления доступом входит:
a) объект;
b) субъект;
c) метод.
49. Цифровой сертификат содержит:
a) открытый ключ пользователя;
b) секретный ключ пользователя;
c) имя пользователя.
50. Криптография необходима для реализации следующих сервисов безопасности:

a) идентификация;
b) экранирование;
c) аутентификация.
51. Криптография необходима для реализации следующих сервисов безопасности:
a) контроль конфиденциальности;
b) контроль целостности;
c) контроль доступа.
52. Экран выполняет функции:
a) разграничения доступа;
b) облегчения доступа;
c) усложнения доступа.
53. Демилитаризованная зона располагается:
a) перед внешним межсетевым экраном;
b) между межсетевыми экранами;
c) за внутренним межсетевым экраном.
54. Экранирование на сетевом и транспортном уровнях может обеспечить:
a) разграничение доступа по сетевым адресам;
b) выборочное выполнение команд прикладного протокола;
c) контроль объема данных, переданных по TCP-соединению.
55. Системы анализа защищенности помогают предотвратить:
a) известные атаки;
b) новые виды атак;
c) нетипичное поведение пользователей.
56. Среднее время наработки на отказ:
a) пропорционально интенсивности отказов;
b) обратно пропорционально интенсивности отказов;
c) не зависит от интенсивности отказов.
57. Туннелирование может использоваться на следующем уровне эталонной семиуровневой модели OSI:
a) сетевом;
b) сеансовом;
c) уровне представления.
58. Принцип усиления самого слабого звена можно переформулировать как:
a) принцип равнопрочности обороны;
b) принцип удаления слабого звена;
c) принцип выявления главного звена, ухватившись за которое, можно вытянуть всю цепь.

59. Политика безопасности:
   a) фиксирует правила разграничения доступа;
   b) отражает подход организации к защите своих информационных активов;
   c) описывает способы защиты руководства организации.
60. При анализе стоимости защитных мер следует учитывать:
   a) расходы на закупку оборудования
   b) расходы на закупку программ
   c) расходы на обучение персонала

Ответы к тесту

1) a, c	2) c	3) c	4) a	5) a, b	6) c	7) a	8) b	9) b	10) b
11) b, c	12) b, c	13) c	14) b	15) a, b	16) b	17) b	18) c	19) a	20) a, b
21) a	22) b, c	23) c	24) a	25) a	26) a, c	27) a	28) b, c	29) a	30) a, c
31) a	32) a, b	33) a, b	34) a, b	35) a	36) a	37) a, c	38) a, c	39) b	40) a
41) b	42) b, c	43) c	44) b, c	45) a	46) c	47) b	48) a, b	49) a	50) c
51) a	52) a	53) b	54) a	55) a	56) b	57) a	58) a	59) b	60) a, b, c

ЛИТЕРАТУРА

1. *Ажмухамедов И.М., Ханжина Т.Б.* Оценка экономической эффективности мер по обеспечению информационной безопасности // Вестник Астраханского государственного технического университета. Серия: Экономика. — 2011. — № 1. — С. 185–190.
2. *Александрович Г.Я., Нестеров С.А., Петренко С.А.* Автоматизация оценки информационных рисков компании // Защита информации. — Конфидент, 2003. — № 2. — С. 78–81.
3. *Андрейчиков А.В., Андрейчикова О.Н.* Анализ, синтез, принятие решений в экономике. — М.: Финансы и статистика, 2000.
4. *Антонова Е.К., Баранова Е.К., Бабаш А.В.* Особенности оценки экономической эффективности системы защиты информации // Материалы 26-й научно-практической конференции «Методы и технические средства обеспечения безопасности информации», 26–29 июня 2017. — СПб.: Изд-во Политехнического университета — 2017. — С. 68–77.
5. *Бабаш А.В., Баранова Е.К.* Актуальные вопросы защиты информации: монография / А.В. Бабаш, Е.К. Баранова. — М.: РИОР: ИНФРА-М, 2017.
6. *Баранова Е.К., Бабаш А.В.* Информационная безопасность и защита информации. — М.: РИОР: ИНФРА-М, 2016.
7. *Баранова Е.К., Бабаш А.В.* Моделирование системы защиты информации: практикум. — М.: РИОР: ИНФРА-М, 2015.
8. *Баранова Е.К.* Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. — 2009. — № 1 (49). — С. 15–26.
9. *Баранова Е.К.* Методики анализа и оценки рисков информационной безопасности. Моделирование и анализ безопасности и риска в сложных системах // Труды Международной научной школы МАБР 2014 (Санкт-Петербург, 18–20 ноября 2014 г.). — СПб., 2014. — С. 132–138.
10. *Баранова Е.К., Забродоцкий А.С.* Процедура применения методологии анализа рисков OCTAVE в соответствии со стандартами серии ИСО/МЭК 27000–27005 // Вестник Московского университета им. С.Ю. Витте. Серия 3: Образовательные ресурсы и технологии. — 2015. — № 3(11). — С. 73–77.
11. *Баранова Е.К., Зубровский Г.Б.* Управление инцидентами информационной безопасности. Проблемы информационной безопасности // Труды I Международной научно-практической конференции «Проблемы информационной безопасности». Гурзуф: Крымский федеральный университет им. В.И. Вернадского, 26–28 февраля 2015 г. — Гурзуф, 2015. — С. 27–33.

12. *Башлы П.Н.* Современные сетевые технологии: учеб. пособие. — М.: Горячая линия — Телеком, 2006.
13. *Башлы П.Н.* Информационная безопасность: учебник. — Ростов-н/Д.: Фолиант, 2005.
14. *Башлы П.Н., Бабаш А.В., Баранова Е.К.* Информационная безопасность. — М.: Изд. центр ЕАОИ, 2010.
15. *Бухтояров В.В., Золотарев В.В., Жуков В.Г.* Поддержка принятия решений при проектировании систем защиты информации: монография. — М.: ИНФРА-М, 2014.
16. *Варфоломеев В.И., Воробьев С.Н.* Принятие управленческих решений: учеб. пособие для вузов. — М.: КУДИЦ-ОБРАЗ, 2001.
17. *Вентцель Е.С.* Исследование операций: задачи, принципы, методология. — М.: Наука, 1988.
18. *Галатенко В.А.* Основы информационной безопасности. — М.: Интернет-университет информационных технологий — ИНТУИТ.РУ, 2003.
19. *Галатенко В.А.* Стандарты информационной безопасности. — М.: Интернет-университет информационных технологий — ИНТУИТ. РУ, 2004.
20. *Грибунин В.Г., Чудовский В.В.* Комплексная система защиты информации на предприятии. — М.: Академия, 2009.
21. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. — М.: ДиаСофт, 2002.
22. *Зубарева Е.В., Васенёва В.А., Николаенко В.Г.* Количественная оценка эффективности инвестиций в информационную безопасность предприятия. // Евразийский союз ученых. — М.: Изд-во ООО «Международный образовательный центр». — 2015. — № 5(14). — С. 63–65.
23. *Завгородний В.И.* Комплексная защита в компьютерных системах: учеб. пособие. — М.: Логос: ПБОЮЛ Н.А. Егоров, 2001.
24. *Карпов Е.А., Котенко И.В., Котухов М.М. и др.* Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / под ред. И.В. Котенко. — СПб.: ВУС, 2000.
25. *Касперский Е.* Компьютерное зловредство. — СПб.: Питер, 2009.
26. *Кремер Н.Ш., Путко Б.А., Тришин И.М. и др.* Исследование операций в экономике. — М.: ЮНИТИ, 2000.
27. *Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН). — СПб.: 2012. — Вып. 20. — С. 27–56.
28. *Ларичев О.И.* Теория и методы принятия решений, а также Хроника событий в Волшебных странах: учебник. — М.: Логос, 2000.

29. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов. — М.: Горячая линия – Телеком, 2004.
30. *Мельников В.В.* Безопасность информации в автоматизированных системах. — М.: Финансы и статистика, 2003.
31. *Медведовский И.Д., Семьянов П.В., Леонов Д.Г. и др.* Атака из Internet. — М.: Солон-Р, 2002.
32. *Мэйволд Э.* Безопасность сетей: пер. с англ. — М.: ЭКОМ, 2002.
33. *Новиков Ю.В., Кондратенко С.В.* Локальные сети: архитектура, алгоритмы, проектирование. — М.: ЭКОМ, 2001.
34. *Ногин В.Д.* Принятие решений при многих критериях: учеб.-метод. пособие. — СПб: ЮТАС, 2011.
35. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер, 2002.
36. *Петренко С.А., Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. — М.: Компания АйТи: ДМК Пресс, 2004.
37. *Прохода А.Н.* Обеспечение интернет-безопасности. Практикум: учеб. пособие для вузов. — М.: Горячая линия – Телеком, 2007.
38. *Розен В.В.* Математические модели принятия решений в экономике: учеб. пособие. — М.: Книжный дом «Университет»: Высшая школа, 2012.
39. *Саати Т.* Принятие решений. Метод анализа иерархий: пер. с англ. — М.: Радио и связь, 1989.
40. *Симонов С.В.* Современные технологии анализа рисков в информационных системах // PCWEEK. — 2001. — № 37. — URL: http://info-sec.edu. nw.ru/arch/analiz.htm.
41. *Смирнов Э.А.* Управленческие решения. — М.: ИНФРА-М, 2001.
42. *Спортак М., Паппас Ф.* Компьютерные сети и сетевые технологии. — М.: ТИД «ДС», 2002.
43. *Тихонов Д.В.* Модели оценки эффективности систем информационной безопасности. Диссертация на соискание степени кандидата экономических наук. Шифр специальности: 08.00.13, 08.00.05. СПб.: 2009. — URL: http://dlib.rsl.ru/01004359710.
44. *Трахтенгерц Э.А.* Компьютерная поддержка принятия решений: Научно-практич. изд. — М.: СИНТЕГ, 1998. — Серия «Информатизация России на пороге XXI века».
45. *Щербаков А.Ю.* Введение в теорию и практику компьютерной безопасности. — М.: Издательство Молгачева С.В., 2001.
46. *Шумский А.А., Шелупанов А.А.* Системный анализ в защите информации: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности. — М.: Гелиос АРВ, 2010.

47. *Хорев П.Б.* Методы и средства защиты информации в компьютерных системах. — М.: Академия, 2006.
48. *Эддоус М., Стэнсфилд Р.* Методы принятия решений. — М.: ЮНИТИ, 1997.
49. *Aubuchon K.* Applying NPV and ROI to Security Investment Decisions. — Washington, DC: U.S. — 2015. — P. 65–74.
50. *Ericson K.A.* The acquisition of expert performance: introduction to some of the issues // K.A. Ericson (Ed.). The road to excellence: the acquisition of expert performance in the arts and sciences, sport and games. — Hillsdale, NJ: Lawrence Erlbaum Associates, 1996.
51. *Lotov A., Bushenkov V., Kamenev G.* Feasible Goals Method Search for Smart Decisions. — Moscow, RAS, 2001.
52. *Peltier T.R.* Information security risk analysis / Auerbach 2001.
53. Risk Watchusers manual. — URL: http://www.riskwatch.com.
54. *Taylor L.* Risk analysis tools & how they work. — URL: http://www.riskwatch.com.

ОГЛАВЛЕНИЕ

По вопросам приобретения книг обращайтесь:
Отдел продаж «ИНФРА-М» (оптовая продажа):
127282, Москва, ул. Полярная, д. 31В, стр. 1
Тел. (495) 280-15-96; факс (495) 280-36-29
E-mail: books@infra-m.ru

•

Отдел «Книга—почтой»:
тел. (495) 280-15-96 (доб. 246)

Учебное издание

Баранова Елена Константиновна
Бабаш Александр Владимирович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие

Оригинал-макет подготовлен в Издательском Центре РИОР

Подписано в печать 25.01.2019.
Формат 60×90/16. Бумага офсетная.
Гарнитура Newton. Печать цифровая.
Усл. печ. л. 21. Уч.-изд. л. 22,69.
Доп. тираж 50 экз. Заказ № 00738
Цена свободная.

ТК 209700 — 1009606 — 250119

ООО «Издательский Центр РИОР»
127282, Москва, ул. Полярная, д. 31В.
Тел.: (495) 280-38-67.
E-mail: info@riorp.ru https://www.riorpub.com

ООО «Научно-издательский центр ИНФРА-М»
127282, Москва, ул. Полярная, д. 31В, стр. 1.
Тел.: (495) 280-15-96. Факс: (495) 280-36-29.
E-mail: books@infra-m.ru http://www.infra-m.ru

Отпечатано в типографии
ООО «Научно-издательский центр ИНФРА-М»
127282, Москва, ул. Полярная, д. 31В, стр. 1
Тел.: (495) 280-15-96, 280-33-86. Факс: (495) 280-36-29