Министерство образования и науки Российской Федерации

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ
(ТУСУР)

Кафедра радиоэлектроники и защиты информации (РЗИ)

ОБЗОР БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ НА БАЗЕ NOVELL NETWARE

Тематический реферат
по дисциплине «Основы вычислительной техники»

Студент группы 180
_____В.Б. Поротиков
_____

Руководитель
_____ _____А.С. Карауш
_____

2004

СОДЕРЖАНИЕ

1. Novell NetWare в корпоративной сети.

В настоящее время много публикаций посвящены компьютерным сетям масштаба предприятия. Так выглядит дословный перевод термина "EnterpriseWide Networks", получившего распространение в западной литературе. В отечественных материалах их чаще называют корпоративными сетями.

Ниже перечислены особенности, наличие одной или нескольких из которых позволяет считать сеть корпоративной:

- во-первых, это большое количество объединенных в общую сеть компьютеров, в том числе большое число файловых серверов, серверов баз данных, приложений и т.д.
- во-вторых, гетерогенный характер сети: различные протоколы, разнородные среды передачи, произведенные разными компаниями компьютерные платформы, различные операционные системы;
- в третьих, подобные сети характеризуются наличием нескольких локальных вычислительных сетей, территориально отстоящих друг от друга.

При переходе от локальной сети к корпоративной необходимо решить следующие задачи:

1. объединить различные компьютерные платформы в единую сеть,
2. реализовать поддержку маршрутизации различных сетевых протоколов,
3. объединить удаленные локальные сети с помощью мостов, маршрутизаторов и шлюзов,
4. организовать доступ большого числа пользователей к ресурсам единой сети и управление ресурсами.

Важность решения первой задачи связано с тем, что каждая из платформ имеет сильные и слабые стороны. Novell предлагает следующее распределение ролей между платформами:

- операционная система NetWare - файловый, почтовый (MHS) и коммуникационный (NetWare Connect) серверы,
- операционная система UnixWare - сервер баз данных и приложений.

При решении второй и третьей задач можно использовать следующие продукты фирмы Novell: NetWare Multi Protocol Router v.3.0 (MPR), NetWare/IP, NetWare FLeX/IP 1.2c, NetWare NFS 1.2c. Используя MPR, можно построить глобальную разнородную сеть на базе NetWare и PC-совместимых компьютеров. В одну сеть могут быть объединены сети, работающие по таким популярным протоколам как IPX, IP, AppleTalk, Novell NetBIOS, OSI, FTAM с использованием физических сред передачи Ethernet, Token Ring, ARCnet, FDDI, LocalTalk. Продукт NetWare/IP обеспечивает полную интеграцию сетей NetWare в среду протокола TCP/IP. Он позволяет пользователям сетей, работающих по протоколу TCP/IP, использовать сети NetWare и приложения для них. Пакеты NetWare FLeX/IP 1.2c и NetWare NFS 1.2c предназначены для использования в сетях, где требуется доступ пользователей UNIX к ресурсам NetWare (принтерам и файлам).

Четвертая задача имеет два аспекта: программный и аппаратный. С точки зрения сетевого программного обеспечения сеть должна выглядеть для пользователя единым пулом разнообразных ресурсов. Пользователю не важно, какой из серверов предоставляет ему те или иные ресурсы. Это позволяет администратору системы более гибко распределять ресурсы по имеющимся в наличии серверам, упрощает и повышает эффективность контроля и управления ресурсами сети. Для управления ресурсами сети во всех современных операционных системах выделяются специальные сервисы. В NetWare 4.x эту роль играют служба каталогов NetWare Directory Services (NDS) и системы управления сетями NMS (NetWare Management System) и ManageWise. С точки зрения аппаратных средств эту задачу можно сформулировать так: обеспечение эффективного доступа пула клиентов к пулу серверов. Практическим решением этой задачи является использование при построении кабельной системы так называемых активных элементов. К ним можно отнести

локальные мосты, маршрутизаторы, шлюзы, а также устройства, использующие технологию Ethernet Switch, и FDDI-концентраторы.

Сеть должна обеспечивать удобство доступа к своим ресурсам - дисковым томам, разделяемым принтерам, устройствам архивации, модемам и другим устройствам коллективного использования.

Все устройства, подключаемые к сети с ОС NetWare, можно разделить на три функциональные группы:

- рабочие станции,
- серверы сети,
- коммуникационные узлы.

Рабочая станция (Workstation) - это персональный компьютер, подключенный к сети, на котором пользователь сети выполняет свою работу. Каждая рабочая станция обрабатывает свои локальные файлы и использует свою операционную систему, например, DOS. Но при этом пользователю доступны ресурсы сети. Можно выделить три типа рабочих станций (PC):

- рабочая станция с локальным диском,
- бездисковая рабочая станция,
- удаленная рабочая станция.

На рабочей станции с диском (жестким или гибким) операционная система загружается с этого локального диска.

Бездисковая PC не имеет ни жесткого, ни гибкого диска. Для такой станции ее операционная система загружается с диска файлового сервера.

Удаленная рабочая станция - это станция, которая подключается к локальной сети через телекоммуникационные каналы связи (например, с помощью телефонной сети).

Сервер сети (Server) - это компьютер, подключенный к сети и предоставляющий пользователям сети определенные услуги, например, хранение данных общего пользования, печать заданий, обработка запроса к СУБД, удаленная обработка заданий и т.д. По выполняемым функциям можно выделить следующие группы серверов:

- Файловый сервер (File Server) - компьютер, хранящий данные пользователей сети и обеспечивающий доступ пользователей к этим данным. ОС NetWare обеспечивает одновременный доступ пользователей к данным, расположенным на файловом сервере. Файловый сервер выполняет следующие функции:
  - хранение данных,
  - архивирование данных,
  - согласование изменений данных, выполняемых разными пользователями,
  - передача данных.
- Сервер баз данных (SQL-Server) - компьютер, выполняющий функции хранения, обработки и управления файлами баз данных. Сервер баз данных выполняет следующие функции:
  - прием и обработка запросов к СУБД, а также пересылка результатов обработки на рабочую станцию,
  - обеспечение секретности данных,
  - согласование изменений данных, выполняемых разными пользователями,
  - взаимодействие с другими серверами баз данных, расположенными в другом месте.
- Сервер прикладных программ (Application Server) - компьютер, который используется для выполнения прикладных программ пользователей.
- Коммуникационный сервер (Communications Server) - устройство или компьютер, который предоставляет пользователям локальной сети прозрачный доступ к своим последовательным портам ввода/вывода.
- Сервер доступа (Access Server) - это выделенный компьютер, позволяющий выполнять удаленную обработку заданий. Программы, инициируемые с удаленной рабочей стан-

ции, выполняются в многозадачной среде этого компьютера. От удаленной рабочей станции принимаются команды, введенные пользователем с клавиатуры, а возвращаются результаты выполнения задания.

- Факс-сервер (Fax Server) - устройство или компьютер, который выполняет рассылку и прием факсимильных сообщений для пользователей локальной сети.
- Сервер резервного копирования данных (Back Up Server) - устройство или компьютер, который решает задачи создания, хранения и восстановления копий данных, расположенных на файловых серверах и рабочих станциях.

К коммуникационным узлам сети относятся следующие устройства:

- повторители,
- мосты, коммутаторы,
- маршрутизаторы,
- шлюзы.

2. Уязвимости и атаки.

Сеть должна обеспечивать удобство доступа к своим ресурсам - дисковым томам, разделяемым принтерам, устройствам архивации, модемам и другим устройствам коллективного использования - в сочетании с эффективной системой их защиты от несанкционированного доступа. Эти функции с успехом решены в NetWare, разные поколения имеют свои характерные отличия, но в них прослеживаются и общие принципы защиты ресурсов. В NetWare 4.x также имеется развитая система сетевого аудита - пассивной системы всестороннего и независимого наблюдения за действиями пользователей.

Источниками уязвимостей, в большинстве своем, являются программисты Novell, т.к. возможность реализации практически любой атаки обеспечивается несовершенством исходного кода самих программных продуктов. Говоря короче, программисты Novell по недосмотру, либо в ввиду невнимательности сами предоставляют возможность злоумышленникам реализовать свои злые намерения.

2.1 Механизмы и типы атак.

В общем случае воздействия на сетевую операционную систему могут быть реализованы по двум направлениям:

- воздействие на файл-сервер с его консоли (локальное воздействие);
- воздействие на файл-сервер с рабочей станции (удаленное воздействие).

2.1.1 Локальные воздействия.

При наличии физического доступа к консоли файл-сервера в сети Novell NetWare возможны следующие воздействия:

- **Отладка логики работы ОС.** Имеется возможность с помощью отладчика повлиять на логику работы ОС изменяя ее код в оперативной памяти так, что в дальнейшем любой пользователь получает возможность беспарольного входа в систему.
- **Использование утилит для непосредственного доступа к жесткому диску файл-сервера на физическом уровне (например, DISKEDIT).** Возможно изменить данные операционной системы, хранящиеся на жестком диске. В частности, можно получить доступ к базе данных BINDERY, в которой содержатся сведения о ресурсах системы, в т.ч. список всех пользователей системы с их правами доступа и образами паролей.

2.1.2 Удаленные воздействия.

В сети Novell NetWare возможно осуществление следующих удаленных воздействий:

- **Исследование сетевого трафика.** Использование программы сетевого анализатора, исследующую сетевой трафик на канальном уровне, позволило обнаружить ошибку, допущенную программистами фирмы Novell. При смене пароля супервизором любому пользователю (в том числе и себе) с помощью программы SYSCON (только v. 3.75-3.76) новый пароль передается по сети в незашифрованном виде и может быть прочитан сетевым анализатором.
- **Подмена рабочей станции - "голландская атака".** Общей проблемой для любой сетевой операционной системы является идентификация и аутентификация ее удаленных друг от друга компонент. Если этой проблеме не придавать значения, то тогда ни что не мешает злоумышленнику послать пакет на файл-сервер от имени одной рабочей станции, находясь на другой станции; или наоборот, послать пакет на рабочую станцию от имени файл-сервера. Данная проблема не была решена в ОС Novell NetWare 3.11 и в результате оказалось возможным реализовать так называемую "голландскую" атаку, результат которой - получение злоумышленником прав другого зарегистрированного в сети пользователя. Эта атака стала возможной, так как в ОС Novell NetWare использовались простейшие методы идентификации пакетов. В частности, пакеты идентифицировались только по номеру счетчика (0 - FFh) и номеру канала (0 - FFh) и не проверялось соответствие адреса станции, от которой пришел пакет, номеру канала, ей присвоенного. В версии Novell NetWare 3.12 и выше в ответ на голландскую атаку введено дополнительное средство идентификации - цифровая подпись пакетов.
- **Использование недостатков в механизме поиска рабочей станцией файл-сервера для его подмены (ложный сервер).** Вследствие того, что текущее количество серверов в Novell NetWare неизвестно, то перед рабочей станцией встает проблема поиска файл-сервера в сети. Эта проблема может решаться посылкой определенного набора пакетов на широковещательный адрес и ожидание ответа с необходимыми данными. Такой механизм поиска сервера используется, например, в ОС Novell NetWare и называется протоколом SAP. Если не придать значения безопасности алгоритма поиска сервера, то ничто не мешает программным образом на любой рабочей станции получить этот широковещательный запрос и послать запросившей станции ответ, в котором прислать свой адрес. В результате, можно добиться того, что запросившая станция будет считать ответившую станцию настоящим файл-сервером и, в дальнейшем, вся информация между файл-сервером и вновь подключившейся станцией будет проходить через третью станцию (ложный сервер).
- **Использование входа в систему специальным пользователем - сервером печати.** Novell API предоставляет функцию ChangeToClientRigths(), которая позволяет служебному серверу очереди (Queue server) использовать права пользователя, который поместил это задание в очередь. Данная функция является, по всей видимости, устаревшей и, возможно, оставлена для совместимости с предыдущими версиями Novell Netware. Она может быть отключена с консоли сервера с помощью команды SET Allow Change To Client Rights = OFF. Таким образом, если удастся идентифицироваться на файл-сервере как сервер очереди, то можно будет выполнить вызов этой функции и получить права конкретного пользователя (в т.ч. и супервизора). Так как сервер печати является, с точки зрения Novell Netware, сервером очереди и часто не имеет пароля, то возможно использование входа в систему этим пользователем для несанкционированного получения широких полномочий.
- **Подмена пользователя при некорректном завершении его сеанса работы с файл-сервером.** В ОС Novell NetWare для корректного окончания сеанса работы пользователя с файл - сервером требуется выдача команды LOGOUT на рабочей станции пользователя для закрытия виртуального канала с сервером. Однако, многие пользователи редко пользуются этой командой, предпочитая просто выключить

или перезагрузить свой компьютер. Такое окончание сеанса работы с файл-сервером является некорректным и в сочетании с отказом от использования цифровой подписи пакетов (а, следовательно, слабой идентификации пакетов) может привести к подмене пользователя в сети.

- **Контроль над рабочей станцией в сети (сетевой шпион).** В связи с объединением компьютеров в сеть появляются сетевые шпионы. Сетевыми шпионами будем называть программные закладки или компьютерные вирусы, основная цель которых - получение контроля над рабочей станцией в сети. Рассмотрим основные функции, присущие сетевым шпионам:
    - перехват и передача вводимой с клавиатуры информации на головную сервер-программу;
    - перехват и передача экранной информации на головную сервер-программу;
    - перехват и передача на головную сервер-программу системной информации о ПК (тип ОС, параметры компьютера, загруженные программы и т.д.);
    - получение контроля сервер-программой над зараженным удаленным компьютером (удаленный запуск программ, копирование данных, удаление данных и т.д.).

2.2 CVE.

Для ликвидации ошибок в исходных кодах программных продуктов и для обеспечения должного уровня безопасности в компьютерных сетях и системах корпорацией MITRE и Департаментом Безопасности Отечества США (U.S. Department of Homeland Security) был создан проект CVE (Common Vulnerabilities and Exposures).

2.2.1 Что такое CVE?

Общие уязвимости и незащищенности (Common Vulnerabilities and Exposures (CVE)) это список или словарь, который предоставляет имена или названия публично известных уязвимостей и незащищенностей информационной безопасности компьютерных систем. Использование общих имен упрощает совместное использование информации из распределенных баз данных и инструментов, которые до сих пор не были легко доступны. Это делает CVE ключом для совместного использования информации. Если отчет от одного из сервисов безопасности входит в список имен CVE (CVE-names), пользователь может быстро и аккуратно получить доступ к исправляющей информации в одной или более распределенных CVE-совместимых (CVE-compatible) баз данных для исправления проблемы.

Большую часть информации сервисы безопасности включают в базу данных безопасности от уязвимостей и незащищенностей, в этих базах данных указания на них (уязвимости) приводятся со значительными изменениями (вплоть до технических подробностей), и не просто определить когда различные базы данных ссылаются на ту же самую проблему. Следствия - потенциальные дыры в системах безопасности и нет эффективного указания на них в различных базах данных. В дополнение каждый поставщик сервисов и продуктов информационной безопасности использует разные методы подсчета числа уязвимостей или незащищенностей, которые они (продукты) обнаруживают, что подразумевает отсутствие стандарта для вычисления среди инструментов.

С стандартизированным списком уязвимостей и незащищенностей, типа CVE, базы данных и инструменты безопасности могут взаимодействовать друг с другом. И администратор будет в точности знать, какую область каждый инструмент защищает, потому что CVE предоставит основания для вычисления защищенности, которую обеспечивают сервисы и инструменты. Это означает, что пользователь может определить какой из инструментов наиболее эффективен и наиболее подходит для специфических нужд объекта. Короче говоря, CVE-совместимые инструменты и базы данных дадут лучшую защищенность, упрощенное взаимодействие, и усиленную защиту.

CVE отмечен лидирующими представителями общества защиты информации. Содержание составляется группой профессионалов, которая включает в себя представителей организаций по защите информации.

2.2.2 Что означает CVE-совместимость (CVE-compatible)?

CVE-совместимость означает что инструмент, веб сайт, база данных или другой продукт безопасности или сервис, использующий CVE-имена способом, позволяющим перекрестно ссылаться на одни и те же имена с другими продуктами, которые также используют CVE -имена.
Имеется в виду:

- CVE-поиск – пользователь может искать используя имена CVE для того, чтобы найти связанную по теме (или проблеме) информацию.
- CVE-выход – информация представляется таким образом, что увязана с CVE-именами.
- Документация - организационный стандарт документации включает в себя описание CVE, CVE-совместимость, и детали того как клиент может использовать CVE-родственную функциональность (имеется ввиду версии продукта) этого продукта или сервиса.

2.2.3 Зачем нужно CVE?

Сообщения об обнаруженных уязвимостях и незащищенностях поступают в CVE. Там после обработки экспертами в соответствующей области они классифицируются, сортируются, им присваиваются имена и они размещаются в базе данных в виде, описанном выше. Далее эта информация свободно распространяется, в результате чего у администраторов ЛВС/информационных ресурсов появляется возможность закрыть брешь в системе безопасности. Нужно отметить, что существуют различные направления работы CVE. Они зависят от сетевых программных продуктов. Существуют базы данных CVE по Unix, Windows NT, Novell и так далее, что делает CVE стандартизированным с точки зрения поиска, перекрестных ссылок, и имен уязвимостей и способов решения этих проблем программным продуктом.

Пример кандидата для включения в списки CVE, касающегося безопасности в Novell:

Name	CAN-2002-0341 (under review)
Description	GWWEB.EXE in GroupWise Web Access 5.5, and possibly other versions, allows remote attackers to determine the full pathname of the web server via an HTTP request with an invalid HTMLVER parameter.
References	• BUGTRAQ:20020227 SecurityOffice Security Advisory:// Novell GroupWise Web Access Path Disclosure Vulnerability • URL:http://marc.theaimsgroup.com/?l=bugtraq&m=101494830315071&w=2
Phase	Proposed (20020502)
Votes	MODIFY(1) Frech NOOP(5) Christey, Wall, Foat, Cole, Cox
Comments	Frech> XF:groupwise-arg-path-disclosure(8311) Christey> Desc: "... which leaks the pathname in an error message."

Он же, на русском:

Имя	CAN-2002-0341 (на рассмотрении)
Описание	GWWEB.EXE в GroupWise Web Access 5.5, и возможно других версий, позволяет удаленному атакующему установить полный путь веб сервера через запрос HTML с недопустимым параметром HTMLVER.
Ссылки	• BUGTRAQ:20020227 SecurityOffice Security Advisory:// Novell Group-

	Wise Web Access Path Disclosure Vulnerability • URL:http://marc.theaimsgroup.com/?l=bugtraq&m=101494830315071&w=2
Фаза	предложен (дата)
Голосования	Имена голосовавших и предмет голосования
Комментарии	Комментарии голосовавших

3. Защитные механизмы и средства.

3.1 Идентификация пользователей.

Служба NDS позволяет пользователю зарегистрироваться на сервере сети и в соответствии со своими полномочиями получить доступ к другим средствам сети. Средство идентификации проверяет правомочность использования сети пользователем. Оно работает в сочетании со списком полномочий доступа (Access Control List), который содержит информацию об объектах. Пользователи не знают о средстве идентификации: оно работает в фоновом режиме. Средство идентификации присваивает уникальную идентификацию каждому пользователю в каждом сеансе регистрации. Именно идентификация, а не пароль пользователя, используется для идентификации запросов пользователя в сети. Этим улучшается защита, поскольку пароль пользователя никогда не циркулирует по сети, где его трудно отследить. При перехвате идентификационных данных злоумышленники не смогут сами зарегистрироваться в сети, поскольку они никак не соотносятся с паролем регистрации пользователя.

Идентификация обеспечивает, что пароль пользователя не выходит за рамки процесса регистрации. Он немедленно конвертируется в другой код, идентифицирующий пользователя и станцию, на которой он зарегистрировался, и действует только во время текущего сеанса. Идентификация обеспечивает также защиту передаваемых сообщений.

3.2 Аутентификация пользователей.

Подключение к сети выполняется с помощью утилиты LOGIN.EXE. Эта программа передаёт на сервер идентификатор, введённый пользователем (рисунок 2.54).

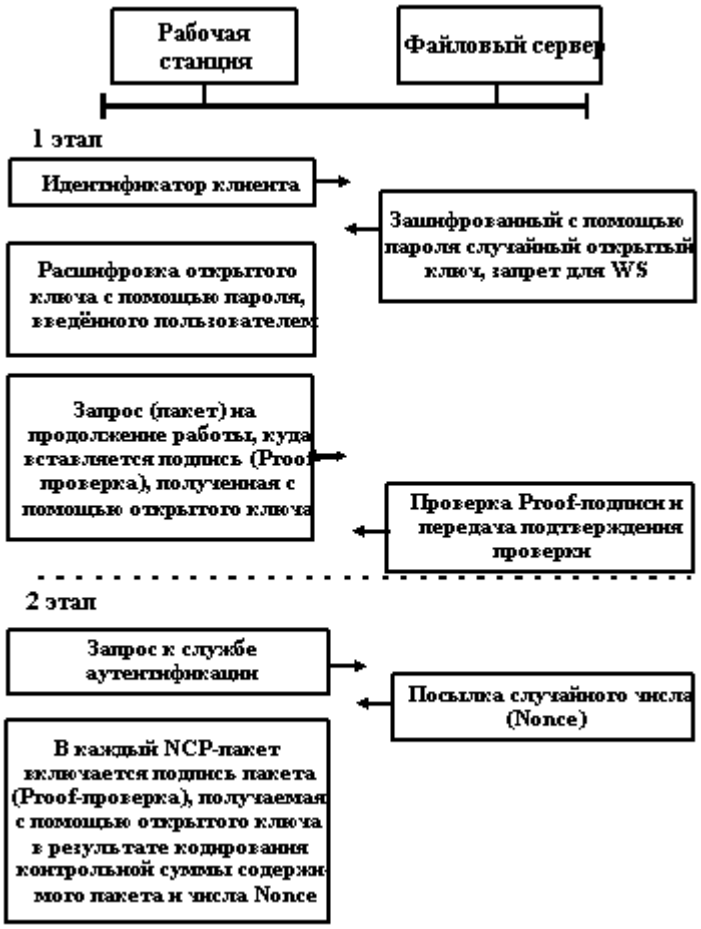

Рис. 3.1. Аутентификация клиента

По этому идентификатору NetWare выполняет поиск соответствующего объекта пользователя в системной базе данных сетевых ресурсов. Если в базе данных хранится значение пароля для этого клиента, то NetWare посылает на рабочую станцию зашифрованный с помощью пароля открытый ключ (симметричное шифрование). На рабочей станции этот ключ расшифровывается с помощью пароля, введённого пользователем, и используется для получения подписи запроса (пакета) к серверу о продолжении работы. Сервер расшифровывает эту подпись с помощью закрытого ключа (асимметричное шифрование), проверяет её и посылает подтверждение на рабочую станцию. В дальнейшем каждый NCP-пакет снабжается подписью, получаемой в результате кодирования открытом ключом контрольной суммы содержимого пакета и случайного числа Nonce. Это число генерируется для каждого сеанса. Поэтому подписи пакетов не повторяются для разных сеансов, даже если пользователь выполняет те же самые действия.

3.3 Авторизация доступа к данным сети.

В NetWare реализованы три уровня защиты данных (рисунок 3.2).
Здесь под аутентификацией понимается:

- процесс подтверждения подлинности клиента при его подключении к сети,
- процесс установления подлинности пакетов, передаваемых между сервером и рабочей станцией.

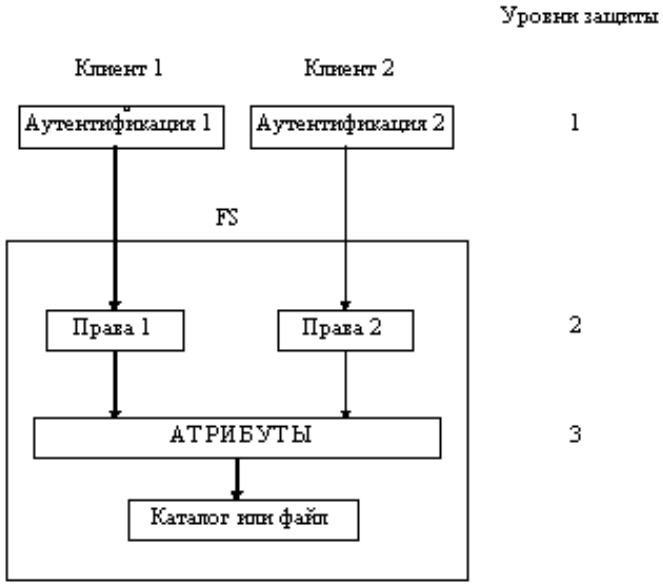

Рис. 3.2. Уровни защиты данных в NetWare.

Права по отношению к файлу (каталогу) определяют, какие операции пользователь может выполнить с файлом (каталогом). Администратор может для каждого клиента сети определить права по отношению к любому сетевому файлу или каталогу. Атрибуты определяют некоторые системные свойства файлов (каталогов). Они могут быть назначены администратором для любого сетевого файла или каталога. Например, чтобы записать данные в файл, клиент должен:

- знать свой идентификатор и пароль для подключения к сети,
- иметь право записи данных в этот файл,
- файл должен иметь атрибут, разрешающий запись данных.

Следует отметить, что атрибуты файла (каталога) имеют более высокий приоритет, чем права пользователей по отношению к этому файлу.

3.4 Определение эффективных прав пользователей по отношению к каталогам и файлам.

Права, которые могут быть предоставлены пользователю (или группе пользователей) по отношению к каталогу или файлу, перечислены в таблице 3.1.
Права и фильтры (маски) наследуемых прав назначаются администратором сети с помощью утилит NetWare. Но назначение прав для каждого пользователя по отношению ко всем требуемым файлам и каталогам - это утомительная задача. В NetWare предлагается механизм наследования прав. Прежде всего введём некоторые определения.
Опекун (Trustees) - это пользователь (или группа пользователей, или другой объект), которому администратор с помощью утилиты (например, FILER) явно назначает права по отношению к какому-либо файлу или каталогу. Такие права называются опекунскими назначениями.
Фильтр наследуемых прав (IRF - Inherited Right Filter) - это свойство файла (каталога), определяющее, какие права данный файл (каталог) может унаследовать от родительского каталога. Фильтр назначается администратором с помощью утилиты (например, FILER).
Наследуемые права - права, передаваемые (распространяемые) от родительского каталога.
Эффективные права - права, которыми пользователь реально обладает по отношению к файлу или каталогу.
Таблица 2.16. Список возможных прав по отношению к каталогу или файлу

Право	Обозначение	Описание
Supervisor	S	Предоставляет все права по отношению к каталогу или файлу, включая возможность назначения этого права другим пользователям. Не блокируется фильтром наследуемых прав IRF. Это право не может быть удалено ниже по дереву каталогов.
Read	R	Чтение существующего файла (просмотр содержимого текстового файла, просмотр записей в файле базы данных и т. д.).
Write	W	Запись в существующий файл (добавление, удаление частей текста, редактирование записей базы данных).
Create	C	Создание в каталоге новых файлов (и запись в них) и подкаталогов. На уровне файла позволяет восстанавливать файл, если он был ошибочно удалён.
Erase	E	Удаление существующих файлов и каталогов.
Modify	M	Изменение имён и атрибутов (файлов и каталогов), но не содержимого файлов.
File Scan	F	Просмотр в каталоге имён файлов и подкаталогов.
Access Control	A	Возможность предоставлять другим пользователям все права, кроме Supervisor. Возможность изменять фильтр наследуемых прав IRF.

3.5 Криптографические методы защиты информации.

Применяемые криптоалгориты и их недостатки:
По сравнении с версией 2.x, где пароли пользователей передавались по сети в открытом виде, криптографическая защиты операционной системы Novell Netware 3.x является более совершенной. К ней относится:

- использование "метода рукопожатия", в результате чего пароль (даже зашифрованный) не передается по сети по время сеанса входа в систему;
- пароли пользователей хранятся на сервере только в зашифрованном виде;
- при вводе неправильного пароля операционная система Novell Netware использует задержку в несколько секунд для предотвращения атаки по словарю. Имеется возможность ограничить количество неправильно набранных паролей.

Пароль любого пользователя, хранящиеся в базе данных связок как свойство "PASSWORD", является зашифрованным. Для его получения операционная система Novell Netware проделывает следующие операции:

- из оригинального пароля пользователя получается 32-байтовая последовательность путем либо сжатия пароля длиной более 32 символов с помощью операции XOR, либо размножением пароля длиной менее 32 символов;
- эта последовательность шифруется операцией XOR с идентификатором объекта (object ID), уникальным для каждого пользователя;
- из этой последовательности получается выходная 16-байтовая последовательность с помощью специального алгоритма хэширования. Именно эта 16-байтовая последовательность и является свойством "PASSWORD", хранимым на сервере. При этом следует отметить, что:
- мощность полного перебора ограничена числом $256^{16} = 2^{128}$ для пароля любой длины. Это, безусловно, выходит за рамки возможностей современной вычислительной техники и в 2^{72} раза превышает криптостойкость DES. Однако максимальная длина пароля в Novell Netware равна 128 символами, что должно давать примерно 2^{750} вариантов полного перебора. Отсюда следует, что на самом деле максимальная длина пароля в 6 раз меньше;

- идентификатор супервизора обычно равен 0x00000001, и шифрование с ним практически бессмысленно. Этот факт позволяет ускорить перебор паролей.

Далее, при вызове функции библиотеки Novell C Interface LoginToFileServer() происходит следующая последовательность действий:

- сервер посылает станции 8-байтовую последовательность случайных чисел;
- на станции из оригинального пароля с помощью алгоритма, описанного выше, получается тот же самый Hash16, и пришедшая последовательность шифруется с его помощью в выходную 8-байтовую последовательность, которая и отправляется обратно серверу;
- сервер шифрует посланную последовательность с помощью Hash16;
- сервер проверяет соответствие полученной и вычисленной последовательности.

Как видно, Hash16 не передается по сети при подключении к серверу. Криптосистема Novell 4.x еще более усилена использованием несимметричных ключей.

3.6 Контроль целостности.

Использование сигнатур для передачи NCP-пакетов.

Необходимость применения сигнатуры (подписи) NCP-пакетов связана со скандалом, разыгравшимся в 1992 году. Тогда голландский студент предложил простой способ "взламывания" файлового сервера NetWare. Этот способ основывается на параллельной работе хаккера и пользователя, имеющего требуемые права (рисунок 3.3).

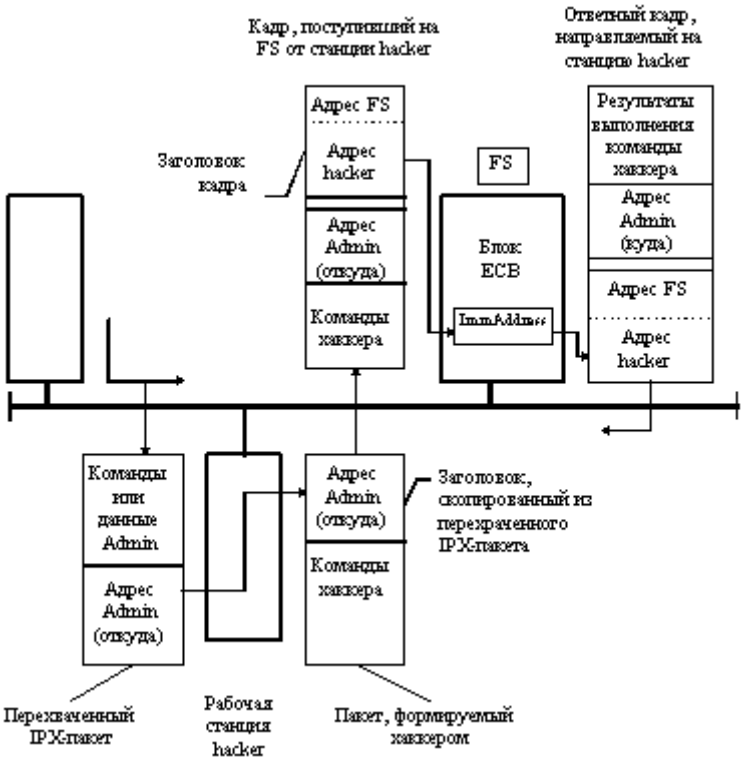

Рис. 3.3. Организация несанкционированного доступа к файловому серверу.

На рабочей станции хакера функционирует программа, которая перехватывает пакеты, передаваемые по шине сети. При формировании пакета программа хаккера выполняет следующие действия:

- переписывает в заголовок формируемого IPX-пакета заголовок перехваченного пакета,
- записывает в поле данных требуемую команду.

Далее пакет посылается на файловый сервер. Файловый сервер пересылает адрес станции hacker в поле ImmAddress блока ECB и использует данные заголовка пакета IPX, чтобы определить номер соединения и возможность выполнения команды. Но в заголовке пакета хакера записан адрес пользователя (адрес Admin), который имеет требуемые права. Поэтому команда хакера выполняется. При формировании сетевым адаптером заголовка ответного кадра адрес станции, куда непосредственно передаётся кадр, выбирается из поля ImmAddress блока ECB. Т. е. станция hacker воспринимается файловым сервером как маршрутизатор или мост. Напомним, что адрес конечной станции-получателя хранится в заголовке пакета IPX (в данном случае это адрес Admin, хотя для хакера это не имеет значения). Таким образом, ответ посылается на станцию hacker, где и обрабатывается. Подпись NCP-пакета (специальное поле в этом пакете) делает невозможным параллельную работу хакера и пользователя. Подпись (сигнатура) пакета - это шифр, для формирования которого используется контрольная сумма содержимого пакета и случайное число Nonce. Шифр создаётся с помощью открытого ключа. Важно отметить, что сигнатура изменяется в каждом пакете. Спрогнозировать последовательность подписей практически невозможно.

NCP-пакеты могут подписываться и рабочими станциями, и файловым сервером. Для инициирования включения подписи в NCP-пакеты администратор должен выполнить следующие действия (для NetWare 3.12 и 4.x):

a. С консоли файлового сервера необходимо ввести SET-команду

SET NCP Packet Signature Option = уровень (по умолчанию 1)

Можно задать один из следующих уровней:

- 0 - сервер не подписывает пакет,
- 1 - сервер подписывает пакет, если этого требует клиент (уровень на станции больше или равен 2),
- 2 - сервер подписывает пакет, если клиент также способен это сделать (уровень на станции больше или равен 1),
- 3 - сервер подписывает пакет и требует этого от всех клиентов (иначе подключение к сети невозможно).

2. На рабочей станции в раздел Netware DOS Requester файла net.cfg необходимо включить строку:

Signature Level = уровень (по умолчанию 1)

Можно задать один из следующих уровней:

- 0 - клиент не подписывает пакет,
- 1 - клиент подписывает пакет, если этого требует сервер (уровень на сервере больше или равен 2),
- 2 - клиент подписывает пакет, если сервер также способен это сделать (уровень на сервере больше или равен 1),
- 3 - клиент подписывает пакет и требует этого от всех серверов (иначе подключение к сети невозможно).

В таблице 3.1 перечислены различные сочетания уровней на сервере и рабочей станции, а также варианты подписи пакета.

Таблица 3.1. Варианты подписи пакета

Если	уровень на сервере = 0	уровень на сервере = 1	уровень на сервере = 2	уровень на сервере = 3
уровень на станции = 0	-	-	-	N

уровень на станции = 1	-	-	+	+
уровень на станции = 2	-	+	+	+
уровень на станции = 3	N	+	+	+

Здесь приняты следующие обозначения:
+ - пакеты подписываются,
- - пакеты не подписываются,
N - рабочая станция не подключается к сети.

3.7 Средства обеспечения информационной безопасности.

3.7.1 Межсетевые экраны.

Учитывая важность проблемы защиты, разработана специальная система firewall ("огненная стена"). Система firewall заменяет маршрутизатор или внешний порт сети (gateway). Защищенная часть сети размещается за ним. Пакеты, адресованные Firewall, обрабатываются локально, а не просто переадресуются. Пакеты же, которые адресованы объектам, расположенным за Firewall, не доставляются. По этой причине хакер вынужден иметь дело с системой защиты ЭВМ Firewall. Схема взаимодействия Firewall с локальной сетью и внешним Интернет показана на рис. 6.3.1.

Рис. 6.3.1. Схема Firewall

Такая схема проще и надежнее, так как следует заботиться о защите одной машины, а не многих. Экран, маршрутизатор и ЭВМ управления экраном объединены небольшой, незащищенной локальной сетью. Основные операции по защите осуществляются здесь на IP-уровне. Эту схему можно реализовать и на одной ЭВМ, снабженной двумя интерфейсами. При этом через один интерфейс осуществляется связь с Интернет, а через второй – с защищенной сетью. Такая ЭВМ совмещает функции маршрутизатора-шлюза, экрана и управления экраном. Возможна реализация Firewall, показанная на рис 6.3.2. Здесь функция экрана выполняется маршрутизатором.

Рис. 6.3.2. Схема Firewall, где функцию экрана выполняет маршрутизатор

В этой схеме доступ из Интернет возможен только к прокси-серверу, ЭВМ из защищенной сети могут получить доступ к Интернет тоже только через прокси-сервер. Ни один пакет посланный из защищенной ЭВМ не может попасть в Интернет и, аналогично, ни один пакет из Интернет не может попасть непосредственно защищенной ЭВМ. Возможны и другие более изощренные схемы, например со вторым “внутренним” Firewall для защиты от внутренних угроз.

Недостатки FireWall происходят от ее преимуществ, осложняя доступ извне, система делает трудным и доступ наружу. По этой причине система FireWall должна выполнять функции DNS (сервера имен) для внешнего мира, не выдавая никакой информации об именах или адресах внутренних объектов, функции почтового сервера, поддерживая систему псевдонимов для своих клиентов. Псевдонимы не раскрываются при посылке почтовых сообщений во внешний мир. Служба FTP в системе может и отсутствовать, но если она есть, доступ возможен только в сервер FireWall и из него. Внутренние ЭВМ не могут установить прямую FTP-связь ни с какой ЭВМ из внешнего мира. Процедуры telnet и rlogin возможны только путем входа в сервер FireWall. Услуги типа NFS, rsh, rcp, finger и т.д. не допускаются. Ни одна из ЭВМ в защищенной сети не может быть обнаружена с помощью PING (ICMP) извне. И даже внутри сети будут возможны только определенные виды трафика между строго определенными машинами. Понятно, что в целях безопасности защищенная сеть не может иметь выходов во внешний мир помимо системы экран, в том числе и через модемы. Экран конфигурируется так, чтобы маршрут по умолчанию указывал на защищенную сеть. Экран не принимает и не обрабатывает пакеты внутренних протоколов маршрутизации (например, RIP). ЭВМ из защищенной сети может адресоваться к экрану, но при попытке направить пакет с адресом из внешней сети будет выдан сигнал ошибки, так как маршрут по умолчанию указывает назад в защищенную сеть. Для пользователей защищенной сети создаются специальные входы для FTP (см. библиографию раздела 6 “Сетевая безопасность в Интернет”), telnet и других услуг. При этом не вводится каких-либо ограничений по транспортировке файлов в защищенную сеть и блокируется передача любых файлов из этой сети, даже в случае, когда инициатором FTP-сессии является клиент защищенной сети. Единственные протоколы, которым всегда позволен доступ к ЭВМ Firewall являются SMTP (электронная почта) и NNTP (служба новостей). Внешние клиенты Интернет не могут получить доступа ни к одной из защищенных ЭВМ ни через один из протоколов. Если нужно обеспечить доступ внешним пользователям к каким-то данным или услугам, для этого можно использовать сервер, подключенный к незащищенной части сети (или воспользоваться услугами ЭВМ управления экраном, что нежелательно, так как снижает безопасность). ЭВМ управления экраном может быть сконфигурирована так, чтобы не воспринимать внешние (приходящие не из защищенной сети) запросы типа FTP, telnet и пр., это дополнительно повысит безопасность. Стандартная система защиты здесь часто дополняется программой wrapper (см. раздел 6 “Сетевая безопасность в Интернет”). Немалую пользу может оказать и хорошая система

регистрации всех сетевых запросов. Системы FireWall часто используются и в корпоративных сетях, где отдельные части сети удалены друг от друга. В этом случае в качестве дополнительной меры безопасности применяется шифрование пакетов. Система FireWall требует специального программного обеспечения. Следует иметь в виду, что сложная и дорогостоящая система FireWall не защитит от “внутренних” злоумышленников. Нужно тщательно продумать систему защиты модемных каналов (сама система FireWall на них не распространяется, так как это не внешняя часть сети, а просто удаленный терминал). Если требуется дополнительная степень защиты, при авторизации пользователей в защищенной части сети могут использоваться аппаратные средства идентификации, а также шифрование имен и паролей.

3.7.2 Средства обнаружения атак и анализа защищенности.

Перед отделами защиты информации возникает задача проверки, насколько реализованные или используемые механизмы защиты информации соответствует положениям принятой в организации политики безопасности. И такая задача будет периодически возникать при изменении обновлении компонентов информационной системы, изменении конфигурации операционной системы и т.п.

Однако администраторы сетей не имеют достаточно времени на проведение такого рода проверок для всех узлов корпоративной сети. Следовательно специалисты отделов защиты информации нуждаются в средствах, облегчающих анализ защищенности используемых механизмов обеспечения информационной безопасности. Автоматизировать этот процесс помогут средства анализа защищенности, называемые на Западе сканерами безопасности (security scanners). Использование этих средств поможет определить уязвимости на узлах корпоративной сети и устранить их до тех пор, пока ими воспользуются злоумышленники.

Функционировать такие средства могут на сетевом уровне, уровне операционной системы (ОС) и уровне приложения. Наибольшее распространение получили средства анализа защищенности сетевых сервисов и протоколов. Связано это, в первую очередь, с универсальностью используемых протоколов. Повсеместное использование таких протоколов, как IP, TCP, HTTP, FTP, SMTP и т.п. позволяют с высокой степенью эффективности проверять защищенность информационной системы, работающей в сетевом окружении. Вторыми по распространенности получили средства анализа защищенности операционных систем. Связано это также с универсальностью и распространенностью некоторых операционных систем. Однако, из-за того, что каждый производитель вносит в операционную систему свои изменения (ярким примером является множество разновидностей ОС UNIX), средства анализа защищенности ОС анализируют в первую очередь параметры, характерные для всего семейства одной ОС. И лишь для некоторых систем анализируются специфичные для нее параметры. Средств анализа защищенности приложений на сегодняшний день не так много, как этого хотелось бы. Такие средства пока существуют только для широко распространенных прикладных систем, типа Web-броузеры (Netscape Navigator, Microsoft Internet Explorer), СУБД (Microsoft SQL Server, Oracle) и т.п.

Применяя средства анализа защищенности можно быстро определить все узлы корпоративной сети, доступные в момент проведения тестирования, выявить все используемые в ней сервисы и протоколы, их настройки и возможности для несанкционированного воздействия (как изнутри корпоративной сети, так и снаружи). Также эти средства вырабатывают рекомендации и пошаговые меры, позволяющие устранить выявленные недостатки.

Средства анализа защищенности сетевых протоколов и сервисов.

Взаимодействие абонентов в любой сети базируется на использование сетевых протоколов и сервисов, определяющих процедуру обмена информацией между двумя и более уз-

лами. Несмотря на то, что при разработке сетевых протоколов и сервисов к ним предъявлялись требования (однако явно недостаточные) по обеспечению безопасности обрабатываемой информации, постоянно появляются сообщения об обнаруженных в протоколах уязвимостях. Поэтому существует необходимость в постоянной проверке всех используемых в корпоративной сети протоколов и сервисов.

Системы анализа защищенности выполняют серию тестов по обнаружению уязвимостей, аналогичных тем, которые применяют злоумышленники при осуществлении атак на корпоративные сети. Сканирование начинается с получения предварительной информации о сканируемой системе, например, разрешенных протоколах и открытых портах, версии операционной системы и т.п., и заканчивая попытками имитации проникновения, используя широко известные атаки. Однако не стоит думать, что при помощи средств анализа защищенности на уровне сети можно тестировать только возможность несанкционированного доступа в корпоративную сеть из сети Internet. Эти средства могут быть использованы и во внутренней сети организации. Системы анализа защищенности на уровне сети могут быть использованы как для оценки уровня безопасности организации, так и для контроля эффективности настройки сетевого программного и аппаратного обеспечения.

В настоящий момент существует более десятка различных средств, автоматизирующих поиск уязвимостей сетевых протоколов и сервисов. Среди коммерческих систем анализа защищенности можно назвать Internet Scanner компании Internet Security Systems, Inc., CyberCop Scanner компании Network Associates (ранее называвшаяся Ballista компании Secure Networks Inc.), NetSonar компании Cisco и ряд других.

Средства анализа защищенности данного класса не только анализируют уязвимость сетевых сервисов и протоколов, но и системного и прикладного программного обеспечения, отвечающего за работу с сетью. К такому обеспечению можно отнести Web-, FTP- и почтовые сервера, межсетевые экраны, броузеры и т.п. Кроме анализа программного обеспечения, некоторые предлагаемые на рынке средства проводят сканирование и аппаратных средств. Как правило, к ним относится коммутирующее и маршрутизирующее оборудование.

Средства анализа защищенности операционной системы

Средства этого класса предназначены для проверки настроек операционной системы, влияющих на ее защищенность. К таким настройкам можно отнести учетные записи пользователей (account), например длина пароля и срок его действия, права пользователей на доступ к критичным системным файлам, уязвимые системные файлы, установленные patch'и и т.п. Системы анализа защищенности на уровне ОС могут быть использованы не только отделами защиты информации, но и управлениями автоматизации для контроля конфигурации операционных систем.

Данные системы в отличие от средств анализа защищенности сетевого уровня проводят сканирование не снаружи, а изнутри анализируемой системы, т.е. не имитируют атаки внешних злоумышленников. Кроме возможностей по обнаружению уязвимостей некоторые системы анализа защищенности на уровне ОС (например, System Scanner компании Internet Security Systems) позволяют автоматически устранять часть обнаруженных проблем или корректировать параметры системы, не удовлетворяющие политике безопасности, принятой в организации.

Как уже упоминалось, средств анализа защищенности операционной системы существует меньше, чем средств проверки сети. Одной из первых известных систем можно назвать COPS (Computerized Oracle and Password System), разработанной соавтором системы SATAN Д. Фармером совместно с Ю. Спаффордом из лаборатории COAST.
Также широко известны системы System Security Scanner и Security Policy Manager компании Internet Security Systems, Inc., Kane Security Analyst компании Intrusion Detection и ряд других.

Internet Scanner.

Система Internet Scanner, разработанная компанией Internet Security Systems, Inc., обеспечивает автоматизированное обнаружение и анализ уязвимостей, а также инвентаризацию программно-аппаратного обеспечения в корпоративной сети. Использование политико-основанного (policy-based) подхода к проведению анализа защищенности позволяет персоналу, отвечающему за защиту информации, сравнивать положения политики безопасности с текущим состоянием постоянно изменяющегося сетевого окружения. Система Internet Scanner помогает в трех областях:

- Предсказание рисков (Risk Prediction) - Каково текущее состояние сети? Какие нарушения политики безопасности существуют?
- Ранжирование рисков (Risk Quantification) - Какие нарушения вызовут наибольший вред? Как данные нарушения могут быть устранены или уменьшен ущерб в случае их эксплуатации злоумышленником?
- Управление рисками (Risk Management) - Соответствует ли существующая политика безопасности реальному сетевому окружению? Увеличивается ли со временем уровень защищенности корпоративных ресурсов?

System Scanner.

Система System Scanner, разработанная компанией Internet Security Systems, Inc., комбинирует автоматизированное управление политикой безопасности с обнаружением и устранением уязвимостей операционных систем, построенных на платформах Windows и Unix. Система System Scanner построена по технологии клиент/сервер и позволяет централизованно собирать и анализировать данные о нарушениях политики безопасности со всех (в т.ч. и территориально удаленных) узлов корпоративной сети. Система System Scanner входит в состав семейства SAFEsuite, предназначенного для обеспечения адаптивного управления безопасностью корпоративной сети. Система System Scanner может быть использована для:

- Анализа и управления настройками различных операционных систем, используемых в организации для обеспечения ее нормального функционирования;
- Обнаружения уязвимостей, позволяющих "обойти" существующие защитные механизмы. К таким уязвимостям могут быть отнесены:
  - неправильная конфигурация операционной системы или системного программного обеспечения,
  - изменение любых файлов,
  - "слабые" пароли и т.д.;
- Анализа изменений уровня защищенности корпоративной сети и т.д.

Database Scanner.

Система Database Scanner, разработанная компанией Internet Security Systems, Inc., является первым в мире продуктом, предназначенным для анализа защищенности систем управления базами данных, использующихся в корпоративной сети. Система Database Scanner позволяет собирать и анализировать данные о нарушениях политики безопасности от всех (в т.ч. и территориально удаленных) баз данных корпоративной сети, работающих под управлением СУБД MS SQL Server, Oracle и Sybase на платформах Windows NT, Windows 2000 и Unix. Система Database Scanner входит в состав семейства SAFEsuite, предназначенного для обеспечения адаптивного управления безопасностью корпоративной сети.

RealSecure.

Система RealSecure, разработанная компанией Internet Security Systems, Inc., обеспечивает автоматизированное обнаружение и реагирование в реальном режиме времени

на атаки, направленные на узлы корпоративной сети. Система RealSecure одинаково эффективно обнаруживает как внешние атаки, так и внутренние злоупотребления, направленные на сервера приложений, Web-сервера, базы данных, рабочие станции, маршрутизаторы, межсетевые экраны и т.д. Система RealSecure использует технологии анализа сетевых пакетов и анализа журналов регистрации. Данная система ориентирована на защиту как целого сегмента сети (network-based), так и на защиту конкретного узла (host-based) корпоративной сети. Система RealSecure входит в состав семейства SAFEsuite, предназначенного для обеспечения адаптивного управления безопасностью корпоративной сети.

4. Управление NDS.

4.1 Понятие об NDS и Bindery. Схема NDS, классы и объекты.

Novell Bindery - это системный файл (или два файла для ранних версий NetWare и три файла для NetWare 3.x), позволяющий отслеживать каждого пользователя. В Bindery хранится подробная информация о полномочиях пользователя, правах доступа к файлу и уровнях защиты.

Связующий объект - это база данных, отслеживающая пользователей, группы и рабочие станции на отдельном сервере NetWare. NetWare v.4 имеет эмуляцию связующего объекта, обеспечивающую совместимость с предыдущими версиями NetWare. В остальном же в операционной системе NetWare v.4 Novell отказалась от Bindery. Связующие объекты, которые использовались в предыдущих версиях, в версии 4.0 NetWare заменяет NetWare Directory Services (NDS). В то время как Bindery используется для отслеживания пользователей и служебных средств только на одном файловом сервере, NDS - это распределенная и дублируемая база данных по именам. Ни один из пользователей не обладает всех полнотой информации о данном сервере, группе или пользователях. Фактически, пользователи даже не будут знать, какой из серверов является "их" сервером.

NetWare Directory Services (NDS) - это реализация службы распределенных каталогов, соответствующая стандартам X.500 ISO (International Organization for Standards). Данные служебные средства отслеживают всех пользователей сети, серверы и ресурсы, даже на больших объединенных сетях. Эта информация хранится в глобальной базе данных, к которой имеют доступ пользователи и администраторы сети, когда им требуется использовать служебные средства сети или управлять ими.

NDS интерпретирует всех пользователей сети и ресурсы как объекты. Объект пользователя - это просто учетная запись пользователя сети (его имя, адрес, адрес узла, сценарий регистрации и другая необходимая административная информация). Ресурсы (серверы, принтеры и тома) также представляются как объекты. Эти объекты имеют характеристики, определяющие, кто может использовать и изменять их. Объекты сохраняются в базе данных NDB (NetWare Directory Database) и организуются в виде иерархической древовидной структуры. При этом такая структура не обязательно должна отражать физическое расположение пользователей и ресурсов в сети. Вместо этого вы можете взять за основу административную структуру фирмы или что-то другое.

Объединение пользователей и ресурсов в каталоге с древовидной схемой может упростить обслуживание сети. Она также упрощает отслеживание и назначение полномочий доступа. Администратор сети или супервизор могут блокировать полномочия доступа, если они не соответствуют пользователю.

Дерево каталога состоит из именованных объектов NDS, представляющих организацию сети. Именованный объект может принадлежать к одной из четырех категорий:

C - название страны (например, FR).

O - название организации (например, PoppuriPC);

OU - название подразделения (например, Sales);

CN - общее имя (например, LISA или Print_Operator).

Вывести на экран дерево каталога вы можете с помощью административной утилиты. Эта утилита выводит дерево в графическом виде и позволяет вам расширять или усекать его части. Одни объекты могут включать в себя другие. Возможность просматривать ветви дерева каталогов облегчает поиск и управление объектами.

Объект может представлять собой контейнер, то есть объект, содержащий другие объекты, или быть листом, то есть объектом, включенным в другой объект. Объект-лист не может содержать других объектов, поэтому его иногда называют конечным объектом. Конечные объекты представляют физические сущности, такие как пользователи, принтеры и серверы.

4.2 Свойства объектов и права на объекты NDS.

Каждый объект имеет характеристики, важнейшая из которых его имя. Характеристики объекта можно задавать при его создании или изменяя их с помощью утилиты NetWare Administrator или NETADMIN. В окне, выводимом на экран утилитой NetWare Administrator, для просмотра различных полей характеристик (таких как ограничения регистрации или права доступа к файловой системе) вы можете щелкать "мышью" на расположенных в правой части командных кнопках, после чего изменять информацию о данных характеристиках. Администратор сети может изменить поле характеристики любого объекта. Для других пользователей изменение или просмотр этих полей можно запретить или ограничить. Перечислим некоторые поля характеристик для объекта-пользователя, которые выводятся на экран утилитой NetWare Administrator:

- имя пользователя, адрес, номера телефона и факса;
- учетная информация;
- ограничения регистрации (время, допустимые рабочие станции, требования к паролю);
- сервер, используемый по умолчанию пользователем;
- группа (или группы), к которой относится пользователь;
- конфигурация задания печати пользователя и управляющие данные принтера;
- используемый пользователем профильный объект.

Физический объект, например, сервер, может иметь следующие характеристики:

- присвоенное серверу название подразделения организации;
- описание сервера;
- расположение сервера;
- сетевой адрес сервера;
- полномочия доступа к серверу;
- список операций сервера;
- информация о состоянии операции сервера.

Полномочиями доступа пользователя к объекту управляет администратор сети.

4.3 Управление разделами NDS.

Для отслеживания объектов NDS использует распределенную базу данных NDB (NetWare Directory Database). В сети с несколькими серверами баз данных расположена не на одном сервере, а в сети серверов, что обеспечивает ее "выживание" в случае отказа сервера. Для этого используется сегментация базы данных по разделам и хранение каждого раздела на соответствующем сервере сети. Для создания резервных копий и улучшения производительности можно копировать разделы на другие серверы. Для создания, удаления, комбинирования, разделения, синхронизации или перестраивания разделов используется утилита управления разделами. Для параллельных операций с разделами используется синхронизация. Для установления порядка событий и обеспечения корректной работы администраторов при изменении разделов NDS использует отметки о дате и времени. Начальная организация каталога NDS задается при установке NetWare. При этом автоматически соз-

дается пользователь ADMIN (администратор). После установки NetWare с помощью NetWare Administrator или NETADMIN можно создать объекты подразделений для других подразделений организации.

5. Управление пользователями и группами в дереве NDS.

5.1 Шаблоны и сценарии регистрации пользователя.

Шаблон USER_TEMPLATE представляет собой объект Каталога, который создается почти так же, как и пользователи, и имеет те же свойства. Эти свойства можно будет использовать по умолчанию при создании новых пользователей в том же контексте, где создан данный шаблон. Профиль Profile является объектом своего специального класса и предназначен для хранения общей процедуры регистрации, которую можно назначить для любых пользователей (в отличие от личной и контейнерной, привязанных к конкретным пользователям и их положению в Каталоге). Изменения в шаблоне могут действовать только на свойства создаваемых после этого пользователей данного контейнера, а изменения в профиле - на всех пользователей любых контейнеров, которым назначено его использование.

5.2 Настройка требований к паролям пользователей.

С помощью утилиты SETPASS назначается пароль пользователю, осуществляются настройки пароля. Можно обязать пользователей регулярно сменять эти пароли. Администраторы и супервизоры могут задавать уникальные пароли пользователей. В учетных данных пользователя вы можете задать параметр, вынуждающий пользователя периодически менять свой пароль. Можно задать назначения пользователям случайных паролей.

5.3 Создание пользователей и групп.

В NetWare 3.x создание, обслуживание и удаление пользователей из базы осуществляется с рабочей станции утилитой SYSCON.EXE. Утилита SYSCON.EXE обеспечивает управление пользователями и группами, взаимодействуя с Bindery. С ее помощью задаются все их свойства (кроме относящихся к системе печати):

- Имя пользователя (группы) - может быть модифицировано по клавише F3;
- Полное имя (Full Name) пользователя (группы) - произвольное символьное поле;
- Идентификатор (User ID, Group ID) - восьмиразрядное шестнадцатеричное число, назначаемое системой при создании объекта. User ID используется как имя почтового каталога пользователя в каталоге SYS:MAIL (с отброшенными начальными нулями);
- Отношения подчиненности по управлению бюджетом задаются двумя списками: Managed Users and Groups (кому является менеджером) и Managers (кого имеет менеджером);
- Вхождения пользователей в группы задается для групп списком членов, для пользователей - списком принадлежности к группам;
- Ограничения регистрации (защита);
- Ограничение бюджета (временный запрет регистрации, введенный менеджером);
- Дата истечения бюджета - со следующего за ней дня регистрация под данным именем запрещается;
- Ограничения на время работы (задается график разрешенного времени в получасовых интервалах на все дни недели);
- Ограничение на количество станций, на которых можно одновременно зарегистрироваться под данным именем;
- Процедура регистрации;
- Опекунские назначения в файлы и каталоги;

Установка ограничений и изменение балансов бюджетов по умолчанию в опциях администратора SYSCON позволяет управлять созданием личного каталога, балансом (при установленной системе учета) и ограничениями бюджета для вновь создаваемых пользователей. Для создания большого числа равноправных пользователей удобны утилиты MAKEUSER.EXE и USERDEF.EXE. В NetWare 4.x обслуживание пользователей выполняется утилитами NETADMIN или NWADMIN. Возможные права и ограничения аналогичны NetWare 3.x с поправкой на систему имен. Создание типовых пользователей облегчается применением шаблонов (User Template) и утилиты UIMPORT.

5.4 Присвоение пользователям полномочий по доступу к объектам NDS и ресурсам файловой системы. Разграничение прав на объекты NDS.

Права, которые могут быть предоставлены пользователю (или группе пользователей) по отношению к каталогу или файлу, перечислены в таблице 6.1. Права и фильтры (маски) наследуемых прав назначаются администратором сети с помощью утилит NetWare. Но назначение прав для каждого пользователя по отношению ко всем требуемым файлам и каталогам - это утомительная задача. В NetWare предлагается механизм наследования прав. Прежде всего введём некоторые определения.

- Опекун (Trustees) - это пользователь (или группа пользователей, или другой объект), которому администратор с помощью утилиты (например, FILER) явно назначает права по отношению к какому-либо файлу или каталогу. Такие права называются опекунскими назначениями.
- Фильтр наследуемых прав (IRF - Inherited Right Filter) - это свойство файла (каталога), определяющее, какие права данный файл (каталог) может унаследовать от родительского каталога. Фильтр назначается администратором с помощью утилиты (например, FILER).

Наследуемые права - права, передаваемые (распространяемые) от родительского каталога.
Эффективные права - права, которыми пользователь реально обладает по отношению к файлу или каталогу.

Таблица 6.1. Список возможных прав по отношению к каталогу или файлу

Право	Обозначение	Описание
Supervisor	S	Предоставляет все права по отношению к каталогу или файлу, включая возможность назначения этого права другим пользователям. Не блокируется фильтром наследуемых прав IRF. Это право не может быть удалено ниже по дереву каталогов.
Read	R	Чтение существующего файла (просмотр содержимого текстового файла, просмотр записей в файле базы данных и т. д.).
Write	W	Запись в существующий файл (добавление, удаление частей текста, редактирование записей базы данных).
Create	C	Создание в каталоге новых файлов (и запись в них) и подкаталогов. На уровне файла позволяет восстанавливать файл, если он был ошибочно удалён.
Erase	E	Удаление существующих файлов и каталогов.
Modify	M	Изменение имён и атрибутов (файлов и каталогов), но не содержимого файлов.
File Scan	F	Просмотр в каталоге имён файлов и подкаталогов. По отношению к файлу - возможность видеть структуру каталогов

		от корневого уровня до этого файла (путь доступа).
Access Control	A	Возможность предоставлять другим пользователям все права, кроме Supervisor. Возможность изменять фильтр наследуемых прав IRF.

Права доступа к объектам NDS и их свойствам.

Системная база данных сетевых ресурсов (СБДСР) представляет собой совокупность объектов, их свойств и значений этих свойств. В NetWare 4.x эта база данных называется NDS (NetWare Directory Services), а в NetWare 3.x - Bindery. Отличия NDS от Bindery описаны в отдельном разделе, который посвящён глобальному сетевому каталогу (NDS). Объекты NDS связаны между собой в иерархическую структуру, которую часто называют деревом NDS. На верхних уровнях дерева (ближе к корню [Root]) описываются логические ресурсы, которые принято называть контейнерными объектами. На самом нижнем (листьевом) уровне располагаются описания физических ресурсов, которые называют оконечными объектами. В качестве контейнерных объектов используются объекты типа [Root] (корень), C (страна), O (организация), OU (организационная единица). Оконечные объекты - это User (пользователь), Group (группа), NetWare Server (сервер NetWare), Volume (том файлового сервера), Directories (директория тома) и т. д. Оконечные объекты имеют единое обозначение - CN.

В NetWare 4.x разработан механизм защиты дерева NDS. Этот механизм очень похож на механизм защиты файловой системы, который был рассмотрен ранее. Чтобы облегчить понимание этого механизма, оконечный объект можно интерпретировать как файл, а контейнерный объект - как каталог, в котором могут быть созданы другие контейнерные объекты (как бы подкаталоги) и оконечные объекты (как бы файлы). В отличие от файловой системы здесь права по отношению к какому-либо объекту можно предоставить любому контейнерному или оконечному объекту дерева NDS. В частности допустимо рекурсивное назначение прав объекта по отношению к этому же объекту. Администратор сети может для каждого объекта в дереве NDS определить значения свойств этого объекта. Для объекта User - это имя Login, требования к паролю, пароль пользователя, пользовательский сценарий подключения и т. д. Права и фильтры наследуемых прав назначаются администратором с помощью утилит NetWare 4.x (NWADMIN или NETADMIN). Но назначение прав объектов по отношению ко всем требуемым объектам и свойствам - это утомительная задача. Предлагаемый в NetWare 4.x механизм наследования прав в дереве NDS напоминает механизм наследования прав в файловой системе.

Таблица 6.2. Список возможных прав по отношению к свойству объекта

Права	Обозначение	Описание
Supervisor	S	Гарантирует все привилегии по отношению к свойству объекта. Это право может быть блокировано фильтром наследуемых прав IRF, который может быть назначен для свойства. Фильтры IRF назначаются для объекта и его свойства отдельно.
Compare	C	Позволяет при поиске объекта (например, с помощью утилиты NLIST) сравнивать значение свойства с любой константой. Однако это право не обеспечивает чтения значения свойства. После операции сравнения возвращается результат: True или False.
Read	R	Позволяет читать значение свойства из базы данных NDS. Право Read включает право Compare.
Write	W	Позволяет добавлять, изменять или удалять значение свойства. Право Write включает право Add Self.

Add Self	A	Позволяет опекуну (User) добавлять или удалять самого себя как значение свойства. Это право имеет смысл только для свойств, которые содержат имена пользователей в качестве значений, например, для свойства Members (участники) объекта Group (группа).

Определения опекуна (Trustees), фильтра наследуемых прав (IRF), наследуемых прав, эффективных прав совпадают с соответствующими определениями для файловой системы. Только понятия файл, каталог, пользователь (группа пользователей) следует заменить соответственно на оконечный объект, контейнерный объект, произвольный объект. Ниже приведены эти определения.

6. Аудит в системах NetWare.

Система учета NetWare позволяет отслеживать деятельность пользователей на конкретных серверах. Благодаря этому можно оценить использование ресурсов и при необходимости изменить их, или затребовать на основе этих данных оплату за использование ресурсов. В NetWare 4 учет ведется на отдельных серверах, и делается это во многом аналогично предыдущим версиям NetWare.

Аудиторская система NetWare позволяет отслеживать происходящие в сети события специальному сетевому пользователю - аудитору. Категориями событий могут быть отслеживание тома и отслеживание контейнера. Каждая аудиторская группа может иметь свой пароль. Поэтому, например, аудитор, который отслеживает событие томов, не может отслеживать события контейнера. Однако можно задать аудитора, который будет отслеживать все события.

6.1 Аудит объектов NDS.

События томов.

Сначала аудитор выбирает том для отслеживания, затем разрешает отслеживание перечисленных ниже событий (аудитор может также отслеживать действия отдельных пользователей, файлов или каталогов):

- Создание и удаление каталогов.
- Создание, открытие, удаление, переименование, запись и сохранение файлов.
- События очередей.
- События серверов, такие как изменение даты и времени, останов сервера, а также монтирование и демонтирование томов.

Пользовательские события, такие как регистрация, завершение работы, прерывание связи, предоставление полномочий и аннулирование учетных записей.

События службы каталогов.

События службы каталогов отслеживаются для отдельных контейнеров. Аудитор сначала выбирает контейнер, затем разрешает отслеживание в контейнере следующих событий:

- события службы каталогов, например, изменение паролей, защиты, ограничений доступа, перемещение, удаление или переименование записей.
- действия конкретного пользователя, такого как супервизор.

7. Настройка безопасности в сетях NetWare..

Защита с помощью пароля обеспечивает регистрацию в системе только уполномоченных пользователей, а чтобы ограничить регистрацию определенным временем и конкретными рабочими станциями, можно использовать сценарии регистрации. Можно также ограни-

чить те области сети, к которым будет иметь доступ пользователь после регистрации. Как описывается ниже, для этого используется два типа полномочий доступа.

- Полномочия объекта, каталога или файла определяют тех пользователей, которым предоставлены права доступа к объекту, файлу или каталогу.
- Права на объекты и характеристики.

Служба каталога NetWare Directory Services обеспечивает более высокий уровень защиты, чем это предусматривалось в предыдущих версиях NetWare. Администраторы могут предоставлять руководителям подразделений и начальникам отделов права на создание и управление объектами, находящимися в контейнерах, представляющих их подразделения. Решающее значение в NetWare v.4 имеет планирование. При правильном планировании задается структура NetWare Directory Services, которая соответствует структуре и нуждам организации и упрощает назначение полномочий доступа.

Полномочия доступа и защита имеют для операционной системы жизненно важное значение. При правильном управлении защитой предотвращение потери или порчи данных из-за действий неуполномоченных пользователей и их секретность будут обеспечены. Первая "линия обороны" против неуполномоченных пользователей - это регистрация в системе с помощью пароля. Кроме того, назначение полномочий доступа к файлам позволяет ограничить доступ пользователей к файловой системе. Полномочия доступа позволяют также управлять использованием различных ресурсов сети. Полномочия доступа в NetWare группируются следующим образом:

- полномочия доступа к объектам управляют доступом к объектам системных ресурсов;
- полномочия владения управляют тем, кто может просматривать и изменять характеристики объектов;
- полномочия SMS управляют доступом к объектам в приложениях SMS (Storage Management System);
- полномочия доступа к каталогам определяют, кто может обращаться к каталогам на томах (дисках) и файлам в них;
- права доступа к файлам обеспечивают контроль доступа к файлам в каталогах на пофайловой основе.

При назначении пользователям полномочий доступа к каталогам, объектам или файлам NetWare нужно учитывать ряд моментов. Право доступа пользователя к объекту можно предоставить путем выбора или спецификации объекта и назначением полномочий. Если пользователи имеют права доступа к файлам и каталогам (Access Rights), то они могут назначить полномочия доступа к этим объектам (изменив соответствующие их характеристики). Чтобы задать для объекта права доступа к нему, пользователь должен иметь полномочия записи (Write) к списку управления доступом ALC (Access Control List) объекта. Список ALC аналогичен списку полномочий файлов и каталогов. В случае каталогов и подкаталогов, если пользователь имеет определенные полномочия в родительском каталоге, то эти полномочия он имеет также в подкаталоге. Однако, чтобы ограничить его полномочия в этом подкаталоге, супервизор может использовать фильтр IRF. Фильтр наследуемых полномочий IRF (Inherited Rights Filter) определяет, какие полномочий пользователи могут наследовать из порождающих каталогов и объектов-контейнеров. Действующие полномочия пользователя на доступ к файлу, каталогу или объекту вычисляются на основе следующих параметров (по умолчанию никаких полномочий кроме доступа пользователя с своему частному каталогу и общедоступному каталогу ему не предоставляется):

- прав доступа, присвоенных каталогу, файлу или объекту;
- прав доступа к порождающему каталогу или объекту-контейнеру;
- прав доступа с перечисленным объектам, назначенным пользователю или его группе;
- эквивалентов защиты пользователя;
- фильтра IRF для каталога, файла или объекта.

8. Защита серверов и рабочих станций.

8.1 Защита сети и ее данных.

Наиболее важной частью вашей сети являются данные и устройства их хранения. Все другое можно заменить. Вы можете заменить аппаратуру сервера, но не сможете снова запустить сеть, если у вас нет резервных копий данных. Кроме того, время простоя сети может обойтись в круглую сумму. Иногда возникает необходимость в NetWare SFT Level III (о чем мы уже говорили и будем говорить ниже). Следующие разделы описывают шаги, которые необходимо предпринять для защиты дорогостоящего оборудования и предотвращения потери данных.

8.2 Защита от кражи

Так как файловый сервер часто содержит ценные данные, его нужно защитить от кражи. Хотя важное значение имеет архивизация данных, сам сервер также необходимо защищать, так как он обеспечивает средства доступа к данным:

- Прикрепить шасси сервера к столу и заприть корпус. Это предотвратит извлечение жесткого диска, который легко можно вынести из здания.
- Запереть сервер в защитном корпусе с нужной системой охлаждения, предотвращающей перегрев сервера.
- Создание центра данных, входав помещение которого требуется ограничить.
- Разместить сервер в центральном обслуживающем центре, где круглые сутки присутствует персонал.
- Сотрудники должны быть компетентными и знать процедуры защиты.

8.3 NetWare SFT Level III

NetWare SFT Level III - это дополнительный программный продукт Novell, обеспечивающий отказоустойчивость. Это обеспечивает постоянную доступность для пользователя важных приложений. Конфигурация NetWare SFT Level III состоит из двух серверов, связанных высокоскоростной линией передачи данных. Один сервер зеркально отображает данные другого и становится немедленно доступным после выхода одного сервера из строя. На пользователях это никак не отразится. NetWare SFT Level III - это чисто программное решение, работающее на стандартном сервере. NetWare SFT Level III защищает от сбоев оперативной памяти, выхода из строя диска и сетевых адаптеров. Для защиты от стихийных бедствий и проблем с электропитанием пользователи можно географически удалить друг от друга (однако это требует высокоскоростной линии связи). Кроме того, пока работает один сервер, на другом можно выполнять обслуживающие процедуры и изменения. После этого файловая система данного сервера синхронизируется с другим. Для улучшения производительности NetWare SFT Level III Novell рекомендует использовать двухпроцессорные системы. Один процессор выполняет весь ввод-вывод и зеркальное отображение, а другой - служебные утилиты и серверные приложения. На каждом сервере вам потребуются также MSL (Mirrored Servel Link). MSL - это обычно каналы Ethernet (100 Мбит/сек) или волоконнооптические линии.

8.4 Процедуры архивизации.

Хотя NetWare предусматривает ряд встроенных механизмов защиты данных, таких как дублирование каталогов файлов и переназначение плохих блоков, вы должны архивировать данные жесткого диска, чтобы они были доступны даже при выходе диска из строя. Чтобы вам не пришлось переконфигурировать всю сеть, нужно также создавать резервные копии системной информации и конфигурации, включая учетные данные и пароли поль-

зователей. Вы должны иметь расписание архивизации. Перечислим типы архивизации, имеющие важное значение в стратегии архивизации:

- Нужно архивировать весь сервер, включая структуру его каталогов, учетные данные пользователей и другую системную информацию. Это следует делать регулярно и после внесения изменений.
- Нужно регулярно копировать файлы данных или делать это так часто, насколько часто происходят изменения.
- Процедура инкрементальной архивизации всей системы обеспечивает полную архивизацию всей системы на регулярной основе и промежуточное сохранение измененных и новых файлов.

Система архивизации с ротацией обеспечивает одновременное существование многих копий. Некоторые копии можно хранить в другом месте (на случай пожара), однако перемещать данные нужно аккуратно с учетом возможной кражи. Выполнение тестирования процедуры восстановление позволит убедиться в правильной работе процедур архивизации/восстановления. Для тестирования можно предусмотреть резервный сервер. Хотя это и дорогостоящий вариант, выход из строя основного сервера может обойтись значительно дороже.

8.5 Защита от злоумышленников.

Для получения доступа к сети злоумышленники могут использовать различные методы. Предотвратить доступ таких лиц к локальной сети можно с помощью регистрации пользователей и обеспечения их выхода из сети. Можно установить регистрацию пользователя только на определенной рабочей станции и в определенное время. Если злоумышленник получи доступ к сети на уровне супервизора, то он может создать другую учетную запись, а затем стереть ее, изменив регистрируемую в систему информацию. Другую угрозу представляет неуполномоченный доступ пользователей с удаленных рабочих станций, но система с обратным вызовом может обеспечить защиту от таких злоумышленников. Когда пользователи выполняют подключение по номеру с удаленной рабочей станции, система "вешает трубку" и в свою очередь проверяет номер абонента. Однако такое средство обратного вызова не может использоваться для защиты удаленной локальной сети или постоянно подключенной системы. Необходимо предотвратить раскрытие злоумышленниками паролей и перекрыть все обходные методы вхождения в сеть.

8.6 Предотвращение перехвата данных.

Необходимо позаботиться о предотвращении перехвата данных, которые передаются по сети. С этой целью можно использовать волоконно-оптический кабель или методы кодирования данных. (NetWare 4.x включает в себя новое средство защиты - цифровую подпись NCP.)

8.7 Использование бездисковых рабочих станций.

Использование бездисковых рабочих станций предотвращает переписывание и передачу данных пользователем.

8.8 Защита от вирусов.

Компьютерные вирусы могут нанести большой ущерб сети. Особенно это важно учитывать, когда пользователи работают в локальных сетях, расположенных далеко от тома или в дороге на портативных компьютерах. Вирусы могут переноситься через электронные "доски объявлений", общедоступные утилиты и демонстрационные диски. Поэтому важно иметь и использовать обнаруживающее компьютерные вирусы программное обеспечение. Вирусы можно иногда обнаружить даже в программном обеспечении, которое поставляется в виде готовых пакетов. При установке любого программного обеспечения и обнов-

лении программ в системе нужно делать проверку на вирусы. Чтобы предотвратить доступ пользователей к выполняемым файлам в программных каталогах, можно использовать полномочия доступа. Сейчас существует множество антивирусных программ, а некоторые программные пакеты имеют встроенные средства защиты от вирусов. Для защиты серверов NetWare от известных и неизвестных вирусов можно использовать Untouchable Network NLM фирмы Fifth Generation System. Это средство использует идентификационный процесс, который позволяет распознать даже вирусы, которые изменяются при выполнении (так называемые самомодифицирующиеся или мутирующие вирусы). Кроме того, это позволяет регулярно выполнять проверку на вирусы путем отслеживания изменений в выполняемых файлах. Для самой себя и своей базы данных эта программа создает специальный защищенный раздел диска.

Мутирующие вирусы - наиболее опасный и труднораспознаваемый тип вирусов. Генератор мутаций впервые появился в вирусе, получившим условное название Pogue. Сам вирус может быть резидентным или нерезидентным и поражать только файлы .EXE или .COM, или те и другие. Что же представляет собой генератор мутаций? Обычный вирус имеет всегда один и тот же код, благодаря чему из этого кода можно выделить характерный фрагмент - маску вируса, после чего по наличию этой маски определять пораженные файлы и исправлять их. Именно так и работали антивирусные программы. Однако потом появились шифрованные вирусы, которые искать по маске стало невозможно. Два экземпляра одного вируса, зашифрованные с разными ключами, не будут иметь практически ни одного совпадающего байта (кроме шифрующего фрагмента).

До последнего времени против компьютерных вирусов применялись в основном программные средства. Однако стали появляется и аппаратные. Например, существует специальная антивирусная плата Thunderbyte (главный дистрибьютор этих плат - фирма NOVIX). Основное преимущество антивирусных аппаратных средств в том, что в отличие от программ антивирусов они начинают работать еще до загрузки операционной системы, а следовательно, способны отслеживать и обезвреживать в момент активизации даже загрузочные вирусы. Антивирусная программа Thunderbyte записана в СППЗУ и не может быть модифицирована. Она загружается в качестве расширения BIOS до других программ и занимает 1К ОЗУ. Плата устанавливается в восьмибитовый разъем шины ISA, EISA или MCA и постоянно следит за специфической активностью, характерной для компьютерных вирусов.

8.9 Проблемы с электропитанием и их решение.

Неконтролируемое электропитание может вывести аппаратуру из строя или привести к ее остановке. Сервер с надежно защищенными данными будет бесполезен, если нет доступа к этим данным. Электропитание редко бывает постоянным и стабильным. Это можно видеть по миганию электроламп или телевизора, которые изредка замечает каждый. Такие пиковые броски крайне отрицательно действуют на аппаратуру. Броски и перебои в питании могут привести к следующим неприятностям:

- Порча данных. Электрическая нестабильность может изменить состояние памяти или запортить информацию, передаваемую по кабелю в пакетах данных. Такие броски могут изменить программу в памяти и привести к ее сбою. Такие ошибки, которые часто принимают за ошибки в программе, могут вызываться помехами в электропитании.
- Выход из строя аппаратуры. Сильные броски питания могут привести к порче аппаратуры. Особенно уязвимы при этом микросхемы и блоки питания. Чтобы предотвратить это, можно использовать сетевые фильтры, но если бросок очень сильный (что иногда бывает во время грозы), такой фильтр не спасает. Поэтому лучше воспользоваться блоком бесперебойного питания (UPS).
- Медленная "деградация" аппаратуры. Аппаратура, регулярно подвергающаяся броскам и падениям напряжения в сети, со временем выйдет из строя.

Кроме того, источником проблемы часто бывает плохое заземление или его отсутствие. Сетевые фильтры часто используют заземление, направляя броски питания "в землю". Если заземление отсутствует, эти броски вернутся обратно в сеть. Для оценки качества электропитания в здании разработаны различные устройства. Многие из них позволяют проверить качество проводки и заземления. По некоторым оценкам до 90% выхода аппаратуры из строя вызвано плохой проводкой и неправильным заземлением.

Электрическое оборудование создает помехи. Такие механизмы как кондиционеры, лифты и холодильники, и даже лазерные принтеры, могут приводить при включении к броскам питания. Фактически, любое устройство с нелинейным использованием электроэнергии может приводить к броскам питания, влияющим на другие устройства. Проблемы электропитания можно классифицировать следующим образом:

- Шумы и броски питания могут приводить к немедленному выходу из строя чувствительного электронного оборудования. Большинство источников питания компьютеров имеют встроенную защиту от бросков, превышающих норму. Дешевые устройства предохраняют от таких бросков остальную электронику тем, что просто перегорают (в лучшем случае это будет предохранитель).
- Понижение питания - это падение напряжения ниже номинального уровня, что вызывается обычно перегрузкой сети. Длительное понижения питания может привести к выходу из строя блока питания.
- Повышение напряжения также может вывести из строя блок питания.
- Высокочастотные гармонические колебания вызываются проблемами в заземлении, Это может приводить к ошибкам при передаче данных по телекоммуникационным линиям.

8.10 Проблемы с заземлением и их решения.

В опубликованном в 1991 г. фирмой Novell отчете указывалось, что многие проблемы вызываются плохим заземлением. Здесь же предлагались и некоторые решения. Проложенный в зданиях провод заземления с низким сопротивлением предохраняет людей от удара током. Хорошее заземление обычно отводит электрические разряды в землю. Если оборудование не заземлено, то при прикасании к нему человека разряд может пройти в землю через него. В указанном отчете отмечается, что существующая практика заземления несовместима с требованиями цифровой электроники. Подключение электронного оборудования к заземлению может подвергать это оборудование шумам, которые ищут наиболее короткий путь в землю.

Проблемам заземления особенно подвержено сетевое оборудование. Сетевые устройства обычно подключаются к различным источникам питания, которые заземлены. Когда эти сети связываются сетевым кабелем, кабель представляет собой мост между двумя заземленными системами. Это приводит к тому, что энергия сети сбалансируется, перетекая "из земли в землю". Эти потоки проходят через подключенные к кабелю компьютерные системы и вызывают шумы. Чтобы решить эти проблемы, согласно отчету, оборудование на одном конце следует изолировать от оборудования на другом, подключенным к другому источнику питания.

В большой сети "одноточечного" заземления обычно достичь невозможно. Объединенные сети образуют связи между близкими или удаленными пунктами, любой из которых может создать проблемы из-за плохой электросети. Наличие отдельных источников питания может означать разные здания со своими трансформаторами. Каждый транформатор имеет собственные электрические характеристики.

Одно из решений этих проблем состоит в подключении всей сети к одному источнику питания и одному проводу заземления. Однако обычно это непрактично и противоречит назначению сети - предоставлению распределенных вычислительных ресурсов удаленным друг от друга пользователям. Единственным практичным решением является ста-

билизация питания и соответствующая точка заземления в месте токоположения каждой сетевой компоненты.

Следующий рисунок иллюстрирует метод подключения оборудования сети. Обратите внимание на использование стабилизатора питания и источника бесперебойного питания для питания сервера. Если позволяет бюджет, аналогичные устройства должны быть подключены к рабочей станции.

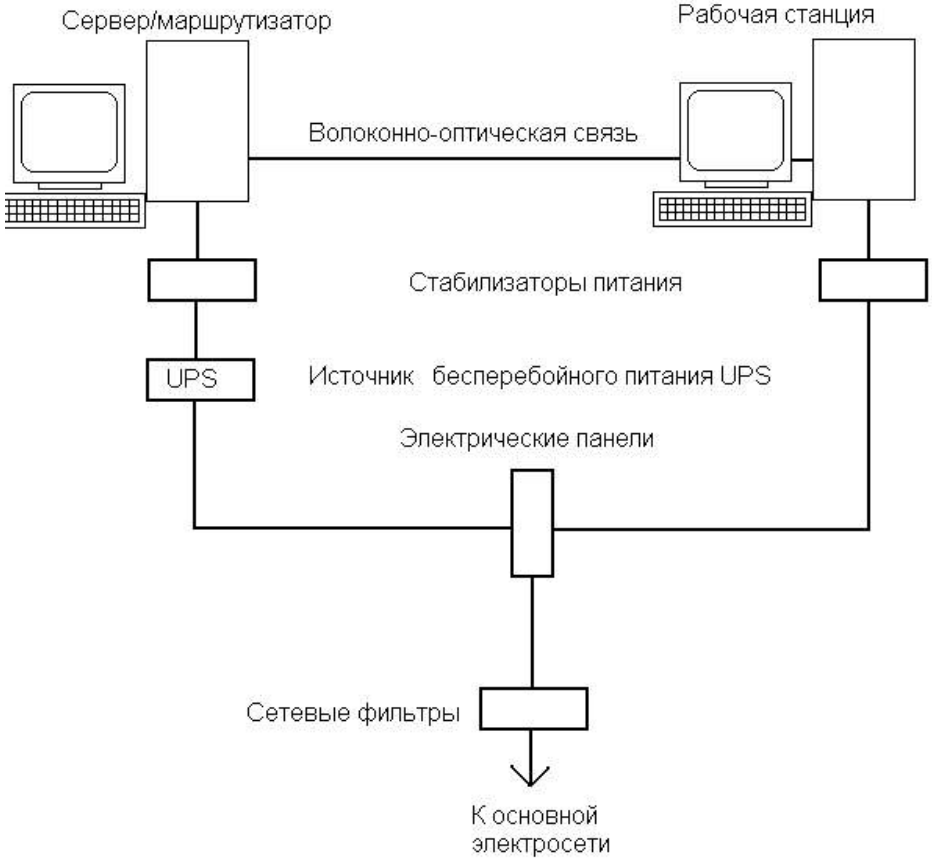

Рис. 8.1 Метод подключения оборудования сети.

Глядя на эту иллюстрацию, можно сказать следующее. Не следует прокладывать сетевые кабели параллельно с проводами питания и другими источниками помех, такими как электромоторы. Иначе броски питания могут проникнуть в сеть. В некоторых схемах нейтральный провод преднамеренно заземляется для уменьшения шумов. Это создает волнообразные помехи низкой частоты, которые могут привести к порче данных.

Сегмент локальной сети должен подключаться к сети питания, отходящей от одного источника питания. Сегменты не должны иметь общую с другими источниками питания точку заземления.

Следующий рисунок иллюстрирует схему объединения двух сетей. Чтобы установить связи по заземлению между сетями, используется непроводящий волоконно-оптический кабель. Основной причиной разделения источников питания является вероятное различие потенциалов заземления, что может приводить к проблемам в чувствительном электрооборудовании. Каждая локальная сеть этой схемы имеет автономное оборудование, и здесь можно легко контролировать проблемы с заземлением и шумами. Заметим, что устройства объединенной сети подключаются к стабилизаторам питания. Если использование волоконно-оптического кабеля невозможно, то для кабеля следует предусмотреть дополнительную защиту от нестабильности питания.

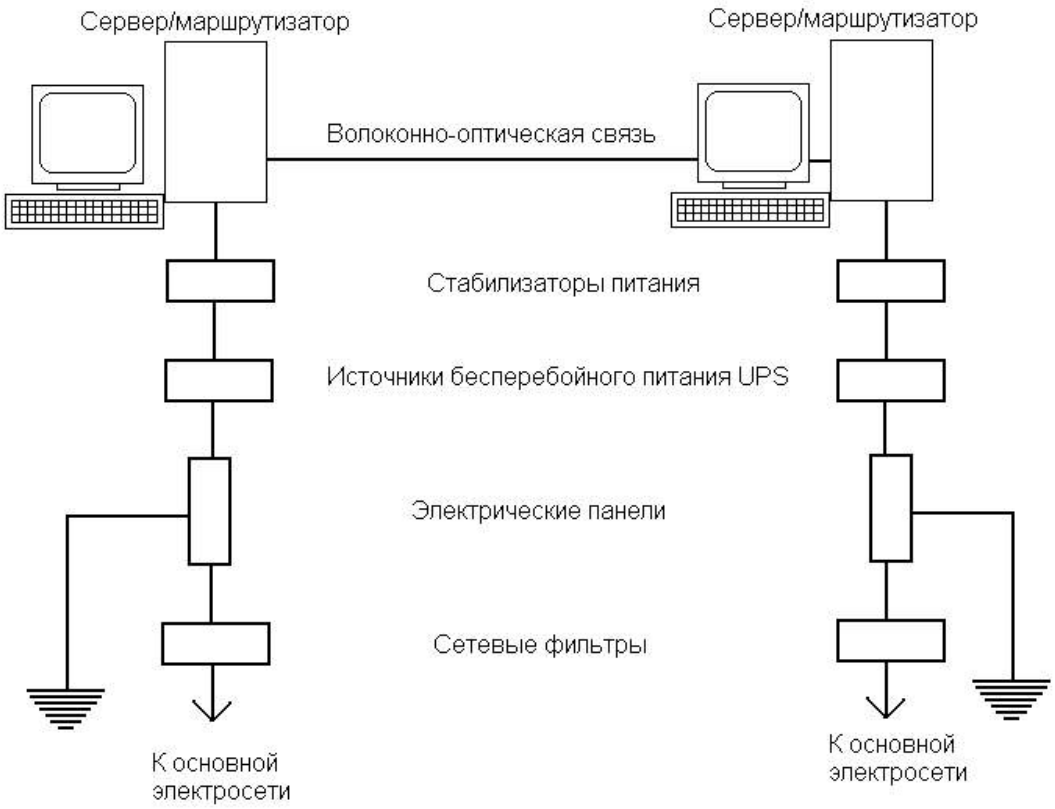

Рис. 9.2 Схема объединения двух сетей.

8.10.1 Источники бесперебойного питания.

Источник бесперебойного питания (UPS) обеспечивает электропитания для компьютеров и других устройств при падении или исчезновении напряжения в сети. В его состав входит один из следующих основных элементов:

- Система батарей.
- Инерционный UPS обеспечивает непрерывное питание компьютера при кратковременных отключениях сети.
- Инерционный электродвигатель, вращающий электрогенератор.

Источники бесперебойного питания могут работать в оперативном режиме или быть резервными. Резервные источники питания включаются только при отказе основного электропитания. Такие источники бесперебойного питания имеют специальную схему со временем переключения менее 5 мсек. Источник бесперебойного питания, работающий в оперативном режиме, обеспечивает непрерывное электропитание компьютера. При отказе внешнего источника питания компьютер продолжает работать от батареи UPS. Хотя такие источники бесперебойного питания лучше, они более дороги. Однако они обеспечивают равномерное "сглаженное" питание для компьютерных модулей. Примерами являются источники бесперебойного питания модели Matrix 3000 и 5000 фирмы American Power Conversion.

8.10.2 Сетевые фильтры.

Основное назначение сетевых фильтров состоит в защите системы от бросков питание. UPS необходим для защиты от провалов питания, повышения напряжения и отключения питания. Большинство из них может справляться с повышением напряжения до 800 вольт. Чтобы подавлять более сильные броски питания, нужен сетевой фильтр.

Список источников.

1. www.citforum.ru
2. http://novell.h1.ru
3. http://valentin.narod.ru/doc/nw/book1.html
4. www.novell.com/documentation/nw51/index.html
5. http://netware.nwsoft.ru/?id=docs
6. http://valentin.narod.ru/doc/nw/book2.html