Информационная безопасность в сетях ЭВМ

Защита данных в компьютерных сетях становится одной из самых открытых проблем в

современных информационно-вычислительных системах. Насегодняшний день

сформулировано три базовых принципа информационной безопасности, задачей которой

является обеспечение:

- целостности данных - защита от сбоев, ведущих к потере информации или ее

уничтожения;

- конфиденциальности информации;

- доступности информации для авторизованных пользователей.

Рассматривая проблемы, связанные с защитой данных в сети, возникает вопрос о

классификации сбоев и несанкционированности доступа,что ведет к потере или

нежелательному изменению данных. Это могут быть сбои оборудования (кабельной

системы, дисковых систем, серверов, рабочих станций ит.д.), потери информации

(из-за инфицирования компьютерными вирусами, неправильного хранения архивных

данных, нарушений прав доступа к данным),некорректная работа пользователей и

обслуживающего персонала. Перечисленные нарушения работы в сети вызвали

необходимость создания различных видов защитыинформации. Условно их можно

разделить на три класса:

- средства физической защиты;

- программные средства (антивирусные программы, системы разграничения

полномочий, программные средства контроля доступа);

-административные меры защиты (доступ в помещения, разработка стратегий

безопасности фирмы и т.д.).

Одним из средств физической защиты являются системы архивирования и дублирования

информации. В локальных сетях, где установлены один-двасервера, чаще всего

система устанавливается непосредственно в свободные слоты серверов. В крупных

корпоративных сетях предпочтение отдается выделенномуспециализированному

архивационному серверу, который автоматически архивирует информацию с жестких

дисков серверов и рабочих станций в определенное время,установленное

администратором сети, выдавая отчет о проведенном резервном копировании.

Наиболее распространенными моделями архивированных серверовявляются Storage

Express System корпорации Intel ARCserve for Windows.

Для борьбы с компьютерными вирусами наиболее часто применяются антивирусные

программы, реже - аппаратные средства защиты. Однако,в последнее время

наблюдается тенденция к сочетанию программных и аппаратных методов защиты. Среди

аппаратных устройств используются специальныеантивирусные платы, вставленные в

стандартные слоты расширения компьютера. Корпорация Intel предложила

перспективную технологию защиты от вирусов в сетях,суть которой заключается в

сканировании систем компьютеров еще до их загрузки. Кроме антивирусных программ,

проблема защиты информации вкомпьютерных сетях решается введением контроля

доступа и разграничением полномочийпользователя. Для этого используются

встроенные средства сетевых операционных систем, крупнейшим производителем

которых является корпорацияNovell. В системе, например, NetWare, кроме

стандартных средств ограничения доступа (смена паролей, разграничение

полномочий), предусмотрена возможностькодирования данных по принципу "открытого

ключа" с формированием электронной подписи для передаваемых по сети пакетов.

Однако, такая система защиты слабомощна, т.к. уровень доступа и возможность

входа в систему определяются паролем, который легкоподсмотреть или подобрать.

Для исключения неавторизованного проникновения в компьютер­ную сеть используется

комбинированный подход - пароль +идентификация пользователя по персональному

"ключу". "Ключ" представляет собой пластиковую карту (магнитная или совстроенной

микросхемой - смарт-карта) или различные устройства для идентификации личности

по биометрической информации - по радужной оболочкеглаза, отпечаткам пальцев,

размерам кисти руки и т.д. Серверы и сетевые рабочие станции, оснащенные

устройствамичтения смарт-карт и специальным программнымобеспечением, значительно

повышают степень защиты от несанкционированного доступа.

Смарт-карты управления доступом позволяют реализовать такие функции, как

контроль входа, доступ к устройствам ПК, к программам,файлам и командам. Одним

из удачных примеров создания комплексного решения для контроля доступа в

открытых системах, основанного как на программных, так и нааппаратных средствах

защиты, стала система Kerberos, в основу которой входят три компонента:

- база данных, которая содержит информацию по всем сетевым ресурсам,

пользователям, паролям, информационным ключам и т.д.;

- авторизационный сервер (authentication server), задачей которого является

обработка запросов пользователей на предоставлениетого или иного вида сетевых

услуг. Получая запрос, он обращается к базе данных и определяет полномочия

пользователя на совершение определенной операции.Пароли пользователей по сети не

передаются, тем самым, повышая степень защиты информации;

-Ticket-granting server (сервер выдачи разрешений) получает от авторизационного

сервера "пропуск" с именемпользователя и его сетевым адресом, временем запроса,

а также уникальный "ключ". Пакет, содержащий "пропуск", передается также

взашифрованном виде. Сервер выдачи разрешений после получения и расшифровки

"пропуска" проверяет запрос, сравнивает "ключи" и притождественности дает

"добро" на использование сетевой аппаратуры или программ.

По мере расширения деятельности предприятий, роста численности абонентов и

появления новых филиалов, возникает необходимостьорганизации доступа удаленных

пользователей (групп пользователей) к вычислительным или информационным ресурсам

к центрам компаний. Для организацииудаленного доступа чаще всего используются

кабельные линии и радиоканалы. В связи с этим защита информации, передаваемой по

каналам удаленного доступа,требует особого подхода. В мостах и маршрутизаторах

удаленного доступа применяется сегментация пакетов - их разделение и передача

параллельно по двумлиниям, - что делает невозможным "перехват" данных при

незаконном подключении "хакера" к одной из линий. Используемая при

передачеданных процедура сжатия передаваемых пакетов гарантирует невозможность

расшифровки "перехваченных" данных. Мосты и маршрутизаторы удаленногодоступа

могут быть запрограммированы таким образом, что удаленным пользователям не все

ресурсы центра компании могут быть доступны.

В настоящее время разработаны специальные устройства контроля доступа к

вычислительным сетям по коммутируемым линиям. Примером можетслужить,

разработанный фирмой AT&T модуль Remote Port Securiti Device (PRSD), состоящий

из двух блоков размером с обычный модем: RPSD Lock (замок),устанавливаемый в

центральном офисе, и RPSD Key (ключ), подключаемый к модему удаленного

пользователя. RPSD Key и Lock позволяют устанавливать несколькоуровней защиты и

контроля доступа:

 - шифрование данных, передаваемых по линии при помощи генерируемых цифровых

ключей;

- контроль доступа с учетом дня недели или времени суток.

Прямое отношение к теме безопасности имеет стратегия создания резервных копий и

восстановления баз данных. Обычно эти операциивыполняются в нерабочее время в

пакетном режиме. В большинстве СУБД резервное копирование и восстановление

данных разрешаются только пользователям с широкимиполномочиями (права доступа на

уровне системного администратора, либо владельца БД), указывать столь

ответственные пароли непосредственно в файлах пакетнойобработки нежелательно.

Чтобы не хранить пароль в явном виде, рекомендуется написать простенькую

прикладную программу, которая сама бы вызывала

утилитыкопирования/восстановления. В таком случае системный пароль должен быть

"зашит" в код указанного приложения. Недостатком данного методаявляется то, что

всякий раз присмене пароля эту программу следует перекомпилировать.

Применительно к средствам защиты от НСД определены семь классов защищенности

(1-7) средств вычислительной техники (СВТ) и девятьклассов

(1А,1Б,1В,1Г,1Д,2А,2Б,3А,3Б) автоматизированных систем (АС). Для СВТ самым

низким является седьмой класс, а для АС - 3Б.

Рассмотрим более подробно приведенные сертифицированные системы защиты от НСД.

Система "КОБРА" соответствует требованиям 4-ого класса защищенности (для СВТ),

реализует идентификацию и разграничениеполномочий пользователей и

криптографическое закрытие информации, фиксирует искажения эталонного состояния

рабочей среды ПК (вызванные вирусами, ошибкамипользователей, техническими сбоями

и т.д.) и автоматически восстанавливает основные компоненты операционной среды

терминала.

Подсистема разграничения полномочий защищает информацию на уровне логических

дисков. Пользователь получает доступ копределенным дискам А,В,С,...,Z. Все

абоненты разделены на 4 категории:

- суперпользователь (доступны все действия в системе);

 -администратор (доступны все действия в системе, за исключением изменения

имени, статуса иполномочий суперпользователя, ввода или исключения его из списка

пользователей);

- программисты (может изменять личный пароль);

-коллега (имеет право на доступ к ресурсам, установленным ему

суперпользователем).

Помимо санкционирования и разграничения доступа к логическим дискам,

администратор устанавливает каждому пользователю полномочиядоступа к

последовательному и параллельному портам. Если последовательный порт закрыт, то

невозможна передача информации с одного компьютера на другой. Приотсутствии

доступа к параллельному порту, невозможен вывод на принтер.