Министерство образования Республики Беларусь
БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра «Информационные технологии в управлении»

В.Ф. Голиков

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И НАДЕЖНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Пособие для студентов специальностей 1-40 01 01 «Программное обеспечение информационных технологий» и 1-53 01 02 «Автоматизированные системы обработки информации» всех форм обучения

В 2 частях

Ч а с т ь 1

Минск
БНТУ
2010

УДК 621.391.25 (076)
ББК 32.811я7
Г 60

Рецензенты:
Л.М. Лыньков, *И.Е. Зуйков*

Голиков, **В.Ф.**

Г 60 Безопасность информации и надежность компьютерных систем: пособие для студентов специальностей 1-40 01 01 «Программное обеспечение информационных технологий» и 1-53 01 02 «Автоматизированные системы обработки информации» всех форм обучения: в 2 ч. / В.Ф. Голиков. – Минск: БНТУ, 2010. – Ч.1. – 86 с.

ISBN 978-985-525-134-8 (Ч.1).

Рассмотрены методы и средства защиты информации в компьютерных системах за исключением криптографических, а также надежность компьютерной техники. Особое внимание уделено защите от утечки информации по техническим каналам и от несанкционированного доступа. Приведены общие сведения по надежности компьютерной техники и методам ее расчета.

Пособие предназначено для студентов высших учебных заведений, обучающихся по специальностям 1-40 01 01 «Программное обеспечение информационных технологий» и 1-53 01 02 «Автоматизированные системы обработки информации», а также будет полезно для студентов других специальностей, изучающих информационные технологии.

УДК 621.391.25 (076)
ББК 32.811я7

ISBN 978-985-525-134-8 (Ч.1)
ISBN 978-985-525-301-4

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ В ЗАЩИТУ ИНФОРМАЦИИ

Ученые, анализируя тот или иной отрезок истории развития человеческого общества, присваивают ему краткое наименование, в основе которого лежит наиболее характерное свойство, присущее именно данному отрезку истории. Известны раз-личные классификации, например, по классовым признакам, по технологическим и т.д. Если следовать технологической классификации, то сегодня человечество переходит от индустриального общества к информационному. Информация из абстрактного «знания» превращается в материальную силу. Информационные технологии коренным образом изменяют облик материального производства, позволяют экономить материальные ресурсы, создавать новые приборы и системы, в буквальном смысле изменили наши представления о времени и пространстве.

Однако широкое внедрение в жизнь информационных технологий, управляющих жизненно важными процессами, к сожалению, сделало их достаточно уязвимыми со стороны естественных воздействий среды и искусственных воздействий со стороны человека. Возникла проблема обеспечения безопасности информационных систем в широком смысле слова или защиты информации в более узкой постановке.

1.1. Цели защиты информации. Основные понятия

Целями защиты являются: предотвращение утечки, хищения, утраты, искажения, подделки, несанкционированных действий по уничтожению, модификации, копированию, блокированию документированной информации и иных форм незаконного вмешательства в информационные системы.

Под информацией будем понимать сведения о лицах, предметах, фактах, событиях, явлениях и процессах.

Информация может существовать в виде документа (бумажного), физических полей и сигналов (электромагнитных,

акустических, тепловых и т.д.), биологических полей (память человека).

В дальнейшем будем рассматривать информацию в документированной (на бумаге, дискете и т.д.) форме, в форме физических полей (радиосигналы, акустические сигналы). Среду, в которой информация либо создается, либо передается, обрабатывается, хранится, будем называть информационным объектом.

Под безопасностью информационного объекта (ИО) будем понимать его защищенность от случайного или преднамеренного вмешательства в нормальный процесс его функционирования.

Природа воздействия на ИО может быть двух видов: непреднамеренной (стихийные бедствия, отказы, ошибки персонала и т.д.) и преднамеренной (действия злоумышленников). Все воздействия могут привести к последствиям (ущербу) трех видов: нарушению конфиденциальности, нарушению целостности, нарушению доступности.

Нарушение конфиденциальности – нарушение свойства информации быть известной только определенным субъектам.

Нарушение целостности – несанкционированное изменение, искажение, уничтожение информации.

Нарушение доступности (отказ в обслуживании) – нарушается доступ к информации, нарушается работоспособность объекта, доступ в который получил злоумышленник.

В отличие от разрешенного (санкционированного) доступа к информации в результате преднамеренных действий злоумышленник получает несанкционированный доступ (НСД). Суть НСД состоит в получении нарушителем доступа к объекту в нарушении установленных правил.

Под угрозой информационной безопасности объекта будем понимать возможные воздействия на него, приводящие к ущербу.

Некоторое свойство объекта, делающее возможным возникновение и реализацию угрозы, будем называть уязвимостью.

Действие злоумышленника, заключающееся в поиске и использовании той или иной уязвимости, будем называть атакой.

Целью защиты ИО является противодействие угрозам безопасности.

Защищенный ИО – это объект со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.

Комплексная защита ИО – совокупность методов и средств (правовых, организационных, физических, технических, программных).

Политика безопасности – совокупность норм, правил, рекомендаций, регламентирующих работу средств защиты ИО от заданного множества угроз безопасности.

Схематично основное содержание предмета защиты информации представлено на рис. 1.1.

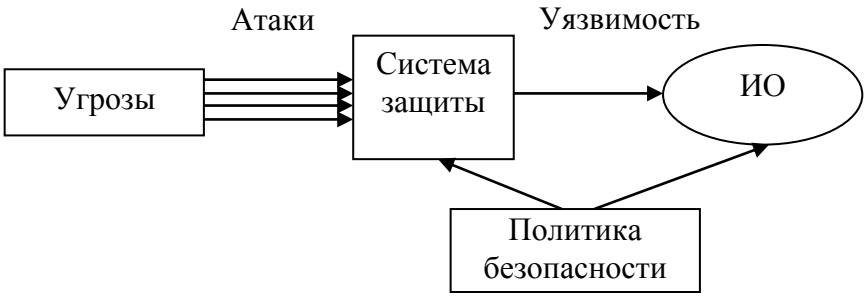

Рис. 1.1. Содержание предмета защиты информации

1.2. Классификация угроз, методов и средств защиты информации

Под угрозой информационной безопасности объекта будем понимать возможные воздействия на него, приводящие к ущербу. К настоящему времени известно большое количество угроз. Приведем упрощенную их классификацию. Угрозы делятся по свойству информации, против которого они направлены: угрозы физической и логической целостности (уничтожение или искажение информации); угрозы конфиденциальности информации; угрозы доступности (работоспособности); угрозы праву собственности.

По происхождению: случайные (отказы, сбои, ошибки, стихийные явления), преднамеренные (злоумышленные действия людей).

По источникам: люди (персонал, посторонние); технические устройства; модели, алгоритмы, программы; внешняя среда (состояние атмосферы, побочные шумы, сигналы и наводки).

Рассмотрим более подробно перечисленные угрозы.

Случайные угрозы обусловлены недостаточной надежностью аппаратуры и программных продуктов, недопустимым уровнем внешних воздействий, ошибок персонала. Методы оценки воздействия этих угроз рассматриваются в других дисциплинах (теории надежности, программировании, инженерной психологии и т.д.).

Преднамеренные угрозы связаны с действиями людей. Это и работники спецслужб, хакеры, работники самого объекта. Огромное количество разнообразных ИО делает бессмысленным перечисление всех возможных угроз для информационной безопасности, поэтому в дальнейшем при изучении того или иного раздела мы будем рассматривать основные угрозы для конкретных объектов. Например, для несанкционированного доступа к информации вычислительной системы злоумышленник может воспользоваться штатными каналами доступа, если нет никаких мер защиты: через терминалы пользователей; через терминал администратора системы; через удаленные терминалы и через нештатные каналы: побочное э/м излучение информации с аппаратуры системы; побочные наводки информации по сети электропитания и заземления; побочные наводки информации на вспомогательных коммуникациях; подключение к внешним каналам связи.

1.3. **Классификация методов защиты информации**

Все методы защиты информации по характеру проводимых действий можно разделить: на законодательные (правовые); организационные; технические; комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации. К таким мерам относятся и издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты т.д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты.

Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т.е. комплексно.

2. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

2.1. Технические каналы утечки информации

Под техническими каналами понимаются каналы доступа к информации, возникающие вследствие либо естественных физических явлений, сопровождающих работу информационных

объектов, либо создаваемых искусственно нарушителем. Наиболее часто технические каналы используются для овладения компьютерной, акустической, телефонной и визуальной информацией.

2.1.1. Канал побочных электромагнитных излучений и наводок (ПЭМИН)

Работа средств вычислительной техники сопровождается электромагнитными излучениями и наводками на соединительные проводные линии, цепи «питания», «земля», возникающими вследствие электромагнитных воздействий в ближней зоне излучения, в которую могут попадать также провода вспомогательной и посторонней аппаратуры. В некоторых случаях информацию, обрабатываемую компьютерами, можно восстановить путем анализа электромагнитных излучений и наводок. В персональном компьютере (ПК) основными источниками электромагнитных излучений являются устройства ввода и вывода информации совместно с их адаптерами (монитор, принтер, клавиатура, печатающее устройство и т.д.), а также центральный процессор. Утечке информации в ПК способствует применение коротких видеоимпульсов прямоугольной формы и высокочастотных коммутирующих сигналов. Исследования показывают, что излучение видеосигнала монитора является достаточно мощным, широкополосным и охватывает диапазон метровых и дециметровых волн. Применение в ПК импульсных сигналов прямоугольной формы и высокочастотной коммутации приводит к тому, что в спектре излучений будут компоненты с частотами вплоть до СВЧ. Хотя энергетический спектр сигналов убывает с ростом частоты, но эффективность излучения при этом увеличивается, и уровень излучений может оставаться постоянным до частот нескольких гигагерц. Резонансы из-за паразитных связей могут вызывать усиление излучения сигналов на некоторых частотах спектра.

Основными цепями распространения опасного сигнала являются: информационные цепи видеосигнала; цепи обмена инфор-

мацией с жестким диском; цепи обмена информацией с ОЗУ; цепи ввода информации с клавиатуры; цепи вывода информации на принтер; цепи питания; вынос наведенных информационных сигналов через подключенные к системному блоку устройства, непосредственно не участвующие или не участвующие в данный момент времени в процессе передачи информации (мышь, клавиатура, информационный кабель принтера).

Наиболее опасными с точки зрения осуществления возможного несанкционированного съема обрабатываемой информации за счет ПЭМИН являются цепи, в которых сигналы имеют периодический характер. Например, информационные цепи видеосигнала, представляющего регулярный сигнал в последовательном коде. Менее опасные – сигналы в цепях обмена информацией с жестким и гибким дисками, цепях клавиатуры, т.к. они носят не регулярный характер. Еще менее опасны сигналы в цепи вывода информации на принтер, в цепи обмена информацией с ОЗУ, передаваемые в параллельном коде.

2.1.2. Канал утечки акустической информации

Наиболее простым способом перехвата речевой информации является подслушивание (прямой перехват). Разведываемые акустические сигналы могут непосредственно приниматься ухом человека, реагирующим на изменение звукового давления, возникающего при распространении звуковой волны в окружающем пространстве. Диапазон частот акустических колебаний, слышимых человеком, простирается от 16…25 Гц до 18…20 кГц в зависимости от индивидуальных особенностей слушателя. Человек воспринимает звук в очень широком диапазоне звуковых давлений. Одной из опорных величин этого диапазона является стандартный порог слышимости. Под ним условились понимать эффективное значение звукового давления, создаваемое гармоническим звуковым колебанием частоты $F = 1000$ Гц, едва слышимым человеком со средней чувствительностью слуха. Порогу слышимости соответствует звуковое давление $P = 2 \cdot 10^{-5}$ Па. В случаях, когда уровни

зву-кового давления, создаваемого звуковой волной, ниже порога слышимости, когда нет возможности непосредственно прослушивать речевые сообщения или когда требуется их зафиксировать (записать), используют микрофоны и радиомикрофоны. Микрофон является преобразователем акустических ко-лебаний в электрические сигналы, а радиопередатчик позволяет передавать эти сигналы на значительные расстояния.

Кроме того, если источник акустической информации находится внутри помещения, то акустическая информация может быть перехвачена с помощью электронного стетоскопа. Акустические колебания источника возбуждают в ограждающих конструкциях помещения (стенах, полу, потолке) микроскопические вибрации, эти вибрации улавливаются и преобразуются в электрические сигналы. Электронный стетоскоп представляет собой вибродатчик, усилитель, оконечное устройство. Вибродатчик – преобразователь вибрации в электрический сигнал. Он прикрепляется к стене, потолку, можно в соседней комнате. Его размеры – несколько сантиметров, вес – десятки–сотни граммов, коэффициент усиления – десятки тысяч. Может соединяться с наушниками, записывающей аппаратурой, с передатчиком.

2.1.3. Канал утечки телефонной информации

Канал утечки речевой информации, передаваемой по телефонным каналам связи, возникает за счет несанкционированного подключения злоумышленника к проводным линям связи или за счет перехвата сообщений, передаваемых по радиоканалу. Подключение к проводным линиям связи может быть контактным и бесконтактным. В качестве оконечных устройств используют специальные магнитофоны, включающиеся по командам (ключевое слово, появление сигнала, команда управления). Часто записывающее устройство может находиться на расстоянии. В этом случае используется телефонный ретранслятор, представляющий собой радиопередатчик, питающийся от телефонной сети. Телефонные ретрансляторы могут быть

закамуфлированы под различные элементы телефонной сети: розетка, конденсатор, фильтр, реле и т.д. Дальность действия несколько сот метров. Для перехвата сообщений, передаваемых по радиоканалу, используется сканирующий приемник, компьютер со специальным программным обеспечением.

2.1.4. Канал утечки визуальной информации

Визуальная информация может быть перехвачена с помощью оптической аппаратуры с большого расстояния (с искусственных спутников земли, с удаленных наблюдательных пунктов), а также с помощью миниатюрной аппаратуры в непосредственной близи от источника информации (фотоаппарат, видеокамера).

2.2. **Методы и средства защиты информации от утечки по техническим каналам**

2.2.1. Защита информации от утечки по каналу побочных электромагнитных излучений и наводок

Для защиты информации от утечки по каналу побочных электромагнитных излучений применяют проведение защитных мероприятий помещений в целом путем их экранирования, защиту излучающей аппаратуры, а если этих мер недостаточно, то используют электромагнитное зашумление.

Экранирование помещений можно выполнить используя различные материалы: листовую сталь, проводящую медную сетку, алюминиевую фольгу. Расчеты показывают, что медная сетка с ячейкой 2,5 мм даст приемлемую эффективность экранирования. Достаточно эффективный, и немаловажно дешевый, экран получается при использовании алюминиевой фольги. Экранировать нужно все помещение: полы, стены, потолки, двери. На практике это может выглядеть следующим образом: выбирается одна наиболее удобно расположенная комната, желательно не имеющая стен, смежных с неконтролируемыми помещениями, а также без вентиляционных отверстий.

На пол, например, под линолеум, укладывается фольга, сетка и т.д., стены под обоями или панелями покрываются фольгой. Потолки можно сделать алюминиевыми подвесными, а на окнах использовать алюминиевые жалюзи, специальные проводящие стекла или проводящие шторы. Важно обеспечить электрический контакт экранов пола, потолка, стен и т.д. по всему периметру помещения.

Для снижения уровня побочных излучений аппаратуры при ее изготовлении используют специальные конструкторские и технологические меры. Например, у персональных компьютеров корпуса системного блока выполняются в виде замкнутого электромагнитного экрана. Крышка системного блока в нижней части имеет специальные пазы, которые при установленной крышке играют роль предельных волноводов. Корпуса разъемов клавиатуры и мыши изнутри корпуса системного блока заключены в электромагнитные экраны. В цепи элементов индикации системного блока включены ферритовые фильтры. Корпус видеомонитора выполняется из металла или пластмассы с напылением токопроводящего материала, экран покрывается прозрачной токопроводящей пленкой. Соединительные кабели помещаются в экран. Необходимо качественное заземление всех экранов. Снижение мощности излучаемых сигналов может быть достигнуто и за счет разрушения периодичности видеосигналов путем введения случайности развертки видеомонитора. Практически без ухудшения воспроизведения изображения возможно снизить амплитуды гармоник излучения. Этот способ получил название способ снятия повторяемости.

Если конструкторскими и технологическими мерами не удается обеспечить требуемые характеристики, возможно применение генераторов шума. Генератор шума представляет собой источник электромагнитных колебаний, спектр которых перекрывает весь частотный диапазон возможных опасных излучений, а мощность достаточна для маскировки полезного сиг-

нала. Конструктивно он может выполняться в виде платы, вставляемой в слот компьютера, или в виде автономного блока. Серьезную проблему представляет защита проводных линий, выходящих за пределы помещений, в которых находится компьютерное оборудование (цепи электропитания, линии телефонной связи, цепи пожарной и охранной сигнализации). Экранирование таких линий позволяет защититься от наводок, распространяемых по этим линиям за пределами защищаемых помещений. Наиболее экономичным способом экранирования считается размещение информационных кабелей в экранирующий распределительный короб. Когда такого короба не имеется, то приходится экранировать отдельные линии связи. Для этого либо используют провода в экранирующей оболочке, либо помещать в такую оболочку (например, фольгу) существующие провода. Эффективно применять при этом скрутку двух (бифиляр) или трех проводов (трифиляр), уменьшающую излучение. При использовании трифиляра третий провод заземляется и служит экраном. Очень эффективен экранированный коаксиальный кабель. Необходимо проследить за тем, чтобы кабели разных линий связи были максимально разнесены для уменьшения взаимных наводок. После проведения работ по экранированию помещения необходимо выполнить работы по заземлению экранов. Обычно это делается путем параллельного подключения к существующему контуру заземления, предварительно проверив его сопротивление (оно должно быть не более 4 Ом).

2.2.2. Защита акустической информации

Для защиты акустической информации от прослушивания обычными микрофонами, находящимися за пределами помещения, необходимо при проектировании и строительстве помещения обеспечить требуемую звукоизоляцию, это достигается использованием двойных рам (стеклопакетов), дверей, звукоизоляционных материалов в стенах, потолках, полах.

Для защиты речевой информации от микрофонов и радиомикрофонов, установленных внутри помещений, применяются генераторы акустических помех. Существуют два типа генераторов акустических помех: генераторы шумовых помех и генераторы звукоподобных сигналов. Оба типа генераторов маскируя полезный сигнал, создают трудности при разговоре. С точки зрения снижения помех и санкционированным слушателям предпочтительнее генераторы звукоподобных сигналов, т.к. при меньшем уровне сигнала они обеспечивают требуемое маскирование полезного сигнала.

Однако наиболее эффективным методом защиты является периодический поиск и изъятие радиомикрофонов. Для этого используют: детекторы радиоизлучений, сканирующие приемники, поисковые комплексы, нелинейные локаторы.

Основой обнаружения работающих радиомикрофонов может быть любой приемник радиосигналов, позволяющий определить факт наличия в помещении источника излучения и его местоположение. Простейшим радиопеленгатором является детектор (индикатор) радиоизлучений. Детектор представляет собой широкополосный приемник радиосигнала со световой или звуковой индикацией. Недостатками такого устройства являются трудности в определении места излучения; помехи фоновых радиоизлучений промышленных источников.

Существует набор тактических приемов преодоления недостатков (отключение электросети, изменение ориентации, измерение фона). Лучшими характеристиками обладают более сложные детекторы с положительной обратной связью (ПОС) по звуковой частоте. Принцип работы детектора с ПОС по звуковой частоте заключается в следующем.

Оконечное устройство детектора изготавливается в виде динамика на длинном проводе. Сигнал звуковой частоты, излучаемый динамиком, принимается радиомикрофоном, преобразуется в радиосигнал, принимается детектором, усиливается и вновь излучается динамиком. Таким образом возникает

ПОС в контуре. Контур возбуждается при наличии работающего радиомикрофона. Перемещая динамик в пространстве легко определить направление на источник радиоизлучения.

Более эффективным средством является сканирующий по частоте приемник. Поскольку рабочая частота радиомикрофона неизвестна и может находиться в диапазоне от десятков МГц до 1 ГГц, то для ее обнаружения необходим приемник с перестраиваемой полосой приема. Такие приемники получили название сканирующих. Существуют малогабаритные сканирующие приемники с телескопическими антеннами, с автоматической и ручной перестройкой частоты в широком диапазоне, с запоминанием частот и другим набором сервисных функций. На базе таких приемников изготавливаются поисковые комплексы, содержащие портативный компьютер, генератор звукового теста, коррелятор. Такие комплексы в автоматическом режиме за несколько минут определяют частоты и уровни излучений, определяют направление и расстояние до скрытых средств.

Описанные ранее средства позволяют обнаружить радиомикрофоны в работающем состоянии (в активном). Если радиомикрофон управляется дистанционно или по программе и на момент поиска выключен (пассивен), то его можно обнаружить с помощью устройства, получившего название нелинейный локатор (НЛ). Принцип действия НЛ основан на преобразовании спектра гармонического сигнала локатора нелинейным элементом радиомикрофона (диодом, транзистором). Что приводит к появлению в спектре отраженного сигнала, гармоники с удвоенной частотой.

Для защиты акустической информации от утечки по вибрационным каналам используются системы виброакустического зашумления, состоящие из генераторов электрических колебаний и преобразователей.

Отличие генераторов вибропомех заключается в мощности колебаний и преобразователей электрических сигналов в

вибросигналы. Генераторы выполняются аналогично генераторам акустических помех, а в качестве преобразователей используются устройства, преобразующие электрические сигналы в энергию упругих колебаний среды.

При возбуждении конструкций, имеющих высокое акустическое сопротивление (кирпичные стены, бетонные перекрытия), согласование в широком частотном диапазоне проще осуществляется с устройствами, имеющими высокий механический импеданс подвижной системы. Такими устройствами являются пьезокерамические преобразователи. Электромагнитные преобразователи имеют худшие характеристики.

Наводимые в конструкциях вибрационные шумы должны маскировать вибрации от полезного речевого сигнала, создавая при этом минимум помех для людей, работающих в помещении.

Помехи создаются за счет акустического сигнала вибродатчика и за счет вибрационных колебаний конструкций. Основная доля при этом падает на акустический паразитный сигнал. Наряду с выбором типа вибратора, необходимо вибропреобразователи располагать не на поверхности конструкции, а в специально изготовленной нише, тщательно заделанной после установки преобразователя.

2.2.3. Защита телефонной информации

Для защиты информации, открыто передаваемой по проводным линиям связи, необходимо иметь технические средства, обнаруживающие факт прослушивания линии. Для этого существует ряд приборов от простейших индикаторов подключения до очень сложных анализаторов характеристик линий. Работа всех этих приборов основана на фиксации изменений параметров телефонной сети при подключении к ним устройств прослушивания. Простейшие приборы реагируют на изменение напряжения в линии или сопротивления, более сложные фиксируют частотные и импульсную характеристики.

При этом, однако, надо помнить, что необходимо иметь значения характеристик до подключения устройств прослушивания, сеть должна иметь стабильные характеристики, подключение устройств должно изменять параметры линии.

Наиболее эффективным способом защиты речевой информации в каналах связи являются методы, основанные на преобразовании речевой информации по определенному алгоритму, делающие невозможным понимание речи.

Получили распространение два способа скремблирования речи: аналоговое скремблирование (аналоговое преобразование) и цифровое криптопреобразование (цифровое скремблирование).

Суть аналогового скремблирования заключается в аналоговом преобразовании речевого сигнала, после которого он становится неразборчивым. Для его понимания необходимо провести обратное преобразование. Такое преобразование осуществляется чаще всего за счет инвертирования частотного спектра речевого сигнала в соответствии с условленным порядком.

Самым надежным способом защиты является криптографическое преобразование речевого сигнала. Речевой аналоговый сигнал преобразуется в цифровой, затем в специальном вычислителе производится специальное математическое преобразование (шифрование) с использованием секретного ключа, зашифрованная информация передается в канал связи. Второй абонент с помощью своего секретного ключа (такого же, что и у первого) расшифровывает информацию и преобразует ее в аналоговый сигнал.

Аппарат, содержащий обе линейки, позволяет осуществлять дуплексную связь. Наличие компрессора и декомпрессора обусловлено низкой скоростью передачи информации по реальным телефонным каналам: 2400–9600 бит/с. На выходе же АЦП при стандартной частоте дискретизации 8 кГц и 8-битовом представлении скорость составляет 64 кбит/с. Компрессор реализует один из алгоритмов сжатия LPC, GSM, CELP. Важ-

ными проблемами в такой связи являются синхронизация работы двух аппаратов и распределение ключевой информации.

3. ОСНОВНЫЕ ФУНКЦИИ СИСТЕМЫ ЗАЩИТЫ ОТ НСД В КОМПЬЮТЕРНЫХ СИСТЕМАХ

В общем случае для типовой компьютерной системы (КС) система защиты от НСД должна обеспечивать:

1. Идентификацию и аутентификацию пользователя при начале работы в КС.
2. Управление доступом к ресурсам и процессам КС.
3. Контроль целостности объектов КС.
4. Мониторинг процессов и событий КС.
5. Управление безопасностью КС.

В КС защита от НСД осуществляется программными, аппаратными или аппаратно-программными средствами.

3.1. Аутентификация пользователя

Аутентификация означает установление подлинности. Обеспечивает работу в сети только санкционированных пользователей. Чаще всего проводится при входе в сеть, но может проводиться и во время работы. Обычно проводится после процесса идентификации, во время которого пользователь сообщает свой идентификатор (называет себя). В процедуре аутентификации участвуют две стороны: пользователь доказывает свою подлинность, а сеть проверяет это доказательство и принимает решение. В качестве доказательства используют: знание секрета (пароля); владения уникальным предметом (физическим ключом); предъявления биометрической характеристики (отпечатка пальца, рисунка радужной оболочки глаза, голоса).

Наиболее распространенное средство аутентификации – пароль. Используется как при входе в систему, так и в процессе работы. Пароль может вводиться с клавиатуры, или с различных носителей цифровой информации или комбинировано. При использовании паролей необходимо соблюдать необхо-

димые требования: по правилам генерации (длина, случайность символов), хранения (хранить в защищенном месте), использования (в зашифрованном виде), отзыва.

В качестве субъектов аутентификации могут выступать не только пользователи, но и различные устройства или процессы. Причем процесс аутентификации может носить обоюдный характер. Обе стороны должны доказать свою подлинность. Например, пользователь, обращающийся к корпоративному серверу, должен убедиться, что имеет дело с сервером своего предприятия. В этом случае процедура называется взаимной аутентификацией.

3.2. Управление доступом к ресурсам и процессам КС

Допущенным в КС субъектам должны предоставляться различные права по доступу к информационному ресурсу и по возможным действиям с ним. Например, доступ к каталогам, файлам, принтерам, доступ к системным функциям: доступ к серверу, установка системного времени, создание резервных копий данных, выключение сервера и т.д. Эти права могут задаваться по-разному. В основном их можно разбить на два класса: произвольный доступ и мандатный доступ.

Произвольный доступ реализуется в операционной системе общего назначения. Задаются определенные операции над определенным ресурсом одному пользователю или группе пользователей, явно указанным своими идентификаторами. При этом пользователь может передавать свои полномочия некоторому процессу, если этим же процессом управляет другой пользователь, то в итоге права одного пользователя становятся доступными другому. Основой произвольного доступа является матрица прав доступа, строки которой соответствуют субъектам (пользователи, процессы и т.д.), а столбцы – объектам (файлы, каталоги и т.д.). В ячейках матрицы содержатся права доступа субъектов к объектам. Пример матрицы прав доступа приведен в табл. 3.1, где R – права доступа пользователя по чтению, W – права доступа пользователя по записи;

C – управление доступом для других пользователей.

Таблица 3.1

Пользователи/Файлы	F1	F2	F3	F4	F5	
Петров	R	W	W		RW	
Иванов	RW		R	R		
Сидоров		RW			R	
Федоров	C	C	C	C	C	

В зависимости от способа представления матрицы прав доступа в ОС различают несколько способов реализации. Наиболее распространенными являются списки прав доступа, биты доступа, парольная защита.

Списки прав доступа. С каждым объектом ассоциируется список пользователей с указанием их прав доступа к объекту. При принятии решения о доступе соответствующий объект проверяется на наличие прав, ассоциированных с идентификатором пользователя, запрашивающего доступ.

Биты доступа. Вместо списка пользователей с объектом связываются биты доступа. Например, в ОС UNIX организованы три категории пользователей. Каждой группе разрешены определенные действия. Каждый пользователь получает определенный бит (номер), который определяет, к какой группе он относится и какими полномочиями наделен.

При реализации мандатного доступа вся информация делится по уровням конфиденциальности, а все пользователи – на группы по уровням допуска к информации различного уровня конфиденциальности. При этом пользователи не имеют возможности изменять уровень доступности информации. Нормативное управление доступом основано на модели Белла-ЛаПадула, которая описывает правила документооборота, принятые в правительственных учреждениях США. Основным наблюдением, сделанным Беллом и ЛаПадулой, является то, что в официальном документообороте всем субъектам и объектам присваивается уровень (метка) безопасности. Для

предотвращения утечки информации к неуполномоченным субъектам с низкими уровнями безопасности не позволяется читать информацию из объектов с высокими уровнями безопас-ности; субъектам не позволяется размещать информацию или записывать ее в объекты с более низким уровнем безопасности. Мандатный доступ является более строгим, исключает волюнтаризм со стороны пользователей. Реализуется в ОС специального назначения.

3.3. Контроль целостности

Подсистема контроля целостности должна контролировать как целостность информационных ресурсов сети, так и целостность системы защиты. Злоумышленник может установить вредоносные программы, типа «троянский конь», поправить системные файлы, предоставить себе несанкционированные полномочия, отключить систему защиты, т.е. нарушить целостность установленного программного обеспечения. Подсистема контроля целостности должна работать пассивно, не мешая работе контролируемой системы. В ходе контроля вычисляется некоторая относительно короткая величина (слепок), зависящая от контролируемых данных, причем любое их изменение должно приводить к существенному изменению этой величины. В простейшем случае в качестве такой величины может использоваться контрольная сумма, более стойкий результат дает использование криптографических методов. Подсистема контроля целостности работает по замкнутому циклу, обрабатывая файлы, системные объекты и атрибуты системных объектов с целью вычисления слепка, затем сравнивает его с предыдущим слепком. При обнаружении расхождения сигнализирует администратору безопасности.

3.4. Аудит

Подсистема аудита предназначена для фиксации событий, связанных с доступом к защищаемым ресурсам. Для этого средствами ОС и (или) прикладных программ ведутся журна-

лы регистрации событий безопасности, в которые записывается информация о времени, источнике, категории события, коде события, субъект, компьютер и т.д. Многие компоненты КС имеют подобные журналы. Например, коммуникационное оборудование (маршрутизаторы Cisco), межсетевые экраны (Check Point) и сетевые ОС, начиная с W-NT. Данные журналы ведутся и системами обнаружения атак, входящими в состав системы защиты информации.

3.5. **Управление безопасностью в КС**

Система защиты информации КС должна быть управляемой. Управляемость необходима для обеспечения ее текущего функционирования (смена паролей, криптографических ключей, изменения списков пользователей, изменения каталогов защищаемых файлов и т.д.) и адаптации к изменившейся политике безопасности сети (изменение правил доступа, изменение длины паролей или ключей, замена используемых криптопротоколов и алгоритмов). При этом функции оперативного управления являются обязательными, т.к. без них систему защиты не возможно эксплуатировать. Функции адаптации к политике безопасности желательны и должны закладываться на этапе проектирования.

3.6. **Программные средства защиты от НСД**

3.6.1. Защита средствами операционной системы

Для защиты информации от несанкционированного доступа одиночных ПК (не входящих в локальные или глобальные сети) используются программные средства операционных систем или прикладные программы, а также специальные программно-аппаратные средства.

Исторически сложилось так, что до недавнего времени при разработке ОС всеобщего назначения (Windows, Unix) вопросам защиты от НСД уделялось мало внимания. И это вполне объяснимо. Они были рассчитаны на применение пользовате-

лями, не обрабатывающими конфиденциальную информацию. В современных версиях ОС эти недостатки по заявлению разработчиков устранены, т.е. большинство описанных выше функций защиты могут быть реализованы. Однако остается открытым вопрос о степени доверия к надежности встроенных функций защиты, поскольку программные коды, например, Windows, не известны.

3.6.2. Защита средствами прикладных программ

Существует ряд программных продуктов, работающих под управлением незащищенных ОС, выполняющих защиту от НСД в КС. Эти программы в основном выполняют функции, сформулированные ранее, и отличаются друг от друга непринципиально. Поэтому коротко рассмотрим наиболее разрекламированное средство – Sekret Net.

Основные выполняемые функции: идентификация пользователей до загрузки ОС (возможно с использованием аппаратых средств); регламентация доступа к физическим и логическим устройствам (дискам, портам, файлам, папкам); контроль целостности ПО защиты; организация и ведение журнала безопасности (регистрация всех событий, относящихся к безопасности).

Средства защиты от НСД, реализованные в виде программ, не могут обеспечить защиту от квалифицированного злоумышленника. Существует достаточно атак, в результате которых злоумышленник перехватывает пароли, списки, присваивает себе полномочия администратора, выдает себя за санкционированного пользователя, модифицирует ОС в части управления и контроля доступа. Для надежной защиты информационных ресурсов ПК необходимо, чтобы критичные для безопасности операции осуществлялись в изолированной ОС, недоступной злоумышленнику. Такая среда создается путем использования аппаратно-программных средств (АПС) защиты от НСД.

3.7. **Аппаратно-программные средства защиты от НСД**

АПС защиты обеспечивает выполнение всех функций по защите в своей, изолированной операционной среде, недоступной злоумышленнику. По своей архитектуре наиболее эффективные устройства представляют собой автономный компьютер с собственным процессором, памятью, BIOS, операционной системой. АПС защиты управляет включением защи-щаемого компьютера, процессом авторизации (идентификации и аутентификации), процессом допуска пользователей и процессов к информационным ресурсам ПК и т.д. Современные АПС защиты реализуют криптографические алгоритмы шифрования и протоколы аутентификации и контроля целостности. Наиболее известным средством защиты является аппаратно-программный комплекс «Аккорд», который имеет большое количество модификаций. Это наиболее надежное и дорогостоящее изделие, разработано в России ОКБ «САПР», на белорусском рынке представляется фирмой «Марфи».

«Аккорд» включает три подсистемы: управления доступом, регистрации и учета, обеспечения целостности. Подсистема управления доступом осуществляет идентификацию, проверку подлинности и контроль допуска субъектов: в систему; к внешним устройствам; к файлам, папкам, каталогам. Подсистема регистрации и учета осуществляет указанные функции в отношении: входа (выхода) субъектов доступа в (из) системы; запуска (завершения) программ и процессов (заданий, задач); доступа программ субъектов к защищаемым файлам, включая их создание и удаление; доступа программ субъектов доступа к внешним устройствам ПЭВМ; изменений полномочий субъектов доступа; создаваемых защищаемых объектов доступа. Подсистема обеспечения целостности отвечает за целостность программных средств и обрабатываемой информации.

4. АТАКИ В КОМПЬЮТЕРНЫХ СЕТЯХ

4.1. Общие сведения об атаках

Атакой на КС называется действие или последовательность действий нарушителя, которые приводят к реализации угроз, путем использования уязвимостей этой КС. Уязвимости делят на уязвимости: за счет наличия недостатков в аппаратно-программном продукте по вине разработчика; добавленные администратором при настройке КС; внесенные пользователем КС (короткий пароль, игнорирование политики безопасности). Атака состоит из следующих этапов: сбор информации, реализация атаки, завершение атаки.

Сбор информации. Изучение окружения атакуемой системы (определяется провайдер жертвы, адреса доверенных узлов, трафик, режим работы организации, телефонные номера и т.д.); идентификация топологии сети (определяется количество компьютеров, способ их соединения, организация выхода в глобальную сеть); идентификация узлов (проводится разведка IP-адреса узла, его доступности); идентификация сервисов и портов (определяется наличие установленных сервисов типа Telnet, FTP, Web-сервера и наличие доступа к ним, открытость портов); идентификации ОС (определяется тип ОС); определение роли узла (маршрутизатор, МСЭ, сервер); определение уязвимостей узла (на основе собранной информации определяется наличие уязвимостей).

Реализация атаки. Реализация атаки заключается в проникновении в систему и установления контроля над ней. Контроль может быть непосредственный, например, через Telnet, или с помощью установленной программы.

Завершение атаки. На этом этапе злоумышленник убирает следы своей атаки с целью невозможности его идентификации. Для этого используют: подмену адреса источника атаки путем создания пакетов с фальшивыми адресами источника; проводят очистку журнала регистрации событий. Либо атаку проводят с уже взломанных промежуточных серверов или proxy-серверов. Маскируют внедренные программы путем присоединения их к стандартным либо присвоением им названий,

похожих на названия стандартных программ. Изменяют контрольные суммы файлов и папок.

Большинство известных атак можно разбить на следующие группы: удаленное проникновение (атака, в результате которой реализуется удаленное управление компьютером через сеть); локальное проникновение (внедряется программа, которая управляет компьютером (Get Admin); удаленный отказ в обслуживании (перегрузка потоком сообщений узла, который не в состоянии их переработать); локальный отказ в обслуживании (узел занят обработкой некоторой задачи и все остальные игнорирует (зацикливание)); сетевое сканирование (сеть подвергается запросам программы, анализирующей топологию, доступные сервисы и уязвимости (nmap, Satan)); взлом паролей (запуск программы, подбирающие пароли пользователей (Crack)); анализ протоколов (с помощью анализатора протоколов просматривается трафик, извлекаются идентификаторы, пароли).

4.2. **Технология обнаружения атак**

Технология обнаружения атак основывается: на признаках, описывающих нарушения политики безопасности (что); источниках информации, в которых ищутся признаки нарушения политики безопасности (где); методах анализа информации, получаемой из соответствующих источников (как).

Признаками атак являются: повтор определенных событий; неправильные или несоответствующие текущей ситуации команды; признаки работы средств анализа уязвимостей; несоответствующие параметры сетевого трафика; непредвиденные атрибуты; необъяснимые проблемы.

Повтор определенных событий. Злоумышленник, пытаясь осуществить несанкционированное проникновение, вынужден совершать определенные действия несколько раз, т.к. с одного раза он не достигает своей цели. Например, подбор пароля

при аутентификации; сканирование портов с целью обнаружения открытых.

Неправильные или несоответствующие текущей ситуации команды. Обнаружение неправильных запросов или ответов, ожидаемых от автоматизированных процессов и программ. Например, в процессе аутентификации почтовых клиентов системы вместо традиционных процедур вдруг обнаружены иные команды, оказалось, что свидетельствует о попытке злоумышленника получить доступ к файлу паролей почтового шлюза.

Признаки работы средств анализа уязвимостей. Имеется ряд средств автоматизированного анализа уязвимостей сети: nmap, Satan, Internet Scanner, которые в определенном порядке обращаются к различным портам с очень небольшим интервалом времени. Такие обращения являются признаками атак.

Несоответствующие параметры сетевого трафика. Например, некорректные параметры входного и выходного трафика (в ЛВС приходят из внешней сети пакеты, имеющие адреса источника, соответствующие диапазону адресов внутрен-ней сети. Из ЛВС выходят пакеты с адресом источника, находящегося во внешней сети. Адрес источника запрещен, адрес источника и получателя совпадают); некорректные значения параметров различных полей сетевых пакетов (взаимоисключающие флаги); аномалии сетевого трафика (параметры сетевого трафика отличатся от традиционных: коэффициент загрузки, размер пакета, среднее число фрагментированных пакетов, использование нетипичного протокола); непредвиден-ные атрибуты (запросы пользователей, их действия характеризуются неким типовым профилем, отклонения от него – это признак атаки, например, работа в нерабочее время в выходные, в отпуске; нетипичное местоположения пользователя, нетипичные запросы сервисов и услуг).

Необъяснимые проблемы. Проблемы с программным и аппаратным обеспечением, с системными ресурсами, с производительностью.

Источниками информации об атаках являются журналы регистрации событий (ЖРС) или сетевой трафик.

Журналы регистрации событий ведутся рабочими станциями, серверами, межсетевыми экранами (МСЭ), системами обнаружения атак. Типовая запись в таком журнале ведется по следующей форме:

Таблица 4.1

Дата	Время	Источник (программа, которая регистрирует событие)	Категория (название события: входное, выходное, изменение политики доступа к объекту)	Код события	Пользователь (субъект, с которым связано событие: Ad, User, system)	Компьютер (место, на котором произошло событие)

Изучение сетевого трафика позволяет проводить анализ содержания пакетов или последовательностей пакетов.

Примеры обнаружения атак по ЖРС и сетевому трафику.

Обнаружение сканирования портов. Отслеживая записи в ЖРС, замечаем: идет поток запросов из одного адреса через короткие промежутки времени (5–10 запросов в секунду) к портам, номера которых перебираются последовательно (это признак простейшего сканирования). В более сложном сканировании признаки маскируют: увеличивают временные интервалы между запросами и номера портов изменяют по случайному закону.

Обнаружение подмены адреса источника сообщения. Каждому пакету присваивается уникальный идентификатор, и если пакеты исходят из одного источника, то очередной пакет получает номер на единицу больше. Если приходят пакеты из разных источников, а их идентификаторы последовательно нарастают, то это свидетельствует о фальшивом адресе источника.

Аналогично можно использовать поле времени жизни. Пакеты, отправленные из различных источников, при приеме в узле имеют одинаковые значения (примерно) оставшегося вре-

мени жизни, хотя оно должно быть разным. Следовательно, они отправлены из одного источника.

Обнаружение идентификации типа ОС. Специальной программой формируются пакеты уровня TCP в заголовках, в которых используются комбинации флагов, не соответствующие стандартам. По реакции узла на эти пакеты определяется тип ОС. Данная комбинация флагов и является признаком идентификации типа ОС.

Обнаружение троянских программ. При передаче троянской программы идет обращение к портам с вполне определенными номерами. Поэтому если получены пакеты с этими номерами портов, то это свидетельствует о возможном наличии в передаваемых данных троянской программы. Кроме того, троянские программы могут быть распознаны по наличию ключевых слов в поле данных.

Обнаружение атак «Отказ в обслуживании». Обнаружение производится по превышению числа запросов в единицу времени; по совпадению адресов отправителя и получателя; по номерам портов, указанных в пакетах (пересылка пакета с 19 на 17 или 13 на 37 зацикливает атакуемый компьютер).

Для координации деятельности мирового сообщества по защите в сети Интернет создан Координационный центр CERT/CC. Он собирает всю информацию об атаках и дает рекомендации пользователям. Адрес этого центра в Интернете: WWW.cept.org.

4.3. **Методы анализа информации при обнаружении атак**

4.3.1. Способы обнаружения атак

Способы обнаружения атак можно разделить: на обнаружение признаков аномального поведения защищаемой системы; обнаружение признаков злоумышленных действий субъектов.

Обнаружение признаков аномального поведения защищаемой системы.

Составляется совокупность признаков нормального (без вмешательства злоумышленника) поведения системы – эталон признаков нормального поведения. Реальное поведение непрерывно или дискретно сравнивается с эталонным, если они не совпадают, то, возможно, это следствие злоумышленных действий. Таким образом, отклонение реального поведения от эталонного – признак атаки. Структурная схема системы для обнаружения признаков аномального поведения защищаемой системы изображена на рис. 4.1.

При данном способе обнаруживаются любые атаки (в том числе и неизвестные), приводящие к отклонению поведения от нормального. При этом необходимо иметь эталон признаков нормального поведения. Это возможно, если процесс функционирования системы является стабильным (каждый день решаются одни и те же задачи, например, в супермаркете, банке) и описывается некой устойчивой совокупностью признаков. Все изменения в поведении таких систем – плановые, прогнозируемые, могут быть учтены путем корректировки эталона (подключение филиала банка). Режим работы систем жестко регламентируем. Для таких систем целесообразно использовать описанный способ. Например, сотрудники организации используют электронную почту только в рабочее время: $t \in$ [9-00, 18-00] – эталон; если $t_Р$ = 23–15, то имеет место отклонение от эталона.

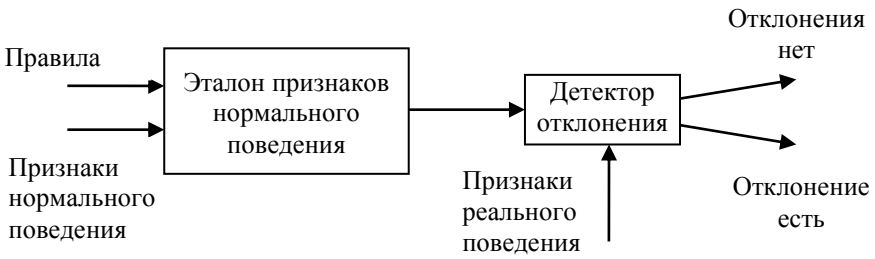

Рис. 4.1. Обнаружение признаков аномального поведения защищаемой системы

Обнаружение признаков злоумышленных действий субъектов.

Создается база шаблонов признаков злоумышленных действий. Реальные действия субъекта сравниваются с шаблонами признаков злоумышленных действий. При обнаружении совпадений делается вывод о наличии атаки. Таким образом, совпадение действия субъекта с одним из шаблонов – признак атаки (рис. 4.2).

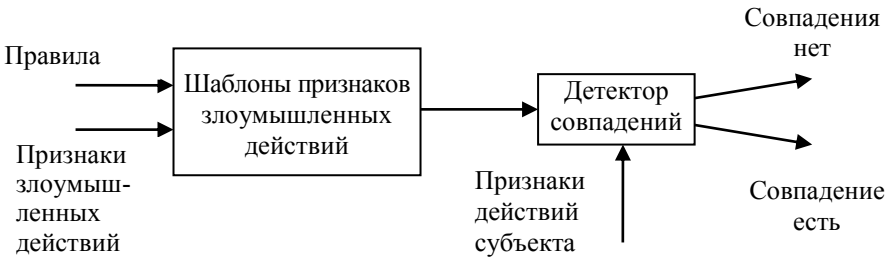

Рис. 4.2. Обнаружение признаков злоумышленных действий субъектов

Данный способ должен применяться для систем, решающих разнообразные задачи, взаимодействуя с различными узлами, поведение которых является нестабильным и для которых невозможно составить эталон нормального поведения. Он требует наличия базы шаблонов признаков злоумышленных действий и не пригоден для обнаружения неизвестных атак.

4.3.2. Методы анализа информации при обнаружении атак

Составление эталона признаков нормального поведения системы – сложная задача, т.к. в компьютерной системе протекает большое количество процессов, она взаимодействует с различными пользователями, действия которых трудно формализуются. Аналогичные трудности встречаются и при реализации второго способа обнаружения атак.

Принята следующая классификация признаков (параметров): числовые параметры (размер сообщения, длительность

временного интервала); категориальные параметры (имя файла, команда, ключевое слово); параметры активности (количество соединений в единицу времени).

Чем больше признаков используется, тем больше шансов обнаружить атаку, хотя анализ слишком большого количества параметров требует больших вычислительных ресурсов, при этом производительность контролируемого узла, объем операционной и дисковой памяти снижаются. Большинство числовых параметров поведения системы носят случайный характер и имеют разброс значений от одного наблюдения к другому. Поэтому при составлении эталона необходимо оперировать с вероятностными характеристиками этих случайных величин (МОЖ, дисперсия, квантиль, закон распределения). Следовательно, при таком подходе задача сравнения эталона с реальным поведением может рассматриваться как задача статистической классификации. Например, как задача проверки статистической гипотезы или задача распознавания образов.

При использовании аппарата проверки статистической гипотезы выдвигается гипотеза (одномерная), что среднее значение эталонного признака $\overline{\overline{X}}_{Эj}$, равно среднему значению реального признака $\overline{\overline{X}}_{Pj}$, т.е. H_0: $\overline{\overline{X}}_{Эj} = \overline{\overline{X}}_{Pj}$ при альтернативе H_1: $\overline{\overline{X}}_{Эj} \neq \overline{\overline{X}}_{Pj}$. Наблюдая реальные значения X_{PJ} и имея решающее правило, гипотеза принимается или отвергается с заданной вероятностью.

Ограничения. Необходимо знать законы распределения величин X_{PJ}, $X_{ЭJ}$. Особенно сложно определить $f(X_{ЭJ}/H_1)$. Для этого необходимо имитировать атаку на систему и определить условную плотность вероятности (т.е. обучить систему обнаружения).

Описанную процедуру следует применять для всех признаков поведения. И если хотя бы по одному из них результат от-

рицателен, то принимается решение о наличии атаки. При этом существуют ошибки: ложная тревога и пропуск атаки. Вероятность ошибок тем больше, чем реальные вероятностные характеристики признаков отличаются от гипотетических.

Перспективным способом анализа информации при обнаружении атак можно считать теорию нейронных сетей.

К настоящему времени информационное сообщество накопило большое количество информации о злоумышленных действиях. Известно, что негативные действия сопровождаются определенными признаками. Поскольку в сетях все действия осуществляются посредством генерации битовых потоков (сигнатур), то по многим повторяющимся атакам имеется банк сигнатур (строка символов, определенные команды, последовательность команд). В задачах обнаружения признаков злоумышленных действий эти сигнатуры играют роль шаблонов. Сетевой трафик анализируется на наличие в нем сигнатур атак. Эта задача детерминированная. Детектор обнаружения ищет совпадение сигнатур трафика с сигнатурами атак. Например, ищет некорректные значения полей в заголовке пакетов. При этом обеспечивается простота реализации, высокая скорость функционирования, отсутствие ложных тревог, одна-ко при этом невозможно обнаружить неизвестные атаки (шаблоны отсутствуют), небольшая модификация атаки делает ее не обнаруживаемой.

5. МЕЖСЕТЕВЫЕ ЭКРАНЫ

5.1. Общие сведения

При подключении любой закрытой компьютерной сети к открытым сетям, например, к сети Internet, высокую актуальность приобретают угрозы несанкционированного вторжения в закрытую сеть из открытой, а также угрозы несанкционированного доступа из закрытой сети к ресурсам открытой. По-

добный вид угроз характерен также для случая, когда объединяются отдельные сети, ориентированные на обработку конфиденциальной информации совершенно разного уровня секретности. При ограничении доступа этих сетей друг к другу возникают угрозы нарушения установленных ограничений.

Неправомерное вторжение во внутреннюю сеть из внешней может выполняться как с целью несанкционированного использования ресурсов внутренней сети, например, хищения информации, так и с целью нарушения ее работоспособности.

Угрозы несанкционированного доступа во внешнюю сеть из внутренней сети актуальны в случае ограничения разрешенного доступа во внешнюю сеть правилами, установленными в организации. Такое ограничение, что особенно характерно для взаимодействия с открытыми сетями, может понадобиться в следующих случаях: для предотвращения утечки конфиденциальных данных; при запрете доступа, например, в учебных заведениях; к информации нецензурной и нежелательной направленности; в случае запрета служебного доступа к развлекательным компьютерным ресурсам в рабочее время.

Бороться с рассмотренными угрозами безопасности межсетевого взаимодействия средствами универсальных операционных систем не представляется возможным. Универсальная операционная система – это слишком большой и сложный комплекс программ, который, с одной стороны, может содержать внутренние ошибки и недоработки, а с другой – не всегда обеспечивает защиту от ошибок администраторов и пользователей.

Поэтому проблема защиты от несанкционированных действий при взаимодействии с внешними сетями успешно может быть решена только с помощью специализированных программно-аппаратных комплексов, обеспечивающих целостную защиту компьютерной сети от враждебной внешней среды. Такие комплексы называют межсетевыми экранами, брандмауэрами или системами Fire Wall. Межсетевой экран устанавливается на стыке между внутренней и внешней сетями и

функции противодействия несанкционированному межсетевому доступу берет на себя.

5.2. Функции межсетевого экранирования

Для противодействия несанкционированному межсетевому доступу брандмауэр должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис. 5.1). При этом все взаимодействия между этими сетями должны осуществляться только через межсетевой экран. Организационно экран входит в состав защищаемой сети.

Межсетевой экран должен учитывать протоколы информационного обмена, положенные в основу функционирования внутренней и внешней сетей. Если эти протоколы отличаются, то брандмауэр должен поддерживать многопротокольный режим работы, обеспечивая протокольное преобразование отличающихся по реализации уровней модели OSI для объединяемых сетей. Чаще всего возникает необходимость в совместной поддержке стеков протоколов SPX/IPX и TCP/IP.

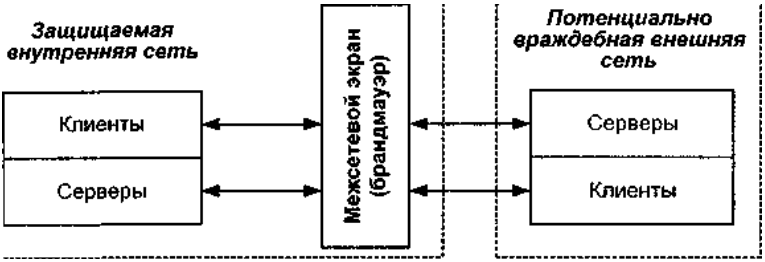

Рис. 5.1. Схема подключения межсетевого экрана

Брандмауэр не является симметричным. Для него отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю сеть и наоборот. В общем случае работа межсетевого экрана основана на динамическом выполнении двух

групп функций: фильтрации проходящих через него информационных потоков; посредничества при реализации межсетевых взаимодействий.

В зависимости от типа экрана эти функции могут выполняться с различной полнотой. Простые межсетевые экраны ориентированы на выполнение только одной из данных функций. Комплексные экраны обеспечивают совместное выполнение указанных функций защиты. Собственная защищенность брандмауэра достигается с помощью тех же средств, что и защищенность универсальных систем.

Чтобы эффективно обеспечивать безопасность сети, комплексный брандмауэр обязан управлять всем потоком, проходящим через него, и отслеживать свое состояние. Для принятия управляющих решений по используемым сервисам межсетевой экран должен получать, запоминать, выбирать и обрабатывать информацию, полученную от всех коммуникационных уровней и от других приложений. Недостаточно просто проверять пакеты по отдельности.

Устройство, подобное межсетевому экрану, может использоваться и для защиты отдельного компьютера. В этом случае экран, уже не являющийся межсетевым, устанавливается на защищаемый компьютер. Такой экран, называемый брандмауэром компьютера или системой сетевого экранирования, контролирует весь исходящий и входящий трафик независимо от всех прочих системных защитных средств. При экранировании отдельного компьютера поддерживается доступность сетевых сервисов, но уменьшается или вообще ликвидируется нагрузка, индуцированная внешней активностью. В результате снижается уязвимость внутренних сервисов защищаемого таким образом компьютера, поскольку первоначально сторонний злоумышленник должен преодолеть экран, где защитные средства сконфигурированы особенно тщательно и жестко.

5.2.1. Фильтрация трафика

Фильтрация информационных потоков состоит в их выборочном пропускании через экран, возможно, с выполнением некоторых преобразований и извещением отправителя о том, что его данным в пропуске отказано. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов принятой политики безопасности. Поэтому межсетевой экран удобно представлять как последовательность фильтров, обрабатывающих информационный поток. Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путем выполнения следующих стадий: анализа информации по заданным в интерпретируемых правилах критериям, например, по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена; принятия на основе интерпретируемых правил одного из следующих решений: не пропустить данные; обработать данные от имени получателя и возвратить результат отправителю.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например, преобразование данных, регистрация событий и др. Соответственно правила фильтрации определяют перечень условий, по которым с использованием указанных критериев анализа осуществляется: разрешение или запрещение дальнейшей передачи данных; выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры: служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные; непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов; внешние характеристики потока информации, например, временные, частотные характеристики, объем данных и т.д.

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. Чем выше уровень модели OSI, на котором брандмауэр фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

5.2.2. Выполнение функций посредничества

Функции посредничества межсетевой экран выполняет с помощью специальных программ, называемых экранирующими агентами или просто программами-посредниками. Данные программы являются резидентными и запрещают непосредственную передачу пакетов сообщений между внешней и внутренней сетью.

При необходимости доступа из внутренней сети во внешнюю сеть или наоборот вначале должно быть установлено логическое соединение с программой-посредником, функционирующей на компьютере экрана. Программа-посредник проверяет допустимость запрошенного межсетевого взаимодействия и при его разрешении сама устанавливает отдельное соединение с требуемым компьютером. Далее обмен информацией между компьютерами внутренней и внешней сети осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений, а также осуществлять другие защитные функции.

Функции фильтрации межсетевой экран может выполнять без применения программ-посредников, обеспечивая прозрачное взаимодействие между внутренней и внешней сетью. Вместе с тем программные посредники могут и не осуществлять фильтрацию потока сообщений.

В общем случае экранирующие агенты, блокируя прозрачную передачу потока сообщений, могут выполнять следующие функции: идентификацию и аутентификацию пользователей; проверку подлинности передаваемых данных; разграничение доступа к ресурсам внутренней сети; разграничение доступа к ресурсам внешней сети; фильтрацию и преобразование потока

сообщений, например, динамический поиск вирусов и прозрачное шифрование информации; трансляцию внутренних сетевых адресов для исходящих пакетов сообщений; регистрацию событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов; кэширование данных, запрашиваемых из внешней сети.

Идентификация и аутентификация пользователей необходима не только при их доступе из внешней сети во внутреннюю, но и наоборот. Распространенным способом аутентификации является использование одноразовых паролей. Пароль не должен передаваться в открытом виде через общедоступные коммуникации. Это предотвратит получение несанкционированного доступа путем перехвата сетевых пакетов, что возможно, например, в случае стандартных сервисов типа Telnet. Удобно и надежно также применение цифровых сертификатов, выдаваемых доверительными органами, например, центром распределения ключей. Большинство программ-посредников разрабатывается таким образом, чтобы пользователь аутентифицировался только в начале сеанса работы с межсетевым экраном. После этого от него не требуется дополнительная аутентификация в течение времени, определяемого администратором.

Проверка подлинности получаемых и передаваемых данных необходима не только для аутентификации электронных сообщений, но и мигрирующих программ (Java, ActiveX Controls), по отношению к которым может быть выполнен подлог. Проверка подлинности сообщений и программ заключается в контроле их цифровых подписей. Для этого также могут применяться цифровые сертификаты.

Разграничение доступа к ресурсам внутренней или внешней сети. Способы разграничения к ресурсам внутренней сети ничем не отличаются от способов разграничения, поддерживаемых на уровне операционной системы. При разграничении

доступа к ресурсам внешней сети чаще всего используется один из следующих подходов:

– разрешение доступа только по заданным адресам во внешней сети;

– фильтрация запросов на основе обновляемых списков недопустимых адресов и блокировка поиска информационных ресурсов по нежелательным ключевым словам;

– накопление и обновление администратором санкционированных информационных ресурсов внешней сети в дисковой памяти брандмауэра и полный запрет доступа во внешнюю сеть.

Фильтрация и преобразование потока сообщений выполняется посредником на основе заданного набора правил. Здесь следует различать два вида программ посредников: экранирующие агенты, ориентированные на анализ потока сообщений для определенных видов сервиса, например, FTP, HTTP, Telnet; универсальные экранирующие агенты, обрабатывающие весь поток сообщений, например, агенты, ориентированные на поиск и обезвреживание компьютерных вирусов или прозрачное шифрование данных.

Программный посредник анализирует поступающие к нему пакеты данных, и если какой-либо объект не соответствует заданным критериям, то посредник либо блокирует его дальнейшее продвижение, либо выполняет соответствующие преобразования, например, обезвреживание обнаруженных компьютерных вирусов. При анализе содержимого пакетов важно, чтобы экранирующий агент мог автоматически распаковывать проходящие файловые архивы.

Брандмауэры с посредниками позволяют также организовывать защищенные виртуальные сети (Virtual Private Network – VPN), например, безопасно объединить несколько локальных сетей, подключенных к Internet, в одну виртуальную сеть. VPN обеспечивают прозрачное для пользователей соединение локальных сетей, сохраняя секретность и целостность передава-

емой информации путем ее динамического шифрования. При передаче по Internet возможно шифрование не только данных пользователей, но и служебной информации – конечных сетевых адресов, номеров портов и т.д.

Трансляция внутренних сетевых адресов. Данная функция реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов посредник выполняет автоматическое преобразование IP-адресов компьютеров-отправителей в один «надежный» IP-адрес, ассоциируемый с брандмауэром, из которого передаются все исходящие пакеты. В результате все исходящие из внутренней сети пакеты оказываются отправленными межсетевым экраном, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью. IP-адрес брандмауэра становится единственным активным IP-адресом, который попадает во внешнюю сеть.

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа. Кроме повышения безопасности трансляция адресов позволяет иметь внутри сети собственную систему адресации, не согласованную с адресацией во внешней сети, например, в сети Internet. Это эффективно решает проблему расширения адресного пространства внутренней сети и дефицита адресов внешней сети.

Регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и составление отчетов. В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий должно быть определено уведомление администратора, т.е. выдача предупредительных сигналов. Многие межсетевые экраны содержат мощную систему регистрации, сбора и анализа статистики. Учет может вестись по адресам клиента и сервера, идентификаторам пользователей, времени сеансов, времени соединений, количеству переданных/принятых данных, действиям администратора и пользователей. Системы учета позволяют произве-

сти анализ статистики и предоставляют администраторам подробные отчеты. За счет использования специальных протоколов посредники могут выполнить удаленное оповещение об определенных событиях в режиме реального времени.

Кэширование данных, запрашиваемых из внешней сети. При доступе пользователей внутренней сети к информационным ресурсам внешней сети вся информация накапливается на пространстве жесткого диска брандмауэра, называемого в этом случае proxy-сервером. Поэтому если при очередном запросе нужная информация окажется на proxy-сервере, то посредник предоставляет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого proxy-сер-вера. Функция кэширования успешно может использоваться для ограничения доступа к информационным ресурсам внешней сети. В этом случае все санкционированные информационные ресурсы внешней сети накапливаются и обновляются администратором на proxy-сервере. Пользователям внутренней сети разрешается доступ только к информационным ресурсам proxy-сервера, а непосредственный доступ к ресурсам внешней сети запрещается. Экранирующие агенты намного надежнее обычных фильтров и обеспечивают большую степень защиты. Однако они снижают производительность обмена данными между внутренней и внешней сетями и не обладают той степенью прозрачности для приложений и конечных пользователей, которая характерна для простых фильтров.

5.2.3. Особенности межсетевого экранирования на различных уровнях модели OSI

Брандмауэры поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный межсетевой экран удобно представить в виде совокупности

неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI. Чаще всего комплексный экран функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели. Соответственно различают такие неделимые брандмауэры (рис. 5.2), как экранирующий маршрутизатор, экранирующий транспорт (шлюз сеансового уровня), а также экранирующий шлюз (шлюз прикладного уровня).

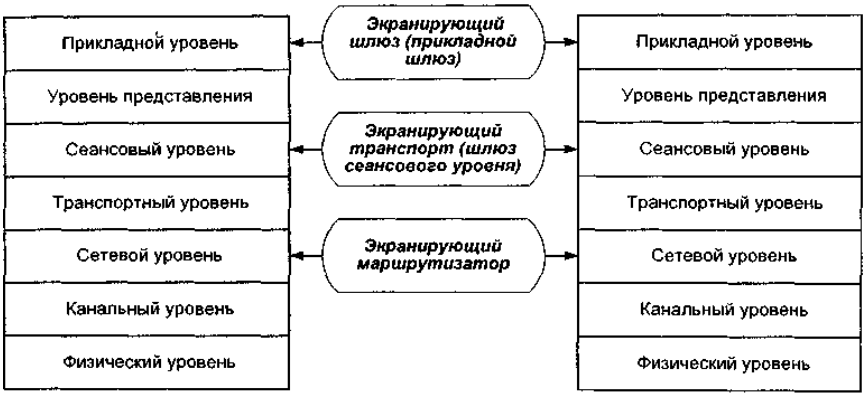

Рис. 5.2. Типы межсетевых экранов, функционирующих на отдельных уровнях модели OSI

Учитывая, что используемые в сетях протоколы (TCP/IP, SPX/IPX) не однозначно соответствуют модели OSI, то экраны перечисленных типов при выполнении своих функций могут охватывать и соседние уровни эталонной модели. Например, прикладной экран может осуществлять автоматическое зашифровывание сообщений при их передаче во внешнюю сеть, а также автоматическое расшифровывание криптографически закрытых принимаемых данных. В этом случае такой экран функционирует не только на прикладном уровне модели OSI, но и на уровне представления. Шлюз сеансового уровня при своем функционировании охватывает транспортный и сетевой уровни модели OSI. Экранирующий маршрутизатор при

анализе пакетов сообщений проверяет их заголовки не только сетевого, но и транспортного уровня.

Межсетевые экраны каждого из типов имеют свои достоинства и недостатки. Многие из используемых брандмауэров являются либо прикладными шлюзами, либо экранирующими маршрутизаторами, не поддерживая полную безопасность межсетевого взаимодействия. Надежную же защиту обеспечивают только комплексные межсетевые экраны, каждый из которых объединяет экранирующий маршрутизатор, шлюз сеансового уровня, а также прикладной шлюз.

5.3. **Экранирующий маршрутизатор**

Экранирующий маршрутизатор, называемый еще пакетным фильтром, предназначен для фильтрации пакетов сообщений и обеспечивает прозрачное взаимодействие между внутренней и внешней сетями. Он функционирует на сетевом уровне модели OSI, но для выполнения своих отдельных функций может охватывать и транспортный уровень эталонной модели. Решение о том, пропустить или отбраковать данные, принимается для каждого пакета независимо на основе заданных правил фильтрации. Для принятия решения анализируются заголовки пакетов сетевого и транспортного уровней. В качестве анализируемых полей IP- и TCP (UTP)-заголовков каждого пакета выступают: адрес отправителя; адрес получателя; тип пакета; флаг фрагментации пакета; номер порта источника; номер порта получателя.

Адреса отправителя и получателя являются IP-адресами. Эти адреса заполняются при формировании пакета и остаются неизменными при передаче его по сети.

Поле типа пакета содержит код протокола ICMP, соответствующего сетевому уровню, либо код протокола транспортного уровня (TCP или UDP), к которому относится анализируемый IP-пакет.

Флаг фрагментации пакета определяет наличие или отсутствие фрагментации IP-пакетов. Если флаг фрагментации для анализируемого пакета установлен, то данный пакет является подпакетом фрагментированного IP-пакета.

Номера портов источника и получателя добавляются драйвером TCP или UDP к каждому отправляемому пакету сообщения и однозначно идентифицируют приложение-отправитель, а также приложение, для которого предназначен этот пакет. Например, при использовании протокола передачи файлов FTP реализация данного протокола на сервере по умолчанию получает номер TCP-порта 21. Каждый Telnet-сервер по умолчанию имеет TCP-порт 23. Для возможности фильтрации пакетов по номерам портов необходимо знание принятых в сети соглашений относительно выделения номеров портов протоколам высокого уровня.

При обработке каждого пакета экранирующий маршрутизатор последовательно просматривает заданную таблицу правил, пока не найдет правила, с которыми согласуется полная ассоциация пакета. Здесь под ассоциацией понимается совокупность параметров, указанных в заголовках данного пакета. Если экранирующий маршрутизатор получил пакет, не соответствующий ни одному из табличных правил, он применяет прави-ло, заданное по умолчанию. Из соображений безопасности это правило обычно указывает на необходимость отбраковки всех пакетов, не удовлетворяющих ни одному из других правил.

В качестве пакетного фильтра может использоваться как обычный маршрутизатор, так и работающая на сервере программа, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Современные маршрутизаторы, например, маршрутизирующие устройства компаний Cisco, позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты как на входе, так и на выходе.

К достоинствам экранирующих маршрутизаторов относятся: простота самого экрана, а также процедур его конфигурирования и установки; прозрачность для программных приложений и минимальное влияние на производительность сети; низкая стоимость, обусловленная тем, что любой маршрутизатор в той или иной степени представляет возможность фильтрации пакетов.

Однако экранирующие маршрутизаторы не обеспечивают высокой степени безопасности, так как проверяют только заголовки пакетов и не поддерживают многие необходимые функции защиты, например, аутентификацию конечных узлов, криптографическое закрытие пакетов сообщений, а также проверку их целостности и подлинности. Экранирующие маршрутизаторы уязвимы для таких распространенных сетевых атак, как подделка исходных адресов и несанкционированное изменение содержимого пакетов сообщений. «Обмануть» межсетевые экраны данного типа не составляет труда: достаточно сформировать заголовки пакетов, которые удовлетворяют разрешающим правилам фильтрации.

5.4. Шлюз сеансового уровня

Шлюз сеансового уровня, называемый еще экранирующим транспортом, предназначен для контроля виртуальных соединений и трансляции IP-адресов при взаимодействии с внешней сетью. Он функционирует на сеансовом уровне модели OSI, охватывая в процессе своей работы также транспортный и сетевой уровни эталонной модели. Защитные функции экранирующего транспорта относятся к функциям посредничества.

Контроль виртуальных соединений заключается в контроле квитирования связи, а также контроле передачи информации по установленным виртуальным каналам.

При контроле квитирования связи шлюз сеансового уровня следит за установлением виртуального соединения между рабочей станцией внутренней сети и компьютером внешней се-

ти, определяя, является ли запрашиваемый сеанс связи допустимым. Такой контроль основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP. Однако если пакетный фильтр при анализе TCP-заголов-ков проверяет только номера портов источника и получателя, то экранирующий транспорт анализирует другие поля, относящиеся к процессу квитирования связи.

Чтобы определить, является ли запрос на сеанс связи допустимым, шлюз сеансового уровня выполняет следующие действия. Когда рабочая станция (клиент) запрашивает связь с внешней сетью, шлюз принимает этот запрос, проверяя, удовлетворяет ли он базовым критериям фильтрации, например, может ли DNS-сервер определить IP-адрес клиента и ассоциированное с ним имя. Затем, действуя от имени клиента, шлюз устанавливает соединение с компьютером внешней сети и следит за выполнением процедуры квитирования связи по протоколу TCP.

5.5. **Прикладной шлюз**

Прикладной шлюз, называемый экранирующим, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает наиболее надежную защиту межсетевых взаимодействий. Защитные функции прикладного шлюза, как и экранирующего транспорта, относятся к функциям посредничества. Однако прикладной шлюз в отличие от шлюза сеансового уровня может выполнять существенно большее количество функций защиты, к которым относятся следующие: идентификация и аутентификация пользователей при попытке установления соединений через брандмауэр; проверка подлинности информации, передаваемой через шлюз; разграничение доступа к ресурсам внутренней и внешней сетей; фильтрация и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации; регистрация событий, реагирование на задаваемые события, а также анализ зарегистрирован-

ной информации и генерация отчетов; кэширование данных, запрашиваемых из внешней сети.

Учитывая, что функции прикладного шлюза относятся к функциям посредничества, он представляет собой универсальный компьютер, на котором функционируют программные посредники (экранирующие агенты) – по одному для каждого обслуживаемого прикладного протокола (HTTP, FTP, SMTP, NNTP и др.).

Посредник каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе. Прикладной шлюз, так же как и шлюз сеансового уровня, перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию через шлюз, функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетью. Однако посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня. Во-первых, посредники прикладного шлюза связаны с конкретными приложениями (программными серверами), а во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели OSI.

Прикладные шлюзы используют в качестве посредников специально разработанные для этой цели программные серверы конкретных служб TCP/IP – серверы HTTP, FTP, SMTP, NNTP и др. Эти программные серверы функционируют на брандмауэре в резидентном режиме и реализуют функции защиты, относящиеся к соответствующим службам TCP/IP. Трафик UDP обслуживается специальным транслятором содержимого UDP-пакетов.

Как и в случае шлюза сеансового уровня, для связи между рабочей станцией внутренней сети и компьютером внешней сети соответствующий посредник прикладного шлюза образует два соединения: от рабочей станции до брандмауэра и от

брандмауэра до места назначения. Но в отличие от канальных посредников посредники прикладного шлюза пропускают только пакеты, сгенерированные теми приложениями, которые им поручено обслуживать. Например, программа-посредник службы HTTP может обрабатывать лишь трафик, генерируемый этой службой. Если в сети работает прикладной шлюз, то входящие и исходящие пакеты могут передаваться лишь для тех служб, для которых имеются соответствующие посредники. Так, если прикладной шлюз использует только программы-посредники HTTP, FTP и Telnet, то он будет обрабатывать лишь пакеты, относящиеся к этим службам, блокируя при этом пакеты всех остальных служб.

Фильтрация потоков сообщений реализуется прикладными шлюзами на прикладном уровне модели OSI. Соответственно посредники прикладного шлюза в отличие от канальных посредников обеспечивают проверку содержимого обрабатываемых пакетов. Они могут фильтровать отдельные виды команд или информации в сообщениях протоколов прикладного уровня, которые им поручено обслуживать. Например, для службы FTP возможно динамическое обезвреживание компьютерных вирусов в копируемых из внешней сети файлах. Кроме того, посредник данной службы может быть сконфигурирован таким образом, чтобы предотвращать использование клиентами команды PUT, предназначенной для записи файлов на FTP-сервер. Такое ограничение уменьшает риск случайного повреждения хранящейся на FTP-сервере информации и снижает вероятность заполнения его гигабайтами ненужных данных.

При настройке прикладного шлюза и описании правил фильтрации сообщений используются такие параметры, как название сервиса, допустимый временной диапазон его использования, ограничения на содержимое сообщений, связанных с данным сервисом, компьютеры, с которых можно пользоваться сервисом, идентификаторы пользователей, схемы аутентификации и др.

5.6. **Установка и конфигурирование межсетевых экранов**

Для эффективной защиты межсетевого взаимодействия система FireWall должна быть правильно установлена и сконфигурирована. Данный процесс осуществляется путем последовательного выполнения следующих этапов: разработки политики межсетевого взаимодействия; определения схемы подключения, а также непосредственного подключения межсетевого экрана; настройки параметров функционирования брандмауэра.

Перечисленные этапы отражают системный подход к установке любого программно-аппаратного средства, предполагающий, начиная с анализа, последовательную детализацию решения стоящей задачи.

5.6.1. Разработка политики межсетевого взаимодействия

Политика межсетевого взаимодействия является той частью политики безопасности в организации, которая определяет требования к безопасности информационного обмена с внешним миром. Данные требования обязательно должны отражать два аспекта: политику доступа к сетевым сервисам; политику работы межсетевого экрана.

Политика доступа к сетевым сервисам определяет правила предоставления, а также использования всех возможных сервисов защищаемой компьютерной сети. Соответственно в рамках данной политики должны быть заданы все сервисы, предоставляемые через сетевой экран, и допустимые адреса клиентов для каждого сервиса. Кроме того, должны быть указаны правила для пользователей, описывающие, когда и какие поль-зователи каким сервисом и на каком компьютере могут воспользоваться. Отдельно определяются правила аутентифи-

кации пользователей и компьютеров, а также условия работы пользователей вне локальной сети организации.

Политика работы межсетевого экрана задает базовый принцип управления межсетевым взаимодействием, положенный в основу функционирования брандмауэра. Может быть выбран один из двух таких принципов: запрещено все, что явно не разрешено; разрешено все, что явно не запрещено.

В зависимости от выбора решение может быть принято как в пользу безопасности в ущерб удобству использования сетевых сервисов, так и наоборот. В первом случае межсетевой экран должен быть сконфигурирован таким образом, чтобы блокировать любые явно не разрешенные межсетевые взаимодействия. Учитывая, что такой подход позволяет адекватно реализовать принцип минимизации привилегий, он с точки зрения безопасности является лучшим. Здесь администратор не сможет по забывчивости оставить разрешенными какие-либо полномочия, так как по умолчанию они будут запрещены. Доступные лишние сервисы могут быть использованы во вред безопасности, что особенно характерно для закрытого и сложного программного обеспечения, в котором могут быть различные ошибки и некорректности. Принцип «запрещено все, что явно не разрешено», в сущности является признанием факта, что незнание может причинить вред.

При выборе принципа «разрешено все, что явно не запрещено» межсетевой экран настраивается таким образом, чтобы блокировать только явно запрещенные межсетевые взаимодействия. В этом случае повышается удобство использования сетевых сервисов со стороны пользователей, но снижается безопасность межсетевого взаимодействия. Администратор может учесть не все действия, которые запрещены пользователям. Ему приходится работать в режиме реагирования, предсказывая и запрещая те межсетевые взаимодействия, которые отрицательно воздействуют на безопасность сети.

*5.6.2. **Определение схемы подключения***

Для подключения межсетевых экранов могут использоваться различные схемы, которые зависят от условий функционирования, а также количества сетевых интерфейсов брандмауэра.

Брандмауэры с одним сетевым интерфейсом (рис. 5.3) не достаточно эффективны как с точки зрения безопасности, так и с позиций удобства конфигурирования. Они физически не разграничивают внутреннюю и внешнюю сети, а соответственно не могут обеспечивать надежную защиту межсетевых взаимодействий. Настройка таких межсетевых экранов, а также связанных с ними маршрутизаторов представляет собой довольно сложную задачу, цена решения которой превышает стоимость замены брандмауэра с одним сетевым интерфейсом на брандмауэр с двумя или тремя сетевыми интерфейсами. Поэтому рассмотрим лишь схемы подключения межсетевых экранов с двумя и тремя сетевыми интерфейсами. При этом защищаемую локальную сеть будем рассматривать как совокупность закрытой и открытой подсетей. Здесь под открытой подсетью понимается подсеть, доступ к которой со стороны потенциально враждебной внешней сети может быть полностью или частично открыт. В открытую подсеть могут, например, входить общедоступные WWW-, FTP- и SMTP-серверы, а также терминальный сервер с модемным пулом.

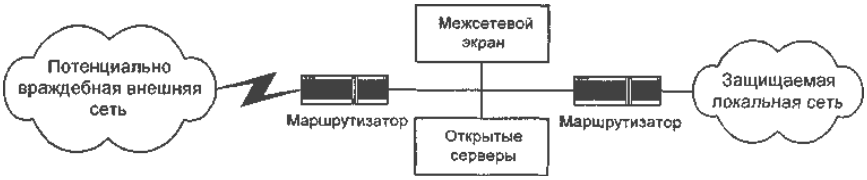

Рис. 5.3. Защита локальной сети брандмауэром с одним сетевым интерфейсом

Среди всего множества возможных схем подключения брандмауэров типовыми являются следующие: схема единой защи-

ты локальной сети; схема с защищаемой закрытой и незащищаемой открытой подсетями; схема с раздельной защитой закрытой и открытой подсетей.

Схема единой защиты локальной сети является наиболее простым решением (рис. 5.4), при котором брандмауэр целиком экранирует локальную сеть от потенциально враждебной внешней сети. Между маршрутизатором и брандмауэром имеется только один путь, по которому идет весь трафик. Обычно маршрутизатор настраивается таким образом, что брандмауэр является единственной видимой снаружи машиной. Открытые серверы, входящие в локальную сеть, также будут защищены межсетевым экраном. Однако объединение серверов, доступных из внешней сети, вместе с другими ресурсами защищаемой локальной сети существенно снижает безопасность межсетевых взаимодействий. Поэтому данную схему подключения брандмауэра можно использовать лишь при отсутствии в локальной сети открытых серверов или когда имеющиеся открытые серверы делаются доступными из внешней сети только для ограниченного числа пользователей, которым можно доверять.

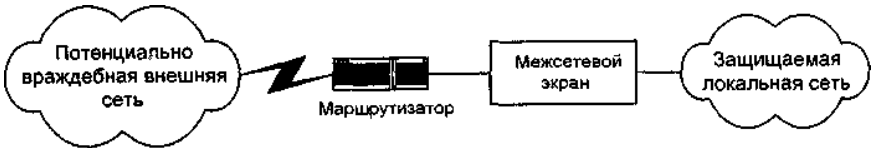

Рис. 5.4. Схема единой защиты локальной сети

При наличии в составе локальной сети общедоступных открытых серверов их целесообразно вынести как открытую подсеть до межсетевого экрана (рис. 5.5). Данный способ обладает более высокой защищенностью закрытой части локальной сети, но обеспечивает пониженную безопасность открытых серверов, расположенных до межсетевого экрана. Некоторые брандмауэры позволяют разместить эти серверы на себе. Но такое решение не является лучшим с точки зрения загрузки компьютера и безопасности самого брандмауэра.

Учитывая вышесказанное, можно сделать вывод, что схему подключения брандмауэра с защищаемой закрытой подсетью и незащищаемой открытой подсетью целесообразно использовать лишь при невысоких требованиях по безопасности к открытой подсети.

Рис. 5.5. Схема с защищаемой закрытой и незащищаемой открытой подсетями

В случае же, когда к безопасности открытых серверов предъявляются повышенные требования, то необходимо использовать схему с раздельной защитой закрытой и открытой подсетей. Такая схема может быть построена на основе одного брандмауэра с тремя сетевыми интерфейсами (рис. 5.6) или на основе двух брандмауэров с двумя сетевыми интерфейсами (рис. 5.7). В обоих случаях доступ к открытой и закрытой подсетям локальной сети возможен только через межсетевой экран. При этом доступ к открытой подсети не позволяет осуществить доступ к закрытой подсети.

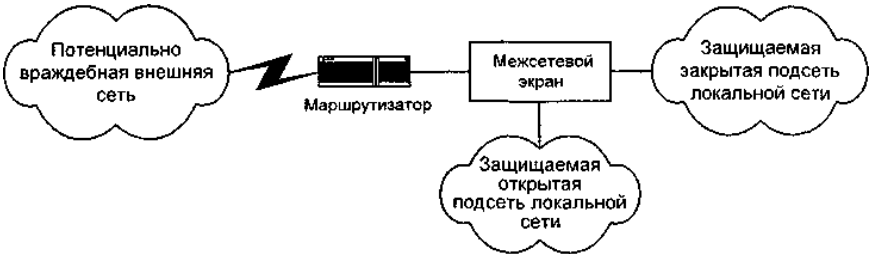

Рис. 5.6. Схема с раздельной защитой закрытой и открытой подсетей

на основе одного брандмауэра с тремя сетевыми интерфейсами

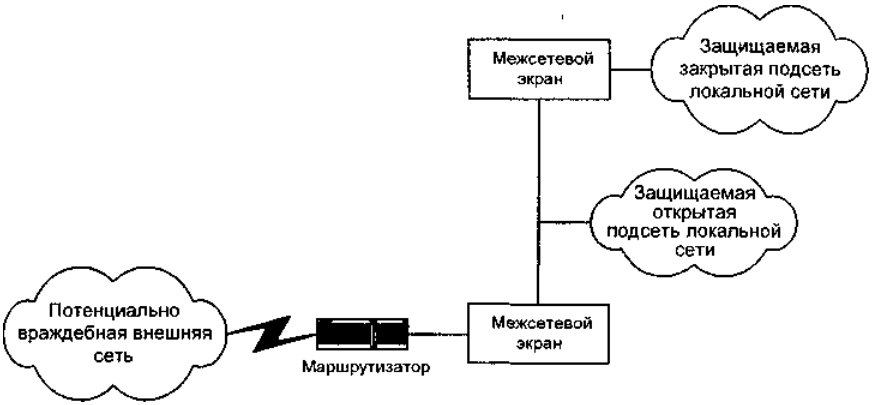

Рис. 5.7. Схема с раздельной защитой закрытой и открытой подсетей на основе двух брандмауэров с двумя сетевыми интерфейсами

Из последних двух схем большую степень безопасности межсетевых взаимодействий обеспечивает схема с двумя брандмауэрами, каждый из которых образует отдельный эшелон защиты закрытой подсети. Защищаемая открытая подсеть здесь выступает в качестве экранирующей подсети. Обычно экранирующая подсеть конфигурируется таким образом, чтобы обеспечить доступ к компьютерам подсети как из потенциально враждебной внешней сети, так и из закрытой подсети локальной сети. Однако прямой обмен информационными пакетами между внешней сетью и закрытой подсетью невозможен.

5.7. Настройка параметров функционирования межсетевого экрана

Межсетевой экран представляет собой программно-аппаратный комплекс защиты, состоящий из компьютера, а также функционирующих на нем операционной системы и специального программного обеспечения. Следует отметить, что это специ-

альное программное обеспечение часто также называют брандмауэром.

Компьютер брандмауэра должен быть достаточно мощным и физически защищенным, например, находиться в специально отведенном и охраняемом помещении. Кроме того, он должен иметь средства защиты от загрузки ОС с несанкционированного носителя. После установки на компьютер брандмауэра выбранной операционной системы, ее конфигурирования, а также инсталляции специального программного обеспечения можно приступать к настройке параметров функционирования всего межсетевого экрана. Этот процесс включает следующие этапы: выработку правил работы межсетевого экрана в соответствии с разработанной политикой межсетевого взаимодействия и описание правил в интерфейсе брандмауэра; проверку заданных правил на непротиворечивость; проверку соответствия параметров настройки брандмауэра разработанной политике межсетевого взаимодействия.

Формируемая на первом этапе база правил работы межсетевого экрана представляет собой формализованное отражение разработанной политикой межсетевого взаимодействия. Компонентами правил являются защищаемые объекты, пользователи и сервисы. В число защищаемых объектов могут входить обычные компьютеры с одним сетевым интерфейсом, шлюзы (компьютеры с несколькими сетевыми интерфейсами), маршрутизаторы, сети, области управления. Защищаемые объекты могут объединяться в группы. Каждый объект имеет набор атрибутов, таких как сетевой адрес, маска подсети и т.п. Часть этих атрибутов следует задать вручную, остальные извлекаются автоматически из информационных баз, например NIS/NIS+, SNMP MIB, DNS. Следует обратить внимание на необходимость полного описания объектов, так как убедиться в корректности заданных правил экранирования можно только тогда, когда определены все сетевые интерфейсы шлюзов и маршрутизаторов. Подобную информацию можно получить

автоматически от SNMP-агентов. При описании правил работы межсетевого экрана пользователи наделяются входными именами и объединяются в группы. Для пользователей указываются допустимые исходные и целевые сетевые адреса, диапазон дат и времени работы, а также схемы и порядок аутентификации. Определение набора используемых сервисов выполняется на основе встроенной в дистрибутив брандмауэра базы данных, имеющей значительный набор TCP/IP-сервисов. Нестандартные сервисы могут задаваться вручную с помощью специальных атрибутов. Прежде чем указывать сервис при задании правил, необходимо определить его свойства. Современные брандмауэры содержат предварительно подготовленные определения всех стандартных TCP/IP-сервисов, разбитых на четыре категории – TCP, UDP, RPC, ICMP.

6. ВИРТУАЛЬНЫЕ ЗАЩИЩЕННЫЕ СЕТИ

6.1. Принципы построения

Распределенные корпоративные сети могут создаваться на базе отдельных компьютеров или локальных вычислительных сетей (ЛВС) посредством соединения их через специально проложенные каналы связи, через каналы связи общего пользования и через открытые компьютерные сети типа Интернет.

Корпоративные сети на базе Интернет наиболее привлекательны, т.к. обладают рядом преимуществ: относительно малой стоимостью; высокой пропускной способностью; высокой масштабируемостью (размеры сети не ограничиваются каналами передачи данных). Но при этих преимуществах имеется серьезная проблема – обеспечение безопасности информации. В этих сетях необходимо защищать информацию в процессе передачи ее по открытым каналам связи, а также обеспечивать защиту ЛВС и отдельных компьютеров от несанкционированного допуска со стороны внешней среды (пользователей Интернет).

Защита информации при передаче ее по открытым каналам связи требует: аутентификации взаимодействующих сторон; шифрования информации; подтверждения подлинности и целостности доставленной информации; защите от повтора, задержки и удаления сообщений; защите от отрицательных фактов отправления и приема сообщений.

ЛВС и отдельные компьютеры, объединенные через открытую глобальную сеть в единую компьютерную сеть, обеспечивающую защищенность передаваемой и хранимой информации, называются виртуальной частной сетью (VPN). Открытая глобальная сеть может быть основой огромного числа виртуальных частных сетей (рис. 6.1).

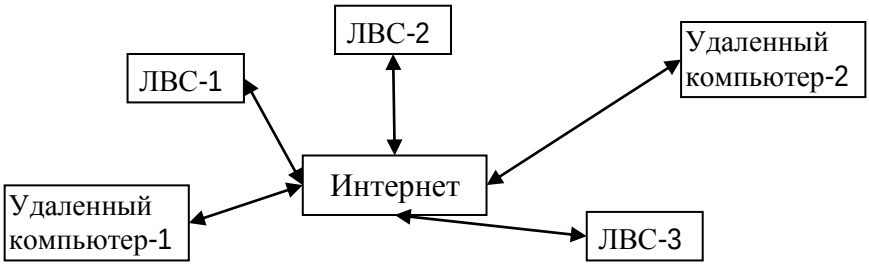

Рис. 6.1. Пример VPN

Защита информации при передаче по открытым каналам основана на создании защищенных виртуальных каналов связи, криптозащищенных туннелей или туннелей VPN. Каждый туннель VPN – соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений (рис. 6.2, маршрут ЛВС-1—1—2—3—9—8—ЛВС-2).

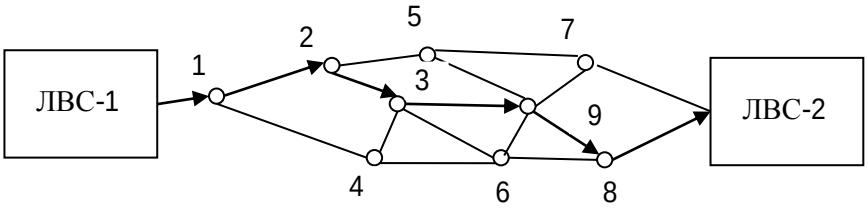

Рис. 6.2. Образование туннеля VPN

Защищенные виртуальные каналы могут прокладываться (рис. 6.3): от каждого компьютера ЛВС-1 до каждого компьютера ЛВС-2, если внутри ЛВС нужно также обеспечит защиту; от пограничного маршрутизатора или МСЭ ЛВС-1 до пограничного маршрутизатора или МСЭ ЛВС-2; от провайдера Интернет ЛВС-1 до провайдера Интернет ЛВС-2 (если можно быть уверенным в том, что в проводных каналах опасность несанкционированного доступа гораздо меньше, чем в каналах с разделением пакетов).

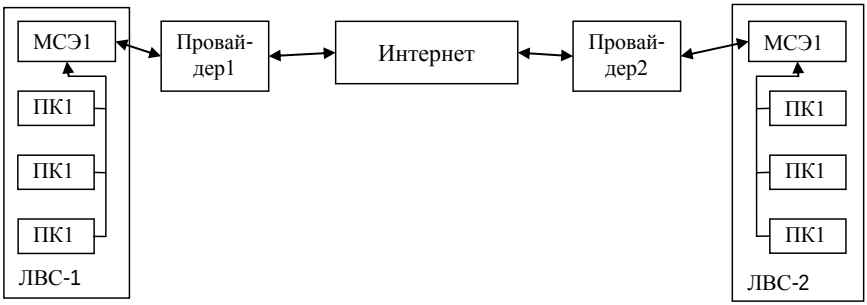

Рис. 6.3. Возможные каналы VPN

Создание защищенного туннеля выполняют компоненты виртуальной сети, функционирующие в узлах, между которыми создается туннель. Эти узлы называются инициатором и терминатором туннеля. Инициатор инкапсулирует (встраивает) пакеты в новый пакет, содержащий в качестве адреса отправителя адрес инициатора, адреса получателя адрес терминатора; вложенный пакет полностью шифруется и подписывается ЭЦП. Терминатор, получив пакет, извлекает из него зашифрованный пакет, расшифровывает его и отправляет конечному адресату в ЛВС. Инициатор и терминатор должны использовать одинаковые криптопротоколы и поддерживать протокол безопасного распределения ключей.

6.2. **Протоколы VPN-сетей**

Протоколы VPN появились сравнительно недавно. Они являются свободными для распространения и реализации. Для независимости от прикладных протоколов и приложений протоколы VPN работают на одном уровне из более низких уровней: канальном, сетевом и сеансовом.

Канальному уровню соответствуют протоколы PPTP, L2F, L2TP; сетевому – IPSec, SKIP; сеансовому – SSL/TLS, SOCKS. Чем ниже уровень протокола, тем он «прозрачней» для пользователя. Однако набор услуг безопасности при этом снижается. В VPN сетях криптозащита может одновременно выполняться на всех уровнях модели, однако при этом снижается скорость преобразования. Поэтому практически шифрование используется только на одном уровне.

6.2.1. Канальный уровень

Протокол PPTP (Point – to – Point Tunneling Protocol) представляет собой расширенный PPP. В этом протоколе конкретные алгоритмы шифрования и аутентификации не установлены. Клиенты удаленного доступа в операционных системах Windows поставляются с версией DES и называются MPPE (Microsoft Point – to – Point Encryption).

Протокол L2F (Layer – 2 Forwarding) позволяет использовать для удаленного доступа к провайдеру не только PPP, но и другие протоколы (SLTP), а для переноса по сети Интернет не только IP, как PPTP. В нем также не установлены конкретные алгоритмы шифрования и аутентификации. Протокол L2F является компонентом операционной системы IOS компании Cisco, которая устанавливается во все ее устройства межсетевого взаимодействия. С 1996 года эти протоколы объединены и названы протоколами туннелирования второго уровня L2TP (Layer – 2 Tunneling Protocol). Этот протокол поддерживают Microsoft, Cisco, 3Com. Протокол L2TP работает независимо

от протоколов сетевого уровня, на которых функционируют различные ЛВС IP, IPX, NetBEUI. Пакеты этих протоколов шифруются, подписываются и инкапсулируются в пакеты Internet – IP, передаются по виртуальным каналам. Однако возникают сложности при организации и поддержке нескольких каналов в связи с необходимостью контроля состояния каждого канала. Поэтому протоколы канального уровня лучше всего подходят для создания защищенного удаленного доступа к ЛВС.

6.2.2. Сетевой уровень

Протокол Ipsec (Internet Protocol Security) входит в состав протокола IP v.6. Он предусматривает стандартные алгоритмы: аутентификации пользователей при инициализации туннеля, шифрования и электронной цифровой подписи, управления ключами. Туннель Ipsec между ЛВС поддерживает множество индивидуальных каналов передачи данных. Ipsec может работать только с IP, поэтому его используют вместе с L2TP, который не зависит от протокола транспортного уровня и работает с IPX.

Протокол SKIP (Simple Key management for Internet Protocol) управляет работой с ключами, использует алгоритм Диффи–Хелманна, но не поддерживает переговоров по поводу используемого алгоритма шифрования. Если получатель не смог расшифровать пакет, то он уже не сможет этого сделать. Версия протокола ISAKMP не содержит этот недостаток и включена в Ipsec. В IPv.4 может применяться как SKIP, так и ISAKMP.

6.2.3. Сеансовый уровень

Протоколы сеансового уровня (посредники) шифруют, ретранслируют трафик из защищаемой сети в открытую сеть Internet для каждого сокета в отдельности.

Protocol SSL/TLS (Security Sokets Lauer/Transport Lauer Security) создает защищенный туннель между конечными точками виртуальной сети, обеспечивая взаимную аутентификацию абонентов, шифрование и подлинность циркулирующих по туннелю данных. Он использует комплексно и симметричное шифрование, и ассиметричное. Открытые ключи пользователей размещаются в цифровых сертификатах, заверенных ЭЦП Сертификационного центра.

Protocol SOCKS устанавливает аутентифицированный сеанс клиентского компьютера с сервером, исполняющим роль посредника. Посредник проводит любые операции, запрашиваемые клиентом, осуществляя при этом контроль за трафиком, и может блокировать конкретные приложения пользователей. Протоколы сеансового уровня по сравнению с канальными и сетевыми протоколами, которые просто открывают или закрывают канал для всего трафика в обоих направлениях, могут пропускать не весь трафик и ограничивать его направление.

7. СОЗДАНИЕ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ И ОЦЕНКА УРОВНЯ ИХ БЕЗОПАСНОСТИ

Общая методология создания защищенных компьютерных систем и оценка уровня их безопасности изложена в группе международных стандартов ИСО/МЭК 15408-99 «Общие критерии оценки безопасности информационных технологий» и в их белорусских аналогах СТБ 34.101.1-3.2004 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Часть 2. Функциональные требования безопасности. Часть 3. Гарантийные требования безопасности». Эти стандарты формализуют процессы создания и оценки современных информационных систем. Поскольку безопасность таких систем невозможно

оценить количественно, то предложено судить о безопасности по тому набору требований безопасности, который реализован в той или иной системе. В стандартах изложены процедуры формирования таких наборов, их оформление и использование.

7.1. **Требования безопасности**

Требования безопасности – это все требования, реализация которых необходима для обеспечения безопасности информационной системы. Эти требования диктуются необходимым уровнем конфиденциальности, доступности и целостности информации, обрабатываемой в системе, а также уровнем опасности среды, в которой используется система.

Требования безопасности подразделяют на функциональные и гарантийные. Функциональные требования – это совокупность необходимых функций системы, обеспечивающих безопасность информации. Гарантийные требования – это совокупность требований, подтверждающих то, что функциональные требования сформированы правильно, реализованы в полном объеме и корректно.

7.1.1. Функциональные требования безопасности

Все элементарные функциональные требования, называемые в стандарте элементами, образуют нижний уровень в иерархической структуре функциональных требований. Элементы группируются в компоненты, которые образуют следующий уровень иерархии. Объединение идет по общему домини-рующему признаку. Функциональные компоненты объединяются в семейства, а семейства – в классы. Всего сформировано 11 классов, 66 семейств, 135 компонентов.

Класс формулирует одну из обобщенных функций безопасности. Ему присваивается название и маркировка. Например, класс FIA «Идентификация и аутентификация». Маркировка трехбуквенная, «F» обозначает, что это класс функциональных требований, IA – абривиатура названия.

Семейство формулирует некоторую часть класса. Имеет название и семибуквенную маркировку. Например, семейство FIA_UID «Идентификация пользователя».

Компонент – составная часть семейства. Имеет маркировку и название. Например, FIA _UID.1 «Выбор момента идентификации».

Элемент маркируется дополнительной цифрой и сопровождается описанием. Например, FIA _UID.1.2 «Каждый пользователь должен быть успешно идентифицирован до разрешения любого действия».

В описании любого класса имеется схема, показывающая иерархию компонентов внутри семейств, например, рис. 7.1. При последовательном соединении компонентов компонент, который находится выше по иерархии, обеспечивает больший уровень безопасности. Например, для семейства-1 компонент-1 включает компоненты-2 или 3, компонент-2 включает компонент-1, но является только частью компонента-3. Для семейства-2 компоненты-1 или 2 находятся на одном уровне иерархии и должны использоваться вместе, причем вместо компонента-2, можно использовать компонент-3, если его функции достаточно.

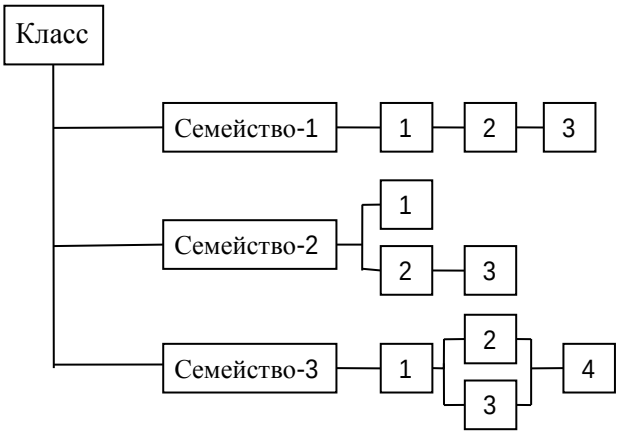

Рис. 7.1. Пример структуры функциональных требований

7.1.2. Гарантийные требования безопасности

Гарантийные требования безопасности основываются на активном исследовании безопасности системы на всех этапах жизненного цикла. Не достижение целей безопасности возникает вследствие преднамеренного использования или случайной активизации уязвимостей. Причинами уязвимостей являются: неполнота выбранных функциональных требований; некорректная реализация функциональных требований; несоответствующие условия эксплуатации.

Форма представления «Гарантийные требования безопасности» аналогична форме представления «функциональные требования»: класс – семейство – компонент – элемент.

Каждый класс имеет название и маркировку из трех символов. Первый символ «А» означает, что это класс гарантийных требований. Например, класс ADF «Разработка».

Семейство охватывает некоторую часть класса, имеет название и семибуквенную маркировку. Например, семейство ADF_FSP «Функциональная спецификация».

Компонент – составная часть семейства. Имеет маркировку и название. Например, ADF_FSP.1 «Неформальная функциональная спецификация».

Семейства гарантийных требований содержат только иерархические компоненты (компонент с большим номером содержит больше требований, чем компонент с меньшим).

Элемент гарантий маркируется дополнительной цифрой и буквой, сопровождается описанием. Например, ADF_FSP1.1E «Эксперт должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию свидетельств».

Элемент гарантий принадлежит к одному из трех типов: элементы действий разработчика (маркируются символом D); элементы представления и содержания свидетельств (маркируются символом C); элементы действий эксперта (маркируются символом E).

Пример структуры гарантийных требований одного класса изображен на рис. 7.2.

Всего сформировано 10 классов, 44 семейства, 93 компонентов. Перечислим классы гарантийных требований: ADF «Разработка», ALC «Поддержка жизненного цикла», ATE «Тестирование», AVA «Оценка уязвимостей», ADO «Поставка и эксплуатация», ACM «Управление конфигурацией», AGD «Руководства», AMA «Поддержка гарантий», APE «Оценка профиля защиты», ASE «Оценка задания по безопасности».

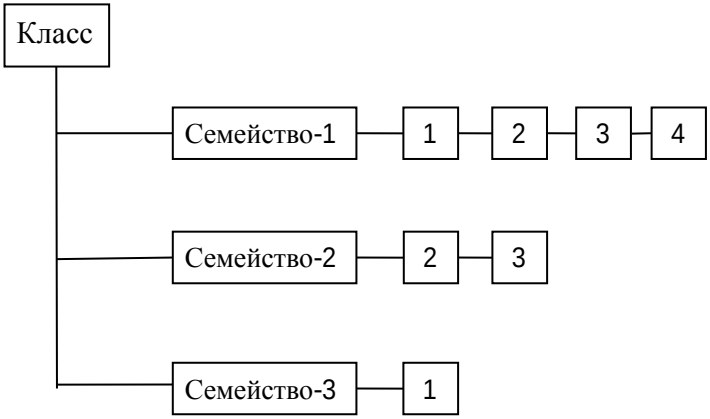

Рис. 7.2. Пример структуры гарантийных требований

7.1.2. Оценочные уровни доверия

Гарантийные требования, предъявляемые к безопасности конкретной системы, группируют в уровни гарантий. Всего предлагается 7 уровней. Каждый уровень включает компоненты из различных классов и семейств. Чем выше номер уровня гарантий, тем больше доверия к безопасности системы. Например, уровень 1 предусматривает только функциональное тестирование безопасности системы. Может использоваться, когда достаточно только уверенности в правильном функционировании, а угрозы безопасности отсутствуют. Оценка может проводиться без помощи разработчика с минимальными затратами. Уровень 7 предусматривает формальную верификацию проекта безопасности системы. Применим

при разработке безопасных систем, работающих в условиях высокого риска. Компоненты этого уровня обеспечивают гарантию посредством анализа функциональной спецификации, полной спе-цификации интерфейсов, эксплуатационной документации, про-ектов верхнего и нижнего уровней, а также структурированного представления реализации.

7.2. **Профиль защиты и задание по безопасности**

Профили защиты (ПЗ) представляет собой независимый от реализации типовой набор требований безопасности для совокупности изделий определенного вида, отвечающий соответствующим целям безопасности. ПЗ предназначен для многократного использования и определяет требования безопасности изделий, включая функциональные и гарантийные требования, в отношении которых установлено, что они являются достаточными и эффективными для достижения установленных целей безопасности.

Профили защиты разрабатываются и используются как стандартизованные наборы требований с целью повышения обоснованности задания требований безопасности изделий, оценки безопасности и возможности проведения сравнительного анализа уровня безопасности различных изделий.

Задание по безопасности (ЗБ) содержит совокупность требований безопасности для конкретного изделия, которые обеспечивают достижение установленных целей безопасности. ЗБ представляет собой набор требований безопасности, которые могут быть определены ссылкой на профили защиты, ссылкой на отдельные стандартизованные требования или же содержать требования в явном виде.

ЗБ формируется разработчиком изделия и является основой для проведения оценки и сертификации изделия.

Структура профиля защиты строго регламентирована. Он содержит следующие разделы.

1. ВВЕДЕНИЕ ПЗ
1.1. Идентификация ПЗ
1.2. Аннотация ПЗ
2. ОПИСАНИЕ ОО
3. СРЕДА БЕЗОПАСНОСТИ ОО
3.1. Предположения безопасности
3.2. Угрозы
3.3. Политика безопасности организации
4. ЦЕЛИ БЕЗОПАСНОСТИ
4.1. Цели безопасности для ОО
4.2. Цели безопасности для среды
5. ТРЕБОВАНИЯ БЕЗОПАСНОСТИ ИТ
5.1. Функциональные требования безопасности ОО
5.2. Требования доверия к безопасности ОО
5.3. Требования безопасности для среды ИТ
6. ЗАМЕЧАНИЯ ПО ПРИМЕНЕНИЮ
7. ОБОСНОВАНИЕ
7.1. Логическое обоснование целей безопасности
7.2. Логическое обоснование требований безопасности

Задание по безопасности по структуре во многом похоже на ПЗ и содержит дополнительную информацию, разъясняющую, каким образом требования ПЗ должны быть реализованы для конкретного изделия.

8. НАДЕЖНОСТЬ ФУНКЦИОНИРОВАНИЯ АППАРАТУРЫ

8.1. Основные понятия, термины и определения

Надежностью устройства называют свойство, обеспечивающее возможность выполнения этим устройством заданных функций с заданными характеристиками в определенных условиях эксплуатации и в течение требуемого интервала времени. Состояние устройства, при котором оно выполняет заданные функции с заданными характеристиками, называют

работоспособностью. Свойство устройства сохранить работоспособность в течение требуемого интервала времени называют безотказностью. Нарушение работоспособности устройства называют отказом. Вследствие отказа возникает состояние неработоспособности, при котором устройство не удовлетворяет хотя бы одному из предъявленных к нему технических требований. Появление отказа не всегда означает потерю свойства надежности. Конечно, существуют устройства, дальнейшее использование которых невозможно уже после первого отказа. Такие устройства называют невосстанавливаемыми или устройствами одноразового действия. Примерами могут служить электрическая лампочка и баллистическая ракета. Однако очень многие устройства в системах управления и в системах передачи и приема информации используются многократно после устранения появляющихся отказов. Свойство, которое заключается в возможности восстановления работоспособности устройства после устранения отказа, называют восстанавливаемостью. Более общим понятием является свойство ремонтопригодности устройства, заключающееся в возможности предупреждения, обнаружения и устранения отказов путем проведения ремонтов и технического обслуживания.

Состояние работоспособности устройства в произвольно выбранный момент времени, называют готовностью. Если устройство, находясь в режиме ожидания, окажется работоспособным в произвольно выбранный момент времени и, начиная с этого момента, будет сохранять работоспособность в течение заданного интервала времени, то тогда обеспечивается оперативная готовность устройства.

Для многофункциональных устройств отказ, приводящий к потере части функций, может рассматриваться как состояние, при котором лишь снижается эффективность функционирования устройства.

Для некоторых устройств имеет значение свойство сохраняемости, т.е. способность непрерывно сохранять исправное и

работоспособное состояние (заданные характеристики) во время и после хранения и транспортировок.

Сохранение работоспособности (при установленной системе технического обслуживания и ремонтов) до предельного состояния называют долговечностью.

Итак, потенциальное свойство системы – ее надежность – в общем случае проявляется в виде составляющих: безотказности, ремонтопригодности, сохраняемости и долговечности. В зависимости от назначения системы каждая из указанных составляющих может иметь большее или меньшее значение. Так, для систем одноразового действия главной является безотказность, а для систем длительной (непрерывной или циклической) эксплуатации – безотказность и восстанавливаемость (ремонтопригодность).

В дальнейшем предполагается, что любое исследуемое устройство может находиться только в двух состояниях: работоспособном и неисправном. Однако это не единственный способ описания состояний устройства. Иногда приходится рассматривать случаи, когда устройство может находиться в одном из многих (более двух) состояний, т.е. когда кроме полной работоспособности представляет интерес частичная – выполнение лишь некоторых функций. В связи с этим различают полный отказ, до устранения которого использование устройства невозможно, и частичный отказ, до устранения которого остается возможность хотя бы частичного использования устройства.

Отказы делятся на внезапные и постепенные. Внезапные отказы возникают в результате скачкообразного изменения заданных параметров устройства. Причинами таких отказов являются, например, обрывы, нарушения контактов, короткие замыкания, пробои, механические разрушения. Постепенные отказы, возникающие в результате старения, характеризуются постепенным ухудшением заданных параметров устройств. Причинами подобных отказов могут быть изменения характе-

ристик электронных приборов с течением времени, приводящие к выходу этих характеристик за допустимые пределы.

8.2. **Основные показатели надежности**

Количественно свойства надежности оцениваются с помощью показателей надежности. Различают единичные показатели надежности, относящиеся к одному из указанных выше свойств, составляющих надежность устройства, и комплексные показатели надежности, относящиеся к нескольким таким свойствам.

Так как отказ является случайным событием, то интервал времени от момента включения устройства до первого отказа (наработка до первого отказа) представляет случайную величину. Обозначим эту величину x. Любая случайная величина характеризуется рядом вероятностных характеристик, таких как интегральная функция распределения вероятностей $F(t) = P(x \le t)$, где t – некоторый фиксированный момент времени, дифференциальная функция распределения вероятностей $f(t) = d F(t)/dt$, математическое ожидание случайной величины x, равное

$$m = \int_0^\infty tf(t)dt .$$

8.2.1. Единичные показатели надежности

Единичные показатели безотказности выражаются через перечисленные вероятностные характеристики времени работы до отказа. Основными показателями безотказности являются: вероятность отказа, вероятность безотказной работы, среднее время работы до отказа (средняя наработка на отказ), интенсивность отказов.

Вероятность отказа. Вероятность того, что отказ произойдет после включения через время, не превышающее заданной величины t, т. е. что $x \le t$, называется вероятностью отказа

$$q(t) = P(x \le t), \quad t > 0.$$

Функция $q(t)$ монотонно возрастает от нуля до единицы. График функции $q(t)$ изображен на рис. 8.1.

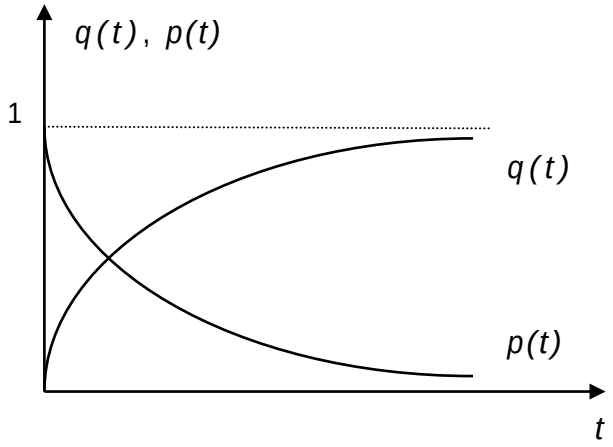

Рис. 8.1. Вероятность безотказной работы и вероятность отказа

Вероятность безотказной работы. Вероятность безотказной работы на заданном временном интервале, т.е. вероятность того, что наработка до первого отказа превышает заданную величину t, равна

$$p(t) = P(x > t) = 1 - q(t), \quad t > 0.$$

Функция $p(t)$ монотонно убывает от единицы до нуля (предполагается, что в момент включения устройство работоспособно). Графики функций $q(t)$, $p(t)$ показаны на рис. 8.1.

Средним временем работы до отказа называется математическое ожидание случайной величины x и равно

$$T_{\text{ср}} = \int_0^\infty tf(t)t = \int_0^\infty p(t)dt .$$

Интенсивность отказов. Интенсивностью отказов называется величина $\Lambda = \frac{1}{p(t)}\frac{dp(t)}{dt} = \frac{f(t)}{p(t)}$. Интенсивность отказов имеет смысл среднего количества отказов в бесконечно малый промежуток времени.

Рассуждая аналогично, будем считать, что восстановление является случайным событием, а интервал времени от момента отказа до момента восстановления представляет собой случайную величину. Обозначим эту величину x. Интегральная функция распределения вероятностей восстановления равна $F_в(t) = P(x \le t)$, где t – некоторый фиксированный момент времени, дифференциальная функция распределения вероятностей $f_в(t) = d\,F_в(t)/dt$, математическое ожидание случайной величины x, равное

$$m = \int_0^\infty t f_в(t)dt\,.$$

Основными показателями восстанавливаемости являются: вероятность восстановления, вероятность невосстановления, среднее время восстановления, интенсивность восстановлений.

Вероятность восстановления. Вероятность того, что восстановление произойдет после отказа за время, не превышающее заданной величины t, т.е. что $x \le t$, называется вероятностью восстановления.

$$p_в(t) = P(x \le t), \quad t > 0.$$

График функции $p_в(t)$ изображен на рис. 8.2.

Вероятность невосстановления. Вероятность того, что время восстановления превышает заданную величину t, равна

$$q_в(t) = P(x > t) = 1 - p_в(t), \quad t > 0.$$

Функция $q_в(t)$ монотонно убывает от единицы до нуля (предполагается, что в момент включения устройство работоспособно). График функции $p_в(t)$ показан на рис. 8.2.

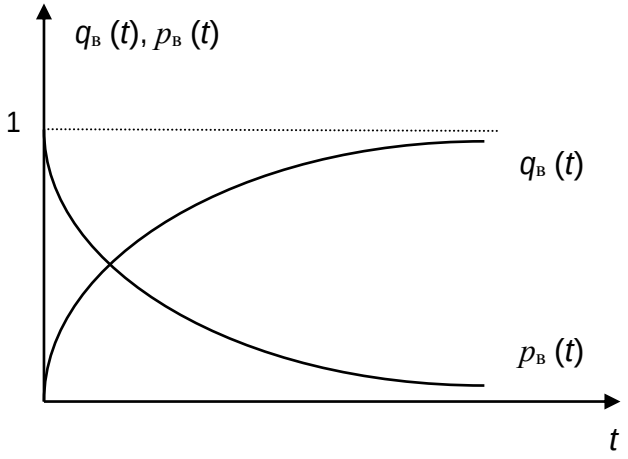

Рис. 8.2. Вероятность восстановления и **в**ероятность невосстановления

Среднее время восстановления. Средним временем восстановления называется математическое ожидание случайной величины x и равно

$$T_в = \int_0^\infty t f_в(t) t = \int_0^\infty p_в(t) dt\,.$$

Интенсивность восстановлений. Это величина $\mu_в = \frac{1}{p_в(t)} \times \frac{dp_в(t)}{dt} = \frac{f_в(t)}{p_в(t)}$. Интенсивность восстановлений имеет смысл среднего количества восстановлений в бесконечно малый промежуток времени.

8.2.2. Комплексные **показа**тели **надежности**

Комплексные показатели надежности зависят одновременно от нескольких свойств надежности, например, от безотказности и восстанавливаемости. Основные из них: коэффициент готовности, коэффициент оперативной готовности, коэффициент простоя.

Коэффициентом готовности называется вероятность того, что если система включена, то в произвольный момент времени она находится в работоспособном состоянии

$$K_{\text{г}} = \frac{T_{\text{ср}}}{T_{\text{ср}} + T_{\text{в}}}.$$

Коэффициент оперативной готовности. Коэффициентом оперативной готовности называется вероятность того, что при включении системы в произвольный момент времени она будет работоспособна и безотказно проработает в течение времени t. Коэффициент численно равен произведению коэффициента готовности на вероятность безотказной работы

$$K_{\text{ог}} = K_{\text{г}} \cdot p(t).$$

8.3. **Основные математические модели**

8.3.1. Зависимость интенсивности отказов от времени

Опыт эксплуатации очень многих электронных приборов и некоторых электромеханических элементов показывает, что для этих элементов характерны следующие три вида зависимостей интенсивности отказов от времени, соответствующих трем «периодам жизни» этих устройств (рис. 8.3):

1) интенсивность отказов монотонно уменьшается, что характерно для периода приработки, в течение которого прояв-

ляются все дефекты, обусловленные главным образом технологическими причинами, а не свойствами конструкции;

2) интенсивность отказов остается приблизительно постоянной, что соответствует так называемому периоду нормальной эксплуатации. В этот период возникают в основном внезапные отказы;

3) интенсивность отказов монотонно возрастает, что свидетельствует о наступлении периода износа, вызванного процессами старения. В этом периоде превалируют постепенные отказы.

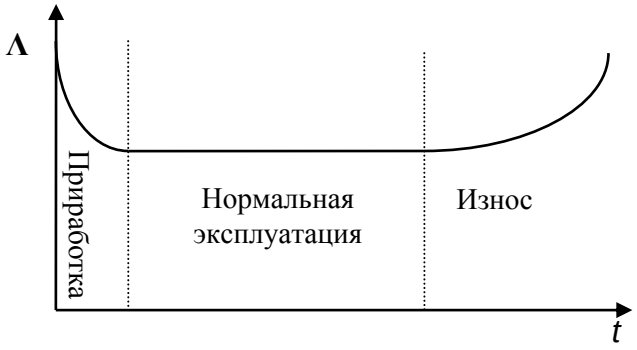

Рис. 8.3. Зависимость интенсивности отказов от времени

Интенсивность отказов существенно зависит от электрических нагрузок и нагрузок, обусловленных воздействием внешних условий (электрические и тепловые нагрузки, вибрации).

Наибольший практический интерес представляет период нормальной эксплуатации.

Принято считать, что для этого периода время безотказной работы имеет экспоненциальный закон распределения вероятностей.

8.3.2. Экспоненциальное распределение времени безотказной работы

Экспоненциальное распределение времени безотказной работы имеет следующие вероятностные характеристики:

дифференциальная функция распределения вероятностей $f(t) = \lambda e^{-\lambda t}$;

интегральная функция распределения вероятностей $F(t) = 1 - e^{-\lambda t}$;

математическое ожидание случайной величины $m = \frac{1}{\lambda}$.

На рис. 8.4 изображены графики вероятностных характеристик. Единичные показатели безотказности при экспоненциальном распределении времени безотказной работы равны:

вероятность отказа $q(t) = 1 - e^{-\lambda t}$;

вероятность безотказной работы $p(t) = e^{-\lambda t}$;

среднее время работы до отказа $T_{ср} = \frac{1}{\lambda}$;

интенсивность отказов $\Lambda = \lambda$.

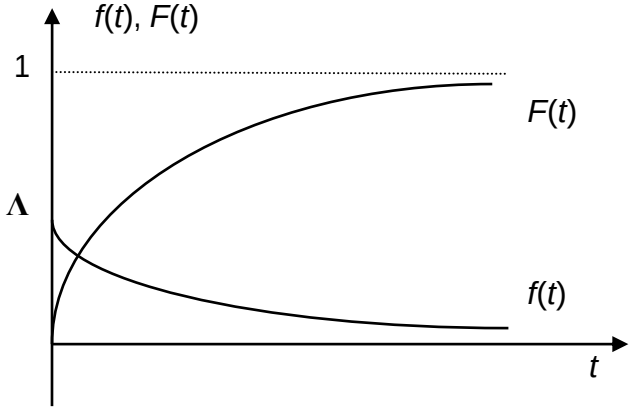

Рис. 8.4. Графики вероятностных характеристик

Как видно из последнего выражения при экспоненциальном распределении времени безотказной работы интенсивность отказов постоянна и не зависит от времени. Таким образом, период нормальной эксплуатации характеризуется экспоненциальным распределением интервала безотказной работы.

8.3.3. Пуассоновский поток отказов

Для восстанавливаемой системы имеет место повторяющиеся потоки случайных событий: поток отказов и поток восстановлений. Рассмотрим вероятностные характеристики потока отказов. Обозначим через x_t количество отказов в интервале от 0 до t, а вероятность того, что за время от 0 до t произойдет не менее n отказов, обозначим как $F_n(t) = P(x_t) \geq n$.

Среднее число отказов на интервале от 0 до t. Среднее число отказов на интервале от 0 до t – это математическое ожидание случайной величины x_t, равное

$$H(t) = m(x_t) \quad \text{или} \quad H(t) = \sum_{m=1}^{\infty} F_n(t).$$

Интенсивность потока отказов. Это величина, численно равная количеству отказов за бесконечно малый интервал времени, отнесенных к величине этого интервала:

$$\Lambda(t) = d(H(t)/dt.$$

Поток отказов называется пуассоновским, если время между отказами подчиняется экспоненциальному распределению, т.е. дифференциальная функция распределения $f(t) = \lambda\ e^{-\lambda t}$. Для пуассоновского потока отказов справедливо $P(x_t = n) = \frac{(\lambda t)^n}{n!}\ e^{-\lambda t}$.

Среднее число отказов на интервале от 0 до t равно $H(t) = \lambda t$, а интенсивность потока отказов – $\Lambda(t) = \lambda$. Следовательно, поток отказов в период нормальной эксплуатации системы является пуассоновским.

Аналогичные характеристики вводятся для потока восстановлений.

8.4. Расчет безотказности аппаратуры.

Компьютерная система, как любая радиоэлектронная аппаратура, состоит из большого количества элементов, которые объединены в блоки и устройства. Отказ каждого элемента (блока, устройства) по-разному влияет на работоспособность всей системы. Есть элементы, отказы которых приводит к полному нарушению работоспособности всей системы. Например, отказ процессора. Есть элементы, отказы которых приводят к частичному нарушению работоспособности всей системы. Например, отказ винчестера. Есть элементы, при отказе которых система использует резервные элементы, путем реконфигурации своей структуры.

Для расчета безотказности системы, состоящей из элементов, отказы которых приводит к полному нарушению работоспособности всей системы, используют последовательную схему надежности (рис. 8.5, *а*).

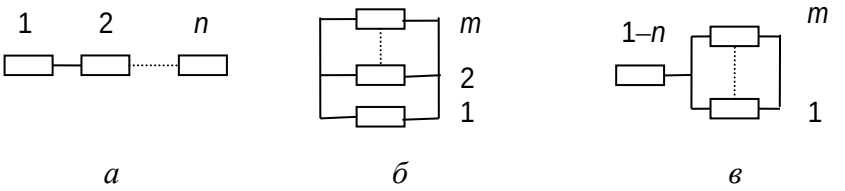

Рис. 8.5. Основные схемы надежности

Для расчета безотказности системы, состоящей из элементов, отказы которых не приводят к нарушению работоспособности всей системы, используют параллельную схему надежности (рис. 8.5, *б*). Для расчета безотказности системы, состоящей из элементов первого и второго типа, используют последовательно-параллельную схему надежности (рис. 8.5, *в*). Расчет показателей безотказности системы ведется через показатели безотказности элементов. Получим основные расчетные соотношения.

Для последовательно соединенных элементов.

Если $p_i(t)$ – вероятность безотказной работы i-го элемента, где $i = \overline{1,n}$,то:

$$p_c(t) = \prod_{i=1}^{n} p_i(t), \quad q_c(t) = 1 - p_c(t), \quad T_{\text{ср}} = \int_0^{\infty} p_c(t)dt .$$

При экспоненциальном распределении времени безотказной работы $p_i(t) = e^{-\lambda_i t}$, где λ_i – интенсивность отказов i-го элемента (приводится в справочниках), поэтому

$$p_c(t) = e^{-\lambda_c t}, \text{ где } \lambda_c = \sum_{i=1}^{n} \lambda_i , \quad q_c(t) = 1 - e^{-\lambda_c t},$$

$$T_{\text{ср}} = \frac{1}{\lambda_c}.$$

Для параллельно соединенных элементов.

Если $q_i(t)$ – вероятность отказа i-го элемента, где $i = \overline{1,m}$, то

$$q_c(t) = \prod_{i=1}^{m} q_i(t), \quad p_c(t) = 1 - q_c(t), \quad T_{\text{ср}} = \int_0^{\infty} p_c(t)dt .$$

При экспоненциальном распределении времени безотказной работы $q_i(t) = 1 - e^{-\lambda_i t}$, поэтому

$$q_c(t) = \prod_{i=1}^{m} (1 - e^{-\lambda_i t}), \quad p_c(t) = 1 - \prod_{i=1}^{m} (1 - e^{-\lambda_i t}),$$

$$T_{\text{ср}} = \int_0^{\infty} p_c(t)dt .$$

Для последовательно-параллельно соединенных элементов.

При этом соединении вначале находится вероятность безотказной работы параллельно соединенных элементов по приведенным выше формулам, обозначим ее $p_m(t)$, затем вероят-

ность безотказной работы последовательно соединенных элементов $p_n(t)$, затем вероятность безотказной работы системы, как $p_c(t) = p_n(t) \cdot p_m(t)$, а затем $q_c(t) = 1 - p_c(t)$, $T_{\text{ср}} = \int_0^\infty p_c(t)dt$.

Пример расчета.

Пусть схема надежности системы – последовательно-параллельная (рис. 8.6), время безотказной работы всех элементов – экспоненциальное с интенсивностями отказов: $\lambda_1 = 10^{-5}$1/ч, $\lambda_2 = 2 \cdot 10^{-5}$ 1/ч, $\lambda_3 = 4 \cdot 10^{-5}$ 1/ч, $\lambda_4 = 5 \cdot 10^{-5}$ 1/ч. Найдем основные показатели безотказности системы за время $t = 10000$ ч.

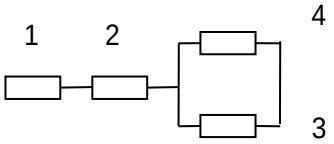

Рис. 8.6. Схема надежности системы

Безотказность составных частей равна:

$$P_n(t) = p_1(t) \cdot p_2(t) = e^{-(\lambda_1+\lambda_2)t},$$

$$p_m(t) = 1 - q_3(t) \cdot q_4(t) = 1 - (1 - e^{-\lambda_3 t}) \cdot (1 - e^{-\lambda_4 t}).$$

Показатели безотказности системы равны:

$$p_c(t) = p_n(t) \cdot p_m(t) = e^{-(\lambda_1+\lambda_2)t} \cdot (1 - (1 - e^{-\lambda_3 t}) \cdot (1 - e^{-\lambda_4 t})) = 0{,}645;$$

$$q_c(t) = 1 - e^{-(\lambda_1+\lambda_2)t} \cdot (1 - (1 - e^{-\lambda_3 t}) \cdot (1 - e^{-\lambda_4 t})) = 0{,}355;$$

$$T_{\text{ср}} = \int_0^\infty p_c(t)dt = \int_0^\infty e^{-(\lambda_1+\lambda_2)t} \cdot (1 - (1 - e^{-\lambda_3 t}) \cdot (1 - e^{-\lambda_4 t}))dt = 18450 \text{ ч.}$$

Литература

1. Герасименко, В.А. Основы защиты информации / В.А. Герасименко, А.А. Малюк. – М.: Московский государственный инженерно-физический институт, 1997.
2. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; под ред. В.Ф. Шаньгина. – М.: Радио и связь, 1999.
3. Мельников, В.В. Защита информации в компьютерных системах / В.В. Мельников. – М.: Финансы и статистика, 1997.
4. «Шпионские штучки» и устройства для защиты объектов и информации: справочное пособие. – СПб., 1996.
5. Хореев, А.И. Защита информации. Технические каналы утечки информации / А.И. Хорев. – М., 1998.
6. Ярочкин, В.И. Информационная безопасность: учебник для вузов / В.И. Ярочкин. – Изд. 2. – Минск: Академический проект, 2005.
7. Зима, В.М. Безопасность глобальных сетевых технологий / В.М. Зима, А.А. Молдавян, Н.А. Молдовян. – СПб., 2001.
8. Правовые и организационно-технические методы защиты информации: учебное пособие / В.Ф. Голиков. – Минск: БГУИР, 2004.
9. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель: СТБ 34.101.1-2004(ИСО/МЭК 15408-1:1999).
10. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности: СТБ 34.101.2-2004 (ИСО/МЭК 15408-2:1999).
11. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 3. Гарантийные требования безопасности: СТБ 34.101.3-2004 (ИСО/МЭК 15408-3:1999).
12. Левин, Б.Р. Теория надежности радиотехнических систем / Б.Р. Левин. – М.: Советское радио, 1978.

Учебное издание

ГОЛИКОВ Владимир Федорович

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И НАДЕЖНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ

Пособие для студентов специальностей 1-40 01 01 «Программное обеспечение информационных технологий» и 1-53 01 02 «Автоматизированные системы обработки информации» всех форм обучения

В 2 частях

Ч а с т ь 1

Редактор Л.Н. Шалаева
Компьютерная верстка Н.А. Школьниковой

Подписано в печать 06.05.2010.
Формат 60×84 1/16. Бумага офсетная.
Отпечатано на ризографе. Гарнитура Таймс.
Усл. печ. л. 5,00. Уч.-изд. л. 3,91. Тираж 100. Заказ 474.

Издатель и полиграфическое исполнение:
Белорусский национальный технический университет.
ЛИ № 02330/0494349 от 16.03.2009.
Проспект Независимости, 65. 220013, Минск.