МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»

Кафедра безопасности информационных систем

Н.Н. Мошак, Т.М. Татарникова

ОРГАНИЗАЦИЯ БЕЗОПАСНОГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

Учебное пособие

Санкт-Петербург
2014

УДК 519.718

Мошак Н.Н., Татарникова Т.М. Организация безопасного доступа к информационным ресурсам: Учеб. пособие. СПб: ГУАП, 2014.

Рецензент: Молдовян Н.А.

Учебное пособие предназначено для изучения основных разделов дисциплины «Защита сетей от несанкционированного доступа» и содержит описание угроз информационным и вычислительным ресурсам компьютерных сетей, характеристику методов аутентификации, основанных на применении пароля, биометрических характеристик и OTP-токенов, рекомендации к построению политики информационной безопасности инфотелекоммуникационной сети, а также краткие выводы по главам для закрепления пройденного материала.

Предназначено для подготовки бакалавров по направлению 090900 – Информационная безопасность.

Содержание

ВВЕДЕНИЕ

Информация, как результат обработки, передачи и хранения определяет с одной стороны действия людей, которые с ней работают и с другой стороны сложность технического и программного обеспечения, созданного человеком для защиты информации.

Последствия потери, подлога или хищения данных, хранящихся в вычислительных системах, а также нарушения работоспособности самих вычислительных средств могут быть очень высоки.

Обеспечение безопасности данных в вычислительных сетях подчиняется общей концепции информационной безопасности.

Стандарт ГОСТ Р ИСО 7498-2-99 определяет три основные задачи обеспечения безопасности (защиты) компьютерных систем и сетей:

- Обеспечение целостности информации.
- Обеспечение доступности информации.
- Обеспечение конфиденциальности.

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

Целостность является важнейшим аспектом информационной безопасности, особенно в тех случаях, когда информация используется для управления различными процессами, например техническими, социальными и т.д. Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к негативным последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

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

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

Конфиденциальность является самым проработанным у нас в стране аспектом информационной безопасности. Однако, практическая реализация мер по обеспечению конфиденциальности современных информационных систем в России связана с такими трудностями, как закрытость сведений о технических каналах утечки информации, а также законодательные и технические проблемы в области пользовательской криптографии.

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

Решение задачи доступа к конфиденциальной информации реализуется с

помощью систем контроля и управления доступом как для контроля перемещения людей по территории охраняемого объекта, обеспечения безопасности персонала и посетителей, так и для сохранности материальных и информационных ресурсов предприятия.

Сегодня системы контроля и управления доступом используются на промышленных предприятиях, в офисах, магазинах, на автостоянках и автосервисах, в жилых помещениях.

Нарушение любой из трех категорий – целостности, конфиденциальности и/или доступности приводит к нарушению информационной безопасности в целом. Так, нарушение доступности приводит к отказу в доступе к информации, нарушение целостности приводит к фальсификации информации и, наконец, нарушение конфиденциальности приводит к раскрытию информации.

Выделение этих категорий в качестве базовых составляющих информационной безопасности обусловлено необходимостью реализации комплексного подхода при обеспечении режима информационной безопасности. Кроме этого, нарушение одной из этих категорий может привести к нарушению или полной бесполезности двух других. Например, хищение пароля для доступа к компьютеру (нарушение конфиденциальности) может привести к его блокировке, уничтожению данных (нарушение доступности информации) или фальсификации информации, содержащейся в памяти компьютера (нарушение целостности информации).

Угрозы целостности, конфиденциальности и несанкционированного доступа к важной информации, а также работоспособности вычислительных систем могут быть выполнены при постоянном участии человека либо выполняется «злоумышленными» программами без непосредственного участия человека.

Задачи по защите от реализации угроз одинаковы независимо от их типа и включают следующие этапы:

1) преградить несанкционированный доступ к корпоративным ресурсам;

2) сделать невозможным несанкционированное использование компьютерных ресурсов, если доступ к ним все-таки осуществлен;

3) своевременно обнаружить факт несанкционированных действий и устранить причины, а также последствия их реализации.

Способы решения перечисленных задач по защите от несанкционированных действий со стороны людей и компьютерных программ существенно отличаются друг от друга. Могут применяться как специальные механизмы защиты, такие как шифрование, заполнение трафика, управление маршрутизацией, цифровая подпись, контроль доступа, обеспечение целостности, аутентификация, нотаризация, так и общие механизмы защиты, такие как доверительная функциональность, метки безопасности, аудиторская проверка, которые могут быть задействованы для усиления последних.

На практике услуги безопасности должны быть включены в соответствующие уровни логической структуры сети для обеспечения требований ее политики информационной безопасности.

Учебное пособие раскрывает существующие способы решения задач по защите информации в вычислительных сетях и поддерживающие их технологии защиты.

1 ОБЩИЕ ВОПРОСЫ ОРГАНИЗАЦИИ КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1 Структура и функции сети

Компьютерная сеть – это сложный комплекс взаимосвязанных и согласованно функционирующих программных и аппаратных компонентов. Изучение сети в целом предполагает знание принципов работы ее отдельных элементов:

- компьютеров;
- коммуникационного оборудования;
- операционных систем;
- сетевых приложений.

Весь комплекс программно-аппаратных средств сети может быть описан многослойной моделью. В основе любой вычислительной сети лежит аппаратный слой. Его составляют стандартизованные компьютерные платформы.

Платформенный подход предполагает разработку не с «нуля», а с использованием специально разработанным для этой сети набором аппаратных решений, служб и примитивов, специально разработанных программных продуктов (программная платформа).

Основные слои компьютерной сети составляют:

Первый слой – Компьютеры - от персональных до супер компьютеров. Например, для всемирного экологического мониторинга США построили суперкомпьютер с объявленным быстродействием $3 \cdot 10^{13}$ флопс.

Второй слой – это коммуникационное оборудование: кабельные системы, повторители, мосты, коммутаторы, маршрутизаторы и модульные концентраторы. Сегодня коммуникационное устройство может представлять собой сложный специализированный мультипроцессор, который нужно конфигурировать, оптимизировать, администрировать и обеспечивать его информационную безопасность. Оборудование второго слоя раньше считалось дополнительным, но сейчас по сложности реализации и выполняемым функциям стало основным как по влиянию на характеристики сети, так и по стоимости. Изучение принципов работы коммуникационного оборудования требует знания протоколов, используемых как в локальных, так и глобальных сетях.

Третьим слоем, образующим программную платформу сети, являются **операционные системы.**

Операционные системы обеспечивают управление локальными и распределенными ресурсами, а именно:

– планирование ресурса – кому, когда, в каком количестве выделить данный ресурс, речь идет о разделяемом ресурсе;

– мониторинг состояния ресурса, то есть получение и анализ оперативной информации о состоянии ресурса: занят/свободен, в случае делимого ресурса – какая часть занята/свободна;

– обеспечивает взаимодействие с другими операционными системами;

– безопасность и защищенность данных.

Самым верхним слоем являются различные сетевые приложения, такие как сетевые базы данных, почтовые системы, средства архивирования данных, системы автоматизации коллективной работу и др.

Сетевая операционная система выполняет:

– управление отдельными ресурсами: распределения оперативной памяти между процессами; планирование и диспетчеризация процессов управления процессорами;

– обмен сообщениями в сети: адресацию и буферизацию сообщений, выбор маршрута передачи, т.е. обеспечивают транспортировку сообщений.

Функционально сетевая операционная система делится на две части:

– Серверную, которая предоставляет собственные ресурсы локальных серверов в общее пользование, обеспечивает обработку запросов удаленного доступа к собственной файловой системе и базам данных, управляет очередями запросов удаленных пользователей к своим локальным серверам.

– Клиентскую, которая обеспечивает доступ к удаленным ресурсам и услугам и их использование, прием ответов от удаленных серверов и преобразование их в локальный формат, выполняет распознавание запроса, преобразование формы запроса.

Для конечного пользователя сеть – это набор сетевых служб или услуг, с помощью которых он, например, получает доступ к удаленному файлу, принимает и отправляет сообщения по электронной почте, распечатывает документ на принтере, подключенному к другому компьютеру и многое другое. Кроме собственно обмена данными, сетевые службы должны решать и более специфические задачи. К таким задачам относятся обеспечение непротиворечивости нескольких копий данных, размещенных на разных машинах (служба репликации), администрирование учетных записей пользователей, мониторинг сети, обеспечение безопасности, доставка данных по запросу, в том числе мультимедийной информации в реальном времени – изображений, видео и аудио.

Компьютерные сети можно классифицировать по различным критериям. Деление на локальные и глобальные сети происходит по территориальному признаку, то есть по площади покрываемой территории. Другим важным признаком классификации сетей является назначение предоставляемых услуг – это сети операторов связи, которые оказывают общедоступные услуги и корпоративные сети, оказывающие услуги сотрудникам только того предприятия, которое владеет сетью.

Сегодня различия между локальными и глобальными компьютерными сетями стали сглаживаться. Изолированные ранее локальные сети объединяются друг с другом, при этом в качестве связующей среды используются глобальные сети. Тенденция сближения различных типов сетей характерна не только для локальных и глобальных компьютерных сетей, но и для телекоммуникационных сетей других типов. К телекоммуникационным сетям, кроме компьютерных, относятся, телефонные сети, радиосети и телевизионные сети. Во всех них в

качестве ресурса, предоставляемого клиентам, выступает информация.

Телефонные сети оказывают интерактивные услуги. Радио и телевизионные сети оказывают широковещательные услуги.

Конвергенция телекоммуникационных сетей идет по многим направлениям. Прежде всего, наблюдается сближение видов услуг, предоставляемых клиентам. Сближение сетей происходит сегодня на основе цифровой передачи информации различного типа, метода коммутации пакетов и программирования услуг. Представление голоса и изображения в цифровой форме сделало возможным передачу аудио-, видео и компьютерного трафика по одним и тем же цифровым каналам

В настоящее время для удовлетворения возрастающих потребностей пользователей операторы местной телефонной связи предлагают услугу "Triple Play Services" – голос, видео, передача данных - доступ в Интернет, которую с полным основанием можно назвать универсальной услугой связи XXI века.

Технологии Triple Play создают широкий спектр новых информационных услуг. Приведем примеры наиболее популярных предоставляемых и потенциальных услуг.

Услуги передачи данных:

- высокоскоростной доступ в Интернет;
- сетевое резервное копирование (backup);
- сетевые диски (виртуальное дисковое пространство);
- персональные файловые ресурсы в Интернете;
- доступ к игровым серверам.

Голосовые услуги:

- городская и междугородная телефония;
- радиовещание по IP.

Видеоуслуги:

- телевещание по IP (IPTV, HD-IPTV);
- платные видеоканалы PPV (Pay Per View);
- видео по требованию VoD (Video on Demand);
- персональный видеомагнитофон PVR;
- видеотелефония;
- услуга видеоконференц-связи;
- видеонаблюдение;
- игровые видеоприставки.

В результате конвергенции сетевых технологий и появления новых информационных услуг появился термин – инфокоммуникационная сеть, который говорит о двух составляющих современной сети – информационной (компьютерной) и телекоммуникационной.

Инфокоммуникационная сеть в общем случае состоит из следующих компонентов:

- Сети доступа
- Магистральной сети
- Информационных центров.

Сеть доступа и магистральная сеть строятся на основе коммутационных узлов. Каждый такой узел оснащен некоторым количеством портов, которые соединяются с портами других коммутационных узлов каналами связи. Сеть доступа составляет нижний уровень иерархии инфокоммуникационной сети. К этой сети подключаются конечные (терминальные) узлы – оборудование, установленное у пользователей (абонентов, клиентов) сети. Основное назначение сети доступа – концентрация информационных потоков, поступающих по многочисленным каналам связи от оборудования пользователей, в сравнительно небольшим количеством узлов магистральной сети. Сеть доступа, как и инфокоммуникационная сеть в целом, может состоять из нескольких уровней. Коммутационные узлы нижнего уровня мультиплексируют информацию, поступающую по абонентским каналам, и передают ее коммутационным узлам верхнего уровня, чтобы те, в свою очередь передали ее коммутационным узлам магистральной сети.

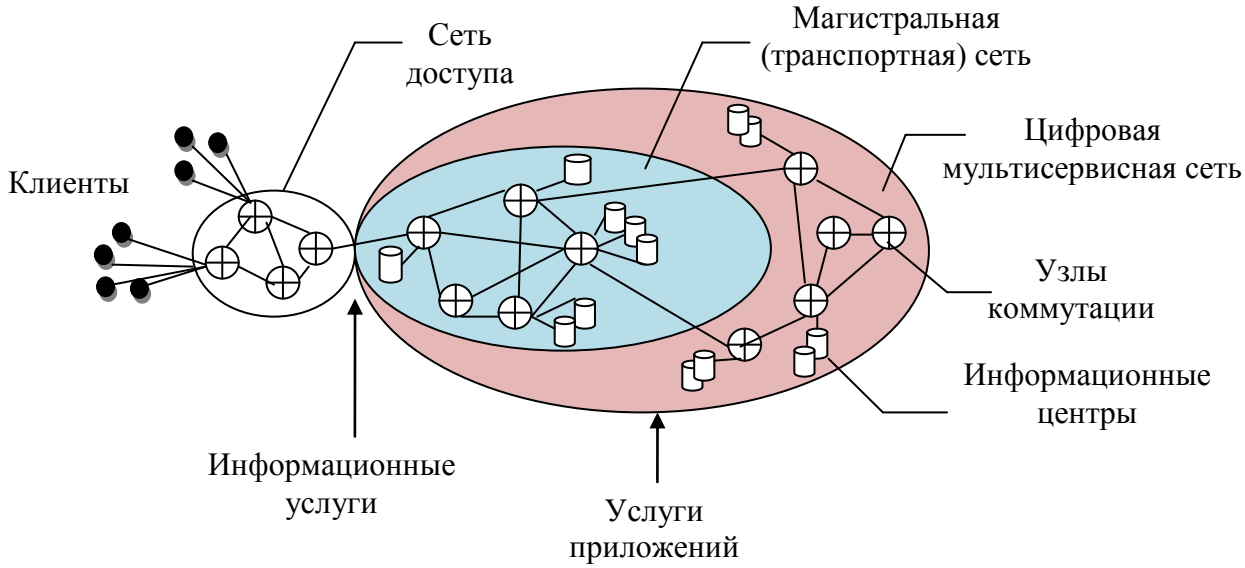


Рис. 1.1. Фрагмент функциональной структуры инфокоммуникационной сети

Магистральная сеть объединяет отдельные сети доступа и выполняет функции транзита трафика между ними по высокоскоростным каналам.

Информационные центры – это собственные информационные ресурсы сети, на основе которой осуществляется обслуживание пользователей. В таких центрах хранится информация двух типов:

пользовательская информация, то есть та, которая непосредственно интересует пользователей сети и предоставляется как информационные услуги

вспомогательная информация, помогающая предоставлять услуги пользователям (услуги приложений).

Примером информационных услуг первого типа могут служить web-доступ, справочные услуги, поиск мультимедийных файлов, распределенная обработка, интерактивная речь, интерактивное видео и другие.

Услугами второго типа являются электронная торговля, дистанционное

образование, развлечения, биллинг, видеоконференци и другие.

1.2 Формат информационного пакета

Данные в сетях передаются блоками. Такие блоки принято называть *Пакеты* или *Кадры* (Packet, Frame). Каждый стандарт вычислительной сети определяет свой формат пакета. Они различаются по длине, расположению полей, однако, в независимости от типа сети, структура пакета одинакова (рис. 1.2).

Назначение полей:

Преамбула (Preamble) – служит для синхронизации работы приемника и передатчика;

АП – Адрес Приемника (DA – Destination Address) - адрес станции, которой направляется пакет;

АИ – Адрес Источника (SA – Source Address) – адрес передающей станции;

Поле Данных (Data) – содержит управляющую информацию, собственно данные либо пакет с другим протоколом (при передах через шлюзы);

ПОО – Поле Обнаружения Ошибок (CRC) – служит для определения достоверности полученной информации.

Рис. 1.2. Структура пакета

В качестве адресов могут использоваться логические или аппаратные (физические) адреса.

Логический адрес (Logical Address) – определяется используемым протоколом обмена данными и может быть изменен в процессе работы. С помощью логических адресов можно создать группы устройств, выполняющих одинаковые функции – серверы, маршрутизаторы и т.п. Это упрощает управление работой сети.

Физический адрес (Physical Address) – определяется стандартом локальной сети, однозначно идентифицирует в сети данный узел и не может быть изменен после подключении устройства к сети. В Ethernet на сетевом адаптере устанавливается ПЗУ, в которой прошит физический адрес сетевого адаптера. Изменить его можно, только заменив микросхему ПЗУ.

В качестве адреса приемника могут использоваться:

Широковещателъный или Общий Адрес (Broadcast). Пакет с таким адресом принимается и обрабатывается всеми станциями сети. Широковещательный адрес используется и при логической адресации.

Групповой Адрес (Multicast). Пакет с таким адресом принимается и обрабатывается определенной группой станций. Например, только серверами, только маршрутизаторами и т.п. Этот адрес может быть только логическим.

Частный Адрес (Unicast или Private). Пакет с таким адресом принимается и обрабатывается только определенной станцией, адрес которой соответствует частному адресу. В качестве частных адресов используются логические или физические адреса.

1.3 Система адресации

При объединении нескольких сетей возникает проблема адресации в них компьютеров.

Адрес – уникальный идентификатор компьютера в сети.

Адрес узла сети должен уникально идентифицировать компьютер в сети любого масштаба.

Схема назначения адресов должна сводить к минимуму ручной труд администратора и вероятность дублирования адресов.

Адрес должен иметь иерархическую структуру, удобную для построения больших сетей.

Адрес должен быть удобен для пользователей сети, а это значит, что он должен иметь символьное представление например, Server3 или www.cisco.com.

Адрес должен иметь по возможности компактное представление, чтобы не перегружать память коммуникационной аппаратуры – сетевых адаптеров, маршрутизаторов и т.п.

Наибольшее распространение получили три схемы адресации узлов.

Аппаратные (*hardware*) *адреса* (*MAC-адреса*). Эти адреса предназначены для сети небольшого или среднего размера, они не имеют иерархической структуры. Такой адрес обычно используется только аппаратурой, поэтому его стараются сделать по возможности компактным и записывают в виде двоичного или шестнадцатеричного значения, например 0081005e24a8. Аппаратные адреса либо встраиваются в аппаратуру компанией-изготовителем, либо генерируются автоматически при каждом новом запуске оборудования, причем уникальность адреса в пределах сети обеспечивает оборудование. Использование аппаратных адресов связано с известным недостатком - при замене аппаратуры, например, сетевого адаптера, изменяется и адрес компьютера.

MAC-адрес имеет формат 6 байтов: старшие 3 байта – идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем.

Символьные адреса или DNS-имена. Эти адреса предназначены для запоминания людьми и поэтому обычно несут смысловую нагрузку. Символьные адреса легко использовать как в небольших, так и крупных сетях. Для работы в больших сетях символьное имя может иметь сложную иерархическую структуру.

Числовые составные адреса (*IP-адреса*). Символьные имена удобны для людей, но из-за переменного формата и потенциально большой длины их передача по сети не очень экономична. Поэтому в больших сетях в качестве адресов узлов используют числовые составные адреса фиксированного и компактного форматов. В них поддерживается двухуровневая иерархия, адрес делится на старшую часть – номер сети и младшую – номер узла. Такое деление позволяет передавать сообщения между сетями только на основании номера сети, а номер узла используется только после доставки сообщения в нужную сеть.

IP-адреса версии 4 представляют собой 32-битовые идентификаторы, структура которых оптимизирована для решения основной задачи протокола IP – маршрутизации. Обычно для удобства представления IP-адресов используется их цифровое написание в виде 4-х разрядов, разделенных точками, например 192.168.123.132.

Для распознавания узлов, сетей и подсетей используется понятие «маска подсети». Для понимания, как маска подсети используется для определения адреса сети и узла необходимо представить IP-адрес в двоичном обозначении.

IP-адрес 192.168.123.132 – это (в двоичном обозначении) 32-разрядный номер 11000000010100001111011100000100. Такой номер сложно интерпретировать, поэтому лучше разбить его на четыре части по восемь двоичных знаков. Эти 8-разрядные секции называются «октеты». Тогда данный IP-адрес будет иметь вид: 11000000.10101000.01111011.10000100. Этот номер ненамного понятнее, поэтому в большинстве случаев следует преобразовывать двоичный адрес в формат разделенных точками разрядов (192.168.123.132). Десятичные числа, разделенные точками, и есть октеты, преобразованные из двоичного в десятичное обозначение.

В этом примере маской подсети является 255.255.255.0. Значение этого номера понятно, если знать, что число 255 в двоичном обозначении соответствует числу 11111111; таким образом, маской подсети является номер:

11111111.11111111.11111111.0000000

Расположив следующим образом IP-адрес и маску подсети, можно выделить составляющие сети и узла:

11000000.10101000.01111011.10000100 – IP-адрес (192.168.123.132)
11111111.11111111.11111111.00000000 – маска подсети (255.255.255.0)

Первые 24 разряда (число единиц в маске подсети) распознаются как адрес сети, а последние 8 разрядов (число оставшихся нолей в маске подсети) – адрес узла. Таким образом, получаем следующее:

11000000.10101000.01111011.00000000 – адрес сети (192.168.123.0)
00000000.00000000.00000000.10000100 – адрес узла (000.000.000.132)

или 192.168.123.0 – адрес сети. 0.0.0.132 – адрес узла.

Из данного примера с использованием маски подсети 255.255.255.0 видно, что код сети 192.168.123.0, а адрес узла 0.0.0.132. Когда пакет с конечным

адресом 192.168.123.132 доставляется в сеть 192.168.123.0 (из локальной подсети или удаленной сети), компьютер получит его из сети и обработает.

Почти все десятичные маски подсети преобразовываются в двоичные числа, представленные единицами слева и нолями справа.

Символьные и числовые адрес относятся к классу логических адресов.

В современных сетях для адресации узлов применяются, как правило, одновременно все три приведенные выше схемы. Пользователи адресуют компьютеры символьными именами, которые автоматически заменяются в сообщениях, передаваемых по сети, на числовые номера. С помощью этих числовых номеров сообщения передаются из одной сети в другую, а после доставки сообщения в сеть назначения вместо числового номера используется аппаратный адрес компьютера. Проблемой установления соответствия между адресами различных типов занимается специальная служба разрешения имен DNS (Domain network service).

Служба DNS организует имена узлов в иерархию доменов. Домен - это набор узлов, в некотором смысле связанных между собой. Все эти узлы могут принадлежать к одной сети (например, все машины, входящие в состав локальной сети университета), все они также могут принадлежать к одной организации (например, все компьютеры, принадлежащие правительству), наконец, все они могут быть просто близко расположены друг от друга в географическом смысле. Например, все учебные заведения входят в состав домена edu**,** а каждому университету или колледжу соответствует свой субдомен, в состав которого входят все его компьютеры. Например электротехническому университету соответствует домен eltech**.**edu, а радиотехническому факультету этого университета – radio.eltech.edu. Все компьютеры, входящие в состав локальной сети данного факультета, должны содержать в своем названии имя домена. Например, полное имя компьютера person1 будет person1.radio.eltech.edu. Это имя называется полным доменным именем (fully qualified domain name, FQDN*).* Оно точно идентифицирует сетевой узел в рамках всемирной сети.

Иерархическая древовидная структура допускает использование в имени произвольного количества составных частей (рис. 1.3).

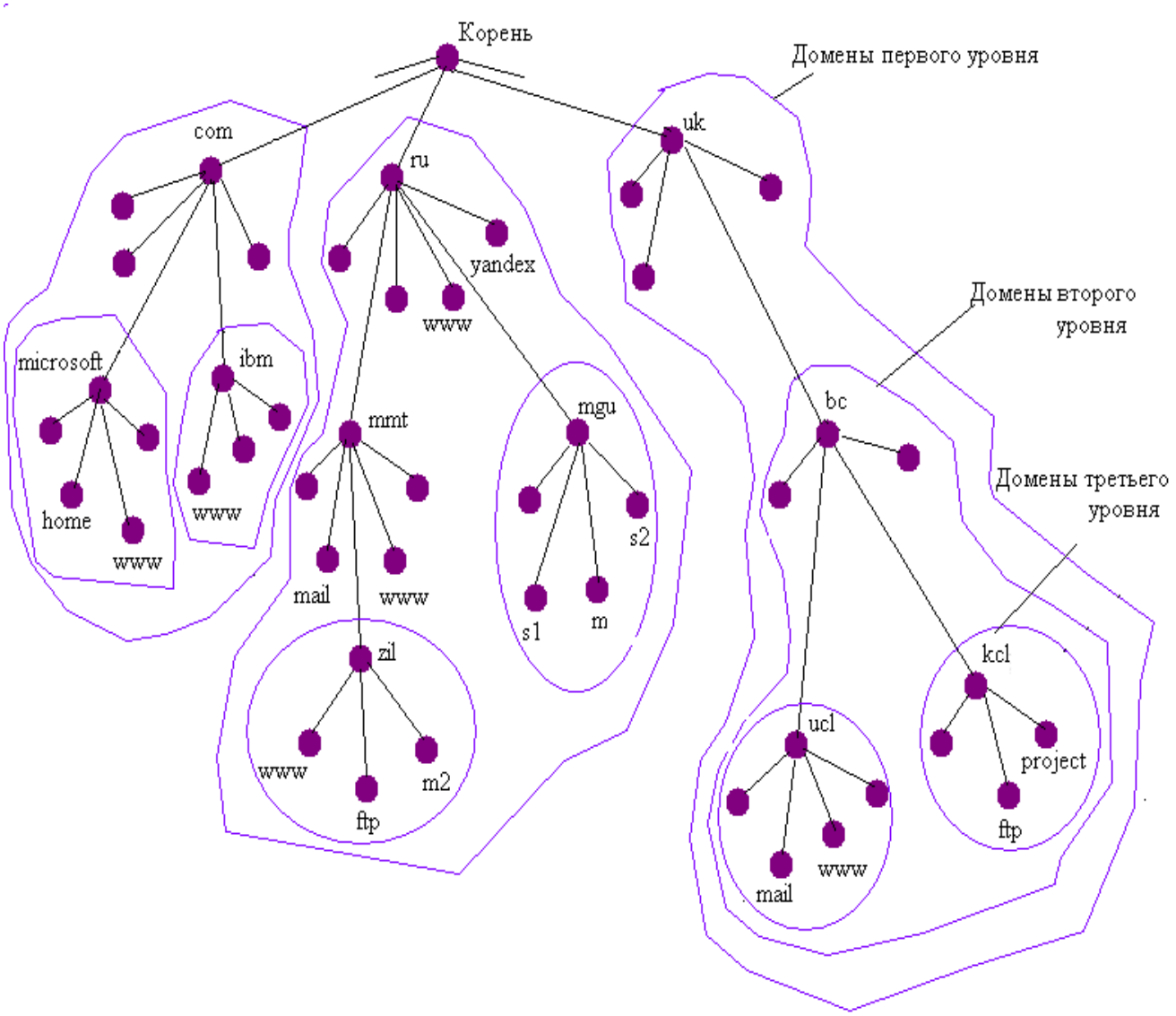


Рис. 1.3. Пространство доменных имен

Иерархия доменных имен аналогична иерархии имен файлов, принятой во многих популярных файловых системах. Дерево имен начинается с корня, обозначаемого здесь точкой (.). Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т. д. Младшая часть имени соответствует конечному узлу сети. В отличие от имен файлов, при записи которых сначала указывается самая старшая составляющая, затем составляющая более низкого уровня и т. д., запись доменного имени начинается с самой младшей составляющей, а заканчивается самой старшей. Составные части доменного имени отделяется друг от друга точкой. Например, в имени partnering.microsoft.com составляющая partnering является именем одного из компьютеров в домене Microsoft.com.

Разделение имени на части позволяет разделить административную ответственность за назначение уникальных имен между различными людьми или организациями в пределах своего уровня иерархии. Так, для примера, приведенного на рис. 3, один человек может нести ответственность за то, чтобы все имена, которые имеют окончание «ru», имели уникальную следующую вниз

по иерархии часть, то есть все имена типа www.ru, mail.mmt.ru или m2.zi1.mmt.ru будут отличаться второй по старшинству частью.

Разделение административной ответственности позволяет решить проблему образования уникальных имен без взаимных консультаций между организациями, отвечающими за имена одного уровня иерархии. Очевидно, что должна существовать одна организация, отвечающая за назначение имен верхнего уровня иерархии.

Совокупность имен, у которых несколько старших составных частей совпадают, образуют *домен* имен *(domain)*. Например, имена wwwl.zil.mmt.ru, ftp.zil.mmt.ru, yandex.ru и sl.mgu.ru входят в домен ru, так как все эти имена имеют одну общую старшую часть – имя ru. Другим примером является домен mgu.ru. Из представленных на рис. 3 имен в него входят имена sl.mgu.ru, s2.mgu.ru и m.mgu.ru. Этот домен образуют имена, у которых две старшие части всегда равны mgu.ru. Имя www.mmt.ru в домен mgu.ru не входит, так как имеет отличающуюся составляющую mmt.

Если один домен входит в другой домен как его составная часть, то такой домен могут называть поддоменом *(*subdomain*)*, хотя название домен за ним также остается. Обычно поддомен называют по имени той его старшей составляющей, которая отличает его от других поддоменов. Например, поддомен mmt.ru обычно называют поддоменом (или доменом) mmt. Имя поддомену назначает администратор вышестоящего домена. Хорошей аналогией домена является каталог файловой системы.

Если в каждом домене и поддомене обеспечивается уникальность имен следующего уровня иерархии, то и вся система имен будет состоять из уникальных имен.

По аналогии с файловой системой, в доменной системе имен различают краткие имена, относительные имена и полные доменные имена. Краткое имя – это имя конечного узла сети: хоста или порта маршрутизатора. Краткое имя - это лист дерева имен. Относительное имя – это составное имя, начинающееся с некоторого уровня иерархии, но не самого верхнего. Например, wwwi.zil - это относительное имя. *Полное доменное имя (fully qualified domain name, FQJDN)* включает составляющие всех уровней иерархии, начиная от краткого имени и кончая корневой точкой: wwwl.zil.mmt.ru.

Необходимо подчеркнуть, что компьютеры входят в домен в соответствии со своими составными именами, при этом они могут иметь совершенно различные IP-адреса, принадлежащие к различным сетям и подсетям. Например, в домен mgu.ru могут входить хосты с адресами 132.13.34.15, 201.22.100.33, 14.0.0.6. Доменная система имен реализована в сети Internet, но она может работать и как автономная система имен в крупной корпоративной сети, использующей стек TCP/IP, но не связанной с Internet.

В Internet корневой домен управляется центром InterNIC. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166.

Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, так называемые *географические домены***.**

Каждая страна (государство) имеет свой географический домен из двух букв, например:

- для России – ru
- для Австралии – au
- для Англии – uk
- для Бельгии – be и т.д.

Для различных типов организаций существуют *организационные домены*, использующие следующие обозначения**:**

- corn – коммерческие организации (например, microsoft.com);
- edu – образовательные (например, mitedu);
- gov – правительственные организации (например, nsf.gov);
- org – некоммерческие организации (например, fidonet.org);
- net – организации, поддерживающие сети (например, nsf.net).

Каждый домен администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Чтобы получить доменное имя, необходимо зарегистрироваться в какой-либо организации, которой InterNIC делегировал свои полномочия по распределению имен доменов. В России такой организацией является РосНИИРОС (Российский научно-исследовательский институт развития общественных сетей**)**, которая отвечает за делегирование имен поддоменов в домене ru.

Соответствие между доменными именами и IP-адресами может устанавливаться как средствами локального узла, так и средствами централизованной службы. На раннем этапе развития Internet на каждом узле вручную создавался текстовый файл с известным именем hosts. Этот файл состоял из некоторого количества строк, каждая из которых содержала одну пару «IP-адрес – доменное имя», например 102.54.94.97 – rhino.acme.com.

По мере роста Internet файлы hosts также росли, и создание масштабируемого решения для разрешения имен стало необходимостью.

Таким решением стала централизованная служба DNS, основанная на распределенной базе отображений «доменное имя – IP-адрес». Служба DNS использует в своей работе протокол типа «клиент-сервер». В нем определены DNS-серверы и DNS-клиенты. DNS-серверы поддерживают распределенную базу отображений, а DNS-клиенты обращаются к серверам с запросами о разрешении доменного имени в IP-адрес.

Служба DNS использует текстовые файлы почти такого формата, как и файл hosts, и эти файлы администратор также подготавливает вручную. Однако служба DNS опирается на иерархию доменов, и каждый сервер службы DNS хранит только часть имен сети, а не все имена, как это происходит при использовании файлов hosts. При росте количества узлов в сети проблема масштабирования решается созданием новых доменов и поддоменов имен и добавлением в службу DNS новых серверов.

Для каждого домена имен создается свой DNS-сервер. Этот сервер хранит только имена, которые заканчиваются на следующем ниже уровне иерархии.

(Аналогично каталогу файловой системы, который содержит записи о файлах и подкаталогах, непосредственно в него «входящих».) Именно при такой организации службы DNS нагрузка по разрешению имен распределяется более-менее равномерно между всеми DNS-серверами сети. Например, этот сервер хранит отображения только имен типа mail.mmt.ru, www.mmt.ru, а все остальные отображения должны храниться на DNS-сервере поддомена zil.

Каждый DNS-сервер кроме таблицы отображений имен содержит ссылки на DNS-серверы своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов. Для обслуживания корневого домена выделено несколько дублирующих друг друга DNS-серверов, IP-адреса которых являются широко известными (их можно узнать, например, в InterNIC).

Процедура разрешения DNS-имени во многом аналогична процедуре поиска файловой системой адреса файла по его символьному имени. Действительно, в обоих случаях составное имя отражает иерархическую структуру организации соответствующих справочников - каталогов файлов или таблиц DNS. Здесь домен и доменный DNS-сервер являются аналогом каталога файловой системы. Для доменных имен, так же как и для символьных имен файлов, характерна независимость именования от физического местоположения.

Процедура поиска адреса файла по символьному имени заключается в последовательном просмотре каталогов, начиная с корневого. При этом предварительно проверяется кэш и текущий каталог. Для определения IP-адреса по доменному имени также необходимо просмотреть все DNS-серверы, обслуживающие цепочку поддоменов, входящих в имя хоста, начиная с корневого домена. Существенным же отличием является то, что файловая система расположена на одном компьютере, а служба DNS по своей природе является распределенной.

Существуют две основные схемы разрешения DNS-имен. В первом варианте работу по поиску IP-адреса координирует DNS-клиент:

– DNS-клиент обращается к корневому DNS-серверу с указанием полного доменного имени;

– DNS-сервер отвечает, указывая адрес следующего DNS-сервера, обслуживающего домен верхнего уровня, заданный в старшей части запрошенного имени;

– DNS-клиент делает запрос следующего DNS-сервера, который отсылает его к DNS-серверу нужного поддомена, и т. д., пока не будет найден DNS-сервер, в котором хранится соответствие запрошенного имени IP-адресу. Этот сервер дает окончательный ответ клиенту.

Такая схема взаимодействия называется нерекурсивной или итеративной, когда клиент сам итеративно выполняет последовательность запросов к разным серверам имен. Так как эта схема загружает клиента достаточно сложной работой, то она применяется редко.

Во втором варианте реализуется рекурсивная процедура:

– DNS-клиент запрашивает локальный DNS-сервер, то есть тот сервер, который обслуживает поддомен, к которому принадлежит имя клиента;

– если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту; это может соответствовать случаю, когда запрошенное имя входит в тот же поддомен, что и имя клиента, а также может соответствовать случаю, когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше;

– если же локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и т. д. точно так же, как это делал клиент в первом варианте; получив ответ, он передает его клиенту, который все это время просто ждал его от своего локального DNS-сервера.

1.4 Классы сетей

IP-адреса распределены по классам. Наиболее распространены классы A, B и C. Классы D и E существуют, но обычно не используются конечными пользователями. Каждый из классов адресов имеет свою маску подсети по умолчанию.

В версии IP версии 4 (IPv4) имеется пять классов адресов, приведенных в табл. 1.1, где жирным шрифтом выделена старшая часть IP-адреса, указывающая номер сети.

Табл. 1.1

Класс	Первые биты IP-адреса	Наименьший **номер сети**	Наибольший **номер сети**	Максимальное число сетей	Максимальное число узлов в каждой сети
A	0	**0.**0.0.0	**127.**0.0.0	$2^{7}-2$	$2^{24}-2$
B	10	**128.0.**0.0	**191.255.**0.0	$2^{14}-2$	$2^{16}-2$
C	110	**192.0.0.**0	**223.255.255.**0	$2^{21}-2$	$2^{8}-2$
D	1110	**224**.0.0.0	**255.**255.255.255		
E	1111	**240**.0.0.0	**255**.255.255.255		

Большие сети используют адреса класса A, средние – класса B, маленькие – класса C.

В IPv4 существуют определенные соглашения об использовании адресов.

1) Сеть с номером 0.0.0.0 зарезервирована для использования в служебных сообщениях, а сеть с номером 127.0.0.0 используется для петлевого соединения (пересылки пакетов самим себе), поэтому общее количество сетей класса A равно 126.

2) Маршрутизация пакета в публичной сети всегда производится на основании классического IP-адреса номера сети, согласно табл. 1, поэтому адрес сети не может быть назначен ни одному узлу.

3) Адрес узла со всеми двоичными “1” предназначен для адресации всем узлам соответствующей сети (широковещательная рассылка), поэтому этот адрес не может быть назначен ни одному узлу. Совместно с пунктом 2 это означает, что число узлов в любой сети уменьшается на 2.

4) В каждом классе имеется диапазон сетевых адресов для частного использования, которые в публичных сетях отсутствуют. Они используются для построения локальных корпоративных сетей. В классе А – это сеть 10.0.0.0, в классе В – диапазоны сетей от 172.16.0.0 до 172.31.0.0, в классе С – диапазон сетей от 192.168.0.0. до 192.168.255.255.

Основное назначение адресов класса D – распространение информации по схеме «один-ко-многим» для групповой рассылки в Интернет аудио- и видеоинформации. Узел, который хочет осуществить рассылку, с помощью протокола группового обслуживания Интернет (Internet Group Management Protocol – IGMP) сообщает о создании в сети мультивещательной группы с определенным адресом. Устройства, которые хотят присоединиться к создаваемой группе, высылают свое подтверждение. Одно и то же устройство может входить в несколько групп, в одну и ту же группу могут входить устройства различных сетей.

Адреса класса Е зарезервированы для будущих применений.

Маршрутизация пакета в публичной сети всегда производится на основании классического IP-адреса номера сети, согласно табл.1. Номер сети принято обозначать с помощью маски, количество лидирующих “единиц” в маске показывает число старших разрядов, которые определяют номер сети. Запись маски производится в формате IP-адреса. Таким образом, для сети класса А стандартная маска имеет вид 255.0.0.0 (в двоичном коде 11111111.00000000.00000000.00000000), для сети класса В – 255.255.0.0 (11111111.11111111.00000000.00000000), для сети класса С – 255.255.255.0 (11111111.11111111.11111111.00000000).

Наличие только четырех классов адресов часто бывает неудобно. Например, администратору необходимо создать сеть из 8000 узлов. Сеть класса С (254 узла) слишком мала, а сеть класса В (65534) слишком велика. Эта проблема решается с помощью создания подсетей, путем переназначения части битов узла в качестве битов сети. Процесс заимствования части битов всегда начинается с крайнего левого бита.

Системный администратор, выделивший блок IP-адресов, возможно, администрирует сети, организованные не соответствующим для них образом. Например, имеется глобальная сеть с 150 узлами в трех сетях (в разных городах), соединенных маршрутизатором TCP/IP. У каждой из этих трех сетей 50 узлов. Выделяем сеть класса С 192.168.123.0. Это значит, что адреса с 192.168.123.1 по 192.168.123.254 можно использовать для этих 150 узлов.

Два адреса, которые нельзя использовать в данном примере – 192.168.123.0 и 192.168.123.255, так как двоичные адреса с составляющей узла из одних единиц и нолей недопустимы. Адрес с 0 недопустим, поскольку он используется для определения сети без указания узла. Адрес с числом 255 (в двоичном обозначении адрес узла, состоящий из одних единиц) используется для доставки сообщения на каждый узел сети. Следует просто запомнить, что первый и последний адрес в любой сети и подсети не может быть присвоен отдельному узлу.

Теперь осталось дать IP-адреса 254 узлам. Это несложно, если все 150 компьютеров являются частью одной сети. Однако в данном примере 150 компьютеров работают в трех отдельных физических сетях. Вместо запроса на большее количество адресных блоков для каждой сети сеть разбивается на подсети, что позволяет использовать один блок адресов в нескольких физических сетях.

В данном случае сеть разбивается на четыре подсети с помощью маски подсети, которая увеличивает адрес сети и уменьшает возможный диапазон адресов узлов. Другими словами, мы «одалживаем» несколько разрядов, обычно используемых для адреса узла, и используем их для составляющей сети в адресе. Маска подсети 255.255.255.192 позволяет создать четыре сети с 62 узлами в каждой. Это возможно, поскольку в двоичном обозначении 255.255.255.192 – то же самое, что и 1111111.11111111.1111111.11000000. Первые две цифры последнего октета становятся адресами сети, поэтому появляются дополнительные сети 00000000 (0), 01000000 (64), 10000000 (128) и 11000000 (192). (Некоторые администраторы применяют только две из этих подсетей, используя номер 255.255.255.192 в качестве маски подсети. Для получения дополнительной информации по этому вопросу предлагается обратиться к RFC 1878. В этих четырех сетях последние 6 двоичных цифр можно использовать в качестве адресов узлов.

Использование маски подсети 255.255.255.192 преобразует сеть 192.168.123.0 в четыре сети: 192.168.123.0, 192.168.123.64, 192.168.123.128 и 192.168.123.192. Эти четыре сети будут иметь следующие действующие адреса узлов:

192.168.123.1-62
192.168.123.65-126
192.168.123.129-190
192.168.123.193-254

Не забываем, что двоичные адреса узлов с одними только единицами и нолями недействительны, поэтому нельзя использовать адреса со следующими числами в последнем октете: 0, 63, 64, 127, 128, 191, 192 или 255.

Обратим внимание на следующие два адреса узлов: 192.168.123.71 и 192.168.123.133. Если использовать по умолчанию маску подсети класса С 255.255.255.0, оба адреса будут в сети 192.168.123.0. Однако, если использовать маску подсети 255.255.255.192, они окажутся в разных сетях: 192.168.123.71 – в сети 192.168.123.64, в то время как 192.168.123.133 – в сети 192.168.123.128.

1.5 Характеристики сети

Потенциально высокая производительность − это одно из основных свойств компьютерных сетей. Это свойство обеспечивается возможностью распараллеливания работ между несколькими компьютерами сети. Существует несколько основных характеристик производительности сети:

- время реакции;

– пропускная способность;
– задержка передачи и вариация задержки передачи.

Время реакции сети является интегральной характеристикой производительности сети с точки зрения пользователя. В общем случае время реакции определяется как интервал времени между возникновением запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос.

Очевидно, что значение этого показателя зависит от типа службы, к которой обращается пользователь, от того, какой пользователь и к какому серверу обращается, а также от текущего состояния элементов сети – загруженности сегментов, коммутаторов и маршрутизаторов, через которые проходит запрос, загруженности сервера и т. п.;

Поэтому имеет смысл использовать также и *средневзвешенную оценку времени реакции сети,* усредняя этот показатель по пользователям, серверам и времени дня (от которого в значительной степени зависит загрузка сети).

Время реакции сети обычно складывается из нескольких составляющих (рис.1.4). В общем случае в него входит время подготовки запросов на клиентском компьютере (t_1), время передачи запросов между клиентом и сервером через сегменты сети и промежуточное коммуникационное оборудование (t_2 – $t_{n\text{-}1}$), время обработки запросов на сервере (t_n), время передачи ответов от сервера клиенту $\left(t'_{n-1} - t'_2\right)$ и время обработки получаемых от сервера ответов на клиентском компьютере (t'_1).

Пропускная способность – это метрическая характеристика, которая отражает объем данных, переданных сетью или ее частью в единицу времени. Пропускная способность уже не является пользовательской характеристикой, так как она говорит о скорости выполнения внутренних операций сети – передачи пакетов данных между узлами сети через различные коммуникационные устройства. Она непосредственно характеризует качество выполнения основной функции сети – транспортировки сообщений – и поэтому чаще используется при анализе производительности сети, чем время реакции.

Пропускная способность измеряется либо в битах в секунду, либо в пакетах в секунду. Пропускная способность может быть мгновенной, максимальной и средней.

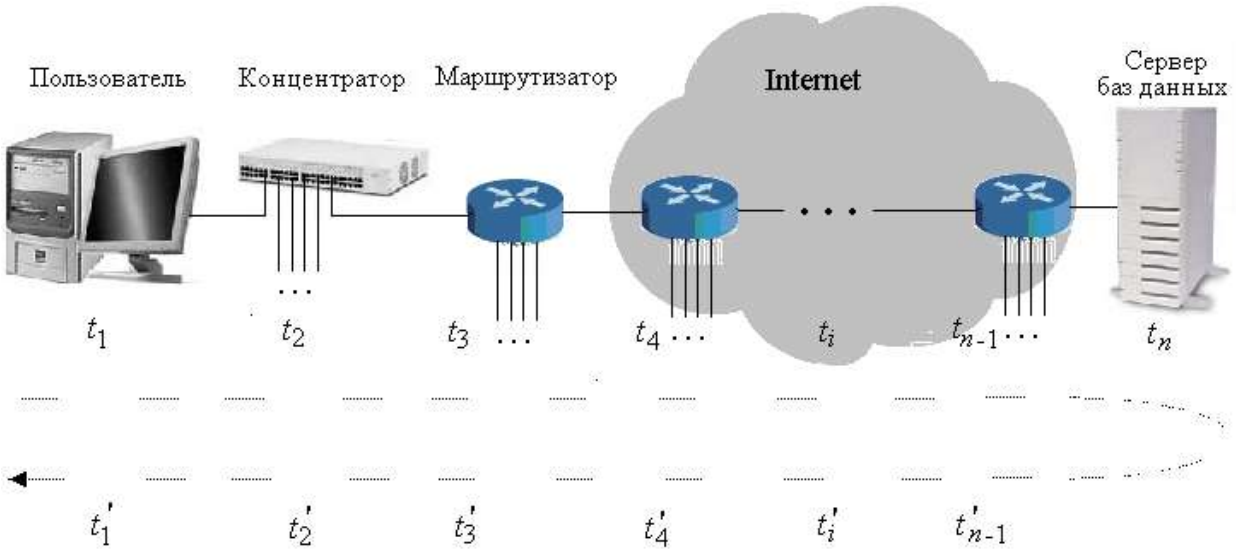


Рис. 1.4. Время реакции сети – это интегральная характеристика

Средняя пропускная способность вычисляется путем деления общего объема переданных данных на время их передачи, причем выбирается достаточно длительный промежуток времени – час, день или неделя.

Мгновенная пропускная способность отличается от средней тем, что для усреднения выбирается очень маленький промежуток времени – например, 10 мс или 1 с.

Максимальная пропускная способность – это наибольшая мгновенная пропускная способность, зафиксированная в течение периода наблюдения.

Пропускную способность можно измерять между любыми двумя узлами или точками сети, например между клиентским компьютером и сервером, между входным и выходным портами маршрутизатора. Для анализа и настройки сети очень полезно знать данные о пропускной способности отдельных элементов сети.

Из-за последовательного характера передачи пакетов различными элементами сети общая пропускная способность любого составного пути в сети будет равна минимальной из пропускных способностей составляющих элементов маршрута.

Иногда необходимо оперировать с общей пропускной способностью сети, которая определяется как среднее количество информации, переданной между всеми узлами сети в единицу времени. Этот показатель характеризует качество сети в целом, не дифференцируя его по отдельным сегментам или устройствам.

Задержка передачи определяется как задержка между моментом поступления пакета на вход какого-либо сетевого устройства или части сети и моментом появления его на выходе этого устройства. Этот параметр производительности по смыслу близок ко времени реакция сети, но отличается тем, что всегда характеризует только сетевые этапы обработки данных; без задержек обработки компьютерами сети. Например, задержку передачи запроса от пользователя к серверу баз данных на рис. 1.4 характеризуют временные составляющие от t_2 до t_{n-1} включительно.

Обычно качество сети характеризуют величинами максимальной задержки передачи и вариацией задержки. Не все типы трафика чувствительны к задержкам передачи, которые характерны для компьютерных сетей, – обычно задержки не превышают сотен миллисекунд, реже – нескольких секунд. Такого порядка задержки пакетов, порождаемых файловой службой, службой электронной почты или службой печати, мало влияют на качество этих служб с точки зрения пользователя сети. С другой стороны, такие же задержки пакетов, переносящих голосовые данные или видеоизображение, могут приводить к значительному снижению качества предоставляемой пользователю информации – возникновению эффекта «эха», невозможности разобрать некоторые слова, дрожанию изображения и т. п.

Пропускная способность и задержки передачи являются независимыми параметрами, так что сеть может обладать, например, высокой пропускной способностью, но вносить значительные задержки при передаче каждого пакета.

Надежность и безопасность.

Для оценки надежности сетей используются различные характеристики, в том числе: *коэффициент готовности,* означающий долю времени, в течение которого система может быть использована; *безопасность,* то есть способность системы защитить данные от несанкционированного доступа; отказоустойчивость – способность системы работать в условиях отказа некоторых ее элементов.

Расширяемость означает возможность сравнительно легкого добавления отдельных элементов сети (пользователей, компьютеров, приложений, сервисов), наращивания длины сегментов сети и замены существующей аппаратуры более мощной.

Масштабируемость означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этой производительность сети не ухудшается.

Прозрачность – свойство сети скрывать от пользователя детали своего внутреннего устройства, упрощая тем самым его работу в сети.

Управляемость сети подразумевает возможность централизованно контролировать состояние основных элементов сети, выявлять и разрешать проблемы, возникающие при работе сети, выполнять анализ производительности и планировать развитие сети.

Совместимость означает, что сеть способна включать в себя самое разнообразное программное и аппаратное обеспечение.

1.6 Виды сетевого трафика

Одновременная передача разнородного трафика – голоса, видео и текста – сделало актуальным вопросы обеспечения качества обслуживания (Quality of Service, QoS). Методы QoS призваны минимизировать уровень задержек для чувствительного к ним трафика, например, голосового, и одновременно гарантировать среднюю скорость для трафика данных.

Понятие качества обслуживания является сугубо статистическим. В условиях, когда пакеты передаются конечным узлам в сеть в случайные моменты времени, очереди в коммуникационных узлах также представляют собой случайные процессы, что приводит к тому, что мгновенная скорость потока данных и задержки пакетов также носят случайный характер. Поэтому все параметры, которыми измеряется качество обслуживания в сетях, являются статистическими. Как правило, это средние значения и вариации скорости информационного потока и задержек на каком-либо заранее оговоренном промежутке времени.

Качество обслуживания рассматривается с двух позиций – с точки зрения потребителя услуги (клиента) и с точи зрения поставщика услуг (провайдера). Для потребителя качество обслуживания – это некоторые желательные условия, обеспечивающие нормальную работу приложений. Для поставщика качество обслуживания – это фактические характеристики сети, наблюдаемые в результате мониторинга.

Естественной основой нормального сотрудничества клиента и провайдера является договор, который называется соглашение об уровне обслуживания (Service Level Agreement, SLA).

В SLA-соглашении должно указываться:

– какие показатели качества, и на каком уровне обещает обеспечивать провайдер;

– каким образом провайдер будет выполнять свои обещания;

– каким образом будет измеряться качество предоставляемых услуг;

– что произойдет, если провайдер не сможет обеспечить обещанное качество;

– как SLA будет меняться с течением времени.

Таким образом, каждому виду сетевого трафика требуются определенные условия, которые можно охарактеризовать следующими четырьмя основными параметрами: надежность, задержка, флуктуация и пропускная способность (табл. 1.2). Все вместе они формируют то, что называют качеством обслуживания, необходимым для предоставления услуги.

Табл. 1.2

Вид трафика	Надежность	Задержка	Флуктуации	Пропускная способность
Электронная почта	Высокая	Низкая	Слабые	Низкая
Передача файлов	Высокая	Низкая	Слабые	Средняя
Веб-доступ	Высокая	Средняя	Слабые	Средняя
Удаленный доступ	Высокая	Средняя	Средние	Низкая
Аудио по заказу	Низкая	Низкая	Сильные	Средняя
Видео по заказу	Низкая	Низкая	Сильные	Высокая
Телефония	Низкая	Высокая	Сильные	Низкая
Видеоконференции	Низкая	Высокая	Сильные	Высокая

Первые четыре вида услуг предъявляют высокие требования к надежности – некорректная доставка битов должна быть исключена. Четыре последних вида услуг толерантны к ошибкам.

Приложения, занимающиеся передачей файлов, включая электронную почту и видео, не чувствительны к задержкам. Однако интерактивные приложения – например, обеспечивающие веб-доступ или удаленный доступ – к ним более критичны. У трафика реального времени строгие требования к задержкам. С другой стороны, проигрывание видео- или аудиофайлов, хранящихся на сервере, допускает некоторое их наличие.

Неравномерная задержка доставки пакетов (флуктуации) имеет важное значение при организации удаленного доступа. Видео- и особенно аудиоданные исключительно чувствительны к флуктуациям.

Высокая пропускная способность не требуется при передаче электронной почты или при удаленном доступе, но для передачи видеоданных любых типов необходима высокая производительность сети в целом.

Охарактеризуем некоторые виды трафика с точки зрения качества обслуживания.

Цифровая речь. Этот вид трафика характеризуется низким коэффициентом пульсаций, высокой чувствительностью к задержкам передачи, отражающихся на качестве воспроизводимого непрерывного сигнала, и низкой чувствительностью к потерям информационных элементов, требует режима переноса в сессии, при котором необходимо сохранять с заданной точностью временное расположение элементов потока относительно друг друга.

Свойство сохранять с заданной точностью временное расположение элементов потока относительно друг друга в сессии принято называть изохронностью потока. Укажем два основных требования, предъявляемые трафиком к своей передаче в сеансе связи:

1) поддержание заданной величины постоянной составляющей сетевой задержки (network delay, transit delay или latency) элементов потока, определяющей реальное время их доставки;

2) обеспечение заданной величины переменной составляющей сетевой задержки или ее флуктуации (jitter), которая определяет требуемый уровень изохронности потока.

Для поддержания непрерывности передачи в реальном времени, цифрового речевого сигнала значение постоянной составляющей сетевой задержки ячеек от абонента до абонента не должно превышать величины порядка 0,3 – 0,5с. Речь традиционно трактуется как трафик от непрерывного источника, имеющий чередующиеся периоды активности и молчания. В этой связи для повышения использования пропускной способности канала связи при передаче речевой информации необходимо учитывать статистику речевых сигналов. Качество восприятия речи некритично к паузам между словами (группами слов) до 300 мс, а для 10% случаев до 1 с. Время задержки не обязательно должно быть симметричным относительно участвующих в переговорах абонентов. Однако на разборчивость речи значительное влияние

оказывает переменная составляющая случайной задержки речевого сигнала при передаче по сети связи. Например, доля речевых пакетов, задержка которых превышает на 50 мс, допустимую, не должна превышать 1% от общего количества переданных пакетов. Требуемый уровень изохронности, который может быть допущен в инфокоммуникационной сети с пакетной коммутацией, важен по двум причинам. Во-первых, в таких сетях величина переменной составляющей сетевой задержки должна быть, по крайней мере, меньше, чем величина требуемой изохронности передачи. Выбор указанного ограничения на передачу определяется тем, что, например, для передачи речи в силу психофизиологических особенностей человека она должна заканчиваться ко времени возобновления звучания в пункте назначения вновь прибывших речевых сегментов и полезно знать точность, с которой это возобновление звуковых сегментов должно происходить. Во-вторых, проектируемые пакетные инфокоммуникационные сети должны обеспечивать поддержание переменной задержки в заданных границах для различных типов изохронного трафика и эти границы должны быть известны.

Например, потеря почти половины речевых фрагментов с незначительной длительностью звучания (около 19мс) снижает разборчивость речи лишь на 20%. При этом для фрагментов с длительностью звучания до 250 мс при удовлетворительном воспроизведении речи вероятность потери не должна превышать 1%. Использование различных методов устранения избыточности речевой информации приводит к широкому диапазону возможных скоростей цифрового преобразования речи (от 1,2 до 64 кбит/с). Как правило, при уменьшении скорости передачи сложность устройств кодирования-декодирования растет, качество звучания падает, а влияние искажений и шумов на разборчивость увеличивается.

Одним из важных факторов эффективного использования пропускной способности канала является выбор оптимального алгоритма кодирования/декодирования речевой информации – кодека. Большинство кодеков, применяемых в IP – телефонии, описаны рекомендациями семейства «G» стандарта H.323.

В нормативных документах Мининформсвязи России для обеспечения приемлемого качества сообщения и минимальных задержек при кодировании/декодировании в оборудовании службы голосовых сообщений (СГС) рекомендуется применять метод адаптивной дифференциальной импульсно-кодовой модуляции (АДИКМ) со скоростью 32 кбит/с. Этот метод кодирования должен считаться основным.

Сегодня на российском рынке большинство операторов используют оборудование, соответствующее скорости передачи для одного голосового соединения для фиксированных сетей стандарта МСЭ-Т – 8 и 16 кбит/с и для мобильных стандарт ETSI GSM Full Rate, т.е. 13 кбит/с. Исходя из этих соображений, 16 кбит/с достаточно для одного голосового соединения для фиксированных и мобильных сетей.

Видеоинформация. Величина постоянной составляющей сетевой задержки ячеек для видеоинформации может варьироваться в широком

диапазоне: в то время как низкоскоростная 64Кбит/с видеоконференция может допускать величину транзитной задержки прядка 300мс, - высокоскоростная видеоконференция 1,5Мбит/с требует гарантии запаздывания не более 5мс, а для видео HDTV должна быть гарантирована величина равная 1мс. Для потока MPEG-2 указанная величина задержки не должна превышать 4мс (ограниченную 150мкс на коммутатор).

Для качественного восприятия плавности движущегося изображения, которое определяется количеством отличающихся изображений в секунду (не менее 25 кадров/с), величина переменной составляющей их сетевой задержки также должна быть, по крайней мере, меньше, чем величина требуемой изохронности передачи. В то время как мерцание зависит только от частоты перерисовки экрана на приеме и может обеспечиваться высокой скоростью сканирования изображений, находящихся в памяти приемника цифрового видео (монитора) самим приемником, например, с частотой 75 и более кадров/с (задержка появления/исчезновения видеоизображений должна заканчиваться до его угасания на сетчатке, где оно остается несколько миллисекунд. Для видеопотока MPEG-2 сеть ATM должна гарантировать величину переменной составляющей сетевой задержки не выше 500 мкс для соединений типа «точка-точка». Сеть, транспортирующая поток MPEG-2, должна гарантировать также величину доли потерянных пакетов из общего объема переданных CLR менее чем 1.7×10^{-9}. Как и речевая информация, видеоинформация также обладает довольно большой избыточностью и при ее передаче могут также применяться различные методы сжатия. Выбор стандарта сжатия определяет соответственно и качество передаваемого сигнала, а также необходимую полосу пропускания. Технология MPEG-2 при практически незаметном ухудшении качества позволяет уменьшить скорость оцифрованного несжатого видео с 270Мбит/с до 16 Мбит/с для видео студийного уровня и до 4-5 Мбит/с для видео общего пользования. Стандарт M-JPEG требует полосы 15-21 Мбит/с. Ширина полосы пропускания для передачи компьютерной анимации может варьироваться в широких пределах: от 14,4кбит/с для анимации на странице Web со сменой кадра в три секунды до потока в несколько Гбит/с.

Существуют **два основных типа видеоприложений**: интерактивное видео (например, видеоконференции) и потоковое видео (IPTV, которое может использовать как одно-, так и многоадресную рассылку). На основании проведенного анализа рекомендаций МСЭ-Т и IETF обобщим основные требования к характеристикам QoS при реализации передачи видеоданных.

Требования для трафика интерактивного видео. Для интерактивного видео (видеоконференций) к характеристикам QoS предъявляются следующие требования:

– интерактивный видеотрафик (в соответствии с «Базовыми основами QoS») должен быть промаркирован AF41;

– потери – не более 1%;

– однонаправленная задержка – не более 150 мс;

– флуктуация задержки – не более 30 мс;

– минимально-гарантированная полоса пропускания (LLQ) должна быть равна размеру сессии видеоконференции плюс 20%. Например, сессия видеоконференции в 384 кбит/с требует настройки 460 кбит/с полосы трафика гарантированного приоритета.

Так как видеоконференция включает аудиокодек G.711 для речи, то она имеет и соответствующие голосовому трафику требования к потерям, задержке и колебаниям задержки. Однако трафик видеоконференции радикально отличается от трафика голоса.

Главный секрет технологии потокового мультимедиа заключается в буферизации проигрываемых данных. Установленный на настольном компьютере программный медиаплеер осуществляет соединение с сервером и запрашивает поток. Сервер начинает передавать медиапоток, адресуя его плееру. Тот, в свою очередь, буферизует информацию за несколько секунд, используя для этого жесткий диск клиентского компьютера. При такой буферизации кратковременные задержки в потоковой передаче, вызванные перегрузками в сети, не окажут заметного влияния на качество проигрывания мультимедийной информации. И чем больше буфер, тем меньше влияние сетевых сбоев на качество передачи.

Потоковые серверы способны обеспечивать непрерывный доступ к уже готовым файлам мультимедиа. Такой режим классифицируется как предоставление аудио- или видеоданных по запросу. Информация о происходящих в данный момент событиях может быть передана и непосредственно, при помощи подключенных к компьютеру микрофона или видеокамеры, и затем в виде медиапотока транслироваться на заданную аудиторию. Этот режим передачи потока называется Web-вещанием или технологией Webcast. Наиболее часто применяемый режим потокового мультимедиа – это передача одноадресного потока. Она используется в тех случаях, когда необходимо предоставить доступ к мультимедийным данным по запросу. Потоковый медиасервер генерирует отдельный одноадресный поток для каждого клиента, запросившего доступ к необходимому ресурсу. Таким образом, любой пользователь может получить доступ к любому источнику медиаданных в произвольный момент времени. Проблемы возникают лишь тогда, когда множество пользователей одновременно запрашивают доступ к одному и тому же потоковому медиасерверу, и в этом случае общую требуемую полосу пропускания необходимо будет вычислить исходя из суммы всех потоков. То есть одноадресное вещание требует выделения определенной полосы пропускания для каждого пользователя.

Групповое вещание – альтернативный режим вещания, при котором один медиапоток обеспечивает информацией одновременно многих пользователей данной услуги. Поскольку групповое вещание требует гораздо меньшей полосы пропускания, чем адресное, оно иногда используется для прямой трансляции репортажей с места событий. Групповое потоковое вещание довольно эффективно и для предоставления множественного доступа к наиболее популярным статичным файлам мультимедиа (например, с помощью потоковой технологии можно предоставить возможность всем сотрудникам корпорации

посмотреть выступление главного директора). Организация групповой передачи требует тщательной проработки сетевого управления.

Потоковый трафик, к которому можно отнести услуги «видео и аудио по запросу», интернет-вещание, предъявляет высокие требования к потерям, флуктуации задержки и менее чувствителен к постоянной составляющей задержки.

Для потокового видео к характеристикам QoS предъявляются следующие требования:

– потоковое видео (одноадресной или многоадресной рассылки) в соответствии с «Базовыми основами QoS» должно быть промаркировано CS4;

– потери – менее 2 %;

– постоянная составляющая сетевой задержки – менее 4-5 с (в зависимости от возможности буферизации видеоприложений);

– отсутствие значительных требований к флуктуации задержки;

– требования по гарантиям полосы (CBWFO) должны зависеть от формата кодирования скорости видеопотока;

– потоковое видео обычно однонаправленное и поэтому в удаленных филиалах маршрутизаторы можно не настраивать на поддержку потокового видео в направлении от филиала к центру;

– «неважные» приложения потокового видео, такие как видео для развлечения, могут быть промаркированы DSCP CS1 и для них необходим минимум гарантий полосы пропускания в очереди CBWFO (с использованием класса Интернет/scavenger).

Приложения потокового видео менее требовательны к QoS, поскольку менее чувствительны к задержкам (может пройти несколько секунд перед началом видеокартинки) и нечувствительны к колебаниям задержки (благодаря буферизации на уровне приложений). Однако потоковое видео может содержать такую важную информацию, как электронное обучение или трансляцию корпоративных совещаний и, следовательно, требовать гарантий QoS. “Неважное” видеосодержание (подобное фильмам, музыкальным видеоклипам и др.) может рассматриваться как Интернет-сервис (сервис, который хуже “Best Effort”). Это означает, что потоки работают пока есть полоса пропускания, но вытесняются при возникновении перегрузок в сети.

Для мониторинга качества при передаче видеопотоков вводится новая метрика – QoE (Quality of Experience). Для IPTV QoE определяется в проекте рекомендации G.IPTV – QoE. Метрика QoE используется не только для IPTV, но и для, например, аудиоинформации. Метрика QoE регламентируется в рекомендации P10/G100 и в соответствии с этой рекомендацией определяется как глобальная приемлемость приложений или услуг, субъективно воспринимаемая оконечным пользователем. При этом отмечается, что экспериментальное качество включает в себя предоставляемое качество всеми элементами, участвующими в предоставлении и получении услуг из конца в конец – терминалами, сетями, инфраструктурой услуг и т.д., а также качество восприятия услуг клиентом. Кроме того, глобальная приемлемость может

зависеть от конкретно предоставляемого контента и расположения пользователя к услуге.

Асинхронный трафик, в отличие от изохронного, допускает сравнительно большие вариации постоянной задержки (определяемые прикладными применениями) и некритичен к поддержанию изохронности при передаче по каналам связи. Однако предъявляет достаточно жесткие требования к достоверности передачи (порядка 10^{-5} – 10^{-7} на бит) и к сохранности информации (вероятность засылки не по адресу порядка 10^{-6} на пакет), так как утраченные данные восстанавливаются за счет повторной передачи. Пользователям чаще всего требуется независимый темп передачи и приема данных, многорежимный обмен (интерактивный обмен данными, передача файлов), обеспечение конфиденциальности. Не допускаются вставки и/или потери отдельных элементов потока данных. Очень важным требованием во многих применениях является сохранение порядка следования данных. Интенсивность посылки пакетов асинхронного трафика в сеть и их размер могут изменяться в широких пределах, например, коэффициент пульсаций трафика (отношения максимальной мгновенной интенсивности трафика к его средней интенсивности) протоколов без установления соединений может доходить до 200, а протоколов с установлением соединений – до 20. Требования к ширине полосы пропускания асинхронного трафика лежат в широких диапазонах: от десятков кбит/с для низкоскоростных интерактивных приложений до сотен Мбит/с для приложений, ориентированных на работу с графическими данными.

В табл. 1.3 показаны допустимые значения потери пакетов для различных информационных потоков.

Табл. 1.3

Допустимые значения вероятности потери пакетов

Трафик	Формат	Допустимые значения
Речь обычного качества	МККТТ G.711. ИКМ (64 кбит/с)	$<10^{-3}$
Речь высокого качества	МККТТ G.727. Полосная АДИКМ (64 кбит/с)	$<10^{-5}$
Телевидение обычного качества	Сжатие сигналов (средняя скорость 10 Мбит/с)	$<10^{-9}$
Телевидение высокой четкости	Сжатие сигналов (средняя скорость 100 Мбит/с)	$<10^{-10}$
Передача данных	HDLC (от 64 кбит/с до 100 Мбит/с)	$<10^{-6}$

Мультимедиа. Необходимость транспортировать мультимедиа-объекты по сетям передачи данных выдвинуло целый ряд дополнительных требований к ИТС. Требования к передаче **мультимедиа-объектов** определяются комбинацией различных видов трафика, передаваемых по сети. Кроме того, при передаче мультимедийного потока для устранения смещения (skew) по времени

может потребоваться межпотоковая синхронизация изохронных потоков, так как, например, для обеспечения синхронизации речи с движением губ на приеме skew между аудио- и видеоинформацией не должно превышать 120мс. Проблема межпотоковой синхронизации является одной из составных частей проблемы обеспечения QoS-норм переноса приложений мультимедиа. При этом процедуры механизмов защиты информации, например, аутентификации и авторизации пользователей ИКС необходимо включить в интерактивные сценарии их взаимодействия с контентом Web-, видео- или аудио- приложений в процессе установления соединения, о чем речь пойдет ниже. Противоречивость требований к качеству передачи информации обуславливает необходимость создание ИКС с таким набором сетевых служб, чтобы обеспечить возможность доставки всего пакета инфоуслуг с заданным сквозным качеством QoS на базе единой сетевой инфраструктуры со специальными комбинированными процедурами обслуживания и дообслуживания очередей.

1.7 Коммуникационное оборудование

В сетях с небольшим (10-30) количеством компьютеров используется одна из типовых топологий – общая шина, кольцо, звезда или полносвязная сеть. Все они обладают свойством однородности. Однородность структуры упрощает процедуру наращивания числа компьютеров, облегчает обслуживание и эксплуатацию сети.

При построении корпоративных сетей использование типовых структур порождает различные ограничения, к ним относятся:

– ограничения на длину связи между узлами;

– ограничения на количество узлов в сети;

– ограничения на интенсивность трафика, порождаемого узлами сети.

Для снятия этих ограничений используются специальные методы структуризации сети и специальное структурообразующее оборудование — повторители, концентраторы, мосты, коммутаторы, маршрутизаторы. Оборудование такого рода называют коммуникационным, имея в виду, что с помощью него отдельные сегменты сети взаимодействуют между собой.

Под физической структуризацией понимается конфигурация связей, образованных отдельными частями кабеля, а под логической – конфигурация информационных потоков между компьютерами сети. Физическая и логическая топологии могут совпадать, а могут и не совпадать.

Физическая структуризация сети.

Простейшее из коммуникационных устройств – повторитель (repeator) – используется для физического соединения сегментов кабеля локальной сети с целью увеличения общей длины сети. Повторитель передает сигналы, приходящие из одного сегмента сети в другие ее сегменты (рис. 1.5) и позволяет преодолеть ограничения на длину линий связи за счет улучшения качества передаваемого сигнала. Повторитель восстанавливает мощность сигнала амплитуду.

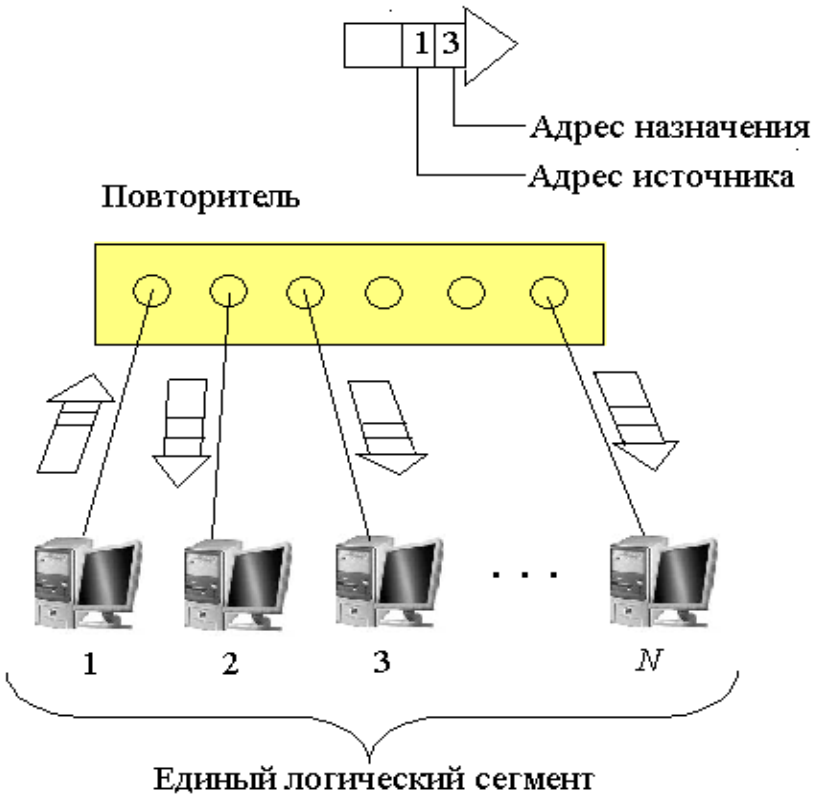


Рис. 1.5. Повторитель Ethernet синхронно повторяет биты кадра на всех своих портах

Повторитель, который имеет несколько портов и соединяет несколько физических сегментов, часто называют концентратором (concentrator) или хабом (hub). Концентратор - многопортовый повторитель.

Концентратор всегда изменяет физическую топологию сети, но при этом оставляет без изменения ее логическую топологию.

Концентраторы образуют из отдельных физических отрезков кабеля общую среду передачи данных – логический сегмент (рис. 1.6).

Поэтому сети, построенные на основе концентраторов, не могут расширяться в требуемых пределах – при определенном количестве компьютеров в сети или при появлении новых приложений всегда происходит насыщение передающей среды, и задержки в ее работе становятся недопустимыми. Эта проблема может быть решена путем логической структуризации сети с помощью мостов, коммутаторов и маршрутизаторов.

Важной проблемой, не решаемой путем физической структуризации, остается проблема перераспределения передаваемого трафика между различными физическими сегментами сети. Для повышения эффективности работы сети необходимо учитывать неоднородность информационных потоков.

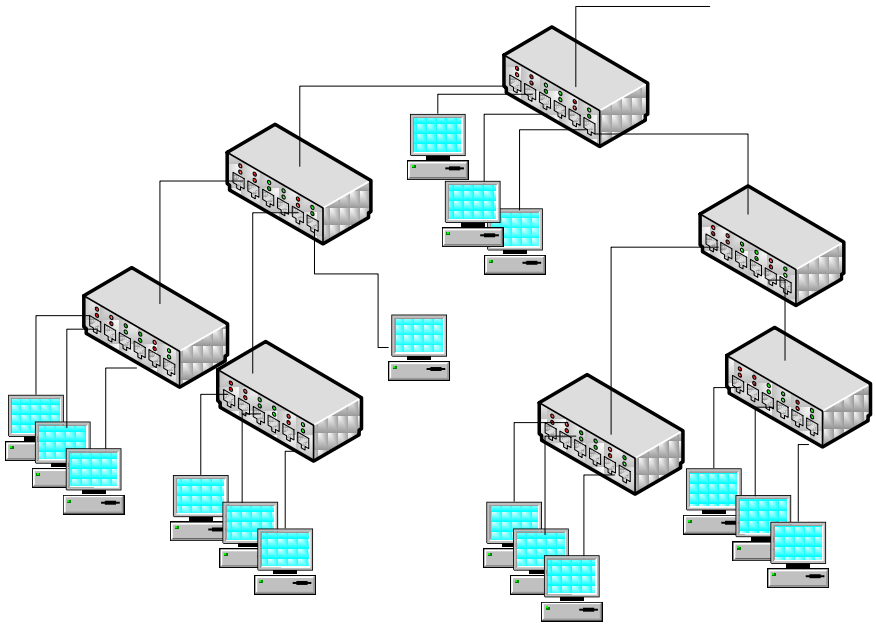


Рис. 1.6. Логический сегмент, построенный с использованием концентраторов

Логическая структуризация сети.

Крупные сети практически никогда не строятся без логической структуризации. Для отдельных сегментов и подсетей характерны типовые однородные топологии базовых технологий, и для их объединения используется оборудование, обеспечивающее локализацию трафика, мосты, коммутаторы, маршрутизаторы и шлюзы.

Распространение трафика, предназначенного для компьютеров некоторого сегмента сети, только в пределах этого сегмента, называется локализацией трафика. Логическая структуризация сети – это процесс разбиения сети на сегменты с локализованным трафиком.

Для логической структуризации сети используются такие коммуникационные устройства, как мосты, коммутаторы, маршрутизаторы и шлюзы.

Мост (bridge), а также его быстродействующий функциональный аналог - *коммутатор* (switching hub), делит общую среду передачи данных на логические сегменты. Логический сегмент образуется путем объединения нескольких физических сегментов (отрезков кабеля) с помощью одного или нескольких концентраторов. Каждый логический сегмент подключается к отдельному порту моста/коммутатора (рис. 1.7). При поступлении кадра на какой-либо из портов мост/коммутатор повторяет этот кадр, но не на всех портах, как это делает концентратор, а только на том порту, к которому подключен сегмент, содержащий компьютер-адресат.

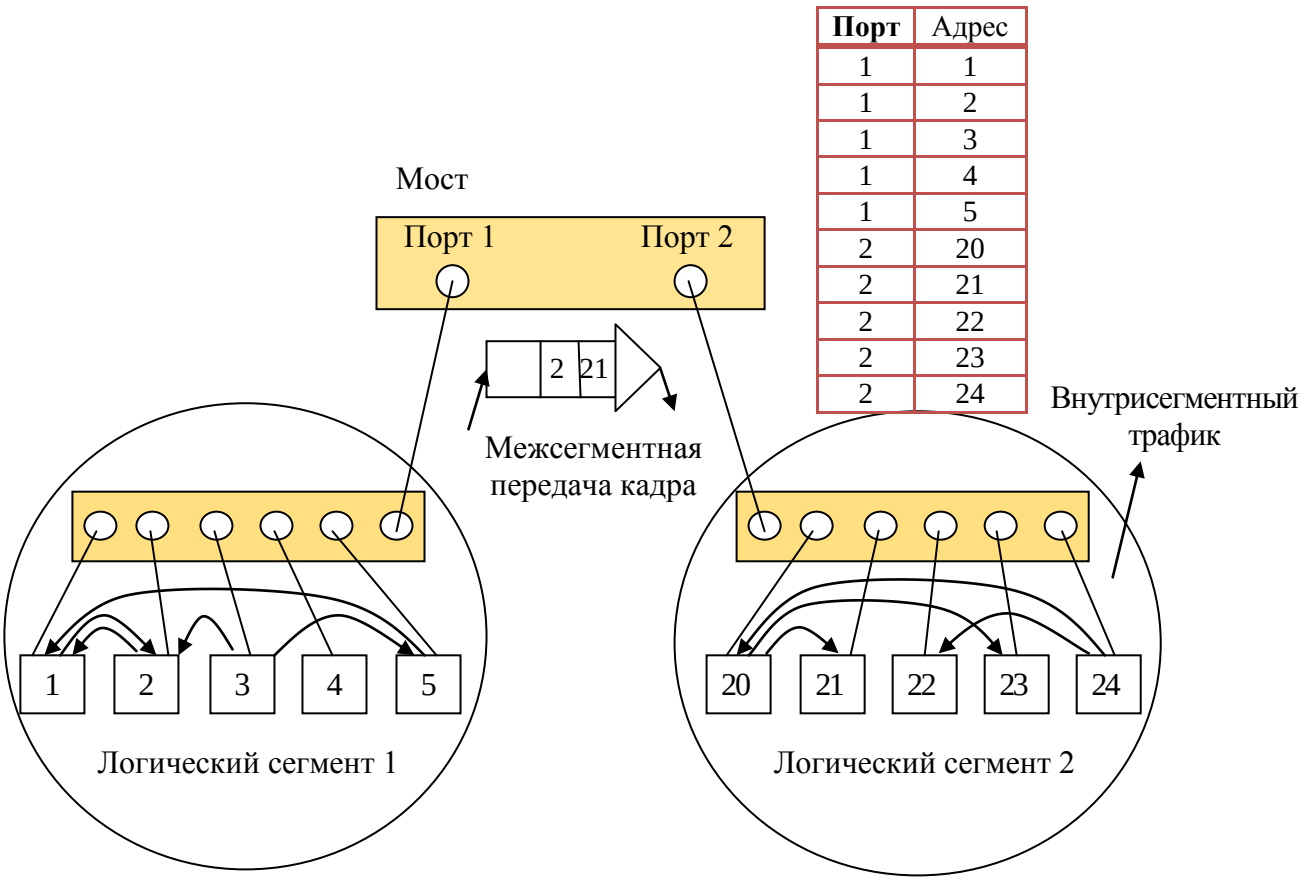


Рис. 1.7. Разделение сети на логические сегменты

Разница между мостом и коммутатором состоит в том, что мост в каждый момент времени может осуществлять передачу кадров только между одной парой портов, а коммутатор одновременно поддерживает потоки данных между всеми своими портами. Другими словами, мост передает кадры последовательно, а коммутатор параллельно.

При работе коммутатора среда передачи данных каждого логического сегмента остается общей только для тех компьютеров, которые подключены к этому сегменту непосредственно. Коммутатор осуществляет связь сред передачи данных различных логических сегментов. Он передает кадры между логическими сегментами только при необходимости, то есть только тогда, когда взаимодействующие компьютеры находятся в разных сегментах.

Существуют три архитектурных решения реализации коммутаторов, различающиеся способами комплексирования его функциональных модулей. Это коммутаторы на основе матрицы, общей шины и общей памяти.

*Коммутаторы на основе матрицы***.**

Коммутатор матричного типа обеспечивает самый быстрый способ взаимодействия входных портов с выходными. Построение таких коммутаторов осуществляется на основе двоичных коммутационных элементов с двумя входами и двумя выходами.

Детальное представление одного из возможных вариантов реализации коммутационной матрицы для 8 портов дано на рис. 1.8. Во входном порту по

адресу назначения, записанного в служебной части информационного кадра на основании просмотра адресной таблицы определяется номер выходного порта. Эта информация добавляется к байтам исходного кадра в виде специального ярлыка – тега (tag). Для данного примера тег представляет собой 3-х разрядное двоичное число, соответствующее номеру выходного порта.

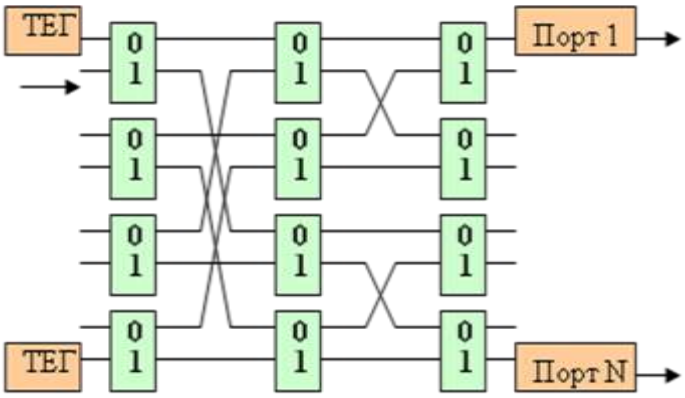
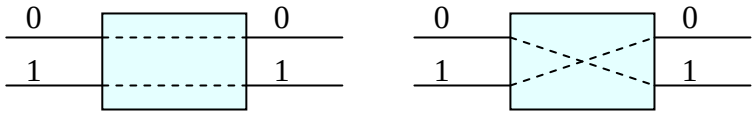


Рис. 1.8. Вариант реализации коммутационной матрицы для восьми портов

Матрица состоит из трех уровней (каскадов) двоичных переключателей – коммутационных элементов, которые соединяют свой вход с одним из двух выходов в зависимости от значения бита тега.

Коммутационный элемент может работать в одном из двух режимов: «транзит» или «кросс» (рис. 1.9).



а) б)

Рис. 1.9. Режимы работы коммутационного элемента:
а) «транзит» б) «кросс»

Переключатели первого уровня управляются первым битом тега, второго – вторым, а третьего – третьим.

Известным недостатком этой технологии является отсутствие буферизации данных внутри коммутационной матрицы – если составной канал невозможно построить из-за занятости выходного порта или промежуточного КЭ, то данные должны накапливаться в буферных запоминающих устройствах (БЗУ) порта коммутатора.

*Коммутаторы на базе общей шины***.**

Коммутаторы с общей шиной для связи входных портов с выходными применяют высокоскоростную шину, используемую в режиме разделения времени. В этой архитектуре шина (моноканал) пассивна, а активную роль выполняют специализированные процессоры портов.

Пример такой архитектуры приведен на рис. 1.10.

Кадр должен передаваться по шине небольшими частями, по несколько байт, чтобы передача кадров между несколькими портами происходила в псевдопараллельном режиме, не внося задержек в передачу кадра в целом. Размер такой ячейки данных определяется производителем коммутатора.

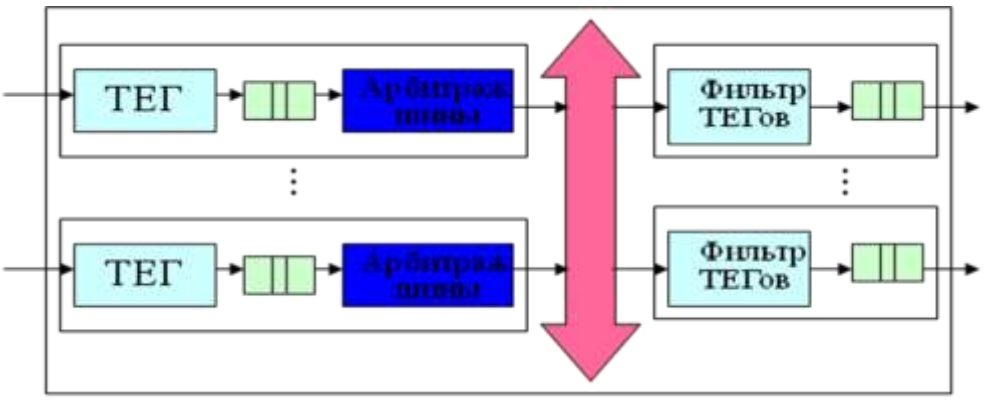


Рис. 1.10. Структура коммутатора на базе общей шины

Во входном порту формируется тег, в котором указывает номер порта назначения и добавляется к информационной ячейке, переносимой по шине. Каждый выходной порт содержит фильтр тегов, который выбирает только те теги, которые предназначенные данному порту.

Шина не может осуществлять промежуточную буферизацию, но считается, поскольку информационный кадр разбивается на небольшие ячейки, то задержек с начальным ожиданием доступности выходного порта в такой схеме не возникает.

Для того чтобы шина не была узким местом коммутатора, ее производительность должна быть в несколько раз выше скорости поступления данных на входные порты.

Коммутатор с разделяемой памятью.

В коммутационной схеме с общей разделяемой памятью входные и выходные порты коммутатора соединены между собой не через шину, а через общую память. Пример такой архитектуры приведен на рис. 1.11.

Входные порты (конкретно, специализированные процессоры этих портов) соединяются с переключаемым входом разделяемой памяти, а выходные порты соединяются с переключаемым выходом этой памяти. Переключением входа и выхода разделяемой памяти управляет менеджер очередей. Менеджер организует в разделяемой памяти несколько очередей данных, по одной для каждого выходного порта. Входные порты передают менеджеру запросы на запись данных в очередь того порта, который соответствует адресу назначения пакета. Менеджер по очереди подключает вход памяти к одному из входных портов, и тот переписывает данные в очередь определенного выходного порта. По мере заполнения очередей менеджер производит также поочередное подключение выхода разделяемой памяти к выходным портам, и данные из очереди переписываются в выходной буфер соответствующего порта.

К недостаткам коммутаторов этого типа относят ее высокую сложность и

стоимость.

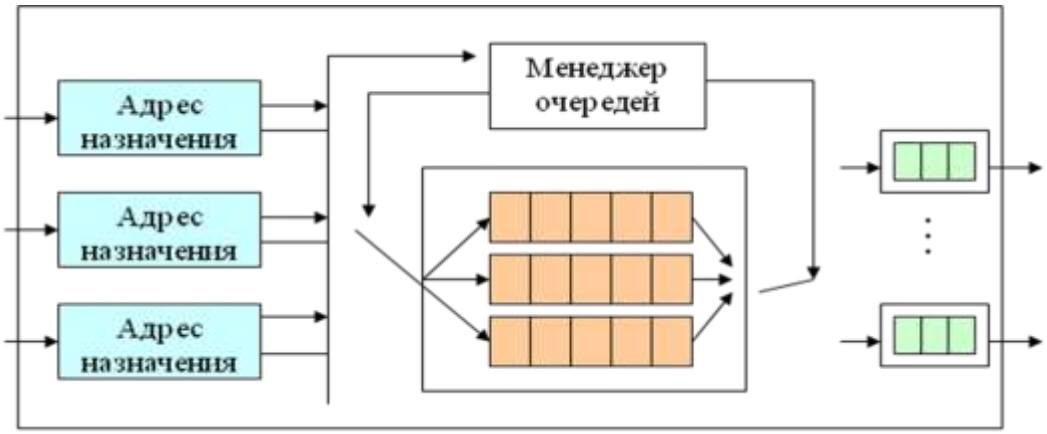


Рис. 1.11. Структура коммутатора на базе общей памяти

Маршрутизатор (*router*).

Маршрутизаторы образуют логические сегменты посредством явной адресации, поскольку используют не плоские аппаратные, а составные числовые адреса. В этих адресах имеется поле номера сети, так что все компьютеры, у которых значение этого поля одинаково, принадлежат к одному сегменту, называемому в данном случае подсетью.

Кроме локализации трафика маршрутизаторы выполняют еще много других полезных функций: они осуществляют выбор наиболее рационального маршрута из нескольких возможных.

Маршрутизатор имеет в своем распоряжении базу топологической информации о том, между какими подсетями корпоративной сети имеются связи и в каком состоянии (работоспособном или нет) они находятся. На основании такой карты сети маршрутизатор принимает решение о выборе одного из нескольких возможных маршрутов доставки пакета адресату в соответствии с таблицей маршрутов.

Таблица маршрутов в общем случае содержит следующие колонки.

– Пункт назначения (Destination) – определяет IP-адрес сети назначения.

– Маска сети (Subnet Mask) – задает количество лидирующих бит в IP-адресе, которые определяют адрес сети.

– Пункт пересылки (Next Hop) – задает IP-адрес интерфейса следующего маршрутизатора, на который следует направить поступивший пакет.

– Интерфейс (Interface) – задает собственный выходной порт, маршрутизатора, на который следует направить поступивший пакет.

– Метрика (Metric) – задает предпочтение в выборе альтернативных маршрутов. Маршруты с меньшей метрикой более предпочтительны.

Например, на рис. 1.12 для связи рабочей станций PC2 локальной вычислительной сети ЛВС1 и PC1 сети ЛВС6 через глобальные вычислительные сети (ГВС) имеется два маршрута: M1-M5-M7 и M1-M6-M7.

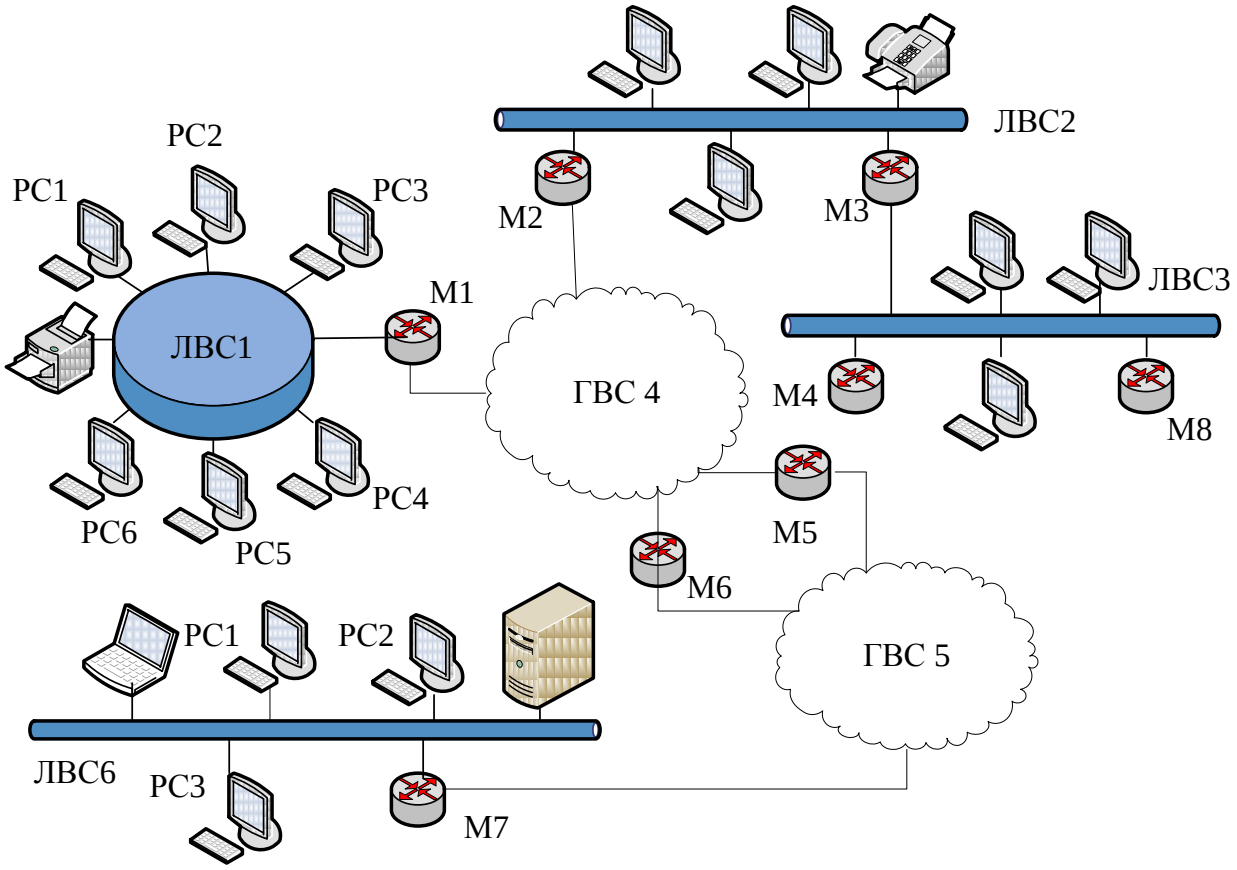


Рис. 1.12. Структура интерсети, построенной на основе маршрутизаторов

Рассмотрим пример работы маршрутизатора в качестве межсетевого узла, сопрягающего разные сети внутри корпоративной.

Пусть, например, для нашего случая администратор получил адрес сети 135.38.0.0 (адрес класса B, маска сети 255.255.0.0). В этой сети 16 битов выделено под адрес сети и 16 битов – на адрес узла. Администратору необходимо иметь 8000 узлов, на это необходимо выделить только 13 битов на адреса узлов (2^{13} = 8192), следовательно, оставшиеся 16 – 13 = 3 бита адреса узла можно переназначить как адрес сети. Тогда маска образованной подсети в двоичном коде будет иметь вид 11111111.11111111.**111**00000.00000000 или 255.255.224.0 (жирным шрифтом выделены заимствованные биты адреса узлов класса B).

В результате такого деления получим следующие адреса подсетей, приведенные в табл. 1.4.

Табл. 1.4

Номер сети	Число узлов в подсети
~~**10000111 00100110 000**00000 00000000~~ ~~**135. 38. 0.** 0~~	~~8190~~
10000111 00100110 00100000 00000000 **135. 38. 32.** 0	8190
10000111 00100110 01000000 00000000 **135. 38. 64.** 0	8190
10000111 00100110 01100000 00000000	8190

135. 38. 96. 0	
10000111 00100110 10000000 00000000 **135. 38. 128.** 0	8190
10000111 00100110 10100000 00000000 **135. 38. 160.** 0	8190
10000111 00100110 11000000 00000000 **135. 38. 192.** 0	8190
~~**10000111 00100110 111**00000 00000000~~ ~~**135. 38. 224.** 0~~	~~8190~~

Две полученные подсети 135.38.0.0 и 135.38.224.0 использовать нельзя, т.к. сетевой адрес первой подсети 135.38.0.0 совпадает с адресом исходной классической сети класса B, а адрес широковещательной рассылки внутри второй подсети 135.38.224.0 совпадает с адресом широковещательной рассылки исходной классической сети класса B. Теперь одну из оставшихся 6 подсетей (например, подсеть 135.38.32.0) администратор использует для своих нужд, а оставшиеся 5 сетей может отдать другому администратору.

Архитектура местоположения подсети 135.38.32.0 приведена на рис. 1.13.

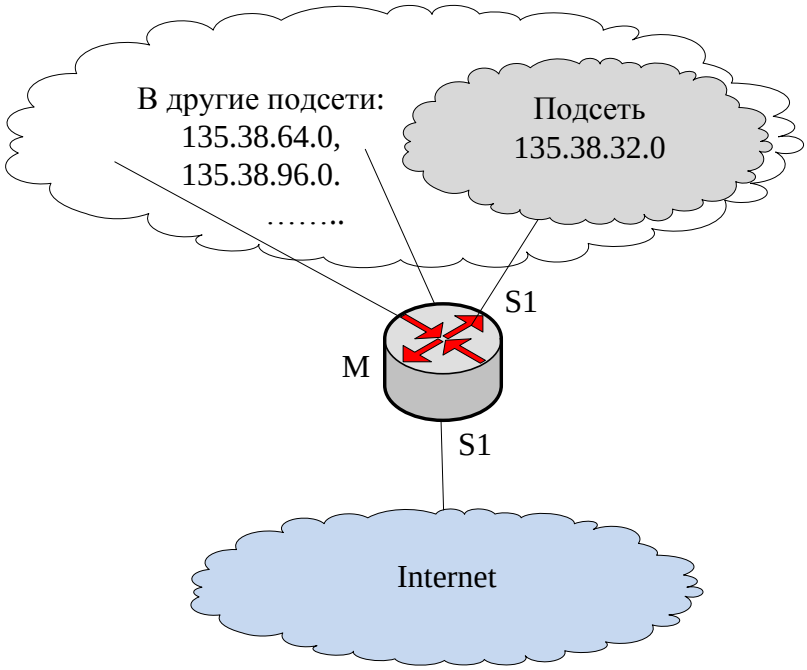


Рис. 1.13. Архитектура местоположения подсети 135.38.32.0

Для обслуживания подсети 135.38.32.0 маршрутизатор M (рис. 1.13) использует таблицу маршрутов (табл. 1.5).

Табл. 1.5

Пункт назначения (Destination)	Маска сети (Subnet Mask)	Пункт пересылки (Next Hop)	Интерфейс (Interface)	Метрика (Metric)
135.38.32.0	255.255.224.0	0.0.0.0	s1	1

Default		0.0.0.0	s2	20

Для определения дальнейшего маршрута следования поступившего пакета маршрутизатор производит следующие операции.

1) Поступивший IP-адрес в двоичном коде с помощью логической операции “И” складывается поразрядно с маской сети первой строки таблицы маршрутизации. Правило сложения разрядов с помощью логической операции “И”: 0+0=0, 0+1=0, 1+0=0, 1+1=1.

2) Полученный в результате сложения адрес сети сравнивается с IP-адресом пункта назначения первой строки. При их совпадении поступивший пакет направляется на интерфейс s1.

3) В случае несовпадения те же операции, начиная с пункта 1, проделываются с последующими строками маршрутной таблицы, если они имеются.

4) Все поступившие пакты из подсети 135.38.32.0 направляются по умолчанию на интерфейс s2.

Например, пусть из публичной сети поступили следующие пакеты с IP-адресами назначения: 135.38.16.15, 135.38.56.211, 135.38.92.10. Определим, на какие интерфейсы они будут направлены.

Для определения номера адресуемой сети складываем по “И” IP-адрес назначения первого пакета с маской сети, получаем

IP=135.38.16.15 → 10000111. 00100110. 00010000. 00001111
Mask=255.255.224.0 → 11111111. 11111111. 11100000. 00000000

Destination = 10000111. 00100110. 00000000. 00000000 $_2$→135. 38.0.0.

Такой записи в таблице маршрутизации нет, пакет уничтожается.

Для второго пакета

IP=135.38.56.211 → 10000111. 00100110. 00111000. 11010011
Mask= 255.255.224.0 → 11111111. 11111111. 11100000. 00000000

Destination = 10000111. 00100110. 00100000. 00000000 $_2$→ 135.38.32.0.

Пакет будет направлен на интерфейс s1.

Для третьего пакета

IP=135.38.92.10 → 10000111. 00100110. 01011100. 00001010
Mask=255.255.224.0 → 11111111. 11111111. 11100000. 00000000

Destination = 10000111. 00100110. 01000000. 00000000 $_2$ → 135.38.64.0.

Такой записи в таблице маршрутизации нет, пакет уничтожается.

Другой важной способностью маршрутизатора является способность связывать в единую сеть подсети, построенные с использованием разных сетевых технологий, например Ethernet и X.25.

Маршрутизаторы позволяют объединять сети с различными принципами организации в единую internet-сеть. Название интерсеть подчеркивает ту

особенность, что образованное с помощью маршрутизаторов объединение компьютеров представляет собой совокупность нескольких сетей, сохраняющих большую степень автономности, чем несколько логических сегментов одной сети. В каждой из сетей, образующих интерсеть, сохраняются присущие им принципы адресации узлов и протоколы обмена информацией. Поэтому маршрутизаторы могут объединять не только локальные сети с различной технологией, но и локальные сети с глобальными.

В результате, маршрутизатор оказывается сложным интеллектуальным устройством, построенным на базе нескольких мощных процессоров. Такой специализированный мультипроцессор работает, как правило, под управлением специализированной операционной системы.

Когда пакет прибывает на маршрутизатор/шлюз, то в порту отрезаются заголовки и концевики кадров, и остаются только поля данных, которые и передаются в общее поле памяти маршрутизатора. Далее анализируется заголовок пакета, и в соответствии с записанным в нем заданием, строится последовательный алгоритм (цепочка команд) обработки пакета протокольными процессами. В маршрутизаторе/шлюзе одновременно выполняется несколько заданий, так как протоколы могут иметь свои копии по уровням Эталонной модели взаимодействия открытых систем (ЭМВОС) и общая память разделена на секции. Это обеспечивает параллельную обработку пакетов в маршрутизаторе. Типичная архитектура маршрутизатора/шлюза приведена на рис. 1.14.

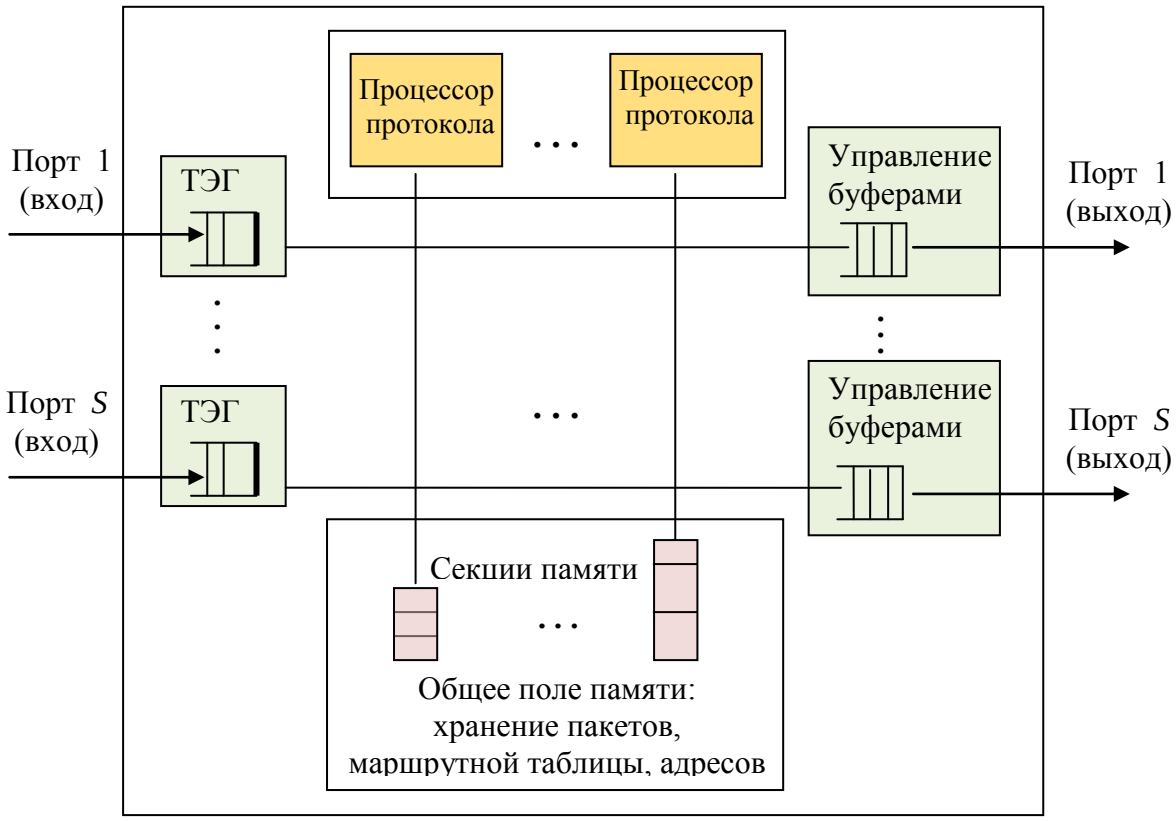


Рис. 1.14. Архитектура маршрутизатора\шлюза

Кроме перечисленных устройств отдельные части сети может соединять *шлюз* (*gateway*). Обычно основной причиной, по которой в сети используют шлюз, является необходимость объединить сети с разными типами системного и прикладного программного обеспечения. Например, шлюз e-mail может переводить электронные письма в формат SMS-сообщений для мобильных телефонов.

Выводы по первой главе

Вычислительная сеть – это совокупность компьютеров, соединенных линиями связи. Линии связи образованы кабелями, сетевыми адаптерами и другими коммуникационными устройствами. Все сетевое оборудование работает под управлением системного и прикладного программного обеспечения.

Основная цель вычислительной сети – обеспечить ее пользователям потенциальную возможность совместного использования ресурсов всех компьютеров.

В стеке протоколов TCP/IP используются три типа адресов: локальные (называемые также аппаратными), IP-адреса и символьные доменные имена. Все эти типы адресов присваиваются узлам составной сети независимо друг от друга.

IP-адрес имеет длину 4 байта и состоит из номера сети и номера узла. Для определения границы, отделяющей номер сети от номера узла, реализуются два подхода. Первый основан на понятии класса адреса, второй - на использовании масок.

Класс адреса определяется значениями нескольких первых бит адреса. В адресах класса A под номер сети отводится один байт, а остальные три байта - под номер узла, поэтому они используются в самых больших сетях. Для небольших сетей больше подходят адреса класса C, в которых номер сети занимает три байта, а для нумерации узлов может быть использован только один байт. Промежуточное положение занимают адреса класса B.

Другой способ определения, какая часть адреса является номером сети, а какая номером узла, основан на использовании маски. Маска - это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые в IP-адресе должны интерпретироваться как номер сети.

В стеке протоколов TCP/IP применяется доменная система символьных имен, которая имеет иерархическую древовидную структуру, допускающую использование в имени произвольного количества составных частей. Совокупность имен, у которых несколько старших составных частей совпадают, образуют домен имен. Доменные имена назначаются централизованно, если сеть является частью Internet, в противном случае – локально.

Соответствие между доменными именами и IP-адресами может устанавливаться как средствами локального хоста с использованием файла hosts, так и с помощью централизованной службы DNS, основанной на распределенной базе отображений «доменное имя - IP-адрес».

Для снятия ограничений на: длину связей между узлами вычислительной сети, на количество узлов в сети и на интенсивность трафика, порождаемого

узлами сети, используются специальные методы структуризации сети и специальное структурообразующее оборудование — повторители, концентраторы, мосты, коммутаторы, маршрутизаторы. С помощью этого оборудования отдельные сегменты сети взаимодействуют между собой, поэтому называется коммуникационным.

Существуют два варианта структуризации: физическая и логическая. Под физической структуризацией понимается конфигурация связей, образованных отдельными частями кабеля. Под логической структуризацией понимается конфигурация информационных потоков между компьютерами сети. Физическая структуризация реализуется с помощью повторителей и концентраторов, логическая – с помощью мостов, коммутаторов разной архитектуры, маршрутизаторов, шлюзов.

2. УГРОЗЫ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫМ СЕТЯМ И ТЕХНОЛОГИИ ЗАЩИТЫ

2.1 Жизненный цикл сетевой атаки

Вопросы сетевой безопасности и раннего обнаружения атак с каждым днем становятся все более и более насущными как для частных пользователей, корпоративных сетей так и для средних и крупных операторов связи. Сетевые атаки последнее время приобретают массовый характер. Известны случаи вывода из строя крупных всемирных порталов, банков, оборонных ведомств.

Прежде чем начать разговор о способах выявления атак, определим, что же она собой представляет. Итак, атака - это совокупность действий злоумышленника, приводящих к нарушению информационной безопасности компьютерной сети (КС). Результатом успешно реализованной атаки может стать, например, несанкционированный доступ нарушителя к информации, хранящейся в КС, потеря работоспособности системы или искажение содержимого (данных) КС. В качестве потенциальных целей могут рассматриваться серверы, рабочие станции пользователей или коммуникационное оборудование сети. В общем случае любая атака может быть разделена на четыре стадии, как показано на рис. 2.1.

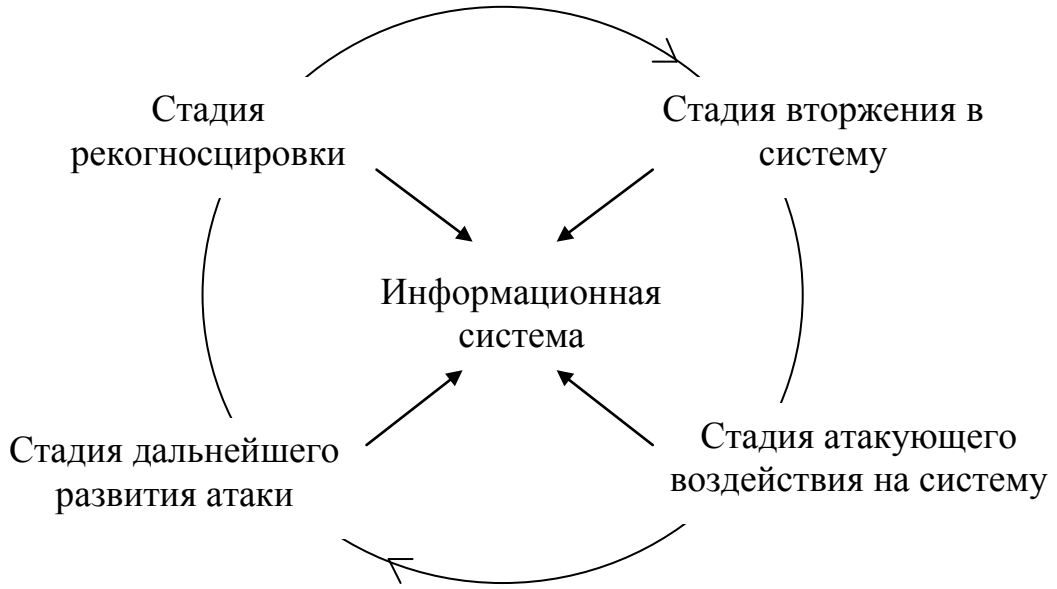


Рис. 2.1. Жизненный цикл типовой атаки

Рекогносцировка. На этом этапе нарушитель старается получить как можно больше информации об объекте атаки, чтобы на ее основе спланировать дальнейшие этапы вторжения. Примерами такой информации являются: тип и версия операционной системы, установленной на хостах компьютерной сети информационной системы, список пользователей, зарегистрированных в системе, сведения об используемом прикладном программном обеспечении (ПО) и др.

Вторжение. На этом этапе нарушитель получает несанкционированный доступ к ресурсам тех хостов, на которые совершается атака.

Атакующее воздействие. На данной стадии реализуются те цели, ради которых и предпринималась атака. Например, нарушение работоспособности ИС, кража конфиденциальной информации, хранимой в системе, удаление или модификация данных и др. При этом атакующий часто выполняет операции, направленные на удаление следов его присутствия в КС.

Развитие атаки. Когда злоумышленник стремиться расширить объекты атаки, чтобы продолжить несанкционированные действия на других составляющих КС.

Рассмотрим конкретные примеры, демонстрирующие, как могут реализовываться эти стадии. На этапе рекогносцировки действия нарушителя могут быть нацелены на получение следующих данных:

– информация о структуре и топологии компьютерной сети. Для получения данных этого типа нарушитель может воспользоваться стандартными утилитами типа «traceroute», входящими в состав практически любой операционной системы (ОС), которые позволяют сформировать список IP-адресов транзитных маршрутизаторов вплоть до хоста-объекта нападения. Информацию о структуре ИС злоумышленник может получить и путём обращения к DNS-серверу;

– информация о типе ОС. Один из наиболее распространённых методов определения типа ОС основан на том факте, что различные системы по-разному реализуют правила взаимодействия с сетевыми протоколами: при одних и тех же сетевых запросах разные ОС отправляют в ответ отличные друг от друга данные, используя которые можно с большой долей вероятности определить характеристики атакуемой ОС и даже тип аппаратной платформы;

– информация о типе прикладных сервисов. Эти знания нарушитель получить путём сканирования открытых портов и анализа заголовков ответов, полученных от этих служб;

– информация о зарегистрированных пользователях. Данные этого типа злоумышленник может извлечь из базы данных SNMP MIB, установленной на рабочих станциях и серверах компьютерной сети.

Когда необходимая информация собрана, можно начинать *вторжение.* Любое вторжение основано на наличии в компьютерной сети уязвимостей, и использование хотя бы одной из них открывает злоумышленнику вход в систему.

Примеры уязвимостей: ошибки при конфигурировании сетевых служб компьютерной сети, и ошибки в программном обеспечении, использование «слабых» и «нестойких» паролей, и отсутствие необходимых средств защиты. Результат: нарушитель получает несанкционированный доступ к ресурсам атакованного узла, что позволяет ему перейти к следующей стадии информационной атаки.

На стадии *атакующего воздействия* нарушитель выполняет те действия, которые позволяют ему осуществить цель атаки. Например, извлекает из системы управления базами данных атакованного узла сети конфиденциальную информацию.

После атакующего воздействия нарушитель может перевести атаку в фазу её *дальнейшего развития*. Для этого в систему обычно несанкционированно внедряться программа, с помощью которой можно организовать атаку на другие узлы ИС. После установки такой программы опять начинается первый этап атаки - сбор информации о следующей цели.

В основном атаки имеют распределенный массовый характер, когда на информационный узел сети осуществляется одновременное обращение с десятков тысяч (и более) зараженных компьютеров. Узел не справляется с таким количеством одновременных запросов и выходит из строя, прекращая выполнять свои основные функции. Данный вид атаки является самым популярным и именуется «Отказ в обслуживании» или DoS атакой (Denied of Service attack) . По статистике, 90% всех отказов атакуемых узлов были инициированы именно DoS-атаками.

Другим неприятным моментом DoS-атаки является огромное количество входящего сетевого трафика, который зачастую оплачивается. Что влечет большие расходы компании, подвергшейся атаки.

2.2 Классификация угроз безопасности функционирования корпоративных сетей

Общая классификация типов угроз, которым подвергается компьютерная сеть, приведена на рис. 2.2.

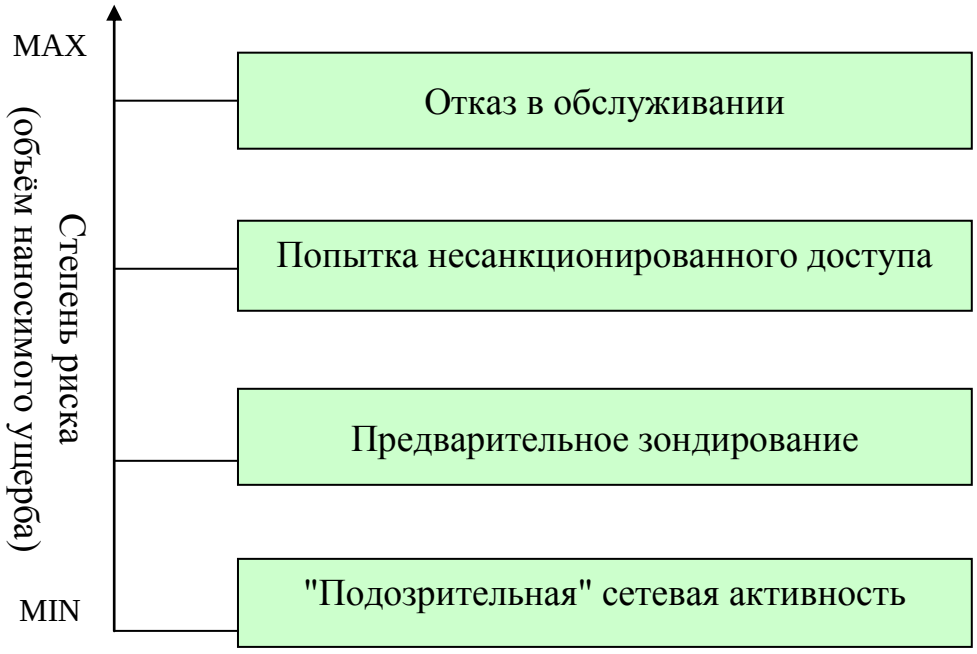


Рис. 2.2. Классификация видов угроз безопасности функционирования сетей

Классификация произведена по степени риска, то есть объему наносимого ущерба в случае успешной реализации атаки как на информацию, защищаемую в сети, так и собственно на саму сеть.

Дадим более подробную характеристику каждому классу угроз и приведем примеры наиболее представительных из них и их характерные признаки.

Класс угроз «Отказ в обслуживании».

Отказ в обслуживании – это любое действие или последовательность действий, которая приводит любую часть атакуемой системы к выходу из строя, при котором та перестает выполнять свои функции. Причиной может быть несанкционированный доступ, задержка в обслуживании и т.д. К угрозам этой группы относятся:

– *Фрагментация данных*.

При передаче пакета данных протокола IP по сети может осуществляться деление этого пакета на несколько фрагментов. Впоследствии, при достижении адресата, пакет восстанавливается из этих фрагментов. Злоумышленник может инициировать посылку большого числа фрагментов, что приводит к переполнению программных буферов на приемной стороне и, в ряде случаев, к аварийному завершению системы. Данная атака эффективна против компьютеров с операционной системой Windows. Другие варианты подобных атак используют неправильные смещения в IP-фрагментах, что приводит к некорректному выделению памяти, переполнению буферов и, в конечном итоге, к сбоям в работе систем.

Методы противодействия: для выявления таких атак необходимо осуществлять и анализировать сборку пакетов "на лету", а это существенно повышает требования к аппаратному обеспечению (производительности процессора, памяти и т.п.) средства контроля информационных потоков.

– *Ping flooding*. (от англ. *ping-flood*, дословно: наводнение пакетами) – тип атаки на сетевое оборудование, ставящий своей целью отказ в обслуживании. Ключевой особенностью (по сравнению с остальными видами флуд-атак) является возможность осуществления атаки «бытовыми средствами», такими как программы и утилиты, входящие в состав домашних/офисных версий операционных систем.

Злоумышленник посылает продолжительные серии эхо-запросов по протоколу ICMP[1]. Атакуемая система тратит свои вычислительные ресурсы, отвечая на эти запросы. Таким образом, существенно снижается производительность системы и возрастает загруженность каналов связи.

Методы противодействия: блокирования трафика с отдельных узлов и сетей, отключение ответов на ICMP-запросы, понижение приоритета обработки ICMP-

[1] ICMP (англ. *Internet Control Message Protocol* - межсетевой протокол управляющих сообщений) - сетевой протокол, входящий в стек протоколов TCP/IP, в основном используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных, например, запрашиваемая услуга недоступна, или узел или маршрутизатор не отвечают. Сетевым администраторам предоставляет средства для тестирования достижимости узлов сети: компьютер или маршрутизатор посылают по сети эхо-запрос, в котором указывают IP-адрес узла, достижимость которого нужно проверить. Успешная доставка эхо-ответа означает нормальное функционирование всей транспортной системы сети.

сообщений, отбрасывание или фильтрация ICMP-трафика средствами межсетевого экрана.

– *Атака UDP bomb* основана на передаче пакетов по протоколу UDP[2], в которых содержится неправильный формат служебных полей. Некоторые версии сетевого программного обеспечения приводят при получении подобного пакета к аварийному завершению системы.

Методы противодействия: для распознавания данной атаки необходимо анализировать форматы служебных полей.

– *SYN flooding* - одна из разновидностей сетевых атак типа «отказ в обслуживании», которая заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP[3]) в достаточно короткий срок.

При установлении соединения по протоколу TCP приемная сторона, получив запрос на соединение (пакет с флагом SYN), посылает источнику ответ (пакет с флагами SYN и ACK) о готовности установить это соединение. При этом система размещает в своей памяти служебную запись об устанавливаемом соединении и хранит ее до тех пор, пока источник не пришлет пакет-подтверждение либо не истечет время ожидания данного пакета. Злоумышленник посылает большое количество запросов на установление соединения без передачи пакетов подтверждения. Вследствие этого происходит резкое снижение производительности и при определенных обстоятельствах аварийное завершение системы.

Методы противодействия: для распознавания данной атаки необходимо анализировать загрузку канала и определять причины снижения пропускной способности.

– *Атака SMURF* - это одна из наиболее опасных атак DoS, поскольку при ее реализации на целевые узлы осуществляется усиленное воздействие. Эффект усиления возникает из-за рассылки направленных широковещательных ping-запросов на узлы сети, которые должны сгенерировать ответные сообщения.

Атака SMURF заключается в передаче в сеть широковещательных запросов от имени компьютера-жертвы. В результате компьютеры, принявшие такие широковещательные пакеты, отвечают компьютеру-жертве, что приводит к существенному снижение пропускной способности канала связи и, в ряде случаев, к полной изоляции атакуемой сети.

---

[2] UDP (User Datagram Protocol) - протокол в группе протоколов Internet, предоставляющий прикладным процессам транспортные услуги без подтверждения гарантий доставки. Обеспечивает ненадежную доставку датаграмм и не поддерживает соединений из конца в конец. Это означает, что пакеты могут быть потеряны, продублированы или прийти не в том порядке, в котором они были отправлены. К заголовку IP-пакета добавляет два поля: "порт", обеспечивающее мультиплексирование информации между разными прикладными процессами, и "контрольная сумма", позволяющее поддерживать целостность данных.

[3] **TCP (Transmission Control Protocol)** - транспортный протокол, передающий поток данных с предварительной установкой соединения, за счёт этого дающий уверенность в достоверности получаемых данных. Осуществляет повторный запрос в случае потери данных и устраняет дублирование при получении двух копий одного пакета данных. В отличие от UDP гарантирует, что приложение получит данные точно в такой же последовательности, в какой они были отправлены, и без потерь.

Методы противодействия: Для распознавания данной атаки необходимо анализировать загрузку канала и определять причины снижения пропускной способности.

– *Атака Land* - использует уязвимости реализаций стека TCP/IP в некоторых операционных системах. Она заключается в передаче на открытый порт компьютера-жертвы TCP-пакета с установленным флагом SYN, причем исходный адрес и порт такого пакета соответственно равны адресу и порту атакуемого компьютера. Это приводит к тому, что компьютер-жертва пытается установить соединение сам с собой, в результате чего сильно возрастает загрузка процессора и может произойти "зависание" или перезагрузка системы. Успешное применение такой атаки к маршрутизатору может вывести из строя всю сеть организации.

Методы противодействия: защититься от данной атаки можно, например, фильтруя пакеты между внутренней сетью и сетью Интернет по правилу, указывающему подавлять пакеты, пришедшие из сети Интернет, но с исходными адресами компьютеров внутренней сети.

– *Атака DNS flooding* - это атака, направленная на сервера имен Интернет. Она заключается в передаче большого числа DNS запросов и приводит к тому, что у пользователей нет возможности обращаться к сервису имен и, следовательно, обеспечивается невозможность работы обычных пользователей.

Методы противодействия: Для выявления данной атаки необходимо анализировать загрузку сервера DNS и выявлять источники запросов.

Класс атак «Попытка несанкционированного доступа».

Попытка несанкционированного доступа представляет собой любое действие или последовательность действий, которая приводит к попытке чтения файлов или выполнения команд в обход установленной политики безопасности. Также включает попытки злоумышленника получить привилегии, большие, чем установлены администратором системы. К этой группе угроз относятся:

– *Переполнение буферов*. Данная атака заключается в посылке на компьютер-жертву сообщения, приводящего к переполнению буфера-приемника. Переполнение буфера возможно из-за отсутствия проверки длины принимаемых данных в большинстве приложений. При переполнении буфера обычно происходит затирание части кода или других данных приложения, в связи с чем, появляется возможность исполнения собственного кода, подготовленного злоумышленником, на компьютере-жертве (возможно, в привилегированном режиме). Атака, связанная с переполнением буферов приложений и нацеленная на осуществление несанкционированного доступа, является одной из самых распространенных.

Методы противодействия: для выявления и противодействия атакам такого типа необходимо осуществлять фильтрацию протоколов прикладного уровня с учетом особенностей конкретных приложений.

– *Атака DNS spoofing* – результатом данной атаки является внесение навязываемого соответствия между IP адресом и доменным именем в кэш-памяти сервера DNS. В результате успешного проведения такой атаки все пользователи сервера DNS получат неверную информацию о доменных именах и IP адресах. Данная атака характеризуется большим количеством DNS пакетов с одним и тем же

доменным именем. Это связано с необходимостью подбора некоторых параметров DNS обмена.

Методы противодействия: для выявления такой атаки необходимо анализировать содержимое DNS трафика.

– *Атака IP spoofing* (*syslog*) – связана с подменой исходного IP адреса в сети Интернет. Действие атаки заключается в передаче на компьютер-жертву сообщения от имени другого компьютера внутренней сети. Поскольку протокол syslog используется для ведения системных журналов, путем передачи ложных сообщений на компьютер-жертву можно навязать информацию или скрыть следы несанкционированного доступа.

Методы противодействия: выявление атак, связанных с подменой IP адресов, возможно при контроле получения на одном из локальных узлов пакета с исходным адресом этого же узла или при контроле получения на внешнем узле пакетов с IP адресами внутренней сети.

Класс атак «Предварительное зондирование».

Предварительное зондирование - любое действие или последовательность действий по получению информации из или о сети (например, имена и пароли пользователей), используемые в дальнейшем для осуществления неавторизованного доступа.

– *Сканирование Half scan*.

Атака состоит в незаметном выявлении каналов информационного воздействия на систему. Злоумышленник посылает пакеты установления соединения и при получении ответов от системы сбрасывает соединение. При этом стандартные средства не фиксируют попытку установления соединения, в то время как злоумышленник определяет присутствие служб на определенных портах.

Методы противодействия: *д*ля определения сканирования необходимо фиксировать попытки установления соединения.

– *Сканирование сети посредством DNS*.

Известно, что прежде чем начинать атаку, злоумышленники осуществляют выявление целей, т.е. выявление компьютеров, которые будут жертвами атаки, а также компьютеров, которые осуществляют информационный обмен с жертвами. Одним из способов выявления целей заключается в опросе сервера имён и получение от него всей имеющейся информации о домене.

Методы противодействия: для определения такого сканирования необходимо анализировать DNS-запросы, приходящие, быть может, от разных DNS серверов, но за определенный, фиксированный промежуток времени.

– *Сканирование TCP портов*.

Сканирование портов представляет собой известный метод распознавания конфигурации компьютера и доступных сервисов. Для успешного проведения атак злоумышленникам необходимо знать, какие службы установлены на компьютере-жертве.

Методы противодействия: выявить данную атаку можно путем полного перехвата трафика TCP и анализа номеров портов. Кроме того, существуют возможности противодействия TCP сканированию. Это противодействие можно

осуществлять, например, передавая TCP пакеты от имени сканируемого компьютера на компьютер злоумышленника, таким образом, вводя его в заблуждение.

– *Сканирование UDP портов*.

Другой вид сканирования портов основывается на использовании протокола UDP и заключается в следующем: на сканируемый компьютер передаётся UDP пакет, адресованный к порту, который проверяется на предмет доступности. Если порт недоступен, то в ответ приходит сообщение о недоступности, в противном случае ответа нет. Данный вид сканирования достаточно эффективен. Он позволяет за короткое время сканировать все порты на компьютере-жертве. Кроме того, этот вид сканирования широко известен в Интернет.

Методы противодействия: противодействовать сканированию данного рода возможно путём передачи сообщений о недоступности порта на компьютер злоумышленника.

Класс атак «Подозрительная сетевая активность» представляет класс атак, характерной особенностью которых является наличие сетевого трафика, выходящего за рамки определения "стандартного" трафика. Подобная активность может указывать на подозрительные действия, осуществляемые в сети. К данной группе угроз относятся:

– *Использование маршрутизации источника*.

При пересылке пакетов IP по сети Интернет обычно используется динамическая маршрутизация, то есть решение о направлении дальнейшего продвижения каждого конкретного пакета по сети принимается каждым отдельным маршрутизатором в момент получения данного пакета исходя из алгоритма маршрутизации. Однако, существует и возможность указания в пакете конкретного маршрута, по которому должен быть послан пакет. Эта возможность может быть использована злоумышленником для обхода элементов защиты (например, межсетевого экрана) локальной сети.

Методы противодействия: Для противодействия подобной атаке необходимо запретить маршрутизацию источника внутри локальной сети.

– *Дублирующий IP-адрес*.

Каждая система в сети Интернет характеризуется своим уникальным цифровым адресом. Если обнаруживается, что одна система (имеющая другой MAC-адрес) посылает пакет с IP адресом, совпадающий с адресом другой, то значит одна из этих систем была неправильно настроена. Подобная техника может применяться атакующей стороной, для незаметной подмены работающей "доверенной" системы и осуществления атак от ее имени.

Методы противодействия: защита от данной атаки может быть реализована путем хранения для всех активных систем пары адресов (IP и MAC) и анализа адресов в заголовках пакетов, пересылаемых по локальной сети.

2.2 Методы обнаружения атак

В качестве одного из базовых средств защиты сетевых информационных ресурсов сегодня выступают системы обнаружения атак (СОА), позволяющие своевременно выявлять и блокировать атаки нарушителей.

Процесс выявления атак (рис. 2.3) начинается со сбора данных, необходимых для определения факта атаки на ресурсы сети. В частности, можно анализировать сведения о пакетах данных, поступающих из внешней сети в корпоративную сеть компании, производительность программно-аппаратных средств (вычислительную нагрузку на узлы сети, загруженность оперативной памяти, скорость работы прикладного программного обеспечения и др.), сведения о доступе к определенным файлам и т.д. Полезно также иметь полную информацию о регистрации пользователей при входе в корпоративную сеть.

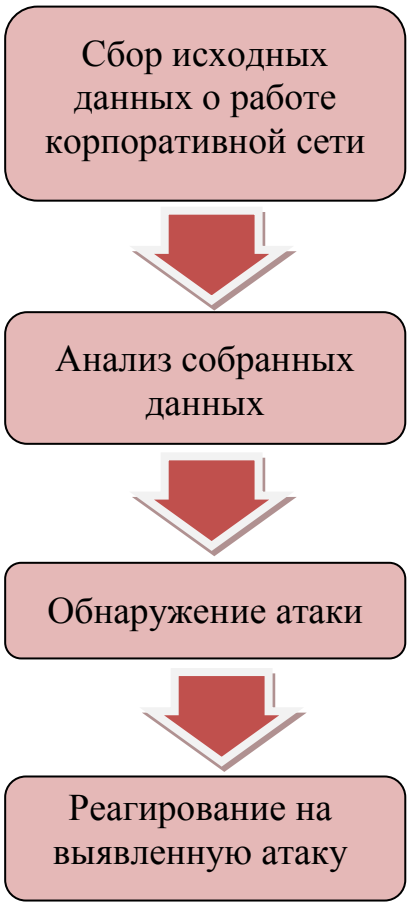


Рис. 2.3. Схема процесса обнаружения атаки

Сбор исходной информации традиционно осуществляется с помощью специализированных датчиков СОА, размещаемых на разных элементах сети. Существуют два типа таких датчиков – сетевые и узловые. Первые предназначены для сбора информации о пакетах данных, передаваемых в тех сегментах сети, где они установлены. Узловые датчики размещаются на определённые компьютеры и собирают информацию о событиях, возникающих на этих компьютерах (например, сведения о сетевом трафике, поступающем на узел или системных событиях, регистрируемых в журналах аудита операционной системы узла сети). При этом один узел может отслеживаться сразу несколькими

узловыми датчиками, каждый из которых предназначен для сбора определенной информации.

Анализ данных, собранных сетевыми и узловыми датчиками, проводиться СОА с использованием специальных методов выявления атак. Существуют две основные группы таких методов – сигнатурные и поведенческие.

Сигнатурные методы описывают каждую атаку в виде специальной модели или сигнатуры, в качестве которой могут применяться:

- строка символов,
- семантическое выражение на специальном языке,
- формальная математическая модель.

Суть сигнатурного метода в следующем: в исходных данных, собранных сетевыми и узловыми датчиками СОА выполняется процедура поиска сигнатуры атаки с использованием специализированной базы данных сигнатур атак. Преимуществом данных методов является высокая точность определения факта атаки, а очевидным недостатком – невозможность обнаружения тех атак, сигнатуры которых пока не определены.

Поведенческие методы базируются не на моделях атак, а на моделях штатного процесса функционирования (поведения) сети. Принцип работы любого из таких методов основан на обнаружении несоответствия между текущим режимом работы сети и режимом работы, соответствующим штатной модели данного метода. Любое несоответствие рассматривается как атака. Преимущество методов данного типа - возможность обнаружения новых атак без модификаций или обновлений параметров модели. К сожалению, создать точную модель штатного режима функционирования сети очень сложно.

Для того чтобы лучше понять специфику сигнатурного и поведенческого метода выявления атак рассмотрим их конкретные примеры, реализованные в современных СОА.

Сигнатурные методы выявления атак.

Среди сигнатурных методов выявления атак наиболее распространён метод контекстного поиска, который заключается в обнаружении в исходной информации определённого множества символов. Так, например, для выявления атаки на Web-сервер, направленной на получение несанкционированного доступа к файлу паролей, проводится поиск последовательности символов «GET */etc/passwd» в заголовке HTTP-запроса. Для расширения функциональных возможностей контекстного поиска в некоторых случаях используются специализированные языки, описывающие сигнатуру атаки.

Использование контекстного поиска позволяет эффективно выявлять атаки на основе анализа сетевого трафика, поскольку данный метод позволяет наиболее точно задать параметры сигнатуры, которую необходимо выявить в потоке исходных данных.

В ряде не коммерческих СОА были реализованы ещё два сигнатурных метода: анализа состояний и метод, базирующийся на экспертных системах.

Метод анализа состояний основан на формировании сигнатуры атак в виде последовательности переходов сети из одного состояния в другое. По сути,

каждый такой переход определяется по наступлению в корпоративной сети определённого события, а набор таких событий задается параметрами сигнатуры атаки. Как правило, сигнатуры атак, созданные на основе анализа состояний, описываются математическими моделями, базирующимися на теории конечных автоматов или сетей Петри. На рис. 2.4 приведена сеть Петри, описывающая сигнатуру атаки, которая выполняет подбор пароля для получения несанкционированного доступа к ресурсам корпоративной сети. Каждый переход корпоративной сети в новое состояние в модели сети Петри связан с попыткой ввода пользователем пароля. Если пользователь в течение одной минуты четыре раза подряд введёт неправильный пароль, то метод зафиксирует факт осуществления атаки.

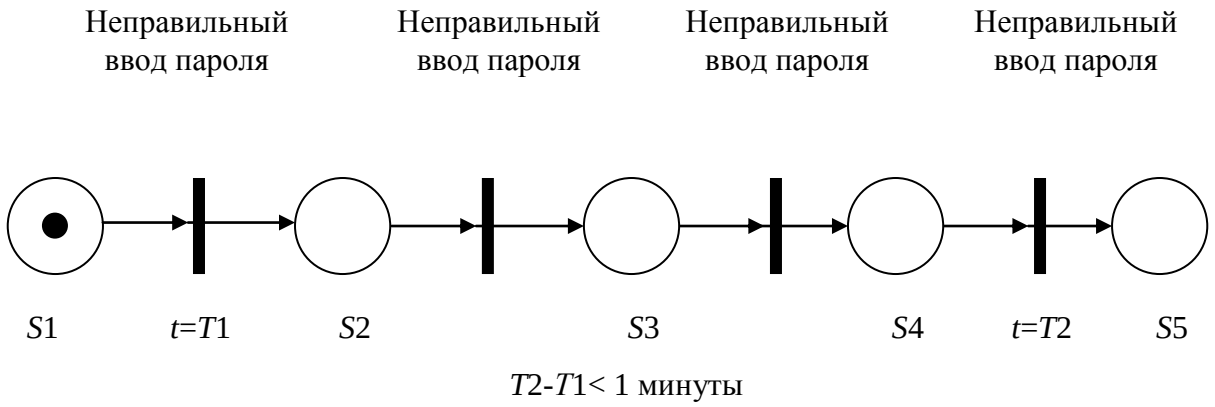


Рис. 2.4. Сеть Петри, описывающая сигнатуру атаки по подбору пароля

Методы выявления атак, базирующиеся на экспертных системах, позволяют описывать модели атак на естественном языке с высоким уровнем абстракции. Экспертная система – это система, которая в контексте обнаружения атак принимает решение о принадлежности того или иного события к классу атак на основании имеющихся правил. Эти правила (rules) основаны на опыте специалистов и хранятся в специальном хранилище, которое представляет собой базу знаний. Результирующая база знаний должна описывать характерные признаки атак, которые должна обнаруживать СОА. Исходные данные о работе корпоративной сети образуют базу данных экспертной системы и служат основанием для принятия решений о наличии атаки.

Экспертные системы нуждаются в постоянном обновлении для того, чтобы оставаться актуальными.

Этот метод продемонстрировал, что он является сравнительно эффективным, если известны точные характеристики атаки. К достоинствам данного метода можно отнести простоту реализации, скорость функционирования и отсутствие ложных тревог.

Однако сетевые атаки постоянно изменяются, поскольку злоумышленники используют индивидуальные подходы, программное обеспечение и аппаратные средства регулярно совершенствуются. Поэтому даже специальные постоянные обновления базы знаний экспертной системы не способствуют точной

идентификации всего диапазона атак. Таким образом, главными недостатками метода экспертных систем являются неспособность к обнаружению неизвестных атак и тот факт, что небольшие изменения в атаке приводят к невозможности ее обнаружения.

Одной из наиболее перспективных сигнатурных групп являются методы, основанные на биологических моделях. Для их описания могут использоваться генетические или нейросетевые алгоритмы.

На сегодняшний день все методы, базирующиеся на биологических моделях, находятся пока в стадии исследования и коммерческого применения не имеют.

Таким образом, сигнатурный подход выявления атак сводится к обнаружению злоупотреблений, которое сводится в написании атаки в виде шаблона (pattern) или сигнатуры (signature) и поиске данного шаблона в контролируемом пространстве. Типичными представителями, реализующими данную идею, являются антивирусные сканеры (работают с базой данных сигнатур вирусов) и системы обнаружения сетевых атак (работают с базой данных сигнатур удаленных атак). Система, построенная данным образом, может обнаруживать все известные атаки, но она мало приспособлена для обнаружения новых, еще неизвестных атак.

Подход, реализованный в таких СОА, очень прост и именно на нем основаны практически все предлагаемые сегодня на рынке системы обнаружения атак. Однако администраторы сталкиваются с проблемами при эксплуатации этих систем. Первая проблема заключается в создании механизма описания сигнатур, то есть языка описания атак. А вторая проблема, плавно вытекающая из первой, каким образом нужно записать атаку, чтобы зафиксировать все возможные ее модификации.

Схема типичной системы обнаружения атак с применением сигнатурного метода показана на рис. 2.5.

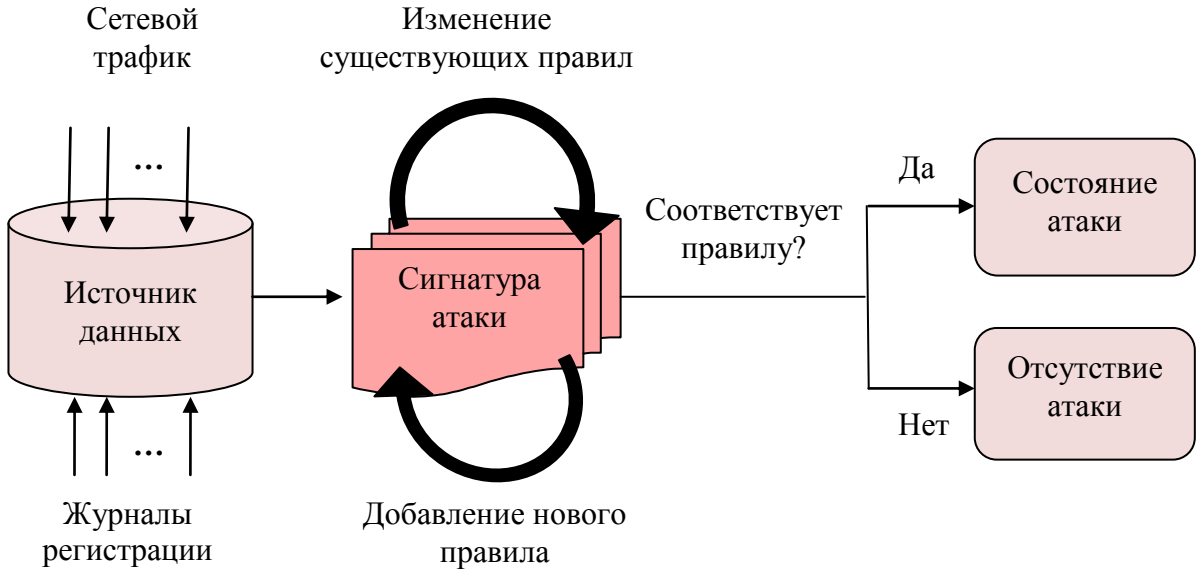


Рис. 2.5. Схема типичной системы обнаружения атак с применением сигнатурного метода

Обычно системы обнаружения атак задействуют в качестве источника данных журналы регистрации и сетевой трафик. Однако наиболее часто их применяют именно для анализа трафика.

Поведенческие методы выявления атак.

Как уже отмечалось, поведенческие методы применяются для выявления атак по отклонениям от штатной работы корпоративной сети. Среди них наиболее распространены те, которые базируются на статистических моделях. Такие модели определяют статистические показатели, характеризующие параметры штатного поведения сети. Если с течением времени наблюдается определенное изменение данных параметров от заданных значений, то фиксируется факт обнаружения атаки.

Как правило, в качестве таких параметров могут выступать: уровень загрузки процессора, нагрузка на каналы связи, штатное время работы пользователей, количество обращений к сетевым ресурсам и др. Все множество параметров, которые включаются в шаблон штатного поведения сети, могут быть отнесены к следующим распространенным группам:

– числовые параметры (количество переданных данных по различным протоколам, загрузка центрального процессора, число файлов, к которым осуществляется доступ, и т.д.);

– категориальные параметры (имена файлов, команды пользователя, открытые порты и т.д.);

– параметры активности (число обращений к файлам или соединений за единицу времени и др.).

Очень важно правильно выбрать контролируемые параметры для системы обнаружения атак. Малое их число или неправильно отобранные параметры могут привести к тому, что модель описания поведения субъектов системы будет неполной, и многие атаки останутся за пределами ее рассмотрения. С другой стороны, слишком большое число параметров мониторинга вызовет снижение производительности контролируемого узла за счет увеличенных требований к потребляемым ресурсам (оперативной и дисковой памяти, загрузке процессора и т.д.).

Примерами подобных статистических моделей могут служить пороговая модель, модель среднего значения и среднеквадратичного отклонения или ее многовариационная модель.

В пороговой модели, как явствует из названия, для каждого статистического параметра определены пороговые величины. Если наблюдаемый параметр превышает заданный порог, то вызвавшее это событие является признаком потенциальной атаки. Например, превышение заданного количества запросов на доступ к ресурсам корпоративной сети может свидетельствовать о факте обнаружения атаки «отказ в обслуживании». Или, например, статистический анализ может помочь в обнаружении необычного события, заключающегося в том, что зарегистрированный пользователь, который никогда ранее не входил в сеть в не рабочее время (например, от 6 часов вечера до 8 часов утра), вдруг подключился к системе в 2 часа ночи.

И хотя пороговая модель достаточно эффективна и надежна для некоторых типов атак, широкого распространения в настоящее время она не получили из-за

своих недостатков. Один из основных недостатков – это трудность задания порогового значения. Слишком большое пороговое значение приведет к тому, что многие атаки не будут обнаружены, а чересчур малое – обусловит большое число ложных срабатываний. Выбор этих значений – очень нетривиальная задача, которая требует глубоких знаний о работе контролируемой корпоративной сети.

Модель среднего значения и среднеквадратичного отклонения для каждого статистического параметра на основе математического ожидания и дисперсии определяет доверительный интервал, в пределах которого должен находиться данный параметр. Если текущее значение параметра выходит за его границы, то фиксируется осуществление атаки. Например, если для каждого пользователя корпоративной сети определён доверительный интервал для времени его работы в системе, то факт регистрации пользователя вне этого интервала может рассматриваться как попытка получения несанкционированного доступа к ресурсам сети;

Многовариационная модель аналогична модели среднего значения и среднеквадратичного отклонения, но позволяет одновременно учитывать корреляцию между большим количеством статистических показателей.

Поведенческий метод может быть реализован также при помощи нейронных сетей и экспертных систем. В последнем случае база правил экспертной системы описывает штатное поведение корпоративной сети. Так, при помощи экспертной системы можно точно специфицировать взаимодействие между узлами сети, которое всегда осуществляется по определенным протоколам в соответствии с действующими стандартами. Если же в процессе обмена информацией между узлами будет выявлена неизвестная команда, или нестандартное значение одного из параметров, это может служить признаком атаки.

Очевидно, что данная технология основана на очевидном выводе, что аномальное поведение субъекта (системы, программы, пользователя), то есть, как правило, атака или какое-нибудь враждебное действие, часто проявляется как отклонение от нормального поведения. Примером аномального поведения может служить большое количество соединений за короткий промежуток времени, высокая загрузка центрального процессора и коэффициент сетевой нагрузки или использование периферийных устройств, которые обычно не используются. И если описать профиль нормального поведения субъекта, то любое отклонение от него можно охарактеризовать как аномальное поведение. Однако аномальное поведение не всегда является атакой. Например, таким не является прием большого числа ответов на запрос об активности станций от системы сетевого управления. Многие системы обнаружения атак идентифицируют данный случай как атаку типа «отказ в обслуживании». С учетом этого факта можно заметить, что возможны две крайности при использовании системы обнаружения аномалий:

1) обнаружение аномального поведения, которое не является атакой, и отнесение его к классу атак (false positive);

2) пропуск атаки, которая не попадает под определение аномального повеления (false negative).

Понятно, что последний случай гораздо более опасен, чем ложное причисление аномального поведения к классу атак.

Поэтому при настройке и эксплуатации систем такой категории администраторы сталкиваются с двумя задачами:

1) построение профиля субъекта – трудно формализуемая и времяемкая задача, требующая от администратора большой предварительной работы;

2) определение граничных значений характеристик поведения субъекта для снижения вероятности появления одного из двух вышеназванных крайних случаев.

Схема типичной системы обнаружения аномального поведения представлена на рис. 2.6.

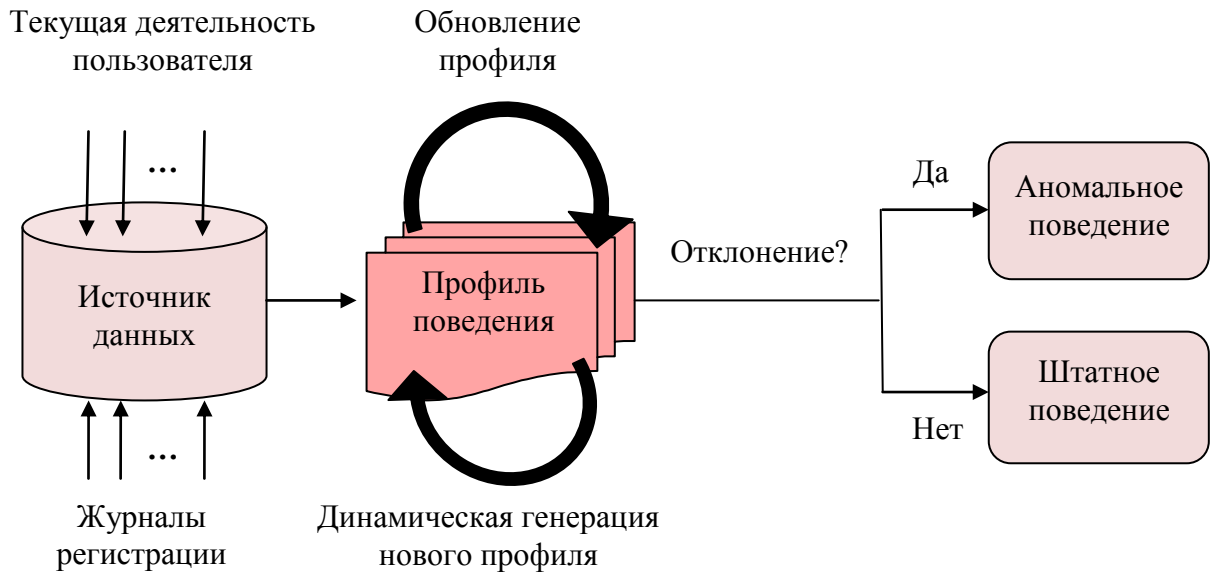


Рис. 2.6. Схема типичной системы обнаружения аномального поведения

Обычно системы обнаружения аномальной активности используют в качестве источника данных журналы регистрации и текущую деятельность пользователя.

Данный подход получает все большее развитие в современных системах обнаружения атак – все чаще этот подход используют различные производители систем обнаружения атак. Так, распределенные и обычные DoS-атаки (отказ в обслуживании) обнаруживаются именно благодаря контролю за отклонениями от обычной сетевой нагрузки.

Практические аспекты выявления атак.

Обнаружение атак должно осуществляться на различных уровнях сети (рис. 2.7). На самом нижнем уровне СОА должны быть способны выявлять атаки на конкретных узлах сети – рабочих станциях, серверах и маршрутизаторах. Следующий уровень обнаружения – сетевые сегменты, состоящие из группы узлов сети. Обнаружение атак также возможно и в более крупных объединениях элементов сети – в локальных, территориально-распределённых и глобальных системах. При этом в зависимости от инфраструктуры защищаемой сети на разных уровнях могут использоваться разные методы выявления атак.

Рассмотрим, как могут использоваться сигнатурный и поведенческий методы для обнаружения атак на различных стадиях развития.

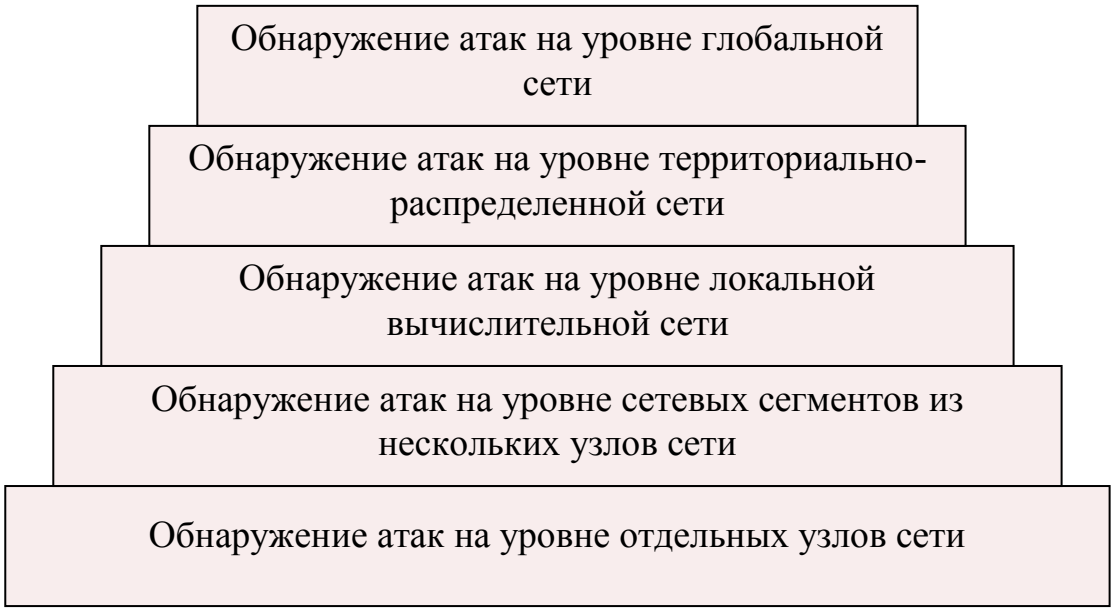


Рис. 2.7. Многоуровневая схема обнаружения атак в корпоративной сети

Следует отметить, что на стадии рекогносцировки, когда осуществляется сбор информации, эффективны лишь сигнатурные методы выявления атак. Это связано с тем, что все операции получения необходимой нарушителю информации в большинстве случаев не вызывают никакого отклонения штатного режима работы сети. Примерами признаков, характерных для этого этапа, являются: формирование запроса к DNS-серверу, получение информации из базы эталонных данных или многократные TCP-запросы на установление соединения с различными портами и т.д. На стадии рекогносцировки могут использоваться, как сетевые, так и узловые датчики.

На стадии вторжения обнаружить атаку можно при помощи и сигнатурных, и поведенческих методов. Любое вторжение характеризуется определёнными признаками, которые с одной стороны могут быть представлены в виде сигнатуры, а другой – описаны как некое отклонение от штатного поведения сети. Наиболее эффективно сочетание обоих методов, при этом для получения необходимых исходных данных применимы любые (узловые или сетевые) датчики.

Эффективное выявление атак на этапах атакующего воздействия и развития атаки возможно только при помощи поведенческих методов, поскольку действия нарушителей зависят от целей проводимой атаки и фиксированным множеством сигнатур атак однозначно не определяются. Учитывая тот факт, на двух последних стадиях жизненного цикла атаки, самыми характерными объектами являются узлы, в этом случае наиболее целесообразно применение узловых датчиков. Применение сигнатурного и поведенческого методов для обнаружения атак на различных стадиях ее существования приведено в табл. 2.1.

Табл. 2.1

Стадия атаки	Метод обнаружения	
	Сигнатурный	Поведенческий
Рекогносцировка	+ СУ	–
Вторжение	+ СУ	+ СУ
Атакующее воздействие	–	+ У
Развитие	–	+ У

Примечание: + - метод применим; – - метод неприменим; СУ - используются сетевые и узловые датчики; У - используются узловые датчики.

Обнаружение атак на ресурсы корпоративной сети является весьма сложным технологическим процессом, который связан со сбором немалых объемов информации о функционировании сети, анализом этих данных и, наконец, выявлением факта атаки. Для эффективного обнаружения атаки на всех стадиях её жизненного цикла требуется совместное применение как поведенческих, так и сигнатурных методов. Соответственно, только комплексный подход к данной проблеме позволит значительно снизить риск вторжения в информационную систему и исключит потерю конфиденциальной информации.

2.3 Программные закладки

В процессе передачи или хранения данных в сети актуальным становится вопрос защиты информационных массивов, баз данных и программных средств от различных воздействий. При этом, для защиты от несанкционированного доступа к информации во время ее передачи и хранения используются криптографические методы и, соответственно, средства (программные или аппаратные) для их реализации. Для поддержания целостности и авторизации сообщений в электронном виде применяются системы цифровой аутентификации (цифровая подпись).

Кроме того при работе этих средств защиты необходимо обеспечить потенциальное невмешательства присутствующих прикладных или системных программ в процесс обработки информации средствами защиты.

Приведем несколько примеров:

Служба безопасности одного из крупных коммерческих банков зарегистрировала действия, которые могли быть проделаны лишь при знании некоторой конфиденциальной информации, которая хранилась в виде базы данных в зашифрованном виде. Уязвимость алгоритма шифрования не была доказана, утери паролей для шифрования выявлено не было. Изучение компьютеров выявило наличие в загрузочных секторах ПЭВМ своеобразных вирусов – программ, которые сохраняли вводимую с клавиатуры информацию (в том числе и пароли для шифрования) в несколько зарезервированных для этого секторов.

Другой пример: одно из малых предприятий, занятое посреднической

деятельностью, и, как следствие, обладающее конфиденциальной информацией о предметах возможных сделок, также использовало шифрование как средство защиты своих интересов. В данном случае использовался стандарт ГОСТ 28147-89. Для шифрования использовалась плата Krypton-3, реализующая данный алгоритм шифрования, который, как известно, обеспечивает гарантированную защиту информации. Через некоторое время выяснилось, что шифруемая информация становится известной третьей стороне. А еще через некоторое время была выявлена внедренная в систему закладка, подменившая собой плату шифрования. При этом алгоритм ГОСТ был заменен другим, крайне простым и легко читаемым без ключа.

Третий пример: спор противников и сторонников программы Pretty Good Privacy (PGP) был завершен написанием закладки, подделывающей электронную подпись под файлами, выполненную данной программой.

Во всех трех случаях программа никак не проявляла себя внешне, однако, сохраняла весь ввод с клавиатуры в скрытом файле. В дальнейшем злоумышленникам требовалось лишь считать файл или просмотреть сектора, чтобы узнать пароли и по ним расшифровать интересовавшие их данные.

Такие программы большинство специалистов сразу назвали закладкой – по аналогии с незаметно внедряемыми в помещения миниатюрными электронными системами звукового подслушивания или телевизионного наблюдения.

Программная закладка – это компьютерная программа, которая обладает хотя бы одним из трех перечисленных ниже свойств:

– вносит произвольные искажения в коды других программ, находящихся в оперативной памяти компьютера (программная закладка первого типа);

– переносит фрагменты информации из одних областей оперативной или внешней памяти компьютера в другие (программная закладка второго типа);

– произвольно искажает выводимую на внешние компьютерные устройства или в канал связи информацию, полученную в результате работы других программ (программная закладка третьего типа).

Программные закладки можно также классифицировать по методу их внедрения в компьютерную систему:

– программно-аппаратные закладки, ассоциированные с аппаратной средой компьютера (как правило, аппаратной средой является BIOS – набор программ, записанных в виде машинного кода в постоянном запоминающем устройстве);

– загрузочные закладки, ассоциированные с программами первичной загрузки, которые располагаются в загрузочных секторах (загрузочными называются несколько секторов диска, из которых в процессе выполнения начальной загрузки компьютер считывает программу, берущую на себя управление этим компьютером с целью последующей загрузки операционной системы);

– драйверные закладки, ассоциированные с драйверами (компьютерными файлами, в которых содержится информация, необходимая операционной системе для управления подключенными к компьютеру периферийными устройствами);

– прикладные закладки, ассоциированные с прикладным программным обеспечением общего назначения (текстовые редакторы, утилиты, антивирусные мониторы и программные оболочки);

– исполняемые закладки, ассоциированные с исполняемыми программными модулями, содержащими код этой закладки (чаще всего эти модули представляют собой пакетные файлы, которые состоят из команд операционной системы, выполняемые друг за другом, как если бы их набирали с клавиатуры компьютера);

– закладки-имитаторы, интерфейс которых совпадает с интерфейсом некоторых служебных программ, требующих ввода конфиденциальной информации (паролей, криптографических ключей, номеров кредитных карточек);

– замаскированные закладки, которые маскируются под программные средства оптимизации работы компьютера (файловые архиваторы, дисковые дефрагментаторы) или под программы игрового и развлекательного назначения.

При рассмотрении программной закладки и ее свойств возникают некоторые аналогии с программным вирусом. Однако некоторое существенное отличие между этими понятиями существует.

Компьютерный вирус – программа, которая может включать в другие программы свою, иногда модифицированную копию, способную к дальнейшему размножению и выполнению вредных воздействий. Вирус может присоединиться к исполняемому файлу, соответствующим образом изменив его, может уничтожить некоторые файлы или встроиться в цепочку драйверов. Основная цель компьютерных вирусов – дестабилизация работы, уничтожение программ или наборов данных, то есть нанесение максимального ущерба вычислительной системе. Действие компьютерных вирусов не является направленным – воздействию подвергаются все программные объекты, предусмотренные алгоритмом работы вируса вне зависимости от содержащейся в них информации. Как правило, компьютерные вирусы попадают в вычислительную систему в процессе ее эксплуатации вместе с получаемыми из различных источников (внешние носители, компьютерные сети) программами или данными.

Программная закладка – это программа или фрагмент программы, скрытно внедряемый в защищенную систему и позволяющий лицу или процессу, внедрившему его, осуществлять в дальнейшем несанкционированные действия к тем или иным ресурсам защищенной системы. Основной целью программных закладок может быть получение или создание условий для получения информации о паролях, кодовых комбинациях, обрабатываемых данных и передача собранных сведений заданному адресу по сети, электронной почте и т.д. или просто копирование в другие, легко доступные области памяти. Закладка отличается направленным воздействием на программные объекты, содержащие интересующую информацию. Программные закладки могут попадать в вычислительную систему как на этапе ее разработки, так и в процессе ее эксплуатации. Особенностью закладок является то, что они фактически становятся неотделимы от прикладных или системных программ, если внедрены в них на стадии разработки путем обратного

проектирования (путем дисассемблирования прикладной программы, внедрения кода закладки и последующей компиляции).

Объединяет вирусы и программные закладки только то, что и вирус, и закладка должны скрывать свое присутствие в операционной среде компьютерной системы.

Для того чтобы программная закладка могла произвести какие-либо действия по отношению к другим программам или данным, процессор должен приступить к исполнению команд, входящих в состав кода программной закладки. Это возможно только при одновременном выполнении двух следующих условий:

– программная закладка должна попасть в оперативную память компьютера;

– исполнение кода закладки, находящейся в оперативной памяти, начинается при выполнении ряда условий, которые называются активизирующими.

Это достигается путем анализа и обработки закладкой прерываний, таких как:

– прерывания от таймера;

– прерывания от внешних устройств;

– прерывания от клавиатуры;

– прерывания при работе с диском;

– прерывания операционной среды, (в том числе прерывания при работе с файлами и запуск исполняемых модулей).

В противном случае активизации кода закладки не произойдет, и она не сможет оказать какого-либо воздействия на работу компьютера.

Кроме того, возможен случай, когда при запуске программы (в этом случае активизирующим событием является запуск программы) закладка разрушает некоторую часть кода программы, уже загруженной в оперативную память, и, возможно, систему контроля целостности кода или контроля иных событий и на этом заканчивает свою работу.

Таким образом, можно выделить закладки:

– Резидентного типа – которые находятся в памяти постоянно с некоторого момента времени до окончания сеанса работы персонального компьютера (выключения питания или перезагрузки). Они начинают работу при загрузке операционной среды или запуске некоторой программы (которая по традиции называется вирусоносителем), а также запущена отдельно.

– Нерезидентного типа – которые начинают работу по аналогичному событию, но заканчивают ее самостоятельно по истечении некоторого промежутка времени или некоторому событию, при этом выгружая себя из памяти целиком.

Существуют три основные группы деструктивных действий, которые могут осуществляться программными закладками:

– копирование информации пользователя компьютерной системы (паролей, криптографических ключей, кодов доступа, конфиденциальных электронных документов) в ее оперативной или внешней памяти либо в памяти другой компьютерной системы, подключенной к ней посредством локальной или глобальной компьютерной сети;

– изменение алгоритмов функционирования системных, прикладных и служебных программ (например, введение изменений в программу разграничения доступа может привести к тому, что она разрешит вход в компьютерную систему всем без исключения пользователям вне зависимости от правильности введенного пароля);

– навязывание определенных режимов работы (например, блокирование записи на диск при стирании информации, причем она, естественно, не уничтожается и может быть впоследствии скопирована злоумышленником).

У всех без исключения программных закладок, независимо от метода их внедрения в компьютерную систему, срока пребывания в оперативной памяти и выполняемых действий, есть одна важная общая черта: в программных закладках обязательно присутствует операция записи в оперативную или внешнюю память компьютерной системы. Без этой операции никакое негативное влияние программной закладки на компьютерную систему невозможно. Ясно, что для целенаправленного воздействия программная закладка должна выполнять также операцию чтения, иначе в ней может быть реализована только функция разрушения (например, стирание или замена информации в определенных секторах жесткого диска).

Жизненный цикл программной закладки выглядит следующим образом (рис. 2.8):

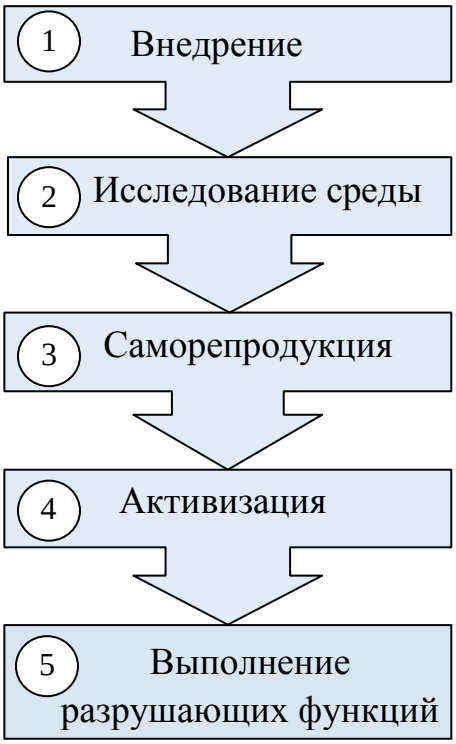


Рис. 2.8. Этапы жизненного цикла программной закладки

Обобщенно функционирование уже внедренной программной закладки можно представить в виде схемы, приведенной на рис. 2.9.

Структурно программную закладку (ПЗ) можно представить в виде четырех функциональных блоков: исследования, активизации, проявления деструктивных действий (разрушения) и маскировки. В маскировку может входить и защита от

исследования закладки – противодействие обнаружению программной закладки. Наличие блоков исследования и маскировки не является обязательным.

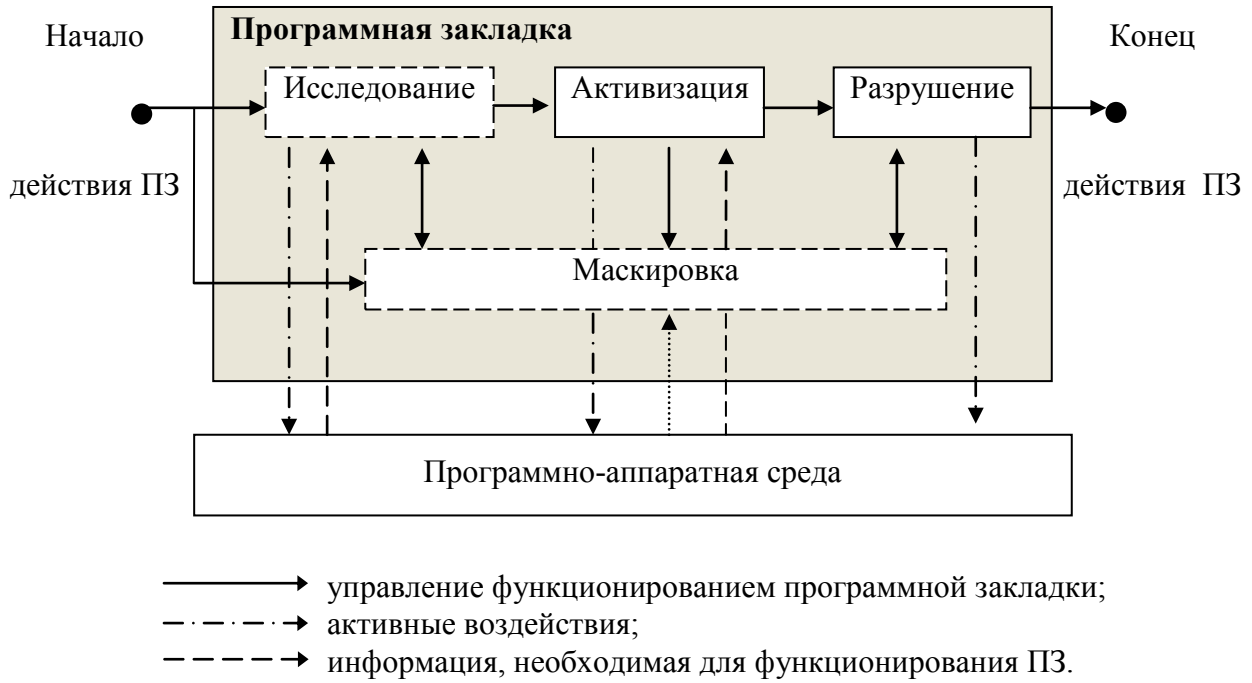


Рис. 2.9. Схема функционирования программной закладки

Начало функционирования программной закладки осуществляется в момент передачи управления программе-носителю закладки (на схеме – точка начало функционирования ПЗ).

Выполнению разрушающей функции предшествуют процессы исследования и активизации. Процесс исследования заключается в определении наиболее уязвимых мест безопасности системы, установки резидентных модулей и т.д. Так программная закладка получает информацию для дальнейшей активизации. Активизация программной закладки представляет собой непосредственный переход к разрушающей функции посредством проверки выполнения некоторого логического условия или условий в программно-аппаратной среде.

Выполнение разрушающей функции – завершающий этап жизненного цикла программной закладки.

Соответствующие внутренние и внешние связи программной закладки показаны на схеме рис. 2.9. Передача управления внутри программной закладки осуществляется в одном направлении – в сторону задействования разрушающей функции.

За время своего жизненного цикла программная закладка активно воздействует на программно-аппаратную среду, как результат проявления разрушающей функции, так и с целью исследования окружающей программно-аппаратной среды.

Маскировка необходима для сокрытия присутствия закладки. Процесс маскировки может быть начат в любой момент функционирования программной

закладки. Особенностью данного процесса является наличие защиты от исследования закладки вследствие активного воздействия программно-аппаратной среды на область программной закладки.

Методы защиты от закладок основаны на семантическом анализе программного обеспечения – носителя закладки. Известны следующие методы защиты от ПЗ.

Метод поиска программных закладок по сигнатурам. Его использование подразумевает применение побитного сравнения программ и наборов данных с сигнатурами (наборами двоичных кодов), однозначно идентифицирующими ту или иную из уже известных вредоносных программ.

Достоинство данного метода заключатся в гарантированности результатов в отношении известных вредоносных программ вне зависимости от времени их внедрения в систему и динамики изменения контролируемых программ и наборов данных. К недостаткам можно отнести необходимость постоянного обновления и пополнения набора сигнатур, а также неспособность определять новые виды вредоносных программ.

Как расширение метода поиска вредоносного программного обеспечения по сигнатурам можно рассмотреть *метод эвристического анализа*, который позволяет опять же путем сравнения выявить в кодах программ, комбинации, характерные для вредоносных программ и предупредить о возможно внедренной закладке или вирусе. Этот метод позволяет производить поиск ранее неизвестного вредоносного программного обеспечения, но не позволяет принять однозначное решение о его присутствии в системе.

Кроме того, к недостаткам вышеизложенных методов можно добавить еще один. Они могут не дать ожидаемых результатов при внедренных вредоносных программах, способных навязывать конечный результат проверок или модифицировать свой код.

Метод экспериментов. Заключается в проведении многократных экспериментов с изучаемой программой и сравнительном анализе полученных результатов. Изучаемая программа рассматривается как «черный ящик», алгоритм работы которого восстанавливается путем подбора входных данных и анализа выходных.

Эффективность метода экспериментов слабо зависит от программной реализации системы и определяется в первую очередь сложностью анализируемых алгоритмов. Метод экспериментов эффективен при анализе программ, реализующих относительно простые алгоритмы.

Метод экспериментов редко применяется в чистом виде. Чаще он служит дополнением к динамическому или статическому методу. Это обусловлено тем, что, как правило, восстанавливаемые алгоритмы оказываются слишком сложными для данного метода.

Статический метод. Заключается в переводе двоичных кодов программ на язык, понятный аналитику. Как правило, в качестве такого языка выступает язык assembler, а основу для такого перевода составляют программы дизассемблирования (дизассемблеры). Дальнейшая работа после дизассемблирования сводится к анализу полученных листингов. К достоинствам

данного метода можно отнести возможность восстановления алгоритма работы практически любого программного обеспечения, а к недостаткам – высокую трудоемкость, вызванную необходимостью анализа листингов дизассемблированных программ, как правило, имеющих большой объем. Поэтому, метод применим, в основном, для анализа небольших программ.

Динамический метод. Предполагает использование для выявления алгоритмов работы программы специальных программных средств, называемых отладчиками (debugger), позволяющих наблюдать за ходом выполнения, загруженной в оперативную память программы. При этом возможно выполнение программы по шагам, останов выполняемой программы в заранее обозначенных точках и просмотр фактически любой информации о состоянии системы.

Перечисленные методы семантического анализа программного кода позволяет выявлять не только ранее неизвестные вредоносные участки кода, но и различного рода ошибки в самом программном обеспечении, то есть устранить предпосылки вредоносного программного воздействия. С другой стороны, реализация методов защиты от закладок требует длительного времени, больших трудозатрат и высококвалифицированного персонала.

Последовательность выявления закладок в программно-аппаратной среде в общем виде может быть представлена в виде следующей последовательности шагов.

1) Выделяется группа прерываний, существенных с точки зрения обработки информации программой, относительно которой проводится защита. Обычно это прерывания int 13h, int 40h (запись и чтение информации на внешние накопители прямого доступа), int 14h (обмен с RS232 портом), int 10h (обслуживание видеотерминала), а также в обязательном порядке прерывания таймера int 8h, int 1Ch и прерывания клавиатуры int 9h и int 16h.

2) Для выделенной группы прерываний определяются точки входа (адреса входа) в ПЗУ используя справочную информацию, либо выполняя прерывание в режиме трассировки.

3) Для выделенных адресов создаются цепочки исполняемых команд от точки входа до команды IRET – возврату управления из BIOS.

Надо отметить, что запись в сегмент BIOS невозможна и поэтому закладки в BIOS не могут применять механизм преобразования своего кода во время его исполнения в качестве защиты от изучения.

В цепочках исполняемых команд выделяются:

– команды работы с портами;

– команды передачи управления;

– команды пересылки данных.

Они используются либо для информативного анализа, либо порождают новые цепочки исполняемых команд.

Порождение новых цепочек исполняемых команд происходит тогда, когда управление передается внутри сегмента BIOS.

4) В цепочках анализируются команды выделенных групп.

Определяются:

опасные действия первой группы: в прерываниях какого-либо класса присутствуют команды работы с недокументированными портами.

Наличие таких команд, как правило, указывает на передачу информации некоторому устройству, подключенному к параллельному интерфейсу (общей шине), например, встроенной радиопередающей закладке.

Данная ситуация имела место при закупке одной из партий персональных ЭВМ, где были обнаружены радиомаяки, посылавшие сигнал при выполнении программ тестирования и начальной загрузки в BIOS.

опасные действия второй группы: в прерываниях какого-либо класса присутствуют команды работы с портами, участвующие в работе другого класса прерываний;

опасные действия третьей группы: в цепочках присутствуют команды перемещения данных из BIOS в оперативную память (кроме таблицы прерываний и RAM BIOS);

опасные действия четвертой группы: в цепочках присутствуют команды передачи управления в оперативную память или в сегменты расширенного BIOS.

В случае если опасных действий не обнаружено, аппаратно-программная среда ПЭВМ без загруженной операционной среды считается безопасной.

Для проверки операционной системы используется аналогичный алгоритм:

1) По таблице прерываний определяются адреса входа для существенно важных прерываний.
2) Данные прерывания выполняются покомандно в режиме трассировки с анализом каждой команды по вышеприведенному алгоритму. В этом случае команды типа JMP не анализируются, поскольку в режиме покомандного выполнения переходы происходят автоматически.

Выполнение происходит до того момента, когда будет достигнут адрес ПЗУ.

Для полного анализа необходимо выполнить все используемые программой функции исследуемого прерывания.

Выводы по второй главе

Атака – это совокупность действий злоумышленника, приводящих к нарушению информационной безопасности компьютерной сети (КС).

В общем случае любая атака может быть разделена на четыре стадии: рекогносцировка, вторжение, атакующее воздействие, развитие.

Все угрозы ресурсам сети могут быть классифицированы по степени риска на следующие: отказ в обслуживании, попытка несанкционированного доступа, предварительное зондирование, "подозрительная" сетевая активность. Перечисленные классы угроз упорядочены по убыванию степени риска.

Системы обнаружения атак позволяют своевременно выявлять и блокировать атаки нарушителей.

Процесс выявления атаки состоит из следующих этапов:

- сбор данных, необходимых для определения факта атаки на ресурсы сети;
- анализ данных, собранных сетевыми и узловыми датчиками;

– выявление атаки;

– реагирование на выявленную атаку.

При анализе данных, собранных сетевыми и узловыми датчиками, система обнаружения атак использует сигнатурные и поведенческие методы выявления атак.

Сигнатурные методы описывают каждую атаку в виде специальной модели или сигнатуры. В исходных данных, собранных сетевыми и узловыми датчиками выполняется процедура поиска сигнатуры атаки с использованием базы данных сигнатур атак. Преимущество сигнатурных методов – высокая точность определения факта атаки, а недостаток – невозможность обнаружения тех атак, сигнатуры которых пока не определены.

Поведенческие методы базируются на моделях штатного процесса поведения сети. Методы основаны на обнаружении несоответствия между текущим режимом работы сети и режимом работы, соответствующим штатной модели данного метода. Любое несоответствие рассматривается как атака. Преимущество поведенческих методов – возможность обнаружения новых атак без модификаций или обновлений параметров модели, недостаток – сложно создать точную модель штатного режима функционирования сети.

Обнаружение атак должно осуществляться на различных уровнях корпоративной сети: конкретных узлах корпоративной сети, сетевых сегментах, локальных, территориально-распределённых и глобальных системах.

Программная закладка отличается от компьютерного вируса направленным воздействием. И вирус, и закладка должны скрывать свое присутствие в операционной среде компьютерной системы. Особенностью ПЗ является то, что они становятся неотделимы от прикладных или системных программ, если внедрены в них на стадии разработки или путем обратного проектирования.

Структурно программная закладка состоит из четырех основных функциональных блоков: исследования, активизации, проявления деструктивных действий (разрушения) и маскировки.

Методы защиты от ПЗ основаны на семантическом анализе носителя закладки**.**

3 ОРГАНИЗАЦИЯ ДОСТУПА К РЕСУРСАМ СЕТИ

3.1 Основные этапы допуска

Процесс допуска пользователя в любой компьютерной системе состоит из трех взаимосвязанных последовательно выполняемых процедур: идентификации, аутентификации и авторизации.

Идентификация – процедура распознавания субъекта по его идентификатору. В процессе регистрации субъект предъявляет свой идентификатор системе, которая проверяет его наличие в своей базе эталонных данных. Субъекты с известными системе идентификаторами считается легальными (законными), остальные относятся к нелегальным.

Сам идентификатор может представлять собой последовательность любых символов и должен быть заранее зарегистрирован в системе администратором службы безопасности. В процессе регистрации администратором в базу эталонных данных системы защиты для каждого пользователя заносятся следующие элементы данных:

– фамилия, имя, отчество и, при необходимости, другие характеристики пользователя;

– уникальный идентификатор пользователя;

– имя процедуры установления подлинности;

– используемая для подтверждения подлинности эталонная информация, например, пароль;

– ограничения на используемую эталонную информацию, например, минимальное и максимальное время, в течение которого указанный пароль будет считаться действительным;

– полномочия пользователя по доступу к корпоративным ресурсам.

Аутентификация – процедура проверки подлинности субъекта, которая позволяет достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует. Для этого он должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному (пароль, ключ и т. п.).

Авторизация – процедура предоставления субъекту определенных прав доступа к ресурсам системы после прохождения им процедуры аутентификации. Для каждого субъекта в системе определяется набор прав, которые он может использовать при обращении к ее ресурсам.

Для того чтобы обеспечить управление и контроль над данными процедурами, дополнительно используются процессы администрирования и аудита.

Администрирование – процесс управления доступом субъектов к ресурсам системы. Данный процесс включает:

– создание идентификатора субъекта (учетной записи пользователя) в системе;

– управление данными субъекта, используемыми для его аутентификации (смена пароля, издание сертификата и т. п.);

– управление правами доступа субъекта к ресурсам системы.

Аудит – процесс контроля (мониторинга) доступа субъектов к ресурсам системы, включающий протоколирование действий субъектов при их доступе к ресурсам системы в целях обнаружения несанкционированных действий.

Таким образом, в общем случае речь идет о пяти основных процедурах доступа. При этом возможен различный подход к расстановке приоритетов при выполнении этих процедур.

Общая схема идентификации и установления подлинности пользователя при его доступе в компьютерную систему представлена на рис. 3.1.

Если в процессе аутентификации подлинность пользователя установлена, то система защиты должна определить его полномочия по использованию корпоративных ресурсов для последующего контроля установленных полномочий.

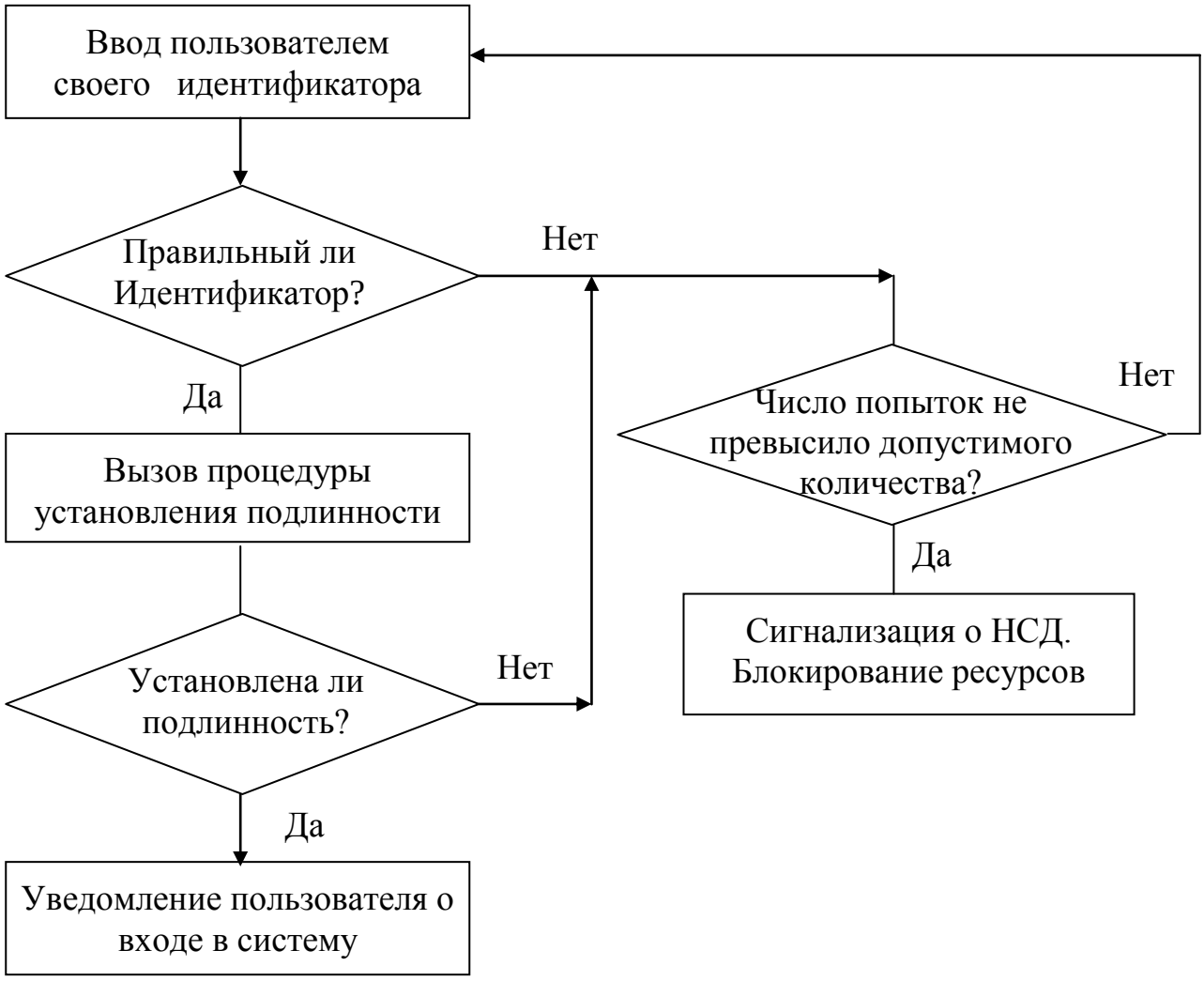


Рис. 3.1. Схема идентификации и аутентификации пользователя при доступе в компьютерную систему

3.2 Роль, задачи и виды аутентификации

Система аутентификации независимо состоит из пяти элементов.

Первый элемент – субъект доступа – конкретный человек или процесс, который должен проходить аутентификацию.

Второй элемент – идентификатор – опознавательный знак, который выделяет этого человека или этот процесс среди других.

Третий элемент – аутентификатор – отличительная характеристика, подтверждающая принадлежность идентификатора субъекту доступа.

Четвертый элемент – администратор – владелец системы, который несет ответственность за использование системы, и в разграничении авторизованных пользователей и остальных полагается на механизм аутентификации.

Пятый элемент – механизм аутентификации, который позволяет проверить присутствие отличительной характеристики.

При успешном прохождении аутентификации субъекту доступа должны быть выданы некоторые права (привилегии).

Для этого служит механизм управления доступом. С помощью этого же механизма субъект доступа лишается прав (привилегий), если аутентификация была неуспешной.

Примером аутентификации является вход физического лица в систему по паролю. Процесс включает в себя процедуру сравнения пароля, введенного с клавиатуры, с паролем, установленным либо самим пользователем, либо администратором системы. Процедура завершается успешно, если оба пароля совпадают. В этом случае механизм управления доступом разрешает пользователю продолжать работу на компьютере, и система использует имя пользователя каждый раз, когда ей требуется решение службы управления доступом к защищенному ресурсу.

В компьютерных системах аутентификация и управление доступом обычно реализуются как две разные функции. Процесс аутентификации подтверждает подлинность имени пользователя. Управление доступом осуществляется путем сравнения имени пользователя с правилами доступа, связанными с конкретным файлом или другим ресурсом.

Пользователь является не единственным субъектом, который подлежит аутентификации. В настоящее время необходимо аутентифицировать и системы, действующие без вмешательства человека. Например, не только сервер может проверить пользователя, пытающегося получить доступ, но и пользователь может проверить сервер на его принадлежность компании, предоставляющей услуги.

Для подтверждения свой подлинности субъект должен предоставить некоторую секретную информацию, которая должна быть доступна только ему одному. Он может предъявлять системе различные виды информации.

Фактор аутентификации – определенный вид информации, предоставляемый субъектом системе при его аутентификации.

Выделяют три фактора аутентификации, используемые в различных комбинациях:

на основе знания чего-либо,
обладания чем-либо,
на основе биометрических характеристик
Примеры факторов аутентификации приведены в табл. 3.1.

Табл. 3.1

Факторы аутентификации

Фактор аутентификации	Классификация типов факторов аутентификации NCSC-TG-0171[4]	Примеры факторов аутентификации
1-й тип: на основе знания чего-либо	Type 1: Authentication by Knowledge	– Пароль или парольная фраза – PIN-код (Personal Identification Number)
2-й тип: на основе обладания чем-либо	Type 2: Authentication by Ownership	– Физический ключ – Карта с магнитной полосой – OTP-токен, генерирующий одноразовый пароль
3-й тип: На основе биометрических характеристик	Type 3: Authentication by Characteristic	– Отпечаток пальца – Рисунок сетчатки глаза – Голос

Сегодня в некоторых компаниях организуется еще и контроль доступа в помещение, то есть в определенные помещения доступ предоставляется только ограниченному числу лиц. Например, в серверную комнату может войти только администратор или в комнату финансового отдела компании могут иметь доступ только его сотрудники. Если при этом установить для компьютеров, находящихся в этих помещениях, строго определенные IP-адреса, то тогда появляется возможность более качественно выполнять аутентификацию при доступе сотрудников к ресурсам компьютерной сети. Им предоставляется доступ к определенным действиям или данным только в том случае, если они это делают в строго определенном помещении и соответственно с определенных компьютеров, имеющих определенные IP-адреса. В этом случае иногда говорят об использовании «четвертого» типа фактора аутентификации – на основе места проведения процедуры. Данный фактор не считается дополнительным, так как его нельзя использовать отдельно от других факторов для аутентификации субъекта. Например, нельзя обеспечить, чтобы только определенный сотрудник работая на строго определенном рабочем месте (компьютере).

В последнее время наметились тенденции интеграции логических средств аутентификации и средств контроля и управления доступом. Смарт-карты,

[4] NCSC-TG-017 – документ «A Guide to Understanding Identification and Authentication in Trusted Systems», опубликованный U.S. National Computer Security Center. Руководство содержит комплекс рекомендуемых инструкций по процедурам идентификации и аутентификации.

используемые для аутентификации пользователя при доступе к ресурсам компьютерной системы, интегрируются с RFID (радиочастотной идентификацией). В этом случае появляется возможность дополнительно использовать их для аутентификации человека при его доступе в различные помещения. По-прежнему в этом случае речь будет идти об использовании аутентификации «на основе обладания чем-либо». Это расширяет возможности использования смарт-карты, дает дополнительные удобства для пользователя, но не повышает качество аутентификации.

Аутентификация может быть реализована с помощью одного из трех факторов аутентификации. Например, в процессе аутентификации у пользователя может быть запрошен пароль, либо потребуется представить отпечаток пальца.

Аутентификация, в процессе которой используется только один фактор аутентификации, называется однофакторной.

Аутентификация, в процессе которой используется несколько факторов аутентификации, называется многофакторной.

Например, в процессе аутентификации пользователь должен использовать смарт-карту и дополнительно пароль (или PIN-код). Также используются понятия двухфакторной и трехфакторной аутентификации при использовании комбинации двух и трех факторов аутентификации соответственно.

В документе NCSC-TG-017 вводятся термины для различных видов многофакторной аутентификации: типа 12, типа 23 и типа 123. Аутентификация типа 12, например, использует два фактора аутентификации: первый – «на основе знания чего-либо» и второй – «на основе обладания чем-либо». Трехфакторная аутентификация использует комбинацию трех факторов аутентификации – «на основе знания чего-либо», «на основе обладания чем-либо» и «на основе биометрии». Эту аутентификацию называют аутентификация типа 123.

Если для аутентификации используется только один фактор аутентификации, она оказывается уязвимой. При многофакторной аутентификации используется несколько (два и более) факторов аутентификации, что обеспечивает большую безопасность.

Наиболее распространено использование комбинации двух факторов при аутентификации пользователя в банкомате. Требуется одновременно использовать карту с магнитной полосой и PIN-код.

3.3. Парольная аутентификация

Основными и наиболее часто применяемыми методами установления подлинности пользователей являются методы, основанные на использовании паролей или парольная аутентификация.

Парольная аутентификация – аутентификация на основе обладания неким секретным знанием – «на основе знания чего-либо».

Под **паролем** понимается некоторая последовательность символов, сохраняемая в секрете и предъявляемая при обращении к компьютерной системе. Ввод пароля, как правило, выполняется с клавиатуры после соответствующего запроса системы.

Для особо надежного опознавания могут применяться и методы, основанные на использовании технических средств определения сугубо индивидуальных характеристик человека (голоса, отпечатков пальцев, структуры зрачка и т.д.). Однако такие средства требуют значительных затрат и поэтому используются редко.

Существующие парольные методы проверки подлинности пользователей при входе в корпоративную информационную систему можно разделить на две группы:

– методы проверки подлинности на основе простого пароля;

– методы проверки подлинности на основе динамически изменяющегося пароля.

Пароль подтверждения подлинности пользователя при использовании простого пароля не изменяется от сеанса к сеансу в течении установленного администратором службы безопасности времени его существования (действительности).

При использовании динамически изменяющегося пароля пароль пользователя для каждого нового сеанса работы или нового периода действия одного пароля изменяется по правилам, зависящим от используемого метода.

3.3.1 Использование простого пароля

Процедура опознавания с использованием простого пароля может выть представлена в виде следующей последовательности действий (рис. 3.2):

1) пользователь посылает запрос на доступ к компьютерной системе и вводит свой идентификатор;

2) система запрашивает пароль;

3) пользователь вводит пароль:

4) система сравнивает полученный пароль с паролем пользователя, хранящимся в базе эталонных данных системы защиты, и разрешает доступ, если пароли совпадают; в противном случае пользователь к ресурсам компьютерной системы не допускается.

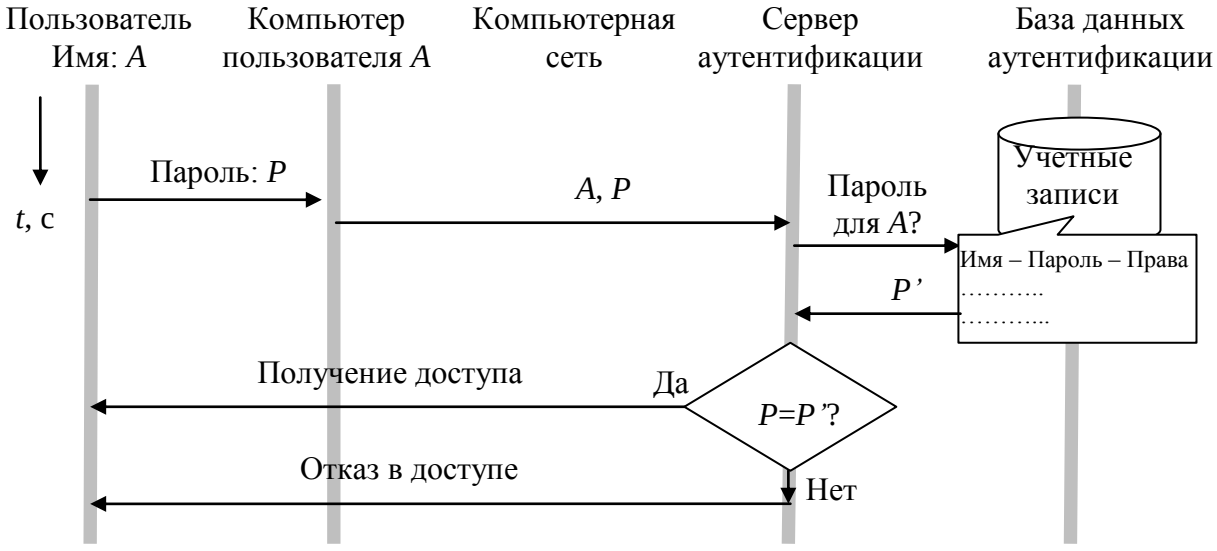


Рис. 3.2. MMS-диаграмма процедуры опознавания с использованием простого пароля

Поскольку пользователь может допустить ошибку при вводе пароля, то системой должно быть предусмотрено допустимое количество повторений для ввода пароля.

При работе с паролями должна предусматриваться и такая мера, как недопустимость их распечатки или вывода на экраны мониторов. Поэтому система защиты должна обеспечивать ввод пользователями запрошенных у них паролей без отображения этих паролей на мониторах.

Можно выделить следующие основные способы повышения стойкости системы защиты на этапе аутентификации

- повышение степени нетривиальности пароля;
- увеличение длины последовательности символов пароля;
- увеличение времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля;
- повышение ограничений на минимальное и максимальное время действительности пароля.

Чем нетривиальнее пароль, тем сложнее его запомнить. Плохо запоминаемый пароль может быть записан на листе бумаги, что повышает риск его раскрытия. Выходом здесь является использование определенного числа не записываемых на бумаге пробелов или других символов в начале, внутри, а также в конце последовательности основных символов пароля. Кроме того, отдельные символы пароля могут набираться на другом регистре (например, вместо строчных быть прописными или наоборот), что также не должно отражаться на листе бумаги. В этом случае незаконно полученный лист бумаги с основными символами пароля не будет являться достаточным условием раскрытия пароля целиком.

Вероятность подбора пароля уменьшается также при увеличении его длины и времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля. Ожидаемое время раскрытия пароля $t_{\text{р}}$ можно вычислить на основе следующей полученной экспериментально приближенной формулы:

$$t_{\text{р}} = \left(\text{A}^{k} \cdot t_{\text{в}} \right) / 2,$$

здесь:

A – число символов в алфавите, используемом для набора символов пароля;

k – длина пароля в символах, включая пробелы и другие служебные символы;

$t_{\text{в}}$ – время ввода пароля с учетом времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля.

Например, если A=26 символов (учтены только буквы английского алфавита), $t_{\text{в}}$=2 секунды, а k=6 символов, то ожидаемое время раскрытия $t_{\text{р}}$ приблизительно равно одному году. Если в данном примере после каждой неудачной попытки ввода пароля предусмотреть временную задержку в 10 секунд, то ожидаемое время раскрытия увеличится в 5 раз.

Из приведенной выше формулы становится понятно, что повышения стойкости системы защиты на этапе аутентификации можно достигнуть и

увеличением числа символов алфавита, используемого для набора символов пароля. Такое увеличение можно обеспечить путем использования нескольких регистров (режимов ввода) клавиатуры для набора символов пароля, например, путем использования строчных и прописных латинских символов, а также строчных и прописных символов кириллицы.

Обычно термины «формат пароля», «длина пароля», «частота смены паролей» не различаются и называются одним общим термином – парольные политики. Парольные политики необходимы для повышения стойкости парольной защиты.

Современные парольные политики задают минимальную длину паролей (обычно 6–8 символов) и их рекомендуемую длину (10–12 символов). Максимальная длина пароля, как правило, ограничена особенностями реализации механизма аутентификации.

Для исключения необходимости запоминания пользователями длинных и нетривиальных паролей в системе защиты может быть предусмотрена возможность записи паролей в зашифрованном виде на информационные носители, например, магнитные карты, носители данных в микросхемах и т.д., а также считывания паролей с этих информационных носителей. Такая возможность позволяет повысить безопасность за счет значительного увеличения длины паролей, записываемых на носители информации. Однако, при этом администрации службы безопасности следует приложить максимум усилий для разъяснения пользователям вычислительной системы о необходимости тщательной сохранности носителей информации с их паролями.

На степень информационной безопасности при использовании простого парольного метода проверки подлинности пользователей большое влияние оказывают ограничения на минимальное и максимальное время действительности каждого пароля. Чем чаще меняется пароль, тем обеспечивается большая безопасность.

Минимальное время действительности пароля задает время, в течение которого пароль менять нельзя, а максимальное – время, по истечении которого пароль будет недействительным. Соответственно, пароль должен быть заменен в промежутке между минимальным и максимальным временем его существования. Поэтому понятно, что более частая смена пароля обеспечивается при уменьшении минимального и максимального времени его действительности.

Аутентификация на основе хэшированного пароля.

В большинстве используемом в настоящее время программного обеспечения применяются пароли не в чистом виде, а их хэш-значения, получаемые с помощью вычисления криптографической хэш-функции.

Пример прохождения пользователем процедуры аутентификации на основе хэшированного пароля (рис. 3.3.):

1. Пользователь вводит свои имя *A*, и пароль *P* на рабочей станции.

2. Рабочая станция вычисляет хэш-значение *h* от введенного пароля. Имя пользователя и хэш-значение передаются по сети серверу аутентификации.

3. Сервер аутентификации сравнивает результат вычисления хэш-значения (*h*) от введенного пользователем пароля с хэш-значением, хранящимся в учетной записи пользователя (*h'*).

4. В случае совпадения аутентификация признается успешной.

Как известно, хэш-функции строятся на основе однонаправленных функций. Это свойство хэш-функции делает невозможным восстановление исходной информации при её известном хэш-значении.

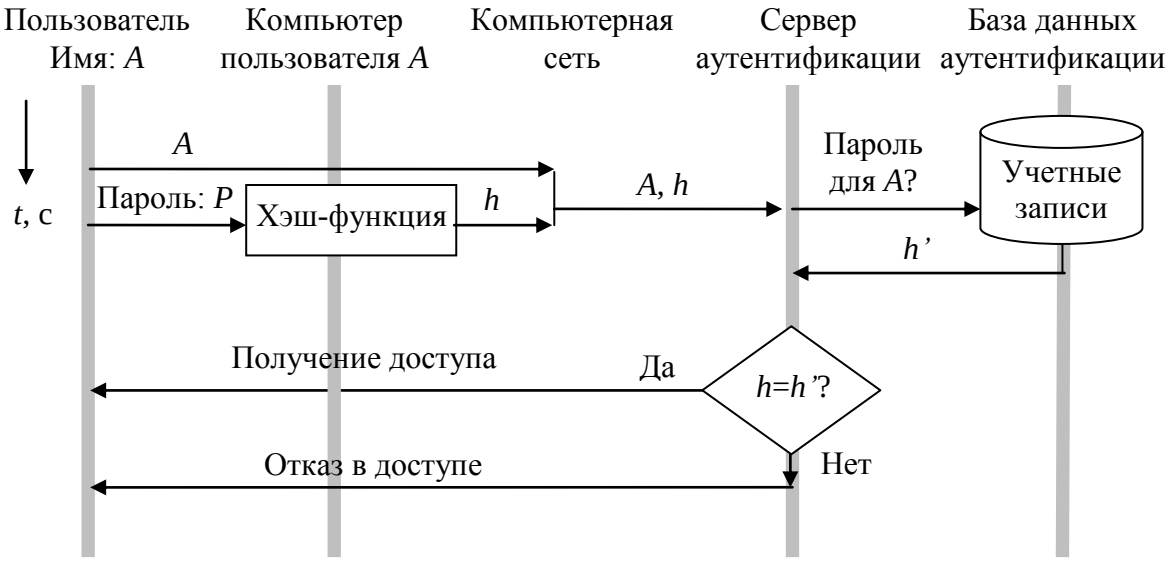


Рис. 3.3. Диаграмма процедуры аутентификации на основе хэшированного пароля

Таким образом, восстановить открытое значение пароля из базы данных аутентификации, где он хранится в виде хэш-значения, практически невозможно. Из этого следует, что в базе эталонных данных системы защиты пароли никогда не следует хранить в явной форме.

Аутентификация на основе PIN-кода.

PIN-код (Personal Identification Number) – это разновидность пароля, обычно используемого для аутентификации на локальном устройстве.

Несмотря на слова Identification (идентификационное) и Number (число), послужившие основой для аббревиатуры, PIN-код редко служит в качестве идентификатора пользователя. Например в торговых автоматах и банкоматах применяется карта с магнитной полосой или смарт-карта, а PIN-код используется для аутентификации пользователя.

Обычно PIN-код торгового автомата или банкомата состоит из четырех цифр. Таким образом, один из каждых 10000 клиентов имеют один и тот же PIN-код. По сути PIN-код похож на «простой пароль».

Разница между PIN-кодом и паролем состоит в области и условиях их использования.

Обычно для решений, в которых используется PIN-код, характерно следующее:

– в локальном устройстве, в котором осуществляется аутентификация с помощью PIN-кода, имеется интерфейс для пользователя, а не для программ. Никто не может ввести PIN-код, не используя клавиатуру данного устройства.

– PIN-код не передается по сети и не может быть перехвачен.

С учетом этих особенностей использовать термин PIN-код для обозначения простого пароля неверно, поскольку между этими терминами есть функциональная разница. Аутентификация по PIN-коду обычно используется в двухфакторной аутентификации типа 12.

3.3.2 Использование динамически изменяющегося пароля

Методы проверки подлинности на основе динамически изменяющегося пароля обеспечивают большую безопасность, так как частота смены паролей и них максимальна – пароль для каждого пользователя меняется ежедневно или через несколько дней. При этом каждый следующий пароль по отношению к предыдущему изменяется по правилам, зависящим от используемого метода проверки подлинности.

Существуют следующие методы парольной защиты, основанные на использовании динамически изменяющегося пароля:

– методы модификации схемы простых паролей;

– метод «запрос-ответ»;

– функциональные методы.

Наиболее эффективными из данных методов являются функциональные методы.

Методы модификации схемы простых паролей.

К методам модификации схемы простых паролей относят случайную выборку символов пароля и одноразовое использование паролей.

При использовании первого метода каждому пользователю выделяется достаточно длинный пароль, причем каждый раз для опознавания используется не весь пароль, а только его некоторая часть. В процессе проверки подлинности система запрашивает у пользователя группу символов по заданным порядковым номерам. Количество символов и их порядковые номера для запроса определяются с помощью датчика псевдослучайных чисел.

При одноразовом использовании паролей каждому пользователю выделяется список паролей. В процессе запроса номер пароля, который необходимо ввести, выбирается последовательно по списку или по схеме случайной выборки.

Недостатком методов модификации схемы простых паролей является необходимость запоминания пользователями длинных паролей или их списков. Запись же паролей на бумагу или в записные книжки приводит к появлению риска потери или хищения носителей информации с записанными на них паролями.

Метод «запрос-ответ».

При использовании метода «запрос-ответ» в сети заблаговременно создается и особо защищается массив вопросов, включающий в себя как вопросы общего характера, так и персональные вопросы, относящиеся к конкретному пользователю, например, вопросы, касающиеся известных только пользователю случаев из его жизни

Для подтверждения подлинности пользователя система последовательно задает ему ряд случайно выбранных вопросов, на которые он должен дать ответ. Опознание считается положительным, если пользователь правильно ответил на все вопросы.

Основным требованием к вопросам в данном методе аутентификации является уникальность, подразумевающая, что правильные ответы на вопросы знают только пользователи, для которых эти вопросы предназначены.

Функциональные методы.

Среди функциональных методов наиболее распространенными являются метод функционального преобразования пароля, а также метод «рукопожатия».

Метод функционального преобразования основан на использовании некоторой функции F, которая должна удовлетворять следующим требованиям

– для заданного числа или слова X легко вычислить $Y=F(X)$;

– зная X и Y, сложно или невозможно определить функцию $Y=F(X)$.

Необходимым условием выполнения данных требований является наличие в функции $F(X)$ динамически изменяющихся параметров, например, текущих даты, времени, номера дня недели, или возраста пользователя.

Пользователю сообщается:

– исходный пароль – слово или число X, например число 31;

– функция $F(X)$, например, $Y=(X \bmod 100)D+W^3$, где (X mod 100) -операция взятия остатка от целочисленного деления X на 100, D -текущий номер дня недели, а W - текущий номер недели в текущем месяце);

– периодичность смены пароля, например, каждый день, каждые три дня или каждую неделю.

Паролями пользователя для последовательности установленных периодов действия одного пароля будут соответственно X, $F(X)$, $F(F(X))$, $F(F(F(X)))$ и т. д., т.е. для 1-го периода действия одного пароля паролем пользователя будет $F(X)$. Поэтому для того, чтобы вычислить очередной пароль по истечении периода действия используемого пароля, пользователю не нужно помнить начальный (исходный) пароль, важно лишь не забыть функцию парольного преобразования и пароль, используемый до настоящего момента времени.

С целью достижения высокого уровня безопасности функция преобразования пароля, задаваемая для каждого пользователя, должна периодически меняться, например, каждый месяц. При замене функции целесообразно устанавливать и новый исходный пароль.

Согласно **методу «рукопожатия»** существует функция F, известная только пользователю и самой системе, доступ к которой он хочет получить. Данная

функция должна удовлетворять тем же требованиям, которые определены для функции, используемой в методе функционального преобразования.

При входе пользователя в вычислительную систему системой защиты генерируется случайное число или случайная последовательность символов X и вычисляется функция $F(X)$, заданная для данного пользователя (рис. 3.4). Далее X выводится пользователю, который должен вычислить $F'(X)$ и ввести полученное значение в систему. Значения $F(X)$ и $F'(X)$ сравниваются системой и, если они совпадают, то пользователь получает доступ в ВС.

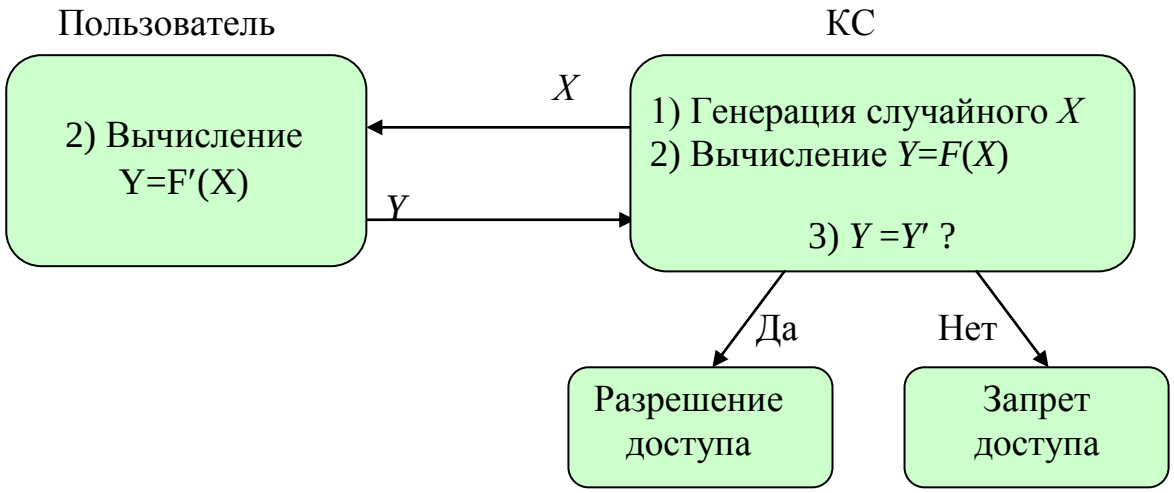


Рис. 3.4. Схема аутентификации по методу «рукопожатия»

Для высокой безопасности функцию «рукопожатия» целесообразно циклически менять через определенные интервалы времени, например, устанавливать разные функции для четных и нечетных чисел месяца

Достоинством метода «рукопожатия» является то, что никакой конфиденциальной информации между пользователем и компьютерной системой не передается. По этой причине эффективность данного метода особенно велика при его применении в компьютерных сетях для подтверждения подлинности пользователей, пытающихся осуществить доступ к серверам или базам данных.

В некоторых случаях может оказаться необходимым пользователю проверить подлинность той вычислительной системы, к которой он хочет осуществить доступ. Необходимость во взаимной проверке может понадобиться и когда два пользователя КС хотят связаться друг с другом по линии связи. Методы простых паролей, а также методы модификации схем простых паролей в этом случае не подходят. Наиболее подходящим здесь является метод «рукопожатия». При его использовании ни один из участников сеанса связи не будет получать никакой секретной информации.

Приведем пример, доказывающий данное утверждение. Пусть данная типовая структура корпоративной сети, приведенная на рис. 3.5. На ней изображены:

– вспомогательный (Proxy) сервер, основными функциями которого является коммутация трафика между интерфейсами Int-1, Int-2 и Int-3 в соответствии со списками доступа администратора;

– узлы локального и удаленного пользователя;

– серверы:
DHCP для конфигурирования хостов,
AAA для аутентификации, авторизации и учета,
e-mail для обработки почтовых сообщений,
DB1и DB2 для хранения документации группового использования.

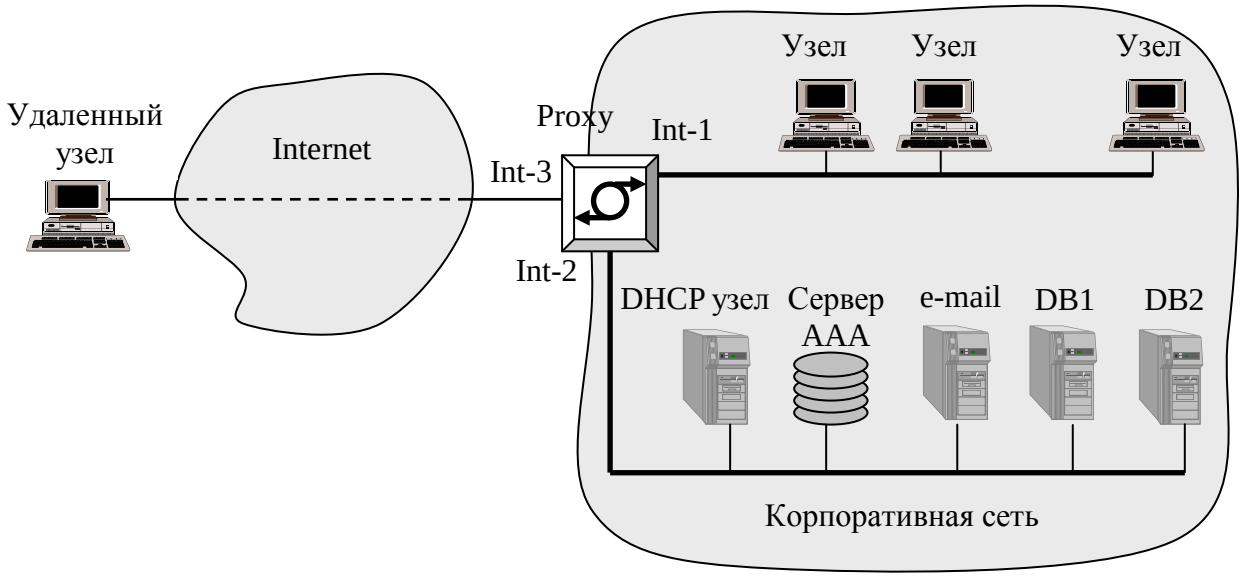


Рис. 3.5. Типовая схема корпоративной сети

При попытке подключения пользователя к корпоративной сети proxy-сервер запрашивает его имя и пароль. Полученный ответ сравнивается с записью в списке доступа вида: имя пользователя (*Name* или *User ID*) – пароль (P*assword*), которая внесена администратором сети и хранится на AAA-сервере.

Proxy-сервер посылает удаленному узлу пользователя некоторое случайное число *V*, а хост возвращает другое число *W*, вычисленное по заранее известной функции с использованием имени (*Name*) и пароля (*Password*). Иначе говоря, *W=F*(*V, Name, Password*). Предполагается, что злоумышленник в состоянии перехватить пересылаемые по сети значения *V, Name* и *W*, и ему известен алгоритм вычисления функции *F*. Существо формирования *W* состоит в том, что исходное элементы (биты) случайного числа *V* различным образом «перемешиваются» с неизвестным злоумышленнику элементами пароля *Password*. Затем полученный зашифрованный текст подвергается сжатию. Такое преобразование называется дайджест-функцией (digest function) или хэш-функцией, а результат – дайджестом. Точная процедура формирования дайджеста определена алгоритмом MD5 и описана в RFC 1321, PS. Proxy-сервер запрашивает у AAA-сервера истинное значение *W*, пересылая ему значения Name и *V*. Сервер AAA на основании полученных от proxy-сервера значений *V* и *Name* и имеющегося у него в базе данных пароля *Password* по тому же алгоритму

вычисляет *W* и возвращает его proxy-серверу. Proxy-сервер сравнивает два значения *W*, полученные от хоста и от AAA-сервера: если они совпадают, то хосту посылается сообщение об успешной аутентификации.

После успешной аутентификации пользователя proxy-сервер на основании списка управления доступом производит авторизацию, то есть определяет к каким серверам DB1 и DB2 группового использования может обращаться пользователь, а сервера DB1 и DB2 определяют какие операции (только чтение или чтение/запись) он может осуществлять.

Для последующего возможного анализа успешных и неуспешных соединений пользователей выполняется процедура учета, которая состоит в ведении записей истории соединений пользователей.

На рис. 3.6 приведена процедура аутентификации пользователя со следующими исходными данными: имя пользователя (*Name*) Ivanov, пароль (*Password* = K1m), случайное число (*V*) 123456. Процедура перемешивания состоит в последовательном перемешивании полубайтов пароля и случайного числа. Вычисление дайджеста состоит в вычислении остатка перемешенного числа по модулю *Password*.

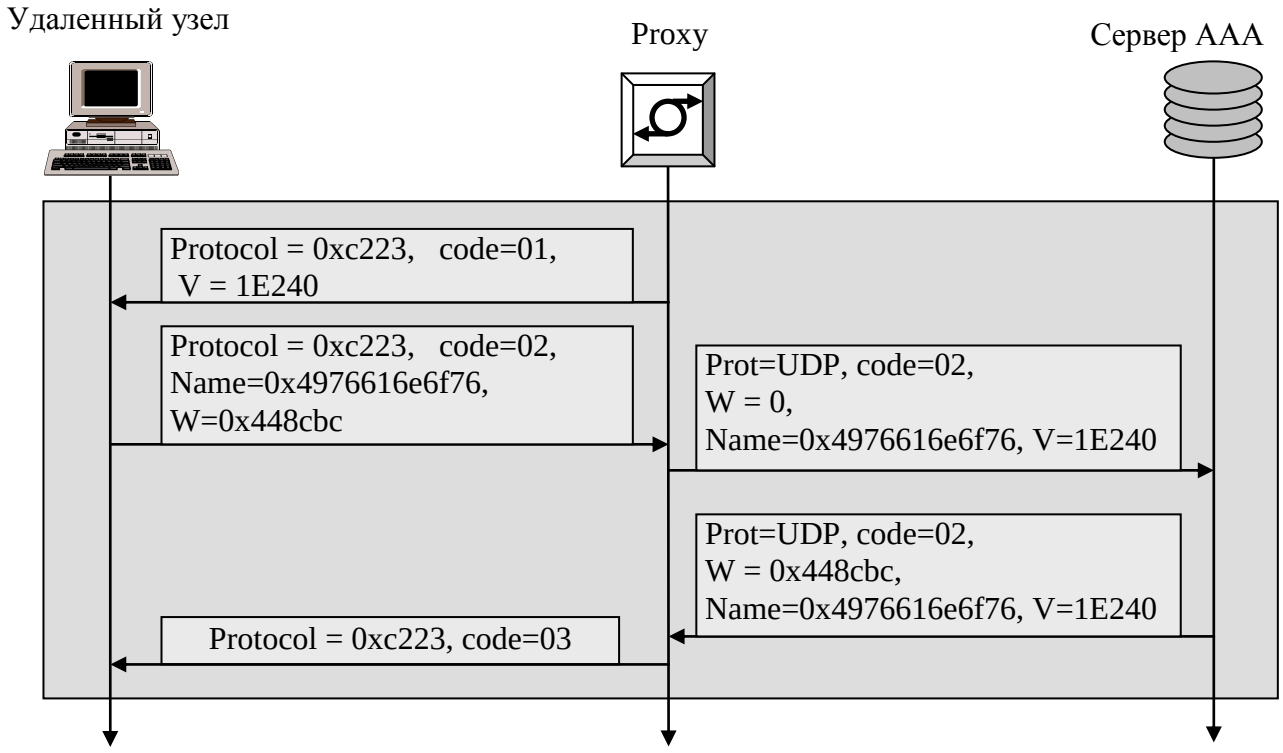


Рис. 3.6. Процедура аутентификации пользователя

– В первом сообщении proxy-сервер запрашивает (code=01) по протоколу аутентификации CHAP (Protocol = 0xc223) у удаленного пользователя ответ на случайное число V = 123456 = 0x1E240. Хост удаленного пользователя производит следующие операции.

1) Подставляет имя пользователя, используя таблицу кодов ASCII (табл.3.2).

Табл. 3.2

№	(0) 000	(1) 001	(2) 010	(3) 011	(4) 100	(5) 101	(6)110	(7) 111
(0) 0000	**NUL**	**DLE**	**SP**	**0**	**@**	**P**	**'**	**p**
(1) 0001	**SOH**	**DC1**	**!**	**1**	**A**	**Q**	**a**	**q**
(2) 0010	**STX**	**DC2**	**“**	**2**	**B**	**R**	**b**	**r**
(3) 0011	**ETX**	**DC3**	**#**	**3**	**C**	**S**	**c**	**s**
(4) 0100	**EOT**	**DC4**	**$**	**4**	**D**	**T**	**d**	**t**
(5) 0101	**ENQ**	**NAK**	**%**	**5**	**E**	**U**	**e**	**u**
(6) 0110	**ACK**	**SYN**	**&**	**6**	**F**	**V**	**f**	**v**
(7) 0111	**BEL**	**ETB**	**'**	**7**	**G**	**W**	**g**	**w**
(8) 1000	**BS**	**CAN**	**(**	**8**	**H**	**X**	**h**	**x**
(9) 1001	**HT**	**EM**	**)**	**9**	**I**	**Y**	**i**	**y**
(a) 1010	**LF**	**SUB**	*****	**:**	**J**	**Z**	**j**	**z**
(b) 1011	**VT**	**ESC**	**+**	**;**	**K**	**[**	**k**	**{**
(c) 1100	**FF**	**IS4**	**,**	<	**L**	\	**l**	|
(d) 1101	**CR**	**IS3**	**-**	**=**	**M**	**]**	**m**	**}**
(e) 1110	**SO**	**IS2**	**.**	>	**N**	^	**n**	~
(f) 1111	**S1**	**IS1**	**/**	**?**	**O**	**_**	**o**	**DEL**

Для определения двоичного кода символа следует к коду колонки приписать код строки, а для определения шестнадцатеричного – к значению кода колонки приписать значение кода строки. В соответствии с табл.4.1 имя пользователя Ivanov представляется как 0x4976616e6f76, а пароль K1m – как 0x4b316d.

2) Перемешивает байты пароля 0x**4b316d** и случайного числа 0x*01e240*, получая перемешанное число *F*=0x**4***0***b***13***e***1***2***6***4***d***0*.

3) Вычисляет ответ как *W* = *F* mod *Password* = 40b13e1264d0 mod 0x4b316d = 71129994781904 mod 4927853 = 4493476 = 0x448cbc.

– Во втором сообщении хост возвращает ответ в виде *Name*=0x4976616e6f76 и *W* = 0x448cbc.

– В третьем сообщении proxy-сервер запрашивает истинное значение *W* у AAA-сервера, посылая ему те же значения *Name* и *V*.

– В четвертом сообщении proxy-сервер получает от AAA-сервера истинное значение *W*, соответствующее *Name*=0x4976616e6f76 и *V*=0x1E240.

– В пятом сообщении proxy-сервер подтверждает (code=03) легитимность пользователя.

3.3.3. Недостатки методов аутентификации с запоминаемым паролем

Методы аутентификации с запоминаемым паролем обладают многими недостатками – пароль можно украсть, подсмотреть, подобрать (угадать) и т.д. Кроме того, довольно легко ввести в заблуждение пользователей и администраторов системы, заставив их открыть свой пароль, или же просто принудить их к открытию своего пароля.

Ниже в табл. 3.3 приведены известные атаки на системы, в которых используется аутентификация на основе пароля, а также способы защиты от подобных атак.

Табл. 3.3

Атаки на пароли и защита от них

Описание атаки	Защита от данной атаки
Кража парольного файла	
Злоумышленник может прочитать пароли пользователя из парольного файла или резервной копии	*Хэширование пароля* Каждая организация, разрабатывающая парольную аутентификацию, должна снабжать свои приложения этой защитой.
Злоумышленник, перебирая пароли, производит в файле паролей или его копии поиск, используя слова из большого заранее подготовленного им словаря. Злоумышленник вычисляет хэш-значение для каждого пробного пароля с помощью того же алгоритма, что и программа аутентификации.	*Безопасность файла* Доступ на чтение к файлу паролей должен быть предоставлен лишь небольшому числу доверенных пользователей. *Хэшированные с шумами (помехами) пароли* Генерирование хэш-значения различным способом для каждого пользователя намного усложняет атаку со словарем: злоумышленник должен при подборе пароля каждого пользователя еще и подбирать способ хэширования пароля. Это достигается в системах с помощью использования меняющегося значения, называемого шумом. *Правила формата пароля* Такие правила могут требовать, чтобы пароль содержал как минимум одну цифру, как минимум один «специальный» символ, комбинации заглавных и строчных букв, и т.д.
Подбор пароля	
Исходя из знаний личных данных пользователя, злоумышленник пытается войти в систему с помощью имени пользователя и одного или нескольких паролей, которые он мог бы использовать (в том числе пароля, установленного по умолчанию).	*Правила формата пароля* Как для «атаки со словарем» выше. *Изменение пароля, установленного по умолчанию* Пароль, установленный по умолчанию, должен изменяться сразу после первого использования. По возможности следует вовсе исключить практику использования общеизвестных паролей. *Автоматическое блокирование* После нескольких безуспешных попыток

	входа система или блокирует учетную запись пользователя на некоторое время, или вовсе аннулирует ее.
Социотехника	
На пользователей: Злоумышленник представляется администратором и вынуждает пользователя или открыть свой пароль, или сменить его на указанный им пароль. *На администраторов*: Злоумышленник представляется законным пользователем и просит администратора заменить пароль для данного пользователя.	*Политика нераскрытия паролей* В организации должны быть разработаны административные процедуры, запрещающие сообщать пароли другим лицам при любых обстоятельствах. Организация должна также извещать пользователей о том, что администратор никогда не обратится к пользователю с таким требованием. *Политика смены паролей* В организации должна действовать политика, согласно которой администратор меняет пароль пользователя только при условии, что он может установить его личность и передать новый пароль пользователю безопасным способом. Средства самостоятельного управления паролями могут удовлетворять обоим критериям.
Принуждение	
Для того чтобы заставить пользователя открыть свой пароль, злоумышленник использует угрозы или физическое принуждение.	В некоторых системах предусматривается возможность для пользователя подавать сигнал о том, что вход осуществляется под принуждением. Обычно это реализуется с помощью специального пароля при входе в систему – пароль «вход под принуждением».
Подглядывание из-под плеча	
Расположенный рядом злоумышленник или видеокамера следит за тем, как пользователь вводит свой пароль.	*Неотображение пароля* В большинстве систем пароль либо не отображается на экране, либо отображается незначащими символами. В некоторых системах отображается количество таких символов, отличное от введенного. Вопреки этой технологии, злоумышленник может видеть, на какие непосредственно клавиши нажимает пользователь. Также применяются технологии, которые дают пользователю строго ограниченное время для ввода пароля, тем самым заставляя его вводить

	пароль максимально быстро. Таким образом, уменьшается вероятность его подсматривания, а также усложняется его подбор злоумышленником.
Троянский конь	
Злоумышленник скрытно устанавливает программное обеспечение, имитирующее обычный механизм аутентификации, но собирающее имена пользователей и пароли при попытках пользователей войти в систему.	*Антивирусное программное обеспечение* Организация может обнаруживать программы типа «троянский конь» с помощью антивирусного программного обеспечения. *Средства обеспечения контроля целостности файлов* В организации может использоваться система обнаружения вторжений для определения модификации важных файлов, например, программы регистрации.
Аппаратный сниффер клавиатуры	
Злоумышленник скрыто устанавливает в компьютер пользователя аппаратное средство, собирающее информацию, которую вводит пользователю при входе в систему, например, Keykeriki для беспроводных клавиатур, KeyCarbon, KeyDevil или KeyGhost для проводных клавиатур.	*Безопасность рабочих помещений* Служба безопасности компании должна предоставлять доступ в помещения, в которых располагаются компоненты информационной системы предприятия, только тем, кому он разрешен. *Безопасность рабочих мест* Служба безопасности компании должна обеспечить возможность контроля компонентов информационной системы предприятия для защиты от возможности установки в них незаконных аппаратных средств. Контроль над соответствующими компонентами информационной системы предприятия возлагается на сотрудников компании, службу ИТ или службу безопасности компании.
Трассировка памяти	
Злоумышленник использует программу для копирования пароля пользователя из буфера клавиатуры.	*Защита памяти* Некоторые ОС используют аппаратную защиту буферов клавиатуры от возможности ее трассировки.
Отслеживание нажатия клавиш программными средствами	
Для предотвращения использования компьютеров не по	*Безопасность файлов* Доступ на чтение к журналам должен быть

назначению некоторые организации используют программное обеспечение, следящее за нажатием клавиш. Злоумышленник может для получения паролей просматривать журналы соответствующей программы.	предоставлен лишь узкому кругу доверенных пользователей (администраторов) с помощью собственной или резидентной службы контроля доступа.
Регистрация излучения (перехват Ван Эка или фрикинг Ван Эка)	
Вим Ван Эк описал метод, которым злоумышленник может перехватывать информацию с монитора путем регистрации его излучения. Вин Швартау высказал идею приемников Ван Эка, регистрирующих не только видеосигналы.	*Неотображение пароля* Защита от данной атаки такая же как для «подглядывания из-за плеча» выше. *Безопасность излучений* Модернизация устройств для уменьшения излучения с помощью использования современных микрокомпонент, специально разработанных с учетом необходимости уменьшения излучения. Проектирование помещений и планирование расположения оборудования в нем с учетом предотвращения возможности утечки информации через паразитное излучение оборудования.
Анализ сетевого трафика	
Злоумышленник анализирует сетевой трафик, передаваемый от клиента к серверу, для восстановления из него имен пользователей и их паролей.	*Шифрование* Весь сетевой трафик или только пароли могут шифроваться для передачи по сети (использование протокола SSL или VPN-соединений). *Одноразовые пароли* Использование методов аутентификации, в которых пароли пользователей изменяются каждый раз при входе в систему.
Атака на «золотой пароль»	
Злоумышленник ищет пароли пользователя, применяемые им в различных системах – домашняя почта, игровые серверы и т.п. Есть большая вероятность того, что пользователь применяет один и тот же пароль во всех системах.	Шифрование Защита от данной атаки такая же как для атаки «анализ сетевого трафика». *Одноразовые пароли* Защита от данной атаки такая же как для атаки «анализ сетевого трафика».
Атака методом воспроизведения	
Злоумышленник записывает последовательность	*Использование надежных протоколов аутентификации*

передаваемых и получаемых субъектом доступа в процессе аутентификации данных. Позднее он осуществляет попытку аутентификации, передавая и получая записанные данные в той же последовательности.	Надежные протоколы аутентификации предполагают использование при обмене данными с субъектом доступа криптографически защищенных меток времени. *Одноразовые пароли* Защита от данной атаки такая же как для атаки «анализ сетевого трафика».

3.4. Аутентификация с помощью биометрических характеристик

Лицо является основным признаком, по которому производят удостоверение личности человека, когда проверяют его паспорт, водительские права, пропуск для доступа в организацию – все они содержат фотографию человека, предъявляющего данные документы.

Современные технологии способны обеспечить удостоверение личности человека, используя характерные только ему одному характеристики. Данные технологии основаны на использовании знаний биометрики (или биометрии). Данная дисциплина занимается статистическим анализом биологических наблюдений и явлений.

Биометрическая характеристика – это измеримая физиологическая или поведенческая черта живого человека, которую можно использовать для установления личности или проверки декларируемых личных данных.

Поскольку биометрический параметр уникален для данного человека, его можно использовать для однофакторной аутентификации пользователя. Его можно использовать совместно с паролем или с устройством аутентификации (например, таким, как смарт-карта) для обеспечения двухфакторной аутентификации.

Биометрическая аутентификация обычно является одним из наиболее простых методов для пользователей, которые должны проходить аутентификацию. В большинстве случаев хорошо спроектированная биометрическая система просто снимает показания с человека и правильно выполняет аутентификацию.

Биометрические характеристики делятся на физиологические и поведенческие.

Физиологические биометрические характеристики – биометрические характеристики на основе данных, полученных путем измерения анатомических характеристик человека.

К физиологическим биометрическим характеристикам можно отнести:

- радужную оболочку глаза;
- отпечаток пальца;
- лицо;

– кисть;
– сетчатку.

Поведенческие биометрические характеристики – биометрические характеристики на основе данных, полученных путем измерения действий человека.

Характерной чертой для поведенческих параметров является их протяженность во времени – измеряемое действие имеет начало, середину и конец.

К поведенческим биометрическим характеристикам можно отнести:

– голос;
– подпись;
– ритм работы сердца.

Различия между поведенческими и физиологическими характеристиками являются достаточно искусственными.

Поведенческие биометрические параметры зависят от физиологии: голос зависит от формы голосовых связок, подпись – от ловкости кисти и пальцев. Некоторые физиологические биометрические характеристики (например, лицо) могут изменяться в зависимости от возраста или поведения человека. Поведение человека (например, то, как он кладет палец или смотрит в камеру) может влиять на эффективность работы системы аутентификации.

Физиологические биометрические характеристики обычно неизменны в течение жизни человека. Использование этих характеристик для аутентификации обычно воспринимается как насильственное воздействие, часто как вмешательство в частную жизнь человека. Поведенческие биометрические характеристики воспринимаются менее болезненно, но они менее стабильны, чем физиологические черты. Они могут изменяться под влиянием стресса и болезни и в целом обеспечивают, по сравнению с физиологическими параметрами, менее качественную аутентификацию.

3.4.1 Принципы работы биометрических систем

Все биометрические системы работают одинаково (рис. 3.7). Пользователь предоставляет образец – опознаваемое, необработанное изображение или запись физиологической или поведенческой характеристики. С помощью регистрирующего устройства (например, сканера или камеры), этот биометрический образец обрабатывается для получения информации об отличительных признаках, в результате чего получается контрольный шаблон. Шаблоны представляют собой достаточно большие числовые последовательности; сам образец невозможно восстановить из шаблона. Контрольный шаблон и есть пароль пользователя.

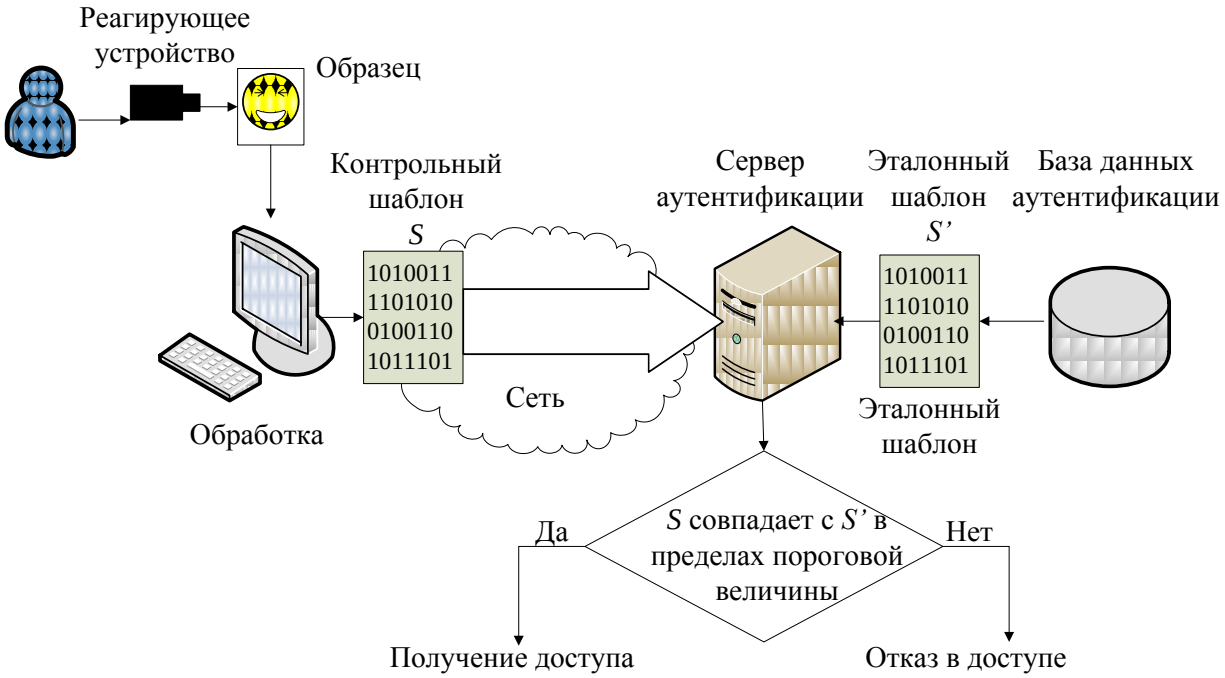


Рис. 3.7. Схема работы биометрической системы

Контрольный шаблон сравнивается с эталонным шаблоном (или зарегистрированным шаблоном), созданным на основе нескольких образцов определенной физиологической или поведенческой характеристики пользователя, взятых при его регистрации в биометрической системе. Поскольку эти два параметра (контрольный и эталонный шаблон) полностью никогда не совпадает, то биометрической системе приходится принимать решение о том, достаточно ли они совпадают. Степень совпадения должна превышать определенную настраиваемую пороговую величину.

Биометрические системы могут ошибаться, контрольный шаблон может быть ошибочно признан:

– соответствующим эталонному шаблону другого лица;

– несоответствующим эталонному шаблону данного пользователя, несмотря на то что этот пользователь зарегистрирован в биометрической системе.

Точность биометрической системы измеряется двумя параметрами:

– коэффициентом неверных совпадений (FMR), также известным под названием ошибка типа I или вероятность ложного допуска (FAR);

– коэффициентом неверных несовпадений (FNMR), также известным под названием ошибка типа II или вероятность ложного отказа в доступе (FRR).

Оба коэффициента отражают способность системы предоставлять ограниченный вход авторизованным пользователям. Системы с низким значением FMR более защищены, а системы с низким значением FNMR более просты в использовании. В общем случае для данных систем при задании пороговой величины действует правило: чем ниже FMR, тем выше FNMR. Таким образом, часто безопасность и простота использования конкурируют между собой.

Простота регистрации и качество шаблонов – важные факторы общей эффективности биометрической системы. Некачественный шаблон может

осложнить работу пользователя, вынуждая его прибегнуть к повторной регистрации в биометрической системе.

В режиме аутентификации биометрическая система проверяет заявленную личность, сверяя контрольный шаблон, сгенерированный из образца, с эталонным шаблоном (1:1 или сравнение один с одним). Для аутентификации необходимо, чтобы идентификатор личности был заявлен, например, вводом имени пользователя с клавиатуры, после чего контрольный шаблон данного лица сравнивается с эталонным шаблоном.

Некоторые системы аутентификации осуществляют очень ограниченный поиск среди многочисленного числа зарегистрированных записей. Например, пользователь с тремя эталонными шаблонами отпечатков пальцев может иметь возможность предоставить для проверки любой из трех пальцев, и система предпримет поиск совпадения 1:1 среди эталонных шаблонов данного пользователя.

Биометрическое распознавание – это процесс определения личности пользователя, состоящий из одного шага. В режиме распознавания система определяет личность пользователя, осуществляя сравнение контрольного шаблона со многими биометрическими эталонными шаблонами (1:N или сравнение один ко многим). В случае нахождения совпадения одновременно определяется и удостоверяется личность пользователя.

Биометрическая идентификация широко распространена и нашла применение в таких областях, как судебная медицина и деятельность правоохранительных органов.

В биометрических системах, работающих только в режиме аутентификации, возможно использование негативной идентификации в процессе регистрации пользователя в биометрической системе, когда один контрольный шаблон сравнивается со многими, чтобы проверить, что данное лицо не зарегистрировано в базе данных, и таким образом, предотвратить двойную регистрацию в системе. Этот режим часто используется в крупных программах по предоставлению социальных пособий, в которых пользователи пытаются регистрироваться несколько раз для получения пособий под разными именами.

Существует нечто среднее между аутентификацией и распознаванием – «сравнение один к нескольким» (1:few). Этот тип приложений предполагает идентификацию пользователя.

по очень маленькой базе зарегистрированных пользователей. Четкого количественного разграничения между системами 1:N и 1:few нет, но любую систему, в которой поиск осуществляется среди более чем 500 записей, следует относить к типу 1:N.

3.4.2 Реализация биометрических систем

Основные физиологические биометрические характеристики, а также виды их реализации приведены в табл. 3.4.

Табл. 3.4

Реализация физиологических биометрических характеристик

Биометрическая характеристика	Регистрирующее устройство	Образец	Исследуемые черты
Радужная оболочка глаза	Видеокамера, работающая в инфракрасном диапазоне, камера для компьютера	Черно-белое изображение радужной оболочки глаза	Полоски и бороздки в радужной оболочке глаза
Отпечаток пальца	Периферийное устройство настольного компьютера, карта стандарта PC card, мышь, микросхема или считыватель, встроенный в клавиатуру	Изображение отпечатка пальцев (оптическое, на кремниевом фото-приемнике, ультразвуковое, или бесконтактное)	Расположение и направление гребешковых выступов и разветвлений на отпечатке пальцев, мелкие детали
Лицо	Видеокамера, камера для ПК, цифровой фотоаппарат	Изображение лица (оптическое, двумерное 2D-фото или трехмерное 3D-фото)	Форма черепа, относительное расположение и форма носа, расположение скул
Кисть	Настенное устройство	Трехмерное изображение верха и боков кисти	Высота и ширина костей и суставов кисти и пальцев
Сетчатка	Настольное или настенное устройство	Изображение сетчатки	Расположение кровеносных сосудов на сетчатке

В стадии разработки находятся новые биометрические технологии, связанные с другими физиологическими характеристиками:

Сравнение ДНК – это самая совершенная биометрическая технология, дающая прямое доказательство идентичности личности (кроме однояйцевых близнецов, у которых одинаковый генотип). Этот метод иногда называется дактилоскопией

ДНК, что сбивает с толку и вводит в заблуждение, поскольку отпечатки пальцев не «проникают до уровня генома». Биометрические системы, основанные на сравнении ДНК, могут быть введены в действие лишь через много лет.

Отпечаток ладони – в этой системе используется расположение линий на ладони человека, также, как в биометрической технологии, использующей отпечатки пальцев.

Сосудистые рисунки – расположение вен в различных частях тела человека, включая запястье и тыльную сторону ладони, а также лицо.

Сигналы, вырабатываемые сердцем (мозгом, легкими), – в этой системе пользователь прикасается к датчику биодинамической подписи и остается с ним в контакте некоторое время (в зависимости от точности измерения – до 8 с). За это время датчик идентифицирует индивидуальные параметры человека.

3.4.3 Поведенческие биометрические характеристики

Основные поведенческие биометрические характеристики, а также виды их реализации приведены в табл. 3.5.

Табл. 3.5

Реализация поведенческих биометрических характеристик

Биометрическая характеристика	Регистрирующее устройство	Образец	Исследуемые черты
Голос	Микрофон, телефон	Запись голоса	Частота, модуляция и продолжительность голосового образа
Подпись	Планшет для подписи, перо для ввода данных	Изображение подписи и показания соответствующих динамических измерений	Скорость, порядок линий, давление и внешний вид подписи
Динамика нажатия клавиш	Клавиатура	Ритм машинописи	Время задержки (время удержания клавиши) время «полета» (время, перехода с одной клавиши на другую)

3.4.4 Атаки на биометрические системы

В табл. 3.3 приведены известные методы атак на системы, использующие аутентификацию с помощью биометрических характеристик, а также способы защиты от подобных атак.

К недостаткам аутентификации с помощью биометрических характеристик можно отнести следующие:

Вмешательство в частную жизнь. Пользователям-клиентам в большей степени, чем пользователям-сотрудникам организаций, небезразличен факт хранения и распространения их биометрических данных. Если в организации устроено централизованное хранилище биометрических параметров,

пользователи, не имея возможности контролировать распространение этих данных, опасаются:

злоупотреблений (например, незаконного обмена с другими организациями);

нецелевого использования (подмены функции).

Личные, культурные и религиозные аспекты. Дактилоскопические системы вызывают неприятие у пользователей, которые считают, что их использование бросает на них тень преступного свойства, поскольку отпечатки пальцев, как известно, применяются в криминалистике.

Возникают также вопросы гигиены (будет ли прибор, регистрирующий геометрию руки, обрабатываться антисептическим раствором после каждого использования?) и травмоопасности (например, в системах сканирования сетчатки, в которых свет направляется в глаз), а также осознание того факта, что пользователи подвергаются риску причинения вреда со стороны преступников – от копирования или использования объектов

Атаки на биометрические системы и защита от них приведены в табл. 3.6.

Табл. 3.6

Описание атаки	Защита от данной атаки
Подделка отличительной черты	
Злоумышленник изготавливает копию физической отличительной черты законного пользователя и предъявляет эту копию биометрическому датчику.	*Снятие показателей с высоким уровнем детализации* При изготовлении эталонного шаблона с законного пользователя снимают дополнительные биометрические показатели, так что простая копия физической отличительной черты законного пользователя не будет отражать все ее параметры.
Воспроизведение поведения пользователя	
Злоумышленник записывает поведенческую отличительную черту пользователя и воспроизводит на биометрическом датчике.	*Изменяемое поведение* При каждой попытке аутентификации система требует от пользователя различного проявления его поведенческой биометрической характеристики, так что просто ее запись и воспроизведение не будут приниматься.
Перехват биометрических показателей	
Злоумышленник перехватывает биометрические показатели законного пользователя в момент их передачи	*Шифрование биометрических данных* Биометрические данные шифруются сразу после их получения

между устройствами.	от пользователя устройством считывания, их передача между устройствами осуществляется только в шифрованном виде.
Воспроизведение биометрической «подписи»	
Злоумышленник воспроизводит показатель биометрического датчика – «подпись», которая далее обрабатывается системой так, словно была получена от реального человека.	*Аутентификация биометрической «подписи»* Меры аутентификации принимаются в отношении биометрических данных, чем гарантируется их поступление только из заслуживающих доверия источников. Использование ЭЦП для обеспечения целостности биометрической «подписи».

3.5 Аутентификация на основе OTP-токена

Одноразовые пароли (OTP, One-Time Passwords) – динамическая аутентификационная информация, генерируемая для единичного использования с помощью аутентификационных устройств (программных или аппаратных).

Одноразовый пароль (OTP) неуязвим для атаки методом анализа сетевого трафика, что является значительным преимуществом перед запоминаемыми паролями. Несмотря на то, что злоумышленник может перехватить пароль методом анализа сетевого трафика, поскольку пароль действителен лишь один раз и в течение ограниченного промежутка времени, у злоумышленника в лучшем случае есть весьма ограниченная возможность представиться пользователем с помощью перехваченной информации.

В качестве возможных устройств для генерации одноразовых паролей обычно используются OTP-токены.

OTP-токен – мобильное персональное устройство, которое принадлежит определенному пользователю и генерирует одноразовые пароли, используемые для аутентификации данного пользователя.

Таким образом, аутентификация с помощью одноразовых паролей, по сравнению с аутентификацией на основе пароля, является аутентификацией с помощью другого фактора аутентификации – аутентификацией «на основе обладания чем-либо».

Другим важным преимуществом применения аутентификационных устройств является то, что многие из них требуют от пользователя введения PIN-кода:

для активации OTP-токена;

в качестве дополнительной информации, используемой при генерации OTP;

для предъявления серверу аутентификации вместе с OTP.

Если дополнительно применяется еще и PIN-код, в методе аутентификации используются два фактора аутентификации, то есть данный метод относится к двухфакторной аутентификации.

Простейшей схемой применения одноразовых паролей служит разделяемый список.

В этом случае пользователь и проверяющий применяют последовательность секретных паролей, где каждый пароль используется только один раз.

Естественно данный список заранее распределяется между сторонами аутентификационного обмена.

Такая схема применяется в настоящее время в некоторых системах «Интернет-банк».

Модификацией этого метода является таблица вопросов и ответов, которая содержит вопросы и ответы, используемые сторонами для проведения аутентификации, причем каждая пара используется только один раз. Существенным недостатком этой схемы является необходимость предварительного распределения аутентифицирующей информации. После того как выданные пароли закончатся, пользователю необходимо получить новый список. Такое решение, во-первых, не удовлетворяет современным представлениям об информационной безопасности, поскольку злоумышленник может украсть или скопировать список паролей пользователя. Во-вторых, постоянно получать новые списки паролей вряд ли кому-нибудь понравится.

Вместе с тем, в настоящее время разработано несколько методов реализации технологии одноразовых паролей, исключающих указанные недостатки. В их основу легли различные криптографические алгоритмы.

Аппаратно-программные OTP-токены

OTP-токены имеют небольшой размер и выпускаются в виде:

– карманного калькулятора;
– брелока;
– смарт-карты;
– устройства, комбинированного с USB-ключом;
– специального программного обеспечения для карманных компьютеров, смартфонов, настольных компьютеров.

Для генерации одноразовых паролей OTP-токены используют хэш-функции или криптографические алгоритмы:

симметричная криптография (криптография с одним ключом) – в этом случае пользователь и сервер аутентификации используют один и тот же секретный ключ;

асимметричная криптография (криптография с открытым ключом) – в этом случае в устройстве хранится закрытый ключ, а сервер аутентификации использует соответствующий открытый ключ.

Существуют различные комбинации использования данных криптографических алгоритмов в реализациях OTP-токенов.

Соответственно механизмы аутентификации, используемые OTP-токенами, можно разделить на две группы:

аутентификация с одним секретным ключом,

аутентификация с открытым ключом.

Обычно в OTP-токенах применяется симметричная криптография. Устройство каждого пользователя содержит уникальный персональный секретный ключ, используемый для шифрования некоторых данных (в зависимости от реализации метода) для генерации OTP. Этот же ключ хранится на сервере аутентификации, который выполняет аутентификацию данного пользователя. Сервер шифрует те же данные и сравнивает два результата шифрования: полученный им и присланный от клиента. Если результаты совпадают, то пользователь успешно проходит аутентификацию.

OTP-токены, использующие симметричную криптографию, могут работать в асинхронном или синхронном режиме. Соответственно методы, используемые OTP-токенами, можно разделить на две группы, работающие:

в асинхронном режиме («запрос-ответ»);

в синхронном режиме («только ответ», «синхронизация по времени», «синхронизация по событию»).

3.5.1 .Метод «запрос–ответ»

В методе «запрос–ответ» OTP является ответом пользователя на случайный запрос от сервера аутентификации (рис. 3.8).

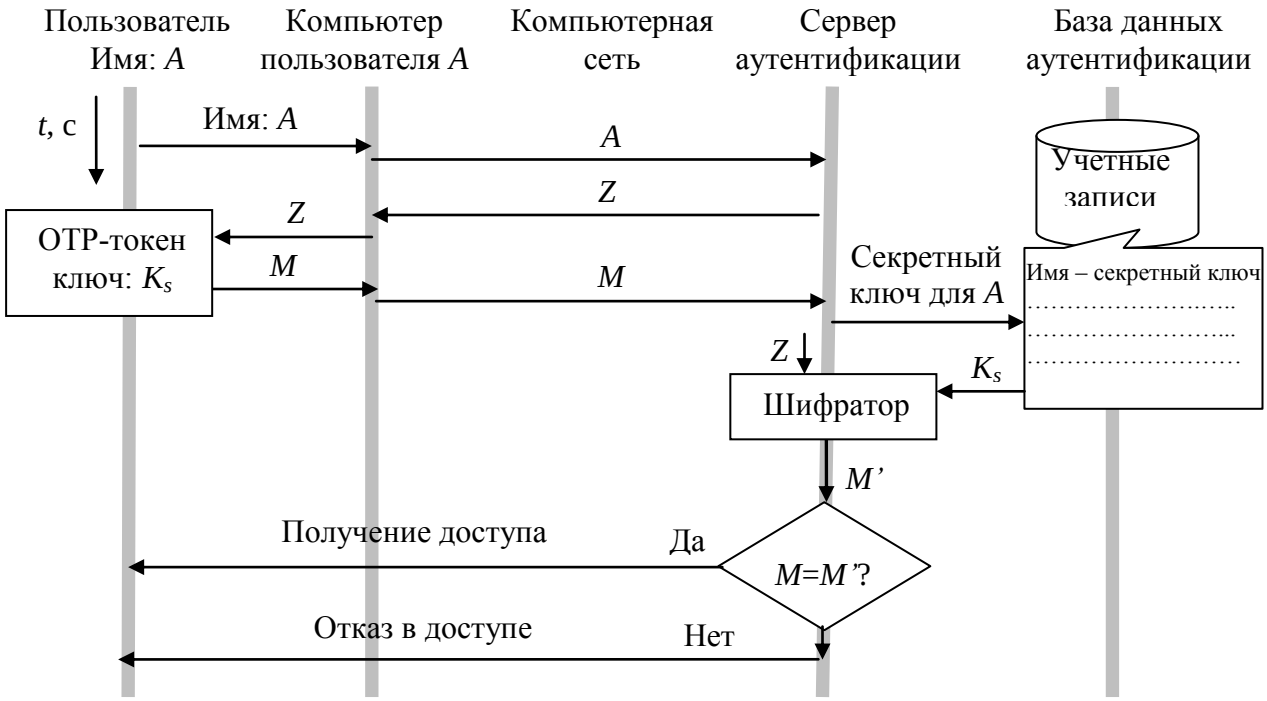


Рис. 3.8. Схема работы метода «Запрос-Ответ»

Пример аутентификации пользователя при использовании OTP-токеном метода «запрос–ответ»:

1. Пользователь вводит свое имя пользователя *A* на рабочей станции.

2. Имя пользователя передается по сети в открытом виде.

3. Сервер аутентификации генерирует случайный запрос *Z*, например, Z=31415926.

4. Запрос *Z* передается по сети в открытом виде.

5. Пользователь вводит запрос *Z* в свой OTP-токен.

6. OTP-токен шифрует запрос *Z* с помощью секретного ключа пользователя K_s, например, K_s=cft6yhnj, в результате получается ответ *M*, например, *M*=27182818, который отображается на экране OTP-токена.

7. Пользователь вводит этот ответ на рабочей станции.

8. Ответ передается по сети в открытом виде.

9. Аутентификационный сервер находит запись пользователя в базе данных аутентификации и с помощью хранимого им секретного ключа K_s пользователя зашифровывает тот же запрос *Z*. Пусть в результате шифрования получен ответ *M'*.

10. Сервер сравнивает представленный ответ от пользователя *M* с вычисленным им самим ответом *M'*.

11. При совпадении значений аутентификация считается успешной.

3.5.2 Метод «только ответ»

В методе «только ответ» аутентификационное устройство и сервер аутентификации генерируют «скрытый» запрос *Z*, используя значения предыдущего запроса *R*. Для начальной инициализации данного процесса используется уникальное случайное начальное значение, генерируемое при инициализации OTP-токена.

Пример аутентификации пользователя при использовании OTP-токеном метода «только ответ» (рис. 3.9):

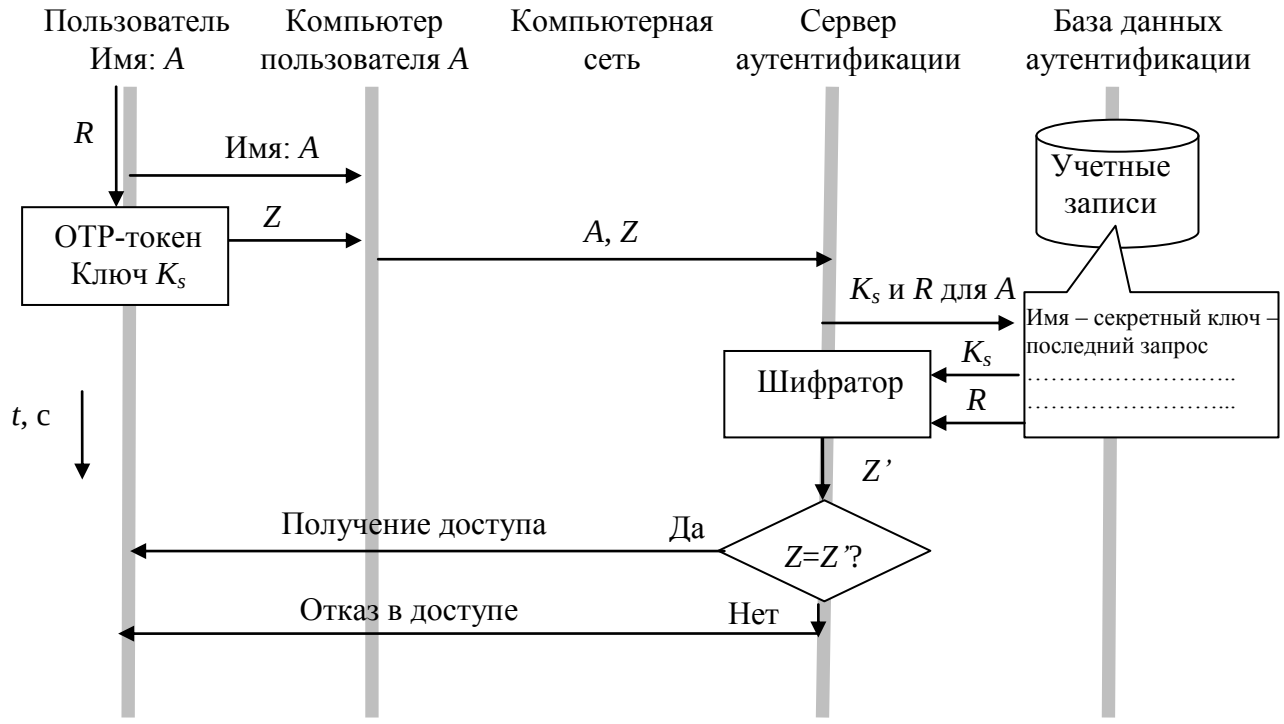


Рис. 3.9. Схема работы метода «только ответ»

1. Пользователь активизирует свой ОТР-токен, который вычисляет и отображает ответ Z на «скрытый» запрос R (R – значение предыдущего запроса, которое хранится в ОТР-токене).

2. Пользователь вводит свое «имя пользователя» A и этот ответ Z, например Z=66260689 на рабочей станции.

3. Имя пользователя и ответ (A и Z) передаются по сети в открытом виде.

4. Сервер находит запись пользователя, генерирует такой же скрытый запрос R и шифрует его с помощью секретного ключа пользователя K_s, получая ответ Z' на свой запрос.

5. Сервер сравнивает представленный ответ от пользователя Z с вычисленным им самим ответом Z'.

6. При совпадении значений аутентификация считается успешной.

3.5.3. Метод «Синхронизация по времени»

В режиме «синхронизация по времени» аутентификационное устройство и аутентификационный сервер генерируют ОТР на основе значения внутренних часов. ОТР-токен может использовать не стандартные интервалы времени, измеряемые в минутах, а специальные интервалы времени обычно равные 30 с.

Пример аутентификации пользователя при использовании ОТР-токеном метода «синхронизация по времени» (рис. 3.10):

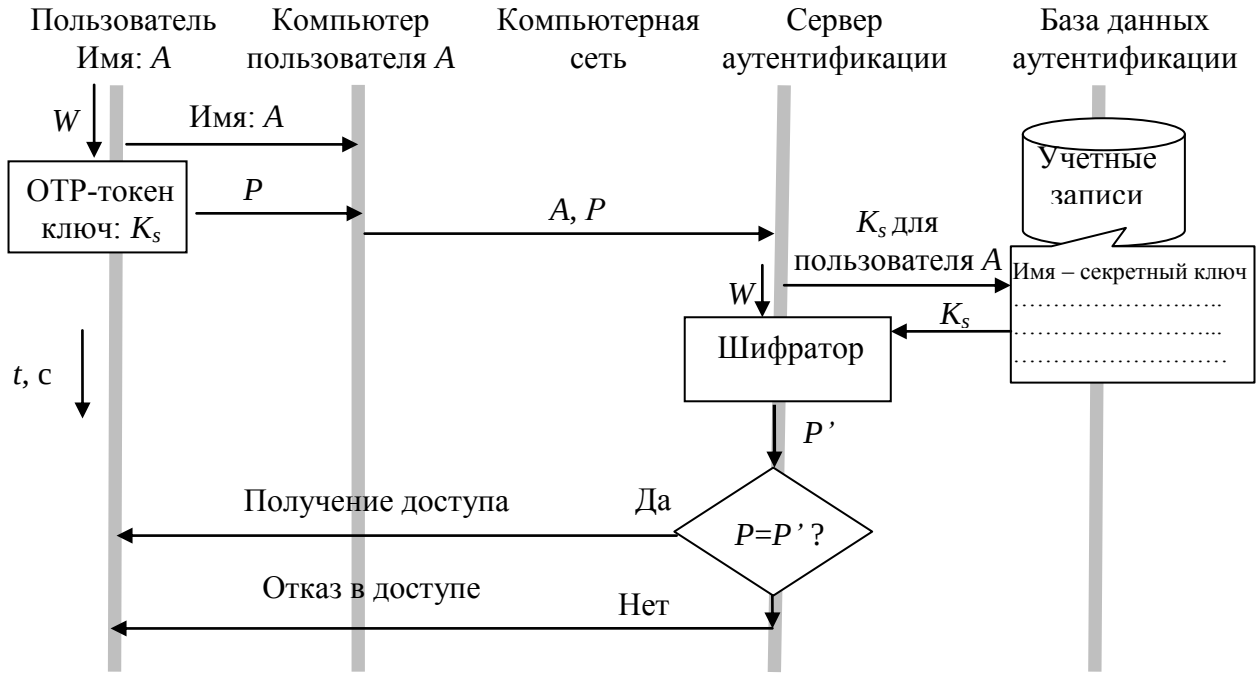


Рис. 3.10. Схема работы метода «Синхронизация по времени»

1. Пользователь активизирует свой ОТР-токен, который генерирует одноразовый пароль *P* (ОТР=*P*), например *P*=96823030. Значение *P* является результатом шифрования показания часов *W* на секретном ключе пользователя K_s.

2. Пользователь вводит свое «имя пользователя», например *A* и этот ОТР *P* на рабочей станции.

3. Имя пользователя и ОТР (*A* и *P*) передаются по сети в открытом виде.

4. Аутентификационный сервер находит запись пользователя и шифрует показание своих часов *W* с помощью хранимого им секретного ключа пользователя K_s, получая в результате ОТР *P'*.

5. Сервер сравнивает ОТР *P*, представленный пользователем, и ОТР *P'*, вычисленный им самим.

6. При совпадении значений *P* и *P'* аутентификация считается успешной.

3.5.4. Метод «синхронизация по событию»

В режиме «синхронизация по событию» ОТР-токен и сервер аутентификации ведут количественный учет прохождения аутентификации данным пользователем, и на основе этого числа генерируют ОТР.

Пример аутентификации пользователя при использовании ОТР-токеном метода «синхронизация по событию» (рис. 3.11):

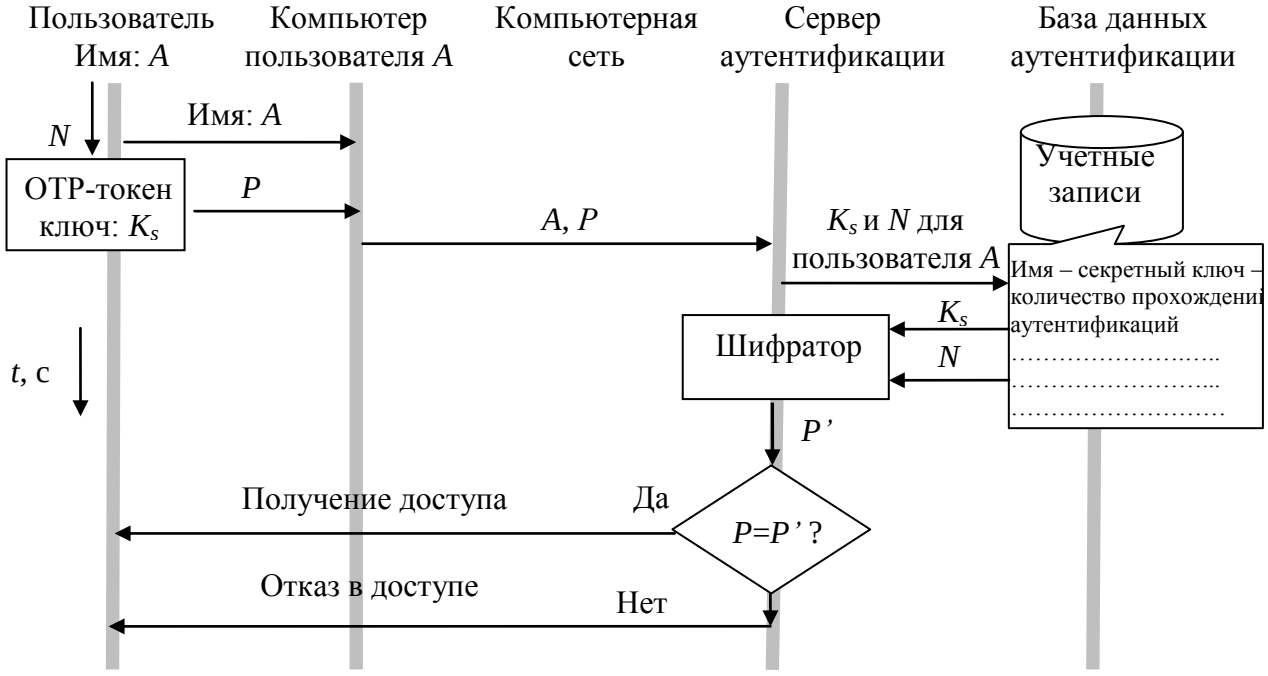


Рис. 3.11. Схема метода «Синхронизация по событию»

1. Пользователь с именем *A* активизирует свой ОТР-токен, который генерирует одноразовы пароль *P* (ОТР=*P*), например *P* =59252459. Значение *P* генерируется в ОТР-токене автоматически, которое является результатом шифрования количества *N* прохождений аутентификации данного пользователя на секретном ключе K_s.

2. Пользователь вводит свое «имя пользователя» *A* и этот ОТР *P* на рабочей станции.

3. Имя пользователя и ОТР (*A* и *P*) передаются по сети в открытом виде.

4. Аутентификационный сервер находит запись пользователя и шифрует значение количества прохождений аутентификации данного пользователя с помощью хранимого им секретного ключа пользователя K_S, получая в результате ОТР, например *P'*.

5. Сервер сравнивает ОТР *P*, представленный пользователем, и ОТР *P'*, вычисленный им самим.

6. При совпадении значений *P* и *P'* аутентификация считается успешной.

Некоторые ОТР-токены могут использовать несколько различных методов реализации аутентификации с помощью ОТР. Наиболее часто комбинируются методы «синхронизация по времени» и «синхронизация по событию».

Сравним рассмотренные методы ОТР-аутентификации.

Метод «запрос–ответ», работающий в асинхронном режиме, предполагает большее количество шагов, совершаемых пользователем, чем любой из синхронных режимов.

Потенциальная проблема всех методов реализации аутентификации с помощью ОТР, работающих в синхронном режиме, – возможность рассинхронизации ОТР-токена и сервера, например:

в режимах «только ответ» или «синхронизации по событию» сбой при аутентификации может привести к «отставанию» сервера от аутентификационного устройства;

в режиме «синхронизации по времени» часы аутентификационного устройства могут уйти вперед или отстать от часов сервера.

При аутентификации с помощью ОТР-токенов, как правило, предусматривается вариант решения проблемы рассинхронизации: сервер генерирует несколько возможных вариантов ОТР – «ответов» от пользователя за некоторый короткий промежуток времени (для нескольких событий или единиц измерения времени).

3.6. Межсетевые экраны

Проблема защиты от несанкционированных действий при взаимодействии с внешними сетями успешно может быть решена с помощью специализированных программно-аппаратных комплексов, обеспечивающих целостную защиту компьютерной сети от потенциально враждебной внешней среды. Такие комплексы называют межсетевыми экранами, брандмауэрами или системами Firewall.

Межсетевой экран – это система межсетевой защиты, позволяющая разделить каждую сеть на две и более части и реализовать набор правил, определяющих условия прохождения пакетов данных через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Internet, хотя ее можно провести и внутри корпоративной сети предприятия.

Использование межсетевых экранов позволяет организовать внутреннюю политику безопасности сети предприятия, разделив всю сеть на сегменты, что позволяет сформулировать основные принципы архитектуры безопасности корпоративной сети:

1) Введение N категорий секретности и создание N выделенных сетевых сегментов пользователей. При этом каждый пользователь внутри сетевого сегмента имеет одинаковый уровень секретности (допущен к информации одного уровня секретности).

2) Выделение в отдельный сегмент всех внутренних серверов компании. Эта мера также позволяет изолировать потоки информации между пользователями, имеющими различные уровни доступа.

3) Выделение в отдельный сегмент всех серверов компании, к которым будет предоставлен доступ из Интернета (создание демилитаризованной зоны для внешних ресурсов).

4) Создание выделенного сегмента административного управления.

5) Создание выделенного сегмента управления безопасностью.

Для противодействия несанкционированному межсетевому доступу брандмауэр должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис. 3.12). При этом все взаимодействия между этими сетями должны осуществляться только через межсетевой экран. Организационно экран входит в состав защищаемой сети.

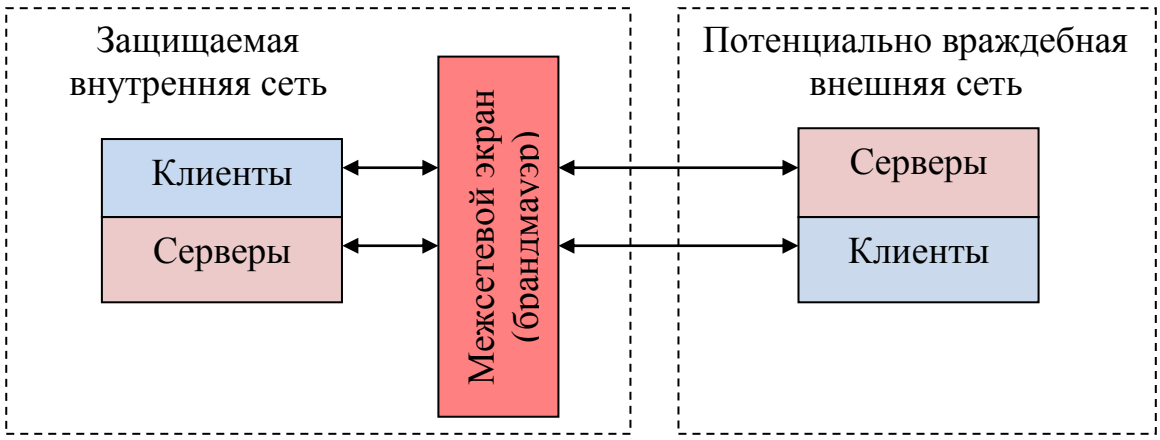


Рис. 3.12. Схема подключения межсетевого экрана

Межсетевой экран 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:

1) фильтрации проходящих через него информационных потоков;

2) 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.

Фильтрация состоит в выборочном пропускании информационных потоков через экран и извещением отправителя о том, что его данным в пропуске отказано (рис. 3.13).

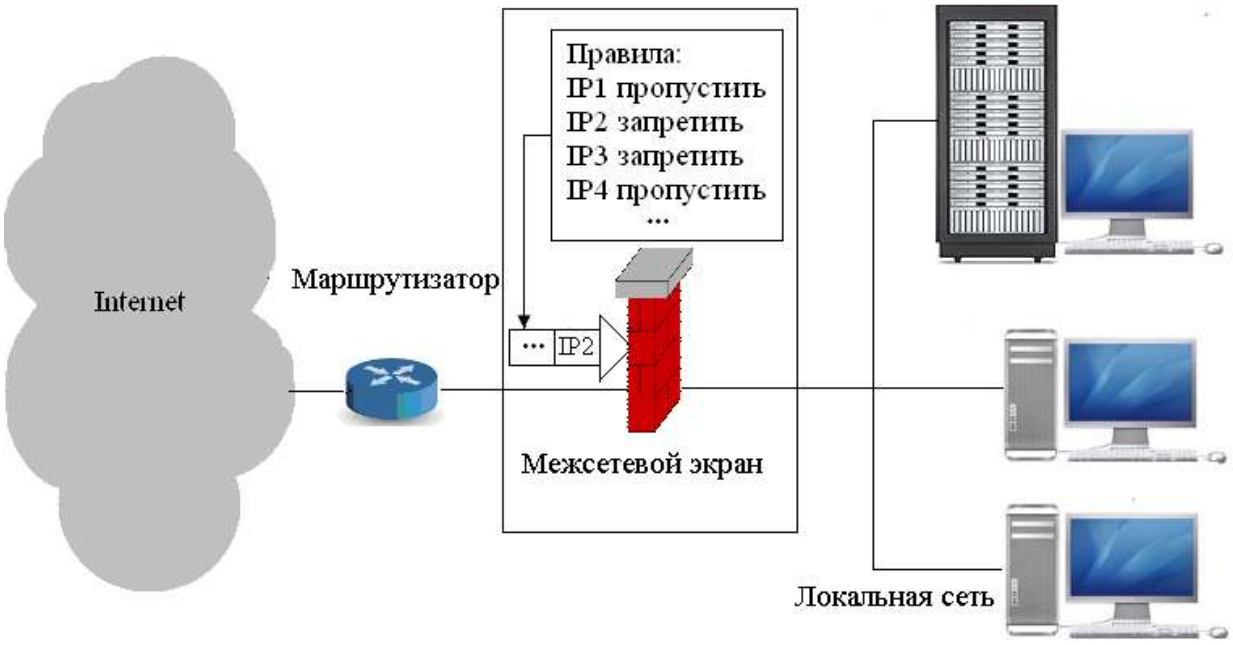


Рис. 3.13. Функция фильтрации, реализованная в межсетевом экране

Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся по своей сути принятой политикой безопасности. Для реализации этой функции Межсетевой экран представляется как последовательность фильтров, обрабатывающих информационный поток (рис.3.14).

Каждый из фильтров предназначен для отдельных правил фильтрации путем выполнения следующих стадий:

1) анализ фильтруемых данных по заданным в правилах политики безопасности критериям, например, по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена;

2) принятие на основе правил принятой политики безопасности одного из следующих решений:

a) не пропустить данные;
b) обработать данные от имени адресата (получателя) и возвратить результат отправителю;
c) передать данные на следующий фильтр для продолжения анализа;
d) пропустить данные, игнорируя следующие фильтры («переброс» данных).

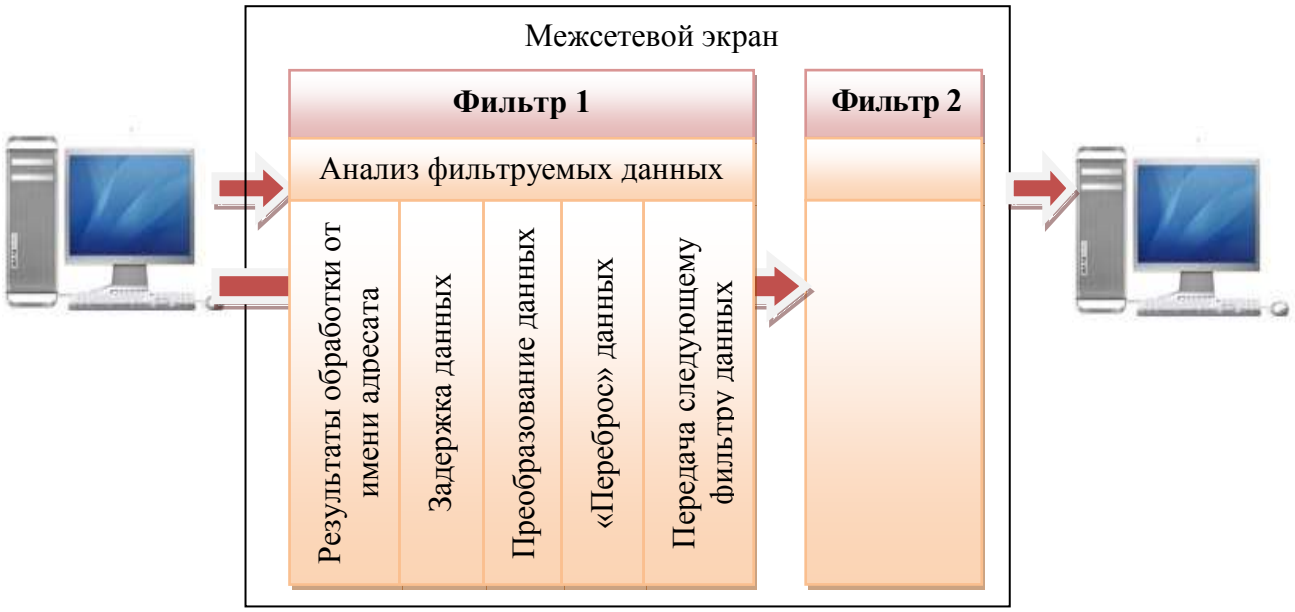


Рис. 3.14. Межсетевой экран как последовательность фильтров

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.

К функциям посредничества в общем случае относятся:

1) *Идентификация и аутентификация пользователей.*

Для высокой степени безопасности необходима идентификация и аутентификация пользователей не только при их доступе из внешней сети во внутреннюю сеть, но и наоборот. Пароль не должен передаваться в открытом виде через общедоступные коммуникации. Оптимальным способом аутентификации является использование одноразовых паролей. Удобно и надежно также применение цифровых сертификатов, выдаваемых доверительными органами, например центром распределения ключей. Большинство программ-посредников разрабатываются 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.

2) *Проверка подлинности передаваемых данных.*

Программы-посредники могут осуществлять проверку подлинности получаемых и передаваемых данных. Это актуально 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 проверке их цифровых подписей. Для этого также могут применяться цифровые сертификаты.

3) *Разграничение доступа к ресурсам внутренней сети.*

Идентификация и аутентификация пользователей при обращении к межсетевому экрану позволяет разграничить их доступ 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 м межсетевого экрана и полный запрет доступа во внешнюю сеть.

4) *Фильтрация и преобразование потока сообщений.*

Под функциями фильтрации и преобразования потока сообщений понимается, например, динамический поиск вирусов и прозрачное шифрование информации.

Фильтрация и преобразование потока сообщений выполняется посредником на основе заданного набора правил.

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.

5) *Трансляция внутренних сетевых адресов для исходящих пакетов сообщений.*

Программы-посредники могут выполнять и такую важную функцию, как трансляцию 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 межсетевым экраном, 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 межсетевого экрана становится единственным активным IP-адресом, который попадает во внешнюю сеть.

Технология заключается в том, что на межсетевом экране, который играет роль маршрутизатора, при выходе во внешнюю сеть во всех сетевых пакетах производится подмена внутреннего адреса на предопределенный внешний адрес. При этом маршрутизатор ведет таблицу соответствия отправленных пакетов таким образом, что для входящих пакетов из внешней сети производится обратная замена внешнего адреса на внутренний (рис. 3.15).

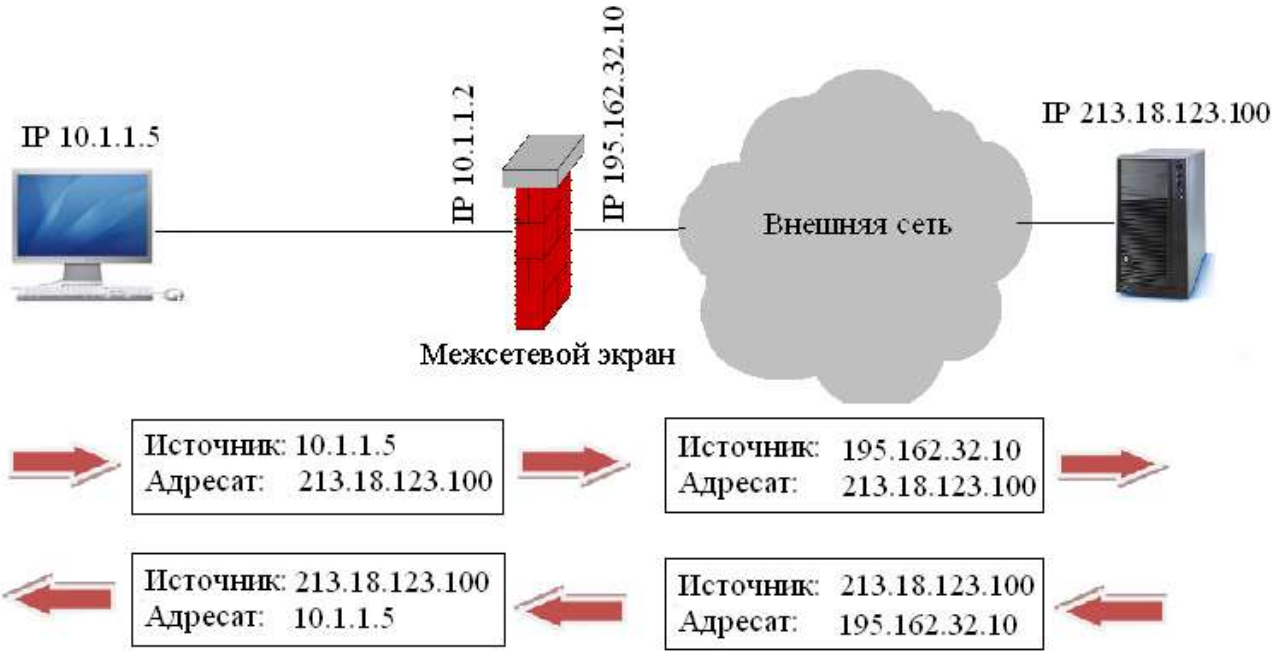


Рис. 3.15. Трансляция адресов на межсетевом экране

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа.

6) *Регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов.*

В качестве обязательной реакции на обнаружение попыток выполнения несанкционированных действий должно быть определено уведомление администратора, то есть выдача предупредительных сигналов. Любой брандмауэр, который не способен посылать предупредительные сигналы при обнаружении нападения, не является эффективным средством межсетевой защиты.

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

7) *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 перешлет ее без обращения к внешней сети, что существенно ускоряет доступ. Администратору следует позаботиться только о периодическом обновлении содержимого proxy-сервера.

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.

Для подключения межсетевых экранов используются различные схемы. Для подключения к внешней сети межсетевой экран может быть использован в качестве внешнего маршрутизатора (рис. 3.16).

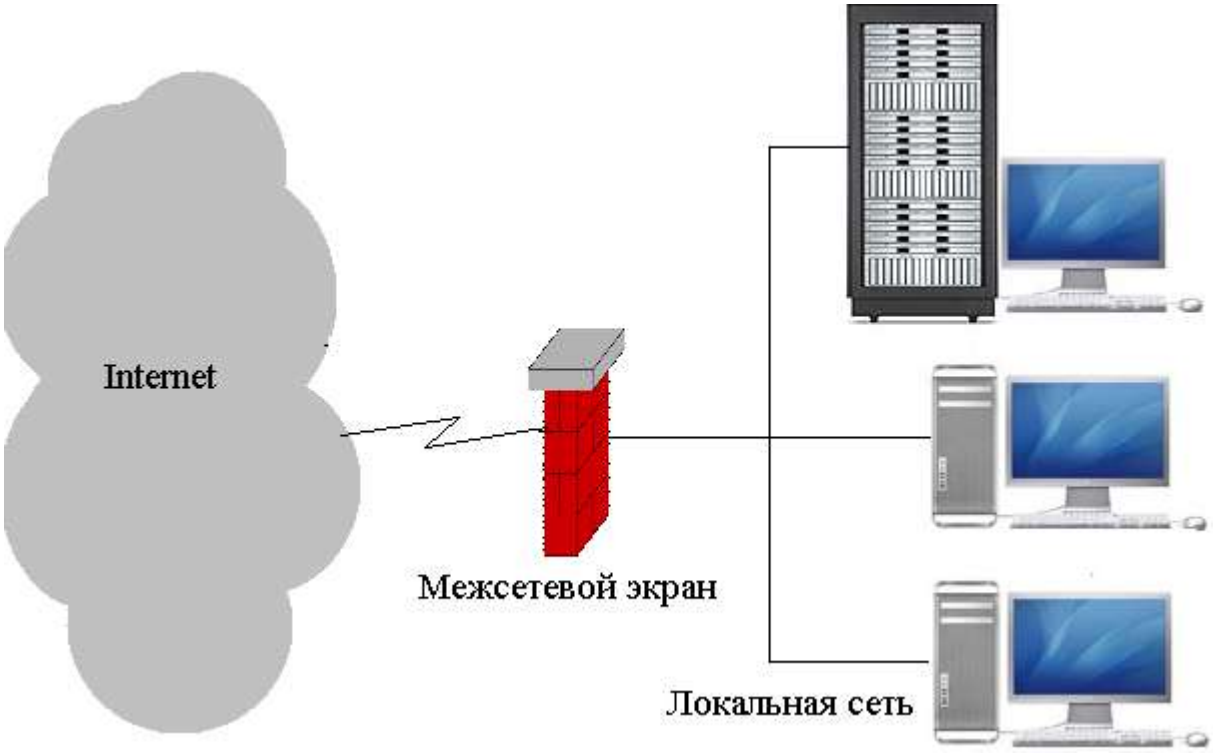


Рис. 3.16. Межсетевой экран с функциями маршрутизатора

Иногда находит применение схема, изображенная на рис. 3.17, однако использовать ее следует только в крайнем случае, поскольку требуется очень аккуратная настройка маршрутизаторов и небольшие ошибки могут образовать серьезные бреши в защите.

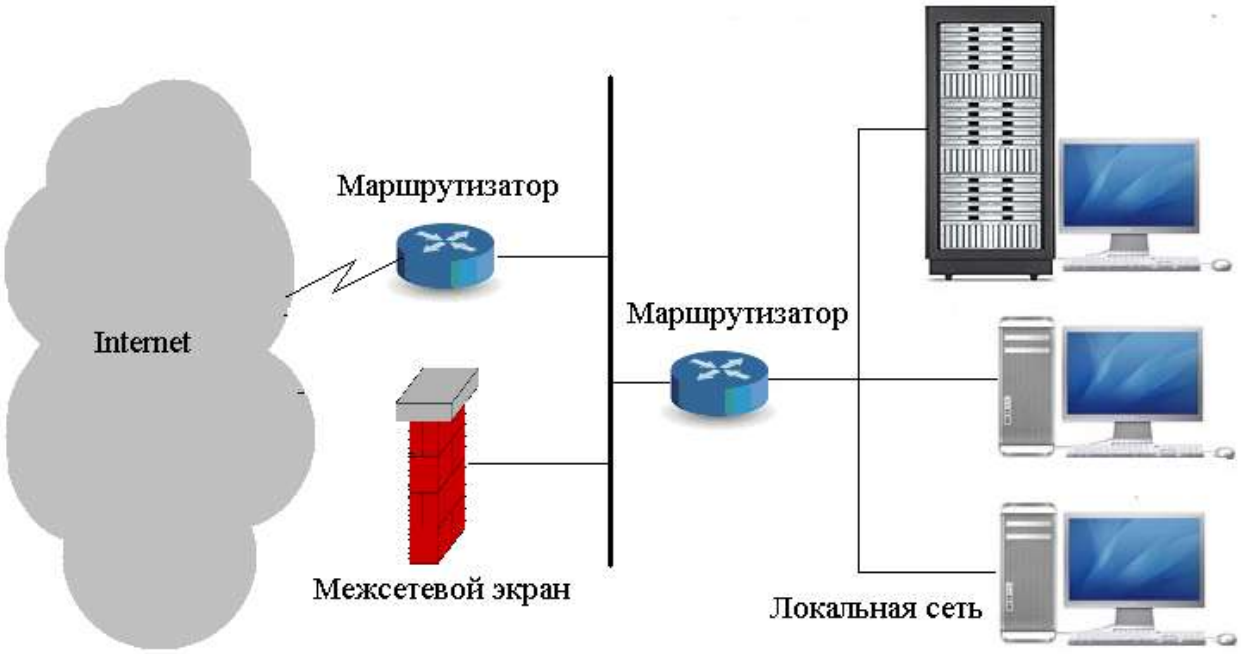


Рис. 5.17. Вариант подключения межсетевого экрана

Если межсетевой экран может поддерживать два Ethernet интерфейса (так называемый dual-homed брандмауэр), то чаще всего подключение осуществляется через внешний маршрутизатор (рис. 3.18).

При этом между внешним маршрутизатором и межсетевым экраном имеется только один путь, по которому идет весь трафик. Обычно маршрутизатор настраивается таким образом, что брандмауэр является единственной видимой снаружи машиной. Эта схема является наиболее предпочтительной с точки зрения безопасности и надежности защиты.

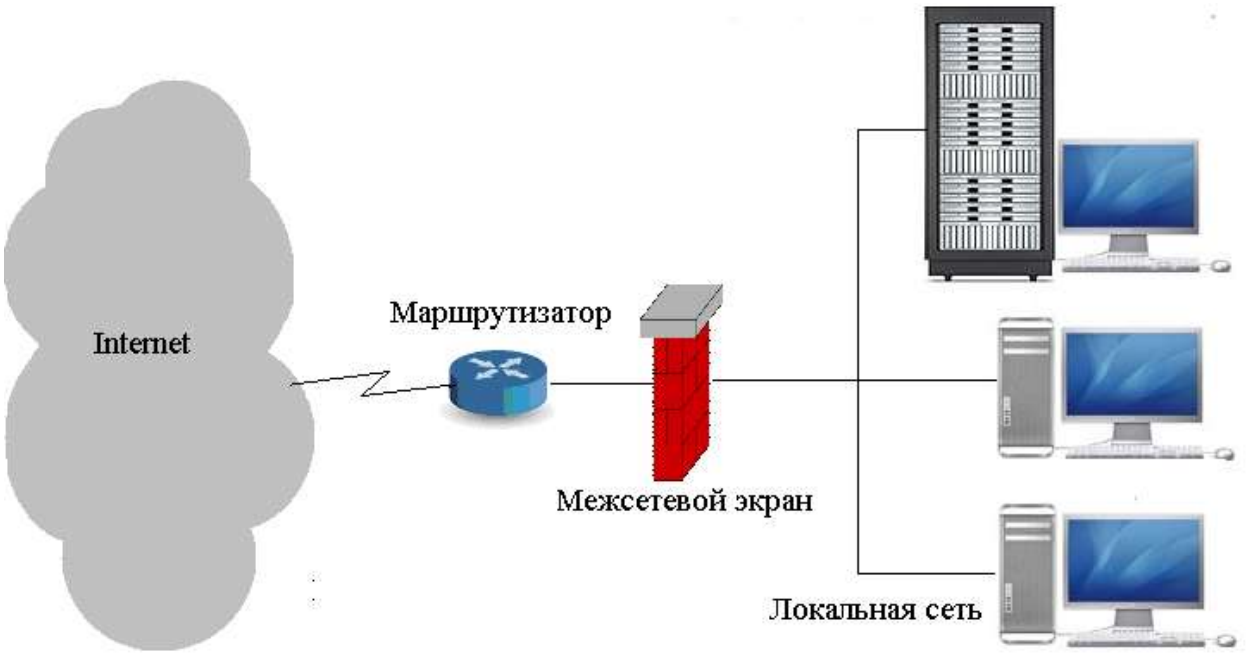


Рис. 3.18. Схема подключения межсетевого экрана, поддерживающего два Ethernet интерфейса

Другая схема представлена на рис. 3.19. В этом варианте межсетевым экраном защищается только одна подсеть из нескольких выходящих из маршрутизатора. В незащищаемой межсетевым экраном области часто располагают серверы, которые должны быть видимы снаружи (WWW, FTP и т.д.). Некоторые производители межсетевых экранов предлагают разместить эти сервера на самом брандмауэре. Такие решения не являются рациональными с точки зрения загрузки машины и безопасности межсетевого экрана.

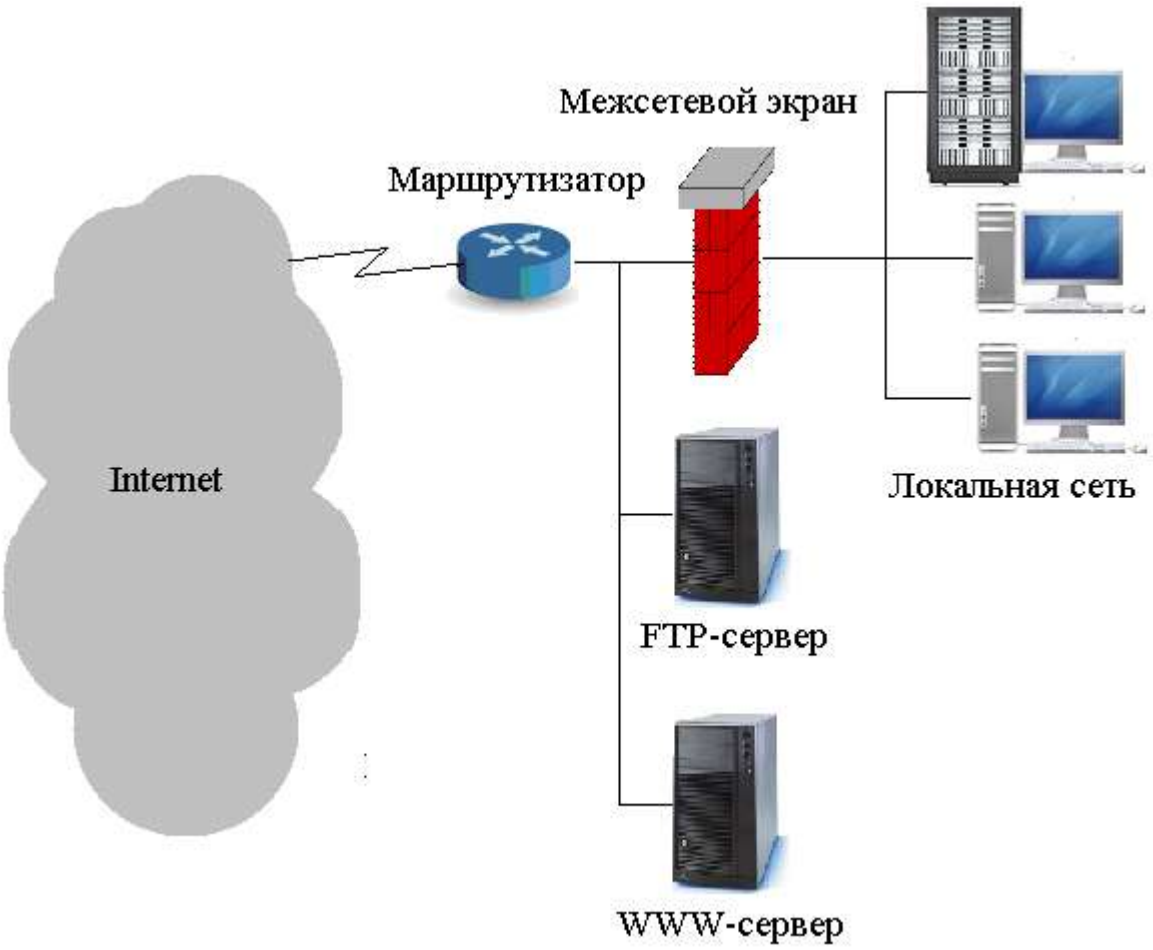


Рис. 3.19. Межсетевой экран защищает только локальную сеть предприятия

Современное развитие бизнеса предполагает, что внутренние ресурсы организации не должны быть полностью закрыты. Ряд узлов, таких как WWW-сервер, FTP-сервер, почтовый сервер, должны быть в той или иной степени доступны для внешних пользователей, в том числе для тех, о ком нет никакой предварительной информации. Возникает вопрос, где размещать такие узлы. Если во внешней сети, перед межсетевым экраном, это значит, что их защищенность будет зависеть только от схемы безопасности операционной системы и приложения, что, как показывает опыт, недостаточно. Если разместить их во внутренней сети, за межсетевым экраном, то тогда придется пропускать внешних пользователей во внутреннюю сеть, а это всегда небезопасно, даже при точной настройке правил доступа. Вполне логично напрашивается вывод – создать для подобных ресурсов отдельную подсеть, свободную от элементов внутренней и

внешней сети. Данная технология получила название демилитаризованной зоны (ДМЗ).

Поскольку обычно межсетевые экраны имеют по два сетевых интерфейса (один во внутреннюю и один во внешнюю сети), то для ДМЗ необходим третий сетевой интерфейс. Отдельные правила, прописанные на межсетевом экране для доступа в ДМЗ, позволят, с одной стороны, обеспечить защиту корпоративных ресурсов, а с другой стороны, не предоставят дополнительного доступа в локальную сеть (рис. 3.20).

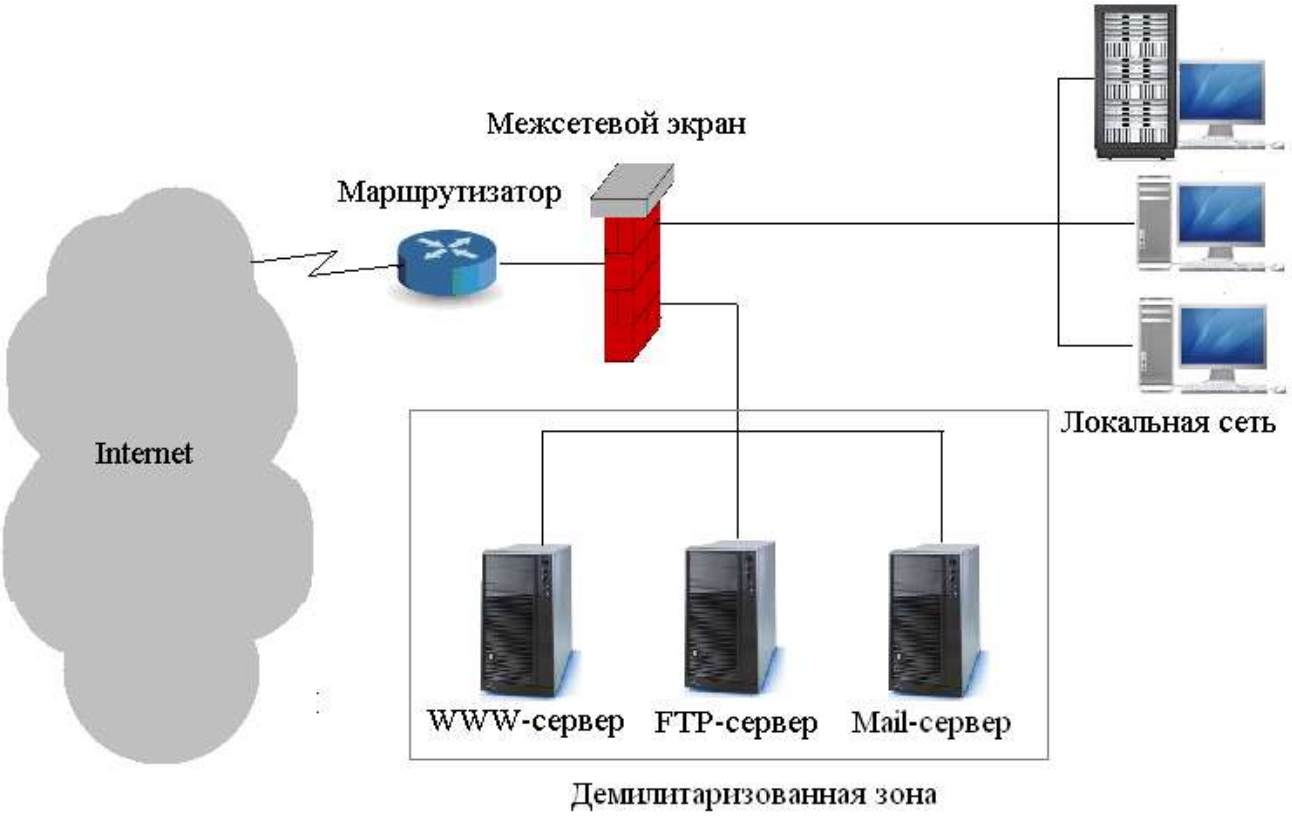


Рис. 3.20. Схема образования демилитаризованной зоны

При этом достаточно много внимания уделяется тому, чтобы пользователи внутренней сети не могли случайно или умышленно открыть брешь в локальную сеть через эти сервера. Для повышения уровня защищенности возможно использовать в одной сети несколько брандмауэров, стоящих друг за другом.

3.7 Протоколы установления подлинности

Общая схема всех протоколов аутентификации такова: сторона *A* и сторона *B* начинают обмениваться сообщениями между собой или с Центром раздачи ключей (ЦРК). ЦРК всегда надежный партнер. Протокол аутентификации должен быть устроен так, что даже если злоумышленник перехватит сообщения между *A* и *B*, то ни *A*, ни *B* не спутают друг друга с злоумышленником. Обмен данными между *A* и *B* будет происходить по алгоритму с закрытым ключом, а вот устанавливаться соединение по алгоритму с открытым ключом.

3.7.1 Аутентификация на основе закрытого разделяемого ключа

Основная идея первого протокола аутентификации, так называемого протокола «ответ по вызову», состоит в том, что одна сторона посылает некоторое число (вызов), другая сторона, получив это число, преобразует его по определенному алгоритму и отправляет обратно. Посмотрев на результат преобразования, и зная исходное число, инициатор может судить, правильно ли сделано преобразование или нет. Алгоритм преобразования является общим секретом взаимодействующих сторон. Будем предполагать, что стороны A и B имеют общий секретный ключ K_{AB}. Этот секретный ключ взаимодействующие стороны как-то установили заранее, например, по телефону. Описанная выше процедура показана на рис. 3.21, где

A,B - идентификаторы взаимодействующих сторон;
R_i - вызов, где индекс указывает кто его послал;
K_i - ключ, индекс которого указывает на его владельца.

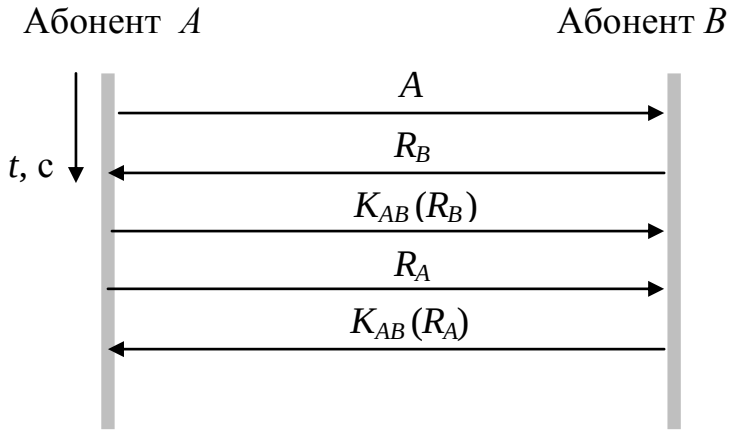


Рис. 3.21. Схема протокола аутентификации «Ответ по вызову»

Кажется, что в протоколе на рис. 4.5. можно сократить количество передач между абонентами A и B:

во-первых, передавая сразу имя абонента A и вызов от него – R_A, то есть объединить первую и третью сессию в первую сессию, т.к. они не пересекаются по передаваемым данным,

во-вторых, вызов от абонента B – R_B и результат шифрования вызова от A на общем секретном ключе K_{AB} – $K_{AB}(R_A)$, то есть объединить вторую и пятую сессии в одну вторую сессию, т.к. данные, передаваемые в этих сессиях не пересекаются.

На рис. 3.22 показана схема, где сокращено количество передач между сторонами, по сравнению с рис. 3.2.1

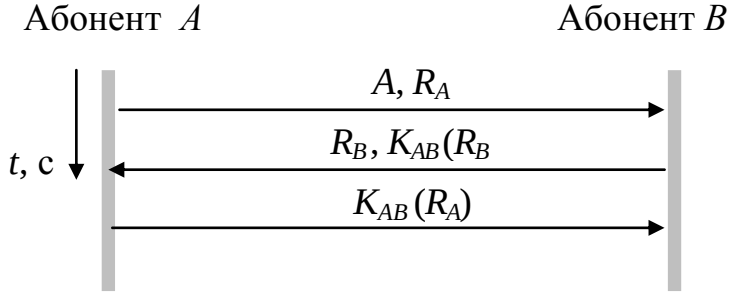


Рис. 3.22. Схема протокола аутентификации «Ответ по вызову» с сокращением количества передач между взаимодействующими сторонами

Схема, показанная на рис. 4.6 подвержена атаке отражением, в которой злоумышленник *C* может воспользоваться уязвимостью этой схемы и представиться абонентом *A* и получить доступ.

На рис. 3.23 показана уязвимость схемы 4.6 и реализация атаки отражением.

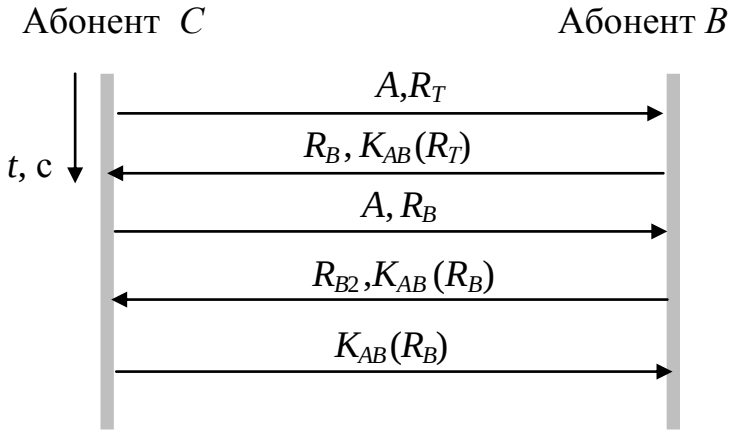


Рис. 3.23. Схема атаки отражением

Есть несколько общих правил построения протоколов аутентификации (протокол проверки подлинности или просто подлинности):

1) Инициатор должен доказать кто он есть прежде, чем вы пошлете ему какую-то важную информацию.

2) Инициатор и отвечающий должны использовать разные ключи.

3) Инициатор и отвечающий должны использовать начальные вызовы из разных непересекающихся множеств.

В схеме на рис.4.6 все эти три правила нарушены.

3.7.2 Установка разделяемого ключа

До сих пор мы предполагали, что *A* и *B* имеют общий секретный ключ. Рассмотрим теперь, как они могут его установить? Например, они могут воспользоваться телефоном. Однако, как *B* убедиться, что ему звонит именно *A*, а не злоумышленник? Можно договориться о личной встрече, куда принести паспорт и прочее, удостоверяющее личность. Однако есть протокол, который позволяет двум незнакомым людям установить общий ключ даже при условии, что за ними следит злоумышленник.

Это протокол обмена ключом Диффи-Хеллмана. Его схема показана на рис. 3.24.

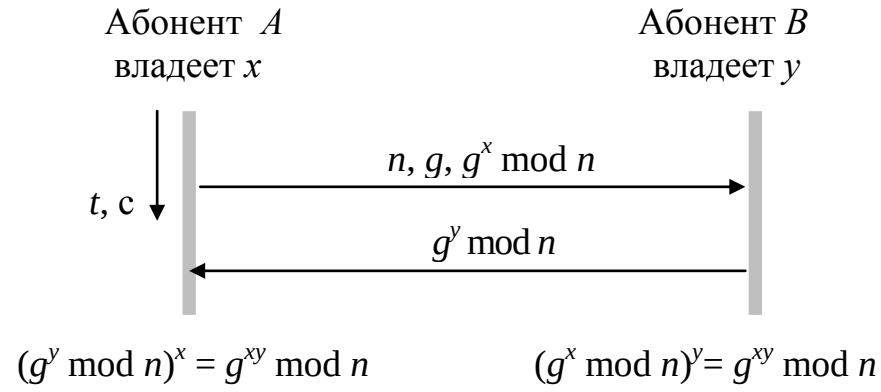


Рис. 3.24. протокол обмена ключом Диффи-Хеллмана

Прежде всего *A* и *B* должны договориться об использовании двух больших простых чисел *n* и *g*, удовлетворяющих определенным условиям. Эти числа могут быть общеизвестны. Затем, *A* выбирает большое число, скажем *x*, и хранит его в секрете. То же самое делает *B*. Его число – *y*.

A отправляет *B* сообщение (n,g,$g^x \bmod n$), *B* отправляет в ответ ($g^y \bmod n$). Теперь *A* выполняет операцию $(g^y \bmod n)^x$, *B* выполняет операцию $(g^x \bmod n)^y$. Теперь оба имеют общий ключ – $g^{xy} \bmod n$.

Например, n=47, g=3, x=8, y=10, то *A* шлет *B* сообщение (47,3,28), поскольку $3^8 \bmod 47 = 28$. *B* шлет *A* (17). *A* вычисляет $17^8 \bmod 47 = 4$, *B* вычисляет $28^{10} \bmod 47 = 4$. Ключ установлен, это – 4.

Злоумышленник следит за всем этим процессом. Единственно, что мешает ему вычислить *x* и *y* – это то, что не известно алгоритма с приемлемой сложностью для вычисления логарифма от модуля для простых чисел. Однако, у этого алгоритма есть слабое место, которое демонстрирует рис. 3.25. Такой прием называется *чужой в середине*.

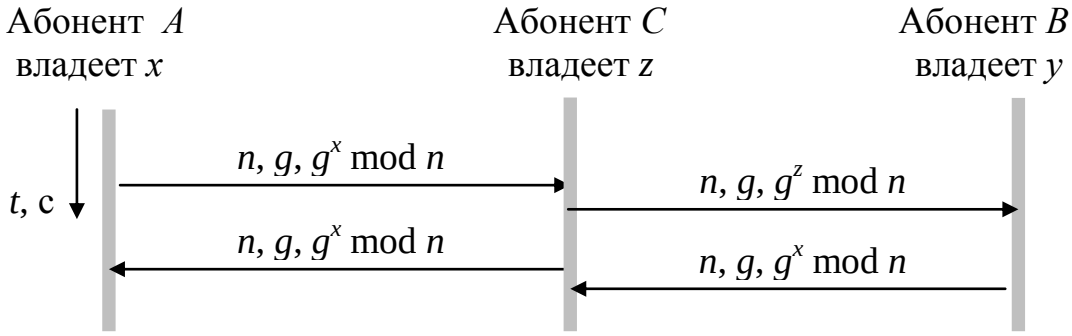


Рис. 3.25. Атака «чужой в середине»

3.7.3 Проверка подлинности через центр раздачи ключей

Договариваться с незнакомцем об общем секрете можно, но вряд ли это следует делать сразу (атака не спелого винограда). Кроме этого, общение с *n*

людьми потребует хранения n ключей, что для общительных или популярных личностей может быть проблемой.

Другое решение можно получить, введя надежный центр распространения ключей (ЦРК). Его использование иллюстрирует рис. 3.27.

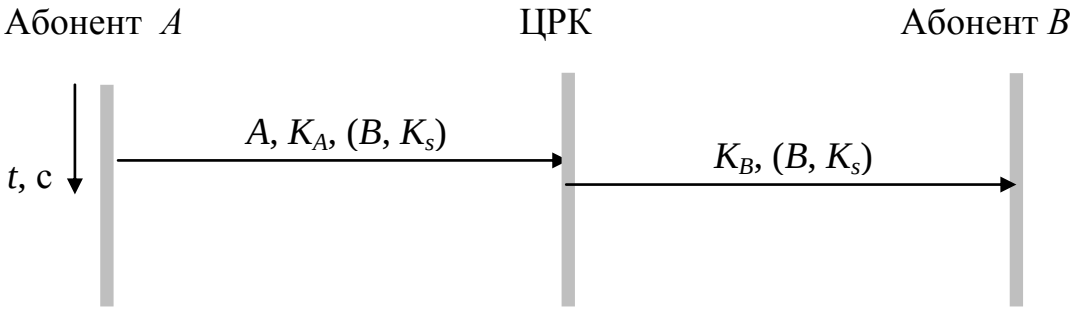


Рис. 3.27. Участие ЦРК в прцессе аутентификации

Идея этого протокола состоит в следующем. A выбирает ключ сессии K_S. Используя свой ключ K_A, шлет в ЦРК запрос на соединение с B. ЦРК знает B и его ключ K_B . С помощью этого ключа ЦРК сообщает B ключ сессии K_S и кто хочет с ним с соединиться.

Однако, решение с использованием ЦРК имеет изъян. Пусть злоумышленник как-то убедил A связаться с B и скопировал весь обмен сообщениями. Позже он может воспроизвести этот обмен за A и заставить B действовать так, как если бы с B говорил A. Этот способ атаки называется *атака подменой*.

Против такой атаки есть несколько решений. Одно из них – *временные метки*. Это решение требует синхронизации часов. Поскольку в сети всегда есть расхождение в показаниях часов, то необходимо выделить определенный допуск, интервал, в течении которого считать сообщений верным. Злоумышленник может использовать приемом атаки подменой в течении этого интервала.

Другое решение использование *разовых меток*. Однако, каждая из сторон должна помнить все разовые метки, использованные ранее. Это обременительно. Кроме этого, если список использованных разовых меток будет утерян по каким-либо причинам, то весь метод перестанет работать. Можно комбинировать решения разовых меток и временных меток.

Более тонкое решение установления подлинности дает многосторонний вызов-ответ протокол. Хорошо известным примером такого протокола является протокол Нидхема-Шредера, вариант которого показан на рис.3.28.

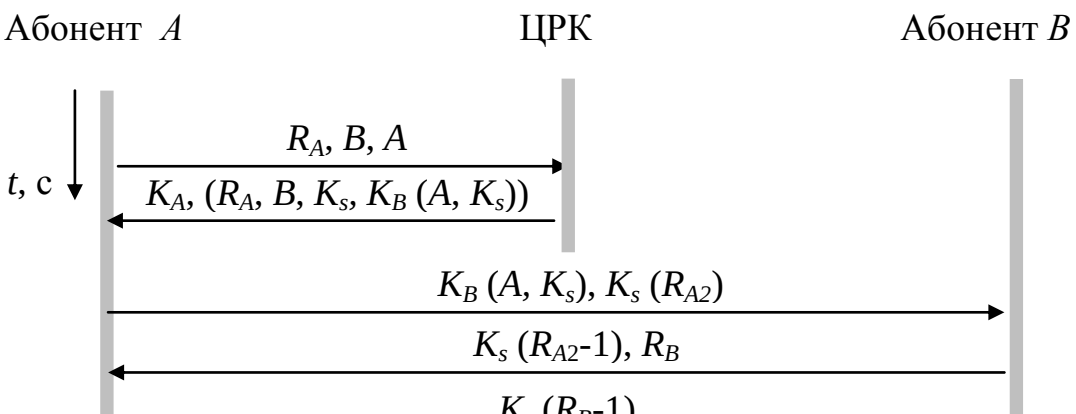


Рис. 3.28. Протокол аутентификации Нидхема-Шредера

В начале *A* сообщает ЦРК, что он хочет взаимодействовать с *B*. ЦРК сообщает ключ сессии, разовую метку R_A, шифруя сообщение ключом *A*. Разовая метка защищает *A* от подмены. Теперь, имея ключ сессии, *A* начинает обмен сообщениями с *B*. R_{A2} и R_B – разовые метки, защищающие *A* и *B* от подмен.

Хотя этот протокол в целом надежен, но все-таки есть небольшая опасность. Если злоумышленник раздобудет все-таки старый ключ сессии, то он сможет подменить сообщение 3 старым и убедить *B*, что это *A*. На рис. 3.29 приведена схема исправленного протокола, предложенного Отвей и Рисом. В этой модификации ЦРК следит, чтобы *R* было одним и тем же в обеих частях сообщения 2.

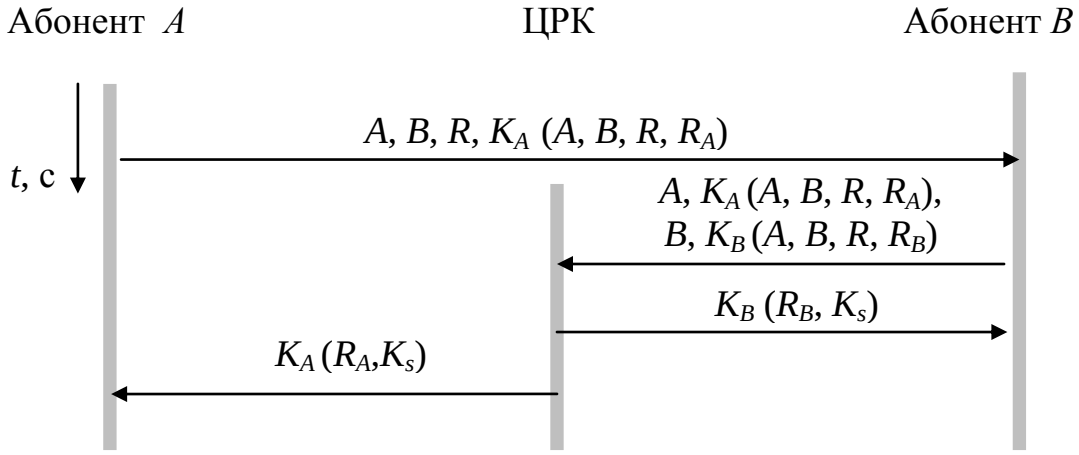


Рис. 3.29.Схема исправленного протокола, предложенного Отвей и Рисом

Установление подлинности протоколом Цербер.

Протокол установления подлинности Цербер используется многими практически действующими системами. Он представляет собой вариант протокола Нидхема-Шредера и был разработан в Массачусетском технологическом университете для безопасного доступа в сеть - предотвратить несанкционированное использование ресурсов сети. В нем использовано предположение, что все часы в сети хорошо синхронизованы.

Протокол Цербер предполагает использование кроме рабочей станции *A* еще трех серверов:

– Сервер установления подлинности (СП) – проверяет пользователей на этапе login;

– Сервер выдачи билета (СВБ) – идентификация билетов;

– Сервер *B* – тот кто должен выполнить работу, необходимую *A*.

Сервер установления подлинности аналогичен Центру раздачи ключей и знает секретный пароль для каждого пользователя. Сервер выдачи билетов выдает билеты, которые подтверждают подлинность заказчиков работ.

На рис. 3.30 показана работа протокола Цербер. Сначала пользователь садится за рабочую станцию и шлет открыто свое имя *A* серверу установления подлинности (СП). СП отвечает ключом сессии K_S и билетом $K_{СВБ}(A,K_S)$ к серверу выдачи билетов (СВБ) для предъявления этого билета на следующем шаге при обращении к СВБ. Все это зашифровано секретным ключом *A*. Когда сообщение 2 пришло на рабочую станцию у *A* запрашивают пароль, чтобы по нему установить K_A, для расшифровки сообщения 2. Пароль перезаписывается с временной меткой, чтобы предотвратить его захват злоумышленником. Выполнив login, пользователь может сообщить станции, что ему нужен сервер *B*. Рабочая станция обращается к СВБ за билетом для использования сервера *B*. Ключевым элементом этого запроса является $K_{СВБ}(A,K_S)$, зашифрованное секретным ключом СВБ. В ответ СВБ шлет ключ K_{AB} для работы *A* и *B*.

Теперь *A* может обращаться непосредственно к *B* с этим ключом. Это взаимодействие сопровождается временными метками, чтобы защититься от подмены. Если позднее *A* понадобиться работать с сервером *C*, то *A* должен будет повторить сообщение 3, но указать там сервер *C*.

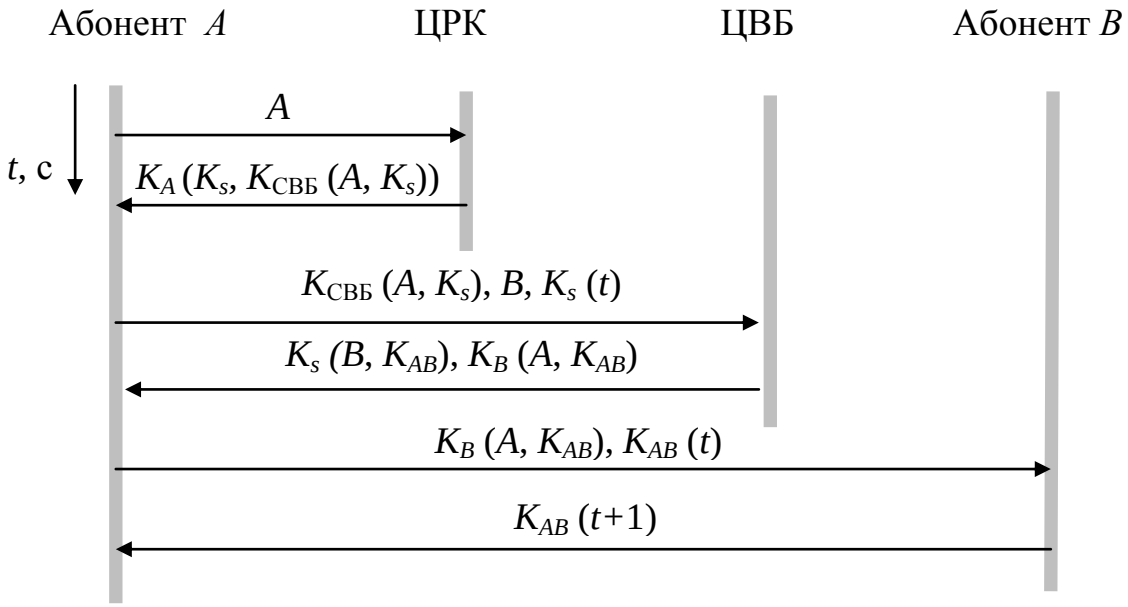


Рис. 3.30. Схема работы протокола Цербер

Поскольку сеть может быть очень большой, то нельзя требовать, чтобы все использовали один и тот же СП. Сеть разбивают на области, в каждой свои СП и СВБ, которые взаимодействую между собой.

Установление подлинности, используя шифрование с открытым ключом.

Установить взаимную подлинность можно с помощью шифрования с открытым ключом. Пусть *A* и *B* уже знают открытые ключи друг друга. Они их используют, чтобы установить подлинность друг друга, а затем использовать шифрование с секретным ключом, которое на несколько порядков быстрее.

На рис. 3.31 показана схема установления подлинности с шифрованием открытыми ключами.

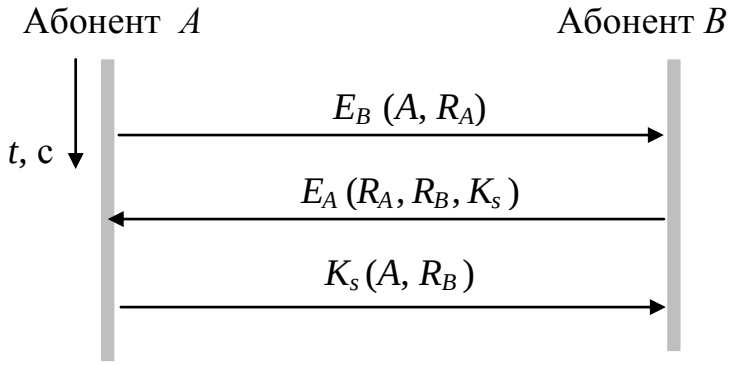


Рис. 3.31. Схема установления подлинности с шифрованием открытыми ключами

Здесь R_A и R_B используются, чтобы убедить A и B в их подлинности. Единственным слабым местом этого протокола является предположение, что A и B уже знают открытые ключи друг друга. Обмен такими ключами уязвим для атаки типа «чужой в середине».

Ривст и Шамир предложили протокол, защищенный от атаки «чужой в средине». Это, так называемый, протокол с внутренним замком. Его идея передавать сообщения в два этапа: сначала только четные биты, затем нечетные.

Выводы по четвертой главе

Основными этапами допуска в компьютерную систему являются идентификация, аутентификация и определение полномочий пользователя. Идентификация необходима для указания компьютерной системе уникального имени обращающегося к ней пользователя. Аутентификация заключается в проверке, является ли пользователь, пытающийся осуществить доступ к корпоративным ресурсам, тем, за кого себя выдает. Определение полномочий необходимо для последующего контроля и разграничения доступа к корпоративным ресурсам.

Основными и наиболее часто применяемыми методами аутентификации пользователей являются методы, основанные на использовании паролей. Они подразделяются на методы проверки подлинности на основе простого пароля и на основе динамически изменяющегося пароля.

Аутентификация на базе простого пароля предполагает, что пароль подтверждения подлинности пользователя не изменяется от сеанса к сеансу в течении установленного администратором службы безопасности времени его действительности.

При использовании динамически изменяющегося пароля для каждого нового сеанса работы или нового периода действия пароль изменяется по правилам, зависящим от используемого метода.

Последовательность и правила установления подлинности пользователей в корпоративной сети устанавливают протоколы аутентификации.

Использование межсетевых экранов позволяет организовать внутреннюю политику безопасности сети предприятия, разделив всю сеть на сегменты. Деление на сегменты позволяет ввести категории секретности и создание уровней секретности, выделить в отдельный сегмент все внутренние серверы компании, создать демилитаризованную зону для внешних ресурсов, создать выделенный сегмент административного управления и выделенный сегмент управления безопасностью.

Работа межсетевого экрана основана на динамическом выполнении двух групп функций: фильтрации информационных потоков и посредничества при реализации межсетевых взаимодействий.

Фильтрация состоит в выборочном пропускании информационных потоков в соответствии с принятой политикой безопасности через экран и извещением отправителя о том, что его данным в пропуске отказано.

Функции посредничества межсетевой экран выполняет с помощью специальных программ-посредников, запрещающих непосредственную передачу пакетов данных между внешней и внутренней сетью. К функциям посредничества относятся: идентификация и аутентификация пользователей, проверка подлинности передаваемых данных, разграничение доступа к ресурсам внутренней сети, поиск вирусов, трансляция внутренних сетевых адресов для исходящих пакетов данных и другие.

4. ПОСТРОЕНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Адекватный уровень информационной безопасности ИКС может быть обеспечен только на основе комплексного подхода, реализация которого начинается с разработки и внедрения эффективной политики безопасности. Такая политика определяет необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски информационной безопасности до приемлемой величины. В широком смысле политика безопасности определяется как система документированных управленческих решений по обеспечению информационной безопасности ИКС. В узком — как локальный нормативный документ, определяющий требования безопасности, систему мер либо порядок действий, а также ответственность сотрудников и механизмы контроля для определенной области обеспечения информационной безопасности.

Целью обеспечения информационной безопасности ИКС является ее надежное и бесперебойное функционирование в условиях возникающих угроз и воздействий, которые могут привести к нарушению работы ее компонент, в т.ч. и подсистемы информационной безопасности.

Основные этапы построения политики информационной безопасности ИКС включают в себя:

– описание объекта защиты;

– определение основных приоритетов информационной безопасности;

– определение модели нарушителя;

– определение перечня угроз информационной безопасности на всех уровнях обработки информации, с учетом нарушения активов базовых услуг безопасности: доступность, конфиденциальность и целостность;

– определение перечня требований информационной безопасности ИКС с учетом ранжирования сетевых активов по уровню важности;

– разработка комплекса организационно-технических мер по реализации требований и построению системы информационной безопасности;

– разработка организационно-технической схемы контроля состояния информационной безопасности ИКС.

4.1. Краткое описание типовой ИКС

В ИКС возможны все «традиционные» для локально расположенных (централизованных) вычислительных систем способы несанкционированного вмешательства в ее работу и доступа к информации. Кроме того, для нее характерны и новые специфические каналы проникновения и несанкционированного доступа к информации, наличие которых объясняется целым рядом их особенностей.

Перечислим основные из особенностей распределенной ИКС:

– территориальная разнесенность компонентов системы и наличие интенсивного обмена информацией между ними;

– широкий спектр используемых способов представления, хранения и передачи информации;

– интеграция данных различного назначения, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в различных удаленных узлах сети;

– абстрагирование владельцев данных от физических структур и места размещения данных;

– использование режимов распределенной обработки данных;

– участие в процессе автоматизированной обработки

– информации большого количества пользователей и персонала различных категорий;

– непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого числа пользователей (субъектов) различных категорий;

– высокая степень разнородности используемых средств вычислительной техники и связи, а также их программного обеспечения.

Типовая функционально-структурная организация ИКС изображена на рис. 4.1.

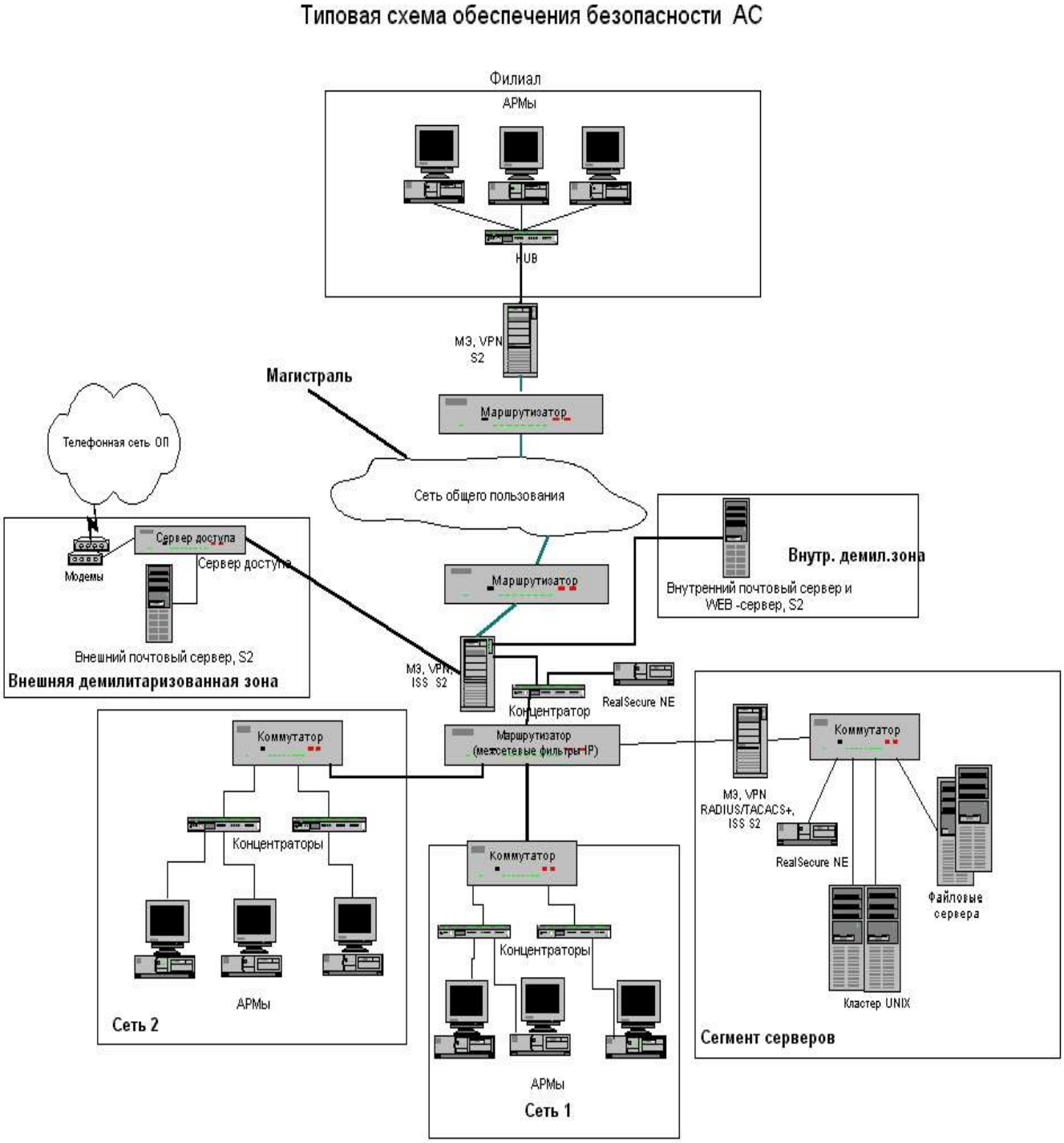


Рис. 4.1. Типовая функционально-структурная организация ИКС

В общем случае корпоративная ИКС на технологии «клиент-сервер», включает в себя следующие функциональные компоненты:

– сервера СУБД и файл-сервера, осуществляющие обработку и хранение инфоуслуг;

– автоматизированные рабочие места (АРМ) – оконечные абонентские системы ИКС;

– корпоративная МСС на основе IP-QoS технологий, включающая в себя локальную вычислительную сеть (ЛВС) и WAN-компоненту, обеспечивающую связь территориально удаленных ЛВС организации. В корпоративную сеть входят структурированные кабельные системы (СКС), на базе которых строятся ЛВС предприятия, сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы, мультиплексоры, межсетевые экраны и т. д.) и внешние каналы связи.

Политика информационной безопасности ИКС строится в соответствии со следующими принципами в порядке убывания их важности:

– доступность информации (обеспечение устойчивого функционирования системы);

– целостность хранимой, обрабатываемой и передаваемой по каналам связи информации;

– конфиденциальность хранимой, обрабатываемой и передаваемой по каналам связи информации.

Нарушения доступности информационных, программных и аппаратных ресурсов может привести к дезорганизации процесса обработки информации (несанкционированный останов СУБД, ОС, уничтожение данных и так далее).

Нарушение целостности данных, а также программных компонентов ИКС, находящихся как на сервере, так и на рабочих станциях может привести к некорректному функционированию программного обеспечения и преодолению системы защиты. Нарушитель, поразив целостность компонент ИКС, может заблокировать ее нормальное функционирование и тем самым осуществить атаку на доступность системы.

Нарушение конфиденциальности может привести к разглашению или утечке информации из ИКС и нанесению материального и морального ущерба юридическим или физическим лицам, обслуживаемым АС, а так же к несанкционированному предоставлению привилегий пользователям СУБД и ОС, что может повлечь доступ и искажение информации в ИКС и служебной информации файлов аудита СУБД и ОС.

Нарушитель, поразив конфиденциальность компонент автоматизированной системы (например, перехватив административные пароли) может исказить какой либо конфигурационный файл и тем самым осуществить атаку на целостность и доступность системы.

4.2. Описание модели нарушителя

Политика информационной безопасности должна строиться с учетом существования групп пользователей, наделенных различными полномочиями.

Основную опасность с точки зрения несанкционированного доступа к информации в ИКС и ее возможного искажения представляют собой действия лица, имеющего (или получившего путем преодоления средств защиты) наибольшие привилегии в автоматизированной системе – привилегии администраторов баз данных, операционных систем и телекоммуникационного

оборудования. Эти привилегии позволяют совершить несанкционированные действия и скрыть свои действия с помощью удаления полей журнала аудита.

Для ИКС можно выделить следующие потенциальные группы нарушителей:

нарушитель, не являющийся пользователем ИКС. Действия: Перехват служебного трафика ИКС с целью получения доступа к аутентификационной информации и формирование ложных SQL-запросов и запросов идентификации и аутентификации. Нарушитель может использовать так же сетевые средства по дезорганизации работы АРМ (вызывающие его зависания и перезагрузки) и серверов ИКС.

привилегированный пользователь СУБД (администратор базы данных (DBA), нарушитель, несанкционированно получивший административные привилегии СУБД). Действия: Несанкционированная настройка параметров СУБД, включая добавление и удаление учетных записей пользователей, присвоение привилегий пользователям, любые изменения данных, хранящихся в СУБД, а также хранимых процедур СУБД, нарушение безопасности СУБД и обрабатываемых данных ИКС.

администратор базы данных. Администратор БД занимается разграничением прав доступа к объектам БД, управляет созданием, модификацией и удалением объектов. Администратор БД владеет информацией о логической структуре данных, имеет представление о хранимой информации, привилегиях доступа пользователей к данным. Может произвести действия, нарушающие безопасность обрабатываемых данных. Привилегированным пользователем может быть нарушитель, несанкционированно получивший административные привилегии и администратор БД.

привилегированный пользователь ОС (администратор ОС сервера ИКС, нарушитель, несанкционированно получивший административные привилегии ОС). Администратор операционной системы занимается управлением и конфигурированием ОС. Отвечает за обеспечение непрерывных сервисов, необходимых для успешной работы СУБД и клиентов системы. Администратор ОС является экспертом в области администрирования применяемой ОС, других системных программных средств, а также в особенностях реализации СУБД в данной ОС. Владеет информацией об особенностях конфигурации, параметров настройки и организации функционирования БД в данной ОС. Привилегированным пользователем может быть нарушитель, несанкционированно получивший административные привилегии и администратор ОС HP-UX. Действия: Несанкционированная настройка параметров ОС, добавление и удаление учетных записей пользователей, присвоение привилегий пользователям, удаление журнала аудита ОС, нарушение безопасности ОС, СУБД и обрабатываемых данных ИКС.

привилегированный пользователь активного сетевого оборудования корпоративной сети (администратор маршрутизаторов, коммутаторов, концентраторов, нарушитель, несанкционированно получивший административные привилегии). Администратор аппаратной платформы (ААП) занимается управлением и конфигурированием аппаратной платформы. Отвечает за обеспечение непрерывных сервисов, необходимых для успешной работы ОС и

поддерживаемых ею приложений. ААП является экспертом в области используемой аппаратной платформы, владеет информацией об используемых физических устройствах, аппаратной конфигурации системы. Действия: Несанкционированная настройка коммутации и маршрутизации, изменение правил разграничения доступа на маршрутизаторах, перехват аутентификационной информации, нарушение функционирование ИКС путем изменения маршрутной информации и правил контроля доступа.

непривилегированный пользователь ИКС. Действия: Несанкционированное получение доступа к СУБД, минуя штатные средства ИКС с целью совершить несанкционированные действия в ИКС.

сотрудник, занимающийся администрированием или обслуживанием рабочих станций ИКС. Действия: Внедрение в операционную среду программных и аппаратных “закладок".

сотрудник, занимающийся администрированием системы информационной безопасности ИКС. Действия: Несанкционированная настройка систем защиты от НСД, систем криптографической защиты информации и предоставление несанкционированных полномочий в этих системах, изменение полномочий и списков доступа в системах защиты от НСД, что может привести к нарушению работоспособности ИКС.

4.3. Значимые угрозы в ИКС

4.3.1. Значимые угрозы нарушения доступности информационных, программных и аппаратных ресурсов

Для различных компонент ИКС существуют следующие угрозы нарушения их доступности.

Для серверов (*ОС и СУБД*)*:*

– удаленные атаки на сетевые сервисы с целью нарушения их работы (перехват паролей и трафика, атаки типа «отказ в обслуживании» – Dos атаки, использование уязвимостей сервисов);

– локальные атаки на систему защиты ОС легальным пользователем (подбор паролей, использование уязвимостей файловой системы, настроек сервисов и драйверов) с целью нарушения работы серверов ИКС;

– изменения конфигурации ОС (файлов CONFIG.SYS и AUTOEXEC.BAT, файлов ядра ОС Windows);

– удаления (модификации) исполняемых файлов прикладного и системного программного обеспечения средствами оболочки Norton Commander;

– неквалифицированные или неправомерные действия администраторов ОС и СУБД, приводящие к нарушению работы ИКС.

Для АРМ ИКС:

– изменения конфигурации ОС;

– удаления (модификации) исполняемых файлов прикладного и системного программного обеспечения;

– внесения компьютерных вирусов;

– эксплуатации программ, осуществляющих некорректные действия, из-за имеющихся в них ошибок или специальных "закладок".

Для мультисервисной сети:

– вывод из строя или изменение конфигурации сетевого оборудования, приводящее к потери доступа к сетевым ресурсам.

Для систем защиты от НСД и средств криптографической защиты информации:

– удаленные атаки на средства защиты от НСД и средства криптографической защиты информации с целью нарушения их работы;

– неквалифицированные или неправомерные действия администраторов систем защиты информации, приводящие к нарушению работы этих систем.

4.3.2. Значимые угрозы нарушения целостности данных и программных ресурсов

Для различных компонент ИКС существуют следующие угрозы нарушения целостности программ и данных.

Для серверов (*ОС и СУБД*):

– несанкционированное изменение компонентов ОС и СУБД;

– несанкционированное изменение содержимого базы данных прикладной задачи нештатными средствами, например, с помощью стандартных редакторов баз данных, при помощи специально разработанного программного обеспечения или неавторизованных SQL-запросов;

– изменение содержимого базы данных защиты несанкционированным образом (не уполномоченными на то лицами);

– модификация, запись, уничтожение любых программ и наборов данных, кроме личных наборов данных пользователей.

Для АРМ ИКС:

– несанкционированное изменение операционной среды рабочих станций, действия нарушителя в ИКС от имени легального пользователя, носящие деструктивный характер или приводящие к искажению информации.

Для мультисервисной сети:

– внесение несанкционированных изменений в настройки коммуникационного оборудования.

4.3.3. Значимые угрозы нарушения конфиденциальности

Для различных компонент ИКС существуют следующие угрозы конфиденциальности информации.

Для серверов (*ОС и СУБД*):

– ознакомление с конфиденциальными данными, хранимыми или обрабатываемыми в системе, лиц, не допущенных к данным сведениям;

– создание неучтенных, незаконных копий информационных массивов;

– использования слабых мест сетевых операционных систем Windows и Unix для Dos-атак, что приводит к полной или частичной потере работоспособности сервера;

– использования недостатков WWW-серверов и их конфигурации (права на каталоги WWW-сервера, CGI-скрипты и т.д.) для получения доступа к неавторизованным данным на WWW-сервере;

– хищение носителей информации, производственных отходов (распечаток, записей, списанных носителей информации и т.п.).

Для мультисервисной сети:

– перехват административных паролей, паролей серверов и сетевого оборудования с помощью прослушивания сети (сниффинга);

– перехват конфиденциального трафика с помощью сниффинга;

– использование захвата IP-соединений и работы вместо администратора или пользователя (технологии спуффинга);

– генерация фальшивых ICMP-пакетов для изменения параметров маршрутизации;

– использования слабых мест в сетевых службах telnet, FTP, NFS, NIS, SMTP, POP3, NNTP, X-Window, r-команд и т.д. для взлома сети;

– использование слабых мест системы DNS для формирования ложных таблиц хостов;

– использование слабых мест почтовой системы для взлома почтовой машины;

– использование протокола SNMP управления сетью для получения сведений о сетевом оборудовании и возможного перехвата и подмены управляющих сетевых сообщений;

– подбор паролей;

– использования недостатков в безопасности в WWW-броузерах и языках Java и ActiveX для получения доступа к данным на локальной машине клиента;

– занесение вируса с почтовой корреспонденцией.

Для систем защиты от НСД и средств криптографической защиты информации:

– компрометация ключевой информации систем криптографической защиты информации;

– расшифрование защищенной криптографическими методами информации с помощью методов криптоанализа.

4.4 Определение перечня требований информационной безопасности ИКС

4.4.1 Общие требования построения защищенной корпоративной сети

При проведении мероприятий по обеспечению информационной безопасности в корпоративной сети, являющейся транспортной средой передачи

информации ИКС, должны быть реализованы следующие требования политики безопасности:

1. Пользователи МСС должны иметь доступ к серверам ИКС, выделенным в отдельный сегмент, по строго определенному набору коммуникационных и прикладных протоколов с использованием механизмов proxy;

2. Внешние по отношению к ИКС абоненты не должны иметь доступа к ресурсам корпоративной сети области кроме ресурсов демилитаризованных зон ЛВС по строго определенному набору коммуникационных и прикладных протоколов;

3. Дистанционное администрирование систем защиты в ИКС должно производиться с использованием шифрования управляющего трафика на уровне IP или с помощью использования управляющих протоколов, поддерживающих шифрование данных (SNMPv2, SNMPv3);

4. Администрирование активного сетевого оборудования корпоративной сети должно контролироваться специалистами подразделения информационной безопасности с помощью механизмов штатного аудита сетевого оборудования. Подсистемы аудита должна администрироваться подразделениями информационной бзопасности.

В основу защиты МСС должно быть положено:

– построение системы защиты сетевого уровня, на технологии виртуальных частных сетей (Virtual Private Network - VPN) с применением протокола SKIP, в т. ч. магистральное шифрование сетевого трафика в региональном сегменте сети;

– применение межсетевых экранов, обеспечивающих защиту сетевого и транспортного уровня, как средства объединения и разграничения ресурсов физических и виртуальных сетей подразделений;

– применение наряду с пакетными фильтрами, средств фильтрации информации прикладного уровня, и proxy-систем;

– построение сегментов сетей на базе активного сетевого оборудования структурированной кабельной системы, и обеспечение на этой базе защиты физического уровня. Сегменты локальных сетей должны определяться по принципу равнокритичности ресурсов, располагаемых в рамках единого сегмента или примерной эквивалентности прав доступа пользователей, концентрированных в данном сегменте. С помощью встроенных в оборудование ЛВС средств защиты должны быть реализованы:

1) использование авторизации адресов оконечных систем портами концентраторов, обеспечивающей доступ к данному порту только с определенной оконечной системы. Следует использовать автоматическое отключение порта при обнаружении неавторизованного адреса;

2) должен быть установлен режим работы портов концентратора, к которым подключены рабочие станции, обеспечивающий прием пакетов, адресованных только данной оконечной системы;

– минимизация числа точек открытого доступа в периметр корпоративной защищенной сети и их обязательный контроль;

– применение средств усиленной аутентификации пользователей и ресурсов корпоративной сети;

– применение систем обнаружения вторжений на сетевом, системном и прикладном уровнях;

– обеспечение дистанционного администрирования и аудита всех компонент системы защиты, организация событийного протоколирования и подотчетности пользователей и администраторов;

– мониторинг безопасности и оперативная сигнализация на основе протокола SNMP;

– защищенные инфоприложения.

Традиционно, на первом месте мер, направленных на обеспечение информационной безопасности IP-систем находится межсетевое экранирование – средство разграничения доступа, служащее для защиты от внешних угроз и от угроз со стороны пользователей других сегментов корпоративной сети.

Важным элементом защиты от несанкционированного проникновения в корпоративную сеть из открытой сети (например, Internet) на транспортном уровне является последовательное (каскадное) включение нескольких фильтров – эшелонов защиты (рисунок 10). Это является важной дополнительной мерой безопасности, поскольку компрометация средств защиты от несанкционированного доступа (НСД) из внешних сетей, обеспечивающих фильтрацию информации на внешних каскадах сети, может быть выявлена до того, как нарушитель доберется до внутренних ресурсов корпоративной сети.

Между открытой и корпоративной сетью устанавливается демилитаризованная зона. Демилитаризованная зона представляет собой сегмент сети, который характеризуется тем, что в нем представляются информационные ресурсы для доступа из открытой сети. Серверы, находящиеся в демилитаризованной зоне и предоставляющие свои ресурсы для открытого доступа, конфигурируются специальным образом для того, чтобы на них не могли использоваться так называемые “опасные” сервисы (приложения), которые могут дать потенциальному нарушителю возможность реконфигурировать систему, компрометировать ее, и, опираясь на скомпрометированные ресурсы, атаковать корпоративную сеть.

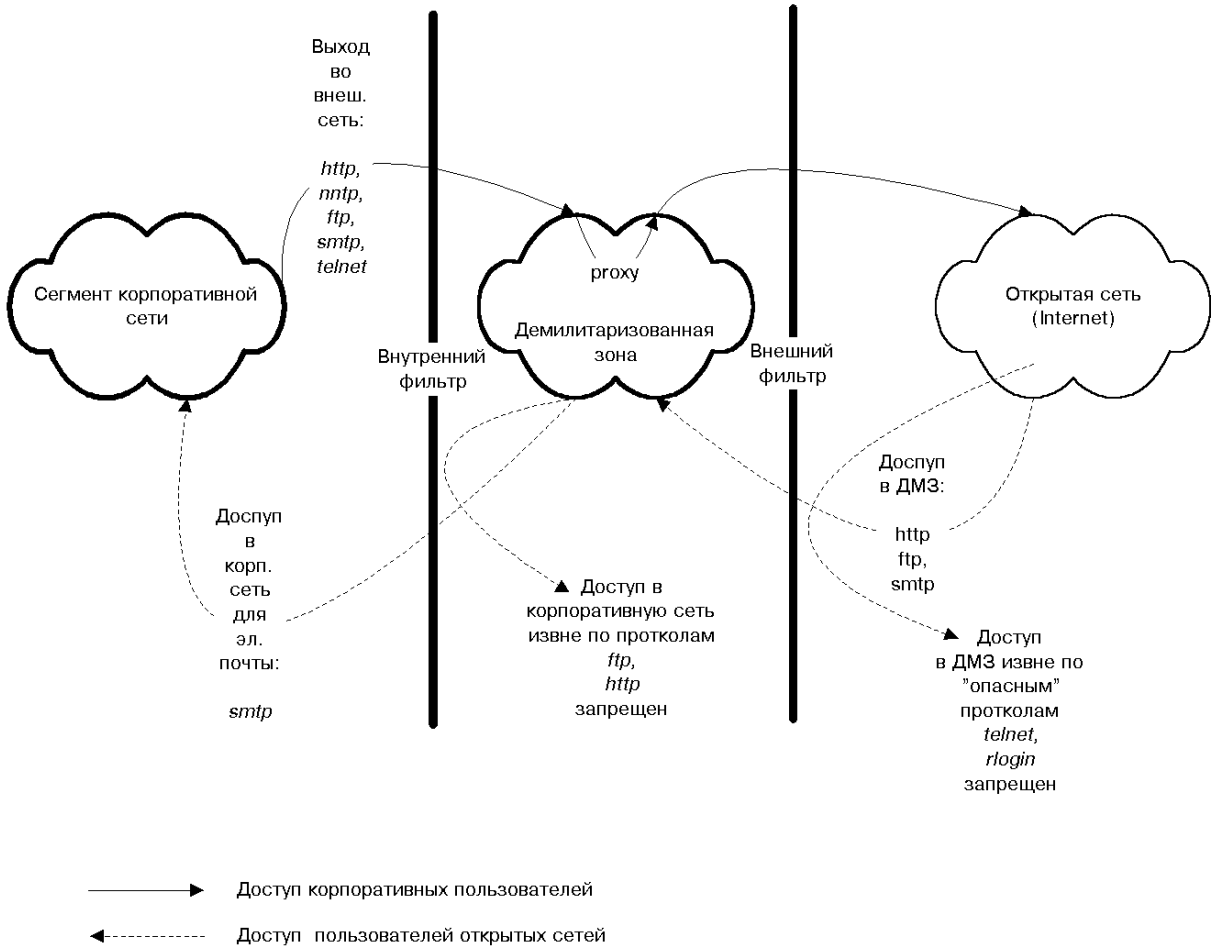


Рисунок 10 - Упрощенный пример политики безопасности при обменах между корпоративной ИКС и открытой сетью

Во внутренней демилитаризованной зоне должны размещаться:

– сервер DNS, «заявляющий» внешним сетям некоторое, строго регламентируемое адресное пространство, используемое приложениями для взаимодействия внешних и внутренних абонентов сети;

– прочие сервера, доступ к которым должен быть обеспечен по незащищенным каналам удаленным пользователям.

Во внешней демилитаризованной зоне должны размещаться:

– сервер доступа внешних абонентов;

– сервер авторизации внешних абонентов.

Демилитаризованные зоны должны быть подключены непосредственно к компьютеру, обеспечивающему межсетевое экранирование и шифрование IP-пакетов корпоративной сети.

В качестве внешнего и внутреннего фильтров применяются межсетевые экраны, которые, в общем случае, могут иметь достаточно сложную структуру. Межсетевые экраны в этом случае должны выполнять кроме пакетной фильтрации и задачу адресной фильтрации типа «разрешить данному хосту доступ в данный сегмент сети к данному серверу в заданном направлении по заданному прикладному протоколу (к заданному приложению)». Кроме того, в демилитаризованной зоне (или в составе внешнего/внутреннего фильтров) можно

использовать посреднические (proxy) сервисы для усиления фильтрационных характеристик промежуточного сегмента между открытой и корпоративной сетью.

Так как для построения системы защиты от НСД в пределах защищаемого сегмента сети, пакетной и адресной фильтрации IP трафика между сегментами недостаточно (хотя бы ввиду незащищенности в локальной сети соответствия IP-адрес – рабочее место), то для контроля доступа между VPN необходимо использовать сетевой экран более высокого уровня с дополнительной авторизацией клиентов и proxy-службами, поэтому доступ в сегмент серверов должен быть организован только через межсетевой экран уровня приложений с помощью механизма организации VLAN на коммутаторах. На этом межсетевом экране также должен устанавливается сервер усиленной аутентификации пользователей СУБД Oracle, маршрутизаторов, межсевых экранов.

Применение межсетевого экранирования уровня приложений для защиты выделенного сегмента серверов обеспечивает защиту серверов от многих видов атак типа DoS и дополнительно защищает как СУБД Oracle с помощью фильтрации на уровне запросов SqlNet, так и других сервисов ОС HP-UX. Настройка межсетевых экранов уровня приложений должна скрыть от пользователей внешних сетей структуру корпоративной сети (IP-адреса, доменные имена и т.д.). На этих межсетевых экранах определяется, каким пользователям, с каких хостов, в направлении каких хостов, в какое время, какими сервисами можно пользоваться. Межсетевые экраны должны описать для каждого пользователя, каким образом он должен аутентифицироваться при доступе к сервису.

Контролируемый доступ из одной сети ЛВС в другую должен осуществляться с фильтрацией трафика на межсетевых экранах осуществляющих фильтрацию на сетевом и транспортном уровнях. Межсетевой трафик между сетями ЛВС должен быть минимизирован. Для построения эшелонированной защиты предусматривается функционирование нескольких, включенных последовательно, межсетевых экранов. В качестве внешнего экрана должны использоваться межсетевые экраны, функционирующие на маршрутизаторах, а именно – встроенные в операционную систему сетевые фильтры и средства контроля доступа. В качестве внутреннего экрана (разделяющего сегмент серверов и сегмент пользователей ИКС, а также обеспечивающего межсетевое экранирование между сетями ЛВС) используется более мощный межсетевой экран уровня приложений. На нем также устанавливается ПО усиленной аутентификации субъектов и объектов региональной системы электронных расчетов (в частности, пользователей СУБД Oracle, межсетевых экранов и маршрутизаторов).

Фильтрация на межсетевых экранах основывается на принципе «все, что не разрешено, то запрещено».

Обязательно должно быть определено правило фильтрации, указывающее подавление пришедших из внешних сетей пакетов с исходными IP-адресами компьютеров внутренней сети, а так же пакеты с установленным битом маршрутизации.

Выполнение политики информационной безопасности в ИКС осуществляется администратором информационной безопасности (АИБ). Разные функции АИБ могут делегироваться нескольким сотрудникам подразделения информационной безопасности. АИБ ИКС должен получать полную статистику по использованию сервисов, попыткам несанкционированного доступа и т.д. Межсетевые экраны должны фильтровать протоколы Telnet, Rlogin (терминалы), FTP (передача данных), SMTP, POP3, HTTP, LP (сетевая печать), Rsh (удаленное выполнение задач), Finger, NNTP (новости Usenet), Sql*Net и другие, а также поддерживать внешнюю авторизацию и аккаунтинг на базе протоколов RADIUS/TACACS и интегрироваться в систему обнаружения вторжений.

Управление всеми внутренними межсетевыми экранами, а так же внешними экранами в части настроек параметров безопасности, возлагается на АИБ, при этом администраторы сети должны иметь возможность доступа к настройкам межсетевых экранов только на чтение.

Для обеспечения надежности функционирования системы защиты следует резервировать межсетевые экраны.

Политика доступа между сегментами корпоративной сети настраивается как независимый набор правил фильтрации для каждой пары интерфейсов (сегментов корпоративной сети) как на маршрутизаторах, так и на межсетевом экране. Критерии фильтрации могут быть основаны на применении одного или нескольких правил фильтрации. Каждое правило формируется на основе применения операций отношения к таким элементам IP-пакета, как:

– IP адрес источника/приемника пакета – эти правила позволяют разрешать или запрещать информационный обмен между некоторыми заданными узлами сети;

– поле «протокол» (TCP, UDP, ICMP и проч.) – правила фильтрации на основе этого поля регламентируют использование инкапсулируемых в IP протоколов;

– поле «порт» для источника/приемника пакета – с понятием «порт» в стеке протоколов TCP/IP ассоциируется некоторое приложение, и правила этой группы могут разрешать/запрещать доступ к заданному узлу по заданному прикладному протоколу (зависимость правил фильтрации по IP-адресам для пар источник/приемник позволяет контролировать направление доступа);

– бинарные данные с заданным смещением относительно заголовка IP. Например, блокировать пакеты с предустановленным маршрутом.

При организации VPN на базе протокола SKIP в зависимости должны быть реализованы следующие требования политики безопасности:

– устанавливается политика доступа информации на защищаемую платформу, которая может выбираться из ряда:

pass unknown – программе разрешается пропускать открытые пакеты от неизвестных (незарегистиррированных) узлов

drop unknown – программе разрешается пропускать пакеты (в том числе открытые) только от зарегистрированных узлов

skip only - программе предписывается работать только под управлением протокола SKIP и полностью запрещается открытый обмен

– прописываются разрешенные сетевые соединения (ассоциации) и устанавливаются атрибуты защиты для них (открытое соединение, шифрование трафика на назначенном для данного соединения алгоритме, цифровая подпись трафика); в случае выбора политики доступа *drop unknown* каждый пакет, принадлежащий незарегистрированному соединению, будет сбрасываться; в случае выбора политики доступа *skip only* все открытые пакеты будут сбрасываться.

Установление жесткой политики контроля доступа skip only для внутренней части корпоративной сети практически исключает несанкционированный доступ извне к информации, обрабатываемой в этой части корпоративной сети.

Применение межсетевых экранов, магистральное шифрование трафика и особенности реализации протокола SKIP (туннелирование IP-пакета и маскирование истинных IP-адресов) обеспечивают невозможность навязывания ложных пакетов из внешних телекоммуникационных сетей, что надежно защищает корпоративную сеть от атаки извне.

Для администрирования оборудования необходимо или пользоваться локальной консолью, или использовать версии telnet и rsh, поддерживающие шифрование трафика.

Для уменьшения вероятности перехвата пакетов необходимо дополнительно настроить сетевое оборудование, чтобы минимизировать распространение пакетов не по адресу.

Необходимо минимизировать число сервисов, запускаемых на хостах, оставив только необходимые сервисы. Следует запретить использование сервисов типа NFS или NIS без использования дополнительной криптозащиты канала.

Какой либо доступ извне к ресурсам, размещенным в ИКС вне демилитаризованных зон, должен быть запрещен. Возможно транслирование незашифрованного трафика извне только в демилитаризованные зоны и обратно. Размещение доступных извне регионального информационных ресурсов и служб в иных сетях, кроме демилитаризованных зон, должно быть запрещено.

Доступ из ИКС минуя межсетевое экранирование уровня приложений, должен быть запрещен.

Пользователи различных подразделений предприятия не должны иметь общих, доступных по записи сетевых устройств.

Пользователи и администраторы всех компонент ИКС должны иметь уникальные идентификаторы в этих компонентах, использование чужих идентификаторов должно быть запрещено. Встроенные в системы учетные записи администраторов этих систем (например, root в ОС HP-UX, SYS в СУБД Oracle) должны использоваться только при технической невозможности совершения требуемой операции с использованием индивидуальной учетной записи администратора этой системы.

4.4.2 Требования к подсистеме обеспечения безопасности сетевого взаимодействия

Подсистема обеспечения безопасности сетевого взаимодействия предназначена для выделения сегментов ЛВС, обрабатывающих конфиденциальную информацию из физической и логической среды ЛВС общего назначения, а также управления потоками данных между сегментами ЛВС путем удаления или преобразования данных, передаваемых по сети.

Должно быть обеспечено выделение сегментов ЛВС, обрабатывающих конфиденциальную информацию и использующих каналы сети ОН.

Сегментация должна осуществляться на канальном, сетевом и прикладном уровнях семиуровневой модели OSI.

Должна обеспечиваться фильтрация на сетевом уровне.

Решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов.

Управление потоками между сегментами сети должно осуществляться в соответствии со следующими принципами:

– фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

– фильтрация с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

– фильтрация с учетом любых значимых полей сетевых пакетов.

Должны быть реализованы механизмы контроля передаваемой по системе обмена электронными сообщениями информации. Контроль передаваемой корреспонденции должен осуществляться путем фильтрования протоколов передачи электронной почты специализированными средствами, устанавливаемыми на серверах, обеспечивающих функционирование почтовой системы внутри ЛВС организации. Фильтрование должно осуществляться в автоматизированном режиме по правилам, устанавливаемым подразделением технической защиты организации. Данные о работе фильтров должны передаваться подсистеме управления безопасности.

Должны быть реализованы механизмы защищенного документооборота, встроенные в автоматизированные системы обработки, хранения и передачи данных. Защита электронного документооборота может осуществляться с применением механизмов управления доступом к компьютерным ресурсам, криптографических и других механизмов, обеспечивающих надежную аутентификацию авторства документа и регистрацию пути следования электронных документов на всех стадиях его жизненного цикла.

Функции подсистемы обеспечения безопасности сетевого взаимодействия:

– защиты от несанкционированного межсетевого взаимодействия;

– защиты передаваемой информации;

– поддержания системы защиты в актуальном состоянии.

4.4.3. Требования информационной безопасности автоматизированных рабочих мест пользователей ИКС

Для надежной защиты данных в корпоративной сети на рабочих станциях пользователей (автоматизированных рабочих местах – АРМ) организуется замкнутая программная среда. Управление замкнутой программной средой должно осуществляться централизованно. Для АРМ, работающих под управлением ОС Windows, замкнутая среда может быть организована с помощью настройки реестра рабочей станции, хранимого в NDS, продуктом Z.E.N.Works фирмы NovellNetware или с помощью аналогичной программы.

Независимо от используемой операционной системы на АРМ, у пользователя не должно быть возможности запускать собственные, не разрешенные явно администратором, задачи.

Необходимо запретить модификации сетевых настроек АРМ, а также использование режима разделения каталогов и файлов на рабочих станциях пользователей, работающих под управлением ОС Windows.

Необходимо обеспечить невозможность неконтролируемого администрирования АРМ и пользователей этих АРМ с применением возможностей системы Z.E.N.Work только одним администратором ЛВС, полностью сохранив возможности администрирования других объектов сети Novell NetWare. Для чего необходимо:

– в контейнере NDS, содержащем объекты защищенных АРМ и пользователей, завести пользователя – администратора этого контейнера, установив ему прямое супервизорское trustee на данный контейнер;

– произвести разделение его пароля на две части, одна из которых передается в службу IT, другая – в службу безопасности;

– установить полный фильтр прав на данный контейнер (назначение необходимых прав на объекты контейнера со стороны внешних объектов производится в дальнейшем выделенным администратором, для чего на внешнюю часть NDS у него должно быть, по крайней мере, право просмотра).

Применяемые в ИКС средства криптографической защиты информации и средства защиты информации (СЗИ) от НСД должны быть сертифицированы. Настройка СЗИ от НСД на каждой рабочей станции осуществляется индивидуально, с учетом решаемых на этой станции задач.

Порядок работы с ключевыми материалами систем криптографической защиты информации должны быть регламентирован.

Программное обеспечения (ПО) требуемое для работы АРМ, включающее системные модули, прикладные программы и библиотеки, хранящиеся на локальном диске, должно выделяться в ядро АРМ, которое подвергается контролю на целостность средствами СЗИ от НСД. Программное обеспечение контроля целостности должно обеспечивать однозначную идентификацию ПО АРМ. Инициализация процедуры контроля целостности должна производится при каждом запуске АРМ. Первично должна проверяться программная оболочка АРМ, которая несет функцию загрузки рабочих библиотек, далее происходит

вход в систему (login), загрузка и проверка целостности библиотек. В случае обнаружения изменений в составе ПО, подсистема обеспечения контроля целостности должна блокировать дальнейшую работу АРМ, и произвести соответствующую запись в системном журнале.

Управление доступом в АРМ должна базироваться на стандартных механизмах идентификации, аутентификации и разграничения доступа предоставляемых:

- BIOS ПЭВМ;
- сертифицированным программно-аппаратным комплексом защиты от НСД Secret Net;
- ОС Windows АРМ;
- сетевой ОС Novell NetWare;
- средствами Oracle SQL*NET + Advanced Networking Option;
- СУБД Oracle;
- средствами усиленной аутентификации ACE Server (SecurID) или Kerberos.

Завершение работы пользователем АРМ должно сопровождаться освобождением всех занимаемых им разделяемых ресурсов (Logout).

Все входящие носители информации должны проверяться на наличие вирусов.

4.4.4. Требования к подсистеме аутентификации и управления доступом

Подсистема аутентификации и управления доступом предназначена для реализации функций защиты компьютерных ресурсов на уровне серверов и рабочих станций ЛВС и защиты элементов системы безопасности путем сопоставления субъектов и объектов ИКС и контроля полномочий субъектов при попытках доступа к защищаемым ресурсам.

Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов. Должна осуществляться идентификация рабочих станций и серверов, узлов сети, внешних устройств ЭВМ по логическим именам или сетевым адресам. Должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам. Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа. Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности носителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Подсистема должна требовать от пользователей идентифицировать себя при запросах на доступ. Должна проверяться подлинность идентификации - аутентификация. Должна присутствовать необходимыми данными для идентификации и аутентификации. КСЗ должен препятствовать доступу к

защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.

Механизмы обеспечения контроля доступа. Механизмы обеспечения контроля доступа используются для обеспечения услуг контроля доступа. Механизмы контроля доступа это те механизмы, которые используются для усиления стратегии ограничения доступа к ресурсу за счет доступа к нему только тех субъектов, которые имеют на это полномочия. Контроль доступа используется для определения полномочий отправителя данных на установление сеанса связи и/или на использование ресурсов в сеансе связи.

Требования, предъявляемые к механизмам управления доступом в равноправных уровнях на стороне получателя для передачи данных в режиме без установления соединения, должны быть известны заранее отправителю и должны быть зарегистрированы в информационной базе административного управления защитой.

Требования, подходы и задачи управления доступом. Механизмы управления доступом являются основой защиты ресурсов, обеспечивая решение задачи разграничения доступа субъектов к защищаемым информационным и техническим ресурсам — объектам. В качестве субъектов в простейшем случае понимается пользователь.

На практике наличие механизмов управления доступом необходимо, даже если в системе может находиться только один прикладной пользователь. Это вызвано тем, что, как правило, в системе должна быть создана учетная запись пользователя с правами администратора, который настраивает параметры системы защиты и права доступа к ресурсам защищаемого объекта. При этом у администратора принципиально иные права, чем у прикладного пользователя.

Механизм управления доступом реализует на практике некоторую абстрактную (или формальную) модель, определяющую правила задания разграничительной политики доступа к защищаемым ресурсам и правила обработки запросов доступа к защищаемым ресурсам.

Дискреционная (матричная) модель. Рассмотрим так называемую матричную модель защиты (ее еще называют дискреционной моделью), получившую на сегодняшний день наибольшее распространение на практике. В терминах матричной модели, состояние системы защиты описывается следующей тройкой: *S*, *O*, *M*,

где S – множество субъектов, являющихся активными структурными элементами модели;

O – множество объектов доступа, являющихся пассивными защищаемыми элементами модели. Каждый объект однозначно идентифицируется с помощью имени объекта;

M – матрица доступа. Значение элемента матрицы *M* [*S*, *O*] определяет права доступа субъекта *S* к объекту *O*.

Права доступа регламентируют способы обращения субъекта *S* к различным типам объектов доступа. В частности, права доступа субъектов к файловым объектам обычно определяют как чтение ®, запись (*W*) и выполнение (*E*).

Основу реализации управления доступом составляет анализ строки матрицы доступа при обращении субъекта к объекту. При этом проверяется строка матрицы, соответствующая объекту, и анализируется, есть ли в ней разрешенные права доступа для субъекта или нет. На основе этого принимается решение о предоставлении доступа.

При всей наглядности и гибкости возможных настроек разграничительной политики доступа к ресурсам, матричным моделям присущи серьезные недостатки. Основной из них – это излишне детализированный уровень описания отношений субъектов и объектов. Из-за этого усложняется процедура администрирования системы защиты. Причем это происходит как при задании настроек, так и при поддержании их в актуальном состоянии при включении в схему разграничения доступа новых субъектов и объектов. Как следствие, усложнение администрирования может приводить к возникновению ошибок.

Многоуровневые (мандатные) модели. С целью устранения недостатков матричных моделей были разработаны так называемые многоуровневые модели защиты, классическими примерами которых являются модель конечных состояний Белла и Ла-Падулы, а также решетчатая модель Д. Деннинг. Многоуровневые модели предполагают формализацию процедуры назначении прав доступа посредством так называемых меток конфиденциальности, или мандатов, назначаемых субъектам и объектам доступа.

Так, для субъекта доступа метки, например, могут определяться в соответствии с уровнем допуска лица к информации, а для объекта доступа (собственно данные) – признаками конфиденциальности информации. Признаки конфиденциальности фиксируются в метке объекта.

В связи с использованием терминов «мандат», «метка», «полномочия» многоуровневую защиту часто называют соответственно либо мандатной защитой, либо защитой с метками конфиденциальности, либо полномочной защитой.

Права доступа каждого субъекта и характеристики конфиденциальности каждого объекта отображаются в виде совокупности уровня конфиденциальности и набора категорий конфиденциальности. Уровень конфиденциальности может принимать одно из строго упорядоченного ряда фиксированных значений, например: конфиденциально, секретно, для служебного пользования, несекретно и т.п.

Основу реализации управления доступом составляют:

1. Формальное сравнение метки субъекта, запросившего доступ, и метки объекта, к которому запрошен доступ.

2. Принятие решений о предоставлении доступа на основе некоторых правил, основу которых составляет противодействие снижению уровня конфиденциальности защищаемой информации.

Таким образом, многоуровневая модель предупреждает возможность пред-намеренного или случайного снижения уровня конфиденциальности защищаемой информации за счет ее утечки (умышленного переноса). То есть эта модель препятствует переходу информации из объектов с высоким уровнем

конфиденциальности и узким набором категорий доступа в объекты с меньшим уровнем конфиденциальности и более широким набором категорий доступа.

Практика показывает, что многоуровневые модели защиты находятся гораздо ближе к потребностям реальной жизни, нежели матричные модели, и представляют собой хорошую основу для построения автоматизированных систем разграничения доступа. Причем, так как отдельно взятые категории одного уровня равнозначны, то, чтобы их разграничить наряду с многоуровневой (мандатной) моделью, требуется применение матричной модели.

С помощью многоуровневых моделей возможно существенное упрощение задачи администрирования (настройки). Причем это касается как исходной настройки разграничительной политики доступа (не требуется столь высокого урони и детализации задания отношения субъект-объект), так и последующего включения в схему администрирования новый субъектов и объектов доступа.

Доступ к сетевым ресурсам. При использовании защищаемого объекта в составе инфокоммуникационной сети встает задача изоляции информационных потоков, циркулирующих в сети.

Согласно формализованным требованиям система защиты должна обеспечивать защищенный механизм ввода и выводи информации для объекта доступа. В данном случае объектом доступа является канал связи.

Разграничение доступа к узлам сети предназначено для изоляции информационных потоков − виртуальной сегментации сетевого пространства. При этом каждому конечному пользователю разрешается взаимодействие с определенным набором серверов, предоставляющих услуги определенные, то есть использование фиксированного набора сетевых служб.

Диспетчером доступа к сетевым ресурсам должна решаться следующая совокупность задач:

1. Должно обеспечиваться разграничение доступа к узлам и к хостам сети на уровне IP адресов и TCP-портов, то есть на уровне сетевых служб и процессов, обеспечивающих доступ к сетевым ресурсам. Таким образом, должно обеспечиваться разграничение доступа по следующим параметрам:
   - пользователям;
   - процессам;
   - времени доступа;
   - по службам доступа (портам);
   - политике безопасности (запрещенные/разрешенные хосты и службы).
2. Должна обеспечиваться виртуальная сегментация сетевого пространства защищаемой сети (сегмента сети).

Виртуальная сегментация сетевого пространства осуществляется на уровне пользователей, что принципиально отличает данный подход логического деления сети на подсети от способов, предполагающих использование дополнительных технических средств физической сегментации на подсети — маршрутизаторов, межсетевых экранов и т.д.

Управление доступом должно осуществляться в соответствии с дискреционным принципом контроля. Дискреционный принцип контроля доступа

должен обеспечивать управление доступом наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и логическим дискам) АС. Для каждой пары (субъект – объект) в системе защиты должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать, переименовать, удалить, запустить), т.е. тех типов доступа, которые являются санкционированными для данного субъекта к данному ресурсу АС (объекту). Контроль доступа должен быть применим к каждому объекту и каждому субъекту. Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей системы защиты и списка защищаемых объектов. Права изменять ПРД должны предоставляться выделенному субъекту (администратору безопасности).

Подсистема аутентификации и управления доступом должна содержать механизмы дискреционного контроля доступа к настройкам системы безопасности субъектов, имеющих административные права (администраторов безопасности). При попытках доступа к настройкам системы безопасности должна осуществляться идентификация и аутентификация субъектов по идентификатору условно-постоянного действия и паролю, длиной не менее 6 символов. При попытках изменения настроек системы безопасности должны проверяться права администрирующих на изменение правил управления доступом.

Требования к средствам разграничения доступа к компьютерным ресурсам внутри корпоративной сети. Средства разграничения доступа к компьютерным ресурсам внутри корпоративной сети предназначены для обеспечения свойств конфиденциальности, целостности и подлинности ресурсов сети путем реализации механизмов управления доступом поименованных субъектов ИКС к поименованным объектам, предотвращения НСД к ресурсам сети и сигнализации попыток НСД.

Требования к подсистеме управления доступом.

Должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов:

– идентификация пользователей при помощи специальных аппаратных средств;

– критерии выявления тривиальных паролей субъектов доступа; минимальная длина, уникальность, срок действия, литерный набор (пароль должен содержать в себе символы по крайней мере двух из наборов: прописные буквы латинского алфавита, строчные буквы латинского алфавита, прописные буквы русского алфавита, строчные буквы русского алфавита, цифры, специальные символы);

– использование при аутентификации широко используемых функций хеширования (ГОСТ Р.34.11-94, MD5, SHA) с вероятностью возникновения

коллизий (совпадения хеш-значений для двух случайно равновероятно выбранных объектов) не более 10-9;

– для системы защиты распределенных сетевых ресурсов должен быть реализован механизм централизованного хранения базы данных учетных записей (распределенный механизм аутентификации);

– распределенный механизм аутентификации должен исключать открытую передачу пароля пользователя по незащищенному каналу;

– после идентификации и аутентификации субъекта полученная идентификация должна надежно связываться со всеми действиями данного пользователя.

Должна осуществляться идентификация рабочих станций и серверов, узлов сети, внешних устройств ЭВМ по логическим именам или сетевым адресам; идентификация программ, томов, каталогов, файлов, записей, полей записей - по именам:

– каждому объекту АС должен соответствовать объект доступа в системе защиты информации;

– всем объектам доступа в системе защиты информации должны быть сопоставлены атрибуты доступа для каждого субъекта доступа.

Должна быть реализована многоуровневая система защиты объектов автоматизированной системы от несанкционированного доступа, включающая следующие уровни защиты:

– внешняя защита;

– защита на уровне аппаратных ресурсов;

– защита на уровне объектов файловой системы;

– защита на уровне ресурсов операционной системы.

Должна быть реализована внешняя защита, предотвращающая доступ посторонних пользователей к защищенной ЭВМ:

– защита от загрузки с постороннего носителя, при помощи специальных аппаратных средств, либо путем частичного или полного преобразования данных на жестком диске;

– функция временной блокировки консоли, обеспечивающая защиту работающего компьютера от постороннего пользователя.

Должна быть реализована защита на уровне аппаратных ресурсов:

– управление доступом к коммуникационным портам компьютера;

– управление доступом к физическим дискам, дисководам и приводам CD-ROM;

– разграничение доступа к локальным и сетевым принтерам;

– запрет работы при изменении аппаратной конфигурации компьютера;

– запрет работы при удалении устройств аппаратной поддержки системы защиты;

– запрет прямого доступа к дискам.

Должна быть реализована защита на уровне объектов файловой системы:

– разграничение доступа к локальным логическим дискам;

– разграничение доступа к каталогам и файлам;

– субъекты доступа в отношении объектов файловой системы должны делиться на три категории – владелец, член группы и другой;

– управление доступом должно осуществляться на основании определения принадлежности субъекта одной из категорий, при этом владелец имеет максимальные права по управлению доступом к объекту, управление доступом членов группы и других осуществляется владельцем или субъектом, имеющим права по управлению доступом субъекта-владельца;

– управление доступом к объектам ФС должно осуществляться в соответствии со следующим принципом: если субъект является зарегистрированным пользователем СЗИ и осуществляет доступ с зарегистрированного в СЗИ АРМ, то он получает доступ в соответствии с групповой принадлежностью; незарегистрированные пользователи доступ не получают; зарегистрированные пользователи, работающие на незарегистрированных АРМ могут получать доступ к объекту без учета групповой принадлежности (как «другие»);

– формирование замкнутой программной среды для пользователя (ограниченного списка программ, разрешенных для запуска).

Должна быть реализована защита на уровне ресурсов операционной системы:

– задание персональной конфигурации операционной системы;

– возможность построения индивидуального списка доступных сетевых ресурсов;

– запрет изменения системного времени;

– запрет редактирования реестра;

– запрет диалогов настроек параметров системы;

– запрет удаленного доступа;

– запрет кэширования сетевых паролей.

Должен быть реализован дискреционный принцип контроля доступа субъектов к защищаемым объектам в соответствии с матрицей контроля доступа:

– матрица доступа должна содержать перечисление санкционированных (разрешенных) операций для каждой пары «субъект–объект» системы защиты. Должно быть задано явное и недвусмысленное перечисление допустимых типов доступа: читать, писать, удалять, запускать, переименовывать, т.е. тех типов доступа, которые являются санкционированными для данного субъекта к данному ресурсу (объекту);

– механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов. Права изменять ПРД должны предоставляться выделенным субъектам: пользователям системы защиты с правами администратора или супервизора.

Должен быть реализован мандатный принцип контроля доступа субъектов к защищаемым ресурсам с помощью меток конфиденциальности:

– должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни иерархической классификации;

– при вводе новых данных в систему должны запрашиваться и получаться от санкционированного пользователя метки этих данных;

– при санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток;

– мандатный принцип контроля доступа должен быть реализован применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов. Под «явным» здесь подразумевается доступ, осуществляемый с использованием системных средств – системных макрокоманд, инструкций языков высокого уровня и т.д., а под «скрытым» - иной доступ, в том числе с использованием собственных программ работы устройствами;

– субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта;

– субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации;

– должна быть предусмотрена возможность изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

Должна быть реализована централизованная подсистема администрирования системы защиты информации:

– права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.);

– система защиты должна обеспечивать идентификацию и аутентификацию администратора безопасности при его запросах на доступ;

– должна быть реализована система агентов для всех защищенных АРМ, позволяющая выделенным субъектам в реальном времени получать информацию и осуществлять централизованное управление политикой безопасности системы защиты;

– возможность делегирования прав (т. е. присвоения пользователю ограниченных административных привилегий управления некоторым набором учетных записей);

– использование универсальных шаблонов настроек политики безопасности;

– возможность моделирования существующей организационной иерархии и административной структуры компании – пользователя СЗИ;

– возможность блокировки учетной записи пользователя или её ограничения по времени работы.

Требования к криптографической подсистеме.

Должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами

доступа (разделяемые) носители данных, а также на съемные портативные носители данных (дискеты, CD-диски, магнитные ленты и др.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа:

– должна выполняться принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

– механизм формирования ключей шифрования (зависимый – на основе какой-либо персональной информации пользователя или группы пользователей; независимый – с использованием датчика случайных чисел);

– используемые алгоритмы шифрования и электронной цифровой подписи;

– форма реализации криптографических алгоритмов (программная или аппаратная);

– скорость шифрования и хеширования (для аппаратной формы реализации криптоалгоритмов).

Должна быть реализована возможность шифрования сетевых соединений обеспечивающая возможность работы на каналах до 100Мбит/с.

Доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом:

– доступ должен предоставляться выделенным субъектам доступа;

– доступ должен быть реализован предусмотренными средствами управления.

Должны использоваться сертифицированные средства криптографической защиты.

Дополнительные требования.

В состав системы должны входить агенты, функционирующие под управлением ряда клиентских ОС (Windows 95/98/Me, Windows NT).

Система защиты может использовать встроенные в ОС механизмы защиты. Для обеспечения свойств гарантии защиты должны быть реализованы собственные защитные механизмы, не зависящие от механизмов ОС.

Должна существовать возможность использования тестовых режимов для СЗИ на этапе ввода в эксплуатацию:

– снятие ограничений на пароль;

– отключение блокировки учетных записей;

– при наличии аппаратных средств аутентификации – возможность входа в систему без электронного идентификатора;

– отключение режимов замкнутой программной среды и контроля атрибутов для пользователя или группы пользователей;

– эксплуатация СЗИ в тестовом режиме должна тесно сопровождаться работой подсистемы регистрации и учета с целью дальнейшего формирования политики безопасности системы защиты.

Требования к средствам защиты от несанкционированного доступа со стороны сетевого окружения. Средства защиты от несанкционированного доступа со стороны сетевого окружения предназначены для автоматизированного

управления доступом путем фильтрации потока данных между узлами сети. В качестве таких средств защиты могут использоваться межсетевые экраны, маршрутизаторы, коммутаторы и прочее активное сетевое оборудование.

Для реализации описанных функций средства защиты должны иметь в своем составе следующие подсистемы: управления доступом, администрирования, регистрации, контроля целостности, восстановления.

При выборе программной платформы для использования в составе комплекса защиты от несанкционированного межсетевого взаимодействия следует определить ряд требований, необходимых для нормального функционирования всего комплекса.

Безусловным требованием является архитектурная совместимость всех компонент комплекса. Следует уделить внимание показателям отказоустойчивости, полноте возможностей разграничения доступа к ресурсам системы, функциональных характеристик средств мониторинга и аудита, а так же эффективности механизмов идентификации и аутентификации, применяемых для администрирования системы.

Поэтому отправной точкой выбора программной платформы должно быть семейство серверных операционных систем. Исходя из этих соображений должны быть использованы операционные системы Windows NT или xNIX.

Подсистема администрирования:

Средство защиты должно предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия. Сеанс администрирования средства защиты должен предваряться запросом идентификатора пользователя и паролем. Доступ к управлению и контролю для подсистемы администрирования должен предоставляться только после ввода уникальных идентификатора и пароля. Должна быть определена возможность смены идентификатора и пароля для доступа к подсистеме администрирования.

Средство защиты должно предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю временного действия. Должно быть предусмотрено ограничение в виде временного интервала или набора временных интервалов для возможности администрирования средства защиты.

Средство защиты должно обеспечивать идентификацию и аутентификацию администратора при его локальных запросах на доступ. Локальный сеанс администрирования возможен только при введении уникальных идентификатора и пароля.

Средство защиты должно обеспечивать идентификацию и аутентификацию администратора при его удаленных а доступ. Удаленный сеанс администрирования возможен только при введении уникальных идентификатора и пароля.

Средство защиты должно препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась. В процессе установления соединения при

введении неверных идентификатора или пароля возможность администрирования не должна быть предоставлена.

При удаленных запросах администратора на доступ к средству защиты идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации. Для этих целей должны применяться криптографические механизмы аутентификации с использованием электронной подписи.

Подсистема регистрации:

Средство защиты должно обеспечивать регистрацию входа (выхода) администратора в систему (из системы) либо загрузка и инициализация системы и ее программный останов.

Регистрация выхода из системы не проводится в моменты аппаратурного отключения средства защиты.

В параметрах регистрации указываются:

– дата, время и код регистрируемого события;

– результат попытки осуществления регистрируемого события - успешная или неуспешная;

– идентификатор администратора, предъявленный при попытке осуществления регистрируемого события.

Средство защиты должно обеспечивать регистрацию запуска программ и процессов (заданий, задач), действий администратора по изменению правил фильтрации.

Простота использования:

Средство защиты должно обеспечивать возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.

Интерфейс управления должен предоставлять возможности для удобного и простого взаимодействия администратора с функциями аудита и управления средства защиты, включая:

– возможность резервного копирования настроек конфигурации на внешний носитель;

– возможность быстрого восстановления параметров конфигурации из резервной области памяти;

– возможность редактирования параметров конфигурации внешними средствами (возможность формирования и импортирования и экспортирования параметров конфигурации в виде текстового файла, размещение комментариев в тексте файла конфигурации);

– графическое представление элементов управления пользовательского интерфейса.

Интерфейс аудита должен предоставлять простое и наглядное представление статистической информации:

– удобная среда просмотра данных журналов регистрации событий, включающая параллельное выполнение всех функций взаимодействия с пользовательским интерфейсом как с помощью клавиатуры, так и мыши;

– возможность формирования выборки из данных статистики по необходимому набору признаков;

– возможность поиска информации в результатах статистических данных по заданному ключевому слову;

– возможность графического представления данных отчета статистики (графики, гистограммы, круговые диаграммы).

Подсистема управления доступом.

Средства защиты должны обеспечивать фильтрацию **на канальном уровне**:

– должна обеспечиваться фильтрация потока данных на основе MAC-адресов отправителя и получателя;

– средства защиты должны выполнять фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов. В настройках параметров фильтрации должна присутствовать возможность допускать или запрещать прохождение сетевыми пакетами из списка адресов указанный сетевой интерфейс;

– должна обеспечиваться фильтрация с учетом даты/времени. Необходимо выполнение возможности определения временных интервалов для выполнения правил фильтрации.

Средства защиты должны обеспечивать фильтрацию **на сетевом уровне:**

– решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов. Фильтрация производится по IP-адресам и MAC-адресам;

– средства защиты должны обеспечивать фильтрацию с учетом любых значимых полей сетевых пакетов (необходимо определиться – что есть значимые поля?);

– должна обеспечиваться фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств. Должна обеспечиваться поддержка фильтрации протокола ICMP;

– средства защиты должны обеспечивать возможность трансляции сетевых адресов. Должно быть реализовано использование функции маскарадинга, подразумевающее режим модификации проходящих пакетов от субъекта подсети в другую подсеть. При этом IP-адрес субъекта (отправителя) изменяется на адрес внешнего сетевого интерфейса экрана. При получении ответа на отправленное данным субъектом сообщение происходит выполнение обратной процедуры;

– должна обеспечиваться фильтрация с учетом даты/времени. Необходимо выполнение возможности определения временных интервалов для выполнения правил фильтрации.

Средства защиты должны обеспечивать фильтрацию **на транспортном уровне:**

– должна обеспечиваться возможность фильтрации запросов на установление виртуальных соединений. При этом, по крайней мере, учитываются транспортные адреса отправителя и получателя. Фильтрация производится IP-адресам для TCP и UDP соединений;

– должна обеспечиваться фильтрация с учетом даты/времени. Необходимо выполнение возможности определения временных интервалов для выполнения правил фильтрации.

Средства защиты должны обеспечивать фильтрацию **на прикладном уровне:**

– должна обеспечиваться возможность фильтрации на прикладном уровне запросов к прикладным сервисам. При этом, по крайней мере, учитываются прикладные адреса отправителя и получателя; Фильтрация производится по сокетам (sockets) для TCP и UDP соединений;

– возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети. Выполнение функций Proxy для используемых прикладных служб – HTTP, FTP, GOPHER, SOCKS. Использование централизованного узла в подсети для обмена информацией определенного прикладного сервиса с внешней средой – POP3, SMTP, IMAP, IRC и т.п.;

– должна обеспечиваться фильтрация с учетом даты/времени. Необходимо выполнение возможности определения временных интервалов для выполнения правил фильтрации.

Подсистема идентификации и аутентификация субъектов сетевой среды:

Межсетевой экран (МЭ) должен обеспечивать возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.

Выполнение данного условия обеспечивает процесс туннелирования. Должны использоваться протоколы шифрованного обмена данными PPTP, SSH, SSL, Kerberos, IPsec и им подобные.

МЭ должен обеспечивать идентификацию и аутентификацию всех субъектов прикладного уровня.

Для работы прикладных сетевых служб необходимо предоставить информацию, однозначно определяющую субъекта прикладного уровня. Процесс аутентификации однозначно подтверждает подлинность данного субъекта. Механизм реализации данного условия включает в себя предоставления личного идентификатора или группы идентификаторов пользователя (UserID) и секретных данных, подтверждающих его персону (password, CheckSum).

Подсистема регистрации:

Должна обеспечиваться возможность регистрации и учета фильтруемых пакетов.

В параметры регистрации включаются адрес, время и результат фильтрации. Фильтрация производится по типам адресов, используемых при фильтрации (MAC, IP, sockets).

Должна обеспечиваться возможность регистрации и учета запросов на установление виртуальных соединений.

Данное условие подразумевает регистрацию средством защиты фильтруемого трафика TCP по значениям в заголовках полей source port, destination port и flags (ACK,SYN) для проходящих через него датаграмм.

Должна обеспечиваться локальная сигнализация попыток нарушения правил фильтрации.

Это подразумевает реализацию возможности информирования администратора безопасности о попытках установления запрещенных соединений непосредственно фильтрующим модулем (звуковое сопровождение, вывод сообщения на экран, световая индикация и т.п.).

Должна обеспечиваться возможность дистанционной сигнализации попыток нарушения правил фильтрации.

Это подразумевает возможность информирования уполномоченных лиц о попытках установления запрещенных соединений с помощью электронной почты, пейджинговой службы, SMS-сообщений, popup-сообщений или внешних систем оповещения.

Должна выполняться регистрация и учет запрашиваемых сервисов прикладного уровня.

Идентификация субъектов прикладного уровня производится посредством связки IP-адреса и номера порта удаленного хоста для устанавливаемого сеанса связи.

Должна быть реализована программируемая реакция на события в МСЭ.

Подразумевается возможность формирования заданного уровня детализации событий в журнале регистрации администратору или уполномоченному лицу. Регистрация категорий событий, таких как установка связи, изменение конфигурации и т.д.

Подсистема контроля целостности.

МЭ должен содержать средства контроля за целостностью своей программной и информационной части:

– контроль целостности должен выполняться по контрольным суммам;

– контроль за целостностью должен выполняться по контрольным суммам как в процессе загрузки, так и динамически;

– механизм верификации контрольных сумм должен использовать аттестованный алгоритм;

– анализ контрольных сумм должен проводиться как в процессе загрузки, так и динамически.

Подсистема восстановления.

Средство защиты должно предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств.

Должен быть реализован механизм восстановления функциональности средства защиты при нарушениях в его штатном режиме работы.

Должно обеспечиваться оперативное восстановление свойств МЭ.

Восстановление функциональности должно производиться сразу после обнаружения сбоя в штатной работе.

4.4.5. Требования к подсистеме криптографической защиты информации

Подсистема криптографической защиты информации предназначена для защиты хранящейся на носителях и передаваемой по сети и на носителях конфиденциальной информации путем преобразования ее криптографическими методами.

Должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, а также на съемные портативные носители данных долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию. Доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом. должны использоваться сертифицированные средства криптографической защиты. Их сертификация проводится специальными сертификационными центрами или специализированными предприятиями, имеющими лицензию на проведение сертификации криптографических средств защиты.

При использовании криптографических средств для управления доступом санкционированных пользователей к информационным ресурсам ограниченного распространения криптографические механизмы являются частью системы дискреционного управления доступом, при этом должно быть предусмотрено использование различных ключей шифрования для групп пользователей в соответствии с их полномочиями по доступу к защищаемым ресурсам. Защита ключей шифрования должна осуществляться механизмами управления доступом к элементам системы безопасности.

В случае необходимости передачи конфиденциальной информации за пределы защищаемых ИКС, требуется криптографическая защита передаваемой информации. Передача информации по каналам сети общего назначения также должна осуществляться с использованием криптографических механизмов. При передаче данных по сети конфиденциальная информация должна шифроваться до начала отправки данных по сети. При передаче данных на носителях – до записи на носитель.

4.4.6. Требования к подсистеме антивирусной защиты

Подсистема антивирусной защиты предназначена для защиты от проникновения в защищаемую ИКС вирусоподобных программ, их выявления и нейтрализации их воздействия на данные и рабочую среду путем их поиска, уничтожения и нейтрализации их вредоносных воздействий.

Антивирусная защита рабочих станций и серверов. Управление антивирусной защитой должно осуществляться централизованно, в соответствии с регламентом антивирусной защиты выделенными субъектами системы безопасности (администраторами антивирусной защиты) и данные, формируемые в результате антивирусных проверок должны передаваться в подсистему управления безопасности.

Должна блокировать вирусные воздействия на системные области:

- загрузочные секторы дисков;
- системные области дисков.
- блокировать вирусные воздействия на общесистемное ПО:
- критичные файлы и данные операционной системы.
- блокировать вирусные воздействия на ПО и данные пользователя.

Должна обеспечивать контроль:

- изменения файлов;
- создания и удаления файлов;
- переименования файлов;
- создания и удаления каталогов;
- переименования файлов;
- перемещения файлов из каталога в каталог;
- содержимого системных областей.

Система должна обнаруживать активные неизвестные стелс-вирусы.

Средняя скорость работы в процессе проверки должна составлять не менее 100 Мбайт в минуту.

Должна запускаться автоматически при инициализации АС, а также в ручном режиме. В активном режиме должна обеспечивать обнаружение вирусов в программах и файлах данных, получаемых по каналам связи и с отчуждаемых носителей. В пассивном режиме запускается как самостоятельная задача и после окончания текущей проверки завершает работу. Работает в пассивном режиме (т.е. запускается как самостоятельная задача) и после окончания текущей проверки завершает работу.

Должна обеспечивать обнаружение заранее известных вирусов:

загрузочных вирусов

файловых вирусов

комбинированных вирусов

обнаружение полиморфных и сложно шифрованных вирусов с помощью эмулятора процессора или другого специального анализатора

стелс-вирусов

макрокомандных вирусов в файлах документов

активных вирусов в памяти

Должна обеспечивать обнаружение заранее неизвестных вирусов, в том числе и стелс-вирусов, полиморфных и шифрованных, с вероятностью, не хуже 0.8. Должна обеспечивать обнаружение вирусов в таких объектах, как архивы, компрессированные исполняемые модули, динамические библиотеки и др.

Должна обеспечивать обнаружение вирусов в объектах, загружаемых на рабочие станции из сети.

Должна обеспечивать среднюю скорость работы не хуже 0.5 Гб/час.

В случае обнаружения вирусов должна обеспечивать возможность удаления или копирования на выделенный носитель зараженных объектов.

Должна обеспечивать удаление обнаруженных вирусов следующих типов:

- известных вирусов (лечение) в загрузочных секторах диска;
- известных файловых вирусов;
- известных вирусов-спутников;
- известных вирусов, внедряющихся в драйверы устройств;
- известных вирусов в пакетных файлах;
- известных комбинированных вирусов ;
- известных стелс-вирусов;
- известных полиморфных и сложно шифрованных вирусов;
- известных макрокомандных вирусов в файлах документов;
- вирусов в объектах, загружаемых на рабочие станции из сети;
- неизвестных вирусов.

Должна обеспечивать удаление уже активизированных вирусов.

Должна обеспечивать самоконтроль целостности (неинфицированности) при запуске.

Должна контролировать целостность системной информации:

- загрузочные секторы дисков;
- системные области дисков.

Должна контролировать целостность критичных файлов и данных операционной системы.

Должна контролировать целостность программ и данных пользователя.

Для повышения устойчивости к вирусным и вирусоподобным воздействиям, контроль целостности должен осуществляться на основе хэш-функции. Вероятность совпадения хеш-значений для двух случайно равновероятно выбранных объектов контроля должна быть не более $10^{-9.}$

Периодически, по мере появления новых вирусов, должно производится обновление. Это затрагивает как механизмы обнаружения и удаления, так и расширение списка известных вирусов и алгоритмов поиска и удаления неизвестных вирусов.

Должна обеспечивать регистрацию событий в системном журнале по следующим параметрам:

- событие;
- дата/время;
- объект;
- тип воздействия.

Должна обеспечивать звуковую сигнализацию при обнаружении попытки заражения системных областей и общесистемного ПО и данных.

Должна обеспечивать звуковую сигнализацию при обнаружении заражения и(или) активного вируса.

Должна обеспечивать удаленный сбор статистики по регистрируемым событиям, удаленную сигнализацию при обнаружении попыток заражения и (или) обнаружении вируса.

Должна обеспечивать удаленную настройку правил регистрации событий.

Должна позволять проводить автоматизированную обработку журналов регистрации.

Требования к антивирусным шлюзам. Антивирусные шлюзы предназначены для защиты от проникновения в защищаемую АС вирусоподобных программ, их выявления и нейтрализации на этапе передачи данных между сегментами сети путем антивирусной проверки содержимого, передаваемого по различным прикладным протоколам.

Для реализации этих функций антивирусные шлюзы должны иметь в своем составе следующие подсистемы:

- подсистема управления;
- подсистема контроля целостности;
- подсистема обнаружения;
- подсистема удаления;
- подсистема гарантированности свойств;
- подсистема регистрации.

Подсистема управления:

Архитектура антивирусных шлюзов должна быть основана на принципе централизованного управления шлюзами как компонентами системы антивирусной защиты АС.

Должна быть реализована архитектура, позволяющая организовать централизованное управление антивирусными шлюзами с помощью средств управления АВС, включающих в свой состав средства антивирусной защиты рабочих станций и серверов.

Антивирусные шлюзы должны быть реализованы в виде агентов АВС, устанавливаемых на серверные ОС, используемые для организации межсетевого взаимодействия в современных гетерогенных АС: (Windows NT/2000/XP, xNix), которые должны обеспечивать выполнение функций антивирусной проверки содержимого передаваемой по сетевым каналам информации.

Управление агентами должно осуществляться по защищенному логическому каналу, с аутентификацией абонентов (должна быть предусмотрена защита от навязывания управляющих воздействий агентам антивирусной системы).

Подсистема управления должна обеспечивать возможность создания логической структуры системы антивирусной защиты, не зависящей от логической структуры ЛВС. Возможность включения в сегмент, защищаемый с помощью АВС не должна зависеть от количества доменов NT, от сегментации сети с помощью средств физической и логической сегментации, а также должна быть реализована возможность управления агентами АВС через межсетевые экраны.

Агенты должны интегрироваться в системы передачи данных (почтовые сервера, прокси-серверы) в качестве дополнительного модуля.

Подсистема контроля целостности должна обеспечивать контроль:

- изменения файлов;
- создания и удаления файлов;
- переименования файлов;
- создания и удаления каталогов;
- переименования файлов;
- перемещения файлов из каталога в каталог;
- содержимого системных областей.

Система должна обнаруживать активные неизвестные стелс-вирусы. Средняя скорость работы в процессе проверки должна составлять не менее 100 Мбайт в минуту. Подсистема должна запускаться автоматически при инициализации АС, а также в ручном режиме.

Контроль целостности должен осуществляться путем перехвата обращений к функциям ОС работы с файловой системой и задания перечня разрешенных действий; путем сравнения зафиксированного эталонного состояния объектов с их текущим состоянием. Фиксация эталонного состояния контролируемых объектов должна осуществляться путем создания эталонных копий, хранение которых осуществляется в защищенных областях жесткого диска или на защищенных внешних носителях. Также должен осуществляться выборочный контроль изменений ветвей реестра (для ОС Windows) с целью предотвращения автоматического запуска внедренных вирусов при старте ОС. Должен существовать удобный пользовательский интерфейс по созданию перечня контролируемых объектов с помощью масок, шаблонов, поискового аппарата.

Подсистема обнаружения:

Подсистема должна осуществлять обнаружение и нейтрализацию вирусоподобных программ, передаваемых по сети с помощью прикладных протоколов передачи данных (SMTP, POP3, HTTP) путем анализа содержимого сетевых пакетов на предмет наличия вирусоподобного кода.

Модуль проверки должен осуществлять постоянную антивирусную проверку всей проходящей по контролируемым протоколам информации. Кроме того, должна быть предусмотрена автоматическая и по команде проверка объектов файловой системы сервера.

Должны быть предусмотрены возможность пересылки зараженных пакетов на определенных адрес, сохранения и регистрации данных о пакетах с целью проведения расследований и сигнализации путем отправки электронных писем на адрес администратора.

Должна осуществляться проверка всех участков полей данных пакетов прикладного уровня.

Должна быть предусмотрена возможность динамического обновления антивирусных баз и динамического обновления списка защищаемых ресурсов, без перезагрузки сервера.

Компоненты АВС должны загружаться в момент старта ОС. Для NT-подобных систем АВС должны загружаться как сервисы, останов которых может осуществлять только пользователь с привилегиями администратора; для xNix-подобных систем должна быть предусмотрена загрузка в автоматическом режиме, не требующем вмешательства пользователя в процесс работы АВС. Для ОС Win95/98 компоненты АВС должны загружаться как сервисы ОС. Должна обеспечивать обнаружение заранее известных вирусов:

- загрузочных вирусов;
- файловых вирусов;
- комбинированных вирусов;
- полиморфных и сложно шифрованных вирусов с помощью эмулятора процессора или другого специального анализатора;
- стелс-вирусов;
- макрокомандных вирусов в файлах документов;
- активных вирусов в памяти.

Должна обеспечивать обнаружение заранее неизвестных вирусов, в том числе и стелс-вирусов, полиморфных и шифрованных, с вероятностью, не хуже 0.8.

Должна обеспечивать обнаружение вирусов в таких объектах, как архивы (ZIP, ARJ, LHA, RAR и др.), компрессированные исполняемые модули (PKLITE, LZEXE, DIET, COM2EXE и др.), динамические библиотеки, файлы почтовых баз данных клиентских почтовых программ (MS Outlook и др.) путем интерпретации форматов перечисленных программ.

Должна обеспечивать обнаружение вирусов в объектах, загружаемых на рабочие станции из сети путем контроля сетевого трафика.

Должна быть совместима с подсистемой контроля целостности, а также с подсистемой регистрации остальных компонент комплекса (регистрации и контроля целостности).

Должна обеспечивать среднюю скорость работы не хуже 0.5 Гб/час

В случае обнаружения вирусов должна обеспечивать запуск подсистемы удаления, с передачей ей в качестве параметров результатов проверки.

Подсистема удаления:

Может работать как самостоятельная подсистема, так и совместно с подсистемой обнаружения и (или) контроля целостности.

Должна обеспечивать удаление обнаруженных вирусов следующих типов:

- известных вирусов (лечение) в загрузочных секторах диска;
- известных файловых вирусов;
- известных вирусов-спутников;
- известных вирусов, внедряющихся в драйверы устройств;
- известных вирусов в пакетных файлах;
- известных комбинированных вирусов;
- известных стелс-вирусов;
- известных полиморфных и сложно шифрованных вирусов;
- известных макрокомандных вирусов в файлах документов;

– вирусов в объектах, загружаемых на рабочие станции из сети;
– известных вирусов в архивах;
– неизвестных вирусов.

Должна обеспечивать удаление уже активизированных вирусов.

Должна быть совместима с подсистемой контроля целостности, а также с подсистемой регистрации остальных компонент комплекса (обнаружения и регистрации).

Должна обеспечивать среднюю скорость работы не хуже 0.5 Гб/час.

Должна иметь удобный интерфейс, позволяющий задавать возможный воздействия (удаление, перемещение, сигнализация) в зависимости от различных критериев.

Подсистема гарантированности свойств:

Должна обеспечивать самоконтроль целостности (неинфицированности) данного АВС при его запуске.

Должна контролировать целостность системной информации:
– загрузочные секторы дисков;
– системные области дисков.

Должна контролировать целостность критичных файлов и данных операционной системы.

Должна контролировать целостность программ и данных пользователя.

Для повышения устойчивости к вирусным и вирусоподобным воздействиям, контроль целостности АВС должен осуществляться на основе хэш-функции. Вероятность совпадения хеш-значений для двух случайно равновероятно выбранных объектов контроля должна быть не более $10^{-9.}$

Периодически, по мере появления новых вирусов, должно производится обновление АВС. Это затрагивает как механизмы обнаружения и удаления, так и расширение списка известных АВС вирусов и алгоритмов поиска и удаления неизвестных вирусов.

Подсистема регистрации:

Должна обеспечивать регистрацию событий в системном журнале по следующим параметрам:
– событие;
– дата/время;
– объект;
– адрес узла сети, с которого пришел зараженный объект;
– тип вируса.

Должна обеспечивать звуковую сигнализацию при обнаружении попытки заражения системных областей и общесистемного ПО и данных.

Должна обеспечивать звуковую сигнализацию при обнаружении заражения и(или) активного вируса.

Должна быть совместима с аналогичными подсистемами остальных компонент комплекса.

Должна обеспечивать удаленный сбор статистики по регистрируемым событиям, удаленную сигнализацию при обнаружении попыток заражения и (или) обнаружении вируса.

Должна обеспечивать удаленную настройку правил регистрации событий.

Должна позволять проводить автоматизированную обработку журналов регистрации.

4.4.7 Требования к подсистеме резервирования и восстановления информации

Подсистема резервирования и восстановления предназначена для обеспечения непрерывной работы АС и ее восстановления путем резервирования программ и данных и восстановления их из резервных копий.

Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность системы и выполнение ею своих задач (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д. Резервному копированию подлежат рабочие конфигурации серверов, на которых хранится и обрабатывается конфиденциальная информация.

Все программные средства, используемые в системе должны иметь эталонные (дистрибутивные) копии. Их местонахождение и сведения об ответственных за их создание, хранение и использование должны быть указаны в формулярах на каждую ПЭВМ (рабочую станцию). Там же должны быть указаны перечни наборов данных, подлежащих страховому копированию, периодичность копирования, место хранения и ответственные за создание, хранение и использование страховых копий данных.

Контроль соответствия состояния защищаемых информационных ресурсов и рабочих конфигураций серверов и АРМ, обрабатывающих конфиденциальную информацию, осуществляется подсистемой контроля эталонного состояния информации и рабочей среды.

Должно обеспечиваться оперативное восстановление программ с использованием эталонных копий и данных, входящих в перечень неизменяемых защищаемых информационных ресурсов (используя страховые копии) в случае их уничтожения или порчи в серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий.

4.4.8 Требования к подсистеме контроля эталонного состояния информации и рабочей среды

Подсистема контроля эталонного состояния информации и рабочей среды предназначена для фиксации и динамического контроля изменений состояния фиксированных наборов данных, эталонного состояния параметров рабочей среды и передаче данных об этих изменениях подсистеме управления

безопасностью путем сравнения текущих характеристик контролируемых объектов с эталонными характеристиками.

Должна быть обеспечена возможность выбора объектов и фиксация их эталонного состояния. Выбор объектов осуществляется на основе перечня защищаемых информационных ресурсов и периодичности их изменений, а также перечня программных средств, участвующих в обработке конфиденциальной информации и степени их влияния на функционирование защищаемой ИКС.

Контроль эталонного состояния должен осуществляться динамически, в соответствии с регламентом, при загрузке ОС серверов, рабочих станций, при регистрации пользователей в ИКС или в системе безопасности. Должна быть реализована функция периодического контроля.

Результаты проверок должны передаваться для обработки подсистеме управления безопасностью.

4.4.9 Требования к подсистеме управления безопасностью

Подсистема управления безопасностью предназначена для контроля эффективности защиты, регистрации данных о событиях в ИКС, событиях в системе безопасности, автоматизированной обработки данных и поддержки принятия решения по выработке управляющих воздействий на другие подсистемы системы безопасности путем сбора и автоматизированной обработки регистрационных данных.

Подсистема управления безопасностью реализует функции поддержания системы защиты в актуальном состоянии: контроля защищенности; управления безопасностью и оценки риска; регистрации и обнаружения атак; управления цифровыми сертификатами.

Комплексный подход к поддержанию системы информационно-компьютерной безопасности в актуальном состоянии должен охватывать следующие функциональные области:

– периодический, а по возможности, динамический контроль защищенности, обеспечивающий своевременное выявление появившихся уязвимостей, которые могут быть использованы для нанесения атак;

– обнаружение атак в режиме реального времени, позволяющее своевременно определить и локализовать попытки выполнения несанкционированных действий и выявить факты несанкционированного воздействия на компьютерные ресурсы;

– централизованное и упреждающее управление, позволяющее на основе автоматизированной поддержки принятия решений, а также эффективного контроля над пользователями и ресурсами сети снизить количество ошибок администрирования и предпринять превентивные меры, не допускающие развития событий по наихудшему сценарию.

Независимо от мощности системы защиты невозможно достигнуть высокой информационной безопасности без контроля защищенности всех объектов компьютерной сети. Эффективный несанкционированный доступ к информации осуществляется только на основе слабостей (уязвимостей) системы защиты

атакуемой компьютерной сети. Поэтому своевременное выявление этих слабостей и устранение найденных уязвимостей позволит предотвратить несанкционированные воздействия на защищаемые компьютерные ресурсы при реализации атак. Любая проверка, не учтенная при контроле защищенности, может привести к наличию скрытой уязвимости и компрометации всей системы защиты.

Контроль защищенности предполагает периодическое, а в некоторых случаях - динамическое, выполнение следующих базовых функций:

– проверку системы защиты на соответствие новым руководящим и нормативным документам в области информационно-компьютерной безопасности;

– контроль правил корректного использования средств защиты в зависимости от их состава и назначения;

– контроль целостности и подлинности компонентов системы защиты;

– контроль корректности модификации параметров конфигурирования системы защиты;

– динамическая регистрация данных о функционировании системы защиты, их анализ и уведомление ответственных лиц при нарушении правильности работы защитных средств;

– тестирование подсистем защиты на правильность реагирования при моделировании процесса реализации возможных атак;

– контроль работоспособности подсистем защиты при моделировании нарушений работоспособности отдельных элементов компьютерной сети;

– проверка на отсутствие ошибок администрирования и конфигурирования;

– анализ политики формирования и использования эталонной информации (ключей, паролей и др.);

– проверка на наличие своевременных обновлений программных средств;

– проверка на отсутствие программных закладок и вирусов.

Проверка системы защиты на соответствие новым руководящим и нормативным документам в области информационно-компьютерной безопасности позволяет своевременно выявить недостатки в системе защиты на основе анализа передового опыта по систематизации предъявляемых к таким системам требований. Так как в нашей стране руководящие документы и стандарты по защите электронной информации появляются не так часто, то полезно ознакомиться со 2-й версий международного стандарта (ISO International Standard 15408) по оценке безопасности информационных технологий (Common Criteria for Information Technology Security Evaluation - Общие критерии оценки безопасности информационных технологий).

Главные преимущества Общих Критериев (ОК) - полнота требований информационной безопасности, гибкость в применении и открытость для последующего развития с учетом новейших достижений науки и техники. Общие Критерии разработаны таким образом, чтобы удовлетворить потребности всех трех групп пользователей, имеющих отношение к средствам и системам защиты (потребителей, разработчиков и экспертов). В Общих критериях проведена

классификация широкого набора функциональных требований и требований гарантированности, определены структуры их группирования и принципы целевого использования. Данный стандарт может быть весьма полезным в качестве руководства при разработке средств и систем с функциями защиты информации, а также при приобретении коммерческих продуктов и систем с такими функциями.

Контроль правил корректного использования средств защиты в зависимости от их состава и назначения состоит в периодическом контроле и пересмотре политики безопасности на ее административном и процедурном уровнях. При изменении структуры, технологических схем или условий функционирования компьютерной системы, как концепция защиты, так и детальные процедурные меры могут меняться, в особенности, конкретные инструкции по информационно-компьютерной безопасности, относящиеся к администраторам и пользователям компьютерной системы.

Контроль целостности и подлинности компонентов системы защиты предполагает периодическое или динамическое выполнение следующих действий:

– контроль наличия требуемых резидентных компонентов системы защиты в оперативной памяти компьютера;

– контроль всех программ системы защиты, находящихся во внешней и оперативной памяти, на соответствие эталонным характеристикам;

– контроль корректности параметров настройки системы защиты, располагаемых как в оперативной, так и во внешней памяти;

– контроль корректности эталонной информации (идентификаторов, паролей, ключей шифрования и т.д.).

При контроле корректности модификации параметров конфигурирования системы защиты подсистема контроля не должна допустить установку параметров, противоречащих политике безопасности, принятой в организации.

Регистрация данных о функционировании системы защиты предполагает фиксацию и накопление информации о следующих действиях:

– действиях всех подсистем защиты;

– действиях всех администраторов и пользователей других категорий по использованию защитных средств.

Кроме регистрации данных о функционировании системы защиты должен быть обеспечен и периодический анализ накопленной информации. Основной задачей такого анализа является своевременное определение недопустимых действий, а также прогнозирование степени безопасности информации и процесса ее обработки в вычислительной системе.

Для возможности и результативности периодического анализа предварительно должны быть подготовлены правила, описывающие политику работы системы защиты по одному из принципов:

– в работе системы защиты допустимо все, что не запрещено;

– в работе системы защиты запрещено все, что явно не допустимо.

Более высокий уровень контроля и безопасности обеспечивает второй принцип, так как на практике не всегда удается полностью учесть все действия, которые запрещены. Надежнее определить все действия, которые разрешены, и запретить все остальные.

При обнаружении подсистемой контроля любых нарушений в правильности функционирования подсистемы защиты должно быть выполнено немедленное уведомление соответствующих представителей службы безопасности.

Тестирование подсистем защиты на правильность реагирования при моделировании процесса реализации возможных атак выполняется с помощью специализированных средств анализа защищенности, которые, как правило, обеспечивают выполнение и оставшихся функций контроля защищенности.

Процесс анализа защищенности предполагает исследование проверяемых объектов для выявления в них «слабых мест» и обобщение полученных сведений, в том числе в виде отчета. Если система, реализующая данную технологию, содержит адаптивный компонент, то устранение найденной уязвимости будет осуществляться автоматически. При анализе защищенности обычно идентифицируются:

- ошибки программно-аппаратных средств;
- программные закладки типа Back Orifice;
- слабые пароли, ключи;
- восприимчивость к проникновению из внешних систем и атакам типа «отказ в обслуживании»;
- отсутствие необходимых обновлений (patch, hotfix) ПО;
- ошибки администрирования, например, выделение незащищенных ресурсов в общее пользование;
- неправильная настройка различных программных систем (межсетевых экранов, серверов, баз данных и др.).

4.4.10 Требования к средствам построения защищенных виртуальных сетей (VPN)

Средства построения защищенных виртуальных сетей (VPN) должны осуществлять логическую сегментацию сетей путем выделения трафика защищаемых АС и обеспечения следующих свойств информации в защищаемом сегменте: подлинности, целостности, конфиденциальности.

Для реализации этих функций VPN должна иметь в своем составе следующие подсистемы:

- управления;
- сегментации;
- регистрации.

Подсистема управления VPN:

Должна осуществлять централизованное управление компонентами VPN в защищаемом сегменте.

– должна быть реализована клиент-серверная архитектура, включающая в себя центр управления компонентами VPN;

– должно быть реализовано централизованное управление настройками компонент VPN (механизм удаленной настройки);

– удаленная настройка должна осуществляться по защищенному каналу с аутентификацией абонентов канала;

– должно быть реализовано централизованное распределение криптографических ключей на базе центра сертификации;

– должен быть графический интерфейс создания и изменения профилей настройки VPN;

– должна быть реализована возможность создания резервной копии конфигурации VPN;

– должен быть обеспечен постоянный контроль выполнения функций защиты агентами, установленными на рабочих станциях и серверах VPN.

В случае, когда локальная сеть является небольшой, то для управления удаленными соединениями с этой сетью достаточно одного сервера удаленного доступа. Однако, если локальная сеть объединяет достаточно большие сегменты и число удаленных пользователей существенно увеличивается, то одного сервера удаленного доступа становится недостаточно. При использовании в одной локальной сети нескольких серверов удаленного доступа высокая эффективность сетевого управления будет достигнута в условиях разделения коммуникационных функций и функций контроля доступа к компьютерным ресурсам. Для централизованного контроля удаленного доступа должен быть выделен отдельный сервер, называемый сервером аутентификации и предназначенный для проверки подлинности удаленных пользователей, определения их полномочий, а также фиксации и накопления регистрационной информации, связанной с удаленным доступом.

Даже при наличии в локальной сети одного сервера удаленного доступа, целесообразно применять централизованную систему аутентификации. Поддержание отдельной базы данных с учетными записями на сервере удаленного доступа приводит к избыточности функций администрирования и может стать причиной несогласованности в правилах контроля доступа к ресурсам сети. Эффективность администрирования и надежность защиты увеличивается, если сервер удаленного доступа запрашивает необходимую для аутентификации информацию непосредственно у сервера, на котором хранится общая база данных системы защиты компьютерной сети.

Доступ удаленных пользователей к ресурсам локальной сети должен контролироваться в соответствии с политикой безопасности, проводимой в организации, которой принадлежит локальная сеть. Надежность разграничения доступа к компьютерным ресурсам может быть обеспечена только в случае надежной аутентификации пользователей. По отношению к удаленным пользователям требования по надежности проверки их подлинности существенно возрастают. Это связано с тем, что удаленным пользователям, в отличие от пользователей локальных, для доступа к ресурсам локальной сети не нужно

проходить процедуру физического контроля полномочий по допуску на территорию организации. При работе с «невидимыми» удаленными пользователями становится значительно труднее гарантировать, что доступ к ресурсам локальной сети смогут получить только лица, имеющие на это соответствующие полномочия.

В случае удаленного доступа к локальной сети для надежной проверки подлинности взаимодействующих сторон должны поддерживаться следующие функциональные возможности:

– согласование используемых протоколов аутентификации и отсутствие жесткой привязки к конкретным протоколам проверки подлинности;

– блокирование любых попыток обхода фазы аутентификации после установки удаленного соединения;

– аутентификация каждой из взаимодействующих сторон - как удаленного пользователя, так и сервера удаленного доступа, что исключает возможность маскировки под одного из участников взаимодействия;

– проведение не только начальной аутентификации перед допуском к ресурсам локальной сети, но и динамической аутентификации взаимодействующих сторон в процессе работы удаленного соединения; данная функция устраняет риск перехвата соединения и маскировки под одного из участников взаимодействия после окончания начальной аутентификации;

– использование одноразовых паролей либо криптозащита передаваемых секретных паролей, исключающая возможность повторного использования перехваченной информации для подложной аутентификации.

Подсистема сегментации:

Защита информации в процессе передачи по открытым каналам связи должна основываться на выполнении следующих функций: защиты трафика от прослушивания путем шифрования логического канала между выделенными абонентами, аутентификации абонентов защищаемой сети и обеспечения подлинности и целостности передаваемых данных с использованием криптографических механизмов.

В случае удаленного доступа к локальной сети для надежной проверки подлинности взаимодействующих сторон должны поддерживаться следующие функциональные возможности:

– согласование используемых протоколов аутентификации и отсутствие жесткой привязки к конкретным протоколам проверки подлинности;

– блокирование любых попыток обхода фазы аутентификации после установки удаленного соединения;

– аутентификация каждой из взаимодействующих сторон - как удаленного пользователя, так и сервера удаленного доступа, что исключает возможность маскировки под одного из участников взаимодействия;

– проведение не только начальной аутентификации перед допуском к ресурсам локальной сети, но и динамической аутентификации взаимодействующих сторон в процессе работы удаленного соединения; данная

функция устраняет риск перехвата соединения и маскировки под одного из участников взаимодействия после окончания начальной аутентификации.

Необходимо использование одноразовых паролей либо криптозащита передаваемых секретных паролей, исключающая возможность повторного использования перехваченной информации для подложной аутентификации.

Вопросы по разделу 4

2.1. Приведите краткое описание типовой ИКС

2.2. Дайте определение основных приоритетов информационной безопасности

2.3. Опишите модели нарушителя в ИКС

2.4. Значимые угрозы в ИКС

3.1. Общие требования построения защищенной корпоративной сети

3.2. Требования к подсистеме обеспечения безопасности сетевого взаимодействия

3.3. Требования к подсистеме обеспечения безопасности сетевого взаимодействия

3.4. Требования к подсистеме аутентификации и управления доступом

3.5. Требования к подсистеме криптографической защиты информации

3.6. Требования к подсистеме антивирусной защиты

3.7. Требования к подсистеме резервирования и восстановления информации

3.8. Требования к подсистеме контроля эталонного состояния информации и рабочей среды

3.9. Требования к подсистеме управления безопасностью

3.10. Требования к средствам построения защищенных виртуальных сетей (VPN)

Заключение

Предотвращать необходимо не только несанкционированный доступ к информации с целью ее раскрытия или нарушения ее целостности, но и попытки проникновения с целью нарушения работоспособности этих систем. Защищать необходимо все компоненты систем: оборудование, программы, данные и персонал.

Все усилия по обеспечению внутренней безопасности систем должны фокусироваться на создании надежных и удобных механизмов принуждения всех ее законных пользователей и обслуживающего персонала к безусловному соблюдению требований политики безопасности, то есть установленной в организации дисциплины прямого или косвенного доступа к ресурсам и информации.

Одним из важнейших аспектов проблемы обеспечения безопасности компьютерных систем является выявление, анализ и классификация возможных путей реализации угроз безопасности, то есть возможных каналов несанкционированного доступа к системе с целью нарушения ее работоспособности или доступа к критической информации, а также оценка реальности реализации угроз безопасности и наносимого при этом ущерба.

Все известные меры защиты компьютерных систем подразделяются на: законодательные, морально - этические, административные, физические и технические (аппаратурные и программные). Все они имеют свои достоинства и недостатки.

Наилучшие результаты достигаются при системном подходе к вопросам безопасности компьютерных систем и комплексном использовании различных методов и средств их защиты на всех этапах жизненного цикла систем.

Основными универсальными механизмами противодействия угрозам безопасности, реализуемыми в конкретных средствах защиты, являются:

- идентификация (именование и опознавание), аутентификация (подтверждение подлинности) и авторизация (присвоение полномочий) субъектов;
- контроль (разграничение) доступа к ресурсам системы;
- регистрация и анализ событий, происходящих в системе;
- контроль целостности ресурсов системы.

Литература

1 И.Р. Конеев, А.В. Беляев Информационная безопасность предприятия. – СПб: БХВ-Санкт-Петербург, 2003.

2 М.С. Вертузаев, О.М. Юрченко, Защита информации в компьютерных системах от несанкционированного доступа. – М.: ДМК Пресс, 2002.

3 А.В. Петраков Основы практической защиты информации. Учебное пособие для вузов. – М.: Радио и связь, 2001.

4 А. Лукацкий Обнаружение атак. –СПб.: БХВ-Санкт-Петербург, 2001.

5 В.В. Домарев Защита информации и безопасность компьютерных систем. – Киев: "DiaSoft", 1999.

6 А.В. Соколов, В.Ф. Шаньгин Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002.

7 М. Ховард, Д. Лебланк Защищенный код/Пер. с англ. – М.: Издательско-торговый дом «Русская редакция», 2003.

8 И.Д. Медведковский, Б.В. Семьянов, Д.Г. Леонов, А.В. Лукацкий Атака из Internet, 2002.

9 В. Зима, А. Молдовян, Н. Молдовян Безопасность глобальных сетевых технологий. – СПб: БХВ-Санкт-Петербург, 2002.