СОДЕРЖАНИЕ

1 ОСНОВЫ БЕЗОПАСНОСТИ СЕТЕВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1.1. Актуальность проблемы обеспечения безопасности сетевых информационных технологий

Объективные причины проблемы обеспечения информационной безопасности:

1. Расширение сферы применения средств вычислительной техники.
2. Развитие и распространение вычислительных сетей.
3. Доступность средств вычислительной техники (прежде всего ПК) в широких слоях населения.
4. Отставание в области создания непротиворечивой системы законодательно-правового регулирования отношений в сфере накопления, использования и защиты информации.
5. Развитие и широкое распространение компьютерных вирусов.

Трудности решения практических задач защиты компьютерной информации связаны с отсутствием развитой стройной теории и необходимых научно-технических и методических основ обеспечения защиты информации.

1.2. Основные понятия информационной безопасности

Информация – сведения о фактах, событиях, процессах и явлениях, о состоянии объектов (их свойствах и характеристиках) в некоторой предметной области, необходимые для оптимизации принимаемых решений в процессе управления данными объектами.

Большие объемы информации накапливаются, хранятся и обрабатываются в автоматизированных системах, построенных на основе современных средств вычислительной техники и связи.

Автоматизированная система (АС) обработки информации – организационно-техническая система, представляющая собой совокупность взаимосвязанных компонентов:

- технических средств обработки и передачи данных
- методов и алгоритмов обработки в виде соответствующего программного обеспечения
- информации (массивов, наборов, баз данных) на различных носителях
- обслуживающего персонала и пользователей системы.

Для обеспечения защиты компьютерной информации необходимо постоянно поддерживать свойства информации и систем ее обработки:

- доступность информации;
- целостность информации;

- конфиденциальность информации.

«Безопасность автоматизированной системы» (системы обработки информации, компьютерной системы) – защищенность всех ее компонентов (технических средств, программного обеспечения, данных, пользователей и персонала) от разного рода нежелательных воздействий.

Угроза - это потенциально возможное событие, явление или процесс, которое путем воздействия на компоненты информационной системы может привести к нанесению ущерба.

Уязвимость - это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

Атака - это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы.

1.3. Классификация уязвимостей

1. По источникам возникновения уязвимостей

А) на этапе проектирования. Например сервис TELNET, в котором имя пользователя и пароль передаются по сети в открытом виде. Это явный недостаток, заложенный на этапе проектирования. Некоторые уязвимости подобного рода трудно назвать недостатками, скорее это особенности проектирования. Например, особенность сетей Ethernet - общая среда передачи.

Б) на этапе реализации (программирования). Ошибки программирования стека TCP/IP, приводящие к отказу в обслуживании; ошибки при написании приложений, приводящие к переполнению буфера и т.п.

В) Уязвимости могут быть следствием ошибок, допущенных в процессе эксплуатации информационной системы: неверное конфигурирование операционных систем, протоколов и служб, использование нестойких паролей пользователей, паролей учетных записей «по умолчанию» и др.

2. по уровню в инфраструктуре ВС

а) Уровень сети - уязвимости сетевых протоколов (стека TCP/IP, протоколов NetBEUI, IPX/SPX).

б) Уровень операционной системы охватывает уязвимости.

в) На уровне баз данных находятся уязвимости конкретных СУБД - Oracle, MS SQL, Sybase и др. Этот уровень рассматривается отдельно, потому что базы данных, как правило, являются неотъемлемой частью АС любой компании.

г) К уровню приложений относятся уязвимости программного обеспечения WEB, SMTP серверов и т.п.

д) Персонал и пользователи системы также уязвимы. Например, один из путей внедрения вредоносных программ - это провоцирование пользователей на запуск присланных по электронной почте приложений.

3. по степени риска

Высокий уровень риск. Возможность получить непосредственный доступ к узлу с правами суперпользователя, или в обход межсетевых экранов или других средств защиты (полный контроль над атакуемым объектом).

Средний уровень риска. Возможность получить информацию, которая с высокой степенью вероятности позволит в дальнейшем получить полный контроль над объектом и доступ к любым его ресурсам.

Низкий уровень риска. Уязвимости, позволяющие осуществлять сбор критичной информации о системе.

1.4. Классификация атак

1. по целям

- нарушение нормального функционирования атакуемого объекта (отказ в обслуживании);
- получение конфиденциальной и критичной информации;
- модификация и фальсификация данных;
- получение полного контроля над объектом атаки.

2. по мотивации действий

- случайность, безответственность, халатность;
- самоутверждение, любопытство;
- вандализм;
- принуждение;
- месть;
- корыстный интерес.

3. по местонахождению нарушителя

- в одном сегменте с объектом атаки;
- в разных сегментах с объектом атаки.

От взаимного расположения атакующего и жертвы зависит механизм реализации атаки. Как правило, осуществить межсегментную атаку бывает сложнее.

4. по механизму реализации атак

- пассивное прослушивание. Перехват трафика сетевого сегмента.
- подозрительная активность. Сканирование портов (служб) объекта атаки, попытки подбора пароля.
- бесполезное расходование вычислительного ресурса. Исчерпание ресурсов атакуемого узла или группы узлов, приводящее к снижению производительности (переполнение очереди запросов на соединение и т п.)
- Нарушение навигации (создание ложных объектов и маршрутов). Изменение маршрута сетевых пакетов, таким образом, чтобы они проходили через хосты и маршрутизаторы нарушителя, изменение таблиц соответствия условных Internet-имен и IP-адресов (атаки на DNS) и т.п.
- выведение из строя. Посылка пакетов определённого типа на атакуемый узел, приводящая к отказу узла или работающей на нём службы (WinNuke и др.)
- запуск приложений на объекте атаки. Выполнение враждебной программы в оперативной памяти объекта атаки (троянские кони, передача управления враждебной программе путём переполнения буфера, исполнение вредоносного мобильного кода на Java или ActiveX и др.)

1.5. Основные механизмы защиты компьютерных систем

Для защиты компьютерных систем от неправомерного вмешательства в процессы их функционирования и несанкционированного доступа (НСД) к

информации используются следующие основные методы защиты (защитные механизмы):

- идентификация (именование и опознавание), аутентификация (подтверждение подлинности) субъектов (пользователей) и объектов (ресурсов, компонентов, служб) системы;
- разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователям;
- регистрация и оперативное оповещение о событиях, происходящих в системе и имеющих отношение к безопасности;
- криптографическое закрытие хранимых и передаваемых по каналам связи данных;
- контроль целостности и аутентичности (подлинности и авторства) передаваемых и хранимых данных;
- изоляция (защита периметра) компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации путем трансляции адресов);
- контроль вложений (выявление компьютерных вирусов, вредоносных кодов и их нейтрализация);
- выявление уязвимостей (слабых мест) системы;
- обнаружение и противодействие атакам (опасным действиям нарушителей).

Все эти механизмы защиты могут применяться в конкретных технических средствах и системах защиты в различных комбинациях и вариациях. Наибольший эффект достигается при их системном использовании в комплексе с другими видами мер защиты.

1.5.1 Идентификация и аутентификация пользователей

Идентификация - это присвоение индивидуальных имен, номеров или специальных устройств (идентификаторов) субъектам и объектам системы, а так же их распознавание. Чаще всего в качестве идентификаторов применяются номера или условные обозначения в виде набора символов.

Аутентификация - это проверка (подтверждение) подлинности идентификации субъекта или объекта системы.

Аутентификация пользователей осуществляется обычно:

- путем проверки знания ими паролей (специальных секретных последовательностей символов);
- путем проверки владения какими-либо специальными устройствами (карточками, ключевыми вставками и т.п.) с уникальными признаками;
- путем проверки уникальных физических характеристик и параметров (отпечатков пальцев, особенностей радужной оболочки глаз, формы кисти рук и т.п.) самих пользователей при помощи специальных биометрических устройств;
- путем проверки специальных сертификатов соответствия, выданных доверенным органом (третьей стороной, которой доверяют оба взаимодействующих субъекта).

Многие современные СЗИ кроме клавиатуры используют и другие типы идентификаторов — магнитные карточки, радиочастотные бесконтактные

(proximity) карточки, интеллектуальные (smart) карточки, электронные таблетки Touch Memory.

Идентификация и аутентификация пользователей должна производиться при каждом их входе в систему и при возобновлении работы после кратковременного перерыва.

1.5.2. Регистрация и оперативное оповещение о событиях безопасности

Механизмы регистрации предназначены для получения и накопления (с целью последующего анализа) информации о состоянии ресурсов системы и о действиях субъектов, признанных потенциально опасными для системы. Анализ собранной информации (аудит) позволяет выявить факты совершения нарушений, характер воздействий на систему, определить, и подсказать метод расследования нарушения и исправления ситуации.

При регистрации событий безопасности в системном журнале обычно фиксируется:

- дата и время события;
- идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;
- действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

В развитых системах защиты подсистема оповещения связана с механизмами оперативного автоматического реагирования на определенные события. Могут поддерживаться следующие основные способы реагирования на обнаружение НСД (возможно с участием администратора безопасности):

- подача сигнала тревоги;
- извещение администратора безопасности;
- извещение владельца информации о НСД к его данным;
- снятие программы (задания) с дальнейшего выполнения;
- отключение (блокирование работы) терминала или компьютера, с которого были осуществлены попытки НСД к информации;
- исключение нарушителя из списка зарегистрированных пользователей и т.п.

1.5.3. Контроль целостности программных и информационных ресурсов

Механизм контроля целостности ресурсов системы предназначен для своевременного обнаружения модификации ресурсов системы. Он позволяет обеспечить правильность функционирования системы защиты и целостность обрабатываемой информации.

Контроль целостности программ, обрабатываемой информации и средств защиты обеспечивается:

- средствами разграничения доступа, запрещающими модификацию или удаление защищаемого ресурса
- средствами сравнения критичных ресурсов с их эталонными копиями (и восстановления в случае нарушения целостности);
- средствами подсчета контрольных сумм (сверток, сигнатур, имитоприставок и т.п.);
- средствами электронной цифровой подписи.

1.5.4. Защита периметра компьютерных сетей

Межсетевые экраны, установленные в точках соединения с сетью Internet - обеспечивают защиту внешнего периметра сети и защиту собственных Internet-серверов, открытых для общего пользования, от несанкционированного доступа.

В межсетевых экранах применяются специальные методы защиты:

- трансляция адресов для сокрытия структуры и адресации внутренней сети;
- фильтрация проходящего трафика;
- управление списками доступа на маршрутизаторах;
- дополнительная идентификация и аутентификация пользователей стандартных служб (на проходе);
- ревизия содержимого (вложений) информационных пакетов, выявление и нейтрализация компьютерных вирусов;
- виртуальные частные сети (для защиты потоков данных, передаваемых по открытым сетям - обеспечения конфиденциальности, - применяются криптографические методы, рассмотренные выше);
- противодействие атакам на внутренние ресурсы.

1.5.5 Разграничение доступа зарегистрированных пользователей к ресурсам ВС

Разграничение (контроль) доступа к ресурсам ВС - это такой порядок использования ресурсов автоматизированной системы, при котором субъекты получают доступ к объектам системы в строгом соответствии с установленными правилами.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе.

Несанкционированный доступ (НСД) - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

Технические средства разграничения доступа к ресурсам АС должны рассматриваться как составная часть единой системы контроля доступа субъектов:

• на контролируемую территорию;

• в отдельные здания и помещения организации;

• к элементам ВС и элементам системы защиты информации (физический доступ);

• к информационным и программным ресурсам АС.

Механизмы управления доступом субъектов к объектам доступа выполняют основную роль в обеспечении внутренней безопасности компьютерных систем. Их работа строится на концепции единого диспетчера доступа.

Диспетчер доступа выполняет:

• проверку прав доступа каждого субъекта к конкретному объекту на основании информации, содержащейся в базе данных системы защиты (правил разграничения доступа);

• разрешение (производит авторизацию) или запрещение (блокирует) доступ субъекта к объекту;

• при необходимости регистрирует факт доступа и его параметры в системном журнале (в том числе попытки несанкционированного доступа с превышением полномочий).

В общем виде работа средств разграничения доступа субъектов к объектам основана на проверке сведений, хранимых в базе данных защиты.

1.5.6. Криптографические методы защиты информации

Криптографические методы защиты основаны на возможности выполнения операции преобразования информации, с помощью специального ключа, без знания которого (с вероятностью близкой к единице за разумное время) невозможно осуществить эту операцию.

В классической криптографии используется только один - ключ, который позволяет отправителю зашифровать информацию, а получателю - расшифровать ее.

В криптографии с открытым ключом имеется два ключа, один из которых нельзя вычислить из другого. Один ключ используется отправителем для шифрования информации, закрытие которой необходимо обеспечить. Другой ключ используется получателем для расшифрования полученной информации. Бывают приложения, в которых один ключ должен быть несекретным, а другой - секретным. Алгоритмы преобразования с открытым и секретным ключами называют асимметричными, поскольку роли сторон владеющих разными ключами из пары различны.

К криптографическим методам защиты относятся:

- шифрование (расшифрование) информации;
- формирование и проверка цифровой подписи электронных документов.

Основным достоинством криптографических методов защиты информации является то, что они обеспечивают высокую гарантированную стойкость защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей).

К числу основных недостатков криптографических методов можно отнести:

- большие затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации;
- трудности с совместным использованием зашифрованной информации;
- высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены.

1.5.7 Контроль целостности и аутентичности данных, передаваемых по каналам связи

Электронная цифровая подпись (ЭЦП) — это последовательность символов, полученная в результате преобразования в технических средствах определенного объема информации по установленному математическому алгоритму с использованием ключей, имеющая неизменяемое соотношение с каждым символом данного объема информации.

Применение электронной цифровой подписи позволяет:

• обеспечить аутентичность (подтверждение авторства) информации;

• обеспечить контроль целостности (в том числе истинности) информации;

• при использовании многосторонней электронно-цифровой подписи обеспечить аутентификацию лиц, ознакомившихся с информацией;

• решать вопрос о юридическом статусе документов, получаемых из автоматизированной системы.

1.5.8. Криптографическое закрытие хранимых и передаваемых по каналам связи данных

Шифрование информации позволяет обеспечить конфиденциальность защищаемой информации при ее хранении или передаче по открытым каналам. На прикладном уровне шифрование применяется для закрытия секретной и конфиденциальной информации пользователей. На системном уровне - для защиты критичной информации операционной системы и системы защиты, предотвращения возможности несанкционированной подмены важной управляющей информации системы разграничения доступа (паролей пользователей, таблиц разграничения доступа, ключей шифрования данных и ЭЦП и т.п.).

Для защиты пакетов, передаваемых по указанным каналам связи, криптопреобразование может осуществляться как на прикладном уровне, так и на транспортном. В первом варианте закрытие информации, предназначенной для транспортировки, должно осуществляться на узле-отправителе (рабочей станции или сервере), а расшифровка т на узле-получателе. Причем преобразования могут производиться как на уровне приложений («абонентское шифрование»), так и на системном (канальном, транспортном) уровне (прозрачно для приложений - «туннелирование»).

Второй вариант предполагает использование специальных средств, осуществляющих криптопреобразования в точках подключения локальных сетей к каналам связи (сетям общего пользования), проходящим по неконтролируемой территории («канальное шифрование», «виртуальные частные сети»).

Криптографические средства могут быть реализованы как аппаратно, так и программно. Использование в системе защиты для различных целей нескольких однотипных алгоритмов шифрования нерационально. Оптимальным вариантом можно считать такую систему, в которой средства криптозащиты являются общесистемными, то есть выступают в качестве расширения функций операционной системы и включают алгоритмы шифрования всех типов (с секретными и открытыми ключами и т.д.).

1.6. Управление механизмами защиты

Основное внимание уделяется реализации самих защитных механизмов, а не средств управления ими. Решить это можно только, обеспечив необходимую гибкость управления средствами защиты.

Недостаточное внимание к проблемам и пожеланиям заказчиков, к обеспечению удобства работы администраторов безопасности по управлению средствами защиты компьютерных систем часто является основной причиной отказа от использования конкретных средств защиты.

Этап внедрения средств защиты информации обязательно в той или иной мере включает действия по первоначальному выявлению, уточнению и соответствующему изменению настроек средств защиты. Эти действия должны проходить для владельцев и пользователей системы как можно более прозрачно.

Средства управления системы защиты должны обеспечивать удобство выполнения необходимых при этом изменений настроек системы защиты.

Для поддержки и упрощения действий по настройке средств защиты необходимо предусмотреть следующее:

- выборочное подключение имеющихся защитных механизмов;

- "мягкий" режим функционирования средств защиты, при котором несанкционированные действия пользователей (действия с превышением полномочий) фиксируются в системном журнале обычным порядком, но не пресекаются. Этот режим позволяет выявлять некорректности настроек средств защиты;
- возможности по автоматизированному изменению полномочий пользователя с учетом информации, накопленной в системных журналах.

Для решения проблем управления средствами защиты в больших сетях необходимо предусмотреть:

- поддержку возможности управления механизмами защиты как централизованно (удаленно, с рабочего места администратора безопасности сети), так и децентрализовано (непосредственно с конкретной рабочей станции). При этом любые изменения настроек защитных механизмов, произведенные централизованно, должны автоматически распространяться на все рабочие станции, которых они касаются (независимо от состояния рабочей станции на момент внесения изменений в центральную базу данных);
- управление механизмами защиты конкретной станции должно осуществляться независимо от активности данной станции;
- в крупных системах замена версий программ средств защиты (равно как и любых других программ) требует от обслуживающего персонала больших трудозатрат и связана с необходимостью обхода всех рабочих станций для получения к ним непосредственного доступа;
- Система защиты в свой состав должна включать подсистему оперативного контроля состояния рабочих станций сети и слежения за работой пользователей.

Для облегчения работы администратора с системными журналами в системе должны быть предусмотрены:

- подсистема реализации запросов, позволяющая выбирать из собранных системных журналов данные об определенных событиях (по имени пользователя, дате, времени происшедшего события, категории происшедшего события и т.п.);
- возможность автоматического разбиения и хранения системных журналов по месяцам и дням в пределах заданного периода. Причем во избежание переполнения дисков по истечении установленного количества дней просроченные журналы, если их не удалил администратор, должны автоматически уничтожаться.
- в системе защиты должны быть предусмотрены механизмы семантического сжатия данных в журналах регистрации, позволяющие укрупнять регистрируемые события без существенной потери их информативности;
- желательно иметь системе средства автоматической подготовки отчетных документов установленной формы.

Универсальные механизмы защиты обладают своими достоинствами и недостатками и могут применяться в различных вариантах и совокупностях в конкретных методах и средствах защиты.

1.8 Цели создания системы обеспечения информационной безопасности

Конечной *целью создания системы обеспечения безопасности информационных технологий* является предотвращение или минимизация ущерба (прямого или косвенного, материального, морального или иного), наносимого субъектам информационных отношений посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

Основной задачей системы защиты является обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов (ресурсов) АС соответствующими множеству значимых угроз методами и средствами.

Обеспечение информационной безопасности - это непрерывный процесс, основное содержание которого составляет управление, - управление людьми, рисками, ресурсами, средствами защиты и т.п. Люди - обслуживающий персонал и конечные пользователи АС, - являются неотъемлемой частью автоматизированной (то есть *«человеко-машинной»)* системы. От того, каким образом они реализуют свои функции в системе, существенно зависит не только ее функциональность (эффективность решения задач), но и ее безопасность.

Рис. 1 Субъекты, влияющие на состояние информационной безопасности

•***сотрудников структурных подразделений*** (конечных пользователей АС), решающих свои функциональные задачи с применением средств автоматизации;

•***программистов,*** осуществляющих разработку (приобретение и адаптацию) необходимых прикладных программ (задач) для автоматизации деятельности сотрудников организации;

•***сотрудников подразделения внедрения и сопровождения ПО,*** обеспечивающих нормальное функционирование и установленный порядок инсталляции и модификации прикладных программ (задач);

•***сотрудников подразделения эксплуатации ТС,*** обеспечивающих нормальную работу и обслуживание технических средств обработки и передачи информации и системного программного обеспечения;

•***системных администраторов*** штатных средств защиты (ОС, СУБД и т.п.);

•***сотрудников подразделения защиты информации,*** оценивающих состояние информационной безопасности, определяющих требования к системе защиты, разрабатывающих организационно-распорядительные документы по вопросам ОИБ

(аналитиков), внедряющих и администрирующих специализированные дополнительные средства защиты (администраторов безопасности);

•***руководителей организации,*** определяющих цели и задачи функционирования АС, направления ее развития, принимающих стратегические решения по вопросам безопасности и утверждающих основные документы, регламентирующие порядок безопасной обработки и использования защищаемой информации сотрудниками организации.

Кроме того, на информационную безопасность организации могут оказывать влияние ***посторонние лица*** и сторонние организации, предпринимающие попытки вмешательства в процесс нормального функционирования АС или несанкционированного доступа к информации как локально, так и удаленно.

1.9 Задачи, решаемые средствами защиты информации от НСД

На технические средства зашиты от НСД возлагают решение следующих основных задач:

- защиту от вмешательства в процесс функционирования АС посторонних лиц (возможность использования автоматизированной системы и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи - сотрудники подразделений организации);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам АС (обеспечение возможности доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям АС для выполнения ими своих служебных обязанностей);
- регистрацию действий пользователей при использовании защищаемых ресурсов АС в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов сотрудниками подразделений компьютерной безопасности;
- оперативный контроль за работой пользователей системы и оперативное оповещение администратора безопасности о попытках несанкционированного доступа к ресурсам системы;
- защиту от несанкционированной модификации (обеспечение неизменности, целостности) используемых в АС программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы и вредоносные «программы-закладки»;
- защиту хранимой, обрабатываемой и передаваемой по каналам связи информации ограниченного распространения от несанкционированного разглашения, искажения подмены или фальсификации;
- обеспечение аутентификации абонентов, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
- гибкое управление всеми защитными механизмами.

Кроме того, системы защиты от НСД должны обладать высокой надежностью, универсальностью, возможностями реализации современных технологий защиты, невысокими требованиями к ресурсам защищаемых компьютеров, широкими возможностями по управлению механизмами защиты, должны работать с разнообразными средствами аппаратной поддержки защитных функций, и ориентироваться на наиболее распространенные операционные системы.

2 БЕЗОПАСНОСТЬ УРОВНЯ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

2.1. Базовые принципы сетевого взаимодействия. Модель OSI

Для организации обмена данными между компьютерами сетевое программное обеспечение должно иметь широкий набор функций, таких как, например, перенаправление ввода/вывода, межпроцессные коммуникации и т.п. Для того, чтобы уменьшить сложность разработки сетей, эти функции организованы в несколько групп, находящихся на различных уровнях. Каждый уровень предоставляет сервис вышележащему уровню и использует сервис, предоставляемый нижележащим уровнем (рис. 2.1).

Многоуровневая архитектура сетевого взаимодействия

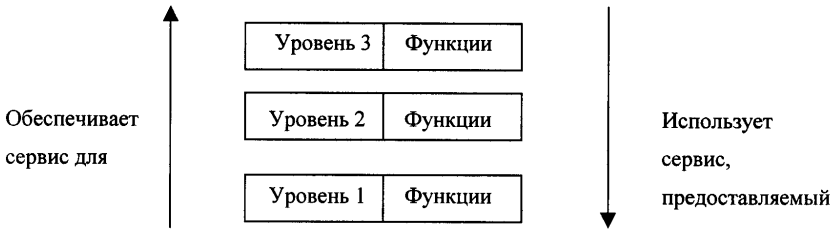

Рис. 2.1

Одноимённые уровни на различных компьютерах сообщаются с использованием определённых протоколов. Например, уровень 2 на одном компьютере общается с уровнем 2 на другом компьютере.

Протокол – совокупность правил и соглашений, используемых при взаимодействии между одноимёнными уровнями (рис 2.2) взаимодействующих систем.

Взаимодействие с использованием протоколов

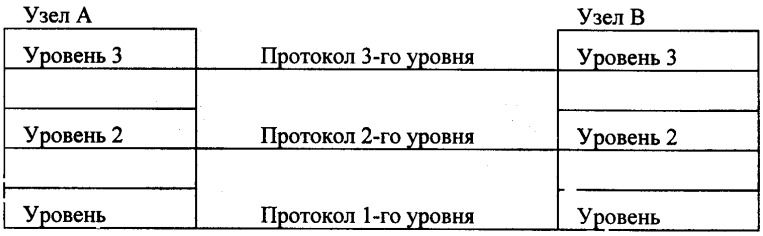

Рис. 2.2

Каждый уровень взаимодействует с одноимённым уровнем на другом компьютере, но данные не перемещаются между уровнями напрямую. Вместо этого данные передаются на смежный нижележащий уровень до тех пор, пока не достигнут самого низкого уровня, откуда они передаются в сетевую среду.

На принимающем компьютере данные также передаются от уровня к уровню, только снизу вверх. Правила взаимодействия между смежными уровнями называются интерфейсом.

Для успешного обмена данными между различными компьютерными системами разработана модель взаимодействия открытых систем (Open Systems Interconnection - OSI), в которой средства сетевого взаимодействия делятся на семь уровней, для которых определены стандартные названия и функции.

2.2. Сетевые анализаторы и "снифферы"

Физический уровень определяет электрические, функциональные и другие параметры физической связи.

Канальный уровень обеспечивает надежную передачу данных через физический канал.

Конкретные реализации функций канального и физического уровней зависят от сетевой технологии.

В настоящее время самой распространённой сетевой технологией является Ethernet (около 80% сетей). Все популярные операционные системы и стеки протоколов поддерживают Ethernet.

Главный недостаток технологии Ethernet - незащищенность передаваемой информации Метод доступа положенный в основу этой технологии требует от узлов, подключенных к сети, непрерывного прослушивания всего трафика. Узлы такой сети могут перехватывать информацию, адресованную своим соседям. Данная уязвимость делает возможным проведение атак, использующих механизм «пассивного прослушивания» Средства для проведения таких атак - это анализаторы протоколов или снифферы.

«Сниффер» обозначает устройство, подключенное к компьютерной сети и записывающее весь ее трафик. Так же «сниффер» - программа, запущенная на подключенном к сети узле и просматривающая весь трафик сетевого сегмента.

Работа "сниффера" использует основной принцип технологии Ethernet - общую среду передачи, то есть любое устройство, подключенное к сетевому сегменту, может слышать и принимать все сообщения, в том числе предназначенные не ему. Сетевые адаптеры Ethernet могут работать в двух режимах:

- селективном (non-promiscuous). Принимаются только сообщения предназначенные только данному узлу. Фильтрация осуществляется на основе MAC-адреса фрейма.
- неселективном (promiscuous). Фильтрация не осуществляется, и узел принимает все фреймы, передаваемые по сегменту.

«Снифферы» переводят сетевой адаптер в неселективный режим и собирают весь трафик сети для последующего анализа. Собранный трафик сегмента может быть отображен на экране, записан в файл и т. п. Так как обмен информации происходит обычно в двоичном формате, в обязанности "сниффера" обычно входит расшифровка (декодирование) и вывод информации в удобном (читаемом) виде.

Тот же принцип пассивного прослушивания трафика лежит в основе работы средств обнаружения атак.

С помощью анализатора протоколов перехват информации в случае нахождения злоумышленника в другом сегменте осуществить невозможно, однако для этого используются другие методы, позволяющие перенаправить трафик из другого сегмента на узел нарушителя и реализующие атаки типа «создание ложного объекта-посредника» на сетевом и транспортном уровнях модели OSI

Так как сниффер - это пассивное устройство, обнаружить его достаточно сложно. Обычно присутствие сниффера можно обнаружить по каким-либо косвенным признакам, свойственным конкретному снифферу или по неселективному режиму работы сетевой карты на узле.

Меры защиты от снифферов следуют из принципа их работы и цели атак:

1. Шифрование информации.

2. Построение сетей на основе интеллектуальных коммутаторов (switches) и их грамотная конфигурация.

3. Использование сетевых адаптеров, не поддерживающих неселективный режим.

4. Обнаружение несанкционированно используемых на компьютерах анализаторов протоколов.

2.3. Защита на канальном уровне

Главное преимущество – прозрачность для протоколов сетевого, транспортного и прикладного уровней. Для защиты данных на канальном уровне используются три протокола:

PPTP (Point-to-Point-Tunneling Protocol);

L2F (Layer 2 Forwarding);

L2TP (Layer 2 Tunneling Protocol).

Протоколы L2F и L2TP являются протоколами туннелирования, а протокол PPTP обеспечивает как туннелирование, так и шифрования данных.

2.3.1. Протокол PPTP

Протокол PPTP (Point-to-Point-Tunneling Protocol) позволяет создавать криптозащищенные каналы для обмена данными по протоколам IP, IPX и NetBEUI. Технология создания защищенного виртуального канала по протоколу **PPTP** предусматривает как аутентификацию удаленного пользователя, так и зашифрованную передачу данных.

Для аутентификации могут использоваться различные протоколы. В реализации **PPTP,** включенной в Windows, поддерживаются протоколы аутентификации **PAP** (Password Authentication Protocol — протокол распознавания пароля) и **CHAP** (Challenge-Handshaking Authentication Protocol— протокол распознавания при рукопожатии). При использовании протокола PAP идентификаторы и пароли передаются по линии связи в незашифрованном виде. При использовании протокола CHAP каждый пароль для передачи по линии связи шифруется на основе случайного числа, полученного от сервера. Такая технология обеспечивает также защиту от повторного использования злоумышленником перехваченных пакетов с зашифрованным паролем.

Программное обеспечение удаленного доступа, реализующее **PPTP,** может использовать любой стандарт криптографического закрытия передаваемых данных.

В протоколе **PPTP** определено три схемы его применения: одна схема – для прямого соединения компьютера удаленного пользователя с Internet и две – для соединения удаленного компьютера к Internet по телефонной линии через провайдера.

При прямом соединении компьютера удаленного пользователя с сетью Internet, пользователь устанавливает удаленное соединение с помощью клиентской части сервиса удаленного доступа. Он обращается к серверу удаленного доступа локальной сети, указывая его IP-адрес, и устанавливает с ним связь по протоколу **PPTP.** Функции сервера удаленного доступа может выполнять и пограничный маршрутизатор локальной сети. Протокол **PPTP** определяет некоторое количество служебных сообщений, которыми обмениваются взаимодействующие стороны. Служебные сообщения передаются по протоколу **TCP.** После успешной аутентификации начинается процесс защищенного информационного обмена.

В этом варианте на компьютере удаленного пользователя должны быть установлены клиент сервера удаленного доступа RAS и драйвер PPTP, которые входят в состав Windows, а на сервере удаленного доступа локальной сети — сервер RAS и драйвер PPTP, входящие в состав Windows. Внутренние серверы локальной сети не должны поддерживать протокол PPTP, так как пограничный маршрутизатор извлекает кадры PPP из пакетов IP и посылает их по сети в необходимом формате – IP, IPX или NetBEUI.

Для случая подсоединения удаленного компьютера к Internet по телефонной линии через провайдера предусмотрена две схемы.

Вариант 1:

- протокол PPTP поддерживается сервером удаленного доступа (RAS – Remote Access Service) провайдера Internet;
- протокол PPTP поддерживается маршрутизатором сети организации;
- защищённый канал образуется между RAS провайдера и маршрутизатором сети организации.

Схема для варианта 1 приведена на рис. 2.3.

Применение PPTP, вариант 1

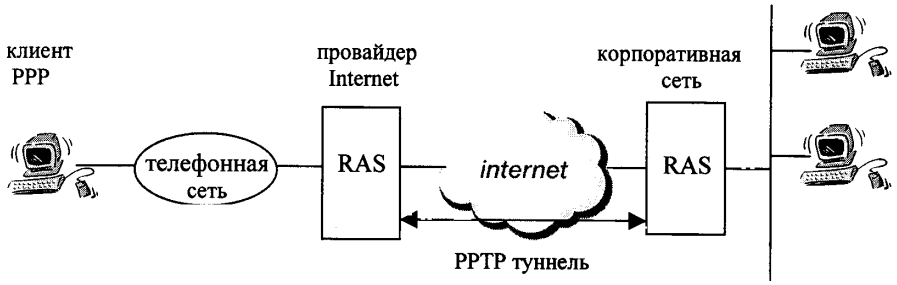

Рис.2.3

В этом варианте компьютер удаленного пользователя не должен поддерживать протокол PPTP.

Процесс установления соединения:

- клиент связывается с сервером удаленного доступа провайдера по протоколу PPP.
- клиент проходит первую аутентификацию у провайдера. Провайдер должен поддерживать протокол PPTP.
- по имени пользователя провайдер устанавливает связь с пограничным маршрутизатором сети организации по протоколу PPTP.
- маршрутизатор аутентифицирует пользователя по протоколам PAP или CHAP.
- если аутентификация прошла успешно, связь считается установленной.

Процесс обмена данными:

- клиент отправляет данные серверу удаленного доступа провайдера по протоколам IP, IPX или NetBEUI (упакованные в PPP).
- сервер удаленного доступа провайдера упаковывает пакеты PPP в пакеты IP, указывая в качестве адреса получателя адрес маршрутизатора, а в качестве адреса отправителя - свой.
- пакеты PPP шифруются с помощью симметричного ключа в качестве которого используется хэш-функция пароля пользователя. В качестве

алгоритма шифрования используется RC-4 или DES.

Схема не нашла широкого применения так как протокол PPTP не всегда поддерживается маршрутизаторами и серверами удаленного доступа провайдера

Вариант 2:

- сервер удаленного доступа не поддерживает PPTP;
- защищенный канал образуется между компьютером удаленного клиента и маршрутизатором сети организации.

Схема для варианта 2 приведена на рис. 2.4.

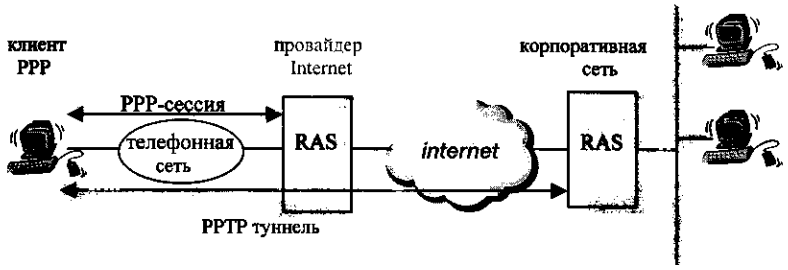

Рис. 2.4

Процесс установления соединения:

- клиент устанавливает связь с сервером удаленного доступа провайдера по протоколу PPTP.
- клиент проходит аутентификацию по протоколам PAP или CHAP.
- клиент устанавливает связь с маршрутизатором сети организации, где работает протокол PPTP (звонок отличается от обычного тем, что вместо телефонного номера указывается IP- адрес сервера удаленного доступа организации.
- клиент проходит аутентификацию на сервере удаленного доступа сети организации.

Обмен данными осуществляется также как в первом варианте.

2.3.2. Протокол L2F

Протоколы L2F и L2TP выполняют только туннелирование. Протокол L2F фактически поглощён протоколом L2TP. Однако протокол L2TP имеет пока только статус проекта стандарта Internet.

Помимо ориентации на различные протоколы информационного обмена, протокол L2F обеспечивает:

- гибкость аутентификации, предусматривающую отсутствие жесткой привязки к конкретным протоколам подтверждения подлинности;

- прозрачность для конечных систем — ни удаленная система, ни рабочие станции локальной сети не должны иметь специальное программное обеспечение, чтобы использовать защитный сервис;

- прозрачность для посредников:

• авторизация должна выполняться так, как в случае непосредственного подключения пользователей к серверу удаленного доступа локальной сети;

• адрес сервера удаленного доступа должен назначаться не сервером провайдера, а сервером локальной сети;

• полнота аудита, предусматривающая регистрацию событий по доступу к серверу локальной сети как сервером удаленного доступа этой сети, так и сервером провайдера.

В случае традиционной службы удаленного доступа аутентификация пользователей осуществляется самим сервером провайдера. При использовании технологии L2F сервер удаленного доступа провайдера использует аутентификацию только для определения необходимости создания виртуального канала и поиска адреса сервера удаленного доступа требуемой локальной сети. Окончательная проверка подлинности выполняется сервером удаленного доступа локальной сети после того, как сервер провайдера с ним связывается.

Недостатки: четвертая версия протокола IP не предусматривает создание криптозащищенного туннеля между конечными точками информационного взаимодействия. Виртуальный защищенный канал может быть создан только между сервером удаленного доступа провайдера и пограничным маршрутизатором локальной сети, а участок между компьютером удаленного пользователя и серверов провайдера остается открытым.

2.3.2. Протокол L2TP

В L2TP добавлена важная функция управления потоками данных, которая не допускает в систему больше информации, чем та способна обработать. Кроме того, в отличие от своих предшественников, L2TP позволяет открывать между конечными абонентами сразу несколько туннелей, каждый из которых администратор может выделить для того или иного приложения. Это обеспечивает безопасность и гибкость туннелирования, а также существенно повышают качество обслуживания виртуальных каналов связи.

По существу протокол L2TP представляет собой расширение PPP-протокола функциями аутентификации удаленных пользователей, установки защищенного виртуального соединения, а также управлением потоками данных. В соответствии с протоколом L2TP (рис. 2.5) в качестве сервера удаленного доступа провайдера должен выступать концентратор доступа (Access Concentrator), который реализует клиентскую часть протокола L2TP и обеспечивает пользователю сетевой доступ к его локальной сети через Internet. Роль сервера удаленного доступа локальной сети должен выполнять сетевой сервер L2TP (L2TP Network Server), функционирующий на любых платформах, совместимых с протоколом PPP.

Схема взаимодействия по протоколу L2TP

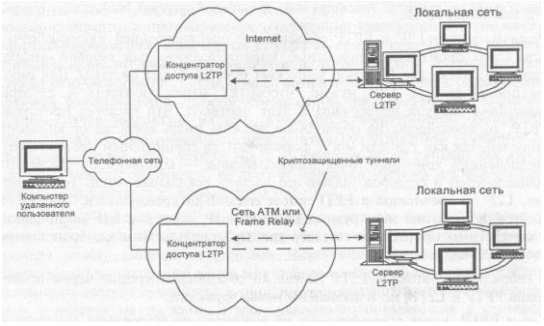

Рис 2.5.

Протокол L2TP предполагает использование схемы, в которой туннель образуется между сервером удалённого доступа провайдера и маршрутизатором корпоративной сети. Сервер удалённого доступа провайдера называется

концентратором доступа (L2TP Access Concentrator, LAC). Маршрутизатор корпоративной сети называется сетевым сервером (L2TP Network Server, LNS).

Схема работы:

- пользователь устанавливает PPP- соединение с провайдером.
- провайдер выполняет частичную аутентификацию узла и пользователя (используется только имя пользователя) с целью определения, нужен ли сервис L2TP.
- провайдер определяет адрес LNS, с которым нужно установить связь.
- устанавливается туннель L2TP между LAC и LNS.
- новому соединению в рамках установленного туннеля присваивается идентификатор вызова (Call ID).
- LAC посылает LNS уведомление о вызове (оно содержит Call ID и информацию для аутентификации, зависящую от используемого протокола -PAP или CHAP).
- корпоративный сервер LNS отправляет на LAC результат аутентификации и некоторую дополнительную информацию, например, выделяет для удалённого клиента IP-адрес.

Результатом является создание «виртуального интерфейса». По туннелю между LAC и LNS инкапсулированные кадры PPP могут передаваться в обоих направлениях. При поступлении PPP-пакета от удаленного пользователя LAC удаляет из него байты обрамления кадра и контрольную сумму, затем инкапсулирует его с помощью L2TP и отправляет серверу LNS, который извлекает из пакета кадр PPP и обрабатывает его стандартным образом.

Обеспечить безопасность на этом этапе позволяет программный продукт Internet Scanner.

2.4. Атаки на протокол ARP

Протокол разрешения адресов – ARP. Функционально протокол ARP состоит из двух частей. Одна часть протокола определяет физические адреса, другая - отвечает на запросы при определении физических адресов.

Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети - протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети, или же протокол глобальной сети (X.25, frame relay), как правило не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу - нахождение IP-адреса по известному MAC - адресу. Он называется реверсивный ARP - RARP {Reverse Address Resolution Protocol) и используется при старте бездисковых станций, не знающих (не имеющих) в начальный момент своего IP-адреса, но знающих адрес LBOCI сетевого адаптера.

В локальных сетях протокол ARP использует широковещательные кадры протокола канального уровня для поиска в сети узла с заданным IP-адресом.

Узел, которому нужно выполнить отображение IP-адреса на MAC - адрес, формирует ARP запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно. Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным. Узел, на котором они совпадают, формирует ARP-ответ, в котором указывает свой IP-адрес и свой MAC - адрес и отправляет его уже целенаправленно,

так как в ARP запросе отправитель указывает свой MAC - адрес. ARP-запросы и ответы используют один и тот же формат пакета.

Протокол ARP является абсолютно незащищённым. Он не обладает никакими способами проверки подлинности пакетов: как запросов, так и ответов. Ситуация усложняется, когда может использоваться самопроизвольный ARP (gratuitous ARP).

Самопроизвольный ARP — такое поведение ARP, когда ARP-ответ присылается, когда в этом (с точки зрения получателя) нет особой необходимости. Самопроизвольный ARP-ответ это пакет-ответ ARP, присланный без запроса. Он применяется для определения конфликтов IP-адресов в сети: как только станция получает адрес по DHCP или адрес присваивается вручную, рассылается ARP-ответ gratuitous ARP.

2.4.1. Ложный ARP-сервер в сети Internet

Рассмотрим обобщенную функциональную схему ложного ARP-сервера (рис. 4.3):

- ожидание ARP-запроса;
- при получении ARP-запроса передача по сети на запросивший хост ложного ARP-ответа, в котором указывается адрес сетевого адаптера атакующей станции (ложного ARP-сервера) или тот Ethernet-адрес, на котором будет принимать пакеты ложный ARP-сервер (совершенно необязательно указывать в ложном ARP-ответе свой настоящий Ethernet-адрес, так как при работе непосредственно с сетевым адаптером его можно запрограммировать на прием пакетов на любой Ethernet-адрес);
- прием, анализ, воздействие и передача пакетов обмена между взаимодействующими хостами.

Ложный ARP-сервер.

Рис. 4.3.1. Фаза ожидания ARP-запроса.

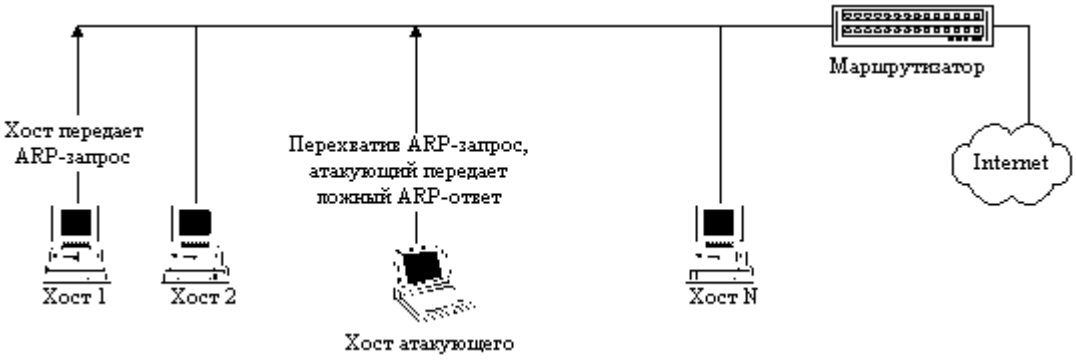

Рис. 4.3.2. Фаза атаки.

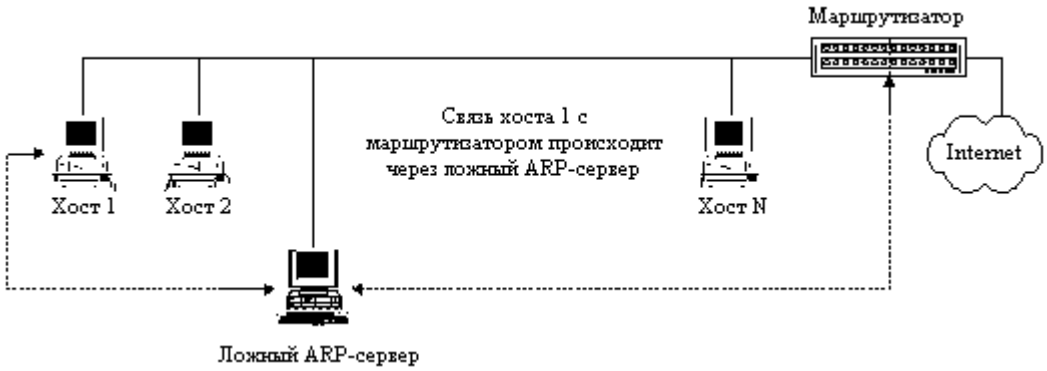

Рис. 4.3.3. Фаза приема, анализа, воздействия и передачи перехваченной информации на ложном ARP-сервере.

Nак как поисковый ARP-запрос кроме атакующего получит и маршрутизатор, то в его таблице окажется соответствующая запись об IP- и Ethernet-адресе атакуемого хоста. Следовательно, когда на маршрутизатор придет пакет, направленный на IP-адрес атакуемого хоста, то он будет передан не на ложный ARP-сервер, а непосредственно на хост. При этом схема передачи пакетов в этом случае будет следующая:

- атакованный хост передает пакеты на ложный ARP-сервер;
- ложный ARP-сервер передает принятый от атакованного хоста пакет на маршрутизатор;
- маршрутизатор, в случае получения ответа на переданный запрос, передает его непосредственно на атакованный хост, минуя ложный ARP-сервер.

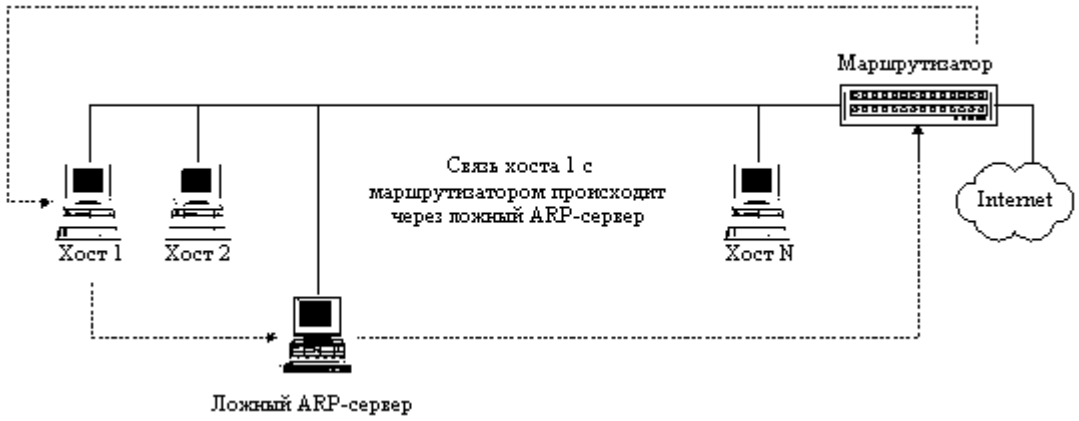

Рис. Петлевая схема перехвата информации ложным ARP-сервером.

В этом случае последняя фаза, связанная с "приемом, анализом, воздействием и передачей пакетов обмена" между атакованным хостом и, например, маршрутизатором (или любым другим хостом в том же сегменте) будет проходить уже не в режиме полного перехвата пакетов ложным сервером (мостовая схема), а режиме "полупере-хвата" (петлевая схема). Действительно, в режиме полного перехвата маршрут всех пакетов, отправляемых как в одну, так и в другую стороны, обязательно проходит через ложный сервер-мост; а в режиме "полуперехвата" маршрут пакетов образует петлю.

Тем не менее довольно несложно придумать несколько способов, позволяющих функционировать ложному ARP-серверу по мостовой схеме перехвата (полный перехват). Например, можно, получив ARP-запрос, самому послать такой же запрос и присвоить себе данный IP-адрес (правда, в этом случае ложному ARP-серверу не удастся остаться незамеченным, так некоторые сетевые ОС (например Windows '95 и SunOS 5.3), как отмечалось ранее, перехватив этот запрос, выдадут

предупреждение об использовании их IP-адреса). Другой, значительно более предпочтительный способ: послать ARP-запрос, указав в качестве своего IP-адреса любой свободный в данном сегменте IP-адрес, и в дальнейшем вести работу с данного IP-адреса как с маршрутизатором, так и с "обманутыми" хостами (кстати, это типичная proxy-схема).

2.4.2. ARP-Spoofing

Перехватив внутри сегмента сети широковещательный ARP запрос, можно послать ложный ARP ответ, в котором объявить себя искомым узлом, (например, маршрутизатором), и, таким образом, перехватывать и активно воздействовать на сетевой трафик «жертвы». Данная атака является внутрисегментной, но так как широковещательные пакеты рассылаются во все сегменты коммутатора, то реализация данной атаки возможна и в сетях с коммутацией (в «свитчеванных» сетях).

Кроме того, нарушитель может отправить ответ, в котором указан MAC - адрес несуществующего или неработающего в данный момент узла, что приведёт к невозможности взаимодействия узла - «жертвы» с искомым узлом.

Схема атаки ARP-Spoofing:

- ожидание ARP запроса.
- передача ложного ARP ответа, в котором указывается адрес сетевого адаптера атакующего (или несуществующий).
- прием, анализ, модификация и передача пакетов обмена между взаимодействующими хостами (досылка через посредника, в качестве которого выступает узел нарушителя).

Так как практически все реализации ARP-протокола в стеках TCP/IP принимают и обрабатывают (добавляют в кэш) ARP-ответы, для которых не было соответствующих запросов, то возможен также вариант атаки на ARP-кэш путем периодической посылки на узел-«жертву» ложных (с искаженными данными) ARP-ответов.

Атака ARP Spoofing используется в локальной сети, построенной на коммутаторах. С ее помощью можно перенаправить поток ethernet-фреймов на другие порты, в соответствии с MAC-адресом. После чего злоумышленник может перехватывать все пакеты на своем порту. Таким образом, атака ARP Spoofing позволяет перехватывать трафик машин, расположенных на разных портах коммутатора.

Для реализации атаки ARP Spoofing, злоумышленник может воспользоваться генераторами ARP-пакетов, например ARPSpoof или nemesis.

Различные сетевые операционные системы по-разному используют протокол ARP для изменения информации в своих ARP таблицах.

Атаки, связанные с уязвимостями протокола ARP являются внутрисегментными и поэтому представляют угрозу для пользователя только в случае нахождения атакующего внутри сегмента сети. Защиты от атак на протокол ARP в общем случае не существует, т.к. используемые уязвимости являются особенностями работы технологии Ethernet (широковещательность). Однако можно выполнить следующее:

- нарушителя нужно искать внутри сетевого сегмента атакуемого объекта;
- полезно вести таблицу соответствия MAC-адресов и IP-адресов, которую

следует периодически обновлять;

- использовать статические записи в таблице ARP хотя бы для наиболее важных узлов сети.

2.6. Атаки сетевого уровня на протокол IP и его защита

2.6.1. Аутентификация на основе IP-адреса (Address Masquerading)

Аутентификация (подтверждение подлинности) на уровне IP относится к компьютерам, а не к пользователям. Поскольку IP-адрес конфигурируется программно, обычно бывает легко задать для узла другой IP-адрес, так что узел будет корректно работать в сети. Если аутентификация осуществляется по IP-адресу узла, это позволит атакующему получить доступ к ресурсам, к которым он при обычных условиях доступа иметь не должен. Такое действие называется Address Masquerading (Адресный маскарад). Протоколы прикладного уровня, как, например, Network File System (NFS), могут быть уязвимыми к таким атакам, если нет дополнительной аутентификации на основе, например имени и пароля пользователя.

Атака «Address Masquerading»

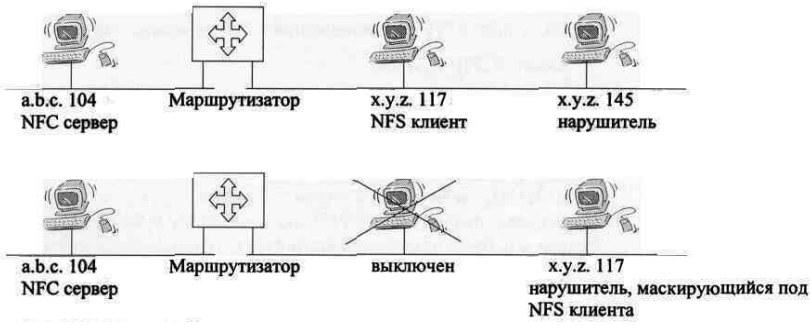

Рис. 2.6

На рис. 2.6 нарушитель, дождавшись отключения легального NFS клиента, присваивает себе его IP-адрес.

2.6.2. Address Spoofing

Address Spoofing в простейшем варианте представляет собой замену адреса отправителя или получателя пакета и отправку такого пакета в сеть.

Более усовершентсвованный вариант техники Address Spoofing называется TCP sequence number attack.

Средства программирования под UNIX позволяют легко управлять сетевыми пакетами, например, формировать их заголовки. Например утилита Nmap, некоторые режимы которой позволяют задать поддельные адреса отправителя пакетов. Под Windows это осуществить несколько сложнее.

2.6.3. Ошибки фрагментации

Большое количество атак на протокол IP связано с одной из его функций - фрагментацией. Посылка специфических пакетов, где определённым образом заполнены поля заголовка, отвечающие за фрагментацию, может привести к зависанию или понижению производительности узла. Как правило, используемыми уязвимостями во всех случаях являются ошибки реализации. Исправление этих

ошибок – это установка пакетов обновления программного обеспечения. Большое число одинаковых фрагментированных пакетов вызывают "замораживание" машины на время атаки. Например, узлу посылается большое количество пакетов с одинаковым полем Identification, помеченных как последний фрагмент со смешением 65520. Это приводит к падению производительности узла практически до нуля.

Защитится можно путем установки соответствующего обновления ПО.

2.7. Атаки на протокол ICMP и его защита

Так как протокол ICMP служит для передачи различных управляющих служебных сообщений, он становиться популярной мишенью для атак.

Атака Sping/Jolt

Атака состоит в посылке нескольких дефрагментированных пакетов ICMP (ICMP_ECHO) больших размеров по частям. Windows, пытаясь собрать пакет, зависает, что приводит к отказу в обслуживании и может привести к нарушению целостности данных.

Для устранения уязвимости необходимо применить патч icmp-fix, который зависит от версии Windows и установленного пакета обновления.

Атака ICMP Request

Атака заключается в посылке пакета ICMP Subnet Mask Address Request по адресу сетевого интерфейса, сконфигурированного на использование нескольких IP-адресов, принадлежащих одной подсети. В результате Windows NT аварийно завершается с подачей сообщения STOP 0x0000000A (0xA0033000, 0x00000002, 0x00000000, 0xf381329B), где четвертый параметр относится к области памяти модуля Tcpip.sys. Атака применима к Windows NT 4.0 Workstation и Server. Уязвимость была ликвидирована в пакете обновления Windows NT Service Pack 4.

Атака ICMP Redirect

Некоторые хосты Netware, устройства автоматизации на производстве и некоторые старые хосты UNIX при получении сообщения ICMP redirect могут либо прекращать работу, либо сообщать о сбое стека TCP/IP.

Кроме того, посылку ложного пакета ICMP redirect можно использовать для искажения на компьютерах адреса основного маршрутизатора (Default Gateway), что приведет к невозможности обмена этих компьютеров с хостами в других сетях.

Для защиты от внешних атак такого рода обычно запрещают прохождение пакетов ICMP redirect через все маршрутизаторы, межсетевые экраны и прокси-устройства. Большинство новых операционных систем могут игнорировать поступающие на вход стека TCP/IP команды ICMP redirect (обычно это делается по умолчанию).

ICMP Timestamp может сообщить о состоянии часов.

Если атакующий определит состояние часов на атакуемом компьютере, то он сможет более эффективно атаковать определенные генераторы псевдослучайных чисел (PRNG), которые используют текущее время, и системы аутентификации, использующие эти генераторы в своей работе.

Обеспечить защиту на сетевом уровне можно с помощью межсетевых экранов. На данном этапе используется межсетевой экран CheckPoint FireWall-1.

3 БЕЗОПАСНОСТЬ СЕТЕВОГО И ПРИКЛАДНОГО УРОВНЯ

3.1. Протокол IPSec

Шифрование данных на сетевом уровне представлено группой протоколов IPSec, основанных на современных технологиях электронной цифровой подписи и шифрования данных.

Протокол IPSec включает в себя:

- протокол аутентификации (Authentication Header, AH), который «привязывает» данные в составе пакета к своеобразной подписи, позволяющей удостовериться как в подлинности отправителя, так и в целостности принятых от него данных;
- протокол конфиденциальности данных Encapsulated Security Payload (ESP), отвечающий за шифрование содержимого отдельных пакетов (и даже некоторых IP-адресов, передаваемых в их составе). Кроме того, протокол ESP обеспечивает аутентификацию и целостность;
- протокол обмена ключами (Internet Key Exchange, IKE), который предназначен для согласования используемых алгоритмов аутентификации и шифрования, ключей и продолжительности их действия, а также для защищенного обмена ключами.

Совместное использование этих протоколов осуществляется следующим образом: между узлами устанавливается защищённый канал с помощью протокола IKE. В рамках установленного канала работает протокол протоколы аутентификации заголовка (AH) и конфинденциальности данных (ESP), которые поддерживают работу в двух режимах:

- туннельный, при котором IP-пакеты защищаются целиком, включая их заголовки;
- транспортный, обеспечивающий полную защиту только содержимого IP-пакетов.

Основным режимом является туннельный. При работе в этом режиме каждый обычный IP-пакет помещается целиком в криптозащищенном виде в конверт IPSec, который в свою очередь инкапсулируется в другой IP-пакет. Туннельный режим обычно реализуют на специально выделенных защитных шлюзах, в качестве которых могут использоваться маршрутизаторы или межсетевые экраны. Между такими шлюзами и формируются защищенные туннели IPSec. После передачи на другую сторону туннеля защищенные IP-пакеты «распаковываются» и полученные исходные IP-пакеты передаются компьютерам приемной локальной сети по стандартным правилам. Туннелирование IP-пакетов полностью прозрачно для обычных компьютеров. На оконечных системах туннельный режим может использоваться для поддержки удаленных и мобильных пользователей. В этом случае на компьютерах должно быть установлено программное обеспечение, реализующее туннельный режим IPSec.

Транспортный режим быстрее туннельного и разработан для применения на оконечных системах. Данный режим может использоваться для поддержки удаленных и мобильных пользователей, а также защиты информационных потоков внутри локальных сетей. Кроме того, транспортный режим может применяться на

шлюзах для защиты внутренних связей между одноранговыми шлюзами. Это обеспечивает эффективную защиту процесса удаленного управления маршрутизаторами, коммутаторами ATM, межсетевыми экранами и другими ключевыми компонентами инфраструктуры сети. Работа в транспортном режиме отражается на всех входящих в группу защищенного взаимодействия системах и в большинстве случаев требуется перепрограммирование сетевых приложений.

3.1.2. Протокол Authentication Header (AH)

Протокол аутентифицирующего заголовка (Authentication Header — AH) обеспечивает целостность IP-пакетов и аутентификацию источника данных, а также защиту от воспроизведения ранее посланных IP-пакетов. Этот протокол защищает от подлога и случайного искажения содержимое IP-пакетов, включая данные протоколов более высоких уровней. Полнота защиты полей IP-заголовков зависит от используемого режима работы— туннельного или транспортного.

Протокол Authentication Header (AH) создает конверт, обеспечивающий аутентификацию источника данных, их целостность и защиту от навязывания повторных сообщений (рис. 3.1). Состав и назначение полей заголовка AH:

Следующий заголовок - указывает тип протокола вышележащего уровня (TCP, UDP, ESP, ICMP)

Длина - указывает длину заголовка в 32-битных словах

SPI (Security Parameter Index) – 32-битный индекс параметров безопасности, определяющий структуру SA (Security Association), содержащую все параметры тунеля IPSec, включая типы криптографических алгоритмов и ключи шифрования.

Порядковый номер - последовательно наращиваемое поле, используется для защиты от ложного воспроизведения

Аутентификационные данные - хэш-функция, вычисленная на основе содержимого пакета с использованием алгоритмов MD5 или SAH1. Симметричный секретный ключ шифрования устанавливается вручную или по протоколу IKE.

Формат заголовка AH

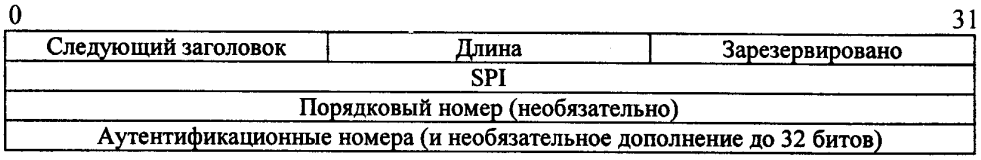

Рис 3.1

Независимо от режима работы, протокол AH предоставляет меры защиты от атак, ориентированных на нарушение целостности и подлинности пакетов сообщений. С помощью этого протокола аутентифицируется каждый пакет, что делает программы, пытающиеся перехватить управление сеансом, неэффективными. Несмотря на нахождение IP-заголовков за пределами защищенного IPSec конверта, протокол AH обеспечивает аутентификацию не только содержимого, но и заголовков IP-пакетов. Но аутентификация по протоколу AH не допускает манипулирование основными полями IP-заголовка во время прохождения пакета, по этому причине данный протокол нельзя применять в среде, где используется механизм трансляции сетевых адресов (Network Address Translation - NAT), так как манипулирование IP-заголовками необходимо для его работы.

3.1.3. Протокол ESP

Протокол инкапсулирующей конфиденциальности данных (Encapsulating Security Payload — ESP) обеспечивает выполнение следующих функций по защите информационного обмена:

- криптографическое закрытие содержимого IP-пакетов;
- частичная защита от анализа трафика путем применения туннельного режима;
- формирование и проверка цифровой подписи IP-пакетов для их защиты от нарушений подлинности и целостности;
- защита от воспроизведения IP-пакетов.

Протокол ESP обеспечивает конфиденциальность данных (рис. 3.2) и выполняет все функции протокола AH по защите зашифрованных не аутентифицируемых потоков данных.

Формат заголовка ESP

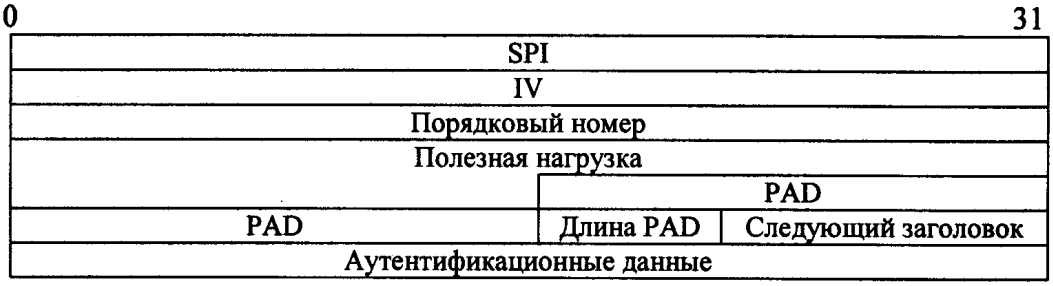

Рис. 3.2

Состав и назначение полей заголовка протокола ESP:

- SPI и порядковый номер - аналогично протоколу AH Полезная нагрузка - передаваемые данные.
- PAD (Padding) - заполнитель, используется для:
  - правильной работы алгоритмов шифрования;
  - правильного расположения данных в пакете ESP;
  - намеренного искажения действительного размера пакета;
- Длина PAD - длина заполнителя.

Спецификация IPSec допускает работу протокола ESP без использования функций AH. В протоколе ESP можно использовать фиктивное шифрование, что равнозначно применению протокола AH без аутентификации IP-заголовка.

3.1.4. Протокол обмена ключами IKE

Протокол IKE обеспечивает распределение ключей и согласование протоколов между участниками обмена. Протокол IKE решает три задачи:

- согласование алгоритмов шифрования и характеристик ключей, которые будут использоваться в защищенном сеансе;
- непосредственный обмен ключами (в том числе возможность их частой смены);
- контроль выполнения всех достигнутых соглашений.

Протокол IKE функционирует в два этапа:

- Установление защищенного соединения для процедуры обмена (IKE SA).
- Согласование всех параметров, ассоциируемых с общим «каналом» SA.

Для установления «канала» инициирующая сторона должна предложить для согласования шесть пунктов: алгоритмы шифрования, алгоритмы хеширования, метод аутентификации, информацию о группе узлов, на которые будет распространяться алгоритм Диффи-Хеллмана, псевдослучайную функцию, с помощью которой предстоит хешировать величины, используемые при обмене ключами (впрочем, допускается непосредственное использование алгоритма хеширования) и тип протокола защиты (ESP или AH).

Предусмотрены три режима обмена информацией об алгоритмах и параметрах защиты и установления «канала» SA. Два из них (основной и агрессивный) относятся к первому этапу функционирования протокола IKE и один (быстрый) — ко второму.

Основной режим (Main mode) реализует стандартный механизм установления «канала» IKE SA. Он включает в себя три процедуры двунаправленного обмена:

Стороны договариваются о базовых алгоритмах и используемых методах хеширования.

Осуществляется обмен открытыми ключами в рамках алгоритма Диффи-Хеллмана и случайными числами (nonce), которые подписываются принимающими сторонами и отправляются обратно для идентификации. По пришедшим обратно подписанным значениям nonce проверяется подлинность сторон.

Открытый ключ, полученный по схеме Диффи-Хеллмана, каждой из сторон хешируется трижды — для генерации первого комбинированного ключа, ключа аутентификации и ключа шифрования, используемого в IKE SA.

Агрессивный режим (Aggressive mode) предназначен для тех же целей, что и основной, но он проще в реализации и одновременно производительнее. Но агрессивный режим не обеспечивает защиту информации, служащей для идентификации сторон, так как такая информация передается по сети до согласования параметров защищенного «канала» SA, т. е. в незашифрованном виде.

Быстрый режим (Quick mode) обеспечивает согласование параметров основного «канала» SA и генерацию новых ключей. Так как все передачи осуществляются по защищенному туннельному соединению, то в реализации он проще. Пакет, передаваемый в данном режиме, обязательно начинается с хеша, который содержит ключ аутентификации, полученный в основном режиме, и служит для аутентификации остальной части пакета.

3.2. Режимы работы IPSec

Протокол IPSec можно использовать как в транспортном, так и в туннельном режиме. В первом случае заголовок IPSec размещается между сетевым (IP) и транспортным.

Транспортный режим разработан для применения на оконечных системах (узел - узел). Работа в этом режиме отражается на всех входящих в группу системах и в большинстве случаев требуется перепрограммирование приложений.

Туннельный режим IPSec применяется на шлюзах, и позволяет быстро развернуть туннельные IPSec-устройства по периметру сети. Обеспечить безопасность трафика между сконфигурированными таким образом сетями – очень просто, не требуется разработки новых приложений или специальных пользовательских программных средств. ПО, обеспечивающее туннельный режим, может размещаться на шлюзе или оконечных системах.

На оконечных системах туннельный режим наиболее часто применяется для поддержки удаленных и мобильных пользователей.

Соединение по протоколу IPSec устанавливается однонаправленным соглашением по безопасности SA (Security Association), поэтому на каждое соединение требуется по два SA-соглашения. Каждое из них определяет различные параметры IPSec-соединения, такие как алгоритмы шифрования и аутентификации, которые будут использованы при обмене информацией между системами, сеансовые ключи шифрования и т. д., управляющие их работой.

3.3. Виртуальные частные сети

Виртуальная частная сеть (VPN) - это технология, обеспечивающая безопасную связь по открытой (общей) сети. В общем случае VPN решает три задачи:

- организация связей между филиалами;
- соединение с партнерами и клиентами;
- взаимодействие мобильных сотрудников с корпоративной сетью.

Истинная частная сеть - принадлежность оборудования сети предприятия и гарантия конфиденциальности информации, передаваемой по этой сети. Такие сети не очень распространены. Гораздо чаще предприятие применяет для связей своих филиалов арендуемые каналы связи.

Частная сеть на арендованных каналах - при аренде канала в таких сетях предприятие делит пропускную способность магистральных каналов и коммутаторов с другими абонентами провайдера. Полоса пропускания арендованного канала полностью выделяется предприятию и является его собственностью. Корпоративные данные практически не доступны для абонентов, не являющихся пользователями корпоративной сети или сотрудниками провайдера. Это обуславливает высокую степень защищенности данных.

Если сети центрального офиса и каждого из филиалов имеют соединения с Интернет, то это дает потенциальную возможность получать доступ к ресурсам любого узла Интернет. Пользователь одного филиала предприятия может получать доступ через Интернет к ресурсам узлов других филиалов или центрального офиса.

Преимущества построения VPN на базе Интернет:

- простота и доступность реализации;
- низкая стоимость.

Недостатки:

- непредсказуемость пропускной способности;
- возможность перехвата информации, передаваемой по открытой сети.

Существуют разнообразные способы построения VPN, отличающиеся распределением функций по поддержанию VPN между корпоративной сетью и провайдером. В одном случае все функции по поддержанию VPN выполняет провайдер, гарантируя конфиденциальность и качество обслуживания клиентского трафика от точки входа в открытую сеть до точки выхода. В другом случае предприятие организует VPN собственными силами, за счет применения специальных VPN-продуктов в своей сети. В качестве таких продуктов могут использоваться:

- маршрутизаторы и межсетевые экраны с дополнительным программным обеспечением, выполняющим шифрование;

- специальные программные и аппаратные средства для создания защищенных каналов.

Как правило, все VPN-продукты обеспечивают только шифрование данных, но не гарантируют пропускную способность. Эта задача может быть решена только силами провайдера.

3.4. Типы VPN-устройств

Существует несколько основных типов VPN-устройств:

- отдельное аппаратное устройство VPN на основе специализированной ОС реального времени, имеющее 2 или более сетевых интерфейса и аппаратную криптографическую поддержку - так называемый «черный ящик»;
- отдельное программное решение, которое дополняет стандартную операционную систему функциями VPN;
- расширение межсетевого экрана за счет дополнительных функций защищенного канала;
- средства VPN, встроенные в маршрутизатор. Устройства VPN могут играть роль шлюза или клиента (рис. 3.3)

Шлюз VPN - это устройство, подключенное к нескольким сетям, выполняющее функции шифрования и аутентификации для узлов позади него. Размещение шлюза VPN аналогично размещению межсетевого экрана.

Клиент VPN - это программный или программно-аппаратный комплекс, сетевые возможности которого модифицированы для выполнения обмена со шлюзами VPN или другими VPN-клиентами. Как правило, VPN - клиент представляет собой программное решение, дополняющее стандартную операционную систему.

Шлюзы и клиенты VPN

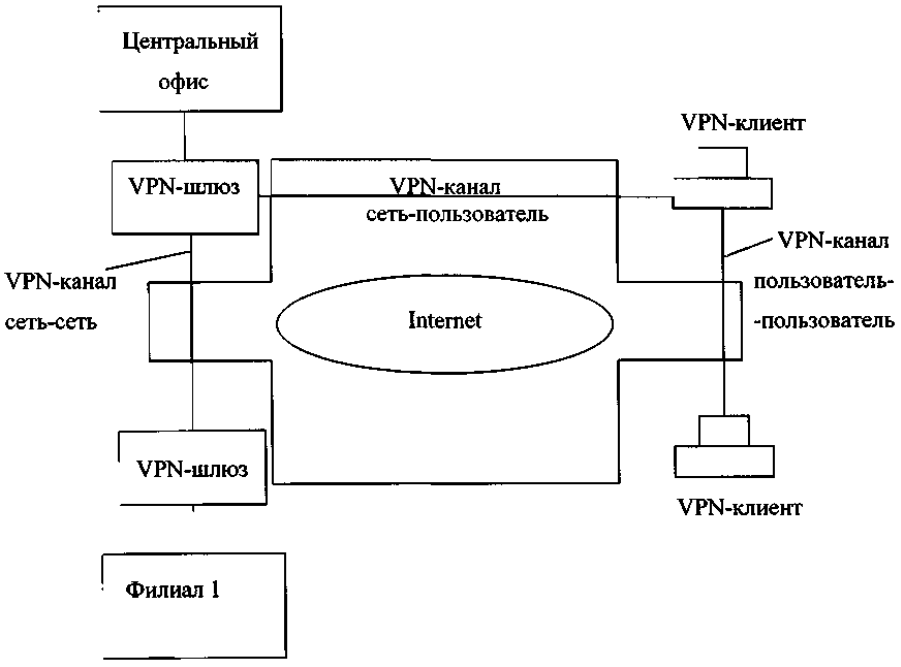

Рис. 3.3

3.5. Атаки на протокол TCP и его защита

3.5.1. Сканирование портов

Схема связи по протоколу TCP предполагает использование портов для идентификации приложений. Следовательно, определив номера открытых портов на удалённом узле, можно узнать о работающих на нём приложениях, сделать вывод о роли этого узла в корпоративной сети, узнать версию операционной системы. Сканирование портов относится к действиям типа «подготовка к атаке». Существует множество средств для проведения сканирования. Утилита Nmap - один из самых известных инструментов подобного рода.

3.5.2. SynFlood

В случае получения запроса на соединение система отвечает на пришедший SYN-пакет SYN/ACK-пакетом, переводит сессию в состояние SYN_RECEIVED и заносит ее в очередь. Если в течении заданного времени от клиента не придет ACK, соединение удаляется из очереди, в противном случае соединение переводится в состояние ESTABLISHED (установлено).

Если очередь входных соединений заполнена, а система получает SYN-пакет, приглашающий к установке соединения, он будет проигнорирован.

Затопление SYN-пакетами основано на переполнении очереди сервера, после чего сервер перестает отвечать на запросы пользователей. После истечение некоторого времени (время тайм-аута зависит от реализации) система удаляет запросы из очереди. Обычно используются случайные (фиктивные) обратные IP-адреса при формировании пакетов, что затрудняет обнаружение злоумышленника.

3.5.3. Address Spoofing

Для формирования ложного TCP-пакета (и последующего перехвата установленного между доверенными узлами виртуального соединения) атакующему необходимо знать текущие значения идентификаторов для данного соединения - Seq и Ack.

Когда атакующий находится в одном сегменте с атакуемым объектом или через его сегмент проходит трафик предполагаемого объекта атаки, то задача получения этих значений и решается путем прослушивания и анализа сетевого трафика. Поэтому наибольший интерес представляют межсегментные атаки, когда атакующий и его цель находятся в разных сегментах сети. В этом случае можно попытаться получить значения идентификаторов путём математического предсказания начального значения идентификатора TCP-соединения экстраполяцией его предыдущих значений или (в самом сложном случае) простым перебором.

3.5.4. Session Hijacking

Схема атаки «Подмена участника соединения» показана на рис.3.5.

Схема атаки «Подмена участника соединения»

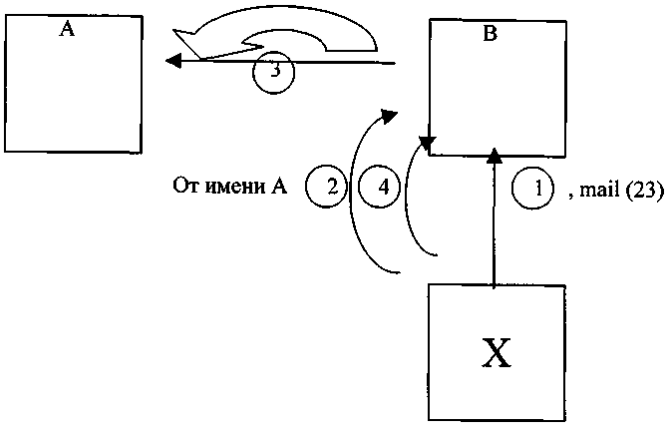

Рис. 3.5

При осуществлении данной атаки перед атакующим возникает следующая проблема. Так как X посылает пакет (шаг 2) на B от имени A, то хост B ответит на A пакетом (шаг 3). A, так как хост A не посылал на хост B никакого пакета с запросом, то A, получив ответ от B, перешлет на B пакет с битом RST - закрыть соединение. Атакующего с хоста X это естественно не устраивает, поэтому одной из атак, целью которых является нарушение работоспособности системы, X должен вывести из строя на некоторое время хост A.

В итоге узел B считает, что к нему подключился пользователь с доверенного хоста A, а на самом деле это атакующий с узла X. И хотя X никогда не сможет получить пакеты с хоста B, но он сможет выполнять на нем команды (например, r-команды).

3.6. Протокол SSL

Протокол SSL (Secure Socket Layer) предназначен для защиты данных, передаваемых между приложениями (клиентом и сервером). SSL работает поверх транспортного протокола, предполагающего установление соединения (TCP). SSL "прозрачен" для служб прикладного уровня, таких, как HTTP и FTP.

Протокол SSL базируется на следующих принципах:

- Защищённый канал передачи данных. Для шифрования данных применяются симметричные алгоритмы (DES,RC4).
- Обязательная аутентификация сервера с использованием асимметричной криптографии (Diffie-Hellman, RSA и FORTEZZA).
- Надежность канала передачи данных. Для контроля целостности передаваемых данных используется специальный алгоритм - Message Authentication Code (MAC). Довольно распространенным является алгоритм MD5. Обычно, и сам MAC-code так же шифруется.

Протокол SSL состоит из двух протоколов (рис. 3.6):

- SSL Record Protocol, используемый для инкапсуляции передаваемых и получаемых данных.
- SSL Handshake Protocol, используемый для установления параметров соединения.

Архитектура SSL

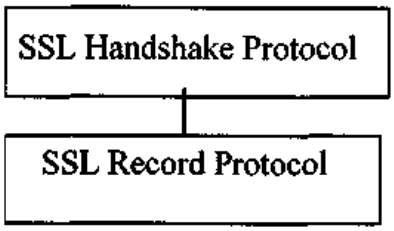

Рис. 3.6

Протокол SSL Record Layer используется для всех SSL коммуникаций.

Параметры соединения по протоколу SSL определяются протоколом SSL Handshake, который работает поверх протокола SSL Record Layer. Когда клиент и сервер устанавливают соединение, они согласовывают такие параметры, как версия протокола и алгоритм шифрования, аутентифицируют друг друга и генерируют ключ сеанса.

Так как обычно SSL используется для организации безопасного доступа по протоколу HTTP, то его поддержка реализована в различных WEB-серверах,

3.7. Протокол SSH

SSH – как собственно программа, так и задействованный в ней протокол.

SSH поддерживает возможность работы с telnet; безопасную работу с протоколом XII благодаря возможности перенаправления соответствующих данных по надежным ssh-каналам; безопасную замену многим r-командам Unix (rsh, rlogin и т.д.), с которыми традиционно связаны проблемы обеспечения безопасности.

Протокол SSH имеет следующую архитектуру:

Архитектура SSH

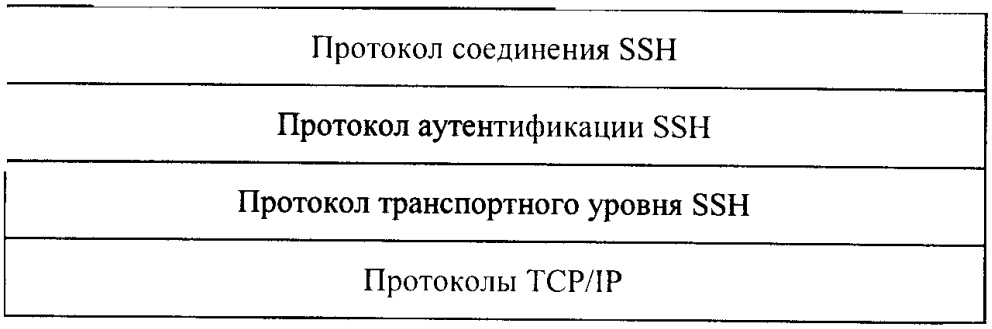

Рис. 3.7

Проект стандарта ssh описывает протоколы ssh и состоит из нескольких документов, которые описывают общую архитектуру протокола, а также протоколы трех уровней: протокол транспортного уровня, протокол аутентификации и протокол соединения.

- Протокол транспортного уровня обеспечивает аутентификацию сервера, конфиденциальность и целостность.
- Протокол аутентификации обеспечивает аутентификацию клиента для сервера.

- Протокол соединения ssh мультиплексирует безопасный (шифруемый) канал, представляя его в виде нескольких логических каналов, которые используются для различных целей (различных видов служб).

Протокол транспортного уровня предусматривает возможность сжатия данных и работает поверх соединения TCP/IP. Протокол аутентификации работает поверх протокола транспортного уровня, а протокол соединения, поверх протокола аутентификации.

С целью повышения безопасности осуществляется не только аутентификация клиента для сервера но и аутентификация сервера клиентом.

Каждый работающий с ssh узел, на котором может выполняться как клиент, так и сервер, должен иметь не менее одного ключа, причем для шифрования допускаются различные криптографические алгоритмы. Несколько узлов могут иметь общий ключ, однако каждый узел должен иметь хотя бы один ключ, с которым работает каждый из требуемых алгоритмов работы с открытыми ключами. В проекте стандарта в настоящее время требуемый алгоритм только один - DSS (Digital Signature Standard).

Ключ узла-сервера используется при обмене открытыми ключами с целью проверки того, что клиент действительно общается с настоящим (а не подмененным) сервером.

Для этого клиент должен знать открытый ключ узла-сервера.

Протоколом предусмотрена возможность отказа от проверки ключа узла-сервера при самом первом обращении клиента к этому серверу. При этом соединение клиент-сервер будет защищено от пассивного прослушивания сети, но возникает опасность атаки типа «временной подмены сервера». Если эта возможность используется, ключ узла-сервера будет автоматически передан клиенту и сохранен в его локальном файле.

Проектом протокола ssh предусмотрено, что между клиентом и сервером происходят переговоры, в результате которых выбираются методы шифрования, форматы открытых ключей и т.п., которые будут использованы в данном сеансе.

3.8. Проблемы безопасности протоколов прикладного уровня

Прикладной уровень в семействе TCP/IP представлен следующими службами:

- Служба разрешения имён (DNS).
- Электронная почта (SMTP, POPS, EMAP).
- Протокол HTTP
- Передача файлов (FTP)
- Протокол удалённого терминала (TELNET).
- Сетевая файловая система (NFS)
- Удалённое выполнение процедур (RPC)
- Мониторинг и управление сетью (SNMP).

Практически все прикладные службы работают по схеме «клиент/сервер».

Протоколы FTP, HTTP, TELNET, POPS спроектированы так, что передаваемая информация не шифруется и может быть легко перехвачена и проанализирована. То есть имеются все предпосылки для осуществления атак типа «пассивное прослушивание». Имена и пароли пользователей передаются в открытом, незашифрованном виде.

Протокол SMTP не имеет никакой аутентификации, в результате легко могут быть отправлены электронные письма с любым обратным адресом при работе напрямую с командами этого протокола. Кроме того, протокол SMTP поддерживает команды VRFY и EXPN, которые позволяют получить информацию о пользователях. Эти команды лучше отключить на уровне конкретного почтового сервера.

Служба DNS имеет две основных проблемы: во-первых, она предназначена для работы с общедоступными данными и может быть использована нарушителем для получения критичной информации о системе, во-вторых, главное назначение DNS - хранение соответствий между именами и адресами узлов и нарушение этого соответствия может привести к нарушению работы многих узлов Internet.

Службы Internet прикладного уровня реализуются по схеме клиент/сервер. Клиентская и серверная части представляют собой обычные приложения.

Как правило, порт серверного процесса (23) находится в «слушающем» режиме. В случае поступления запроса на обслуживание, telnet (имеется ввиду ОС UNIX) назначает каждому удаленному клиенту псевдотерминал (pty) в качестве стандартного файла ввода (stdin), стандартного файла вывода (stdout) и стандартного файла ошибок (stderr). В качестве транспорта TELNET использует протокол TCP.

Примерно также реализованы и остальные службы (FTP, POPS и т. п.).

Проблемы безопасности в данном случае связаны с ошибками реализации службы, т. е. с ошибками программистов. Атаки, использующие подобные уязвимости, имеют механизм реализации «запуск приложений на удалённом узле».

3.9. Меры защиты прикладного уровня

Для защиты применяется регулярное обновление программного обеспечения WEB-серверов, FTP-серверов, почтовых серверов с целью устранения обнаруженных ошибок реализации.

Для защиты DNS существуют два направления:

- переход на защищённый протокол DNSSec;
- разделение пространства имён с целью сокрытия внутреннего пространства имён от внешнего мира.

Дня ликвидации ограничений протокола DNS создана рабочая группа, обеспечивающая аутентификацию и целостность информации, содержащейся в DNS посредством шифрования.

DNSSec реализует три механизма:

- Key Distribution - механизм распределения открытых ключей
- Data Origin Authentication and Integrity - обеспечение целостности и аутентичности информации DNS
- Transaction and request authentication - аутентификация транзакции Key Distribution

1. Обеспечение целостности и аутентичности достигается путём шифрования с открытыми ключами для подписи информации, содержащейся в DNS. Такие криптографические подписи обеспечивают целостность за счет вычисления криптографического хэша (т. е. уникальной контрольной суммы) данных и затем защиты вычисленной величины от несанкционированных изменений посредством ее шифрования. Хэш шифруется с помощью личного ключа из пары ключей, чтобы любой желающий мог воспользоваться открытым ключом для его дешифровки.

Если дешифрованное получателем значение хэша совпадает с вычисленным, то данные достоверны (не подвергались несанкционированному изменению).

2. Аутентификация транзакций. Предполагает шифрование сообщения с помощью секретного ключа. Один и тот же ключ используется как для генерации подписи, так и для ее проверки (т. е. вся процедура является закрытой) и общий секретный ключ (также называемый "общим секретом") известен только узлам из одной локальной сети или (в крайнем случае) в одной территориальной сети.

3. Разделение пространства имён. Служба DNS - один из источников информации о структуре сети. В то же время, для внешнего пользователя достаточно иметь доступ только к небольшой части внутреннего пространства имён. Поэтому необходимо разделение пространства имён. Таким образом:

- Внутренние узлы имеют доступ к внутреннему пространству имён
- Часть внутренних узлов имеет доступ к глобальному пространству имён (это узлы с доступом в Internet)
- Внешние узлы имеют доступ к необходимой (минимальной) части внутреннего пространства имён

3.10. Реализация корпоративной службы DNS

При традиционной схеме реализации корпоративной службы DNS вся информация о домене организации размещена на первичном сервере и доступна любому желающему (рис. 3.8.). Даже если принять какие-то меры по защите первичного сервера, есть ещё вторичный сервер (расположенный у провайдера).

Традиционная реализация DNS-службы

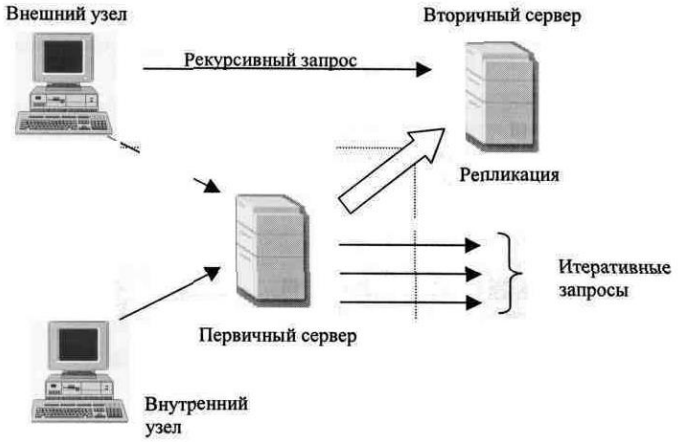

Рис.3.8

Один из вариантов решения - двухсерверная конфигурация (рис. 3.9). Согласно этой схеме, имеются два первичных сервера: на одном из них размещается минимальная версия доменной информации и этот сервер регистрируется в глобальном пространстве имён, другой хранит полную версию и доступ к нему извне блокируется средствами межсетевого экрана. Первый обслуживает внешних клиентов, второй - внутренних.

Двухсерверная конфигурация

Рис. 3.9

Недостаток такой схемы - замедление при обслуживании внутренних клиентов, не имеющих доступа в Internet (при вводе запросов, содержащих ошибки или при обращении к блокированным ресурсам).

Трёхсерверная конфигурация (рис.3.10). В этом случае первичный сервер, содержащий полную версию внутреннего пространства имён, объявлен ответственным за корневой домен и полностью изолирован от внешнего мира.

Внутренние клиенты, не нуждающиеся в доступе к глобальному пространству имён, обслуживаются этим сервером. Внутренние клиенты с доступом в Internet обслуживаются вторичным сервером с полной версией доменной информации.

Трехсерверная конфигурация

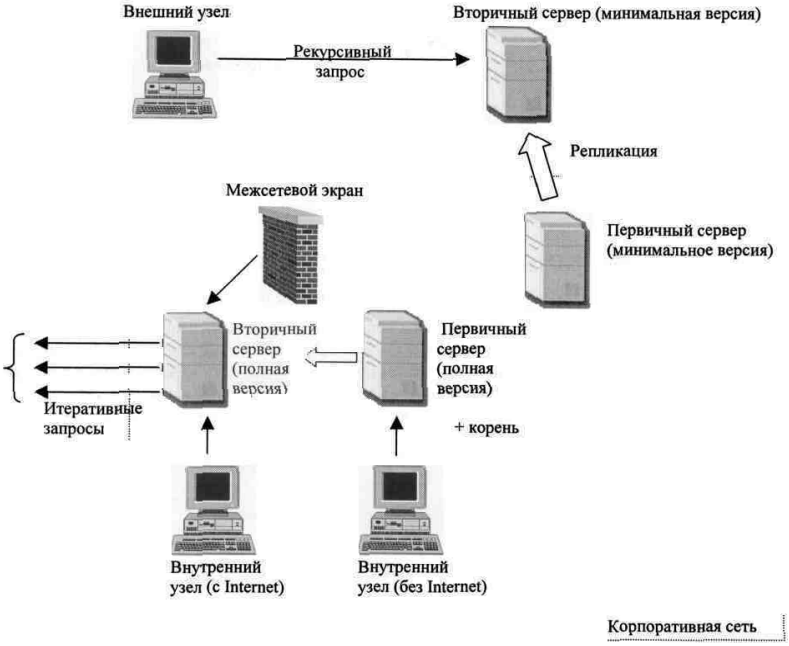

Рис. 3.10

Для трёхсерверной конфигурации (рис. 3.11):

- первичный сервер с минимальной версией доменной информации следует: поместить в демилитаризованную зону, т. к. он должен иметь соединение с Internet и в то же время быть максимально изолированным от внутренней

сети;

- первичный сервер, содержащий полную версию внутреннего пространства имён, и объявленный ответственным за корневой домен можно разместить на любом внутреннем узле, т. к. соединения с Internet не нужно;
- вторичный сервер с полной доменной информацией размещается на одном из улов внутренней сети или на межсетевом экране (доступ к нему извне должен быть блокирован).

Размещение DNS-серверов

Рис. 3.11

4. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

4.1 Основные термины.

Криптография — область знаний, объединяющая принципы, методы и средства преобразования сообщений с целью маскировки содержания информации, невозможности ее искажения и несанкционированного доступа к ней.

Шифрование информации — процесс преобразования открытых данных в зашифрованные с помощью ключа.

Ключ - конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования информации, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма.

Алгоритм криптографического преобразования — набор математических правил, определяющих содержание и последовательность операций, по зашифрованию и расшифрованию информации.

Дешифрование (расшифрование) информации — процесс преобразования зашифрованных данных в открытые при помощи ключа.

Любой криптографический алгоритм зависит от степени защиты ключей. При этом основной проблемой является корректное управление ключами. Данная проблема может быть решена использованием специальных криптографических протоколов.

Криптографический протокол — набор правил и процедур, определяющих использование криптоалгоритма и ключей шифрования.

Криптографически система — совокупность криптоалгоритмов, протоколов и процедур управления ключами.

На практике любой шифр, используемый в той или другой криптосистеме, поддается раскрытию с определенной трудоемкостью. В связи с этим возникает необходимость оценивания криптостойкости применяемых шифров.

Криптостойкость — характеристика шифра, определяющая его стойкость к дешифрованию.

Методы расшифрования (дешифрования) информации незаконным объектом разрабатываются на основе криптоанализа.

Криптоанализ — область знаний о раскрытии шифров (ключей) по имеющемуся зашифрованному тексту.

4.2 Оценка надежности криптоалгоритмов.

Все современные шифры базируются на принципе Кирхгофа, согласно которому секретность шифра обеспечивается секретностью ключа, а не секретностью алгоритма шифрования.

Стойкость криптосистемы зависит от сложности алгоритмов преобразования, длины ключа, а точнее от объема ключевого пространства, метода реализации: при программной реализации необходимо дополнительно защищаться от разрушающих программных воздействий (закладок, вирусов и т. п.).

Методы оценки качества криптоалгоритмов, используемые на практике:

1. всевозможные попытки их вскрытия.

Многое зависит от квалификации, опыта, интуиции криптоаналитиков и от правильной оценки возможностей противника. Обычно считается, что противник знает шифр, имеет возможность его изучения, знает некоторые характеристики

открытых защищаемых данных, например, тематику сообщений, их стиль, стандарты, форматы и т. п.

2. анализ сложности алгоритма дешифрования;

Оценку стойкости шифра заменяют оценкой минимальной сложности алгоритма его вскрытия. Сложность вычислительных алгоритмов можно оценивать числом выполняемых элементарных операций, при этом необходимо учитывать их стоимость и затраты на их выполнение. Качественный шифр невозможно раскрыть способом более эффективным чем полный перебор по всему ключевому пространству, при этом надо рассчитывать только на то, что у противника не хватит времени и ресурсов, чтобы это сделать. Однако проблема состоит в том, что получение строгих доказуемых оценок нижней границы сложности алгоритмов рассматриваемого типа не представляется возможным. Таким образом, всегда возможна ситуация, когда алгоритм вскрытия шифра, сложность которого анализируется, оказывается вовсе не самым эффективным.

3. оценка статистической безопасности шифра.

Проводятся статистические тесты, устанавливающие зависимость изменений в зашифрованном тексте от изменений символов или бит в исходном тексте или ключе, а также анализирующих, насколько выходная зашифрованная последовательность по своим статистическим свойствам приближается к истинно случайной последовательности.

Необходимые условия стойкости криптосистемы, проверяемые статистическими методами:

- отсутствие статистической зависимости между входной и выходной последовательностями;
- выходная последовательность по своим статистическим свойствам не отличается от истинно случайной последовательности;
- при неизменной входной информационной последовательности незначительное изменение ключа приводит к существенному изменению выходной последовательности;
- при неизменном ключе незначительное изменение входной последовательности приводит к существенному изменению выходной последовательности;
- не существует зависимостей между ключами, последовательно используемыми в процессе шифрования.

Существует много различных криптоалгоритмов, при этом нет ни одного, подходящего для всех случаев. В каждой конкретной ситуации выбор криптоалгоритма определяется следующими факторами:

- особенностью защищаемой информации (документы, исходные тексты программ, графические файлы и т.п.);
- особенностями среды хранения или передачи информации;
- ценностью информации, характером защищаемых секретов, временем обеспечения секретности;
- объемами информации, скоростью ее передачи, степенью оперативности ее предоставления пользователю;
- возможностями собственников информации, владельцев средств сбора, обработки, хранения и передачи информации по ее защите;
- характером угроз, возможностями противника.

4.3. Классификация методов шифрования информации.

Современные криптографические методы тесно связаны с методами шифрования сообщений, которые зависят от способа использования ключей.

По характеру использования ключа криптографические методы делятся на одноключевые (симметричные) и двухключевые (асимметричные) (рис. 4.1).

Одноключевые методы являются классическими методами. Для шифрования и расшифрования в них используется один и тот же ключ, сохранение которого в тайне обеспечивает надежность защиты.

Все одноключевые методы по способу шифрования делятся на блочные, поточные и комбинированные. Двухключевые методы преобразования всегда блочные.

Схема классификации криптографических методов защиты информации

Рис. 4.1.

Для блочных методов шифрования открытая информация разбивается на блоки фиксированной длины, каждый из которых шифруется отдельно, независимо от его положения во входной последовательности. Одноключевые (блочные) методы шифрования: шифры перестановки, шифры подстановки, шифры на основе аналитических преобразований, которые по существу являются составными шифрами.

Поточное шифрование основано на сложении символов открытой информации с символами ключа с заданными свойствами. При этом выполняется поэлементное шифрование потока информации. Шифрование и расшифрование, как правило, выполняется с использованием операции сложения по модулю 2.

При комбинированном шифровании применяются принципы блочного и поточного шифрования, то есть возможно использование блочного шифра в поточном режиме (гаммирование, шифрование с обратной связью) и поточного шифра в блочном режиме (шифрование блоков).

Асимметричные (двухключевые) методы шифрования используют два ключа: открытый и секретный. Если открытый ключ используется для шифрования, а

секретный ключ — для расшифрования, то это алгоритм шифрования с открытым ключом.

Если секретный ключ используется для шифрования, а открытый - для расшифрования, то это алгоритм электронной цифровой подписи.

4.4. Блочные шифры.

Блочные шифры представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемых к блоку (части) шифруемого текста. При блочном шифровании информация разбивается на блоки фиксированной длины и шифруется поблочно. Блочные шифры бывают:

- шифры перестановки (transposition, permutation, P-блоки);
- шифры замены (подстановки, substitution, S-блоки).

Шифры перестановок переставляют элементы открытых данных (биты, буквы, символы) в некоторый новый порядок. Различают шифры горизонтальной, вертикальной, двойной перестановки, решетки, лабиринты, лозунговые и др.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу. Различают шифры простой, сложной, парной замены, буквенно-слоговое шифрование и шифры колонной замены. Шифры замены делятся на две группы:

- моноалфавитные (код Цезаря) ;
- полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma).

Блочное шифрование можно осуществлять:

1. Без обратной связи (ОС). Несколько битов (блок) исходного текста шифруются одновременно, и каждый бит исходного текста влияет на каждый бит шифртекста. Однако взаимного влияния блоков нет, то есть два одинаковых блока исходного текста будут представлены одинаковым шифртекстом. Поэтому подобные алгоритмы можно использовать только для шифрования случайной последовательности битов (например, ключей). Примерами являются DES в режиме ECB и ГОСТ 28147-89 в режиме простой замены.

2. С обратной связью. Обычно ОС организуется так: предыдущий шифрованный блок складывается по модулю 2 с текущим блоком. В качестве первого блока в цепи ОС используется инициализирующее значение. Ошибка в одном бите влияет на два блока - ошибочный и следующий за ним. Пример - DES в режиме CBC.

4.4.1. Шифры замены.

Шифр замены – это алгоритм шифрования, который производит замену каждой буквы открытого текста на какой-то символ шифрованного текста. Получатель сообщения расшифровывает его путем обратной замены.

В классической криптографии различают 4 разновидности шифров замены:

- Простая замена, или одноалфавитный шифр. Каждая буква открытого текста заменяется на один и тот же символ шифртекста.
- Омофонная замена. Каждой букве открытого текста ставятся в соответствие несколько символов шифртекста. Например, буква "А" заменяется на цифру 5, 13, 25 или 57 , а буква "Б" — на 7, 19, 31 или 43 и так далее.

- Блочная замена. Шифрование открытого текста производится блоками. Например, блоку "АБА" может соответствовать "РТК", а блоку "АББ" — "СЛЛ".
- Многоалфавитная замена. Состоит из нескольких шифров простои замены. Например, могут использоваться пять шифров простой замены, а какой из них конкретно применяется для шифрования данной буквы открытого текста, — зависит от ее положения в тексте.

Примером шифра простой замены может служить программа ROT13, которую обычно можно найти в операционной системе UNIX. С ее помощью буква "A" открытого текста на английском языке заменяется на букву "N", "B" — на "O" и так далее. Таким образом, ROT13 циклически сдвигает каждую букву английского алфавита на 13 позиций вправо. Чтобы получить исходный открытый текст надо применить функцию шифрования ROT 13 дважды:

$$P = ROT13(ROT13(P))$$

Все упомянутые шифры замены легко взламываются с использованием современных компьютеров, так как замена недостаточно хорошо маскирует стандартные частоты встречаемости букв в открытом тексте.

Разновидностью шифра замены можно считать код, который вместо букв осуществляет замену слов, фраз и даже целых предложений. Например, кодовый текст "ЛЕДЕНЕЦ" может соответствовать фразе открытого текста "ПОВЕРНУТЬ ВПРАВО НА 90°". Однако коды применимы только при определенных условиях: если, например, в коде отсутствует соответствующее значение для слова "МУРАВЬЕД", то нельзя использовать это слово в открытом тексте сообщения, предназначенном для кодирования.

4.4.2. Шифры перестановки.

В качестве ключа в шифрующих таблицах используются:

• размер таблицы;

• слово или фраза, задающие перестановку;

• особенности структуры таблицы.

Одним из самых простых табличных шифров перестановки является простая перестановка, для которой ключом служит размер таблицы.

Например, сообщение

ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ

записывается в таблицу из 5 строк и 7 столбцов поочередно по столбцам.

Заполнение таблицы из 5 строк и 7 столбцов

Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Ь	В	О
М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

Рис. 4.3.

После заполнения таблицы текстом сообщения по столбцам для формирования шифртекста считывают содержимое таблицы по строкам. Если шифртекст записать группами по пять букв, получается такое шифрованное сообщение:

ТНПВЕ ГЛЕАР АДОНР ТИЕЬВ ОМОБТ МПЧИР ЫСООЬ

Отправитель и получатель сообщения должны заранее условиться об общем ключе в виде размера таблицы. Объединение букв шифртекста в 5-буквенные группы не входит в ключ шифра и осуществляется для удобства записи несмыслового текста. При расшифровании действия выполняют в обратном порядке.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый одиночной перестановкой по ключу. Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется **двойной перестановкой**. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровании порядок перестановок должен быть обратным.

Число вариантов двойной перестановки быстро возрастает.- при увеличении размера таблицы:

- для таблицы 3x3 36 вариантов;
- для таблицы 4x4 576 вариантов;
- для таблицы 5x5 14400 вариантов.

Однако двойная перестановка не отличается высокой стойкостью и сравнительно просто "взламывается" при любом размере . таблицы шифрования.

Магическими квадратами – это квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

Шифруемый текст вписывается в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный благодаря перестановке букв исходного сообщения.

Число магических квадратов быстро возрастает с увеличением размера квадрата. Существует только один магический квадрат размером 3x3 (если не учитывать его повороты). Количество магических квадратов 4x4 составляет уже 880, а количество магических квадратов 5x5 — около 250000.

4.5. Поточные шифры.

Поточный шифр — это симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости как от используемого ключа, так и от его расположения в потоке открытого текста.

Синхронные поточные шифры генерируют псевдослучайную последовательность независимо от каких-либо битов открытого или шифрованного текста. При таком шифровании необходима точная синхронизация на концах линии связи. При потере битов или вставке новых при передаче корректное дешифрование становится невозможным. Для синхронизации могут использоваться специальные маркирующие последовательности, вставляемые в шифротекст. Такие шифры не распространяют ошибки: ошибка в шифровании одного бита не влияет на другие биты.

Самосинхронизирующиеся поточные шифры используют предыдущие N битов при генерации, что позволяет автоматически синхронизироваться источнику и получателю. Потерянные или вставленные биты могут быть легко обнаружены.

4.5.1. Гаммирование.

Гаммирование – процесс наложения по определенному закону гаммы шифра на открытые данные. Гамма шифра — это псевдослучайная последовательность, выработанная по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных.

Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы на открытые данные обратимым образом (например, используя сложение по модулю 2).

Процесс дешифрования данных сводится к повторной генерации гаммы шифра при известном ключе и наложении такой гаммы на зашифрованные данные.

Полученный зашифрованный текст является достаточно трудным для раскрытия в том случае, если гамма шифра не содержит повторяющихся битовых последовательностей.

Перед зашифрованием открытые данные разбивают на блоки $T_0^{(i)}$ одинаковой длины, обычно по 64 бита. Гамма шифра вырабатывается в виде последовательности блоков $Г_ш^{(i)}$ аналогичной длины. Уравнение зашифрования можно записать в виде

$$T_ш^{(i)} = Г_ш^{(i)} \oplus T_0^{(i)},\ I = 1\ldots M,$$

где $T_ш^{(i)}$ – i-й блок шифртекста, $Г_ш^{(i)}$ – i-й блок гаммы шифра, $T_0^{(i)}$ – i-й блок открытого текста; M – количество блоков открытого текста.

Процесс расшифрования сводится к повторной генерации гаммы шифра и наложению этой гаммы на зашифрованные данные. Уравнение расшифрования имеет вид

$$T_0^{(i)} = Г_ш^{(i)} \oplus T_ш^{(i)}$$

Получаемый этим методом шифртекст достаточно труден для раскрытия, так как ключ является переменным. Гамма шифра должна изменяться случайным образом для каждого шифруемого блока. Если период гаммы превышает длину всего шифруемого текста и злоумышленнику неизвестна никакая часть исходного текста, то такой шифр можно раскрыть только прямым перебором всех вариантов ключа. В этом случае криптостойкость шифра определяется длиной ключа.

4.5.2. Принципы построения генераторов псевдослучайных кодов.

В качестве ключа используется случайная строка битов, которая объединяется с открытым текстом, также представленным в двоичном виде (например, A=00000, B =00001, C = 00010 и т.д.), с помощью побитового сложения по модулю 2, и в результате получается шифрованный текст. Для решения проблемы генерации двоичной последовательности большой длины широко используются генераторы двоичных псевдослучайных последовательностей.

К криптографически стойкому генератору псевдослучайной последовательности чисел предъявляются три основных требования:

- период гаммы должен быть достаточно большим для шифрования сообщений различной длины;
- гамма должна быть практически непредсказуемой (невозможность предсказать следующий бит гаммы, даже если известны тип генератора и предшествующий кусок гаммы);
- генерирование гаммы не должно вызывать больших технических сложностей.

Длина периода гаммы является самой важной характеристикой генератора псевдослучайных чисел. Чем длиннее ключ, тем труднее его подобрать. Длина периода гаммы зависит от выбранного алгоритма получения псевдо- случайных чисел.

4.6. Криптосистемы с секретным ключом. Модель системы и ее основные свойства.

Модель криптосистемы с секретным ключом представлена на рисунке 4.7

Источник сообщения передает "открытый текст" X, а рандомизатор формирует рандомизируюшую последовательность R. Задача рандомизатора – выровнять частоту появления символов источника сообщения путем перехода к алфавиту большего объема. Источник ключа генерирует некоторый ключ К, а шифратор преобразует открытый текст X в шифротекст (криптограмму), который является некоторой функцией X, а конкретный вид криптограммы определяется секретным ключом и рандомизирующей последовательностью.

Шифротекст передается по незащищенному каналу связи, и несанкционированный получатель имеет все технические возможности для ее перехвата. В соответствии с известным в криптологии "правилом Керхкоффа" предполагается, что алгоритм преобразования известен противнику, и надежность шифра определяется только ключом.

Модель криптосистемы с секретным ключом

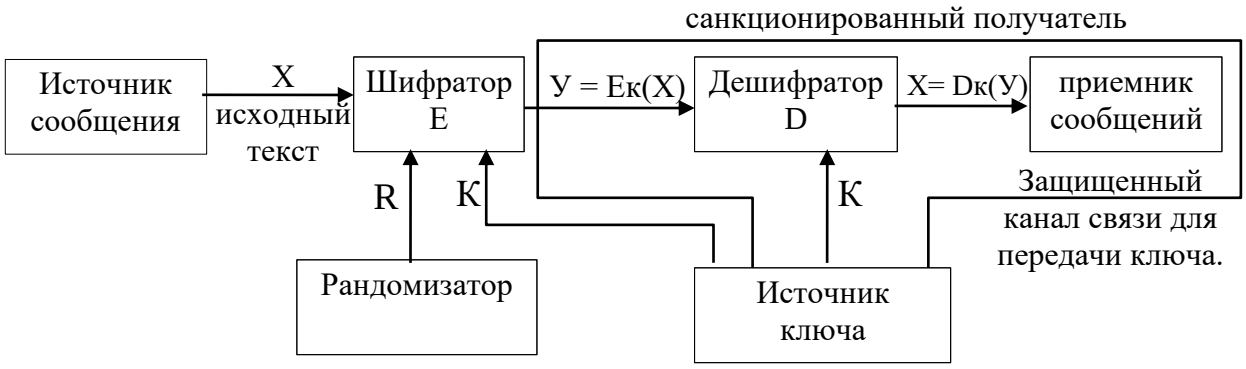

Рис. 4.7.

Дешифратор санкционированного получателя, зная секретный ключ, восстанавливает открытый текст.

При разработке практических шифров используются два принципа: рассеивание и перемешивание. Рассеивание - распространение влияния одного знака открытого текста на множество знаков шифротекста, что позволяет скрыть статистические свойства открытого текста. Перемешивание – использование шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текста. Однако шифр должен не только затруднять раскрытие, но и обеспечивать легкость шифрования и дешифрования при известном секретном ключе. Поэтому была принята идея использовать произведение простых шифров, каждый из которых вносит небольшой вклад в значительное суммарное рассеивание и перемешивание.

4.7. Криптосистемы с открытым ключом. Модель системы и ее основные свойства.

В таких системах для шифрования данных используется один ключ, а для расшифрования — другой ключ (отсюда и название — асимметричные). Первый ключ является открытым и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифрование данных с помощью открытого ключа невозможно.

Для этого используют второй ключ, который является секретным. Ключ расшифрования не может быть определен из ключа зашифрования.

Обобщенная схема асимметричной криптосистемы с открытым ключом показана на рис. В этой криптосистеме применяют два различных ключа: K_B – открытый ключ отправителя A; k_B – секретный ключ получателя B. Генератор ключей целесообразно располагать на стороне получателя B (чтобы не пересылать секретный ключ k_B по незащищенному каналу). Значения ключей K_B и k_B зависят от начального состояния генератора ключей.

Раскрытие секретного ключа k_B по известному открытому ключу K_B должно быть вычислительно неразрешимой задачей.

Характерные особенности асимметричных криптосистем:

1. Открытый ключ K_B и криптограмма C могут быть отправлены по незащищенным каналам, т.е. противнику известны K_B и C.

2. Алгоритмы шифрования и расшифрования

$$E_B : M \to C,$$
$$D_B : C \to M,$$

являются открытыми.

Обобщенная схема асимметричной криптосистемы с открытым ключом

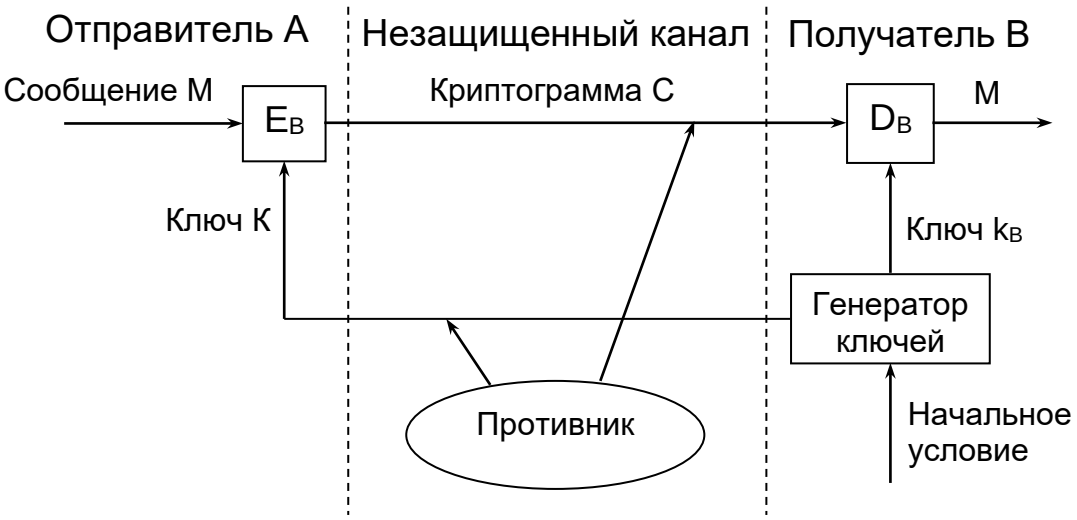

Рис. 4.8.

Защита информации в асимметричной криптосистеме основана на секретности ключа k_B.

У. Биффи и М. Хеллман сформулировали требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы:

1. Вычисление пары ключей (K_B, k_B) получателем В на основе начального условия должно быть простым.

2. Отправитель А, зная открытый ключ K_B и сообщение М, может легко вычислить криптограмму

$$C = E_{K_B}(M) = E_B(M)$$

3. Получатель В, используя секретный ключ k_B и криптограмму С, может легко восстановить исходное сообщение

$$M = D_{K_B}(C) = D_B(C) = D_B[E_B(M)]$$

4. Противник, зная открытый ключ K_B при попытке вычислить секретный ключ k_B наталкивается на непреодолимую вычислительную проблему.

5. Противник, зная пару (K_B, С), при попытке вычислить исходное сообщение М наталкивается на непреодолимую вычислительную проблему

5 БЕЗОПАСНОСТЬ УРОВНЯ ОПЕРАЦИОННЫХ СИСТЕМ 4 ЧАСА

5.1. Модель безопасности ОС Windows. Компоненты системы безопасности.

В сетевой операционной системе Windows существует единая система для идентификации, проверки подлинности (аутентификации), контроля (разграничения) доступа и записи информации о событиях (аудита), связанных с

безопасностью. В рамках данной архитектуры все объекты и все процессы подчиняются требованиям системы безопасности, включающей в себя несколько основных компонентов (рис. 5.5.).

Структурная схема системы безопасности Windows

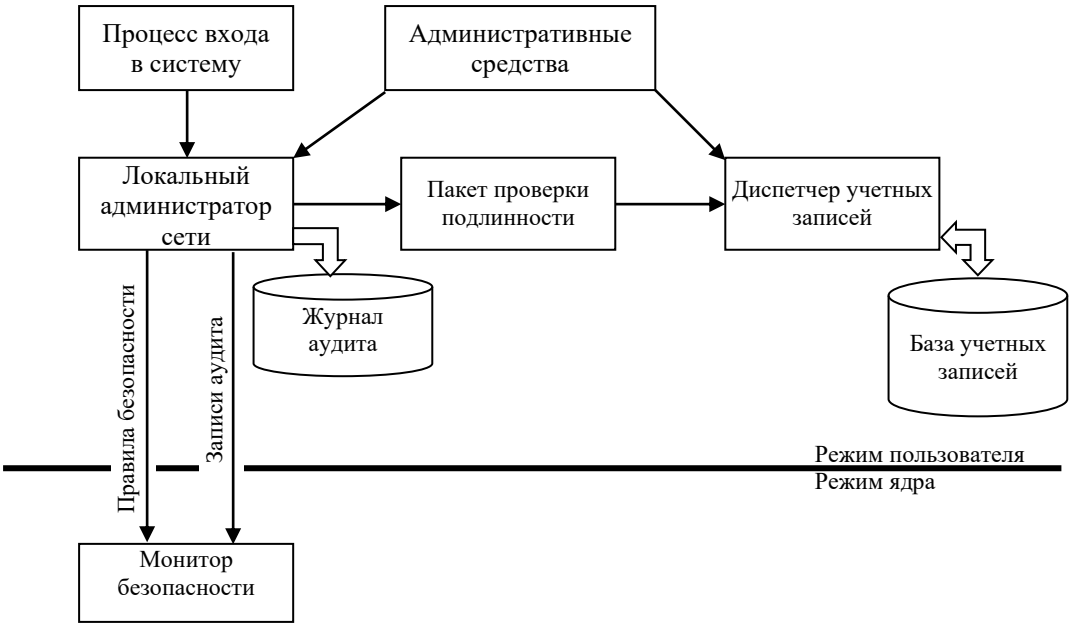

Рис 5.1

Процессы входа в систему обрабатывают запросы пользователей о входе в систему. Сюда включается начальный интерактивный вход в систему через диалоговое окно входа пользователя и процессы удаленного входа, открывающие доступ к серверу Windows с удаленных компьютеров. Вход в систему обязателен для работы с сервером или рабочей станцией Windows 2000/2003.

Центральная часть системы безопасности Windows — Локальный администратор безопасности (Local Security Authority, LSA) - проверяет, наличие у пользователя необходимых полномочий для входа в систему. Этот компонент создает маркеры доступа, управляет локальными правилами безопасности, обеспечивает службы интерактивной проверки подлинности, а также контролирует правила аудита и записывает в журнал аудита сообщения, полученные от Монитора безопасности.

Диспетчер учетных записей (Security Account Manager, SAM) поддерживает базу данных учетных записей. В ней хранятся все учетные записи пользователей и групп. Эта база является частью реестра операционной системы и недоступна обычным пользователям в ходе нормальной работы, обеспечивает службы подтверждения подлинности пользователя, используемые администратором локальной безопасности.

Монитор безопасности (Security Reference Monitor, SRM) проверяет, имеет ли пользователь достаточные права для доступа к объекту. Он работает в режиме ядра. Компоненты ядра и пользовательские процессы обращаются к Монитору безопасности, чтобы выяснить, имеют ли право пользователи и процессы получить доступ к объекту. SRM хранит в себе весь код, ответственный за подтверждение доступа, и это единственная копия данного кода для любой системы Windows. Благодаря этому все проверки выполняются одинаково для всех объектов в системе.

Журнал аудита (Security log) содержит записи о событиях, связанных с работой системы безопасности. Сюда заноситься информация о входах пользователей, изменениях в базе учетных записи и системной политике, событиях доступа пользователей к секретам файлам.

Пакет проверки подлинности (Authentication package) проверяет подлинность пользователя. Windows по умолчанию использует текст проверки подлинности MSV1_0, но эта операционная система может поддерживать несколько таких пакетов, выполненных как динамические библиотеки DLL. Таким образом независимые поставщики программного обеспечения могут включать в Windows свои модули проверки подлинности.

5.2. Пользовательские бюджеты

Модель безопасности Windows основывается на пользовательских учетных записях или бюджетах (user accounts). Администратор может создать любое количество пользовательских бюджетов и сгруппировать их удобным образом. С каждым пользовательским бюджетом связан уникальный идентификатор безопасности (security ID или SID). Пользовательские бюджеты и связанные с ними SID хранятся в базе данных пользовательских бюджетов. Существование двух одинаковых SID исключено. При удалении пользовательского бюджета удаляется также и его SID, поэтому даже при создании пользователя с таким же именем, его новый SID будет отличен от прежнего.

Прежде чем пользователь сможет что-либо сделать в системе, он должен зарегистрироваться.

При регистрации в системе, Windows создает маркер безопасного доступа (Security Access Token). В его состав входят SID пользователя, SID всех групп, к которым пользователь принадлежит и права пользователя.

Когда пользователь пытается получить доступ к объекту, Windows сравнивает информацию, содержащуюся в маркере безопасного доступа со списком контроля доступа к объекту.

Программы, запускаемые пользователем, не должны получать к объектам больших прав доступа, чем имеет сам пользователь. Для отслеживания и управления правами доступа для программ Windows использует субъекты. Субъект - это комбинация маркера безопасного доступа пользователя и программы, действующей от лица пользователя. В архитектуре безопасности Windows существует два класса субъектов:

– Простой субъект (security context) - это процесс, который получил контекст безопасности при регистрации в системе соответствующего пользователя.

– Субъект - сервер (server context) - это процесс, реализованный в качестве защищенного сервера (примером может являться подсистема Win32). Субъект-сервер может иметь в качестве клиентов другие субъекты.

Права пользователя (User Rights) - это правила, определяющие действия пользователя, которые он может произвести.

5.3. Объекты доступа

Атрибуты безопасности, присвоенные объекту, описываются дескриптором безопасности, содержащим следующую информацию:

•Идентификатор безопасности владельца (owner SID), указывающий

пользователя или группу, которые являются владельцами объекта. Владелец объекта может изменять право доступа к объекту.

•Групповой идентификатор безопасности (group SID), используемый только подсистемой POSIX. Все остальные подсистемы Windows его игнорируют.

•Избирательный список контроля доступа (discretionary access control list, ACL), идентифицирующий, какие пользователи и группы имеют (или не имеют) по отношению к объекту права доступа (и какие). Избирательными ACL управляет владелец объекта.

•Системный список контроля доступа ACL, управляющий генерацией системных событий аудита. Системными ACL управляют администраторы безопасности.

Список контроля доступа состоит из элементов контроля доступа (Access Control Elements). Существуют три типа ACE:

•AccessAllowed - предоставляет доступ к объекту

•AccessDenied - отклоняет доступ к объекту

•SystemAudit - используется для ведения протокола событий

Когда пользователь пытается получить доступ к объекту, Windows сравнивает информацию безопасности, содержащуюся в маркере безопасного доступа пользователя, с информацией безопасности, в дескрипторе безопасности объекта.

На основании типа доступа, который пытается получить пользователь, для субъекта создается маска запрашиваемого доступа (desired access mask), которая обычно создается программой, с которой работает пользователь, сравнивается со списком контроля доступа к объекту.

Получение доступа к объекту

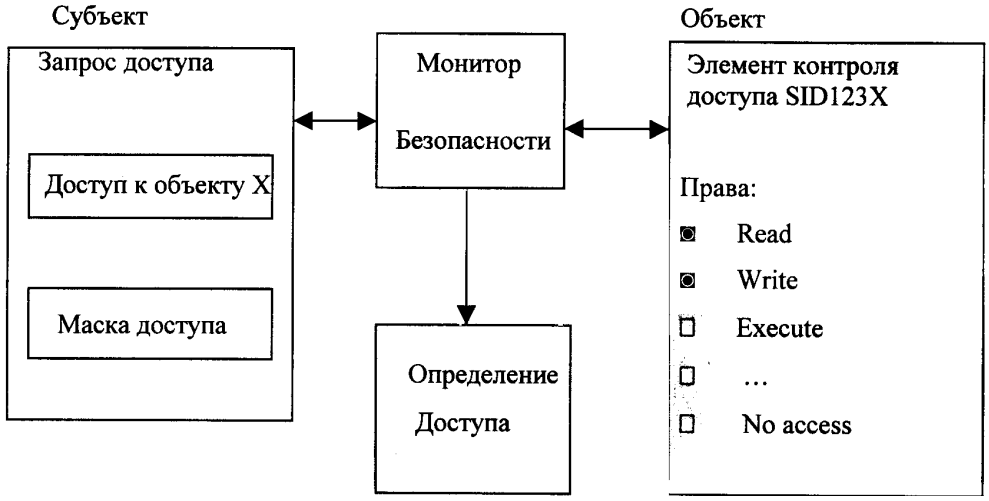

Рис.5.2

5.4. Пользовательские пароли

Учетные записи пользователей хранятся в базе данных учетных записей. В ней для каждого пользователя хранится SID, пользовательское имя, пароль в зашифрованном виде; информация о членстве в группах, общесистемные права, которыми наделен данный пользователь, текстовый комментарий и прочая информация.

База данных учетных записей находится в ключе реестра HKEY_LOCAL_MACHINE\SAM. Этот ключ связан с ключом

HKEY_LOCAL_MACHINE\SECURITY\SAM, так что изменения, внесенные в один ключ, автоматически дублируются в другом. Физически база данных SAM хранится в файле <SYSTEMROOT>\system32\config\sam. Во время работы системы этот файл заблокирован и недоступен. Копия файлов системного реестра обычно может храниться в каталоге <SYSTEMROOT>\repair и на диске аварийного восстановления.

Пароли (точнее, хэш-функция пароля) хранятся в реестре в двух форматах:

- LAN Manager compatible password hash;
- Windows password hash.

LAN Manager Compatible password используется для совместимости с предыдущими версиями операционных систем Microsoft и является менее стойким, чем Windows NT password hash.

LAN Manager compatible password hash получается из пароля, введенного пользователем, следующим образом:

1. Пароль пользователя переводится в верхний регистр;
2. Если пароль составляет меньше 14 символов, он дополняется нулевыми байтами;
3. Полученная 14-сивольная последовательность разбивается посередине на две 7-байтные последовательности;
4. Каждая из полученных 7-байтных последовательностей преобразуется по известному алгоритму для получения 8-байтных DES-ключей с нечетной четностью;
5. Постоянное "магическое" число шифруется при помощи полученных 8-байтных ключей и результаты конвертируются;
6. Полученное 16-байтное значение записывается в реестр.

Windows password hash получается следующим образом:

1. Пароль пользователя конвертируется в Unicode;
2. Полученная строка шифруется по алгоритму md4 для получения 16-байтного значения, которое и хранится в реестре.

Таким образом, Windows позволяет использовать в пароле буквы русского алфавита.

5.5. Windows в сети

Windows использует протокол SMB (Server Message Block - блок серверных сообщений), который определяет алгоритмы функционирования файловой службы в сетевой среде. Во время сеанса SMB по сети должны передаваться пакеты, содержащие информацию конфиденциального характера. Кроме того эти пакеты обычно включают в себя зашифрованные данные протокола NTLM, передаваемые во время фазы аутентификации.

Взломщики, используя существующие сетевые анализаторы, могут легко перехватывать данные, передаваемые по сети. Задача перехвата нужных пакетов и получения из них информации о паролях легко решается с помощью продукта SMB Packet Capture.

Для защиты от подобных атак нужно использовать протокол NTLMv2, либо применять механизм создания виртуальных частных сетей (VPN - Virtual Private Network) типа Microsoft PPTP. Протокол NTLMv2 позволяет защитить данные, передаваемые по внутренней локальной сети, а PPTP обеспечивает защиту информации, передаваемой через такие сети, как, например, Internet.

При отсутствии механизма VPN и технологии подписей SMB взломщик может использовать сеанс SMB для получения несанкционированного доступа в систему. При использовании подписей пакетов SMB операционная система проверяет подлинность каждого пакета, прежде чем принять его к исполнению.

5.6. Проблемы безопасности

1. Пароли

Доступ с правами администратора — наиболее опасная атака уровня ОС, поэтому именно защита административных полномочий должна в первую очередь решаться. Однако, доступ с правами обычного пользователя также может многое дать злоумышленнику. Поэтому защищённость операционной системы во многом определяется политикой в отношении пользовательских паролей.

Алгоритм DES, так же как и алгоритм MD4, является односторонней функцией, которая не позволяет по зашифрованному тексту получить открытый текст. В то же время, существует подход, позволяющий при наличии зашифрованного пароля, в некоторых случаях получить его открытый текст перебором за определенный промежуток времени.

Алгоритм, используемый Windows для получения LAN Manager password hash, предлагает несколько подходов к значительному сокращению перебора. Во-первых, так как пароли конвертируются в верхний регистр, это значительно сокращает пространство возможных паролей. Во-вторых, так как пароль разделяется на две 7-байтные части, каждая из которых шифруется отдельно, нет необходимости перебирать N в 14 степени комбинаций, а достаточно 2 раза по N в 7 степени. В частности, можно сразу же выделить пароли длиной до 7 символов, так как вторая половина LAN Manager password hash для них представляет собой известное постоянное значение. Существуют общедоступные утилиты для взлома паролей, реализующие эти методы.

Для предотвращения такой атаки можно использовать программу syskey. Эта программа позволяет наложить на базу данных учетных записей дополнительный уровень шифрования, с ключом, в скрытом виде, хранящемся в системе, на диске, или получаемом из пароля, заданного администратором. Эта методика позволяет значительно повысить защищенность базы данных учетных записей.

2. Права пользователей

Построение защищённой системы предполагает правильную настройку прав пользователей и список контроля доступа объектов. Это, главным образом:

- Права пользователей по отношению к службам
- Допуски к папкам и файлам
- Допуски к ключам реестра

3. Службы

Многие системные службы, например планировщик задач или сервер баз данных, предоставляют в распоряжение пользователей механизмы запуска команд, исполнять которые будет сама служба. Некоторые планировщики умеют выполнять команды от имени учетной записи пользователя, иначе команда выполняется с привилегиями учетной записи самой службы. Например, в состав Microsoft SQL Server входит собственный планировщик задач и SQL-команд, что дает

пользователям SQL Server возможность выполнять команды операционной системы. В этом случае существует два способа защиты. Во-первых, можно ограничить права пользователей на выполнение команд настройкой самой службы. Большинство служб, таких, как SQL Server и Microsoft Exchange Server, снабжены механизмами аутентификации и контроля доступа. Необходимо убедиться, что такие механизмы корректно сконфигурированы, и следить за их настройкой. Во-вторых, часто подобные службы запускаются от имени системной учетной записи Local System Account, которая мощнее, учетной записи администратора. Чтобы этого избежать, нужно создать отдельную учетную запись для службы и предоставить ей только те права и разрешения, которые необходимы для работы. В результате если кто-то получит возможность работать с данной службой, у него будут лишь те права доступа к системе, которые предоставлены учетной записи службы.

Такой подход особенно важен системной службе планировщика Scheduler. По умолчанию эта служба работает от имени системной учетной записи. Если это не имеет значения, ее можно запускать от имени непривилегированного пользователя.

4. Допуски к папкам и файлам

Файловая система NTFS позволяет настроить доступ пользователей к папкам и файлам компьютера.

Например, файлы операционной системы в каталоге \%systemroot% (чаще всего C:\Winnt) с назначенными по умолчанию разрешениями уязвимы для несанкционированных изменений. Непривилегированные пользователи могут заменить критически важные файлы операционной системы своими версиями, которые система будет исполнять в привилегированном режиме.

5. Доступ к ключам реестра

Windows позволяет настраивать допуски к отдельным ключам реестра. Например, с помощью раздела реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServer\winreg можно указать, кто имеет право удаленного доступа к реестру (независимо от разрешений для конкретных разделов).

6. Ошибки кода ОС

Предусмотрено четкое разделение прикладных и системных процессов, что предохраняет систему от приложений, которые пытаются найти лазейки в системе безопасности. Имеется два режима работы программ. Приложения работают в пользовательском режиме, при котором запрещен доступ к произвольным областям памяти, аппаратуре и другим процессам. Операционная система работает в режиме ядра, и система ограничений здесь значительно слабее. Разделение режимов, в сочетании с другими характеристиками Windows, должно выполнять защиту, но некоторые ошибки программного кода операционной системы дают возможность ее нарушить. Например, такие программы, как getadmin и sechole, могут предоставить непривилегированным пользователям полномочия администратора в любой системе, где есть возможность эти программы запустить. Другая ошибка в программном коде ОС приводит к тому, что пользователи могут повысить привилегии своей учетной записи путем запуска специальной программы-заставки.

5.7. Установка ключей реестра

Защищённость системы зависит от правильной установки некоторых ключей реестра.

Например, по умолчанию файл подкачки «Pagefile.sys» не уничтожается при перезагрузке и его содержимое может быть прочитано любым пользователем.

Для устранения уязвимости необходимо отрегулировать следующий ключ реестра

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\SessionManagerMVIemory Management
Name: ClearPageFileAtShutdown
Type: REG_DWORD
Value: 1

Одним из способов установки троянского коня может быть режим автозапуска компакт-дисков. Для отключения необходимо отредактировать реестр.

Hive:HKEY_CURRENT_USER
Key:Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Name :NoDriveTypeAutorun Value: 181 (Decimal)

5.7.1. Проблемы сетевых соединений

Null - Session. Позволяет подключиться к узлу с пустым именем и паролем и получить информацию об общих ресурсах. Для устранения уязвимости необходимо отредактировать реестр следующим образом:

Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Control\Lsa
Name: RestrictAnonymous
Type: REG_DWORD
Value:1
или
Вариант для Windows NT Workstation: AutoShareServer
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\LanmanServer\Parameters
Name: AutoShareWks
Type : DWORD and press OK.
Value: 0.
или
Вариант для Windows NT Server :
Hive: HKEY_LOCAL_MACHINE
Key: System\CurrentControlSet\Services\LanmanServer\Parameters
Name: AutoShareServer
Type : DWORD and press OK.
Value: 0.

5.8. Настройка системы безопасности

Исходя из источников уязвимостей Windows настройка системы безопасности состоит из следующих моментов:

- политика по отношению к паролям;
- установка прав пользователей;

•установка исправлений;

•установка допусков к объектам (папкам, файлам, ключам реестра); настройка реестра (добавление, установка нужных ключей).

Система анализа защищенности System Scanner (S4) используется для анализа защищенности операционных систем.

6. БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

6.1. Средства защиты информации в базах данных

Системы управления базами данных (СУБД) являются важной составляющей любой корпоративной сети. Выбор конкретной модели СУБД для использования в сети компании определяется многими факторами. Каждая СУБД имеет свои особенности, позволяющие сделать выводы о целесообразности её применения.

В настоящее время наиболее распространёнными СУБД можно назвать:

- Oracle
- Microsoft SQL Server
- Sybase

В целом механизмы обеспечения безопасности, используемые в базах данных, делятся на две группы: базовые механизмы и средства обеспечения сетевой безопасности. Базовые средства предназначены для защиты ресурсов и объектов баз данных. Наличие таких средств обязательно для распределенных систем коллективного доступа, и в той или иной мере они реализованы в любой многопользовательской ОС или СУБД. Сетевые средства служат для защиты систем связи и устранения характерных угроз, возникающих в сетевых средах.

В распределенной информационной среде обязательным является наличие компонентов борьбы с потенциальными угрозами:

- идентификация и проверка подлинности (аутентификация) пользователей (применяются либо соответствующие механизмы ОС, либо SQL-оператор CONNECT);

- управление доступом к данным, когда владелец объекта передает права доступа к нему (привилегии доступа) по своему усмотрению;

- механизм учета всех действий, влияющих на безопасность;

- защита регистрационной информации от искажений.

Основным средством взаимодействия с реляционными СУБД является язык SQL (Structured Query Language) — непроцедурный инструмент определения и манипулирования данными. В самом стандарте SQL уже определены некоторые механизмы обеспечения безопасности. Так, в соответствии с идеологией языка SQL права доступа пользователя к таблицам баз данных контролируются на основе механизма привилегий. То есть для выполнения любого действия над таблицей пользователь должен обладать соответствующей привилегией (реально все возможные действия описываются фиксированным стандартным набором привилегий). Пользователь, создавший таблицу, автоматически становится владельцем всех возможных привилегий на выполнение операций над этой таблицей. В число этих привилегий входит привилегия на передачу всех или некоторых привилегий по отношению к данной таблице другому пользователю, включая привилегию на передачу привилегий.

В стандарте SQL/89 определяется упрощенная схема механизма привилегий. Во-первых, назначение привилегий возможно только при определении таблицы. Во-вторых, пользователь, получивший некоторые привилегии от других, может передать их дальше только при определении схемы.

В стандарте SQL/92 появилась возможность создавать хранимые и представляемые таблицы и задавать или удалять привилегии доступа в любой момент времени, в любой транзакции вне оператора определения схемы. Появились операторы уничтожения таблиц, которые также можно выполнять внутри любой транзакции.

В добавление к возможностям SQL/89 определения ограничений целостности на уровне столбца и(или) таблицы в SQL/92 допустимо отдельное определение ограничений, распространяющееся в общем случае на несколько таблиц. Появилась возможность определения отложенных (проверяемых при завершении транзакции) ограничений целостности. Расширены возможности определения ограничений внешнего ключа (ограничений ссылочной целостности). Введены средства определения, изменения и отмены определения домена (возможно множество значений некоторого типа данных).

6.2. Режимы проверки прав пользователя

В версии 7.0 поддерживается два механизма проверки прав пользователя:

- Стандартный (Standart Security) - права определяются на основании идентификатора и пароля, передаваемых непосредственно SQL Server
- Интегрированный (Integrated Security) - проверка выполняется средствами Windows.

Контроль прав доступа подразумевает проверку того, что может делать пользователь, получив доступ к серверу. При этом SQL Server использует информацию из нескольких системных таблиц (рис. 6.1).

Связь таблиц, используемых при проверке прав доступа

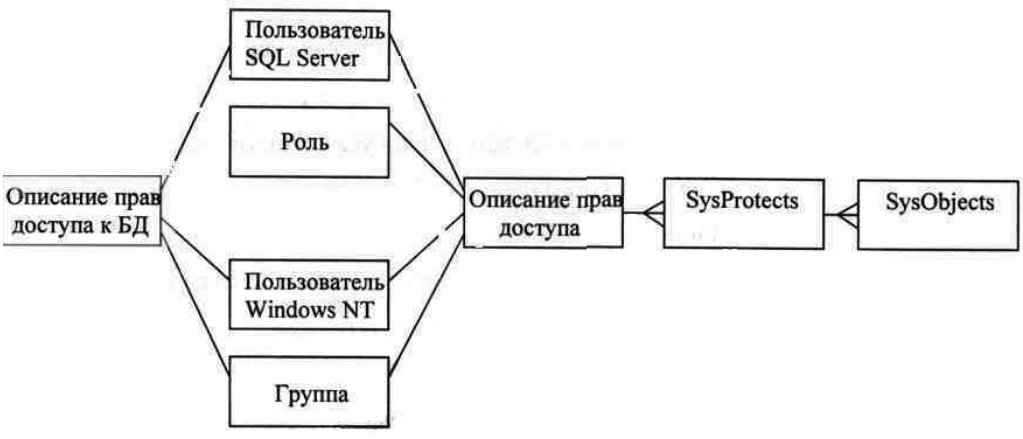

Рис. 6.1

Пользователь, получивший доступ к серверу, автоматически подключается к базе данных (БД), назначенной ему по умолчанию. В рамках этой БД пользователь получает некоторый набор прав (по умолчанию пользователь обладает правами, определенными для роли public).

В таблице SysUsers хранятся два элемента: один описывает права доступа к БД, другой — к объектам БД.

При подключении под именем пользователя Windows серверу передается имя группы, к которой принадлежит пользователь и имя его учетной записи. Сервер ищет в таблице Syslogins запись с упоминанием учетной записи пользователя или группы, к которой он принадлежит. Если она найдена, пользователь получает доступ к серверу. Такая система проверки доступа обеспечивает большую надежность системы безопасности, чем проверка прав средствами SQL Server.

При проверке прав доступа собственными средствами SQL Server в таблице Sysligins ищется запись с упоминанием об идентификаторе, введенном пользователем. При обнаружении сравнивается введенный пароль с хранящимся в таблице. Если идентификатор найден и пароль соответствует записанному ранее, пользователь получает доступ к серверу.

6.3. Получение доступа к БД

Право на доступ к БД организуется установлением связи идентификатора пользователя (Login) и учётного имени (User account) в БД. Учётное имя может быть создано:

- На основании имени группы Windows
- На основании имени учетной записи в домене Windows
- На основании идентификатора пользователя SQL Server

А) Идентификатор пользователя. После установки SQL Server создаются два стандартных идентификатора:

- Sa - Сохранён для совместимости с приложениями, написанными под SQL Server версии 6.x. Имеет пустой пароль.
- BULTINXAdministrators - Служит для обеспечения доступа к серверу всем членам группы администраторов Windows.

Для создаваемой БД есть два учётных имени:

- Dbo - ставится в соответствие системному администратору. Удалить нельзя.
- Guest - служит для допуска пользователей, не имеющих учётного имени в БД

Учётное имя Guest не может быть удалено из БД Master и Tempdb.

Б) Роль - именованный набор прав на уровне сервера или БД. Роль может включать:

- пользователя Windows;
- группу Windows; пользователя SQL Server;
- другие роли.

Принадлежность к роли определяется после подключения пользователя к БД. Имеются роли уровня сервера (например, Sysadmin, Serveradmin и др.) и роли уровня БД (например, db_owner, db_datareader и др.).

Роль Public - стандартная роль уровня БД, ассоциируемая с набором прав по умолчанию для любого пользователя БД.

6.4. Доступ к объектам БД

Доступ к объектам БД регулируется путём установления разрешений (permissions). Имеется несколько типов разрешений.

Выполнение SQL выражений

Здесь необходимо выделить:

- разрешение на создание БД. Это право распространяется на сам оператор, а не на конкретную БД или её объект;
- разрешение на выполнение остальных SQL выражений. Может относиться к БД или её объектам.

Действия с объектами БД

Разрешения на действия с объектами определяют права пользователя при работе с данными или исполнении хранимых процедур:

- разрешения на работу с таблицами и просмотрами;
- разрешения на доступ к определённым полям;
- разрешения на исполнение хранимых процедур.

Предопределённые разрешения - это разрешения, которые получает пользователь в силу принадлежности к определённой роли и разрешения, которыми обладает владелец объекта.

7. ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ

Существует несколько особенностей в построении комплексной защиты, которая основывается на модели адаптивного управления безопасностью и строится в несколько этапов:

1. Разработка политики безопасности.
2. Установка и настройка технических средств.
3. Обучение сотрудников.
4. Периодический аудит.
5. Информационное обеспечение.

Использование модели адаптивной безопасности сети позволяет контролировать практически все угрозы, и своевременно реагировать на них высокоэффективным способом, позволяющим не только устранить уязвимости, которые могут привести к реализации угрозы, но и проанализировать условия, приводящие к появлению уязвимостей. Эта модель также позволяет уменьшить злоупотребления в сети, повысить осведомленность пользователей, администраторов и руководство компании о событиях безопасности в сети.

Современная система защиты информации состоит из традиционных средств защиты, а так же средств для обнаружения уязвимостей и атак.

7.1. Традиционные средства защиты корпоративной сети

1. Межсетевые экраны (МСЭ)

- разграничение доступа внешних пользователей к внутренним корпоративным ресурсам;
- контроль доступа сотрудников к ресурсам сети Internet;
- разграничение доступа между внутренними сегментами корпоративной сети;

Недостатки МСЭ:

- не защищает от авторизованных пользователей;
- не гарантирует 100%-ой защиты от атак;
- не может защитить трафик, не проходящий через него;

- не обеспечивает полной защиты от «мобильного кода» (Java, ActiveX и т.п.);
- не защищает от неправильной конфигурации.

2. Использование контроля доступа
3. Использование аутентификации
4. Использование криптографической защиты

Таким образом, традиционные средства защиты:

- предотвращают, а не упреждают;
- не защищают от внутренних угроз;
- не позволяют оценивать свою эффективность;
- являются статическими, не учитывающему динамику изменений сетевого окружения.

Средства для обнаружения уязвимостей и атак:

1. Средства для анализа защищенности:
   - на уровне сети (Internet Scanner);
   - на уровне операционной системы (System Scanner);
   - на уровне приложений (Database Scanner).
2. Средства для обнаружения атак:
   - на сетевом уровне - Network-based (RealSecure, защищает целый сегмент сети);
   - на уровне операционной системы – Host-based (RealSecure, защищает конкретный узел сети).

7.2. Комплексная система защиты информации

Комплексная система защиты информации включает в себя:

- межсетевые экраны;
- системы обнаружения атак;
- системы анализа защищенности.

Семейство SAFEsuite на сегодняшний день является первым и пока единственным комплексом систем, который включает в себя все компоненты модели адаптивного управления безопасностью сети. Первоначально данное семейство состояло всего из трех систем:

- системы анализа защищенности на уровне сети Internet Scanner;
- системы анализа защищенности на уровне операционной системы System Scanner;
- системы обнаружения атак на уровне сети RealSecure Network Engine.

Затем появились:

- система анализа защищенности на уровне систем управления базами данных (СУБД Database Scanner);
- система обнаружения атак на уровне операционной системы RealSecure System Agent.

Таким образом, если необходимо:

- иметь гарантии, что практически все имеющиеся и вновь появляющиеся в сети уязвимости будут найдены;
- иметь гарантии, что все системы сконфигурированы непротиворечащим политике безопасности компании образом;

- иметь гарантии, что почти все потенциально враждебные уязвимости и атаки обнаруживаются вовремя и им своевременно противопоставляются соответствующие средства защиты;
- обеспечить в реальном времени, не останавливая функционирование сети, реконфигурацию программного и аппаратного обеспечения сети в случае возникновения угрозы;
- обеспечить своевременное уведомление ответственных за сетевую безопасность о возникающих проблемах;
- обеспечить анализ тенденций для более эффективного планирования защиты сети.

то решение этих проблем достигается за счет применения модели адаптивного управления безопасностью.

8. МЕТОДИКА МЭ, РЕАЛИЗУЕМАЯ НА БАЗЕ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ

8.2. Понятие межсетевого экрана

Ряд задач по отражению наиболее вероятных угроз для внутренних сетей способны решать межсетевые экраны (брандмауэры, firewalls).

Для противодействия несанкционированному межсетевому доступу МЭ должен располагаться между защищаемой сетью, являющейся внутренней, и потенциально враждебной внешней сетью (рис. 8.1.). Организационно экран входит в состав защищаемой сети.

Межсетевой экран — это программная или программно-аппаратная система межсетевой защиты, позволяющая разделить две (или более) взаимодействующие сети и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной сети в другую. Межсетевой экран пропускает через себя весь трафик, принимая для каждого проходящего пакета решение — пропускать его или отбросить. Для того чтобы МЭ мог выполнить это, ему необходимо определить набор правил фильтрации.

Схема подключения межсетевого экрана как средства разграничения доступа

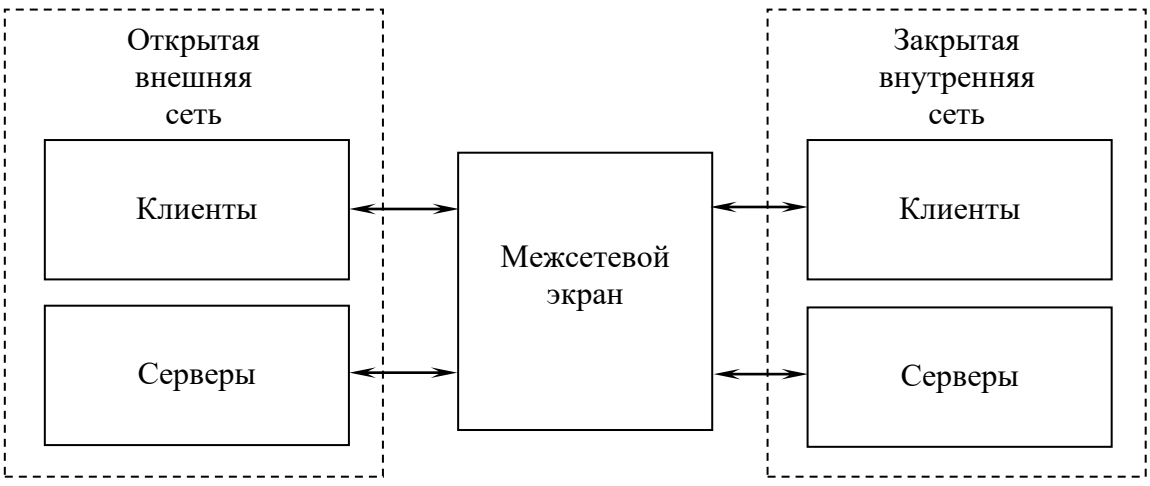

Рис 8.1.

Схемы установления межсетевого экрана при защите корпоративной сети: а) схема единой защиты; б) схема виртуальной корпоративной сети

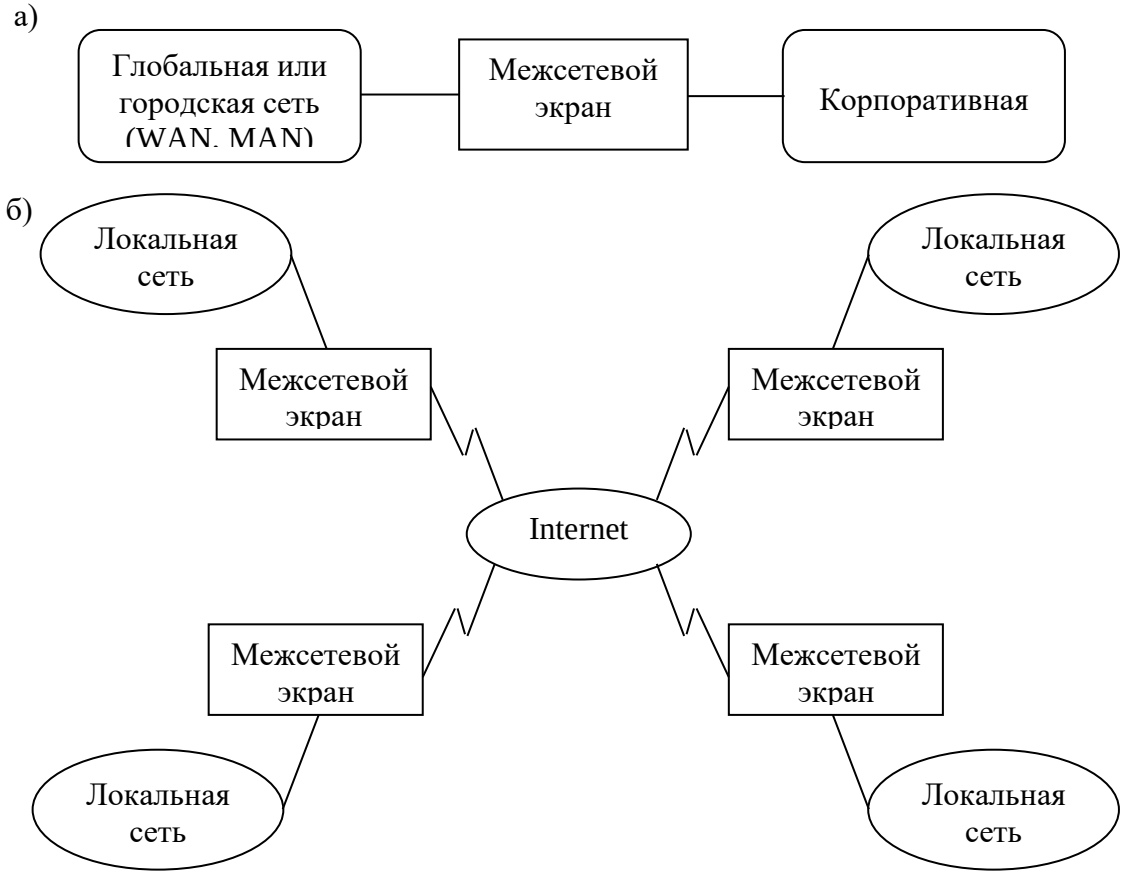

Рис. 8.2.

Правила фильтрации — перечень условий, по которым с использованием заданных критериев разрешается или запрещается дальнейшая передача пакетов (данных), и перечень действий МЭ по регистрации и (или) выполнению дополнительных защитных функций.

Межсетевые экраны позволяют организовать защищенные виртуальные сети. Несколько локальных сетей, подключенных к глобальной сети, объединяются в одну виртуальную корпоративную сеть с применением межсетевых экранов.

Функционирование МЭ основывается на выборе политики сетевой безопасности, формулировке функциональных требований к межсетевым экранам, настройке набора составляющих его компонентов.

Решение о том, фильтровать ли с использованием межсетевого экрана конкретные протоколы и адреса, зависит от принятой в защищаемой сети политики безопасности. Межсетевой экран является набором компонентов, настраиваемых таким образом, чтобы реализовать выбранную политику безопасности.

В рамках данной политики безопасности должны быть заданы все сервисы, предоставляемые через сетевой экран, а также допустимые адреса клиентов для каждого сервиса; должны быть указаны правила для пользователей, описывающие, когда и какие пользователи каким сервисом и на ком компьютере могут воспользоваться. Отдельно определяются правила аутентификации пользователей и компьютеров.

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

В первом случае межсетевой экран должен быть сконфигурирован так, чтобы блокировать любые явно не разрешенные межсетевые взаимодействия. С точки зрения безопасности МЭ является лучшим.

При выборе второго принципа межсетевой экран настраивается таким образом, чтобы блокировать только явно запрещенные межсетевые взаимодействия. В этом случае повышается удобство использования сетевых сервисов со стороны пользователей, но снижается безопасность межсетевого взаимодействия.

Функциональные требования к межсетевым экранам включают в себя: требования к фильтрации на сетевом, сеансовом и прикладном уровнях модели OSI; требования по настройке правил фильтрации и администрированию; требования к средствам сетевой аутентификации; требования по внедрению журналов и учету и др.

В общем случае работа межсетевого экрана основана на динамическом выполнении двух групп функций: фильтрации проходящих через него данных; 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.

Полнота и правильность управления требуют, чтобы МЭ имел возможность анализа и использования: информации о соединениях — информации от всех уровней в пакете; истории соединений — информации, полученной от предыдущих соединений состояния уровня приложения — информации о состоянии, полученной из других приложений; агрегирующих элементов — вычислений разнообразных выражений, основанных на использовании всех вышеперечисленных элементов.

8.2. Фильтрация трафика

Фильтрация информационных потоков состоит в их выборочном пропускании через экран, возможно, с выполнением некоторых преобразований. Фильтрация осуществляется на основе набора правил, предварительно загруженных в экран и являющихся выражением сетевых аспектов принятой политики безопасности. Поэтому межсетевой экран удобно представляет как последовательность фильтров, обрабатывающих информационный поток. Каждый из фильтров предназначен для выполнения отдельных правил фильтрации:

- анализ информации по заданным критериям, например, по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена;

- принятие на основе правил одного из следующих решений: не пропустить данные; обработать данные от имени получателя и возвратить результат отправителю; передать данные на следующий фильтр для продолжения анализа; пропустить данные, игнорируя следующие фильтры.

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например преобразование данных, регистрация событий и др. Соответственно правила фильтрации определяют перечень условий, по которым с использованием указанных критериев анализа

разрешается или запрещается дальнейшая передача данных; выполняются дополнительные защитные функции.

В качестве критериев анализа информационного потока могут использоваться следующие параметры: служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные; непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов; внешние характеристики потока информации, например временные, частотные характеристики, объем данных и т.д. Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. В общем случае, чем выше уровень модели OSI, на котором МЭ фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

8.3 Политика межсетевого взаимодействия,

Политика межсетевого взаимодействия является частью политики безопасности в организации, и определяет требования к безопасности информационного обмена с внешним миром. Данные требования обязательно должны отражать два аспекта:

Политика доступа к сетевым сервисам определяет правила предоставления, а также использования всех возможных сервисов защищаемой системы. Соответственно в рамках данной политики должны быть заданы все сервисы, предоставляемые через сетевой экран, и допустимые адреса клиентов для каждого сервиса. Кроме того, должны быть указаны правила для пользователей, описывающие, когда и какие пользователи каким сервисом и на каком компьютере могут воспользоваться. Отдельно определяются правила аутентификации пользователей и компьютеров, а также условия работы пользователей вне вычислительной сети организации.

Политика работы межсетевого экрана задает базовый принцип управления межсетевым взаимодействием, положенный в основу функционирования МЭ.

8.4. Определение схемы подключения межсетевого экрана

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

МЭ с одним сетевым интерфейсом (рис. 8.3) не достаточно эффективны как с точки зрения безопасности, так и с позиций удобства конфигурирования. Они физически не разграничивают внутреннюю и внешнюю сети, а соответственно не могут обеспечивать надежную защиту межсетевых взаимодействий. Настройка таких межсетевых экранов, а также связанных с ними маршрутизаторов является сложной задачей, цена решения которой превышает стоимость замены МЭ с одним сетевым интерфейсом на МЭ с двумя или тремя сетевыми интерфейсами.

В схемах подключения межсетевых экранов с двумя и тремя сетевыми интерфейсами. Защищаемая локальная сеть рассматривается как совокупность закрытой и открытой подсетей. Открытая подсеть – подсеть, доступ к которой со стороны потенциально враждебной внешней сети может быть полностью или частично открыт. В открытую подсеть могут, например, входить общедоступные WWW-, FTP- и SMTP-серверы, а также терминальный сервер с модемным пулом.

Защита локальной сети МЭ с одним сетевым интерфейсом

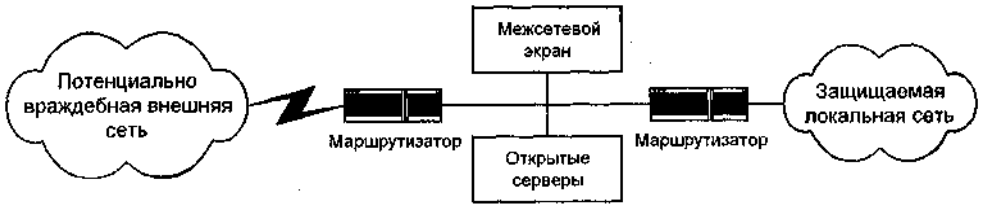

Рис. 8.3.

Среди всего множества возможных схем подключения МЭ типовыми являются:

- схема единой защиты локальной сети;
- схема с защищаемой закрытой и не защищаемой открытой подсетями;
- схема с раздельной защитой закрытой и открытой подсетей.

Схема единой защиты локальной сети является наиболее простым решением (рис. 8.4.), при котором МЭ целиком экранирует локальную сеть от потенциально враждебной внешней сети. Между маршрутизатором и МЭ имеется только один путь, по которому идет весь трафик. Обычно маршрутизатор настраивается таким образом, что МЭ является единственной видимой снаружи машиной. Открытые серверы, входящие в локальную сеть, также будут защищены межсетевым экраном. Однако объединение серверов, доступных из внешней сети, вместе с другими ресурсами защищаемой локальной сети существенно снижает безопасность межсетевых взаимодействий. Поэтому данную схему подключения МЭ можно использовать лишь при отсутствии в локальной сети открытых серверов или когда имеющиеся открытые сервера делаются Доступными из внешней сети только для ограниченного числа пользователей, которым можно доверять.

Схема единой защиты локальной сети

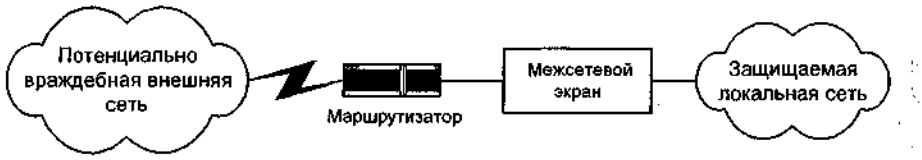

Рис. 8.4.

При наличии в составе локальной сети общедоступных открытых серверов их целесообразно вынести как открытую подсеть до межсетевого экрана. Данный способ обладает более высокой защищенностью закрытой части локальной сети, но обеспечивает пониженную безопасность открытых серверов, расположенных до межсетевого экрана. Некоторые МЭ позволяют разместить эти сервера на себе. Но такое решение не является лучшим с точки зрения загрузки компьютера и безопасности самого МЭ. Таким образом схему подключения МЭ с защищаемой закрытой подсетью и не защищаемой открытой подсетью целесообразно использовать лишь при невысоких требованиях по безопасности к открытой подсети.

В том случае, когда к безопасности открытых серверов предъявляются повышенные требования, необходимо использовать схему с раздельной защитой закрытой и открытой подсетей. Такая схема может быть построена на основе одного

МЭ с тремя сетевыми интерфейсами или на основе двух МЭ с двумя сетевыми интерфейсами. В обоих случаях доступ к открытой и закрытой подсетям локальной сети возможен только через межсетевой экран. При этом доступ к открытой подсети не позволяет осуществить доступ к закрытой подсети.

Из этих двух схем большую степень безопасности межсетевых взаимодействий обеспечивает схема с двумя МЭ, каждый из которых образует отдельный этап защиты закрытой подсети. Защищаемая открытая подсеть здесь выступает в качестве экранирующей подсети. Обычно экранирующая подсеть конфигурируется таким образом, чтобы обеспечить доступ к компьютерам подсети как из внешней сети, так и из закрытой подсети локальной сети. Прямой обмен пакетами между внешней сетью и закрытой подсетью невозможен. При атаке системы с экранирующей подсетью необходимо преодолеть, по крайней мере, две независимые линии защиты, что является весьма сложной задачей. Средства мониторинга состояния межсетевых экранов практически неизбежно обнаружат подобную попытку, и администратор системы своевременно предпримет необходимые действия по предотвращению несанкционированного доступа.

Работа удаленных пользователей, подключаемых через коммутируемые линии связи, также должна контролироваться в соответствии с политикой безопасности, проводимой в организации. Типовое решение этой задачи — установка сервера удаленного доступа (терминального сервера), который обладает необходимыми функциональными возможностями. Терминальный сервер является системой с несколькими асинхронными портами и одним интерфейсом локальной сети. Обмен информацией между асинхронными портами и локальной сетью осуществляется только после соответствующей аутентификации внешнего пользователя.

Подключение терминального сервера должно осуществляться таким образом, чтобы его работа выполнялась исключительно через межсетевой экран. Такое подключение возможно, если терминальный сервер включить в состав открытой подсети при использовании схем подключения МЭ с раздельной защитой открытой и закрытой подсетей.

8.5 Операционная система МЭ

Программно-аппаратный МЭ – это совокупность функционирующих на нем операционной системы (ОС) и специального программного обеспечения. Специальное программное обеспечение часто также называют брандмауэром.

Операционная система МЭ также должна удовлетворять ряду требований:

- иметь средства разграничения доступа к ресурсам системы;
- блокировать доступ к компьютерным ресурсам в обход предоставляемого программного интерфейса;
- запрещать привилегированный доступ к своим ресурсам из локальной сети;
- содержать средства мониторинга/аудита любых административных действий.

8.6. Общие требования к МЭ

Функциональные — решение требуемой совокупности задач защиты: требования к фильтрации на сетевом уровне; требования к фильтрации на прикладном уровне; требования по настройке правил фильтрации и администрированию; требования к сетевой аутентификации; требования по внедрению журналов и учету.

Требования по надежности — способность своевременно, правильно и корректно выполнять все предусмотренные функции защиты;

Требования по адаптируемости — способность к целенаправленной адаптации при изменении структуры, технологических схем и условий функционирования МЭ;

Эргономические — требования по удобству администрирования, эксплуатации и минимизации помех пользователям;

Экономические — минимизация финансовых и ресурсных затрат.

Межсетевые экраны должны удовлетворять следующим группам более детальных требований.

По целевым качествам — обеспечивать безопасность защищаемой внутренней сети и полный контроль над внешними подключениями и сеансами связи. Межсетевой экран должен иметь средства авторизации доступа пользователей через внешние подключения. Типичной является ситуация, когда часть персонала организации должна выезжать, например, в командировки, и в процессе работы им требуется доступ к некоторым ресурсам сети организации. МЭ должен надежно распознавать таких пользователей и предоставлять им необходимые виды доступа.

По управляемости и гибкости — обладать мощными и гибкими средствами управления для полного воплощения в жизнь политики безопасности организации. МЭ должен обеспечивать простую реконфигурацию системы при изменении структуры сети. Если у организации имеется несколько внешних подключений, в том числе и в удаленных филиалах, система управления экранами должна иметь возможность централизованно обеспечивать для них проведение единой политики межсетевых взаимодействий.

По производительности и прозрачности — работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик при максимальной нагрузке. Это необходимо для того, чтобы МЭ нельзя было перегрузить большим количеством вызовов, которые привели бы к нарушению его работы. Система безопасности должна работать незаметно для пользователей сети и не затруднять выполнение легальных действий.

По самозащищенности — обладать свойством самозащиты от любых несанкционированных воздействий. Поскольку межсетевой экран является и ключом и дверью к конфиденциальным данным в организации, он должен блокировать любые попытки несанкционированного изменения его параметров настройки, а также включать развитые средства самоконтроля состояния и сигнализации. Средства сигнализации должны обеспечивать своевременное уведомление службы безопасности при обнаружении любых несанкционированных действий, а также нарушении работоспособности системы безопасности.

8.7. Особенности межсетевого экранирования на различных уровнях OSI

МЭ поддерживают безопасность межсетевого взаимодействия на различных уровнях модели OSI. При этом функции защиты, выполняемые на разных уровнях, отличаются друг от друга. Поэтому комплексный межсетевой экран удобно представить в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI. Чаще всего экран функционирует на сетевом, сеансовом и прикладном уровнях модели. Соответственно различают МЭ: экранирующий маршрутизатор, экранирующий транспорт (шлюз сеансового уровня), а также экранирующий шлюз (шлюз прикладного уровня).

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

– Экранирующие (фильтрующие) маршрутизаторы;

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

- адрес отправителя;
- адрес получателя;
- тип пакета;
- флаг фрагментации пакета;
- номер порта источника;
- номер порта получателя.

Первые четыре параметра относятся к IP-заголовку пакета, а следующие – к TCP- или UDP-заголовку.

–шлюз сеансового уровня;

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

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

При контроле квитирования связи шлюз сеансового уровня следит за установлением виртуального соединения между рабочей станцией внутренней сети и компьютером внешней сети, определяя, является ли запрашиваемый сеанс связи допустимым. Такой контроль основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP. Однако если пакетный фильтр при анализе TCP-заголовков проверяет только номера портов источника и получателя, то экранирующий транспорт анализирует другие поля, относящиеся к процессу квотирования связи.

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

– шлюз прикладного уровня.

Прикладной шлюз, называемый также экранирующим шлюзом, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает наиболее надежную защиту межсетевых взаимодействий. Защитные функции прикладного шлюза, как и экранирующего транспорта, относятся к функциям посредничества. Однако прикладной шлюз, в отличие от шлюза сеансового уровня, может выполнять существен- но большее количество функций защиты, к которым относятся следующие:

- идентификация и аутентификация пользователей при попытке установления соединений через МЭ;
- проверка подлинности информации, передаваемой через шлюз;
- разграничение доступа к ресурсам внутренней и внешней сетей;
- фильтрация и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;
- регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов;
- кэширование данных, запрашиваемых из внешней сети.

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

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

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

9. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ РЕСУРСОВ АС

Построение системы обеспечения безопасности информации в вычислительных системах и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности информации в соответствии с действующим законодательством в области информации, информатизации и защиты информации, других нормативных актов по безопасности, утвержденных органами государственной власти в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.

2. Системность

Системный подход к защите информации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности в ВС.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

3. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами.

Одним из наиболее укрепленных рубежей призваны быть средства защиты, реализованные на уровне операционных систем (ОС) СВТ в силу того, что ОС - это та часть компьютерной системы, которая управляет использованием всех ее ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

4. Непрерывность защиты

Защита информации - не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на

всех этапах жизненного цикла АС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.

5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите АС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки АС в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

6. Преемственность и совершенствование

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования АС и ее системы защиты с учетом изменений в методах и средствах перехвата информации и воздействия на компоненты АС, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

7. Разделение функций

Принцип Разделения функций, требует, чтобы ни один сотрудник организации не имел полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Все такие операции должны быть разделены на части, и их выполнение должно быть поручено различным сотрудникам. Кроме того, необходимо предпринимать специальные меры по недопущения сговора и разграничению ответственности между этими сотрудниками.

8. Разумная достаточность (экономическая целесообразность, сопоставимость возможного ущерба и затрат)

Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы АС, в которой эта информация циркулирует. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока информация находится в обращении, принимаемые меры могут

только снизить вероятность негативных воздействий или ущерб от них, но не исключить их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов компьютерной системы и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

9. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

10. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, в каком это необходимо сотруднику для выполнения его должностных обязанностей.

11. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделении. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений обеспечения безопасности информации.

12. Гибкость системы защиты

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на уже работающую систему, не нарушая процесса ее нормального функционирования. Кроме того, внешние условия и требования с течением времени меняются. В таких ситуациях свойство гибкости системы защиты избавляет владельцев АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

13. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это однако не означает, что информация о конкретной системе защиты должна быть общедоступна.

14. Простота применения средств защиты

Механизмы зашиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

15. Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.

16. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственные лицензии на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными сотрудниками (специалистами подразделений обеспечения безопасности информации).

17. Взаимодействие и координация

Предполагают осуществление мер обеспечения безопасности информации на основе взаимодействия всех заинтересованных министерств и ведомств, предприятий и организаций при разработке и функционировании АС и ее системы защиты информации, подразделений и специалистов органов МВД специализированных предприятий и организаций в области защиты информации, привлеченных для разработки системы защиты информации в АС, координации их усилий для достижения поставленных целей Гостехкомиссией России (на этапе разработки и внедрения АС) и подразделениями безопасности органов МВД (на этапе функционирования системы).

18. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства зашиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

10 ОСНОВНЫЕ ОРГАНИЗАЦИОННЫЕ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО СОЗДАНИЮ И ОБЕСПЕЧЕНИЮ ФУНКЦИОНИРОВАНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ

Организационные меры являются той основой, которая объединяет различные меры защиты в единую систему. Они включают:

• разовые (однократно проводимые и повторяемые только при полном пересмотре принятых решений) мероприятия;

• мероприятия, проводимые при осуществлении или возникновении определенных изменений в самой защищаемой АС или внешней среде (по необходимости);

• периодически проводимые (через определенное время) мероприятия;

• постоянно (непрерывно или дискретно в случайные моменты времени) проводимые мероприятия.

Разовые мероприятия

К разовым мероприятиям относят:

• мероприятия по созданию нормативно-методологической базы (разработка концепции и других руководящих документов) защиты АС;

• мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов АС (исключение возможности тайного проникновения в помещения, исключение возможности установки прослушивающей аппаратуры и т.п.);

• мероприятия, осуществляемые при проектировании, разработке и вводе в эксплуатацию технических средств и программного обеспечения (проверка и сертификация используемых технических и программных средств, документирование и т.п.);

• проведение спецпроверок применяемых в АС средств вычислительной техники и проведения мероприятий по защите информации от утечки по каналам побочных электромагнитных излучений и наводок;

• внесение необходимых изменений и дополнений во все организационно-распорядительные документы (положения о подразделениях, функциональные обязанности должностных лиц, технологические инструкции пользователей системы и т.п.) по вопросам обеспечения безопасности ресурсов АС и действиям в случае возникновения кризисных ситуаций;

• создание подразделения защиты информации (компьютерной безопасности) и назначение нештатных ответственных за ОИБ в подразделениях и на технологических участках, осуществляющих организацию и контроль за соблюдением всеми категориями должностных лиц требований по обеспечению безопасности программно-информационных ресурсов автоматизированной системы обработки информации; разработка и утверждение их функциональных обязанностей;

• мероприятия по разработке политики безопасности, определение порядка назначения, изменения, утверждения и предоставления конкретным категориям сотрудников (должностным лицам) необходимых полномочий по доступу к ресурсам системы;

• мероприятия по созданию системы защиты АС и необходимой инфраструктуры (организация учета, хранения, использования и уничтожения документов и носителей с закрытой информацией, оборудование служебных помещений сейфами (шкафами) для хранения реквизитов доступа, средствами уничтожения бумажных и магнитных носителей конфиденциальной информации и т.п.);

• мероприятия по разработке правил разграничения доступом к ресурсам системы (определение перечня задач, решаемых структурными подразделениями организации с использованием АС, а также используемых при их решении режимов обработки и доступа к данным;

• определение перечней файлов и баз данных, содержащих сведения, составляющие коммерческую и служебную тайну, а также требований к уровням их защищенности от НСД при передаче, хранении и обработке в АС;

• выявление наиболее вероятных угроз для данной АС, выявление уязвимых мест процессов обработки информации и каналов доступа к ней, оценка возможного ущерба, вызванного нарушением безопасности информации, разработку адекватных требований по основным направлениям защиты);

• организация охраны и надежного пропускного режима;

• определение порядка проектирования, разработки, отладки, модификации, приобретения, специсследования, приема в эксплуатацию, хранения и контроля целостности программных продуктов, а также порядок обновления версий используемых и установки новых системных и прикладных программ на рабочих местах защищенной системы (кто обладает правом разрешения таких действий, кто осуществляет, кто

• контролирует и что при этом они должны делать), определение порядка учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих эталонные и резервные копии программ и массивов информации, архивные данные и т.п.;

• определение перечня необходимых регулярно проводимых превентивных мер и оперативных действий персонала по обеспечению непрерывной работы и восстановлению вычислительного процесса АС в критических ситуациях, возникающих как следствие НСД, сбоев и отказов СВТ, ошибок в программах и действиях персонала, стихийных бедствий.

Периодически проводимые мероприятия

К периодически проводимым мероприятиям относят:

• распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.);

• анализ системных журналов (журналов регистрации), принятие мер по обнаруженным нарушениям правил работы;

• пересмотр правил разграничения доступа пользователей к ресурсам АС организации;

• осуществление анализа состояния и оценки эффективности мер и применяемых средств защиты и разработка необходимых мер по совершенствованию (пересмотру состава и построения) системы защиты.

Мероприятия, проводимые по необходимости

К мероприятиям, проводимым по необходимости, относят:

• мероприятия, осуществляемые при кадровых изменениях в составе персонала системы;

• мероприятия, осуществляемые при ремонте и модификациях оборудования и программного обеспечения (санкционирование, рассмотрение и утверждение изменений, проверка их на удовлетворение требованиям защиты, документальное отражение изменений и т.п.);

• проверка поступающего оборудования, предназначенного для обработки закрытой информации, на наличие специально внедренных закладных устройств, инструментальный контроль технических средств на наличие побочных электромагнитные излучения и наводок;

• оборудование систем информатизации устройствами защиты от сбоев электропитания и помех в линиях связи;

• мероприятия по подбору и расстановке кадров (проверка принимаемых на работу, обучение правилам работы с информацией, ознакомление с мерами ответственности за нарушение правил защиты, обучение, создание условий, при которых персоналу было бы невыгодно нарушать свои обязанности и т.д.);

• оформление юридических документов (договоров, приказов и распоряжений руководства организации) по вопросам регламентации отношений с пользователями (клиентами) и третьей стороной (арбитражем, третейским судом) о правилах разрешения споров, связанных с информационным обменом;

• обновление технических и программных средств защиты от НСД к информации в соответствие с меняющейся оперативной обстановкой.

Постоянно проводимые мероприятия

Постоянно проводимые мероприятия включают:

• мероприятия по обеспечению) достаточного уровня физической защиты всех компонентов АС (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности СВТ, носителей информации и т.п.).

• мероприятия по непрерывной поддержке функционирования и управлению (администрированию) используемыми средствами защиты;

• организацию явного и скрытого контроля за работой пользователей и персонала системы;

• контроль за реализацией выбранных мер защиты в процессе проектирования, разработки, ввода в строй, функционирования, обслуживания и ремонта АС;

• постоянно (силами службы безопасности) и периодически (с привлечением сторонних специалистов) осуществляемый анализ состояния и оценка эффективности мер и применяемых средств защиты.