Е.К. Баранова
А.В. Бабаш

Информационная безопасность и защита информации

Учебное пособие

Москва 2012

УДК 004.056
ББК 32.973.202
Б335

Баранова Е.К.

Б335 Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – М.: ЕАОИ, 2012. – 311 с.

ISBN 978-5-374-00301-7

Рассматриваются проблемы уязвимости информации в современных компьютерных системах, анализируются и классифицируются угрозы безопасности информации, конкретизируются задачи систем ее обеспечения, дается обзор методов, технических приемов и аппаратуры защиты информации. Основное внимание уделяется проблемам распознавания пользователей, методам защиты от компьютерных вирусов, защите информации в вычислительных сетях, организационно-правовому обеспечению безопасности информации. Излагаются некоторые методы и этапы построения комплексной системы защиты информации, а также перспективы создания изначально защищенных информационных технологий. Для оптимизации процесса контроля знаний к учебнику прилагается комплект тестовых заданий из 25 вариантов. Для студентов изучающих курс «Информационная безопасность и защита информации», также может быть полезна аспирантам и специалистам, интересующимся вопросами защиты информации.

УДК 004.056
ББК 32.973.202

ISBN 978-5-374-00301-7

Оглавление

Предисловие

Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни, поскольку современное общество все более приобретает черты информационного общества. Информационная безопасность является одной из проблем, с которой сталкивается человечество в процессе массового использования автоматизированных средств передачи, хранения и обработки информации.

Решение проблемы информационной безопасности связано с гарантированным обеспечением трех ее главных составляющих: доступности, целостности и конфиденциальности информации.

В книге рассматриваются проблемы уязвимости информации в современных информационных системах, анализируются и классифицируются угрозы безопасности информации, конкретизируются задачи систем ее обеспечения, дается обзор методов и технических приемов защиты информации. Основное внимание уделяется 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 системы информационной безопасности, а также перспективы создания изначально защищенных информационных технологий.

В главе 1 рассматриваются нормативно-правовые основы обеспечения информационной безопасности, существенное внимание уделено основополагающим нормативным документам, определяющим порядок использования различной информации, а также ответственность за соответствующие нарушения. Кроме этого, изложены общие подходы к обеспечению информационной безопасности на административном

уровне, дано понятие политики безопасности и ее содержание, проанализированы основные угрозы информационной безопасности в контексте ее составляющих.

В главе 2 рассмотрена проблема защиты информационных систем от вредоносных программ. В соответствии с современной классификацией вредоносных программ, изложены основные способы противодействия проникновению вредоносных программ в компьютеры пользователей. В этом же разделе рассматриваются угрозы для мобильных устройств и способы противодействия этим угрозам.

Глава 3 посвящена рассмотрению актуальных в настоящее время вопросов анализа и оценки информационных рисков, угроз и уязвимостей системы. Рассматриваются методики и программный инструментарий для оценки рисков в сфере информационной безопасности, приводятся примеры использования программного пакета методологии CORAS, для анализа рисков информационной безопасности предприятия.

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 отличаются, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого узла, и, во-вторых, тем, что атаке может подвергаться не определенный узел, а информация, передаваемая по сетевым каналам.

С развитием локальных и глобальных сетей именно удаленные атаки становятся лидирующими как по количеству попыток, так и по успешности их реализации, соответственно, обеспечение безопасности вычислительных сетей с точки зрения противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных вычислительных систем состоит в том, что если в локальных вычисли-

тельных сетях наиболее частые угрозы конфиденциальности и целостности информации, то в территориально распределенных сетях на первое место выходит угроза нарушения доступности информации. Все эти вопросы рассмотрены в главе 4. Там же описаны наиболее значимые механизмы защиты вычислительных систем от несанкционированных воздействий, как преднамеренного, так и непреднамеренного характера, такие как идентификация и аутентификация, регистрация и аудит, межсетевое экранирование, VPN и др.

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 глава 5 книги посвящена рассмотрению методов принятия решений, которые могут быть рекомендованы при разработке систем информационной безопасности.

Глава 1.

Общие положения информационной безопасности

1.1. Проблема обеспечения информационной безопасности

1.1.1. Определение понятия «информационная безопасность»

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

«Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации»[1]. Проблема информационной безопасности обусловлена возрастающей ролью информации в общественной жизни. Современное общество все более приобретает черты информационного общества.

С понятием «информационная безопасность» в различных контекстах связаны различные определения. Так, в Законе РФ «Об участии в международном информационном обмене» информационная безопасность определяется как состояние защищенности информационной среды общества, обеспечи-

[1] Доктрина информационной безопасности РФ, от 9 сентября 2000 г. №Пр-1895.

вающее 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 информационная безопасность в национальных масштабах и поэтому имеют очень широкое понятие.

Характерно, что применительно к различным сферам деятельности, так или иначе связанным с информацией, понятие «информационная безопасность» принимает более определенные 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. Нарушителем информационной безопасности может быть сотрудник, нарушивший режим информационной безопасности или внешняя среда, например, высокая температура, может привести к сбоям в работе технических средств хранения информации и др.

Итак, авторское определение «информационной безопасности» следующее.

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 сказать, 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 др.

С другой стороны, рассматривая информацию как субъект управления (технология производства, расписание движения транспорта и др.), можно 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.

Поэтому под защитой информации понимается комплекс мероприятий, направленных на обеспечение информационной безопасности.

Согласно ст. 16 Федерального закона Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ: «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 данного аспекта безопасности, состоящую в том, что информационная безопасность есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. В области 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.

В ряде случаев понятие «информационная безопасность» подменяется термином «компьютерная безопасность». В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем. Несмотря на это, в рамках изучаемого курса основное внимание будет уделяться изучению вопросов, связанных 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:

1) обеспечением доступности информации;
2) обеспечением целостности информации;
3) обеспечением конфиденциальности информации.

Именно доступность, целостность и конфиденциальность (рис. 1.1) – равнозначные составляющие информационной безопасности.

Рис. 1.1. **Базовые составляющие информационной безопасности**

Доступность информации

Информационные системы создаются для получения определенных информационных услуг. Если по тем или

иным причинам предоставить эти услуги пользователям становится невозможно, то это, очевидно, наносит ущерб всем пользователям.

Роль доступности информации особенно проявляется в разного рода системах управления – производством, транспортом и др. Менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество 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 есть важнейший аспект 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 также неточный перевод инструкции по применению лекарственного препарата может нанести вред 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 лишено 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, анкетные данные сотрудников и др. Применительно к вычислительным системам в обязательном порядке конфиденциальные данные – пароли для доступа к системе.

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

Нарушение каждой из трех категорий приводит к нарушению информационной безопасности в целом. Так, на-

рушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

Как уже отмечалось, выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности. Кроме этого, 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 – задача комплексная. 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 закономерно 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 по минимизации всех отрицательных последствий от всеобщей информатизации и содействия развитию всего общества при использовании информации как ресурса его развития.

В этой связи основные задачи информационной безопасности в широком смысле следующие:

- 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, в узком смысле существуют 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 обязательны, 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 жиз-

ненного 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 др.).

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 др. 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, шифрование данных можно выполнить встроенной в операционную систему файловой шифрующей системой EFS (Windows XP) или специальной программой шифрования.

Подчеркнем, что формирование режима информационной безопасности является сложной системной задачей, решение которой в разных странах отличается по содержанию и зависит от таких факторов, как научный потенциал страны, степень внедрения средств информатизации в жизнь общества и 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.

Основополагающие документы по информационной безопасности в Российской Федерации – 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, утвержденная Президентом РФ от 9 сентября 2000 г. №Пр-1895, 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 др. 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.

Федеральный закон «Об информации информационных технологиях и о защите информации», 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 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].

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 ор-

---

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

ганизации 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.

Основные документы в этом направлении следующие:

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

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

- *ст. 138.* Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений;
- *ст. 140.* Отказ в предоставлении гражданину информации;
- *ст. 183.* Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну;
- *ст. 237.* Сокрытие информации об обстоятельствах, создающих опасность для жизни и здоровья людей;
- *ст. 283.* Разглашение государственной тайны;
- *ст. 284.* Утрата документов, содержащих государственную тайну.

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

- *ст.* 272. Неправомерный доступ к компьютерной информации.

1. Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере от 200 до 500 минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев, либо исправительными работами на срок от 6 месяцев до 1 года, либо лишением свободы на срок до 2-х лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от 500 до 800 минимальных размеров оплаты труда или в размере заработной платы или другого дохода осужденного за период от 5 до 8 месяцев, либо исправительными работами на срок от 1 года до 2-х лет, либо арестом на срок от 3 до 6 месяцев, либо лишением свободы на срок до 5 лет.

- *ст.* 273. Создание, использование и распространение вредоносных программ для ЭВМ.

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, – наказывается лишением свободы на срок до 3 лет со штрафом в размере от 200 до 500 минимальных разме-

ров оплаты труда или в размере заработной платы или иного дохода осужденного за период от 2 до 5 месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от 3 до 7 лет.

- *ст. 274.* Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет, либо обязательными работами на срок от 180 до 200 сорока часов, либо ограничением свободы на срок до 2 лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до 4 лет.

1.4. Стандарты информационной безопасности

1.4.1. Требования безопасности к информационным системам

Стандарт ISO/IEC 15408 *«Критерии оценки безопасности информационных технологий»* (издан 1 декабря 1999 г.) относится к оценочным стандартам. Этот международный стандарт стал итогом почти 10-летней работы специалистов нескольких стран. Он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба. Именно поэтому этот 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:

- *функциональные требования* – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
- *требования доверия* – соответствуют пассивному аспекту – предъявляемые 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 определенных организации и/или информационной системы.

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*.

---

[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». Данный труд, называемый чаще всего по цвету обложки «Оранжевой книгой», был впервые опубликован в августе 1983 г.

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 определенной 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 путем добавления 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 количество аналогичных понятий в «Оранжевой книге». «Общие критерии» включают следующие *классы функциональных требований:*

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

Рассмотрим содержание одного из классов.

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

Отказоустойчивость. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В стандарте различаются актив-

ная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

Обслуживание по приоритетам. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.

Распределение ресурсов. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

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

«Общие критерии» – достаточно продуманный и полный документ с точки зрения 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:

1) разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);

2) поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
3) тестирование;
4) оценка уязвимостей (включая оценку стойкости функций безопасности);
5) поставка и эксплуатация;
6) управление конфигурацией;
7) руководства (требования к эксплуатационной документации);
8) поддержка доверия (для поддержки этапов жизненного цикла после сертификации);
9) оценка профиля защиты;
10) оценка задания по безопасности.

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

Степень доверия возрастает от первого к седьмому уровню. Так, оценочный уровень доверия 1 (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. Данный 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 цифровая подпись;
- механизм управления доступом;
- механизм контроля целостности данных;
- механизм аутентификации;

- механизм дополнения трафика;
- механизм управления маршрутизацией;
- механизм нотаризации (заверения).

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

Таблица 1.1

Взаимосвязь функций и механизмов безопасности

Функции	Механизмы							
	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	–	+	–	+	–	–	–	+

«+» механизм используется для реализации данной функцию безопасности;
«-» механизм не используется для реализации данной функции безопасности.

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. Например, 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.

Администрирование сервисов безопасности включает в себя 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 др.);
- управление аутентификацией (распределение информации, необходимой для аутентификации – паролей, ключей и др.);

- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений – частоту отправки, размер и др.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

В 1987 г. Национальным центром компьютерной безопасности США была опубликована интерпретация «Оранжевой книги» для сетевых конфигураций. Данный 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 др.);
- наличие средств реконфигурирования для изоляции и/или замены узлов или 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

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. №1085, она 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[1].

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 с точки зрения 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 – орган 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]Режим доступа: http://www.fstec.ru/

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 – лишь отправные нормативные базис информационной безопасности. Основой практического построения комплексной системы безопасности служит административный уровень, определяющий главные направления работ по защите информационных систем.

Целями административного уровня являются разработка программы работ в области информационной безопасности и обеспечение ее выполнения в определенных условиях функционирования информационной системы.

Задачи административного уровня состоят в разработке и реализации практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем.

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

Административный уровень содержит следующие мероприятия:

1) разработку политики безопасности;
2) анализ угроз и расчет рисков;
3) выбор механизмов и средств обеспечения информационной безопасности.

1.7.2. Разработка политики информационной безопасности

Разработка политики безопасности ведется для определенных 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 этого, 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 систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности.

Этот документ – методологическая основа 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 др.;
- *программное обеспечение* – приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и др.;
- *данные* – хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и др.;
- *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 разграни-

чить их права и обязанности, связанные с их непосредственной деятельностью.

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

- специалист по информационной безопасности;
- владелец информации;
- поставщики аппаратного и программного обеспечения;
- администратор сети;
- 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 др.).

Владелец информации – лицо, непосредственно владеющее информацией и работающее с ней. В большинстве случае 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 – промежуточное звено 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 какой ущерб 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 являются второй важной функцией административного уровня обеспечения информационной безопасности. Во многом облик разрабатываемой системы защиты и состав механизмов ее реализации определяется потенциальными 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, называются *злоумышленниками*.

Чаще всего угроза есть следствие наличия уязвимых мест в защите информационных систем, например, неконтролируемый доступ к персональным компьютерам или нелицен-

зионное программное обеспечение (к сожалению даже лицензионное программное обеспечение не лишено уязвимостей).

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

В этой связи более приемлемый другой способ – способ упреждающей защиты, заключающийся в разработке 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:

- *составляющим информационной безопасности* (доступность, целостность, конфиденциальность), против которых, в первую очередь, направлены угрозы;
- *компонентам информационных систем*, на которые угрозы нацелены (данные, программы, аппаратура, персонал);
- *характеру воздействия* (случайные или преднамеренные, действия природного или техногенного характера);
- *расположению источника угроз* (внутри или вне рассматриваемой информационной системы).

Рис. 1.2. **Классификация угроз информационной безопасности**

Отправной точкой при анализе угроз информационной безопасности служит 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.

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 др.

Угрозы, классифицируемые *по расположению источника угроз*, бывают *внутренние* и *внешние*.

Внешние угрозы обусловлены применением вычислительных сетей и создание 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, позво-

лющим нанести ущерб любой из составляющих информационной безопасности является *несанкционированный доступ (НСД)*. Несанкционированный доступ возможен из-за ошибок в системе защиты, нерационального выбора средств защиты, их некорректной установки и настройки.

Каналы НСД классифицируются по компонентам автоматизированных информационных систем.

Через человека:

- хищение носителей информации;
- чтение информации с экрана или клавиатуры;
- чтение информации из распечатки.

Через программу:

- перехват паролей;
- расшифровка зашифрованной информации;
- копирование информации с носителя.

Через аппаратуру:

- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и др.

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 разведывательной информацией 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*.

Основные источники образования технических каналов утечки любой, в том числе конфиденциальной, информации следующие:

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

Примером реализации системы преобразователей служит 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 др.

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 этой 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 др.) или условия для работы пользователей (система кондиционирования и др.).

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 др. токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются **посторонними проводниками** и то же 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).

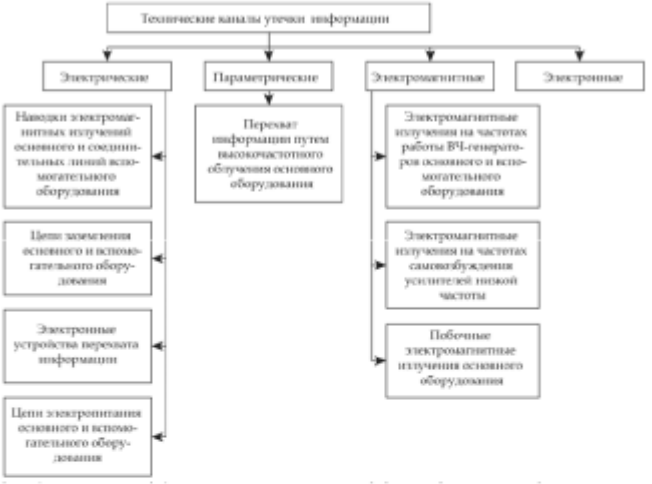


Рис. 1.3. **Технические каналы утечки информации**

Электромагнитные каналы утечки информации. К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений (ПЭМИ) основного и вспомогательного оборудования:

- излучений элементов 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 кото-

рого (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 основного и вспомогательного оборудования входят различного рода высокочастотные 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 др.

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 др. Приемники электрического поля – провода высокочастотных цепей и др. 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 др. К распределенным случайным антеннам относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и др. 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

Самые частые и самые опасные (с точки зрения размера ущерба) – *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 классифицируются 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 др.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и др.).

Основные источники внутренних отказов следующие:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и др.);
- 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, нанесенных информационным системам.

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.

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

Цели такого программного обеспечения следующие:

- 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 определенных вариантов отдельно взятого вируса, а всего «семейства» или даже целого класса вредоносных программ).

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

Подробный анализ данного класса угроз и методы их предотвращения рассмотрены в гл. 4.

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.

В целях 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 точки зрения нарушения целостности не только данные, но и программы. Внедрение рассмотренного ранее вредоносного программного обеспечения – пример подобного нарушения.

Угрозы динамической целостности – дублирование данных или внесение дополнительных сообщений (сетевых пакетов и др.). 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 др. 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 др.), но идея одна – осуществить доступ к данным в тот момент, когда они наименее защищены.

Перехват данных – очень серьезная угроза, и если конфиденциальность действительно является критичной, 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 – угроза 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 др. 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: учебно-практическое пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К. – М.: Изд. центр ЕАОИ, 2010.
2. Галатенко В.А. Основы информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ.РУ, 2003.

3. Галатенко В.А. Стандарты информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ.РУ, 2004.
4. Завгородний В.И. Комплексная защита в компьютерных системах: учеб. пособие. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001.
5. Карпов Е.А., Котенко И.В., Котухов М.М., Марков А.С., Парр Г.А., Рунеев А.Ю. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / под редакцией И.В. Котенко. – СПб.: ВУС, 2000.
6. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов – М.: Горячая линия – Телеком, 2004 .
7. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издательство Молгачева С.В., 2001
8. Руководящие документы ФСТЭК и ГОСТы Российской Федерации по защите информации, а также другая литература по анализу требований к информационной безопасности, размещенные на сайте: http://www.volgablob.ru/wiki/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 ПО и информационная безопасность

Вредоносные программы одна из главных угроз информационной безопасности. Это связано с масштабностью распространения этого явления и, как следствие, огромного ущерба, наносимого информационным системам.

Вредоносные программы создаются специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К данной 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

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

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».

2.1.2. Хронология развития вредоносных программ

Термин *«компьютерный вирус»* появился в середине 1980-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, сетевые черви, 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 др. объекты, скрытность, потенциальная опасность и др.) либо присущи другим программам, которые никакого отношения не имеют к вирусам, либо существуют вирусы, которые не содержат указанных ранее отличительных черт (за исключением возможности распространения).

Приведем одно из общепринятых определений вируса, содержащееся в ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

«Программный вирус» – это исполняемый или интерпретируемый программный код, обладающий свойством несанкцио-

нированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях в целях изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах.

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 половине 1970-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 1980-х гг. компьютеры становятся все более и более популярными. Появляется все больше и больше программ, начинают развиваться глобальные сети. Результатом этого стало появление большого количества 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» было, скорее всего, неготов-

ность 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-го мая 1988-го г. сразу несколько фирм и университетов нескольких стран мира «познакомились» с вирусом «Jerusalem» – в этот день вирус уничтожал файлы при их запуске. Вместе с несколькими другими вирусами, 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 полгода, 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 году 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, количество 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 аре-

стована 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 1990-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. В это же время появляется супервирус – «Чернобыль» – исполняемый вирус под Windows, имеющий следующие особенности. 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 об-

разуется 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 этот вирус.

2000 г. еще можно назвать годом «Любовных Писем». Вирус «LoveLetter», обнаруженный 5 мая, мгновенно разлетелся по всему миру, поразив десятки млн компьютеров практически во всех уголках планеты. Причины этой глобальной эпидемии кроются в чрезвычайно высокой скорости распространения. Вирус рассылал свои копии немедленно после заражения системы 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 века 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 преоб-

ладают 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 др. 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 последующих 2005 и 2006 гг. «громких» инцидентов практически не происходило, но зато двукратно возросло количество разнообразных троянских программ, которые распространялись самыми разными способами: через интернет-пейджеры, веб-сайты, с помощью 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: Lasco – первый пример вируса, не только рассылавшего себя на др. телефоны, но и заражавшего исполняемые файлы Symbian. 4 мар-

та 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 др. 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 для защиты электронной почты для Microsoft Exchange, а 20 июля объявлено о покупке FrontBridge Technologies, разрабатывавшей технологии фильтрации сетевого трафика. Также в 2005 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 о данной уязвимости была опубликована до выхода соответствующего 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.

В заключение нашего небольшого исторического обзора несколько слов о том, что мы имеем сегодня и какие прогнозы на будущее в области борьбы с вредоносным программным обеспечением.

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

Лаборатории Касперского[1], где в отчете за 2011 г. говорится: «Эксперты отметили стремительный рост количества вредоносных писем в спаме на фоне общего снижения доли мусорных сообщений в почтовом трафике. Приемы социальной инженерии в нежелательной почте становятся все изощренней, а спамеры занимаются саморекламой все активнее»[2].

2.1.3. Классификация вредоносного программного обеспечения

К вредоносному программному обеспечению 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[3].

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

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

Пути распространения большинства известных червей следующие:

- 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 др.

Некоторые черви распространяются в виде сетевых пакетов и проникают непосредственно в память компьютера и там самостоятельно активизируют свой код – это так называе-

[1] http://www.securelist.com/ru/encyclopedia
[2] http://wegasat.ru/news-science/497-otchet-laboratorii-kasperskogo
[3] Касперский Е. Компьютерное зловредство. – СПб.: Питер, 2009.

мые «бесфайловые» или «пакетные» черви (например, CodeRed и Slammer).

Классические компьютерные вирусы – это программы, распространяющие свои копии по ресурсам локального компьютера в целях:

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

В отличие от червей, вирусы не используют сетевые сервисы для проникновения в др. 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.

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 ра-

боты 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 количество других операционных систем и приложений, для которых вредоносные программы пока не обнаружены. Что является причиной существования вредных программ в одних системах и отсутствия их в других?

Причиной появления подобных программ, как указывают эксперты Лаборатории Касперского[1], в определенной

[1] http://www.securelist.com/ru/encyclopedia

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 – необходимо, а выполнение всех условий одновременно, – достаточно для появления 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 рано или поздно хакеры и вирусописатели попытаются воспользоваться ей в своих интересах.

Напрашивается естественный вывод: чем популярнее операционная система или приложение, тем чаще она будет 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 поддержкой 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 др. 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 программного обеспечения.

Антивирусная программа – программа, предназначенная 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» – детектирование вируса в незараженном объекте (файле, секторе или системной памяти).

«Пропуск вируса» – недетектирование вируса в зараженном объекте.

«Сканирование по запросу» – поиск вирусов по запросу пользователя. В этом 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 др.). 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 – важный метод 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 всего вас защитит надежная антивирусная защита и защита 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, со-

общениям на интернет-пейджеры. Категорически не следует открывать файлы и ссылки, приходящие из неизвестного источника. Риск заражения снижается также с помощью 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 количеству веб-страниц;
- физическое отключение внутренней сети предприятия от интернета и использование для выхода в интернет выделенных компьютеров и др.;

К сожалению, жесткие ограничительные меры могут конфликтовать с пожеланиями каждого 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 (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 др.).
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 программного обеспечения.

Классификация таких вредоносных программ практически идентична компьютерным «вредителям», это:

- 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 шесть платформ, подверженных заражению.

---

[1] При написании этой главы использованы материалы сайтов:
http://www.securelist.com/ru/analysis/199611795/Vvedenie_v_mobilnuyu_virusologiyu_chast_I
http://www.securelist.com/ru/analysis/199886717/Vvedenie_v_mobilnuyu_virusologiyu_chast_II
http://www.securelist.com/ru/analysis/208050548/Mobilnaya_virusologiya_chast_3
http://www.procontent.ru/media/presentations/ahconferences2007/Kaspersky.pdf

Таблица 2.1

Платформы подверженных заражению

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

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.

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. Основные их них следующие:

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

- 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.

Некоторые вредоносные программы для мобильных устройств такие.

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 Micro Edition. 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 30 странах мира. ComWar – это первый червь, распространяющийся через MMS. Как и Cabir, он способен рассылаться через Bluetooth, однако именно MMS его основной способ размножения, и, если учитывать его масштаб, наиболее опасный 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.

Важнейшие факторы распространения вредоносных программ на мобильных устройствах – уязвимости в исполь-

зуемом программном обеспечении и 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, однако в настоящее время, вместо глобальных эпидемий червей наблюдаются локальные вспышки заражений, ориентированные на жителей одной страны или одного региона. По данным экспертов регионами, для которых проблема мобильных вирусов наиболее актуальна, являются Россия, Китай, Индонезия и страны Западной Европы.

2.2.3. Защита мобильных устройств

Мобильный телефон, как маленький компьютер с 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 стоит устанавливать не подписанное 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 не зараженным, 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». «Монитор» 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.

Эта 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 Антивирус Касперского Mobile Security для платформ Symbian & Windows Mobile, который обеспечивает все необходимые проверки сообщений.

Литература к главе 2

1. Домарев В.В Безопасность информационных технологий. Методология создания систем защиты. – М.: Диа-Софт, 2002.
2. Касперский Е. Компьютерные вирусы – Электронная энциклопедия. – Режим доступа к энциклопедии: http://www.viruslist.com/viruslistbooks.html
3. Касперский Е. Компьютерное зловредство. – СПб.: Питер, 2009.
4. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003.
5. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: 2006.

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.

В современных методиках анализа и оценки рисков, в сфере информационной безопасности (ИБ) [2] используется ряд понятий.

В соответствии с ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения», BS 7799-3:2006 «Система управления ИБ. Руководство по управлению 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 сис-

теме 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 предъявляется повышенных требований в области ИБ.

Полный *(Full)* ***анализ рисков*** – анализ рисков для информационных систем, предъявляющих повышенные требования в области ИБ. Включает в себя определение ценности инфор-

мационных ресурсов, оценку угроз и уязвимостей, выбор адекватных контрмер, оценку их эффективности.

Риск нарушения ИБ *(Security Risk)* – возможность реализации угрозы.

Оценка рисков *(Risk Assessment)* – идентификация рисков, выбор параметров для их описания и получение оценок по этим параметрам.

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 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» выделяются следующие типы ресурсов (рис. 3.1):

- *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.

Рис. 3.1. **Типы ресурсов**

Схема управления рисками информационной безопасности приведена на рис. 3.2.

Рис. 3.2. **Управление рисками ИБ**

При ***анализе рисков***, *ожидаемый ущерб*, в случае реализации угроз, сравнивается с затратами на меры и средства защиты, после чего принимается решение в отношении оцениваемого риска, который может быть:

- *снижен*, например, за счет внедрения средств и механизмов защиты, уменьшающих вероятность реализации угрозы или коэффициент разрушительности;
- *устранен*, за счет отказа от использования подверженного угрозе ресурса;
- *перенесен*, например, застрахован, в результате чего в случае реализации угрозы безопасности, потери будет нести страховая компания, а не владелец ИС;
- *принят*.

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 точки зрения информационной безопасности. 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.

На третьем уровне руководство организации осознает задачи в области ИБ и заинтересовано в использовании стан-

дартов 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 на рис. 3.3 приведено графическое изображение модели зрелости[2],

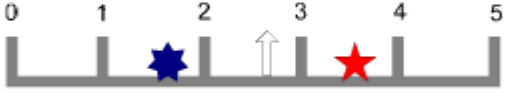


Рис. 3.3. **Графическое изображение модели зрелости**

где ✸ – текущее положение организации;

⇧ – средний показатель для отрасли;

★ – цель организации.

---

[1] Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М.: « ДМК Пресс», 2005. – 383 с.

[2] COBIT 4.1 Российское издание. – М: «Аудит и контроль информационных систем», 2008. – 234 с.

По данным исследований большинство российских компаний находятся ниже третьего уровня зрелости[1]. Однако наблюдается стремление к повышению уровня зрелости с точки зрения информационной безопасности. Инструментом, позволяющим принимать эффективные решения по минимизации последствий нарушения безопасности информации и вероятности их наступления, а также выбору защитных мер, является управление рисками.

Управление рисками – это скоординированные действия по управлению и контролю организации в отношении риска, которые включают в себя *оценку риска, обработку риска, принятие риска* и *сообщение о риске*.[2]

Наиболее трудоемким является процесс оценки рисков, который условно можно разделить на следующие этапы:

- идентификация риска;
- анализ риска;
- оценивание риска.[3]

На рис. 3.4 схематично изображен процесс оценки рисков информационной безопасности.

Рис. 3.4. **Процесс оценки рисков информационной безопасности**

[1] Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М.: « ДМК Пресс», 2005. – 383 с

[2] ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения»

[3] ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»

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

Выделяются следующие типы объектов защиты (см. рис. 3.1):

- информационные активы;
- программное обеспечение;
- физические активы;
- сервисы;
- люди, а также их квалификации, навыки и опыт;
- нематериальные ресурсы, такие как репутация и имидж организации[1].

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

На этапе идентификации рисков так же выполняется идентификация угроз и уязвимостей. В качестве исходных данных для этого используются 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;
- вероятности наступления такого нарушения;
- размеры риска.

Возможный ущерб формируется с учетом стоимости активов и тяжести последствий нарушения их безопасности.

Выделяется три подхода к оценке стоимости активов[2], а именно:

- затратный (затраты, необходимые для создания актива);

---

[1] ISO/IEC 17799-2005 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью»

[2] Федеральный стандарт оценки №1 «Общие понятия оценки, подходы к оценке и требования к проведению оценки»

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

Затем полученные различными подходами результаты обобщаются, получается интегрированная оценка 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 размер возможного ущерба и вероятность реализации угроз, определяется размер риска. Размер рисков вычисляется путем комбинирования возможного ущерба, выражающего вероятные последствия нарушения безопасности активов, и вероятности реализации угроз. Такое комбинирование часто осуществляется с помощью матрицы, где в строках размещаются возможные значения ущерба, а в столбцах – вероятности реализации угрозы, на пересечение – величина риска.

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

Результаты оценки рисков используются для определения экономической целесообразности и приоритетности проведения мероприятий по обработке рисков, позволяют обос-

нованно принять решение по выбору защитных мер, снижающих уровни рисков.

Возможны следующие способы обработки рисков (рис. 3.5):

- принятие рисков;
- уменьшение рисков;
- избежание рисков;
- передача рисков.

Рис. 3.5. **Способы обработки рисков**

Уменьшение риска заключается в подборе и внедрении соответствующих защитных мер, позволяющих уменьшить размер риска до приемлемого уровня.

При выборе защитных мер необходимо учитывать стоимость их приобретения, разработки, внедрения, а также соотношение полученного значения с возможным ущербом в результате реализации угроз. Следует учитывать совместимость планируемых к внедрению и уже используемых защитных мер, а также защитных мер, направленных на снижение других выявленных рисков.

Избежание риска связано с отказом от использования объектов защиты, в результате чего риск полностью исключается.

Передача риска третьей стороне может быть выбрана в случае, если сложно уменьшить риск до приемлемого уровня или контролировать его, либо передача этого риска экономически более оправдана. В качестве третьей стороны может выступать страховая компания или организация, предоставляющая услуги по аутсорсингу информационной безопасности.

Далее выполняется оценка остаточных рисков. Если остаточный риск является неприемлемым, должно быть принято решение о том, как его уменьшить до приемлемого уровня.

Уменьшение всех рисков до приемлемого уровня не всегда возможно или осуществимо с финансовой точки зрения. В этих обстоятельствах может возникнуть необходимость принять риск. Принимаемые остаточные риски должны быть документируются и утверждаются руководством.

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 стандарт ISO/IEC 27005:2008 «Информационные технологии – Методы обеспечения безопасности – Управление рисками информационной безопасности». Данный стандарт заменит 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

[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.

управления рисками, перечисленные в его библиографическом списке: ISO Guide 73, AS/NZS 4360 и NIST SP 800-30.[1]

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

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

[1] http://www.iso27000.ru/blogi/aleksandr-astahov/russkaya-redakciya-iso-27005-na-podhode А. Астахов «Русская редакция ISO 27005 «на подходе».

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 SP 800-30 должен включать процесс управления рисками, показаны на рис. 3.7.

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

Описание рекомендуется делать в соответствии со следующим планом:

- аппаратные средства ИС, их конфигурация;
- используемое ПО;
- интерфейсы системы, 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;
- формальные требования в области ИБ, применимые к данной ИС (законодательство, ведомственные стандарты и др.);
- 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 др.);
- организация физической безопасности;

- управление и контроль внешней по отношению к ИС средой (климатическими параметрами, электропитанием, защитой от затоплений, агрессивной среды и др.).

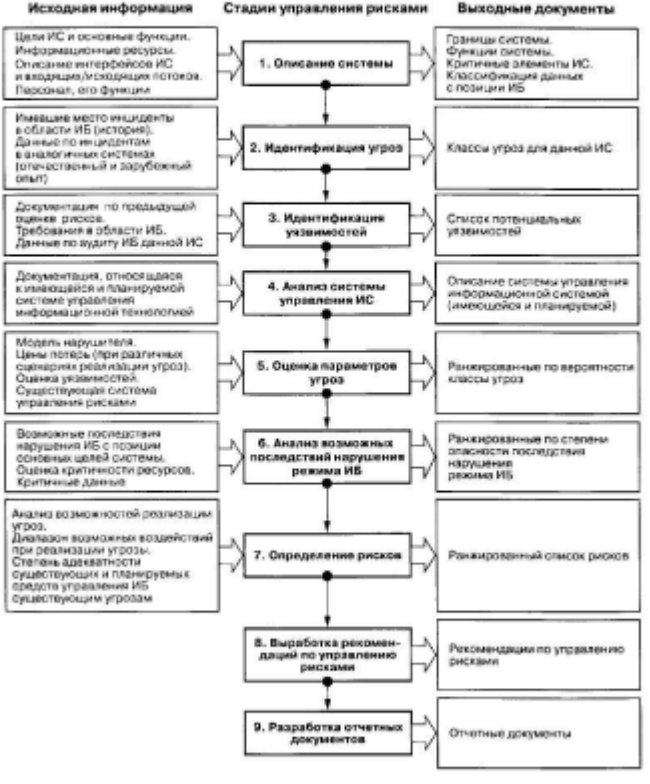


Рис. 3.7. **Процесс управления рисками NIST SP 80-30**

Для получения информации по перечисленным пунктам на практике рекомендуется использовать:

- разнообразные вопросники (check-листы), которые могут быть адресованы к различным группам управленческого и обслуживающего персонала;
- интервью аналитиков, 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 описываются, кто может выступать в качестве нарушителя, возможности и мотивы нарушителя, сценарий реализации угрозы.

Итогом данного этапа 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 принимаются во внимание существующие процедуры и методы обеспечения режима информационной безопасности, данные внутреннего аудита и результаты анализа имевших место инцидентов.

Затем выполняется выбор шкал для оценки параметров рисков. Наиболее распространенная шкала – качественная шкала с несколькими градациями. Оценка проводится экспертом.

С использованием шкал выполняется оценка тяжесть последствия нарушения ИБ и вероятности реализации угроз. Затем измеряется уровень рисков путем комбинирования 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.

Следующий шаг – выработка рекомендаций по управлению рисками. Рекомендации по уменьшению рисков до допустимого уровня являются необходимыми. 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 руководстве по управлению рисками в области безопасности от компании Microsoft риск определяется как вероятность того, что вследствие использования уязвимости в текущей среде пострадают конфиденциальность, целостность или доступность актива.[2] Взаимосвязь компонентов риска показана на рис. 3.8.

Рис. 3.8. **Взаимосвязь компонентов риска**

[1] Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. – М.: « ДМК Пресс», 2005. – 383 с

[2] http://www.microsoft.com/rus/technet/security/guidance/complianceandpolicies/secrisk/default.mspx Руководство по управлению рисками в области безопасности

Управление рисками представляет собой непрерывный процесс, включающий следующие 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.

Этап оценки рисков:

- планирование;
- сбор данных о рисках;
- приоритизация рисков.

Этап поддержки принятия решений:

- определение функциональных требований для снижения рисков;
- выбор возможных решений для контроля;
- проверка предложенных элементов контроля на соответствие функциональным требованиям;
- оценка снижения риска;
- оценка стоимости решения;
- определение наиболее экономически эффективного решения по нейтрализации риска путем анализа выгод и затрат.

Этап реализации контроля:

- включение персонала, процессов и технологий в решение по нейтрализации риска;
- упорядочение решений по нейтрализации риска в рамках предприятия.

Этап оценки эффективности программы управления рисками:

- разработка системы показателей рисков, оценка уровня и изменения риска;
- оценка 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 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, собираются данные по каждому из них.

Для каждого риска определяется 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 назначаются 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.

Стандарты в области управления рисками, принятые в России. В России принят ряд стандартов, регламентирующих деятельность по управлению рисками информационной безопасности:

- ГОСТ Р 51897–2002 «Менеджмент риска. Термины и определения»;
- ГОСТ Р ИСО/МЭК 13335-1–2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепции и модели менеджмента безопасности информационных и телекоммуникационных технологий»;
- ГОСТ Р ИСО/МЭК ТО 13335-3–2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий»;
- ГОСТ Р ИСО/МЭК ТО 13335-4–2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер».

ГОСТ Р 51897-2002 содержит систематизированный перечень терминов и определений в области управления рисками.

В стандартах серии 13335 описаны этапы проведения оценки рисков ИБ, подходы к оценке, правила выбора защитных мер.

Стандарты и методики оценки рисков разных стран мира. Помимо рассмотренных ранее документов по управлению рисками существует множество других, среди них:

- 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 вышеупомянутые документы распространяются бесплатно на английском языке. Данные 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 так же 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.

Тоже 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 убыт-

ки, тратить ресурсы на ликвидацию последствий. Данный подход называется реактивным.

Если подобное «тушение пожаров» организацию не устраивает, то выбирается проактивный подход. Вместо того, чтобы начинать что-то делать лишь после возникновения проблем, организация уменьшает вероятность их появления, для этого выполняется оценка и обработка рисков информационной безопасности, разрабатываются планы проведения профилактических мероприятий.

Организации, которые выбирают проактивный подход и реагирует 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 информационной безопасности необходимо определить, в качественных или количественных показателях выражать риски.

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

Существует несколько моделей качественной оценки. Все они достаточно просты, варианты различаются лишь количеством градаций шкал. Одна из самых распространенных моделей – трехуровневая. Каждый фактор оценивается по шкале «низкий – средний – высокий»[1]. 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 не был выбран, необходимо позаботиться о том, чтобы интерпретация уровней могла отражать различия между уровнями.

---

[1] Ульянов В., Анализ рисков в области информационной безопасности. – Режим доступа: http://www.risk-manage.ru/about/article27/

Трехуровневые качественные шкалы для оценки возможного ущерба, вероятности реализации угроз, размеры 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 в числовых данных, т.е. ожидаемые потери в числовом эквиваленте и вероятность или частоту этих потерь[1].

В результате количественной оценки каждому риску ставится в соответствие возможные финансовые потери в случае его реализации, что может использоваться для обоснования необходимости внедрения защитных мер, а так же рассчитывается вероятность реализации угроз, что позволяет оценить их реальную опасность.

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

Однако у данного подхода есть несколько существенных недостатков. Во-первых, не существует эффективного формализованного метода, позволяющего точно определить стоимости активов. Как, например, точно определить влияние нару-

[1] Методы анализа рисков нарушения безопасности систем управления. – Режим доступа: http://www.eav.ru/publ1.php?publid=2006-05a14

шения информационной безопасности, получившего широкую огласку, на имидж организации? Во-вторых, скрупулезная реализация всех аспектов количественного подхода требует больших затрат.[1]

Количественная оценка точнее, позволяет получить значения рисков, но отнимает 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 информационной безопасности 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 сказано 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 информационной безопасности, и др. Анализ перечисленных факторов

[1] http://www.microsoft.com/rus/technet/security/guidance/complianceandpolicies/secrisk/default.mspx Руководство по управлению рисками в области безопасности

позволяет выбрать подходящий в каждой определенной ситуации подход к оценке рисков.

Сегодня существует три подхода к оценке рисков информационной безопасности[1]:

- базовый;
- детальный;
- комбинированный.

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

Данный 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 если базовый уровень защищенности занижен, то для ряда объектов защиты выбранные меры будут недостаточны.

Если базовых оценок недостаточно, используется *детальная оценка* рисков. В этом случае для каждого объекта защиты или группы объектов защиты определяется перечень актуальных угроз и оценивается вероятность их реализации, а так же степень легкости, с которой угрозы могут реализоваться, т.е. уровень уязвимости.

Данный подход позволяет определить необходимые и достаточные защитные меры, однако связан со значительными затратами времени и средств, а также необходимостью

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

привлечения квалифицированных специалистов. Поскольку оценка проводится одинаково тщательно для всех объектов защиты организации, то определение и реализация необходимых защитных мер для какого-либо критичного объекта защиты может произойти слишком поздно, когда безопасность уже будет нарушена и организация понесет 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 этим в каждом 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 определенного 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:

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

Если нарушение безопасности объекта защиты может причинить ущерб организации, 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 данного 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]

Подобный подход является наиболее предпочтительным 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 – специалистов в рассматриваемой предметной области, путем их опроса.

На качество полученных оценок существенно влияет 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.

---

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

Данный подход не требует значительных средств или времени, однако оценки субъективны, основаны на практическом опыте определеного 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. Причем, современное программное обеспечение для оценки рисков ИБ дает возможность получения как качественных, так и количественных значений оценок [5]. На рис. 3.10 приведены наиболее популярные современные методики анализа и оценки рисков.

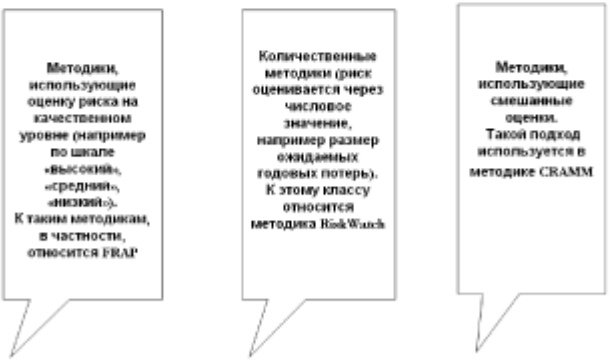


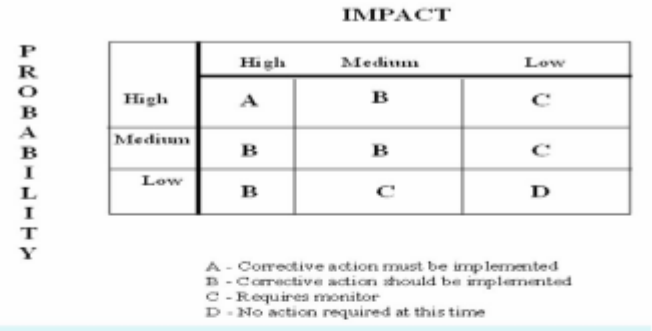
Рис. 3.10. **Методики и программные продукты для оценки рисков ИБ**

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 выбираются наиболее вероятные для данной системы;
   - анализ статистики происшествий связанных с ИБ данной информационной системы 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, оценивается уровень угрозы. Оценка проводится 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).



- *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***

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.

Чтобы использовать экономически эффективные средства защиты, необходимо проводить анализ соотношения за-

трат 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 *RiskWatch* компании *RiskWatch* представляет собой семейство программных средств для анализа рисков [8,9].

- *RiskWatch for Physical Security* – для анализа физической защиты ИС;
- *RiskWatch for Information Systems* – для информационных рисков;
- *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;
- *RiskWatch RW17799 for ISO 17799* – для оценки соответствия ИС требованиям международного стандарта *ISO 17799*.

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

В основе продукта *RiskWatch* 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 характеристики системы. Данные могут вводиться вручную или импор-

тироваться из отчетов, созданных инструментальными средствами исследования уязвимостей информационных систем. Для выявления возможных уязвимостей используется вопросник, база которого содержит более 600 вопросов. Вопросы связаны с категориями ресурсов (рис. 3.12).

Также задается 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)* – показывает, сколько раз в год в среднем данная угроза реализуется в данном месте и *SAFE (Standard Annual Frequency Estimate)* – показывает, 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.

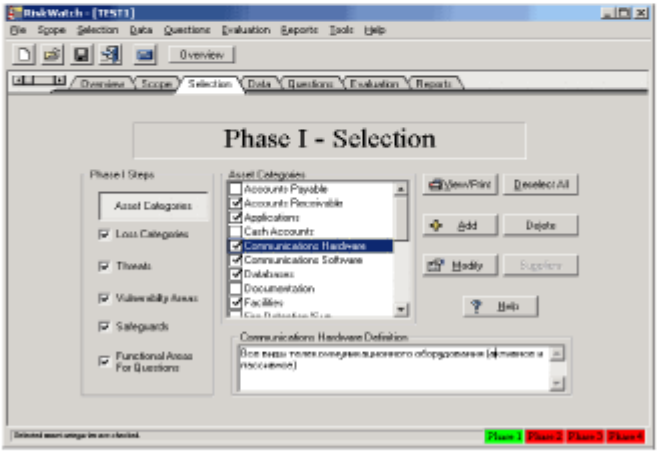


Рис. 3.12. **Определение категорий защищаемых ресурсов**

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

Третий этап – количественная оценка риска. На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности.

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

$$M=PV,$$

где M – математическое ожидание;

P – вероятность возникновения угрозы4

V – стоимость ресурса.

В связи с тем, что *RiskWatch* 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.

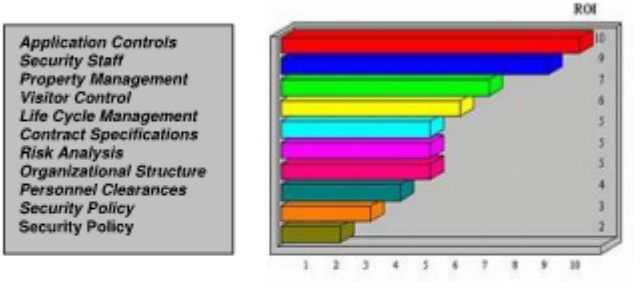


Рис. 3.14. **Пример графика показателя *ROI* для различных мер защиты**

Заметим, что методика *RiskWatch* 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 (Return on Investment* – возврат инвестиций), 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 Analysis and Management Method)* – одна из первых методик анализа рисков в сфере ИБ [6].

Работа над *CRAMM* была начата в середине 1980-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 – универсальный 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* проводятся в три стадии (рис. 3.15).

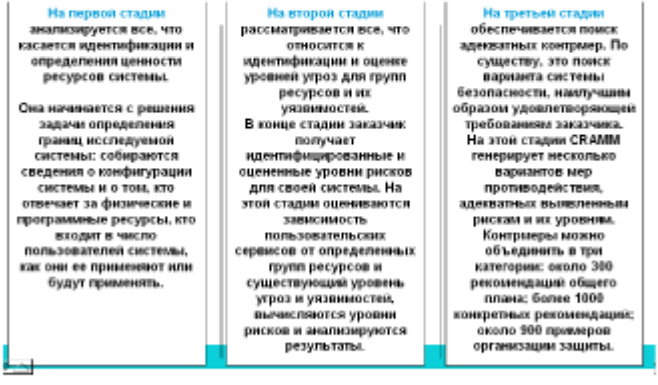


Рис. 3.15. **Методика *CRAMM***

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

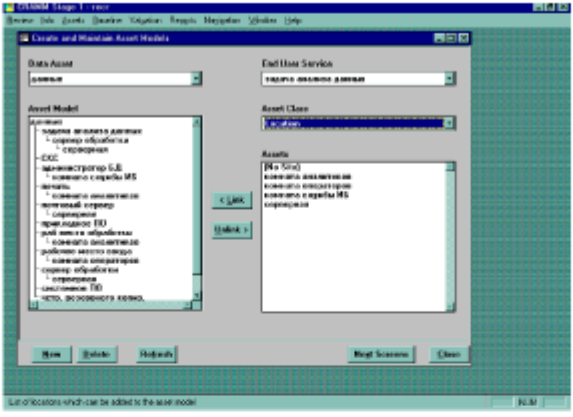


Рис. 3.16. **Идентификация ресурсов и построение модели с позиции ИБ**

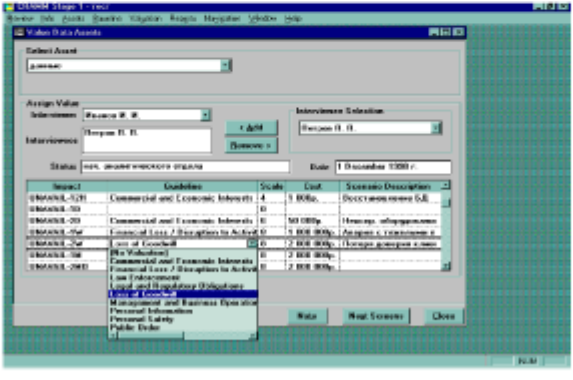


Рис. 3.17. **Оценка ценности информационных ресурсов**

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

Критерии оценки ценности ресурсов следующие:

- 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 тридцати шести 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 в целях 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.

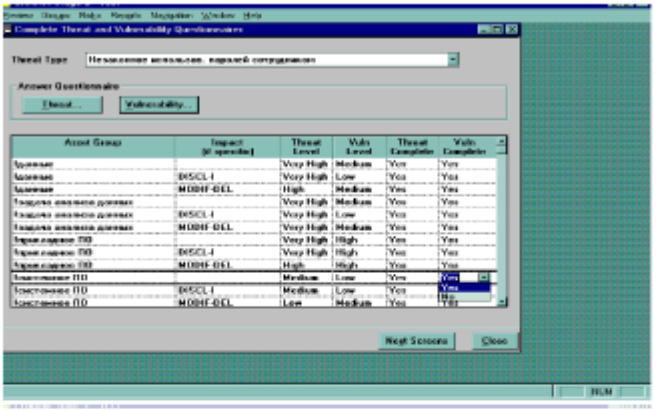


Рис. 3.18. **Угрозы и уязвимости**

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;
- ИБ информационной системы.

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 информационной системе и эффективность существующей практики по обеспечению безопасности, а также предоставить возможность доказательно (в цифрах) убедить руководство в необходимости инвестиций в сферу ее информационной безопасности[1].

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 наиболее оптимальные контрмеры, которые позволят снизить риск до необходимого уровня с наименьшими затратами.

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

На втором этапе проводится опрос ИТ-специалистов в целях 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 др.). Заключительная фаза – указание ущерба по каждой группе ценной информации, расположенной на соответствующих ресурсах, по всем видам угроз.

---

[1] Куканова Н. Современные методы и средства анализа и управления рисками информационных систем компаний. – Режим доступа: http://www.dsec.ru/about/articles/ar_compare/

На третьем этапе проходит определение всех видов пользовательских групп с указанием количества пользователей в каждой группе. Затем фиксируется, к каким группам информации на ресурсах имеет доступ каждая из групп пользователей. В заключение определяются 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 информационной безопасности 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.

В результате выполнения всех действий по данным этапам, на выходе будет сформирована полная модель информационной системы с точки зрения информационной безопасности 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.[1]

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] Методика оценки риска ГРИФ 2006 из состава Digital Security Office. – Режим доступа: http://www.dsec.ru/about/articles/grif_ar_methods/

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

В Risk Advisor реализована методика, позволяющая задать модель информационной системы с позиции информационной безопасности, идентифицировать риски, угрозы, потери в результате инцидентов. Основные этапы работы следующие: 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* описывается модель взаимодействия организации с внешним миром в нескольких аспектах: стратегическом, организационном, бизнес-цели, управление рисками, критерии. Стратегический аспект описывает сильные и слабые стороны организации с внешних позиций, варианты развития, классы угроз и отношения с партнерами.

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

Описание рисков. Задается матрица рисков на основе некоторого шаблона. Риски оцениваются по качественной шкале и разделяются на приемлемые и неприемлемые. Затем выбираются управляющие воздействия (контрмеры) с учетом зафиксированной ранее системы критериев, эффективности

контрмер и их стоимости. Стоимость и эффективность также оцениваются в качественных шкалах.

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

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

Анализ результатов. В результате построения модели можно сформировать подробный отчет (около 100 разделов), посмотреть на экране агрегированные описания в виде графа рисков. [1]

Risk Advisor позволяет автоматизировать различные аспекты управления рисками компании. При этом оценки рисков даются 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 НСД к информации и требования по защите информации различаются в российских руководящих документах и зарубежных стандартах.

В табл. 3.1 приведено сравнение рассмотренных средств оценки рисков информационной безопасности.

---

[1] Режим доступа: http://www.cnews.ru/reviews/free/security2004/ managment/ index4.shtml Методика MethodWare

Таблица 3.1

Средств оценки рисков ИБ

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 Active Directory для описания архитектуры ИС	Невысокая трудоемкость. Возможность описания разношановых 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 статистки 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 требованиям к принятию решений; получает ли он 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 информационных систем 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 служит возможность экономического обоснования расходов организации на обеспечение информационной безопасности и непрерывности бизнеса. Экономически обоснованная стратегия управления рисками позволяет, в конечном счете, экономить средства, избегая неоправданных расходов.

Использование подобного 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 есть основной недостаток подобных программ, так как указанный алгоритм «зашит» в программу и изменению не полежит, т.е. не может быть адаптирован под цели определенной организации.

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

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

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

3. Проведение анализа и оценки рисков добавляет обоснованность рекомендациям по информационной безопасности.

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 информационной системы требованиям одного из стандартов в области информационной безопасности. 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 тре-

бований. 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 данного 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 непреодолимой защиты 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 стоимости защищаемой информации (или других ресурсов – аппаратных, программных);
- затраты нарушителя на несанкционированный доступ к информации должны превышать тот эффект, который он получит, осуществив подобный доступ.

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

<Частота> × <Вероятность> × <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 с точки зрения 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.

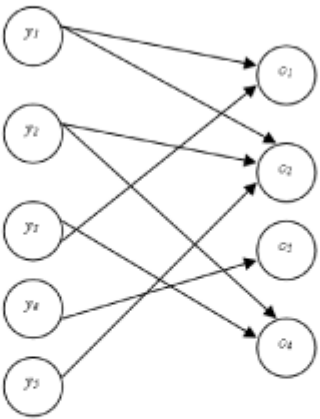


Рис. 3.20. **Пример модели процесса защиты информации в виде двудольного графа**

Следует отметить, что связь между угрозами и объектами не является связью типа «один к одному» – угроза может распространяться на любое количество 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.

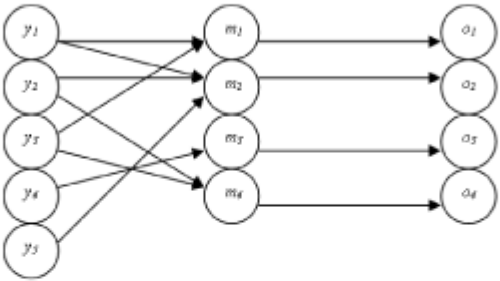


Рис. 3.21. **Пример модели процесса защиты информации в виде трехдольного графа**

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 $T \times O$ 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 достаточно разветвленных графов. Кроме того, процесс построения и модернизации графа легко выполняется с использованием программного обеспечения.

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, предоставляет инструмент для моделирования рисков и угроз, используемый на протяжении всей работы. Программное обеспечение использует язык *UML* (от англ. *Unified Modeling Language* – унифицированный язык моделирования) – язык графического описания для объектного моделирования в области разработки программного обеспечения. *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 программных систем.

В программном обеспечении используются следующие элементы, представленные в табл. 3.2.

Таблица 3.2.

Элементы программного обеспечения

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

На рис. 3.22 представлено главное окно программы.

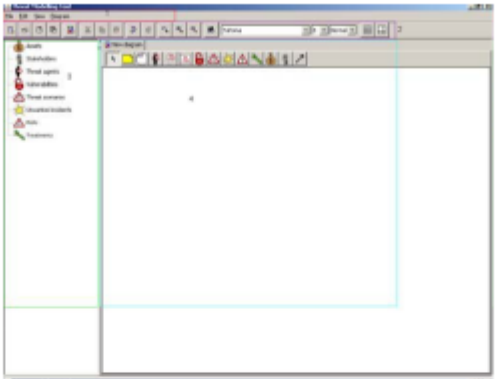
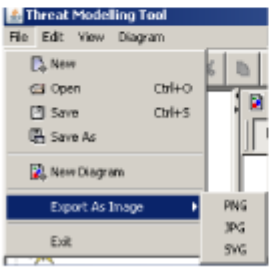


Рис. 3.22. **Главное окно программы *Coras***

Окно программы можно разделить 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.

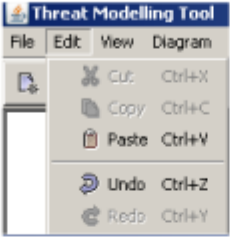
1) File/Файл (рис. 3.23);



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**

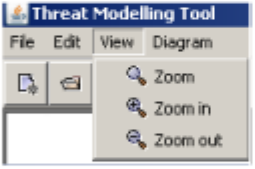
2) Edit/Редактирование (рис. 3.24);



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

Рис. 3.24. **Подменю редактирование**

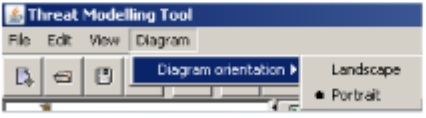
3) View/Вид (рис. 3.25);



1. Масштаб 100%.
2. Приблизить.
3. Отдалить.

Рис. 3.25. **Подменю вид**

4) Diagram/Диаграмма (рис. 3.26).



1. Ориентация:
   1.1. Альбомная.
   1.2. Книжная.

Рис. 3.26. **Подменю диаграмма**

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

Рис. 3.27. **Кнопки главного меню и поиска**

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.

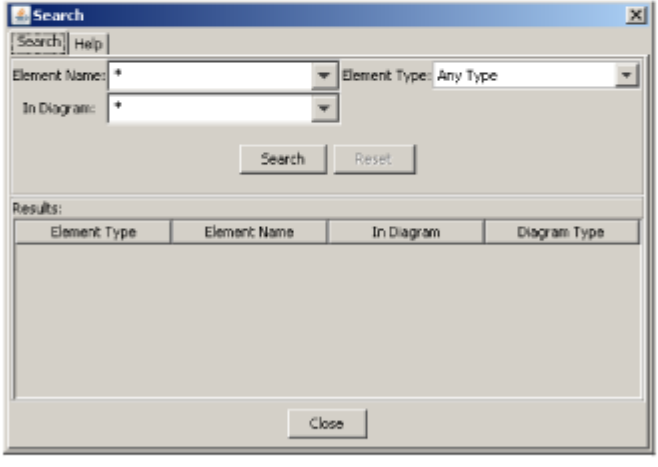


Рис. 3.28. **Окно поиска**

Шапка таблицы – условия поиска: тип элемента, его имя, название диаграммы, её тип.

После того, как поиск завершен, кнопка Reset (Сброс) становится активной. Нажатие на неё сбросит все введенные и найденные данные (рис. 3.29).

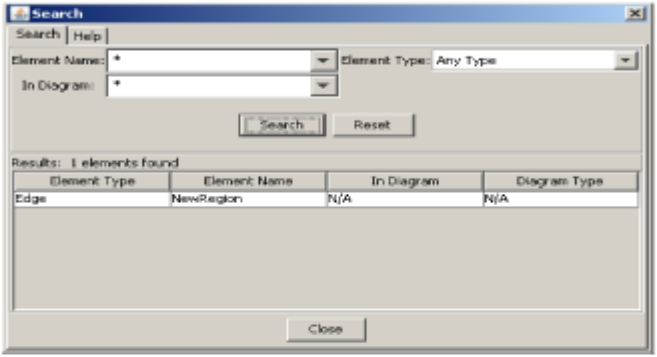


Рис. 3.29. **Результаты поиска**

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

Рис. 3.30. **Редактирование шрифта и страницы**

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

Слева расположены все объекты, используемые в данной модели угроз для анализа рисков информационной безопасности. При этом при добавлении 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 (рис. 3.31).

Рис. 3.31. **Проводник объектов, используемых в диаграмме**

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

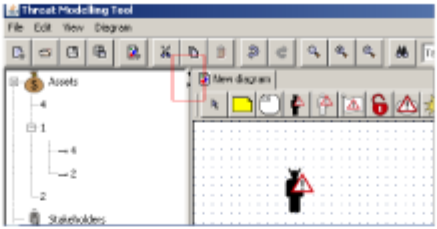


Рис. 3.32. **Скрыть/отобразить проводник**

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, 3.34). В появившемся диалоговом окне ввести имя.

Рис. 3.33. **Вкладка для работы с диаграммой**

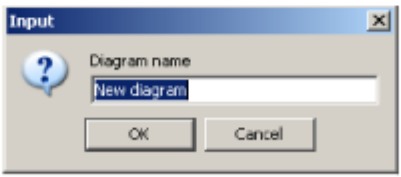


Рис. 3.34. **Изменение имени диаграммы**

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. 3.35. **Панель объектов**

Кроме перечисленных объектов (см. табл. 3.2), 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 её пределами). Первая стрелка служит для выделения, перемещения объектов, последняя (рис. 3.35) – для установления связей между объектами. Для того, чтоб установить связь, необходимо выполнить следующие действия:

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

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

3) объект начинает выделаться синим цветом;

4) не отпуская кнопки мыши, переводим её на объект, являющийся окончанием связи;

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

Установление связей необходимо для генерирования модели рисков.

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

Методология анализа безопасности *Coras* включает в себя семь этапов.

1. Вводная встреча. Целью этого этапа является 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 др. 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 будут 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].

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

Приложение 3.1.

Применение модели с полным перекрытием для анализа рисков информационной безопасности малого предприятия

Постановка задачи: Постройте модель защиты информации с полным перекрытием для малого предприятия, схема которого приведена на рис. П. 1.1[1].

Рис. П. 1.1. **Структурная схема предприятия**

Объекты защиты, угрозы, средства и процесс защиты представлены в табл. П. 1.1, рис. П. 1.2.

[1] В приложении 3.1 использованы материалы работы: Баранова Е.К., Чежин А.А. Анализ и управление рисками в сфере информационной безопасности малого предприятия. Сборник студ. научных работ кафедры информационной безопасности. – М.: РГСУ, 2009.

Таблица П. 1.1

Описание объектов защиты

Помещение	Объект
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	

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.

Статус обрабатываемой информации

Информация, составляющая коммерческую тайну; финансовая документация.

Таблица П. 1.2

Определение и описание множества угроз

Угроза	Описание угрозы
У1 – пожар	Угрожает всей информации, хранимой в помещениях. Приводит к нарушению работоспособности оборудования ИС, безвозвратной утрате информационных и других активов.

Угроза	Описание угрозы
	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 др.). 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)
У4 – потеря информации из-за 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

Угроза	Описание угрозы
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

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.

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, сертифицированных по требованиям защиты речевой информации.

Таблица П. 1.3

Средства защиты подсистем организации

Функциональные подсистемы	*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	

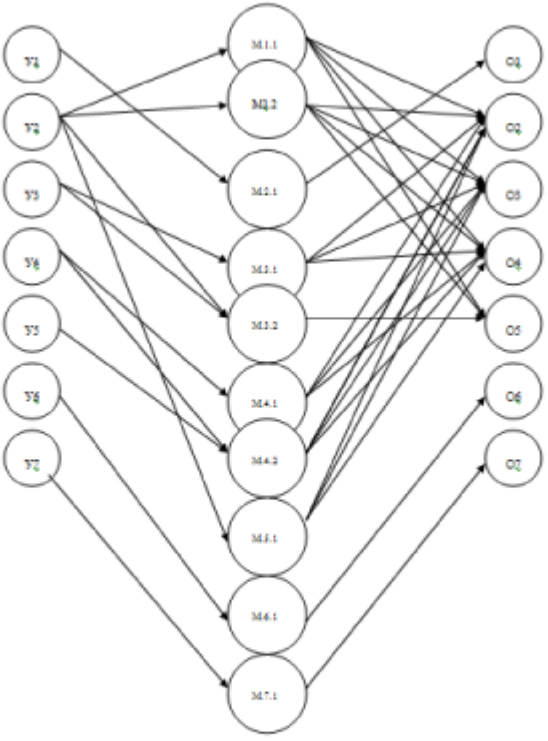


Рис. П. 1.2. **Модель процесса защиты в виде трехдольного графа**

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 определенной программы занимает от 2 до 5 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 информационной безопасности для одной из них, используя методологию Coras и соответствующее программное обеспечение.

ШАГ 1

Задача этого этапа: общее представление об объекте анализа.

Бизнес-школа (рис. П. 2.1), которая представляет собой помещение из шести комнат: приемная, учительская, совмещающая функции кабинета руководства и серверной, трёх идентичных аудиторных классов и мультимедийной лекционной аудитории. Комнаты расположены на первом (цокольном) этаже государственного университета постройки конца XIX века.

---

[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.

Рис. П. 2.1. **Схема бизнес-школы**

Возникает проблема защиты коммерческой информации, персональных данных обучающихся в этом отделении MBA, а также авторской информации (лекционных курсов преподавателей).

Для обработки защищаемой информации используется несколько компьютеров, все они находятся в помещении с окнами. Рядом с каждым компьютером есть внутренний телефон, помимо этого у приёмной и учительской имеется «выход в городскую АТС», хранилище бумажных документов находится в приёмной, серверная находится в соседнем с ней помещении – учительской. Проводная сеть основана на оптоволокне, что исключает возможность снятия информации с кабеля. Выхода в Интернет нет.

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, гарантирующим сохранение коммерческой тайны;
4) парольная защита на ресурсы;
5) помещения оборудованы системами охранной сигнализации, ИБП;
6) 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) средства пожарной безопасности;
13) стоит программа обнаружения закладок.

ШАГ 2

Целью этого этапа является более подробное изучение объекта, определение информации, подлежащей защите.

Персонал состоит из постоянного и переменного:

1) постоянный состав:
   - зав. кафедрой;
   - преподаватели – 5 человек;
   - секретарь;
   - администратор сети и безопасности;
   - сотрудники – 3 человека;
   - уборщицы – 2 человека;
2) переменный состав:
   - учащиеся.

Используя программный продукт, составим диаграмму (рис. П. 2.2) активов (ценной информации, подлежащей защите).

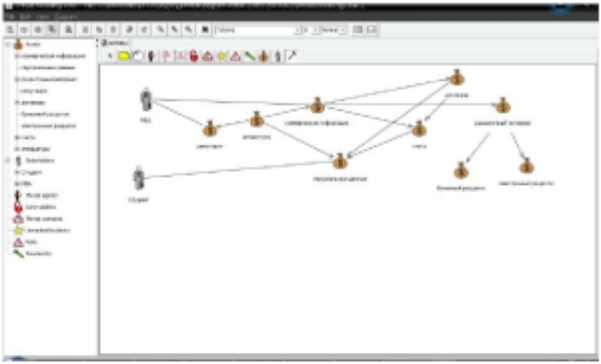


Рис. П. 2.2. **Диаграмма активов**

Элементы анализа можно представить в виде схемы (рис. П. 2.3).

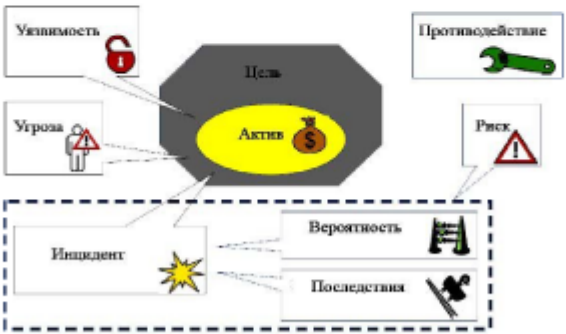


Рис. П. 2.3. **Схема элементов**

Составим табл. П. 2.1 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 П. 2.1

Риски

		
Кто/что причина?	**Как? Какой инцидент? Чему угрожает?**	**Благодаря чему стало возможным – 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. П. 2.2).

Желательно для каждого актива по каждой шкале составить описание: что значит редко, иногда, регулярно и часто в количественном отношении за определенный период времени и др.

Далее в таблицу матрицы рисков вносятся данные по тому, каким является риск: приемлемый или нет.

Таблица П. 2.2

Матрица рисков

Вероятностная шкала	**Шкала последствий нежелательных инцидентов**			
	Незначительные	**Минимальные**	**Средние**	**Катастрофические**
Редко	Приемлемый	Приемлемый	Приемлемый	Неприемлемый
Иногда	Приемлемый	Приемлемый	Неприемлемый	Неприемлемый
Регулярно	Приемлемый	Неприемлемый	Неприемлемый	Неприемлемый
Часто	Неприемлемый	Неприемлемый	Неприемлемый	Неприемлемый

Итоги этого этапа есть вероятность и вес последствий, объединенные в матрицу рисков, по которой становится понятно какой риск приемлемый, а какой нет.

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, чтоб 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. П. 2.1 строим модель угроз, изображенную на рис. П. 2.4.

Благодаря сделанным связям между активами, можно указывать воздействие на более общий актив, если данный инцидент возможен для каждого «подактива».

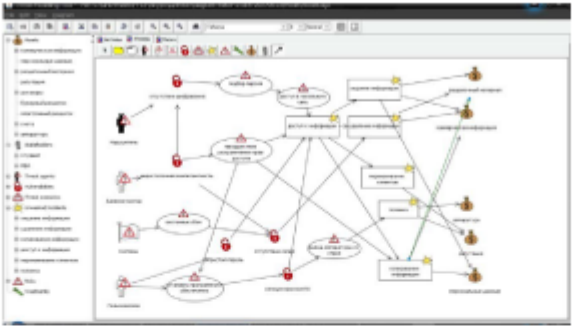


Рис. П. 2.4. **Модель угроз**

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. П. 2.5.

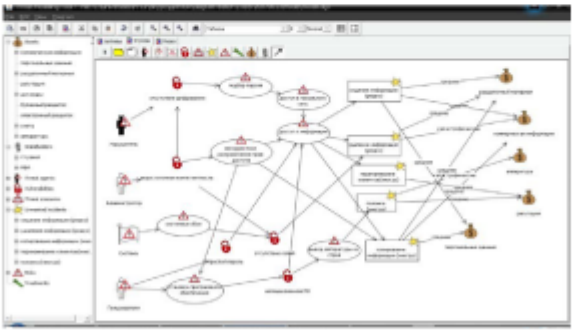


Рис. П. 2.5. **Модель угроз с вероятностными характеристиками**

ШАГ 6

Генерируем диаграмму рисков (щелкаем правой кнопкой мыши по вкладке Угрозы и выбираем Generate risk diagram). Полученная диаграмма представлена на рис. П. 2.6.

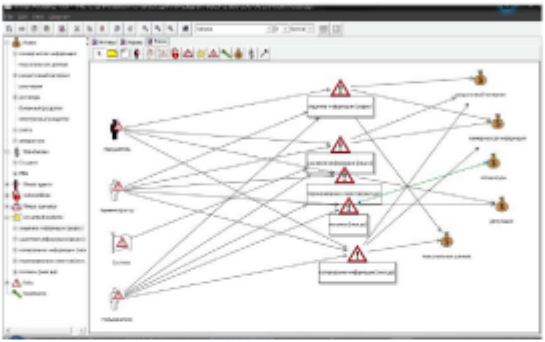


Рис. П. 2.6. **Диаграмма рисков**

Теперь по каждому риску для каждого актива определяем последствия в случае осуществления этого риска (рис. П. 2.7).

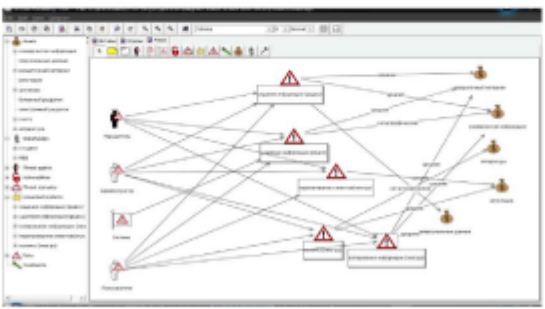


Рис. П. 2.7. **Диаграмма рисков с характеристикой последствий осуществления угрозы**

На диаграмме угроз для каждой уязвимости ставим противодействие (рис. П. 2.8).

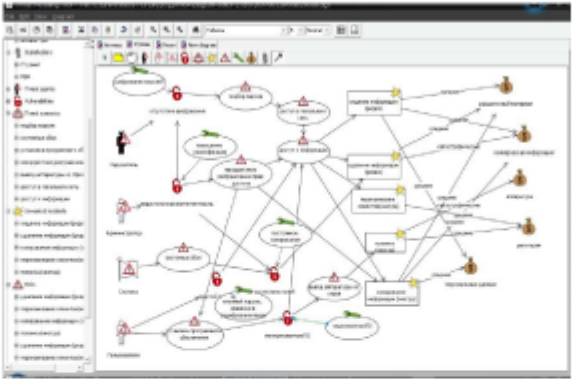


Рис. П. 2.8. **Диаграмма угроз после добавления противодействий**

ШАГ 7

В соответствии с рис. П. 2.7, занесем полученную информацию в матрицу рисков, получим следующую таблицу (таблица 3)

Таблица П. 2.3

Матрица рисков по диаграмме

Вероятностная шкала	**Шкала последствий нежелательных инцидентов**			
	Незначительные	Минимальные	Средние	Катастрофические
Редко			Хищение раздаточного материала. Хищение коммерческой информации. Хищение персональных данных.	Удаление коммерческой информации.

Вероятностная шкала	Шкала последствий нежелательных инцидентов			
	Незначительные	Минимальные	Средние	Катастрофические
			Удаление раздаточного материала.	
Иногда			Переманивание клиентов. Копирование персональных данных. Копирование раздаточного материала.	Поломка аппаратуры. Копирование коммерческой информации.
Регулярно				
Часто				

Внося поправки, в соответствии с табл. П. 2.3, получаем диаграмму неприемлемых рисков (рис. П. 2.9).

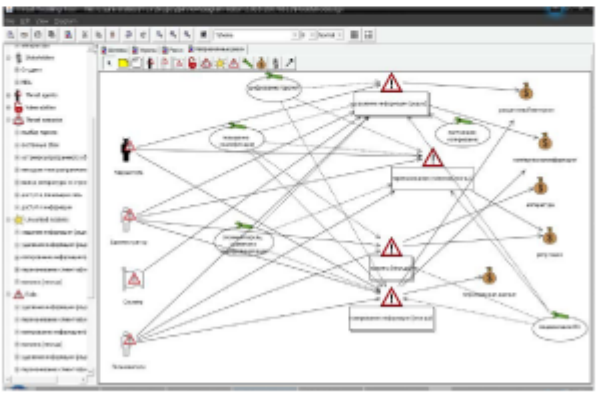


Рис. П. 2.9. **Диаграмма неприемлемых рисков**

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.

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. Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности. // Управление риском. 2009, №1(49), С.15-26.
3. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С. В. Симонов. – М.: Академия АйТи: ДМК Пресс, 2004. – 384 с.
4. Симонов С. Современные технологии анализа рисков в информационных системах // PCWEEK, 2001, №37.
5. Симонов С. Технологии и инструментарий для управления рисками. // JetInfo №2, 2003.
6. The logic behind CRAMM's assessment of measures of risk and determination of appropriate countermeasures. URL: http://www.cramm.com/downloads/techpapers.htm
7. Peltier, Thomas R. Information security risk analysis. Auerbach 2001. ISBN 0-8493-0880-1.
8. RiskWatch users manual. URL: http://www.riskwatch.com
9. 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

Общие сведения о безопасности в компьютерных сетях. Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется с помощью сетевых соединений (коаксиальный кабель, витая пара, оптоволокно) и программно с помощью 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 количеству попыток, так и по успешности их применения и, соответственно, обеспечение безопасности вычислительных сетей с точки зрения противостояния удаленным атакам приобретает первостепенное значение. Специфика распределенных вычислительных систем состоит в том, что если в локальных вычислительных сетях наиболее частыми являются угро-

зы 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 информационной безопасности 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 составляющих «информационной безопасности»:

1) целостности данных;
2) конфиденциальности данных;
3) доступности данных.

Целостность данных – одна из основных целей информационной безопасности 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 информационной безопасности как раз и связана 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 информационной безопасностью, в современных вычислительных сетях необходимо учитывать следующие факторы:

- глобальную 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 исключи-

тельно на платформе Wintel (Windows+Intel), то его практическая применимость вызывает серьезные сомнения.

Корпоративные информационные системы 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 точки зрения информационной безопасности имеет следующие особенности:

- каждый сервис имеет свою трактовку главных аспектов информационной безопасности (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, – самые разрушительные явления, которые могут 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 1960–1970-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 др. сети, именно поэтому принято считать, что сеть ARPA – предшественница 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 1970-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 бло-

ков 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, самые удачные из которых 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 др.;
- *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	Сетевой	Адресация и маршрутизация
1	Канальный	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, 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 1980-х гг. наблюдался подлинный бум, вызванный разработкой Международной организации по стандартизации коммуникационных протоколов (International Standard Organization). 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 этого была 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.

Рис. 4.1. **Сравнительная схема уровневых моделей протоколов OSI и TCP/IP**

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 др. Другими словами, соглашения должны быть приняты для всех уровней, начиная от самого низкого – уровня передачи битов – до самого высокого, реализующего сервис для пользователей сети.

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: физический, канальный, сетевой, транспортный, сеансовый, представительный и прикладной. 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 мо-

мент, 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. Пример такого протокола – 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 определенной 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 – промежуточный, 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.

Таблица 4.2

Распределение функций безопасности по уровням OSI/ISO

Функции 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.

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, связанных с подменой адресов и реализацией обходных маршрутов передачи сообщений. Адресация современного Интернета основана на протоколе IP (Internet Protocol), история которого неразрывно связана с транспортным протоколом TCP.

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 с помощью специальных IP-адресов. Каждый IP-адрес представляет собой 32-битовый идентификатор. Принято записывать IP-адреса в виде 4-х десятичных чисел, разделенных точками.

Для этого 32-х 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. 14. 229

4.4.2. Классы адресов вычислительных сетей

Каждый адрес представляет собой совокупностью двух идентификаторов: сети – NetID, и хоста – HostID. Все возможные адреса разделены на пять классов, схема которых приведена на рис. 4.2.

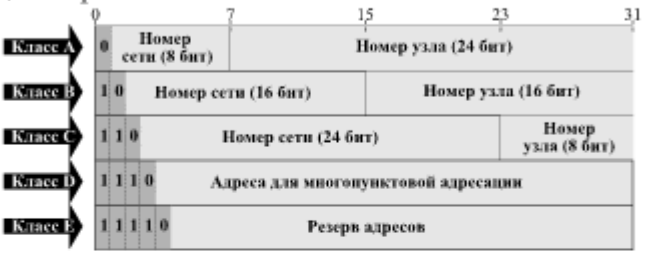


Рис. 4.2. **Классы адресов вычислительных сетей**

Из рис. 4.2 видно, что классы сетей определяют как возможное количество этих сетей, так и количество хостов в них. Практически используются только первые три класса:

Класс A определен для сетей с количеством хостов до 16777216. Под поле NetID отведено 7 бит, под поле HostID – 24 бита.

Класс B используется для среднемасштабных сетей (NetID – 14 бит, HostID – 16 бит). В каждой такой сети может быть до 65 536 хостов.

Класс C применяется для небольших сетей (NetId – 21 бит, HostID – 8 бит) с количеством хостов до 255.

4.4.3. Система доменных имен

Постоянное расширение сети Internet привело к дефициту уникальных адресов для вновь подключаемых узлов. С другой стороны, система адресации в такой сети должна быть уни-

версальной и удобной для пользователя. Последнее обстоятельство особенно было важно с началом использования ресурсов сети не только для специалистов, но и для неподготовленных пользователей, не владеющими тонкостями адресации в сети. Решающим аргументом для перехода альтернативным способам адресации в сети, удобным для работы пользователей, было неудобство запоминания 32-х битового кода, идентифицирующего отдельный узел. Это неудобство проявилось сразу же, когда сеть использовалась узким кругом специалистов. Поэтому появилась альтернативные формы записи 32-х битового IP-адреса – десятичная (195.224.11.77) и шестнадцатеричная (0xffffff80) *дот-нотации*. Последняя форма записи особенно была удобной для программистов, часто применяющих шестнадцатеричный алфавит для записи кода программы.

Впоследствии с появлением в сети различных сервисов (электронная почта и др. службы), а также с увеличением количества узлов и такая форма записи оказалась неудобной, поскольку достаточно сложно запомнить несколько цифровых адресов, даже в десятичной дот-нотации. Это обусловило появление в сети ARPANET принципиально нового способа адресации, заключающегося в присвоении узлам сети доменного имени. В данном случае правильнее говорить о новом способе именования узлов сети, поскольку доменное имя не является логическим адресом, например, как IP-адрес или физическим адресом, как, например, шестибайтовый адрес сетевого интерфейса. Доменное имя – это только лишь удобная для пользователя форма идентификации узла вычислительной сети (сервис).

Домен – группа узлов сети (хостов), объединенных общим именем, которое для удобства несет определенную смысловую нагрузку. Например, домен «*ru*» объединяет узлы на территории России, а домен «*sport*» – узлы, относящиеся к спортивным организациям или содержащие информацию о спорте и др.

В более широком смысле под доменом понимается множество узлов вычислительной сети, которые администрируются и поддерживаются как одно целое.

Доменное имя – это уникальный алфавитно-цифровой идентификатор узла (состоит из символов ASCII-кода – букв от A до Z[1] латинского алфавита и цифр от 0 до 9, также допускается дефис «-»).

Введение доменных имен поставило перед разработчиками задачу определения соответствия между доменным именем и логическим IP-адресом узла сети. Подобная задача разработчиками ARPANET была решена, когда для определения соответствия между логическим IP-адресом и физическим адресом сетевого интерфейса в пределах локальной сети были введены протоколы ARP и RARP. Однако для глобальной сети решение такой задачи более сложно.

Первоначально, когда ARPANET состояла из небольшого количества узлов, соответствие между доменными именами и IP-адресами узлов перечислялись в одном файле (hosts.txt) в виде таблицы соответствия цифрового адреса имени машины. Авторство создания этих таблиц принадлежит Джону Посте-

---

[1] Технология, предлагаемая компанией VeriSign, позволяющая использовать символы национальных алфавитов, в том числе русского, предполагает перекодировку национального доменного имени в код Unicode, а затем по специальному алгоритму преобразует этот код в уникальную последовательность «разрешенных» ASCII-символов. Например, слово «банк» преобразуется в AQYTAPJ2. К этой строке, однозначно соответствующей кириллической записи, добавляется специальный префикс BQ-- (с двумя дефисами), который служит для того, чтобы отличать преобразованные доменные имена от случайных наборов ASCII-символов. Такой формат записи называется RACE (Row-based ASCII Compatible Encoding). В результате адрес узла **www.банк.com** преобразуется в **www.BQ--AQYTAPJ2.com.** Именно RACE-адрес домена хранится в базах данных DNS, благодаря чему перестройка существующей системы доменных имен и замена программного обеспечения не требуются. В настоящее время для работы с национальными доменными именами на узле клиента должна быть установлена специальная программа, преобразующая символы национального алфавита в RACE-формат, который и используется при запросе к DNS. В дальнейшем поддержка мультиязыковых доменов будет встраиваться непосредственно в операционные системы и браузеры.

лю. Именно он первым поддерживал файл hosts.txt, который можно было получить по FTP. Этот файл хранился в сетевом информационном центре Станфордского исследовательского института (SRI). Администраторы сетей передавали в SRI дополнения и изменения, происшедшие в конфигурации администрируемой им сети. Периодически администраторы переписывали этот файл в свои системы.

В локальных сетях файлы hosts используются достаточно успешно до сих пор. Практически все операционные системы от различных версий Unix до Windows последних версий поддерживают эту систему соответствия IP-адресов именам хостов.

Пользователь для обращения к узлу мог использовать как IP-адрес узла, так и его имя. Процедура использования имени заключается в следующем: сначала по имени в файле hosts находят IP-адрес, а затем по IP-адресу устанавливают соединение с удаленным информационным ресурсом. С ростом сети ARPANET это стало чрезвычайно затруднительно, поскольку файл увеличивался в размерах, а его пересылка по сети и хранение на каждом узле требовало значительных ресурсов. Однако главное неудобство заключалось в том, что такой способ не позволял оперативно учитывать все изменения в сети.

В 1984 г. в сети ARPANET стала использоваться служба, получившая название системы доменных имен (*Domain Name System – DNS*). DNS была описана Полом Мокапетрисом в двух документах: RFC-882 и RFC-883 (позже эти документы были заменены на RFC-1034 и RFC-1035).

В соответствии с RFC-1034 и RFC-1035, описывающими DNS, роль доменного имени в процессе установки соединения осталась прежней. Это значит, что главное, для чего используется DNS служба – это получение IP-адреса узла сети. Исходя из этого, любая реализация DNS является прикладным процессом, который работает над стеком протоколов межсетевого обмена TCP/IP. Таким образом, базовым элементом адресации в сетях TCP/IP с введением DNS остался IP-адрес, а доменное именование (система доменных имен) играет роль вспомогательного сервиса.

DNS состоит из трех основных частей:

- пространство (множество) доменных имен (domain name space);
- серверов доменных имен (domain name servers);
- клиентов DNS (Resolver).

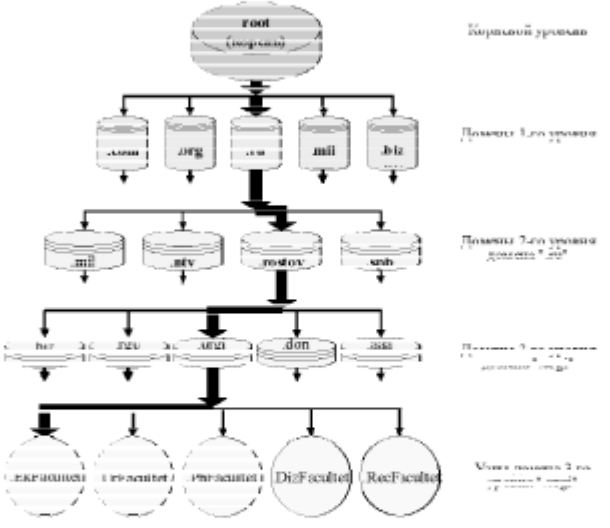


Рис. 4.3. **Дерево доменных имен**

Пространство доменных имен имеет вид дерева (иерархии) узлов, как показано на рис. 4.3 и подчиняется следующим правилам (RFC-1034):

- имя корня – пустая строка, т.е. полное имя обязательно завершается точкой[1];

[1] В некоторых случаях, например, при записи почтовых адресов, заключительная точка должна быть опущена.

- каждый узел дерева должен быть помечен простым именем, включающим допустимые символы;
- прописные и строчные буквы в доменных именах не различаются;
- допустимая длина простого имени не более 63 символов;
- доменные имена узлов в пределах одного домена должны быть уникальны;
- допускается применение одинаковых доменных имен в разных доменах, как (рис. 4.3), где доменное имя «.mil» используется для обозначения домена первого уровня и домена второго уровня, являющегося поддоменом домена «.ru»;
- полное имя узла образуется из последовательности имени самого узла и всех имен доменов, которые с ним связаны (снизу вверх по соответствующей ветви дерева) до корня включительно, записываемых слева направо и разделяемых точками, например, как показано на рис.е 4.3, узлу «.Ekfacultet» соответствует следующее полное доменное имя «.Ekfacultet.urgi.rostov.ru»;
- максимальная длина полного имени – 255 символов, включая точки;
- максимальное число уровней дерева – 127[1];
- кроме полного (абсолютного) имени узла (FQDN, fully qualified domain name) допускается применение относительного (относительно некоторого опорного узла) имена, в этом случае завершающая точка отсутствует;
- поддерево доменных имен вместе со своим корневым узлом называется доменом (поддоменом), например, обозначенная на рис. 4.3 ветвь относится к группе узлов («.Ekfacultet», «.Urfacultet», «.Phfacultet», «.Dizfacultet», «.Recfacultet») и поддоменов («.rostov» «.urgi»), входящих в домен «.ru», а все узлы, показанные на рис. 4.3 на самом нижнем уровне, входят в домен (поддомен) третьего уровня «.urgi» и др.
- объединение узлов в домены является чисто логическим, т.е. не зависящим ни от месторасположения, ни от IP-адреса, ни от способа маршрутизации.

---

[1] На практике применение доменных имен с количеством уровней более трех затруднительно для пользователя.

Полное доменное имя узла используется как ключевая информация для поиска IP-адреса узла в базе данных, содержащей таблицы соответствия доменных имен и логических адресов.

Корень – это множество все узлов Internet. Данное множество подразделяется на домены первого или верхнего уровня (top-level или TLD).

Корневой зоной Интернета и системой корневых серверов управляет ICANN, в частности, ICANN делегирует (передает) права управления зонами первого уровня gTLD (generic top-level domains, домены верхнего организационного уровня) и ccTLD (country code top-level domains, национальные домены).

В соответствии с принятыми правилами право администрирования каждого домена первого уровня передается одной определенной организации (оператору регистра; администратором доменной зоны «ru» является РосНИИРОС). Зарегистрировать домен второго уровня, например, в доменной зоне «ru» можно у одного из многочисленных регистраторов (коммерческие организации, имеющие доступ к общей базе данных оператора регистра для данной доменной зоны). Первоначально в ARPANET было семь доменов верхнего организационного уровня:

1. **com** (коммерческие организации);
2. **edu** (образовательные организации, в основном из США);
3. **gov** (правительственные организации США);
4. **int** (международные организации);
5. **mil** (военные организации США);
6. **net** (организации, обеспечивающие сетевую инфраструктуру);
7. **org** (некоммерческие организации).

В 1990-х гг. к ним были добавлены следующие домены:

8. **aero** (организации, связанные с авиацией);
9. **arpa** (используется для отображения адресов в имена);
10. **biz** (коммерческие организации);
11. **coop** (кооперативы);

12. **info** (разное);
13. **museum** (музеи);
14. **name** (персональные домены);
15. **pro** (лицензированные профессионалы).

Список доменов ccTLD базируется на стандарте двухбуквенных кодов государств и территорий (ISO 3166).

Примеры доменов верхнего уровня ccTLD, соответствующие отдельным государствам, приведены в табл. 4.3.

В Интернете система доменных имен реализована в виде распределенной базы данных, включающей в себя серверы DNS, клиенты DNS (resolver), объединенные общим протоколом запросов к базе данных и обмена информацией между серверами.

Таблица 4.3

Примеры национальных доменов верхнего уровня

Страна	Код	Страна	Код
Аргентина	ar	Кипр	cy
Армения	am	Киргизстан	kg
Австрия	at	Казахстан	kz
Азербайджан	az	Канада	ca
Белорусь	by	Индия	id
Бельгия	be	Латвия	lv
Болгария	bg	Литва	lt
Чехия	cz	Молдова	md
Эстония	ee	Нидерланды	nl
Финляндия	fi	Польша	pl
Франция	fr	Португалия	pt
Германия	de	Россия	ru
Греция	gr	Словакия	sk
Грузия	ge	Словения	si
Дания	dk	Испания	es
Венгрия	hu	Швеция	se
Италия	it	Швейцария	ch
Япония	jp	Узбекистан	uz
Украина	ua	Туркменистан	tm
Великобритания	gb	Соединенные Штаты	us

Информация, соответствующая каждому доменному имени, хранится в записях ресурсов RR (resource records) DNS-сервера. Основным типом хранимой информации является IP адрес. Одному доменному имени может соответствовать несколько IP-адресов (в случае использования нескольких сетевых интерфейсов на компьютере). Кроме этого в записях ресурсов может храниться дополнительная информация, например, максимально допустимое время кэширования[1] полученной информации (TTL, time to live).

В системе доменных имен различают несколько типов DNS-серверов.

В зависимости от типа отклика на запрос серверы делятся на авторитетные (authoritative) и неавторитетные (non authoritative).

Авторитетный отклик (authoritative response) возвращают серверы, которые являются ответственными за зону, в которой описана информация, необходимая клиенту DNS[2].

Неавторитетный отклик (non authoritative response) возвращают серверы, которые не отвечают за зону, содержащую необходимую клиенту информацию.

В зависимости от способа поддержания базы данных авторитетные DNS-серверы делятся на первичные (primary) и дублирующие (secondary)[3].

Первичный сервер доменных имен является ответственным за информацию о определенной доменной зоне[1] и по-

---

[1] Кэширование информации заключается в ее запоминании запросившим узлом или DNS-сервером более низкого уровня. По истечении указанного времени данная информация может быть удалена клиентом.

[2] Очевидно, что система DNS соответствует «клиент-серверной» архитектуре.

[3] На практике для домена второго уровня используются, как минимум, два сервера, ответственных за зону, т.е. дающие авторитетные отклики на запросы. Один первичный сервер и один дублирующий сервер. Эти серверы должны иметь независимые подключения к Интернету, чтобы обеспечить обслуживание запросов к зоне в случае потери связи по одному из сегментов сети.

этому хранит эту информацию, загружает ее для ответов клиентам с локального диска узла, на котором он функционирует. Описание зоны этого сервера ведется непосредственно администратором зоны.

Дублирующий сервер доменных имен также ответственный за эту доменную зону. В его функции входит дублирование первичного сервера на случай нарушения его работы. Кроме этого, дублирующий сервер, обрабатывая часть запросов, снимает нагрузку с первичного сервера.

Администратор дублирующего сервера не изменяет данные описания доменной зоны, а только обеспечивает синхронизацию базы данных дублирующего сервера с базой данных первичного сервера.

Примером такой организации служит система корневых (root-servers) DNS-серверов Интернета. Всего в сети Интернет 13[2] корневых DNS-серверов (табл. 4.4).

Корневые серверы – основа всей системы доменных имен, поскольку они *авторитетные серверы* для корневой зоны и содержат ссылки на такие же серверы зон первого уровня или сами являются *авторитетными* серверами некоторых зон первого уровня (например, com. или net.).

На запрос о домене корневой сервер возвращает как минимум имя и адрес уполномоченного сервера домена первого уровня, в который входит указанный в запросе узел. Обратившись по полученному адресу можно получить имя и адрес уполномоченного сервера домена второго уровня и др.

Из всего списка корневых серверов только один из них (A.ROOT-SERVERS.NET) является первичным, а все остальные дублирующие, хотя они содержат идентичную информацию.

---

[1] Для каждой доменной зоны первичным может быть только один сервер, поскольку «первоисточник» может и должен быть только один.

[2] Число 13 определяется максимальным размером пакета UDP, который не будет фрагментирован в любой реализации (576 байт), в такой пакет как раз помещается ответ о 13 адресах.

Таблица 4.4

Перечень корневых DNS-серверов Internet

№	Обозначение	Доменное имя или организация ответственная за поддержание сервера	IP-адрес
1.	**A**.ROOT-SERVERS.NET	NS.INTERNIC.NET	198. 41.0.4
2.	**B**.ROOT-SERVERS.NET	NS1.ISI.EDU	192.228.79.201
3.	**C**.ROOT-SERVERS.NET	C.PSI.NET	192.33.4.12
4.	**D**.ROOT-SERVERS.NET	TERP.UMD.EDU	128.8.10.90
5.	**E**.ROOT-SERVERS.NET	NS.NASA.GOV	192.203.230.10
6.	**F.ROOT-SERVERS.NET**[1]	**NS.ISC.ORG**	**192.5.5.241**
7.	**G**.ROOT-SERVERS.NET	NS.NIC.DDN.MIL	192.112.36.4
8.	**H**.ROOT-SERVERS.NET	AOS.ARL.ARMY.MIL	128.63.2.53
9.	**I**.ROOT-SERVERS.NET	NIC.NORDU.NET	192.36.148.17
10.	**J**.ROOT-SERVERS.NET	VeriSign	192.58.128.30
11.	**K**.ROOT-SERVERS.NET	RIPE NCC	193.0.14.129
12.	**L**.ROOT-SERVERS.NET	ICANN	198.32.64.12
13.	**M**.ROOT-SERVERS.NET	WIDE	202.12.27.33

Защита DNS-серверов любого уровня, а особенно корневых, является одной из проблем современной сети Интернет.

DNS-клиенты обычно реализуются в виде набора подпрограмм[2], используемых программами, которым требуется сервис доменных имен, например, Internet Explorer. В этом случае DNS-клиент обращается к указанному при настройке DNS-серверу (серверам), интерпретирует ответ и возвращает результат запросившей программе.

---

[1] 15 ноября 2003 г. компания Internet Software Consortium (ISC), ответственная за корневой сервер **F.ROOT-SERVERS.NET**, в сотрудничестве с Московским Internet Exchange (MSK-IX) установила в Москве новый корневой DNS-сервер, являющийся зеркалом (копией) корневого сервера имен **F.ROOT-SERVERS.NET.** По замыслу новый сервер должен значительно повысить скорость доступа к Internet-ресурсам для пользователей в России. MSK-IX – нейтральная сетевая структура, координируемая РосНИИРОС, которая предоставляет возможность поставщикам услуг Интернет (ISP) обмениваться IP-трафиком.

[2] В операционной системе Unix функции клиента реализуются двумя функциями: gethostbyname и gethostbyaddr. Первая функция воспринимает в качестве аргумента имя хоста и возвращает IP адрес, а вторая воспринимает в качестве аргумента IP адрес и возвращает имя хоста.

Обобщенная схема работы системы доменных имен иллюстрируется рис. 4.4. Пользователь инициирует запрос к web-серверу «www.urgi.ru». В соответствии с настройками сетевого подключения DNS-клиент формирует DNS-запрос к ближайшему DNS-серверу[1] (как правило, по умолчанию DNS-сервер провайдера) об IP-адресе узла, на котором функционирует данный web-сервер. Если DNS-сервер провайдера является авторитетным для доменной зоны «.ru», то он возвращает узлу пользователя (а вернее программе, инициировавшей запрос) DNS-отклик, в котором содержится требуемый IP-адрес (в предположении, что такой web-сервер вообще зарегистрирован).

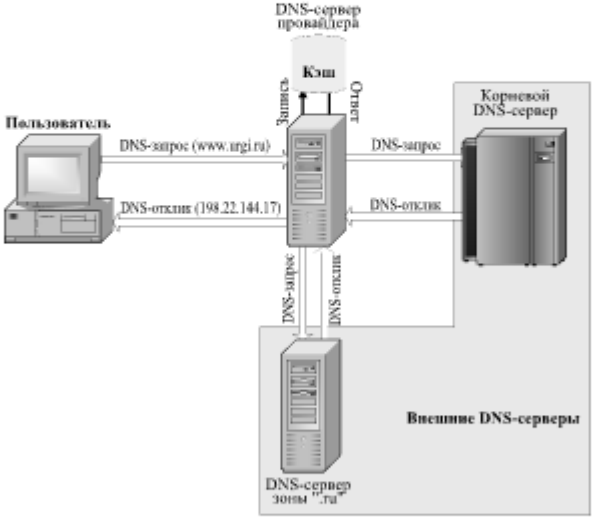


Рис. 4.4. **Схема работы системы доменных имен**

[1] Для начала поиска информации о любом доменном имени или IP-адресе клиенту достаточно знать адреса корневых DNS-серверов.

В случае если DNS-сервер провайдера не авторитетный для доменной зоны «.ru», то он формирует аналогичный DNS-запрос к вышестоящему DNS-серверу (чаще всего, но не обязательно, корневому DNS-серверу). Корневой DNS-сервер в ответ на полученный запрос формирует DNS-отклик, в котором содержится IP-адрес авторитетного для данной доменной зоны DNS-сервера, получив который DNS-сервер провайдера сформирует к нему запрос и полученный отклик вернет клиенту. При этом полученная информация будет занесена в кэш-память DNS-сервера провайдера. В случае повторного запроса от пользователя IP-адреса web-сервера «www.urgi.ru», DNS-сервер провайдера сформирует отклик, используя информацию из кэш-памяти[1] и не будет обращаться к вышестоящему DNS-серверу.

Запросы клиентов (или серверов) могут быть рекурсивными или итеративными. *Рекурсивный запрос* подразумевает, что запрашиваемый сервер должен самостоятельно пробежаться по всей системе серверов (вплоть до корневого) до получения конечного ответа (в том числе отрицательного) и вернуть его клиенту. При этом сам сервер может пользоваться итеративными или рекурсивными запросами. Сервер может отказаться выполнять рекурсивные запросы «сторонних» клиентов. При *итеративном запросе* сервер делает только один шаг поиска и возвращает ссылку на авторитетный сервер (или конечный ответ, если он сам является авторитетным для данного домена). Дальнейший поиск проводится самим клиентом.

Очевидно, что сервер доменных имен и клиентское программное обеспечение реализуют заложенную в DNS архитектуру «клиент-сервер», а программные средства, указанные в последнем пункте позволяют упростить настройку сервера и управление им.

История развития сети Интернет показывает, что DNS-сервер является объектом атак со стороны злоумышленников, поскольку, выведя из строя этот сервер или изменив данные его базы можно, нарушить работу сети.

---

[1] Необходимо иметь ввиду, что при кэшировании используется значение TTL (максимальное время жизни записи).

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).

Пассивным воздействием на распределенную вычислительную систему называется воздействие, которое не оказывает непосредственного влияния 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 – активные воздействия. Это связано с тем, что в самой природе разрушающего воздействия содержится активное начало. Очевидная особенность активного воздействия по сравнению с пассивным есть принципиальная возможность его обнаружения, так как в результате его осуществления в системе происходят определенные изменения. В отличие от

[1] Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet / под ред. проф. П.Д. Зегжды / НПО «Мир и семья-95», 1997.

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 – пассивное воздействие.

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. Данное 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, также 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 служит типовая удаленная атака «отказ в обслуживании».

По расположению субъекта атаки относительно атакуемого объекта:

- внутрисегментное (класс 5.1);
- межсегментное (класс 5.2).

Для понимания сути этих понятий 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 точки зрения удаленной атаки чрезвычайно важно, как по отношению друг к другу располагаются субъект и объ-

ект 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 её 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. 4.5.

Таблица 4.5

Классификация удаленных атак

Типовая удаленная атака	Характер воздействия		Цель воздействия			Условие начала			Наличие обратной связи		Расположение субъекта атаки		Уровень модели OSI						
Класс воздействия	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
Анализ сетевого трафика	+	–	+	–	–	–	–	+	–	+	+	–	–	+	–	–	–	–	–
Подмена доверенного объекта сети	–	+	+	+	–	–	+	–	+	+	+	+	–	–	+	+	–	–	–
Ложный объект сети	–	+	+	+	+	–	–	+	+	+	+	+	–	–	+	–	–	–	–
Отказ в обслуживании	–	+	–	–	+	–	–	+	–	+	+	+	–	+	+	+	+	+	+

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.

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*.

---

[1] Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. Под ред. проф. П. Д. Зегжды/ НПО «Мир и семья-95», 1997.

Анализ сетевого трафика позволяет:

- изучить логику работы распределенной вычислительной сети, это достигается путем перехвата и анализа пакетов обмена на канальном уровне (знание логики работы сети позволяет на практике моделировать и осуществлять др. 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 с помощью данной типовой удаленной атаки информации могут служить имя и пароль пользователя, пересылаемые в незашифрованном виде по сети).

Одна из проблем безопасности распределенной сети есть 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, то 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) – причина

возможного *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 др.), предоставляющих удаленный доступ к ресурсам данного объекта. Данные 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 является соответствующий сервер. В зависимости от различных параметров объектов вычислительной сети, основные из которых – быстродействие ЭВМ, объем оперативной памяти и пропускная способность канала связи – количество одновременно устанавливаемых

виртуальных подключений ограничено, соответственно, ограничено и количество 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 заключается в передаче с одного адреса такого количества запросов на атакуемый объект, которое позволяет трафик. В этом случае, если в системе не предусмотрены правила, ограничивающие количество принимаемых запросов с одного объекта (адреса) в единицу времени, то результатом этой атаки может быть как переполнение очереди запросов и отказа 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 обслуживании» 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:

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 аутентификации 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 – обязательное условие любой защищенной системы, поскольку все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами информационных систем.

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 соответствия подключающегося субъекта тому, 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 др.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи);
- физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и др.) или особенности поведения (особенности работы на клавиатуре и др.).

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 – более надежный метод 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 кроме памяти имеют собственный микропроцессор. Это позволяет реализовать различ-

ные 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 служит системы идентификации пользователя по рисунку радужной оболочки глаза, по почерку, по тембру голоса и др.

Новейшее направление аутентификации – 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 месторасположение 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 предоставляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами. Если ре-

зультат 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 количество повторов есть обязательное условие для защищенных систем) система временно блокируется и выдается 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 информационной безопасности делится на три категории:

1) статическая аутентификация;
2) устойчивая аутентификация;
3) постоянная аутентификация.

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 служат 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. Устойчивая аутентификация реализована в системах использующих 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 информационной системы.

Обычно полномочия субъекта представляются: *списком ресурсов,* доступным пользователю и *правами по доступу* к каждому ресурсу из списка.

Существуют следующие методы разграничения доступа:

1) разграничение доступа по спискам;
2) использование матрицы установления полномочий;
3) разграничение доступа по уровням секретности и категориям;
4) парольное разграничение доступа.

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 строки – идентификаторы субъектов, имеющих доступ в информационную систему, а столбцы – объекты (ресурсы) информационной системы. 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. Недостатки матрицы – ее возможная громоздкость и неоптимальность (большинство клеток – пустые).

Фрагмент матрицы установления полномочий показан в табл. 4.6.

Таблица 4.6

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 9:00 до 17:00
Пользователь 3	Чтение. Запись	Выполнение	Печать с 17:00 до 9:00

Разграничение доступа по уровням секретности и категориям заключается в разделении ресурсов информационной системы 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 конфиденциаль-

ности 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 информационной системы 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 информационной системы.

В ГОСТе Р 50739–95 «*Средства вычислительной техники. Защита от несанкционированного доступа к информации*» и в документах ФСТЭК РФ определены два вида (принципа) управления доступом:

- *дискретное управление доступом;*
- *мандатное управление доступом.*

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 – еще один механизм обеспечения защищенности информационной системы. Этот механизм основан на подотчетности системы обеспечения 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 др.

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, 1 раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется **активным**.

Реализация механизмов регистрации и аудита позволяет решать следующие задачи обеспечения информационной безопасности:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- 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.

Практические средства регистрации и аудита следующие:

- различные системные утилиты и прикладные программы;
- регистрационный (системный или контрольный) журнал.

Первое средство служит обычно дополнением к мониторингу, осуществляемого 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 в целях 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 успеха	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHO
Аудит успеха	26.04.2004	5:35:02	Security	Доступ к объектам	562	admin	GHO
Аудит успеха	26.04.2004	5:35:02	Security	Учетные записи	643	admin	GHO
Аудит успеха	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHO
Аудит успеха	26.04.2004	5:35:02	Security	Доступ к объектам	560	admin	GHO
Аудит успеха	26.04.2004	5:34:48	Security	Доступ к объектам	562	admin	GHO

Рис. 4.5. **Фрагмент журнала безопасности подсистемы регистрации и аудита операционной системы**

Обнаружение попыток нарушений информационной безопасности входит в функции активного аудита, задачи которого заключаются в оперативном выявлении подозрительной активности и предоставлении средств для автоматического реагирования на нее.

Под *подозрительной активностью* понимается поведение пользователя или компонента информационной системы, 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 количество 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 информационной системы 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 в целях 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

Один из эффективных механизмом обеспечения информационной безопасности распределенных вычислительных сетях – 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 информационной безопасности. 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 информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы 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:

- месту расположения в сети – на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;
- 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.

Таблица 4.7

Типы межсетевых экранов и уровни модели ISO/OSI

	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 (табл. 4.7) *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. Основной их недостаток – уязвимость при подмене адресов IP. 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 определенных служб сети Интернет (HTTP, FTP, Telnet и др.) и служат для проверки сетевых пакетов на наличие достоверных данных.

Шлюзы прикладного уровня снижают уровень производительности системы из-за повторной обработки в программе-посреднике. Это незаметно при работе в Интернете по низкоскоростным каналам, но существенно – во внутренней сети.

Межсетевые экраны экспертного уровня сочетают в себе элементы всех трех описанных 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. Межсетевые экраны экспертного уровня 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 определенной организации.

Вместо применения связанных с приложениями программ-посредников, брандмауэры экспертного уровня используют специальные алгоритмы распознавания и обработ-

ки 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 (VPN)

Технология виртуальных частных сетей (VPN – Virtual Private Network) является одним из эффективных механизмов обеспечения информационной безопасности при передаче данных в распределенных вычислительных сетях.

Виртуальные частные сети – комбинация 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:

- 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;
- вычисляется и добавляется в пакет его имитоприставка, обеспечивающая контроль целостности передаваемых данных;
- пакет шифруется (целиком, включая заголовок IP-пакета, содержащий служебную информацию);

• формируется новый заголовок пакета, где вместо адреса получателя указывается адрес его VPN-агента (эта процедура называется инкапсуляцией пакета)

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.

Рис. 4.6. **Технология VPN**

При получении IP-пакета выполняются обратные действия:

– 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);

– согласно настройкам выбираются криптографические алгоритмы и ключи, после чего пакет расшифровывается и проверяется его целостность (пакеты с нарушенной целостностью также отбрасываются);

– после всех обратных преобразований пакет в его исходном виде отправляется настоящему адресату по локальной сети.

Все перечисленные операции выполняются автоматически, работа VPN-агентов незаметна 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.

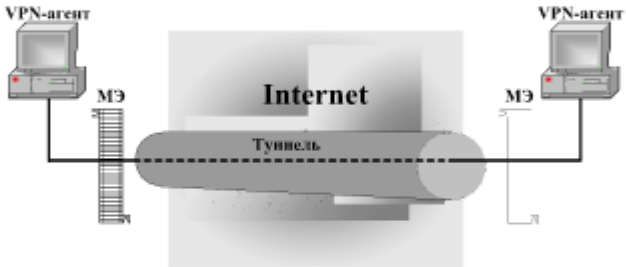


Рис. 4.7. **Пример расположения межсетевых экранов**

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.

Одной из обязательных функций VPN-агентов является фильтрация пакетов. Фильтрация пакетов 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.

Литература к главе 4

1. Башлы П.Н. Современные сетевые технологии: учебное пособие. – М: Горячая линия – Телеком, 2006.
2. Башлы П.Н. Информационная безопасность: учебно-практическое пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К. – М.: Изд. центр ЕАОИ, 2010.
3. Карпов Е.А., Котенко И.В., Котухов М.М., Марков А.С., Парр Г.А., Рунеев А.Ю. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под редакцией И.В.Котенко. – СПб.: ВУС, 2000.
4. Медведовский И.Д., Семьянов П.В., Леонов Д.Г., Лукацкий А.В. Атака из Internet. – М.: Солон-Р, 2002.
5. Мэйволд Э. Безопасность сетей: Пер. с англ. – М.: ЭКОМ, 2002.
6. Новиков Ю.В., Кондратенко С.В. Локальные сети: архитектура, алгоритмы, проектирование. – М.: ЭКОМ, 2001.
7. Олифер В.Г. , Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Питер, 2002.
8. Прохода А.Н. Обеспечение Интернет-безопасности. Практикум: учебное пособие для вузов.- М.: Горячая линия – Телеком, 2007.
9. Спортак Марк, Паппас Френк. Компьютерные сети и сетевые технологии. – М.: ТИД «ДС», 2002.
10. 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 советом. Решения разрабатываются и реализуются с разной степенью профессионализма, поэтому их диапазон практически неограничен – от необдуманных до детально разработанных.

Техническая революция середины XX в. изменил 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 количество 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

[1] В главе 5 использованы материалы учебно-методического пособия: Тимашков П.С. Математические методы принятия решений. – М.: МЭСИ, 2003.

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 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 отличии от исследования операций, в теории принятия решений не существует абсолютно лучшего решения. Решения – лучшее лишь для определенного лица принимающего решение, 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 лицом, принимающим решения (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 [2].

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 др. Главное в деятельности ГПР – достижение согласия при выработке совместных решений.

Иногда наряду с лицом, принимающим решения 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, имеющая общие интересы и старающаяся оказать влияние на процесс выбора и его результат. Примеры таких групп – 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 [10]. 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 человек, который лично работает в рассматриваемой области деятельности, признанный специалист 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 [10]. 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 [10].

В литературе можно встретить и др. и цифры, например, в работе [7], 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 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 отличаются друг от друга 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 – отсутствует выбор.

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 называется **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 выбирается наилучшая. Например, можно выбирать лучший университет, наиболее надежный банк или же банк с оптимальным соотношением выгода-риск, наиболее благоприятный район для покупки квартиры и др. 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.

Также существуют 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 [10].

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 [7].

Множество вариантов A проецируется на числовую ось, так что каждому варианту соответствует определенная 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 приписанным им числовым оценкам и сохранить за вариантами лишь их 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 x 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 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 *n* 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 важнейшая цель работы состоит в выработке и защите 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 количеством критериев полезно произвести декомпозицию задачи и разложить ее на подзадачи, каждая из которых содержит меньшее количество 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 количества критериев приводит, с одной стороны, 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, которая здесь рассматриваться не будет.

Возможный подход, опирающийся на оценку существующего и желательного состояния, следующий. 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. $S \subseteq R^n$ – это

подмножество m – мерного Евклидова пространства (m – количество 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

$$K_j = \gamma_j \cdot f(K_j^D, K_j^S).$$

Возможные виды функции f – это разность K_j^s и K_j^D, показывающая насколько надо улучшить положение или их частное, показывающее во сколько раз надо улучшить положение.

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).

3. В третьем случае значимость критериев определяется на основе оценок текущего и желательного состояние 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 управляющих воздействий.

Если через $K_j^{H(t)}$ обозначить значение, которое j-й критерий примет через время t, то

$$K_j = \gamma_j f(K_j^D, K_j^S, K_j^{H(t)}).$$

Возможны различные виды этой функции, например:

$$K_j = \gamma_j \left[\alpha_j \cdot (K_j^S - K_j^D) + \beta_j \cdot (K_j^D - K_j^{H(t)} \right]$$

или

$$K_j = \gamma_j \left[\alpha_j \cdot \frac{K_j^S}{K_j^D} + \beta_j \cdot \frac{K_j^D}{K_j^{H(t)}} \right],$$

где α_j и β_j – коэффициенты, характеризующие относительную важность разности (частного) K_j^s, K_j^n и, K_j^D $K_j^{H(t)}$.

Во многих случаях целесообразно сосредоточить основное внимание на наиболее важных критериях, установив некоторый порог $K_j \geq const$, где $\overline{j = 1, m}$. 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 др., что во многих случаях может быть сделано ЛПР исходя из его субъективных представлений о важности динамической составляющей в оценке критериев.

5.1.6. Многодисциплинарный характер науки о принятии решений

Термин «принятие решений» встречается в различных научных дисциплинах. Прежде всего следует назвать экономику. Экономика 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 др. научные направления затрагивают проблемы принятия решений. Центральным для этих проблем служит сам акт выбора человеком одного из вариантов решений. В отличии от других научных дисциплин в науке о принятии решений основной предметом – 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 требует 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, информатики, 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 ин-

формации 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 *early screening*), 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**

Схема процесса принятия решений приведена в работе [2] (рис. 5.2).

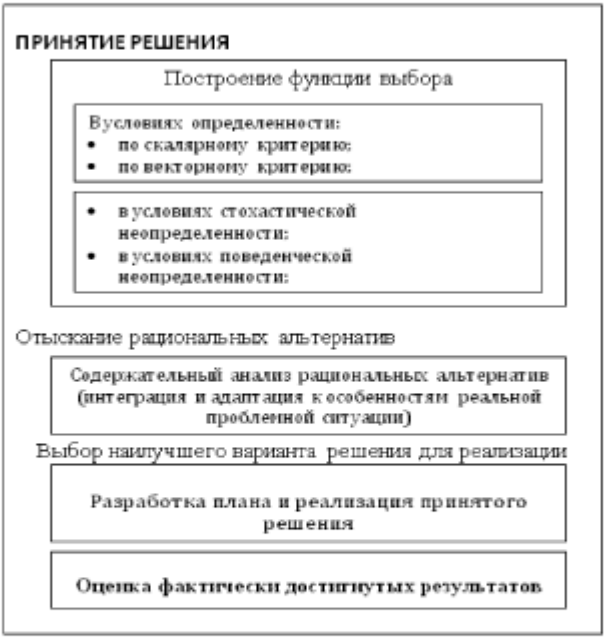


Рис. 5.2. **Схема процесса принятия решений**

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 качест-

вом, 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.

Множеству альтернатив предъявляются определенные требования. Во-первых, множество альтернатив 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 варианты, которые логически непротиворечивы 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 проводиться 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. Цель этой операции – 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.

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 др. Для

этих задач существуют адекватные математические модели процессов и/или устройств, и существуют данные, позволяющие априорно определить параметры моделей.

Характерные особенности проблем третьего класса следующие:

- уникальность выбора в том смысле, что каждый раз проблема новай 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 др.

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 Т. 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 перовой группы является многокритериальная оценка имеющихся на рынке провайдеров сотовой связи, имеющихся в продаже товаров и др. Здесь все возможные альтернативы заданы, критерии определены ЛПР. От ЛПР требуется построить правило сравнения объектов, имеющих оценки по многим критериям.

Примером задач второй группы служит 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.

Таблица 5.1

Классификация методов принятия решений

Содержание информации	Тип информации	Метод принятия решений
1. Экспертная информация не требуется		• метод доминирования; • метод на основе глобальных критериев
2. Информация о предпочтениях на множестве критериев	Качественная информация	• лексикографическое упорядочивание; • сравнение разностей критериальных оценок; • метод припасовывания.
	Количественная оценка предпочтительности критериев	• метод «эффективность–стоимость»; • методы свертки на иерархии критериев; • методы порогов; • методы идеальной точки.
	Количественная информация о замещениях	• метод кривых безразличия; • методы теории ценности.
3. Информация о предпочтительности альтернатив	Оценка предпочтительности парных сравнений	• методы математического программирования; • линейная и нелинейная свертка при интерактивном способе определения ее параметров.

Окончание табл. 5.1

Содержание информации	Тип информации	Метод принятия решений
4. Информация о предпочтениях на множестве критериев и о последствиях альтернатив	Отсутствие информации о предпочтениях; количественная и/или интервальная информация о последствиях	• методы с дискретизацией неопределенности;
	Качественная информация о предпочтениях и количественная о последствиях	• стохастическое доминирование; • методы принятия решений в условиях риска и неопределенности на основе глобальных критериев; • метод анализа иерархий; • методы теории нечетких множеств.
	Качественная информация о предпочтениях и последствиях	• методы практического принятия решений; • методы выбора статистически ненадежных решений.
	Количественная информация о предпочтениях и последствиях	• методы кривых безразличия для принятия решений в условиях риска и неопределенности; • методы деревьев решений; • декомпозиционные методы теории ожидаемой полезности.

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 ус-

ловиях 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 выбор решений из множества альтернатив различного типа при наличии критериев, имеющих разные типы шкал.

В свою очередь, среди методов, образующих четвертую группу, наиболее перспективные – декомпозиционный метод 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 др. 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 количества 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 1970-х гг., и за это время было дано большое количество определений этого понятия:

1. Системы поддержки принятия решений являются человеко-машинными объектами, которые позволяют лицам, при-

нимающим 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 групповых 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 служат 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 таких 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).

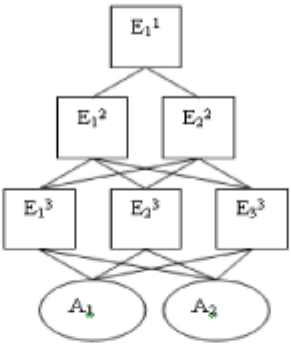


Рис. 5.3. **Иерархическое представление проблемы**

Верхний индекс у элементов указывает уровень иерархии, а нижний – их порядковый номер.

Процесс построения иерархической структуры можно рассмотреть на следующем примере.

Пример 5.1. 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 др.

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 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 проводятся 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?

Процесс построения матрицы парных сравнений можно рассмотреть на следующем примере.

Пример 5.2. Проведите 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 следующим образом (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 $\frac{1}{7}$. 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 5 в позиции один три говорит о том, что для ЛПР тарифы *важней* доступности сети, в то время $\frac{1}{3}$ 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.

Рис. 5.6. **Иерархическая схема задачи выбора нового сотрудника**

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 перечисли 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, расположенном 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.

Таблица 5.3

Сравнение альтернатив относительно критерия «образование»

Альтернатива	Абсолютное	Очень сильное	Сильное	Слабое	Равенство	Слабое	Сильное	Очень сильное	Абсолютное	Альтернатива
A_1	_	_	_	_	_	_	_	_	_	A_2
A_1	_	_	_	_	_	_	_	_	_	A_3
A_2	_	_	_	_	_	_	_	_	_	A_3

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 5.4

Сравнение альтернатив относительно критерия «образование», составленное первым экспертом по резюме кандидатов

Альтернатива	Абсолютное	Очень сильное	Сильное	Слабое	Равенство	Слабое	Сильное	Очень сильное	Абсолютное	Альтернатива
A_1	_	x	_	_	_	_	_	_	_	A_2
A_1	_	_	_	x	_	_	_	_	_	A_3
A_2	_	_	_	_	_	_	x	_	_	A_3

Матрица парных сравнений для анкеты из табл. 5.4 имеет вид:

$$[Образование]_1 = \begin{array}{c|ccc} & A_1 & A_2 & A_3 \\ \hline A_1 & 1 & 7 & 3 \\ A_2 & \frac{1}{7} & 1 & \frac{1}{5} \\ A_3 & \frac{1}{3} & 5 & 1 \end{array}$$

Для агрегирования мнений экспертов принимается среднегеометрическое, вычисляемое по следующей формуле:

$$a_{ij}^{ap} = \sqrt[n]{a_{ij}^{(1)} \cdot a_{ij}^{(2)} \cdot \ldots \cdot a_{ij}^{(n)}},$$

где $a_{ij}^{(k)}$ – оценка элемента, принадлежащего i-ой строке и j-му столбцу матрицы парных сравнений k-ого эксперта.

Логичность критерия становится очевидной, если два равноценных эксперта указывают при сравнении объектов соответственно оценки a и $\frac{1}{a}$, что при вычислении агрегированной оценки дает единицу и свидетельствует об эквивалентности сравниваемых объектов.

В достаточно ответственных задачах при оправданных 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.

Рис. 5.7. **Иерархия для ранжирования экспертов**

Расчет агрегированной оценки в случае привлечения n экспертов, имеющих различную значимость, осуществляется по формуле:

$$a_{ij}^{agr} = a_{ij}^{\alpha_1} \cdot a_{ij}^{\alpha_2} \cdot \ldots \cdot a_{ij}^{\alpha_n},$$

где $a_{ij}^{\alpha_k}$ – оценка объекта, проведенная k-м экспертом с весовым коэффициентом α_k. При этом $\sum_{k=1}^{n} \alpha_k = 1$

Пример 5.3. 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, заполненная следующим образом (табл. 5.5):

Таблица 5.5

Сравнение альтернатив относительно критерия «образование», составленное вторым экспертом по результатам собеседования с кандидатами

Альтернатива	Абсолютное	Очень сильное	Сильное	Слабое	Равенство	Слабое	Сильное	Очень сильное	Абсолютное	Альтернатива
A_1	_	x	_	_	_	_	_	_	_	A_2
A_2	_	_	x	_	_	_	_	_	_	A_3
A_3	_	_	_	_	_	x	_	_	_	A_3

Матрица парных сравнений для анкеты в табл. 5.5, имеет вид:

$$[Образование]_2 = \begin{array}{c|ccc} & A_1 & A_2 & A_3 \\ A_1 & 1 & 7 & 5 \\ A_2 & \frac{1}{7} & 1 & \frac{1}{3} \\ A_3 & \frac{1}{5} & 3 & 1 \end{array}$$

Для объединения оценок суждений двух экспертов строится матрица с средним геометрическим оценок. В данной задаче такой подход не совсем правомерен. Однако, будем считать что суждения двух экспертов обладают одинаковой степенью значимости. Результирующая матрица имеет вид:

$$[Образование] = \begin{array}{c|ccc} & A_1 & A_2 & A_3 \\ A_1 & 1 & \sqrt{7 \cdot 7} & \sqrt{3 \cdot 5} \\ A_2 & \sqrt{\frac{1}{7} \cdot \frac{1}{7}} & 1 & \sqrt{\frac{1}{5} \cdot \frac{1}{3}} \\ A_3 & \sqrt{\frac{1}{3} \cdot \frac{1}{5}} & \sqrt{5 \cdot 3} & 1 \end{array}$$

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 5.4. Предположим, что имеется три фрукта: яблоко, апельсин и ананас. Некто, предположим ребенок, говорит следующее: «Ананас в три раза вкуснее апельсина, а апельсин в 2 раза вкуснее яблока». Следующим высказыванием ребенка на вопрос о его любви к яблокам и ананасам, он говорит, что ананас в 5 раз лучше яблока. В таких высказываниях ребенка несогласованности практически нет, несмотря на то, что исходя из его первого предложения ананас в 6 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 (ИО) (индексом согласованности (ИС)) или отношением однородности (отношением согласованности) в соответствии со следующими формулами:

$$ИО = ИС = \frac{\lambda_{max} - n}{n-1};$$

$$ОО = ОС = \frac{ИО}{М(ио)},$$

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 $OO \le 0,10$. Если для матрицы парных сравнений $OO > 0,10$, 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 $A_{n\times n}$. Символ 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 5.5. 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.

$$det(A - \lambda E) = 0;$$

$$\begin{vmatrix} 1-\lambda & \frac{1}{3} & \frac{1}{2} \\ 3 & 1-\lambda & 3 \\ 2 & \frac{1}{3} & 1-\lambda \end{vmatrix} = 0$$

$$(1-\lambda)\cdot\begin{vmatrix} 1-\lambda & 3 \\ \frac{1}{3} & 1-\lambda \end{vmatrix} - 3\cdot\begin{vmatrix} \frac{1}{3} & \frac{1}{2} \\ \frac{1}{3} & 1-\lambda \end{vmatrix} + 2\cdot\begin{vmatrix} \frac{1}{3} & \frac{1}{2} \\ 1-\lambda & 3 \end{vmatrix} = 0$$

$$(1-\lambda)\cdot\left[(1-\lambda)^2 - 1\right] - 3\cdot\left(\tfrac{1-\lambda}{3} - \tfrac{1}{6}\right) + 2\cdot\left(1 - \tfrac{1-\lambda}{2}\right) = 0$$

При решении данного уравнения получено максимальное собственное значение $\lambda_{max} = 3,05$. Для вычисления главного собственного вектора необходимо решить систему линейных уравнений:

$$\begin{pmatrix} 1 & \frac{1}{3} & \frac{1}{2} \\ 3 & 1 & 3 \\ 2 & \frac{1}{3} & 1 \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = 3,05 \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}; \quad W = \begin{pmatrix} 0,157 \\ 0,594 \\ 0,249 \end{pmatrix}.$$

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

$$\lim_{k \to \infty} \frac{A^k e}{e^T A^k e} = CW,$$

где $e = (1, 1, \ldots, 1)^T$ – вектор составленный из n единиц.

Максимальное собственное значение вычисляется по формуле: $\lambda_{max} = e^T AW$.

Как видно из вышеприведенного 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 количество 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 вычислитель-

ные 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 5.6. Рассмотрим матрицу парных сравнений и вычислим приближенное значение главного собственного вектора:

$$[A] = \begin{array}{c|ccc} & A_1 & A_2 & A_3 \\ A_1 & 1 & \frac{1}{3} & \frac{1}{2} \\ A_2 & 3 & 1 & 3 \\ A_3 & 2 & \frac{1}{3} & 1 \end{array}$$

Просуммируем элементы каждой строки и найдем сумму всех элементов матрицы:

$$W_S = \begin{pmatrix} 1\frac{5}{6} \\ 7 \\ 3\frac{1}{3} \end{pmatrix}; \qquad S = 1\tfrac{5}{6} + 7 + 3\tfrac{1}{3} = 12\tfrac{1}{6}.$$

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 $\lambda_{max} = e^T AW$, рассмотренной ранее:

$$\lambda_{max} = (1\ 1\ 1) \cdot \begin{pmatrix} 1 & \frac{1}{3} & \frac{1}{2} \\ 3 & 1 & 3 \\ 2 & \frac{1}{3} & 1 \end{pmatrix} \cdot \begin{pmatrix} 0,151 \\ 0,575 \\ 0,274 \end{pmatrix} \approx 3,10.$$

При таком вычислении главного собственного вектора и максимального собственного значения может оказаться, что согласованная в действительности матрица является несогласованной по вычислениям и наоборот.

Пример 5.7. Вычислим отношение согласованности рассматриваемой ранее матрицы, взяв в качестве максимального собственного значения его точное и приближенное число.

$$ИС = \frac{3,05-3}{3-1} = 0,025; \qquad OC = \frac{0,025}{0,58} \approx 0,04;$$

$$ИС_* = \frac{3,10-3}{2} = 0,05; \qquad OC_* = \frac{0,05}{0,58} \approx 0,09.$$

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 на клавиши <*Shift*>+<*Enter*> – пакет произведет назначение матрице *M* соответствующих числовых характеристик.

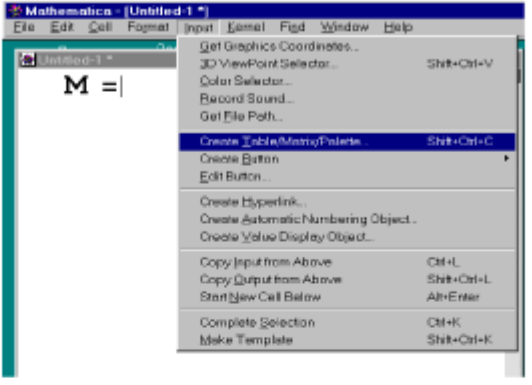


Рис. 5.8. **Меню вставки пакета Mathematica**

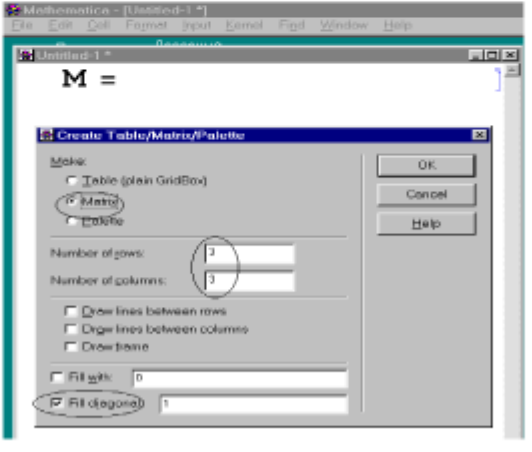


Рис. 5.9. **Определение размерности матрицы в пакете Mathematica**

Вычисление собственных значений выполняется функцией *Eigenvalues[M]*, а собственных векторов *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 на клавиш <*Shift*>+<*Enter*>, Mathematica выдаст результат, представленный на рис. 5.10, где 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 говорит 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.

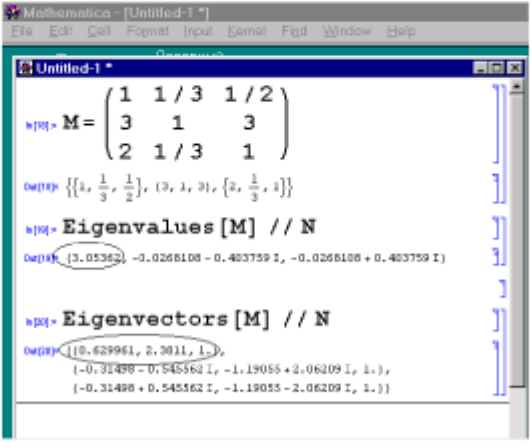


Рис. 5.10. **Вычисление собственных значений и векторов матрицы в пакете Mathematica**

При использовании пакета Mathematica необходимо помнить, что строчные и заглавные буквы различаются. Так, например, название функций должны начинаться с заглавной буквы, в противном случае они не распознаются. Аргументы функций обязаны стоять в квадратных скобках.

Вычисление необходимых величин, даже с помощью 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 вектора и значения с использованием Mathcad. Определим и введем в рабочий документ матрицу A 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 др. вычисления в Mathcad, можно выполнить тремя способами – с помощью панелей инструментов, выбором операции в меню или обращением к соответствующей функции.

Воспользуемся первым вариантом. После того как имя матрицы и оператор присваивания были введены, откроем панель операций с матрицами, щелкнув по кнопке  (рис. 5.11). После этого на появившейся панели щелкнем по кнопке  и зададим размерность матрицы (рис. 5.12).

Рис. 5.11. **Панель операций с матрицами в пакете Mathcad**

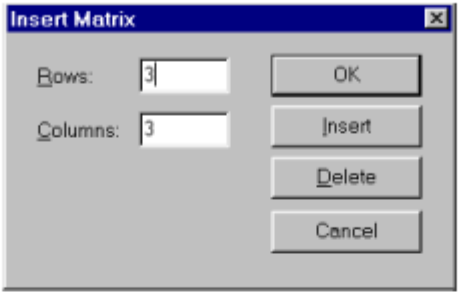


Рис. 5.12. **Окно определения размеров матрицы в Mathcad**

После ввода матрицы присвоим некоторой переменной C значение функции *eigenvals(A)*. Данная 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:

$$A := \begin{pmatrix} 1 & \frac{1}{3} & \frac{1}{2} \\ 3 & 1 & 3 \\ 2 & \frac{1}{3} & 1 \end{pmatrix} \quad C := eigenvals(A)$$

$$C = \begin{pmatrix} 3,054 \\ -0,027 + 0,404i \\ -0,027 - 0,404i \end{pmatrix}$$

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 аргументы: 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:

$$eigenvals(A, C_0) = \begin{pmatrix} 0,237 \\ 0,896 \\ 0,376 \end{pmatrix}$$

Вектор не нормирован. Нормируем его. Для удобства расчетов присвоим главный собственный вектор некоторой переменной *P*. Вычисление суммы *S* координат вектора *P* проведем с помощью кнопки Σ_0 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 складывать. После нахождения суммы проведем деление вектора *P* на сумму *S*.

Фрагмент рабочего документа Mathcad, содержащий перечисленные выше действия, приведен ниже.

$$P := eigenvals(A, C_0)$$

$$S := \sum P = \quad S = 1,509$$

$$\frac{P}{S} = \begin{pmatrix} 0,157 \\ 0,594 \\ 0,249 \end{pmatrix}$$

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:

$$A := \begin{pmatrix} 1 & \frac{1}{4} & \frac{1}{2} \\ 4 & 1 & 3 \\ 2 & \frac{1}{3} & 1 \end{pmatrix}; \quad C := eigenvals(A) \quad C = \begin{pmatrix} 3,018 \\ -9,147 \cdot 10^{-3} + 0,235i \\ -9,147 \cdot 10^{-3} - 0,235i \end{pmatrix};$$

$$eigenvals(A, C_0) = \begin{pmatrix} 0,2 \\ 0,915 \\ 0,349 \end{pmatrix}; \quad P := eigenvals(A, C_0);$$

$$S := \sum P; \quad S = 1,465; \qquad \frac{P}{S} = \begin{pmatrix} 0,136 \\ 0,625 \\ 0,238 \end{pmatrix};$$

$$IS := \frac{C_0 - 3}{2}; \quad IS = 9,147 \cdot 10^{-3}; \quad OS := \frac{IS}{0,58}; \quad OS = 0,016.$$

Нижний индекс ввести можно с помощью кнопки x_n на 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 количества вычислений, за исключением матрицы второго порядка:

Матрица 2 ×2

$$\begin{bmatrix} 1 & a \\ 1/a & 1 \end{bmatrix}$$

Для этого случая $\lambda_{max} = 2$, $W = (\frac{a}{a+1}; \frac{1}{a+1})$.

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

$$\begin{bmatrix} 1 & a & b & c \\ 1/a & 1 & d & e \\ 1/b & 1/d & 1 & f \\ 1/c & 1/e & 1/f & 1 \end{bmatrix}.$$

$$B = \left(\frac{d \cdot f}{e} + \frac{e}{d \cdot f}\right) + \left(\frac{a \cdot e}{c} + \frac{c}{a \cdot e}\right) + \left(\frac{a \cdot d}{b} + \frac{b}{a \cdot d}\right) + \left(\frac{b \cdot f}{c} + \frac{c}{b \cdot f}\right);$$

$$C = 3 - \left(\frac{a \cdot d \cdot f}{c} + \frac{c}{a \cdot d \cdot f}\right) - \left(\frac{a \cdot e}{b \cdot f} + \frac{b \cdot f}{a \cdot e}\right) - \frac{c \cdot d}{a \cdot e} - \left(\frac{c \cdot d}{b \cdot e} + \frac{b \cdot e}{c \cdot d}\right);$$

$$r = \sqrt[3]{\left(-8 + \frac{B^2}{2} + 8C\right) + \sqrt{\left[-\frac{4}{3} \cdot (C + 3)\right]^3 + \left(8 - \frac{B^2}{2} - 8C\right)^2}} +$$

$$+\sqrt[3]{\left(-8+\frac{B^2}{2}+8C\right)-\sqrt{\left[-\frac{4}{3}\cdot(C+3)\right]^3+\left(8-\frac{B^2}{2}-8C\right)^2}}\;;$$

$$\lambda_{max}=\frac{2+\sqrt{r+4}}{2}+\sqrt{\frac{8-r}{4}+\frac{B}{2\cdot\sqrt{r+4}}};$$

$$Q=(\lambda-1)^3+(c+f+e)\cdot(\lambda-1)^2+\left[(a\cdot e-3)+(b+d)\cdot f+\left(\frac{1}{a}+\frac{1}{b}\right)\cdot c+\frac{e}{d}\right]\cdot(\lambda-1)+$$

$$+\left[(a\cdot d\cdot f-c-e-f)+\left(\frac{b\cdot e}{d}+\frac{b\cdot f}{a}\right)+\frac{c\cdot d+a\cdot e-a\cdot d}{b}+\frac{c-b}{a\cdot d}\right].$$

$$W=\begin{bmatrix}\dfrac{c(\lambda-1)^2+(ae+bf)\cdot(\lambda-1)+\left(adf+\dfrac{be}{d}-c\right)}{Q}\\[2ex]\dfrac{e(\lambda-1)^2+\left(df+\dfrac{c}{a}\right)\cdot(\lambda-1)+\left(\dfrac{bf}{a}+\dfrac{cd}{b}-e\right)}{Q}\\[2ex]\dfrac{f(\lambda-1)^2+\left(\dfrac{e}{d}+\dfrac{c}{b}\right)\cdot(\lambda-1)+\left(\dfrac{c}{ad}+\dfrac{ae}{b}-f\right)}{Q}\\[2ex]\dfrac{(\lambda-1)^3-3(\lambda-1)-\left(\dfrac{ad}{b}+\dfrac{b}{ad}\right)}{Q}\end{bmatrix}.$$

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.

Рис. 5.13. **Пример трехуровневой иерархической структуры**

Алгоритм иерархического синтеза для приведенного примера следующие:

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):

$$[E_1^3] = \begin{array}{c|cc} & A_1 & A_2 \\ \hline A_1 & 1 & a_{12} \\ A_2 & 1/a_{12} & 1 \end{array} \Rightarrow \lambda_{max}, W_{E_1^3};$$

$$[E_2^3] = \begin{array}{c|cc} & A_1 & A_2 \\ \hline A_1 & 1 & * \\ A_2 & 1/* & 1 \end{array} \Rightarrow \lambda_{max}, W_{E_2^3};$$

$$[E_3^3] = \begin{array}{c|cc} & A_1 & A_2 \\ \hline A_1 & 1 & \times \\ A_2 & 1/\times & 1 \end{array} \Rightarrow \lambda_{max}, W_{E_3^3}.$$

2. Аналогичным образом обрабатываем матрицы парных сравнений для вышележащих уровней. Данные матрицы построены для того, чтобы определить предпочтительность элементов определенного иерархического уровня относительно элементов вышележащего.

$$[E_1^2] = \begin{array}{c|ccc} & E_1^3 & E_2^3 & E_3^3 \\ \hline E_1^3 & & & \\ E_2^3 & & & \\ E_3^3 & & & \end{array} \Rightarrow \lambda_{max}, W_{E_1^2};$$

$$[E_2^2] = \begin{array}{c|ccc} & E_1^3 & E_2^3 & E_3^3 \\ \hline E_1^3 & & & \\ E_2^3 & & & \\ E_3^3 & & & \end{array} \Rightarrow \lambda_{max}, W_{E_2^2};$$

$$[E_3^2] = \begin{array}{c|cc} & E_2^3 & E_3^3 \\ \hline E_2^3 & & \\ E_3^3 & & \end{array} \Rightarrow \lambda_{max}, W_{E_3^2}.$$

3. Осуществляем иерархический синтез. Последовательно определяем вектора приоритетов альтернатив $W_{E_j^i}^A$ относительно элементов E_j^i, находящихся на всех иерархических уровнях. Для предпоследнего уровня $W^A_{E_1^2} = W_{E_1^2}, W^A_{E_2^2} = W_{E_2^2}, W^A_{E_3^2} = W_{E_3^2}$.

Векторы приоритетов вычисляются в направлении от нижних уровней к верхним с учетом связей между элементами, принадлежащими различным уровням. Вычисление производится путем перемножения соответствующих векторов и матриц:

$$W_{E_1}^{A} = \underbrace{[W_{E_1^1}^{A} \quad W_{E_1^2}^{A} \quad W_{E_1^3}^{A}]}_{матрица} \cdot W_{E_1^j};$$

$$W_{E_2}^{A} = [W_{E_2^1}^{A} \quad W_{E_2^2}^{A} \quad W_{E_2^3}^{A}] \cdot W_{E_2^j};$$

$$W_{E_3}^{A} = [W_{E_3^1}^{A} \quad W_{E_3^2}^{A} \quad W_{E_3^3}^{A}] \cdot W_{E_3^j}.$$

Результирующий вектор приоритетов альтернатив относительно основной цели $W_{E_1}^{A} = [W_{E_1^1}^{A} \quad W_{E_2^2}^{A} \quad W_{E_3^2}^{A}] \cdot W_{E_1^j}$.

Пример 5.8 (из книги Т. Саати). 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, группу ровесников, школьное обучение, религиозный статус и др.

На перечисленные ранее 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; 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 др., влияющих или находящихся под влиянием расположенных ранее элементов.

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 силы 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 (рис. 5.14), 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.

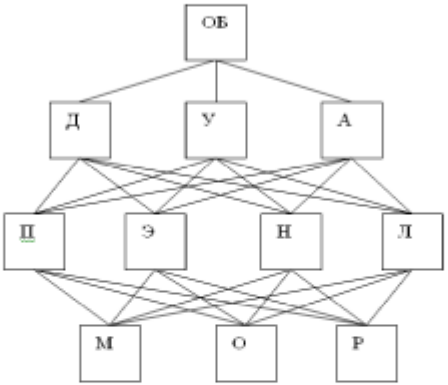


Рис. 5.14. **Иерархическая схема общего благополучия индивидуума**

$$[ОБ] = \begin{array}{c|ccc} & Д & У & А \\ \hline Д & 1 & 6 & 4 \\ У & 1/6 & 1 & 3 \\ А & 1/4 & 1/3 & 1 \end{array}$$

$W_{ОБ} = (0,701;\ 0,193;\ 0,106);$
$\lambda_{max} = 3,26;\ ИС = 0,07;\ ОС = 0,12.$

$$[Д] = \begin{array}{c|cccc} & П & Э & Н & Л \\ \hline П & 1 & 6 & 6 & 3 \\ Э & 1/6 & 1 & 4 & 3 \\ Н & 1/6 & 1/4 & 1 & 1/2 \\ Л & 1/3 & 1/3 & 2 & 1 \end{array}$$

$W_{Д} = (0,604;\ 0,213;\ 0,064;\ 0,119);$
$\lambda_{max} = 4,35;\ ИС = 0,12;\ ОС = 0,13.$

$$[У] = \begin{array}{c|cccc} & П & Э & Н & Л \\ \hline П & 1 & 6 & 6 & 3 \\ Э & 1/6 & 1 & 4 & 3 \\ Н & 1/6 & 1/4 & 1 & 1/2 \\ Л & 1/3 & 1/3 & 2 & 1 \end{array}$$

$W_{Д} = (0,604;\ 0,213;\ 0,064;\ 0,119);$

$\lambda_{max} = 4,35;\ ИС = 0,12;\ ОС = 0,13.$

$$[А] = \begin{array}{c|cccc} & П & Э & Н & Л \\ \hline П & 1 & 1/5 & 1/3 & 1 \\ Э & 5 & 1 & 4 & 1/5 \\ Н & 3 & 1/4 & 1 & 1/4 \\ Л & 1 & 5 & 4 & 1 \end{array}$$

$W_{ОБ} = (0,127;\ 0,281;\ 0,120;\ 0,463);$

$\lambda_{max} = 5,42;\ ИС = 0,47;\ ОС = 0,52.$

$$[П] = \begin{array}{c|ccc} & M & O & P \\ \hline M & 1 & 9 & 4 \\ O & 1/9 & 1 & 8 \\ P & 1/4 & 1/8 & 1 \end{array}$$

$W_{П} = (0,721;\ 0,210;\ 0,069);$

$\lambda_{max} = 4;\ ИС = 0,33;\ ОС = 0,57.$

$$[Э] = \begin{array}{c|ccc} & M & O & P \\ \hline M & 1 & 1 & 1 \\ O & 1 & 1 & 1 \\ P & 1 & 1 & 1 \end{array}$$

$W_{Э} = (0,333;\ 0,333;\ 0,333);$

$\lambda_{max} = 3;\ ИС = 0,0;\ ОС = 0,0.$

$$[Н] = \begin{array}{c|ccc} & M & O & P \\ \hline M & 1 & 9 & 6 \\ O & 1/9 & 1 & 1/4 \\ P & 1/6 & 4 & 1 \end{array}$$

$W_{Н} = (0,713;\ 0,061;\ 0,176);$

$\lambda_{max} = 3,11;\ ИС = 0,06;\ ОС = 0,10.$

$$[Л] = \begin{array}{c|ccc} & M & O & P \\ \hline M & 1 & 5 & 5 \\ O & 1/5 & 1 & 1/3 \\ P & 1/5 & 3 & 1 \end{array}$$

$W_{Л} = (0,701;\ 0,097;\ 0,202);$

$\lambda_{max} = 3,14;\ ИС = 0,07;\ ОС = 0,12.$

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 в целях 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 5.9. 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:

$$ИО_И = ИО_1 + W_{ОБ}^T \cdot \begin{bmatrix} ИО_{21} \\ ИО_{22} \\ ИО_{23} \end{bmatrix} + W_{ОБ}^T \cdot [W_Д \;\; W_У \;\; W_А]^T \begin{bmatrix} ИО_{31} \\ ИО_{32} \\ ИО_{33} \\ ИО_{34} \end{bmatrix};$$

$$ИО_И = 0,07 + (0,701; 0,193; 0,106) \cdot \begin{bmatrix} 0,12 \\ 0,12 \\ 0,47 \end{bmatrix} + (0,701; 0,193; 0,106) \times$$

$$\times \begin{bmatrix} 0,604 & 0,213 & 0,064 & 0,119 \\ 0,604 & 0,213 & 0,064 & 0,119 \\ 0,127 & 0,281 & 0,120 & 0,463 \end{bmatrix} \cdot \begin{bmatrix} 0,33 \\ 0,00 \\ 0,06 \\ 0,07 \end{bmatrix} = 0,42.$$

Для оценки отношения однородности используют следующее выражение:

$$OO_{И} = \frac{ИО_{И}}{M(ИО_{И})},$$

где

$$M(ИО_{И}) = M(ИО_{1}) + W_{ОБ}{}^{T} \cdot \begin{bmatrix} M(ИО_{21}) \\ M(ИО_{22}) \\ M(ИО_{23}) \end{bmatrix} + W_{ОБ}{}^{T} \cdot [W_{Д} \quad W_{У} \quad W_{А}]^{T} \begin{bmatrix} M(ИО_{31}) \\ M(ИО_{32}) \\ M(ИО_{33}) \\ M(ИО_{34}) \end{bmatrix};$$

$$M(ИО_{И}) = 0,58 + (0,701; 0,193; 0,106) \cdot \begin{bmatrix} 0,9 \\ 0,9 \\ 0,9 \end{bmatrix} + (0,701; 0,193; 0,106) \times$$

$$\times \begin{bmatrix} 0,604 & 0,213 & 0,064 & 0,119 \\ 0,604 & 0,213 & 0,064 & 0,119 \\ 0,127 & 0,281 & 0,120 & 0,463 \end{bmatrix} \cdot \begin{bmatrix} 0,58 \\ 0,58 \\ 0,58 \\ 0,58 \end{bmatrix} = 2,06.$$

$$OO_{И} = \frac{ИО_{И}}{M(ИО_{И})} = \frac{0,42}{2,06} = 0,20.$$

Однородность иерархии считается удовлетворительной при значениях $OO_{И} \le 0,10$.

5.3.6. Метод сравнения объектов относительно стандартов

Метод парного сравнения альтернатив не всегда может быть эффективно применен в некоторых практических ситуациях [8].

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.

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) уровень 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.

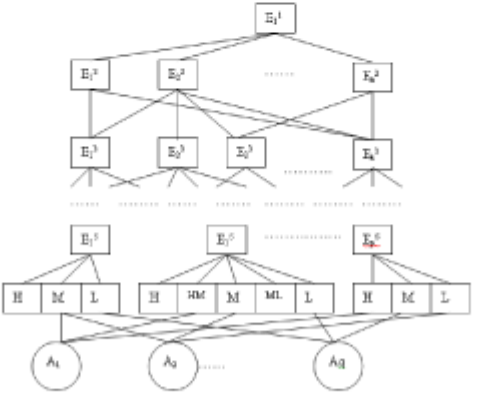


Рис. 5.15. **Иерархическая структура с учетом стандартов**

По каждому стандарту экспертом устанавливается относительная 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 и $\{C_0\}$ 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-ти балльной шкале и вычисляются вектора W_j^s.

ЛПР присваивает каждой альтернативе значение одного стандарта. Процедура идентификации проводится по всем элементам E_j^s. В результате идентификации строится матрица А следующего 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 тоже самое, умножить матрицу A на диагональную матрицу S следующего вида:

$$S = \begin{array}{c|cccc} & E_1^s & E_2^s & \dots & E_p^s \\ \hline A_1 & \left(\sum_{i=1}^{n} w_{i1}\right)^{-1} & 0 & \dots & 0 \\ A_2 & 0 & \left(\sum_{i=1}^{r} w_{i2}\right)^{-1} & \dots & 0 \\ \vdots & \dots & \dots & \dots & \dots \\ A_r & 0 & 0 & \dots & \left(\sum_{i=1}^{t} w_{ip}\right)^{-1} \end{array}$$

Множество нормированным 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.

(9 кегль) Пример 5.10. Пусть задана иерархия, представленная на рис. 5.16.

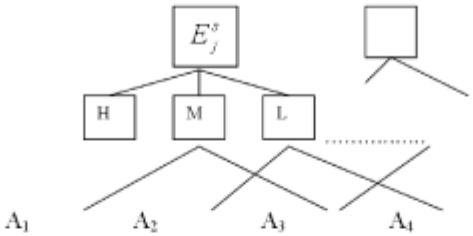


Рис. 5.16. **Одна из ветвей иерархии с учетом стандартов**

Пусть матрица предпочтений стандартов для элемента E_j^s имеет вид:

	H	M	L
H	1	5	7
M	1/5	1	3
L	1/7	1/3	1

$$W_j^S = \begin{pmatrix} 0,696 \\ 0,225 \\ 0,079 \end{pmatrix}.$$

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 второй и четвертый – низкому стандарту. Добавим еще одну альтернативу и присвоим ей значение, соответствующее высокому стандарту:

$$W_j^A = \begin{pmatrix} 0,225 \\ 0,079 \\ 0,225 \\ 0,079 \\ 0,696 \end{pmatrix}, \text{ или нормированный } W_{j\ (норм.)}^A = \begin{pmatrix} 0,173 \\ 0,061 \\ 0,173 \\ 0,061 \\ 0,534 \end{pmatrix}.$$

5.3.7. Многокритериальный выбор в иерархиях с различным количеством и составом альтернатив под критериями

В практике встречаются задачи, когда ранжируемые по множеству критериев альтернативы оцениваются экспертом не по всем критериям [2]. 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 количество 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, используя метод парного сравнения или метод сравнения альтернатив относительно стандартов. На основе экспертных оценок строится матрица A следующего вида:

$$A = \begin{array}{c|cccc} & E_1 & E_2 & \dots & E_p \\ \hline A_1 & a_{11} & a_{12} & \dots & a_{1p} \\ A_2 & a_{21} & a_{22} & \dots & a_{2p} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ A_r & a_{r1} & a_{r2} & \dots & a_{rp} \end{array}$$

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 количество 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 $\overline{X}$.

Процедура 4. Формируются следующие диагональные матрицы S и L:

$$S = \begin{array}{c|cccc} & E_1 & E_2 & \dots & E_p \\ \hline & \left(\sum_{i=1}^{r} a_{j1}\right)^{-1} & 0 & \dots & 0 \\ & 0 & \left(\sum_{i=1}^{r} a_{i2}\right)^{-1} & \dots & 0 \\ & \vdots & \vdots & \dots & \vdots \\ & 0 & 0 & \dots & \left(\sum_{i=1}^{r} a_{ip}\right)^{-1} \end{array}$$

$$L = \begin{array}{c|cccc} & E_1 & E_2 & \dots & E_p \\ \hline & R_1/N & 0 & \dots & 0 \\ & 0 & R_2/N & \dots & 0 \\ & \vdots & \vdots & \dots & \vdots \\ & 0 & 0 & \dots & R_p/N \end{array}$$

R_j – количество альтернатив, находящихся под критерием E_j.

$N = \sum_{j=1}^{p} R_j$ – суммарное количество альтернатив, находящихся под всеми критериями.

С помощью матрицы S нормируются векторы приоритетов альтернатив, образующих матрицу A, путем умножения последней на S справа. Использование критерия L позволяет эксперту или ЛПР изменять при необходимости вес альтернатив, связанных с соответствующими критериями пропорционально отношению R_i/N. Этим обеспечивается повышение приоритета альтернатив, образующих большие группы, и снижение приоритета альтернатив в группах с их относительно небольшим количеством. Необходимость приведенной вычислительной процедуры обусловлена тем, что у критериев с высоким приоритетом в иерархии может находиться большое количество альтернатив, а у критериев с низким приоритетом – значительно меньшее количество 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. Данная процедура реализуется последовательным 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.

$$B = \begin{array}{c|cccc} & E_1 & E_2 & \dots & E_r \\ \hline & \left(\sum_{i=1}^{r} x_i\right)^{-1} & 0 & \dots & 0 \\ & 0 & \left(\sum_{i=1}^{r} x_i\right)^{-1} & \dots & 0 \\ & \vdots & \vdots & \dots & \vdots \\ & 0 & 0 & \dots & \left(\sum_{i=1}^{r} x_i\right)^{-1} \end{array},$$

x_i – значения ненормированного вектора приоритетов альтернатив, полученное после последовательного перемножения матриц $[A]\cdot[S]\cdot[L]\cdot\overline{X}$;

r – количество альтернатив.

Существуют иерархии, у которых альтернативы сгруппированы в подмножества $\{A_1, A_2, \ldots, A_n\}$, $\{A'_1, A'_2, \ldots, A'_s\}$, $\{A''_1, A''_2, \ldots, A''_l\}$, а элементы каждого из таких подмножеств связаны, в свою очередь, с определенными группами критериев $\{K_{11}, K_{12}, \ldots, K_{1l}\}$, $\{K_{21}, K_{22}, \ldots, K_{2r}\}$, $\{K_{n1}, K_{n2}, \ldots, K_{np}\}$ (рис. 5.17).

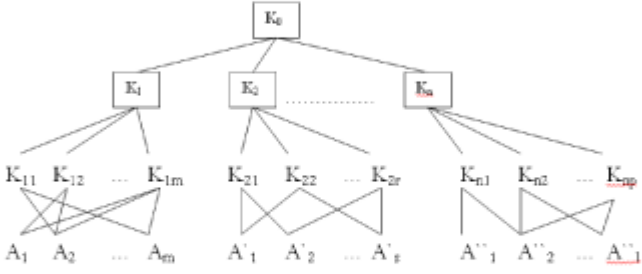


Рис. 5.17. **Иерархия с несколькими ветвями**

Дерево состоит из ряда самостоятельных иерархических ветвей.

Алгоритм синтеза для иерархии с несколькими ветвями.

Шаг 1. Вычисляются векторы приоритетов альтернатив относительно критериев K_{ij}.

$$\{W^{A}_{K_{11}}, W^{A}_{K_{12}}, \ldots, W^{A}_{K_{1m}}\};$$

$$\{W^{A'}_{K_{21}}, W^{A'}_{K_{22}}, \ldots, W^{A'}_{K_{2r}}\};$$

$$\{W^{A''}_{K_{n1}}, W^{A''}_{K_{n2}}, \ldots, W^{A''}_{K_{np}}\}.$$

Шаг 2. Строятся 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:

$$W_1^A = [A_1][S_1][L_1]\overline{X}_1[B_1];$$

$$W_2^A = [A_2][S_2][L_2]\overline{X}_2[B_2];$$

.....

$$W_n^A = [A_n][S_n][L_n]\overline{X}_n[B_n].$$

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. Вычисляется вектор приоритетов критериев X_0 относительно фокуса иерархии K_0.

Шаг 5. Строится результирующая матрица A_0, у которой наименованиями строк являются все рассматриваемые альтернативы, а наименованиями столбцов – критерии K_i. При этом результирующая матрица имеет следующий вид:

$$A_0 = \begin{array}{c|cccc} & K_1 & K_2 & \dots & K_n \\ \hline A_1 & & & & \\ A_2 & W_1^A & 0 & \dots & 0 \\ \dots & & & & \\ A_m & & & & \\ \hline A'_1 & & & & \\ A'_2 & 0 & W_2^A & \dots & 0 \\ \dots & & & & \\ A'_r & & & & \\ \hline A''_1 & & & & \\ A''_2 & 0 & 0 & \dots & W_n^A \\ \dots & & & & \\ A''_p & & & & \end{array}$$

Шаг 6. Определяется результирующий нормированный вектор приоритетов W_0^A всех рассматриваемых альтернатив относительно фокуса иерархии K_0 на основании выражения:

$$W_0^A = [A_0][S_0][L_0]\overline{X}_0[B_0].$$

Достоинством метода является направленность 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 мы будем понимать применение математических, количественных методов для обоснования решений во всех областях целенаправленной человеческой деятельности.

Основные этапы решения любой задачи в исследовании операций следующие:

- 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 ро-

ли 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 (ДП) 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 для 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 .

Рассматривая управляемый процесс, предполагаем, что управление можно разбить на n шагов, т.е. решение прини-

мается 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 $u = (u_1, u_2, \ldots, u_n)$ – управление, переводящее систему из состояние x_0 в состояние x_n. Обозначим через x_k состояние системы после k-ого шага управления. Получаем последовательность состояний $x_0, x_1, \ldots, x_{k-1}, x_k, x_{k+1}, \ldots, x_n$. (рис. 5. 18)

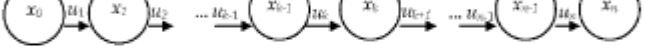


Рис. 5.18. **Переход системы из одного состояния в другое в результате управляющих сигналов**

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):

$$x_k = \phi_k(x_{k-1}, u_k), \tag{5.2}$$

где $k = \overline{1, n}$ – уравнения состояний;

ϕ_k – оператор перехода

2. Целевая функция (1) является аддитивной от показателя эффективности каждого шага, т.е. выигрыш за всю операцию складывается из выигрышей на отдельных шагах.

$$Z = F(x_0, u) = \sum_{k=1}^{n} f_k(x_{k-1}, u_k); \quad (5.3)$$

$$f_k(x_{k-1}, u_k) = Z_k \quad (5.4)$$

где Z_k – показатель эффективности шага k.

Общая постановка задачи ДП. Определите 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 n шагах, либо же строить оптимальное управление шаг за шагом, на каждом этапе расчета оптимизируя лишь один шаг. Обычно второй способ оказывается проще, чем первый, особенно при большом количестве 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 не трудно. 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, если выбирается на данном шаге

управление, при котором эффективность этого шага максимальна, если этот шаг лишит 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, необходимо было бы все наличные средства вложить в производство предметов потребления. Но правильно ли будет такое решение с точки зрения 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, снизится, 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 предстоящих 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 не известно, 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 из возможных исходов предпоследнего шага известно условное оптимальное управление и соответствующий ему условный оптимальный выигрыш на n-м шаге. Теперь можно оптимизировать управление на предпоследнем, $(n-1)$-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 $(n-1)$-шаге, при котором выигрыш за последние два шага максимален. Так мы 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 др., пока не дойдем да первого.

Предположим, что все условные оптимальные управления и условные оптимальные выигрыши за весь «хвост» процесса нам известны. Это значит: известно, что надо делать, как управлять на данном шаге и что из этого получится 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, состояние системы изменится на некоторое новое x_1^*; в этом состоянии подошли ко второму шагу. Тогда тоже известно условное оптимальное управление u_2^*, которое к концу второго шага переводит систему в состояние x_2^*, и др. 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 находятся 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 $u_1^*, u_2^*, \ldots, u_n^*$.

Первый этап – условная оптимизации – несравненно сложнее второго. Второй этап почти не требует дополнительных вычислений.

Принцип оптимальности Беллмана. Уравнения Беллмана. Предположим, что задача

$$Z = F(x_0, u) = \sum_{k=1}^{n} f_k(x_{k-1}, u_k) \to max;$$

$$x_k = \phi_k(x_{k-1}, u_k), \quad k = \overline{1, n};$$

$$u_k \in U_k, \quad k = \overline{1, n};$$

$$x_k \in X_k, \quad k = \overline{0, n}$$

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 выигры-

шей 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.

Рассматривая 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 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. Этот 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} и 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).

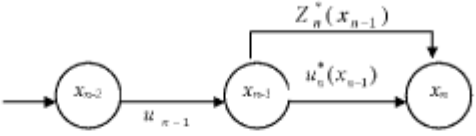


Рис. 5.19. **Оптимальное управление на двух последних шагах**

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 (5.6) 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* –1)-й и др.

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.

$$Z_k^*(x_{k-1}) = \max_{u_k}\{f_k(x_{k-1}, u_k) + Z_{k+1}^*(\phi(x_{k-1}, u_k))\}, k = \overline{n-1, 1} \qquad (5.8)$$

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:

$$Z_{max} = Z_1^*(x_0);$$

$$u_1^* = u_1^*(x_0) \to x_1^* = \phi_1(x_0, u_1^*) \to u_2^* = u_2^*(x_1^*) \to \ldots \to u_n^* = u_n^*(x_{n-1}^*).$$

Заключение. Рассмотренные нами методы принятия решений активно могут использоваться при аудите информационной безопасности, что является сегодня одним из наиболее эффективных инструментов для получения независимой и объективной оценки текущего уровня защищённости 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 однократная процедура, а должен проводиться на регулярной основе. Только в этом случае аудит будет приносить реальную пользу и способствовать повышению уровня информационной безопасности компании.

В приложении 5.1. рассматриваются 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 найдите приближенное $\overline{W}$ и точное W значение главного собственного вектора. Оценить погрешность $\Delta\overline{W} = |W - \overline{W}|$. Определите, является ли матрица парных сравнений согласованной:

1.1. $A = \begin{pmatrix} 1 & 4 & 6 & 8 \\ 1/4 & 1 & 3 & 2 \\ 1/6 & 1/3 & 1 & 3 \\ 1/8 & 1/2 & 1/3 & 1 \end{pmatrix}$

1.2. $A = \begin{pmatrix} 1 & 1/4 & 6 & 8 \\ 4 & 1 & 1/3 & 2 \\ 1/6 & 3 & 1 & 3 \\ 1/8 & 1/2 & 1/3 & 1 \end{pmatrix}$

1.3. $A = \begin{pmatrix} 1 & 3 & 6 & 9 \\ 1/3 & 1 & 1/4 & 2 \\ 1/6 & 4 & 1 & 3 \\ 1/9 & 1/2 & 1/3 & 1 \end{pmatrix}$

1.4. $A = \begin{pmatrix} 1 & 6 & 6 & 8 \\ 1/6 & 1 & 3 & 3 \\ 1/6 & 1/3 & 1 & 1/2 \\ 1/8 & 1/3 & 2 & 1 \end{pmatrix}$

1.5. $A = \begin{pmatrix} 1 & 8 & 3 & 2 \\ 1/8 & 1 & 3 & 2 \\ 1/3 & 1/3 & 1 & 1 \\ 1/2 & 1/2 & 1 & 1 \end{pmatrix}$

1.6. $A = \begin{pmatrix} 1 & 4 & 1 & 4 \\ 1/4 & 1 & 6 & 2 \\ 1 & 1/6 & 1 & 3 \\ 1/4 & 1/2 & 1/3 & 1 \end{pmatrix}$

1.7. $A = \begin{pmatrix} 1 & 4 & 6 & 1 \\ 1/4 & 1 & 3 & 2 \\ 1/6 & 1/3 & 1 & 3 \\ 1 & 1/2 & 1/3 & 1 \end{pmatrix}$

1.8. $A = \begin{pmatrix} 1 & 6 & 1/2 & 8 \\ 1/6 & 1 & 1/8 & 2 \\ 2 & 8 & 1 & 3 \\ 1/8 & 1/2 & 1/3 & 1 \end{pmatrix}$

1.9. $A = \begin{pmatrix} 1 & 4 & 1/9 & 8 \\ 1/4 & 1 & 1 & 2 \\ 9 & 1 & 1 & 3 \\ 1/8 & 1/2 & 1/3 & 1 \end{pmatrix}$

1.10. $A = \begin{pmatrix} 1 & 4 & 6 & 8 \\ 1/4 & 1 & 8 & 1/7 \\ 1/6 & 1/8 & 1 & 3 \\ 1/8 & 7 & 1/3 & 1 \end{pmatrix}$

Задание 2. Преобразуйте матрицу парных сравнений A из задания 1 таким образом, чтобы она стала абсолютно согласованной ($OC = 0$). При этом:

а) оставить первую строку матрицы без изменений;

б) оставить последнюю строку матрицы без изменения.

Задание 3. Найдите 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. $A = \begin{pmatrix} 1 & 3 & 6 & 8 \\ 1/3 & 1 & 4 & 5 \\ 1/6 & 1/4 & 1 & 3 \\ 1/8 & 1/5 & 1/3 & 1 \end{pmatrix}$

3.2. $A = \begin{pmatrix} 1 & 4 & 7 & 8 \\ 1/4 & 1 & 1/3 & 2 \\ 1/7 & 3 & 1 & 2 \\ 1/8 & 1/2 & 1/2 & 1 \end{pmatrix}$

3.3. $A = \begin{pmatrix} 1 & 3 & 2 & 8 \\ 1/3 & 1 & 1/4 & 1/2 \\ 1/2 & 4 & 1 & 3 \\ 1/8 & 2 & 1/3 & 1 \end{pmatrix}$

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. $A = \begin{pmatrix} 1 & 4 & 3 & 5 \\ 1/4 & 1 & 3 & 2 \\ 1/3 & 1/3 & 1 & 1/3 \\ 1/5 & 1/2 & 3 & 1 \end{pmatrix}$

3.6. $A = \begin{pmatrix} 1 & 4 & 2 & 6 \\ 1/4 & 1 & 5 & 2 \\ 1/2 & 1/5 & 1 & 3 \\ 1/6 & 1/2 & 1/3 & 1 \end{pmatrix}$

3.7. $A = \begin{pmatrix} 1 & 4 & 6 & 5 \\ 1/4 & 1 & 1 & 2 \\ 1/6 & 1 & 1 & 3 \\ 1/5 & 1/2 & 1/3 & 1 \end{pmatrix}$

3.8. $A = \begin{pmatrix} 1 & 7 & 1/2 & 8 \\ 1/7 & 1 & 1/8 & 3 \\ 2 & 8 & 1 & 1/5 \\ 1/8 & 1/3 & 5 & 1 \end{pmatrix}$

3.9. $A = \begin{pmatrix} 1 & 4 & 6 & 8 \\ 1/4 & 1 & 8 & 1/7 \\ 1/6 & 1/8 & 1 & 3 \\ 1/8 & 7 & 1/3 & 1 \end{pmatrix}$

3.10. $A = \begin{pmatrix} 1 & 4 & 1/9 & 8 \\ 1/4 & 1 & 1 & 2 \\ 9 & 1 & 1 & 3 \\ 1/8 & 1/2 & 1/3 & 1 \end{pmatrix}$

Задание 4. Найдите 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 (см. рис. 5.5), определите приоритет провайдера, выполнив иерархический синтез. Матрица сравнения критериев относительно цели имеет вид:

5.1. $A = \begin{pmatrix} 1 & 4 & 6 & 2 & 7 \\ 1/4 & 1 & 3 & 4 & 2 \\ 1/6 & 1/3 & 1 & 2 & 1 \\ 1/2 & 1/4 & 1/2 & 1 & 1/3 \\ 1/7 & 1/2 & 1 & 3 & 1 \end{pmatrix}$

5.2. $A = \begin{pmatrix} 1 & 5 & 8 & 2 & 7 \\ 1/8 & 1 & 3 & 4 & 1/2 \\ 1/8 & 1/3 & 1 & 2 & 1 \\ 1/2 & 1/4 & 1/2 & 1 & 1/3 \\ 1/7 & 2 & 1 & 3 & 1 \end{pmatrix}$

5.3. $A = \begin{pmatrix} 1 & 4 & 2 & 2 & 7 \\ 1/4 & 1 & 3 & 2 & 2 \\ 1/2 & 1/3 & 1 & 2 & 1 \\ 1/2 & 1/2 & 1/2 & 1 & 4 \\ 1/7 & 1/2 & 1 & 1/4 & 1 \end{pmatrix}$

5.4. $A = \begin{pmatrix} 1 & 5 & 1 & 2 & 3 \\ 1/8 & 1 & 1/4 & 4 & 1/2 \\ 1 & 4 & 1 & 2 & 1 \\ 1/2 & 1/4 & 1/2 & 1 & 1/3 \\ 1/3 & 2 & 1 & 3 & 1 \end{pmatrix}$

5.5. $A = \begin{pmatrix} 1 & 4 & 6 & 2 & 7 \\ 1/4 & 1 & 3 & 1/2 & 1/4 \\ 1/6 & 1/3 & 1 & 2 & 1 \\ 1/2 & 2 & 4 & 1 & 5 \\ 1/7 & 1/2 & 1 & 1/5 & 1 \end{pmatrix}$

5.6. $A = \begin{pmatrix} 1 & 1/5 & 2 & 2 & 7 \\ 5 & 1 & 3 & 4 & 1/2 \\ 1/2 & 1/3 & 1 & 2 & 1 \\ 1/2 & 1/4 & 1/2 & 1 & 4 \\ 1/7 & 2 & 1 & 1/4 & 1 \end{pmatrix}$

5.7. $A = \begin{pmatrix} 1 & 1 & 6 & 2 & 7 \\ 1 & 1 & 5 & 4 & 5 \\ 1/6 & 1/5 & 1 & 1/4 & 1 \\ 1/2 & 1/4 & 4 & 1 & 6 \\ 1/7 & 1/5 & 1 & 1/6 & 1 \end{pmatrix}$

5.8. $A = \begin{pmatrix} 1 & 5 & 8 & 2 & 1/2 \\ 1/8 & 1 & 3 & 1/4 & 1/2 \\ 1/8 & 1/3 & 1 & 1/7 & 1 \\ 1/2 & 4 & 7 & 1 & 1/3 \\ 2 & 2 & 1 & 3 & 1 \end{pmatrix}$

5.9. $A = \begin{pmatrix} 1 & 1/4 & 1/3 & 2 & 1/5 \\ 4 & 1 & 3 & 4 & 2 \\ 3 & 1/3 & 1 & 2 & 1 \\ 1/2 & 1/4 & 1/2 & 1 & 1/3 \\ 5 & 1/2 & 1 & 3 & 1 \end{pmatrix}$

5.10. $A = \begin{pmatrix} 1 & 5 & 1/3 & 2 & 7 \\ 1/8 & 1 & 3 & 1/4 & 1 \\ 3 & 1/3 & 1 & 2 & 1 \\ 1/2 & 4 & 1/2 & 1 & 8 \\ 1/7 & 1 & 1 & 1/8 & 1 \end{pmatrix}$

Матрицы сравнения альтернатив относительно критериев необходимо взять из предыдущих заданий по следующему правилу (табл. 5.7).

Таблица 5.7

Правила сравнения

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. Постройте трехуровневую иерархическую структуру (пример, см. рис. 5.14). Используя мнения двух экспертов, произведите синтез иерархии, оцените ее согласованность, сделайте соответствующие выводы.

Приложение 5.1.

Использование методов принятия решений в разработке комплексной системы защиты информации

Разработка и эксплуатация сложных информационных систем, 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 др.), 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 лица, принимающего решение.

Можно сказать, что методы обработки мнений экспертов позволяют структурировать множество альтернатив при различных суждениях экспертов. При формировании набора критериев можно учитывать мнение каждого эксперта, а затем объединить это множество в одно. 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 выставляются 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 рассчитываются суммы строк.
4. Строится ранжировка альтернатив:

• ранг 1 присваивается альтернативе, имеющей максимальную строчную сумму;

• ранг 2 – альтернативе, имеющей следующую по величине сумму и так далее.

Таким образом, получается обобщенное мнение экспертов.

(9 кегль) **Пример П 5.1.**

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. П 5.1.

Таблица П. 5.1

Попарное сравнение критериев

	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	**ранг 3**
минимизация расходов на КСЗИ	1		1	1	0,5	3,5	**ранг 1**
комплексность технологий и решений	0,5	0		0,5	0,5	1,5	**ранг 3**
увеличение срока службы инфраструктуры	0,5	0	0,5		0,5	1,5	**ранг 3**
снижение эксплуатационных расходов	0,5	0,5	0,5	0,5		2	**ранг 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 снова 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_i^k и сведение этих значений в морфологическую матрицу.

Набор значений различных показателей (по одному из каждой строки) представляет собой возможный вариант решения проблемы (например, $p_{11}, p_{23}, \ldots, p_{kn}$). Общее число вариантов, содержащихся в морфологической матрице, равно $N = k_1 k_2 \ldots k_n$, где $k_1 k_2 \ldots k_n$ – число значений i-го показателя.

4. Оценка всех имеющихся в морфологической матрице вариантов.
5. Выбор из морфологической матрицы наиболее привлекательного варианта решения проблемы.

Пример П. 5.2.

Рассмотрим объект, который представляет собой помещение из двух комнат: приемная и кабинет директора, рис. П. 5.1. Организация, расположенная в данном помещении, занимается сбором и анализом коммерческой информации. Следовательно, возникает проблема защиты коммерческой и служебной информации.

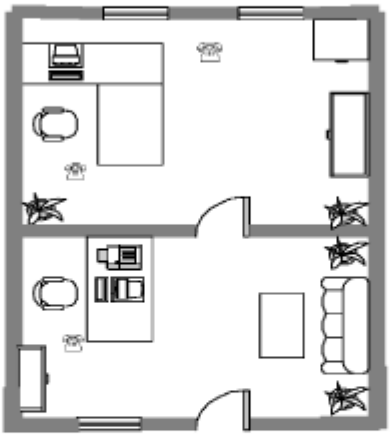


Рис. П. 5.1. **Схема помещений организации**

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 угроза должна рассматриваться в следующем порядке: чему она угрожает, как обнаруживается, частота ее проявления, последствия, как предотвращается.

В нашем случае множество угроз $Y = \{y_1, y_2 \ldots y_n\}$ *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 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. П. 5.2 приведена морфологическая матрица, соответствующая обследуемому объекту.

Таблица П. 5.2

Морфологическая матрица

Функциональные подсистемы	**Элементарные альтернативы**		
Защита окон	A11	A12	A13
Защита от ПЭМИН	A21	A22	
Защита телефонной линии	A31	A32	A33
Защита от НСД персонала	A41	A42	A43
Защита от НСД злоумышленника	A51	A52	A53
Съем с помощью закладок и диктофонов	A61	A62	A63
Защита от вирусов	A71	A72	
Защита от пожаров	A81	A82	

Условные обозначения:

A11 – установка решеток;
A12 – установка жалюзи;
A13 – установка генератора виброакустических помех;
A21 – экранирование;
A22 – снижение уровней информационных ПЭМИН и повышение уровней помех;

A31 – защита телефонного аппарата и линий фильтрами, диодами, конденсаторами, подключенными в цепь;
A32 – изменение напряжения в телефонной линии при разговоре;
A33 – генерация высокочастотных помех в телефонной линии;

A41 – парольная защита;
A42 – система шифрования;
A43 – использование сейфа;

A51 – система контроля доступа;
A52 – система видеонаблюдения;
A53 – охрана периметра;

А61 – использование принципа сравнения уровня сигнала на антенне внутри онтролируемой зоны и вне ее;
А62 – постоянный анализ эфира и фиксация вновь появившихся источников излучения;
А63 – устройство обнаружения диктофонов;

А71 – использование антивирусных программ;
А72 – использование лицензионного программного обеспечения;

А81 – использование охранно-пожарной сигнализации;
А82 – средства пожарной безопасности.

Правила 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 (см. рис. П. 5.2), обозначив перечисленные угрозы через $У_i$, объекты $О_i$.

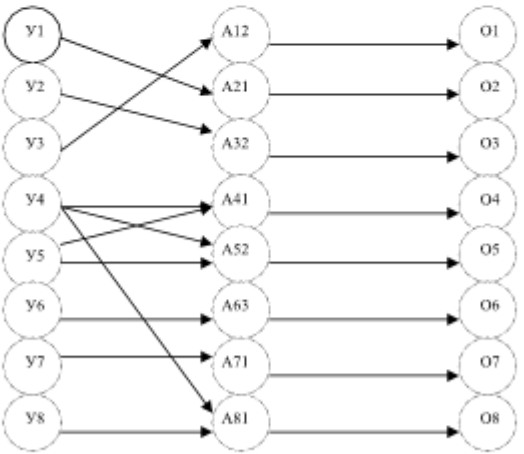


Рис. П. 5.2. **Трехдольный граф для одного из вариантов защиты**

Оценка альтернатив с использованием критериального метода. Наиболее популярным для оценки альтернатив – 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. Пример такого решения – 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 функции аддитивные $Z_\phi = \sum_{i=1}^{N} \frac{P_i f_i(x)_i}{a_i}$ и мультипликативные $Z_\phi = \prod_{i=1}^{N} \frac{f_i(x)^{P_i}}{a_i}$, 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 ком-

пенсации: 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, (в порядке иерархической значимости):

- *устойчивость*, для сложных систем, какими являются КСЗИ, характерны такие формы устойчивости, как надежность, живучесть и др.;
- *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 др.;
- *управляемость* – 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 др.;
- *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* – наиболее сложное качество системы. Самоорганизующаяся система способна изменять свою структуру, параметры, алгоритмы функционирования для повышения эффективности. Принципиально важное свойство этого уровня – 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; условиями 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, потребного для достижения цели;
- *оценка алгоритма функционирования* является 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 выполнения ранжирования *методом строчных сумм*, рассмотренным в предыдущем подразделе, 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, то 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 $i = 1, ..., n$ – количетсво целей;

$j = 1, ..., m_i$ – количество критериев для i-той цели.

Схема целей и критериев представлена на рис. П. 5.3.

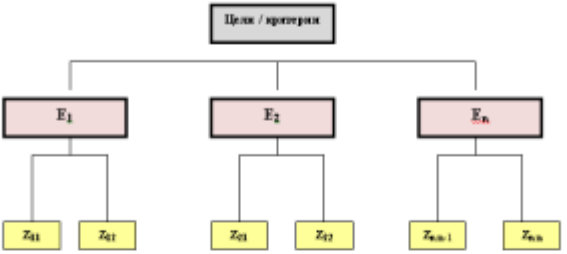


Рис. П. 5.3. **Схема целей и критериев**

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. П. 5. 3.

Таблица П. 5.3

Матрица относительных предпочтений

Альтернативные проекты	Суммарные веса критериев			
	q_{11}	q_{12}	…	q_{nn}
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. П. 5.4. 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 П. 5.4

Финальная матрица оценки альтернатив

Критерии	Z_{11}	Z_{12}	...	Z_{xm}	Финальная оценка
Альтернативные проекты	Суммарные веса критериев				
	q_{11}	q_{12}	...	q_{xm}	
A_1	$P_{1\,1} * q_{11}$	$P_{12} * q_{12}$	...	$P_{1k} * q_{xm}$	F_1
...	...	...	...	...	...
A_n	$P_{n1} * q_{11}$	$P_{n2} * q_{12}$	...	$P_{nk} * q_{xm}$	F_n

Полученная матрица финальных оценок используется для сравнения инновационных проектов и принятия решений об их эффективности.

Пример П. 5.3. Для сравнения альтернативных вариантов построения комплексной системы защиты информации выбирается цель – *повышение эффективности комплексной системы защиты информации*. На рис. П. 5.4 показана схема попарного сравнения целей и критериев.

1. Попарное сравнение и ранжирование подцелей *E1,E2,...* выполняется с использованием метода срочных сумм.

2. Попарное сравнение и ранжирование критериев *Z11, Z12,...; Z21, Z22...; ...* также осуществляется методом строчных сумм.

Например, попарное сравнение критериев для подцели *E1 Совершенствование технологий эксплуатации КСЗИ*, табл. П. 5.5.

Таблица П. 5.5

Попарное сравнение критериев для подцели *E1*

	Z11	Z12	Z13	Z14	Z15	Сумма строк	Веса критериев C_{ij}
Z11		0	0,5	0,5	0,5	1,5	0,15
Z12	1		1	1	0,5	3,5	0,35
Z13	0,5	0		0,5	0,5	1,5	0,15
Z14	0,5	0	0,5		0,5	1,5	0,15
Z15	0,5	0,5	0,5	0,5		2,0	0,2
						Общая сумма 10	

Аналогичным образом получают веса подцелей g_j на множестве *E(E1,E2,...)*.

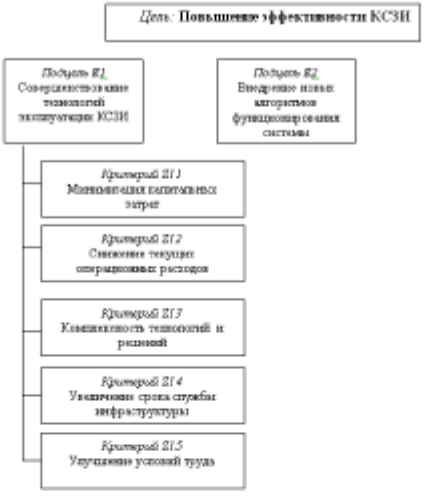


Рис. П. 5.4. **Схема попарного сравнения целей и критериев**

3. Веса подцелей и критериев размещаются в сводной (табл. П. 5.6).

Таблица П. 5.6

Сводная таблица весов подцелей и критериев

N i	Подцели E11,E12,...	Веса целей g_i	Критерии	Веса критериев c_{ij}	Суммарные веса критериев q_{ij}
1	Совершенствование технологии эксплуатации КСЗИ	0.1	Z11 Z12 Z13 Z14 Z15	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	Z21 . .	. . .	. . .
...	...	...	...	...	...

4. Далее формируется матрица относительных предпочтений (см. табл. П. 5.3)
5. Формируется финальная матрица оценки альтернативных проектов (см. табл. П. 5.4)

Заключение. Для практического применения описанных методов принятия решений при разработке КСЗИ на кафедре информационной безопасности и программной инженерии РГСУ под руководством автора 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.

---

[1] Пыжьянова О. Дипломный проект «Программные средства для морфологического анализа альтернативных вариантов системы защиты объекта информатизации» – М., РГСУ, 2007.
Трифонов Д. Курсовая работа «Морфологический анализ альтернативных вариантов системы защиты объекта информатизации» – М., РГСУ, 2008.

[2] Ревин А. Дипломная работа «Моделирование процессов в системе защиты информации с использованием метода трехдольных графов» – М., РГСУ, 2007.

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-практическое издание. Серия «Информатизация России на пороге XXI века». – М.: СИНТЕГ, 1998.
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.

Словарь терминов

Активный аудит – оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации.

Аудит – это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день).

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности.

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.

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

Защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Идентификация – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.

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.

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

Межсетевой экран (брандмауэр, firewall) – это программная или программно-аппаратная система, которая контролирует информационные потоки, поступающие в информационную систему и/или выходящие из нее, также обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

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.

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.

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.

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.

Угроза «информационной безопасности» – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется **атакой** на информационную систему.

Удаленная угроза – потенциально возможное информационное разрушающее воздействие на распределенную вычислительную сеть, осуществляемая программно по каналам связи.

Целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Электронная цифровая подпись – представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом.