Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра интеллектуальных информационных технологий

Ю.И. Иванченко, А.Ю. Деев, А.В. Заговалко

ИНТЕЛЛЕКТУАЛЬНЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие
для студентов специальности «Искусственный интеллект»
специализации «Интеллектуальные компьютерные технологии
защиты информации»

В 3-х частях

Часть 2
Защита информации на уровне операционной системы

Минск 2005

УДК 681.3.067 (075.8)
ББК 32.973я73
И 23

Р е ц е н з е н т :
и.о. директора ОДО «ВирусБлокАда»,
канд. техн. наук Г.К. Резников

Иванченко Ю.И.

И 23 Интеллектуальные компьютерные технологии защиты информации: Учеб. пособие для студ. специальности «Искусственный интеллект» специализации «Интеллектуальные компьютерные технологии защиты информации». В 3 ч. Ч. 2: Защита информации на уровне операционной системы / Ю.И. Иванченко, А.Ю. Деев, А.В. Заговалко. – Мн.: БГУИР, 2005. – 86 с.
ISBN 985-444-702-2 (ч. 2).

Учебное пособие написано по материалам лекций, практических и лабораторных работ, проводимых для студентов БГУИР, в рамках учебных курсов «Теоретические основы защиты информации», «Средства и методы обеспечения информационной безопасности», «Проектирование защищенных систем», «Управление защитой информации».

УДК 681.3.067 (075.8)
ББК 32.973я73

Часть 1 издана в БГУИР в 2003 году.
Иванченко Ю.И., Деев А.Ю., Заговалко А.В. Интеллектуальные компьютерные технологии защиты информации: Учеб. пособие для студентов специализации «Интеллектуальные компьютерные технологии защиты информации» специальности «Искусственный интеллект». В 3 ч. Ч. 1: Общие положения защиты информации. – Мн.: БГУИР, 2003.

ISBN 985-444-702-2 (ч. 2)

ISBN 985-444-561-5

Содержание

1. Аппаратное обеспечение средств защиты операционной системы

Под аппаратным обеспечением средств защиты операционной системы (ОС) традиционно понимается совокупность средств и методов, используемых для решения следующих задач:

- управление оперативной и виртуальной памятью компьютера;
- планирование задач в многозадачной ОС;
- синхронизация выполнения параллельных задач в многозадачной ОС;
- обеспечение корректности совместного доступа задач к ресурсам ОС;
- исключение тупиковых ситуаций в процессе совместного доступа задач к ресурсам ОС.

Перечисленные задачи в значительной степени решаются с помощью аппаратно реализованных функций процессоров и других узлов компьютера. Однако, как правило, для решения этих задач применяются и программные средства.

1.1. Управление оперативной или виртуальной памятью компьютера

Основная угроза, защита от которой реализуется средствами управления оперативной памятью, заключается в том, что один процесс, выполняемый в многозадачной системе, несанкционированно получает доступ к оперативной памяти другого процесса. Это критично для процессов обработки конфиденциальной информации. Если оперативная память, выделенная этому процессу, не будет защищена должным образом от доступа со стороны других процессов, последние получат несанкционированный доступ к конфиденциальной информации. Таким образом, в рассматриваемой ситуации пользователь-злоумышленник может получать доступ к информации, обычно недоступной ему, запустив процесс, получивший доступ к оперативной памяти, принадлежащей другому процессу.

Существуют два основных подхода к обеспечению защиты оперативной памяти процесса от несанкционированного доступа со стороны других процессов:

Первый подход заключается в том, что при каждом обращении процессора к оперативной памяти осуществляется проверка корректности доступа. Теоретически этот подход позволяет создать абсолютно надежную защиту от несанкционированного доступа процесса к "чужой" памяти. Однако при этом станет практически невозможным и взаимодействие процессов. В применяемых на практике операционных системах значительная часть оперативной памяти, выделенной процессу, является разделяемой, т.е. доступной другим процессам. Если запретить подобное разделение памяти между процессами, требования операционной системы к объему оперативной памяти возрастут в несколько раз.

Второй подход к обеспечению защиты оперативной памяти заключается в выделении каждому процессу индивидуального адресного пространства, аппаратно изолированного от других процессов. При этом, по какому бы адресу оперативной памяти ни обратился процесс, он не сможет обратиться к памяти, выделенной другому процессу, поскольку одному и тому же значению адреса в разных адресных пространствах соответствуют разные физические адреса оперативной памяти. При практической реализации этого подхода процессор должен поддерживать логическую адресацию. Данный подход надежно защищает от случайного обращения, но не всегда от преднамеренных попыток доступа.

При любом подходе ОС должна содержать средства отладки, т.е. процесс отладки должен иметь доступ к оперативной памяти отлаживаемого процесса. Следовательно, в политике безопасности должны быть четко предусмотрены средства, позволяющие не допускать запуска отладчиков, когда они не нужны.

1.2. Планирование задач

Планирование задач в многозадачной ОС заключается в распределении операционной системой времени центрального процессора (или процессоров) между параллельно выполняющимися задачами.
В роли задач могут выступать либо процессы, либо потоки или нити.

Основная угроза подсистеме планирования задач (планировщику задач) заключается в том, что злоумышленник сможет приостановить или прекратить выполнение системных процессов, тем самым

блокировать различные функции операционной системы, включая функции, критичные для обеспечения безопасности операционной системы. Для нейтрализации этой угрозы операционная система должна обладать следующими свойствами:

- поддерживается вытеснение задач;
- создание высокоприоритетных задач доступно только привилегированным пользователям;
- критичные для обеспечения безопасности системы задачи защищены от несанкционированного вмешательства в ход их выполнения (например от несанкционированного снижения приоритета);
- фатальный сбой в процессе функционирования одной из задач, критичных для обеспечения безопасности, должен вызывать крах операционной системы.

1.3. Синхронизация выполнения параллельных задач и обеспечение корректности совместного доступа задач к ресурсам

В многозадачных операционных системах с вытеснением задач часто возникает необходимость синхронизации параллельно выполняющихся задач. Синхронизация необходима процессам для организации совместного использования ресурсов, таких как файлы или устройства, а также для обмена данными. Нарушение синхронизации может привести к снижению общей производительности операционной системы, некорректной работе устройств или потере данных.

В процессе функционирования может возникнуть ситуация, когда две или более задач одновременно обращаются к одному и тому же объекту операционной системы. Если при этом режим доступа хотя бы одной задачи допускает изменение данных объекта, не исключено, что обращения других задач к данному объекту будут выполнены некорректно, а если две или более задач одновременно изменяют данные объекта, весьма вероятно, что эти данные окажутся испорчены.

Чтобы избежать этих ситуаций, во многих операционных системах предусматриваются специальные функции, позволяющие задачам ждать появления знаков, выставленных другими задачами, не затрачивая ресурсов операционной системы.

1.4. Предотвращение тупиковых ситуаций

Тупиковая ситуация (другие названия - тупик, клинч) может возникнуть, когда несколько задач одновременно пытаются открыть несколько одних и тех же объектов в режиме монопольного доступа. В результате выполнение всех задач может приостановиться на неопределенное время.

Как правило, операционные системы гарантируют невозможность возникновения тупиковых ситуаций при выполнении прикладными программами кода операционной системы. Обеспечить предотвращение тупиковых ситуаций при выполнении кода прикладной программы должна сама программа.

1.5. Аппаратная защита в процессорах семейства x86

Подавляющее большинство современных персональных компьютеров имеет процессор одной из моделей семейства INTEL X86. Наиболее распространены на сегодняшний день модели Pentium II и Pentium III, однако, поскольку функции аппаратной защиты, начиная с модели i386, изменились незначительно и большинство современных операционных систем используют защитные функции только одной модели, будем рассматривать процессор i386. Более современные процессоры поддерживают все функции i386.

Процессоры модели i386 и более поздних моделей могут работать в одном из трех режимов - реальном режиме, защищенном режиме и режиме эмуляции виртуального 8086 (виртуальный режим). При старте процессора он начинает работу в реальном режиме, в котором защитные функции не поддерживаются. Виртуальный режим процессора предназначен для выполнения в защищенном режиме программ, предназначенных для работы в реальном режиме. В защищенном режиме процессор i386 поддерживает возможность реализации виртуальной памяти со страничной организацией.

1.5.1. Адресация оперативной памяти

Программа, выполняющаяся на процессоре i386 , обращаясь к фрагменту оперативной памяти, должна указать адрес этого фрагмента. Этот адрес складывается из двух составляющих – селектора и смещения. Селектор представляет собой идентификатор сегмента, в котором располагается требуемый фрагмент памяти, а смещение определяет порядковый номер первого байта фрагмента в этом сегменте. При обращении к оперативной памяти необходимый селектор должен быть заранее загружен в один из **сегментных регистров** процессора.

С каждым сегментным регистром связан один **дескрипторный регистр**. При загрузке селектора в сегментный регистр, в дескрипторный регистр, соответствующий этому сегментному регистру, автоматически загружается **дескриптор** сегмента, соответствующий загружаемому селектору. Сегменты, которым соответствуют различные дескрипторы, могут пересекаться и даже совпадать. Дескриптор сегмента может быть **глобальным** или **локальным**. В первом случае дескриптор доступен всем задачам (процессам или потокам), выполняющимся в системе, во втором случае – только одной задаче. Каждая задача, выполняемая в системе, имеет **таблицу локальных дескрипторов**, содержащую дескрипторы, доступные только этой задаче.

1.5.2. Уровни привилегированности

Защита оперативной памяти в процессоре i386 основана на понятии уровня привилегированности. **Уровень привилегированности** (privilege level, PL) – это числовой идентификатор, принимающий значения от 0 до 3, который определяет возможности задачи выполнить команды процессора, модифицировать регистры и области памяти и т.д. Чем меньше числовое значение уровня привилегированности, тем выше этот уровень и тем более полный доступ имеет задача к аппаратным возможностям процессора. Множество задач, обладающих некоторым конкретным уровнем привилегированности, называют кольцом защиты. Например, если код программы имеет уровень привилегированности, равный трем, говорят, что программа выполняется в третьем кольце защиты.

Обычно прикладные программы выполняются в третьем кольце защиты, а код операционной системы – в нулевом кольце. Первое и второе кольца защиты используются редко. Видимо, это объясняется тем, что большинство RISC-процессоров поддерживают только два кольца защиты, и переносимые операционные системы вынуждены учитывать это ограничение. Каждая задача, выполняющаяся на процессоре i386, имеет свой уровень привилегированности. Уровень привилегированности задачи называют **текущим уровнем привилегированности** (current privilege level, CPL).

Каждый дескриптор и каждый селектор также имеют свои уровни привилегированности, называемые соответственно **уровнем привилегированности дескриптора** (descriptor privilege level, DPL) и **запрашиваемым уровнем привилегированности** (requested privileged level, RPL).

1.5.3. Защита сегментов оперативной памяти

Защита сегментов оперативной памяти в процессоре i386 основана на сравнении уровня привилегированности задачи (CPL), уровня привилегированности дескриптора (DPL) и уровня привилегированности селектора (RPL) в момент загрузки селектора в сегментный регистр. Фактически при загрузке селектора в сегментный регистр выполняются следующие три проверки.

1.Проверяется корректность селектора. Если индекс, содержащийся в селекторе, превышает объем таблицы дескрипторов (локальной или глобальной в зависимости от селектора), генерируется исключительная ситуация 11 (отсутствие сегмента) или 12 (ошибка стека) в зависимости от типа загружаемого сегмента.

2.Проверяется совместимость типа загружаемого селектора с типом сегментного регистра. В регистр cs может быть загружен только селектор сегмента кода, в регистр ss – только селектор сегмента стека, в любой другой сегментный регистр – либо селектор сегмента данных, либо селектор сегмента стека, либо селектор доступного для чтения сегмента кода. В случае несовпадения типов селектора и сегментного регистра генерируется исключительная ситуация 13 (общая ошибка защиты).

3. Проверяется достаточность текущего уровня привилегированности задачи для загрузки сегмента. Если загружаемый сегмент является сегментом стека, он может быть загружен только при точном совпадении CPL, RPL и DPL. Если же загружаемый сегмент не является сегментом стека, то для его ус-

пешной загрузки необходимо и достаточно, чтобы и CPL, и RPL были не ниже, чем DPL. В случае неудачной проверки генерируется исключительная ситуация 13.

Таким образом, задача может загрузить селектор сегмента стека в регистр ss тогда и только тогда, когда совпадают все три уровня привилегированности – задачи, селектора и дескриптора сегмента. Отсюда следует, что при изменении уровня привилегированности задачи должен быть изменен сегмент стека задачи. Это происходит автоматически в процессе выполнения процессором машинных команд передачи управления из сегмента в сегмент.

Селектор сегмента кода или данных может быть загружен в сегментный регистр тогда и только тогда, когда задача имеет уровень привилегированности не ниже уровня привилегированности дескриптора сегмента и для доступа к сегменту используется селектор достаточно высокого уровня привилегированности. Низкопривилегированная задача не может обращаться к высокопривилегированным сегментам ни при каких обстоятельствах. Высокопривилегированная задача может понизить свой уровень привилегированности в отношении конкретного сегмента, загрузив в сегментный регистр низкопривилегированный селектор.

Если в сегментный регистр cs загружается селектор, указывающий на дескриптор с уровнем привилегированности, отличным от уровня привилегированности дескриптора, на который указывал селектор, ранее загруженный в регистр cs, изменяется текущий уровень привилегированности задачи. При этом уровень привилегированности задачи может только понижаться. Повышение уровня привилегированности задачи возможно только посредством шлюзов.

1.5.4. Шлюзы

Шлюзы, или вентили, позволяют реализовывать в защищенном режиме процессора i386 передачу управления между кодовыми сегментами с различными уровнями привилегированности. Другими словами, через шлюз задача может перейти из одного кольца защиты в другое, в том числе и из менее привилегированного кольца в более привилегированное кольцо. Шлюз представляет собой дескриптор специального вида, содержащий вместо адреса и границы сегмента ссылку на селектор и смещение в некотором другом сегменте.

Шлюз представляет собой дескриптор специального вида, содержащий вместо адреса и границы сегмента ссылку на селектор и смещение в некотором другом сегменте.

Шлюзы могут быть глобальными и локальными, а также следующих видов:

1. Шлюзы вызовов - используются для смены уровня привилегированности с помощью команды call.
2. Шлюзы задач - используются для переключения задач.
3. Шлюзы прерываний и ловушек - используются для обработки прерываний.

1.5.5. Переключение задач

Процессор i386 поддерживает многозадачность на аппаратном уровне, предоставляя специальные средства для быстрого переключения между задачами. Задачи переключаются командами, которые указывают на сегмент состояния задачи или на шлюз. Также возможно переключение задач в процессе обработки прерываний. Сегмент состояния задачи содержит всю информацию, необходимую для возобновления выполнения задачи после обратного переключения. Селектор этого сегмента для текущей задачи всегда хранится в 16-битовом регистре tr. Каждая задача, выполняемая в системе, имеет свой сегмент состояния. При переключении задач автоматически происходит обновление значения регистра tr. Таким образом, этот регистр всегда содержит селектор сегмента состояния задачи. При возврате управление передается прерванной задаче. Состояние текущей задачи заносится в сегмент состояния задачи, а состояние предыдущей задачи считывается из него.

1.5.6. Обработка прерываний

Таблица прерываний представляет собой сегмент, адрес и граница которого хранятся в регистре idtr. Каждый элемент таблицы прерываний представляет собой шлюз, указывающий на обработчик прерывания. В процессе обработки прерывания уровень привилегированности задачи может измениться. При выполнении команды возврата из прерывания iret – уровень привилегированности задачи автоматически восстанавливается.

Причины прерываний:

- сигнал от внешнего устройства – аппаратное прерывание (IQR);
- возникновение на процессоре исключительной ситуации - внутреннее прерывание;
- выполнение процессором команды вызова прерывания int - программное прерывание.

1.5.7. Страничная организация памяти

При включенной страничной организации оперативной памяти память разбивается на страницы – блоки по 4 Кбайта. Каждой задаче, выполняемой в системе, выделяется 2 в степени 20 – 1048 576 страниц. При каждом обращении задачи к оперативной памяти, процессор преобразовывает логический адрес (определяемый селектором и смещением) в линейный адрес.

Каждая страница в каждый момент времени может находиться в одном из трех состояний:

1. Загружена в оперативную память.
2. Загружена в виртуальную память.
3. Страница отсутствует.

При отключенной страничной адресации памяти линейный адрес попросту совпадает с физическим. При включенной страничной адресации линейный адрес представляет собой 32-битовое число.

2. Модель безопасности Windows NT

Windows NT обладает распределенной инфраструктурой обеспечения информационной безопасности, в которой каждый пользователь и процесс должен быть аутентифицирован, а любой объект обладает метками управления доступом. Решение о предоставлении или отклонении доступа должным образом аутентифицированного пользователя к объекту принимается ядром операционной системы на основе анализа прав и привилегий, присвоенных запрашивающему доступ пользователю. Windows NT сконструирована так, что средства защиты встроены изначально в саму систему как часть спецификаций на разработку.

Прежде чем получить доступ к любому ресурсу, пользователь обязан зарегистрироваться независимо от того, где он работает — на Windows NT Server или Windows NT Workstation. Windows NT обеспечивает защиту па локальном уровне, так как компьютер имеет свою локальную базу политики защиты. Система безопасности — это интегральная часть Windows NT, а не некоторая среда, причем действие ее распространяется на всю операционную систему.

Ключевыми элементами подсистемы защиты являются:
- распорядитель локальной безопасности;
- менеджер защиты учетных записей;
- справочный монитор защиты.

Кроме того, в Windows NT имеются следующие элементы защиты:
- процесс регистрации;
- элементы управления персональным доступом;
- маркеры доступа;
- списки контроля доступа.

2.1. Распорядитель локальной безопасности

Подсистема **Распорядитель локальной безопасности** (Local Security Authority — LSA) — сердце защиты в Windows NT Server. В его обязанности входит;
- предоставление пользователям доступа в систему;
- создание маркеров доступа в процессе регистрации;
- управление интерактивным процессом аутентификации пользователя;
- разрешение Windows NT Server подключаться к программам аутентификации третьих фирм;
- управление локальной политикой защиты;
- контроль политики аудита;
- запись сообщений аудита, посылаемых **Справочным монитором защиты**, в журнал событий.

2.2. Менеджер защиты учетных записей

Менеджер защиты учетных записей (Security Account Manager — SAM) обслуживает работу с базой данных защиты учетных записей, известной как база SAM, в которой содержится информация обо всех учетных записях пользователей, групп и компьютеров. SAM обеспечивает сервис проверки пользователей, применяемый LSA. Невидимый для пользователя **Менеджер защиты учетных записей** отвечает за сравнение информации, вводимой пользователем в диалоговом окне **«**Welcome»**,** с той, что хранится в базе защиты, а также за предоставление пользователю его идентификационного кода (**Security ID - SID**), а также SID всех групп, членом которых он является.

Удаление пользователя уничтожает его SID. Удаленная учетная запись пользователя не восстанавливается, так как для него больше не существует SID. Новая учетная запись с тем же самым именем получит новый SID, и, следовательно, у него не будет привилегий, имевшихся у предыдущей учетной записи.

В зависимости от конфигурации сети могут существовать различные базы SAM на одной или нескольких системах с Windows NT. Выбор конкретной базы SAM определяется тем, где именно пользователь регистрируется — на рабочей станции или в сети. Например:

- В сети, где пользователи имеют локальные учетные записи на каждой рабочей станции, осуществляется доступ к базе SAM, расположенной на том компьютере, где регистрируется пользователь.
- В сети с централизованной базой учетных записей (например в сети с одним мастер-доменом) имеется центральная база SAM, расположенная на первичном контроллере домена. Эта база тиражируется на резервные контроллеры домена. При попытке зарегистрироваться на рабочей станции используется база SAM рабочей станции, а при попытке зарегистрироваться в домене — база SAM первичного контроллера домена или одного из резервных контроллеров. Резервные контроллеры помогают разгрузить первичный контроллер. Windows NT Server, сконфигурированный как сервер, не участвует в процессе аутентификации пользователя.

2.3. Справочный монитор безопасности

Справочный монитор безопасности (Security Reference Monitor — SRM) — компонент Windows NT, предназначенный для усиления политики авторизации доступа и политики аудита, проводимых подсистемой **Распорядителя локальной безопасности**. Он обеспечивает защиту ресурсов или объектов от неавторизованного доступа или модификации. SRM предоставляет услуги для авторизации доступа к объектам, проверки субъектов (учетных записей пользователей) на привилегии и вывод необходимых сообщений аудита. Справочный монитор безопасности содержит только копию кода проверки доступа в систему, что гарантирует осуществление однотипной защиты объектов в Windows NT независимо от типа объекта.

Прямой доступ к объектам в Windows NT не разрешен: все запросы пользователей на доступ к объекту сначала проверяются Справочным монитором безопасности. Например, когда файл открывается на редактирование, Windows NT сравнивает дескриптор защиты файла с информацией о защите, хранящейся в маркере пользователя, и делает вывод о возможности предоставления доступа к файлу. Дескриптор защиты включает в себя все входы контроля доступа (ACE), создающие список контроля доступа (ACL) к файлу. Файл, у которого отсутствует ACL, открыт любому пользователю для любого вида доступа. Справочный монитор безопасности проверяет все ACE в ACL, определяя для конкретного пользователя возможность выполнить определенный вид доступа. Если SRM выдал разрешение на доступ к файлу, дополнительные проверки не ведутся. Дальнейшие попытки доступа к этому файлу осуществляются через созданную ссылку на этот файл.

SRM генерирует сообщения, которые заносятся в журнал событий **Распорядителем локальной безопасности**.

2.4. Процесс регистрации

Интерактивный процесс регистрации — первая линия обороны Windows NT Server от несанкционированного доступа. Процесс начинается с диалогового окна, приглашающего нажать комбинацию клавиш Ctrl+Alt+Del, (перед этим диалоговым окном может появиться предупреждение о легальности использования). Такое начало процесса регистрации надежно защищает от любых программ, выполняемых в фоновом режиме, целью которых является выяснение регистрационных данных пользователя.

После этого появляется второе диалоговое окно процесса WinLogon.

В этом окне пользователь вводит свое имя, имя сервера, рабочей станции или домена, в который ему необходимо получить доступ, и пароль. Если имя или пароль введены с ошибкой, система сообщит о невозможности авторизации доступа. При этом не сообщается, что именно — пароль или имя — вызвало ошибку.

В случае правильного ввода имени, пароля и имени домена система переходит ко второму этапу — аутентификации пользователя.

Система аутентифицирует пользователя, передавая заданные в вводном диалоговом окне параметры в **Менеджер защиты учетных записей** (SAM). SAM сравнивает имя пользователя и пароль с данными, хранящимися в базе пользователей домена. Если имя и пароль совпадают, сервер уведомляет рабочую станцию о подтверждении доступа. Сервер загружает и такую информацию, как привилегии учетной записи пользователя, положение домашнего каталога и т.п. Если для пользователя определен сценарий регистрации, он загружается на рабочую станцию для исполнения.

Если пользователь имеет учетную запись, его пароль верен и у него есть привилегии доступа в систему, подсистема защиты создает объект **маркер доступа**, представляющий пользователя. Он сравним с ключом, содержащим удостоверение личности пользователя. В нем хранится идентификатор защиты (SID), имя пользователя и имена групп, к которым он принадлежит.

Маркер доступа или его копия ассоциируются с любым процессом, выполняемым пользователем (например открытие или печать файла). Комбинация процесс/маркер называется **субъектом**. Субъекты оперируют над объектами Windows NT, вызывая системные сервисы. Когда субъект осуществляет доступ к защищенному объекту, (например файлу или каталогу), содержимое маркера сравнивается с содержимым списка контроля доступа к объекту (ACL), используя стандартную процедуру проверки. При этом определяется, можно ли субъекту предоставить право на выполнение запрашиваемой операции. Эта же процедура может при необходимости сгенерировать сообщения аудита, отражающие результат попытки доступа.

Созданный маркер передается процессу Win32 WinLogon. WinLogon предписывает подсистеме Win32 создать процесс для пользователя, и маркер доступа присоединяется к этому процессу. После этого подсистема Win32 инициирует Program Manager.

2.5. Маркеры доступа

Маркеры доступа являются объектами, содержащими информацию о конкретных пользователях (табл. 2.1). Когда пользователь инициирует процесс, за этим процессом постоянно закрепляется маркер доступа.

Во время регистрации создание и применение маркера доступа критично. Когда пользователь или процесс пользователя пытается осуществить доступ к объекту, хранящиеся в маркере доступа SID и список групп, к которым принадлежит. лежит пользователь, сравниваются со списком контроля доступа ACL к объекту. Если в ACL есть разрешение на доступ пользователя или одной из групп, попытка закончится успешно.

Таблица 2.1

Объекты для маркеров доступа

Маркерный объект	Описание
Идентификатор пользователя (SID)	Уникальным образом идентифицирует пользователя, для которого создан маркер
Идентификатор группы	Идентифицирует группу, к которой принадлежит пользователь
Привилегии	Привилегии, назначенные пользователю
Владелец	SID, назначаемый в качестве владельца любого объекта, созданного для пользователя, представленного данным маркером
Первичная группа	SID, назначаемый в качестве первичной группы любого объекта, созданного для пользователя, представленного данным маркером (специфично для подсистемы posix)
ACL по умолчанию	ACL, назначаемый по умолчанию любому объекту, созданному SID пользователя

2.6. Списки контроля доступа

Списки контроля доступа (Access Control Lists — ACL) — форма персонального контроля доступа - работают совместно с файловой системой для защиты файлов от несанкционированного доступа. Каждый ACL состоит из **входов контроля доступа** (Access Control Entries — ACE), определяют доступ к объекту. ACE, содержащие идентификаторы защиты и особые привилегии доступа, вставляются в ACL при назначении пользователем персонального доступа к объекту. Если владелец объекта не установил персонального доступа к объекту, создастся ACL по умолчанию. В табл. 2.2 показано, какие средства применяются для администрирования различных списков контроля доступа.

Таблица 2.2

Средства администрирования списков контроля доступа

Ресурс	Источник ACL
Файлы	Диспетчер файлов (File Manager)
Принтеры	Диспетчер печати (Print Manager)
Пользователи	Диспетчер учетных записей (User Manager - для рабочих станций) Диспетчер учетных записей домена (User Manager for Domains - для серверов)

Когда пользователь осуществляет доступ к объекту, его персональный SID или SID одной из групп, к которой он принадлежит, сравнивается со списком ACE, а запрашиваемая деятельность — с возможностями доступа, описанными в ACE. В случае совпадения пользователю предоставляется доступ.

ACE сортируются по типу доступа — предоставить или запретить. В Windows NT сначала идет проверка ACE с отказом в доступе, а затем — с предоставлением доступа. Отказ всегда преобладает над предоставлением доступа.

Если хотя бы одной из групп, к которым принадлежит пользователь, запрещен доступ, то независимо от того, имеет ли разрешение на доступ он или остальные группы, в доступе будет отказано. Так что если группе **Все** (Everyone) запрещен доступ к объекту, значит, для всех пользователей, включая владельца ресурса, доступ к объекту запрещен.

2.7. Объекты и субъекты доступа WinNT

Объекты доступа

Файловые объекты – содержат файлы, дисковые каталоги, расположенные на логических дисках, устройства, каналы.

Почтовые ящики – передача сообщений между процессами.

Объектовые директории – объекты, содержащие в себе другие объекты. Они временные. Объекты хранятся в оперативной памяти.

Ключи реестра – подмножество элементов конфигурации ОС.

Процессы – экземпляры программ, выполняющиеся в данный момент на данном компьютере.

Потоки машинных команд.

Диспетчер сервисов – управляет сервисами.

Сервис – исполняемые модули.

Объекты управления окнами, рабочие столы, оконные станции.

Порты – объекты, которые используются при передаче сообщений между процессами.

Секции разделяемой памяти.

Символические связи. Объекты, позволяющие создавать синонимы для имени объекта.

Маркеры – объекты, содержащие информацию о работающем в системе пользователе.

Объект синхронизации события – объекты, использующиеся при асинхронном обращении к файлам.

Пары событий – объекты, использующиеся при передаче сообщения от одного процесса к другому.

Семафоры – для ограничения одновременного обращения разных потоков к объекту.

Субъекты доступа

Пользователи (обычный, псевдопользователь, администратор).

Специальные (временные), членство определяется системой.

Относительные – эти субъекты имеют смысл только при применении к объекту.

2.8. Управление пользователями

Любой пользователь Windows NT Workstation или Windows NT Server характеризуется наличием определенной учетной записи.

Учетной записью называется совокупность прав и дополнительных параметров, ассоциированных с определенным пользователем. У каждого пользователя есть свое **имя** и **пароль**. В домене или в рабочей группе не может быть ДВУХ пользователей с одинаковым именем. В разных доменах имена могут совпадать, так как полное имя пользователя домена определяется по совокупности **Имя домена \ Имя пользователя**.

Большинство сетевых операционных систем поддерживает информацию о пользователях. Они регистрируют их имена и пароли, а также присваивают им личные каталоги. Нередко сетевая ОС хранит дополнительные сведения, например, заданные для пользователя по умолчанию соединения, его полномочия защиты, группы, в которые входит пользователь, фоновую картинку его рабочей области и т.д. В сети Windows NT такая дополнительная информация называется профилем пользователя. В сети Windows NT добавить учетные данные пользователей можно двумя способами: создать новых пользователей или скопировать уже существующих. В любом случае при этом вносятся изменения в следующую информацию:

- учетную информацию о пользователях;
- сведения о членстве в группах;
- информацию профиля пользователя.

2.8.1. Учетные данные пользователей

Учетные данные пользователей идентифицируют в компьютерной сети пользователя, которому дается пользовательское **имя** (username) и **пароль** (password). Эта информация применяется для доступа к сетевым ресурсам и для создания персональной вычислительной среды, включая настройки экрана и расположение личных файлов.

Пароли нужно придумывать так, чтобы их трудно было отгадать. Легко отгадываемые пароли, например, дата рождения, ваша фамилия или имена детей, считаются неподходящим выбором. Если вы хотите создать учетные данные пользователя без пароля (такие, как Гость или аналогичные им в других сетях), оставьте поле пароля пустым. Между тем это будет серьезная брешь в защите сети, поэтому такие учетные данные следует создавать только в том случае, когда они действительно необходимы, а пользователю без пароля лучше не предоставлять прав, позволяющих ему запортить информацию в сети или получить доступ к важным данным.

Запомните свои пароли. Это ваши "ключи от сети". Windows NT не сообщит вам введенного пароля, даже если вы системный администратор. Если вы (или другой пользователь) забудете пароль, можно создать для учетных данных новый, но восстановить старый невозможно.

При регистрации нового пользователя в системе формируется идентификационный код - SID, по которому и дальнейшем система будет его распознавать. Этот уникальный код используется для доступа к ресурсам системы. Именно этот от код, а не имя пользователя определяет право на доступ к ресурсам домена.

Поэтому если удалить какого-нибудь пользователя, а затем создать учетную запись для пользователя с таким же именем, что и у удаленного, "новичок" не получит доступа к ресурсам, доступным удаленному. Все дело и том, что идентификационный код "новичка" будет отличен от кода удаленного пользователя.

2.8.2. Локальные и глобальные учетные записи

Учетные записи пользователей Windows NT подразделяются на **локальные** и **глобальные** записи. Локальные учетные записи определяют права пользователей на конкретном компьютере и не распространяются на домен. Пользователь, зарегистрировавшийся в системе локально, получает доступ только к ресурсам этого компьютера. Локально зарегистрировавшийся пользователь получает доступ и к ресурсам серверов с правами гостя. А чтобы обратиться к ресурсам домена, ему нужно каждый раз регистрироваться, используя свою глобальную учетную запись, или его локальное имя и пароль должны совпадать с глобальными.

Группы помогают организовать пользователей сети по требованиям, функциям и атрибутам. Благодаря полномочиям, присваиваемым группам, ее члены могут совместно работать с ресурсами, например с общим каталогом или принтером.

2.8.3. Диспетчер учетных записей

Диспетчер учетных записей позволяет вводить новых пользователей в систему и изменять их характеристики (табл. 2.3).

Таблица 2.3

Характеристики пользовательских учетных данных

Поле	Значение
Имя пользователя (Username)	Обязательное текстовое поле длиной до 20 символов. Допускает символы верхнего и нижнего регистра, за исключением "/ \ []:; 1 =,+*?<>, но регистр символов не различается
Полное имя (Full Name)	Необязательное текстовое поле, обычно применяемое для хранения полного имени/фамилии пользователя
Описание (Description)	Необязательное текстовое поле, обычно применяемое для полного описания пользователя, его должности в фирме, домашнего адреса и т.д. Длина поля не должна превышать 48 символов
Пароль (Password)	Обязательное текстовое поле длиной до 14 символов (регистр символов различается)
Подтверждение пароля (Confirm Password)	Обязательное текстовое поле, используемое для подтверждения пароля. Такой метод позволяет избежать ошибок при наборе пароля
Пользователь должен изменить пароль при следующей регистрации (User Must Change Password at Next Logon)	Этот независимый переключатель задает принудительную смену пароля пользователем при следующей его регистрации в системе. Следует отметить, что Windows NT не позволяет вносить изменения в учетные данные пользователя при установке данного переключателя и переключателя «Пользователь не может изменять пароль»
Пользователь не может изменять пароль (User Cannot Change Password)	Независимый переключатель, не позволяющий пользователям менять свой пароль. Это средство применяется для общих учетных данных (таких, как Гость), когда изменение пароля одним из пользователей сделает невозможной работу в системе других сотрудников, регистрирующихся под данным именем. Для обычных учетных данных переключатель «Пользователь не может изменять пароль», как правило, не устанавливается
Время действия пароля не ограничено (Password Never Expires)	Независимый переключатель, предотвращающий установку срока действия пароля в соответствии со стратегией защиты. Обычно он применяется для автоматизированных программных служб, которые должны регистрироваться в системе как пользователи. Следует иметь в виду, что установка «Время действия пароля не ограничено» переопределяет переключатель «Пользователь должен изменить пароль при следующей регистрации»
Учетные данные запрещены (Account Disabled)	Поле-переключатель, предотвращающее регистрацию пользователей в сети с помощью этих учетных данных. Оно предлагает простой способ временного «отключения» пользователя
Учетные данные заблокированы (Account Locket)	Эта опция будет выбрана, если учетные данные заблокированы в результате неуспешных попыток регистрации. Ее можно сбросить (чтобы пользователь мог вновь регистрироваться), но не установить
Кнопка Группы	Присваивает членство в группе
Кнопка Профиль (Profile)	Активизирует профиль информации о среде пользователя
Кнопка Дистанционное соединение (Dial-in)	Позволяет пользователям удаленно подключаться к компьютеру с помощью службы удаленного доступа

2.8.4. Учетные записи, заданные по умолчанию

В большинстве сетевых операционных систем предусмотрены два уже созданных пользователя — **Администратор** (Administrator) и **Гость** (Guest).

Пользователь **Администратор** присутствует в сети всегда. Его учетные данные должны иметь сильную защиту с помощью пароля. Администратор управляет общей конфигурацией компьютера и определяет политику защиты, создания/изменения пользователей и групп, создания разделяемых сетевых каталогов и выполнения других задач по обслуживанию программного и аппаратного обеспечения. В Windows NT пользователь Администратор имеет все полномочия. Его можно переименовать, но нельзя удалить.

Учетные данные пользователя **Гость** позволяют работать в сети с ограниченными полномочиями единовременным пользователям или тем, кому не нужны расширенные права. Пользователь Гость часто имеет пустой пароль. Благодаря этому к компьютеру могут подключаться удаленные пользователи. В Windows NT Server версии 4.0 пользователя Гость можно переименовать, но нельзя удалить, а по умолчанию его учетные данные отключены (чтобы пользователь Гость мог регистрироваться в сети, их нужно разрешить).

2.8.5. Копирование пользовательских учетных данных

Если нужно создать учетные данные для большого числа пользователей, например, в университете, где каждый год приходят и уходят сотни студентов, можно определить несколько шаблонов пользователей и при необходимости их копировать. Шаблоны представляют собой учетные данные пользователя со всеми нужными характеристиками, но отключенные с помощью переключателя «Учетные данные запрещены» в Windows NT (в других сетевых ОС имеется аналогичная опция). Если возникает необходимость добавить нового пользователя, достаточно скопировать шаблон. При выполнении такой операции Windows NT копирует значения полей шаблона и позволяет заполнить остальную информацию. Windows NT копирует из шаблона в учетные данные нового пользователя следующие значения:

- Описание (Description).
- Членство в группе (Group Account Memberships).
- Параметры профиля (Profile Settings).
- Пользователь не может изменить пароль (User Cannot Change Password).
- Срок действия пароля не ограничен (Password Never Expires).

Следующие поля в учетных данных (окно New User) ОС Windows NT оставляет пустыми:

- Имя пользователя (Username).
- Полное имя (Full Name).
- Пользователь должен изменить пароль при следующей регистрации (User Must Change Password at Next Logon).
- Учетные данные запрещены (Account Disabled).

Поля «Имя пользователя» и «Полное имя» остаются пустыми для ввода информации о новом пользователе. Переключатель «Пользователь должен изменить пароль при следующей регистрации» устанавливается по умолчанию. В целях защиты, если необходимо, чтобы пользователи изменили присвоенные им пароли при первой регистрации, не сбрасывайте данный переключатель.

2.8.6. Запрет и удаление учетных данных пользователя

Если пользователь больше не должен иметь доступа к рабочей станции, его учетные данные можно отключить. Если в базе данных пользователей оставить активные учетные данные, это позволит потенциальному злоумышленнику продолжать попытки регистрации после блокировки других учетных данных из-за неверного пароля. Запретив учетные данные, вы предотвратите их использование, но сохраните информацию о пользователе, и ее можно будет активизировать в будущем.

Подобный метод полезен для временной блокировки учетных данных отсутствующих сотрудников или отключения тех пользователей, которые себя скомпрометировали. При удалении учетных данных система теряет всю информацию о пользователе. Если учетные данные удалены, а пользователю снова требуется доступ к системе, придется определить их заново и присвоить необходимые полномочия.

Простое создание пользователя с тем же именем не восстановит прежней информации учетных данных, поскольку каждый пользователь идентифицируется для системы не именем, а специальным внутренним идентификатором.

Если пользователь не будет больше работать с системой, следует запретить его учетные данные. Переписав всю важную информацию этого пользователя, вы можете удалить его. Подобная операция уничтожает все параметры и полномочия пользователя, поэтому убедитесь в том, что пользователю действительно не потребуется доступ.

2.8.7. Переименование учетных данных пользователя

Переименовать учетные данные пользователя (включая **Администратор** и **Гость**) можно с помощью Диспетчера учетных записей. Изменить имя пользователя потребуется, например, в том случае, если изменилось выполняемое им задание, или организация реализует новую стратегию именования.

При изменении имени другие характеристики учетных данных не модифицируются. Изменить имена пользователей Администратор и Гость полезно для усиления защиты: злоумышленник, знакомый с заданными по умолчанию именами пользователей Windows NT, не сможет получить доступ к системе, отгадать пароль.

2.8.8. Личные каталоги

В личных (основных) каталогах пользователи хранят свои собственные файлы. Определяя личный каталог в профилях пользователей, можно предоставить им эту частную область. В общем случае обычно устанавливаются полномочия доступа к личному каталогу, разрешающие обращаться к его данным только конкретным пользователям.

По умолчанию Windows NT сохраняет информацию в личном каталоге, если в окне «Сохранить» (Save) не задается явно каталог сохранения. Кроме того, вы попадаете в этот каталог при выходе на приглашение MS-DOS.

2.8.9. Группы

Необходимость задания конкретных полномочий для большого числа пользователей рабочих станций отнимает много времени. К тому же при этом трудно избежать ошибок. В большинстве организаций полномочия определяются не отдельно для каждого пользователя, а с помощью более управляемой концепции защиты — групп пользователей, когда полномочия присваиваются группе. Пользователи, являющиеся членами группы, получают все присвоенные ей полномочия. Членство в группах имеет особенно важное значение в больших сетях.

Группы полезны во многих ситуациях. Предположим, например, что бухгалтерия вашей организации имеет полномочия на доступ ко всем финансовым данным, хранящимся на компьютере. Можно создать в Диспетчере учетных записей группу ФИНАНСЫ и сделать ее членами всех сотрудников данного отдела. Каждый пользователь из группы ФИНАНСЫ будет иметь доступ ко всей финансовой информации.

Группы упрощают назначение полномочий. Присваиваемые группе полномочия будут действовать для каждого ее члена, что позволяет легко внести изменения во всю группу. Например, добавление нового каталога в группу Finance потребует присваивания группе полномочий на этот каталог, к которому в результате смогут обращаться все ее пользователи. Это намного проще, чем давать их каждому пользователю отдельно.

Существуют два основных типа групп: локальные и глобальные. Локальные группы влияют только на рабочую станцию. Глобальные группы влияют на всю сеть и хранятся на главном контроллере домена. Windows 95 и более ранние версии Windows NT не поддерживают информацию о группах, поскольку в данных ОС отсутствует защита ресурсов на уровне отдельных пользователей.

Один пользователь может быть членом нескольких групп, что позволяет создавать группы для многих целей. Например, удобно определить группы в соответствии со структурой организации (администрация, отдел маркетинга, финансовый отдел, производственное подразделение и т.д.). Другие груп-

пы можно создать для главных администраторов, персонала поддержки сети и новых сотрудников. Эта процедура позволяет присвоить полномочия по умолчанию всем членам группы. Если включить пользователя сразу в две группы, то удобно будет, например, определить его полномочия как члена группы ФИНАНСЫ и как нового сотрудника (члена группы НОВЫЕ СОТРУДНИКИ).

Предположим, что член группы ФИНАНСЫ имеет полномочия на доступ к бухгалтерской информации и финансовым данным, а члену группы НОВЫЕ СОТРУДНИКИ к финансовым данным обращаться запрещено (Нет доступа). Сделав пользователя членом обеих групп, вы разрешите ему доступ к бухгалтерской информации, но не к финансовым данным. Когда новый сотрудник заслужит большее доверие, его можно убрать из группы НОВЫЕ СОТРУДНИКИ.

В Windows NT имеется заданная по умолчанию группа Пользователи, которую можно применять для присваивания прав и полномочий всем пользователям сети. При создании пользователей они автоматически становятся членами группы Пользователи. При изменении полномочий заданной по умолчанию группы Users изменяются полномочия всех, кто обращается к компьютеру.

2.8.9.1. Планирование групп

Корректное планирование группы значительно облегчит администрирование и управление пользователями рабочих станций. Опытные администраторы редко присваивают полномочия отдельным пользователям и предпочитают работать с группами. Например, вместо предоставления отдельным пользователям права на резервное копирование системы администратор создает группу и включает в нее пользователей. Благодаря этому при изменениях в процессе резервного копирования достаточно будет модифицировать учетные данные группы. Кроме того, администратор получает удобный способ передачи сообщений всем пользователям, которые могут архивировать данные сети.

В Windows NT Server используются глобальные группы, охватывающие различные компьютеры сети. Они отличаются от локальных групп, создаваемых на Windows NT Workstation.

Присваивание пользователей группам позволяет также отслеживать, кому какие ресурсы необходимы. Например, пользователям, работающим с документами и текстами, необходим доступ к текстовым процессорам, файлам данных и разделяемому каталогу, содержащему документы и шаблоны вашей организации.

При создании групп для сети следует решить, какие пользователи к каким ресурсам будут обращаться. Определите, что общего в доступе отдельных пользователей. В идеальном случае можно присваивать права пользователям, включая их в соответствующие группы. Группы можно строить на основе следующих критериев:

- Функциональные подразделения организации (отдел маркетинга и т.д.).
- Сетевые программы (обработка текста, графика и др.).
- События (званый вечер в компании).
- Сетевые ресурсы (лазерный принтер).
- Местоположение (комната 18).
- Индивидуальные функции (оператор резервного копирования и т.д.).

Если пользователь является членом нескольких групп, некоторые из них могут явным образом разрешать доступ к ресурсу, а другие запрещать его. Запрет доступа отменяет разрешение.

Предположим, что новый пользователь является членом групп ФИНАНСЫ и НОВЫЕ СОТРУДНИКИ. В группе ФИНАНСЫ ему разрешен доступ к каталогу с финансовой информацией, но для членов группы НОВЫЕ СОТРУДНИКИ этот каталог закрыт. В результате такой пользователь не получит доступа к финансовым данным.

В случае конфликтов полномочий Windows NT всегда выбирает наиболее ограничивающие полномочия.

2.8.9.2. Встроенные группы

В большинстве сетевых ОС предусмотрено несколько стандартных групп, назначение которых состоит в удобной организации пользователей и упрощении администрирования. Windows NT также создает при инсталляции стандартные группы пользователей, предоставляя удобные средства администрирования групп. Они могут покрывать все потребности, однако при большом числе пользователей эти

группы можно модифицировать и добавить свои собственные. Для присваивания глобальных полномочий или прав всем локальным пользователям можно также применять специальную группу под именем Все (Everyone). К встроенным (стандартным) относятся следующие группы.

Группа **Операторы учета**. Членам группы разрешено администрирование пользователей и групп. Они могут создавать и удалять учетные данные, а также модифицировать их параметры. Во многих организациях практикуется назначение одного "оператора учетных данных", которому поручается добавление новых пользователей и присваивание им некритичных полномочий. Возможности присваивания прав другим пользователям для членов группы Операторы учета ограничиваются в соответствии с политикой защиты домена.

Группа **Администраторы**. Пользователи группы имеют все права и полномочия на файлы и другие ресурсы на рабочей станции. По умолчанию автоматически создается и включается в группу Администраторы пользователь **Администратор**. Если рабочая станция входит в состав домена, в группу Администраторы будут входить все администраторы домена.

Группа **Операторы архива**. Члены группы могут выполнять команды Backup и Restore, предусмотренные в NT для резервного копирования и восстановления из архива всех файлов на рабочей станции. Применять команды Backup и Restore для работы с собственными файлами могут все пользователи, однако членам группы Операторы архива предоставляются права на все файлы рабочей станции (но только для выполнения команд Backup и Restore).

Группа **Администраторы домена**. Члены группы обладают полномочиями администрирования домена. Пользователи этой группы автоматически включаются в группу Администраторы каждого сервера или рабочей станции домена и имеют все полномочия, предоставленные ее членам.

Группа **Гости домена**. Пользователи, входящие в группу, могут регистрироваться в домене с нестрогой защитой. Данная группа предоставляет ограниченный доступ к сетевым ресурсам.

Группа **Пользователи домена**. Члены группы являются пользователями домена с общими привилегиями. Они автоматически включаются в группы Пользователи каждого сервера или рабочей станции домена и имеют все полномочия членов группы Пользователи.

Группа **Репликатор**. Группа используется службой тиражирования, которая автоматически синхронизирует файлы между рабочими станциями.

Группа **Операторы сервера**. Члены группы могут осуществлять администрирование серверов. Пользователям, входящим в эту группу, разрешается выполнять некоторые административные функции на серверах домена, например конфигурирование устройств или модификацию системных параметров.

Группа **Пользователи**. Члены данной группы имеют обычные права и полномочия пользователей. Группа предназначена для большинства пользователей, т.е. для тех, кто должен иметь доступ к рабочей станции, но не входит при этом в число администраторов системы или сети. Члены группы могут выполнять приложения, управлять файлами на рабочей станции, использовать локальные и сетевые принтеры. Кроме того, им доступны такие операции, как создание и управление собственными группами, работа со своим профилем. Все создаваемые вами новые пользователи автоматически включаются в эту группу.

2.8.9.3. Создание групп

В Windows NT группы создаются практически так же, как пользователи. В **Диспетчере учетных записей** заполните поля Group Name (имя группы), Description (описание) и Members (члены группы).

Поле **Имя группы** (Group Name) идентифицирует локальные группы. К имени группы применяются те же ограничения, что и к имени пользователя. Эти имена должны быть уникальными. Они могут содержать только буквы верхнего или нижнего регистра, цифры или символы, отличные от следующих: " / \ : ; | = + * ? < >.

В поле **Описание** (Description) вводится описание группы.

В поле **Члены группы** (Members) вводится список пользователей.

2.9. Привилегии субъекта NT

Каждый субъект представляет собой право на выполнение субъектом действий, касающихся системы в целом, а не отдельных объектов.

- Привилегия завершать работу и перезагружать.
- Привилегия одного процесса, входа.

При входе в систему пользователь получает привилегии, предоставленные группой и индивидуально. Назначает привилегии администратор. Данные привилегии позволяют проходить некоторые защиты.

- Привилегии создавать резервные копии информации. Позволяют игнорировать разграничение доступа.
- Привилегия восстановления информации.
- Привилегия назначать процессам высокий приоритет.
- Привилегия отлаживать программы, позволяет обращаться к любому процессу по любому методу.
- Привилегия загружать и выгружать драйверы и сервисы.
- Привилегия аудитора – позволяет маскировать свои действия.
- Привилегия администратора.
- Привилегия добавлять запись в журнал аудита, запись любой информации.
- Привилегия назначать процессу маркер доступа.
- Привилегия выступать как часть ОС.

2.10. Файловая система NTFS

NTFS обеспечивает комбинацию эффективности, надежности и совместимости, отсутствующую в FAT. Она разработана для быстрого выполнения стандартных файловых операций типа чтения, записи и поиска, а также улучшенных операций типа восстановления файловой системы на очень больших жестких дисках.

NTFS также включает возможности безопасности, требуемые для файловых серверов и высококачественных персональных компьютеров в корпоративной среде. NTFS поддерживает управление доступом к данным и привилегии владельца, что является важным для целостности корпоративных данных. В то время как каталогам, разделяемым при помощи Windows NT Server, назначаются специфические разрешения, файлам и каталогам NTFS могут назначаться разрешения вне зависимости, разделены они или нет. NTFS - единственная файловая система в Windows NT, которая позволяет назначить разрешения для отдельных файлов.

NTFS является простой, но очень мощной разработкой. Для этой перспективной файловой системы вся информация на томе NTFS является файлом или частью файла. Каждый распределенный на томе NTFS сектор принадлежит некоторому файлу. Даже метаданные (metadata) файловой системы (информация, которая описывает непосредственно файловую систему) являются частью файла.

Эта основанная на атрибутах файловая система поддерживает объектно-ориентированные приложения, обрабатывая все файлы как объекты, которые имеют определяемые пользователем и системой атрибуты.

Каждый файл на томе NTFS представлен записью в специальном файле, называемом главной файловой таблицей (MFA - master file table). NTFS резервирует первые 16 записей таблицы для специальной информации.

Первая запись этой таблицы описывает непосредственно главную файловую таблицу. За ней следует зеркальная запись (mirror record) MFT. Если первая запись MFT разрушена, то NTFS читает вторую запись для отыскания зеркального файла MFT, первая запись которого идентична первой записи MFT. Местоположения сегментов данных MFT и зеркального файла MFT записаны в секторе начальной загрузки. Дубликат сектора начальной загрузки находится в логическом центре диска. Третья запись MFT - файл регистрации (log file) используется для восстановления файлов. Семнадцатая и последующие записи главной файловой таблицы используются собственно файлами и каталогами (также рассматриваются как файлы NTFS) на томе.

Главная файловая таблица отводит определенное количество пространства для каждой записи файла. Атрибуты файла записываются в распределенное пространство MFT. Небольшие файлы и каталоги

(обычно до 1500 байт или меньше) могут полностью содержаться внутри записи главной файловой таблицы.

Подобный подход обеспечивает очень быстрый доступ к файлам. Рассмотрим, например, файловую систему FAT, которая использует таблицу размещения файлов, в которой перечисляются имена и адреса каждого файла. Элементы каталога FAT содержат индекс в таблице размещения файла. В случае если необходимо просмотреть содержимое файла, FAT сначала читает таблицу размещения файлов и убеждается в существовании файла. Далее FAT восстанавливает файл, ища цепочку распределенных блоков, относящихся к этому файлу. В NTFS поиск файла производится только для непосредственного его использования.

Записи каталога помещены внутри главной файловой таблицы так же, как записи файла. Вместо данных каталоги содержат индексную информацию. Небольшие записи каталогов находятся полностью внутри структуры MFT. Большие каталоги организованы в дерево, имея записи с указателями на внешние кластеры, содержащие элементы каталога, которые не могли быть записаны внутри структуры MFT.

2.10.1. Атрибуты файла NTFS

NTFS просматривает каждый файл (или каталог) как набор атрибутов файла. Такие элементы, как имя файла, информация зашиты и даже данные - все это атрибуты файла. Каждый атрибут идентифицирован кодом типа атрибута и необязательно именем атрибута.

Таблица 2.3

Атрибуты файла NTFS

Тип атрибута	Описание
Standard Information (стандартная информация)	Включает бюджет связи и так далее
Attribute List (список атрибутов)	Перечисляет все другие атрибуты (только в больших файлах)
Filename (имя файла)	Атрибут, повторяющийся для длинных и для коротких имен файлов. Длинное имя файла может содержать до 255 символов Unicode. Короткое имя - доступно для MS-DOS, восемь плюс три символа, без учета регистра. Дополнительные имена, или жесткие связи (hard links), используются POSIX и могут быть также включены в качестве дополнительных атрибутов имени файла
Security Descriptor (дескриптор безопасности)	Фиксирует информацию о том, кто может обращаться к файлу, кто является его владельцем и так далее
Data (данные)	Содержит данные файла
Index Root (корень индексов)	Используется при работе с каталогами
Index Allocation (индексное размещение)	Используется при работе с каталогами
Volume Information (информация тома)	Используется только в системном файле тома и включает в частности версию и имя тома
Bitmap (битовый массив)	Предоставляет информацию об использовании записей в MFT или каталоге
Extended Attribute Information (информация расширенного атрибута)	Используется файловыми серверами, которые связаны с системами OS/2. Этот тип атрибута не используется Windows NT
Extended Attributes (расширенные атрибуты)	Используется файловыми серверами, которые связаны с системами OS/2. Этот тип атрибута не используется Windows NT

Если атрибуты файла могут находиться внутри записи файла MFT, они называются резидентными (resident) атрибутами. Например, информация типа имени файла и отметки времени всегда включается в запись файла MFT. Если файл слишком большой, чтобы содержать все атрибуты в записи файла MFT, часть атрибутов является нерезидентной (nonresident). Нерезидентные атрибуты занимают один

или несколько пробегов (run) дискового пространства в другом месте тома (пробег дискового пространства - непрерывная линейная область на диске).

Вообще, все атрибуты могут быть вызваны как поток байтов независимо от того, являются ли они резидентными или нерезидентными.

В табл. 2.4 представлен список всех атрибутов файла, в настоящее время определенных для NTFS. Этот список расширяем, т. е. другие атрибуты файла в будущем могут быть определены в случае необходимости.

2.10.2. Длинные и короткие имена файлов

NTFS поддерживает имена файла до 255 символов. Имена файла NTFS используют набор символов Unicode с 16 битами; однако вопрос доступа из MS-DOS решен. NTFS автоматически генерирует поддерживаемое MS-DOS имя (восемь плюс три символа) для каждого файла. Таким образом, файлы NTFS могут использоваться через сеть операционными системами MS-DOS и OS/2. Это особенно важно для файловых серверов организации, которая использует персональные компьютеры с двумя или всеми тремя этими операционными системами.

Создавая имена файла "восемь плюс три", NTFS также позволяет приложениям MS-DOS и Windows 3.x работать с файлами, имеющими длинные имена NTFS. Кроме того, при сохранении файла приложениями MS-DOS или Windows 3.x на томе NTFS сохраняются и имя файла "восемь плюс три" и длинное имя NTFS.

При сохранении файла приложениями MS-DOS или Windows 3.x на томе NTFS, если приложение сохраняет временный файл, удаляет первоначальный файл и переименовывает временный файл с первоначальным именем, длинное имя файла теряется. Любой уникальный набор разрешений файла также теряется. Разрешения передаются заново из родительского каталога.

Необходимо внимательно подходить к использованию групповых символов типа * и ? вместе с командами del и copy. При выполнении этих команд NTFS работает и с длинным, и с коротким именем файла; таким образом, могут быть удалены или скопированы лишние файлы.

Для копирования или перемещения файлов с чувствительными к регистру длинными именами самым надежным способом является выбор файлов с использованием мыши в Диспетчере файлов. Этот способ позволяет однозначно определить файлы для выполнения операций над ними.

Поскольку NTFS использует набор символов Unicode для имен файлов существует возможность задействования нескольких "запрещенных" символов, которые MS-DOS не может читать в имени файла. Для генерации короткого имени файла в стиле MS-DOS NTFS удаляет все эти символы и любые пробелы из длинного имени файла. Так как имя файла в MS-DOS может иметь только одну точку, NTFS также удаляет все дополнительные точки из имени файла. Далее, в случае необходимости NTFS усекает имя файла до шести символов и добавляет тильду (~) и номер. Например, к каждому недублированному имени файла добавляется ~1. Повторяющиеся имена файлов заканчиваются символами ~2, ~3 и т. д. Расширение имени файла усекается до трех или меньшего количества символов. Наконец, при отображении имени файла в командной строке NTFS транслирует все символы в имени файла и расширении к верхнему регистру.

2.10.3. Безопасность файловой системы NTFS

Основные характеристики **NTFS** (New Technology File System):

- устойчивость к отказам;
- высокая производительность;
- безопасность;
- совместимость;
- удобство в работе.

Уязвимые места NTFS:

- Она не может автоматически определить права.
- Не гарантирует сохранность данных - безопасность только при загруженной NT.

- Не защищает прикладные программы правами read only от изменения прав в автоматическом режиме.
- Права доступа не применяются при резервном копировании на магнитную ленту.

Недостатки:
- Работа с дискетами (NTFS нельзя использовать для форматирования томов меньше 5 мегабайт).
- Большие накладные расходы (не рекомендуется использовать с диском менее 900 мегабайт).
- Нет выделения квот. Для каждого файла, каталога существует ACL, который содержит пользователей и группы, обладающие правом доступа к файлу.

Ограничения NT 4.0 на домен:
- Администраторские права не могут быть на стороне части пользователей.
- Использование доверительных отношение не может решить проблему связи с администратором нескольких доменов.
- Размещение очередей печати и других элементов зависит от их физического расположения. Переход из одного домена в другой вызывает определенные затруднения.
- Система репликации контролеров доменов недостаточно гибкая.

Безопасность NTFS, во-первых, достигается за счет существования файла транзакции, в который записывается изменения в файлах и каталогах и в случае ошибки происходит откат назад. Через некоторое время файл транзакций из оперативной памяти переписывается на жесткий диск. В случае нормального завершения работы файл транзакций обнуляется и в нем остается только последняя контрольная точка оперативной коррекции - дополнительного средства для устойчивости файловой системы. Восстановления файлов по алгоритму:
- анализ;
- повторение;
- возврат.

Во-вторых, в NTFS реализованы следующие возможности:
- отложенная запись;
- одновременное считывание зеркальных дисков;
- для расщепления могут использоваться более двух дисков;
- сжатие файлов.

В-третьих, NTFS предоставляет возможности:
- установка прав доступа;
- включение аудита и владения информацией;
- метки времени последнего обращения;
- безопасное уничтожение файла.

2.10.4. NTFS в Windows 2000. Active Directory

Active Directory – это служба каталогов Microsoft. Она входит в состав Windows 2000 и в ней хранится информация об объектах и службах сети.

Служба каталогов – система указателей, размещенных в базе данных. Она должна обеспечить единую информацию о сети, средства идентификации, управления доступом, навигации и др.

Применяя средства доступа к Active Directory, эту информацию могут получить и пользователи и компьютер и приложения. Архитектура Active Directory основана на концепции иерархии системных имен (**Domain Network System**).

Хотя Active Directory не описана в стандарте RFC, но их структуры все равно похожи и приблизительно сравнимы с современным алфавитным справочником:
1. Алфавитные указатели.
2. Структуры отсортированные по групповым иерархиям.

В Windows NT, DNS и Active Directory связаны:
- в сети должен быть DNS-сервер;

- для домена сети используется иерархическая система DNS имен;
- расположение служб, AD определяет по запросам DNS.

Для работы Active Directory необходим DNS-сервер, в котором определены записи ресурсов – DNS-записи, с помощью которых можно выполнить поиск сетевых служб.

И Windows NT, и Windows 2000 предоставляют вышеописанные возможности, но в Windows NT нельзя использовать безопасное динамическое обновление. Windows 2000 частично поддерживает передачу зоны. Зона в домене идентифицирует те объекты, которыми можно управлять централизовано, а также определять границы области, в пределах которой будет обеспечен заданный уровень безопасности. Управление, создание объектов возложено на пользователей, которые назначены администраторами домена, привилегии которых по сравнению с другими пользователями не выходят за рамки домена. Привилегии, которыми обладает пользователь в первом домене, не распространяются на другие домены (аналогично в целом политике безопасности).

Иерархия AD:
- Комплексы, деревья лесов, доменов и подразделений (organization\unit).
- Домены – структуры деревья – леса.
- Внутри подразделений – сеть – группы пользователей и компьютеров.

Деревья и леса:
- Каждый домен может иметь родителя. Для всех дочерних доменов существует иерархическая структура, но вышележащие домены не могут управлять ресурсами подчиненных доменов
- Используется структура систем имен DNS-домены, которые разделяют одно и то же пространство имен DNS-дерево.
- При использовании различных пространств имен домены могут являться частями одной и той же иерархической структуры.
- Образ – лес, в котором деревья обладают доверительными отношениями.

Базовые концепции AD:

Доменная структура NT4 – плоская, а AD – объемная.
1. Домен: Структура соответствует идеям, заложенным в стандарте X500. Отличия в организации организационных единиц, OU (Organization unit) – позволяет расщепить домен на ряд блоков, упрощающих работу. Группы могут формироваться из компьютеров и пользователей. Это позволяет часть прав делегировать у пользователей. Эти OU организуются в иерархию, имеющую трехмерность.
2. Группы (как в NT4.0). Использование групп противоречит основополагающим принципам службы каталогов (все объекты должны образовывать иерархическую структуру в соответствии с тем, как они расположены в дереве каталога), но все равно является основным средством распределения ресурсов.
3. Объекты – пользователи. Все ресурсы точно так же, как в NT4.0
4. Узел – Site – группа компьютеров, локальная сеть (LAN) не является полноправной частью AD, а связана с физическим расположением компьютеров, но тем не менее это неотъемлемая часть организации данных (используется в BackOffice)

В AD используется совершенно новая технология – **Global Catalog** (GC) – содержит все объекты из всех доменов; с каждым объектом хранится сокращенное описание его характеристик. Одна из функций GC - поиск объекта во всем дереве.

Рекомендовано размещать GC в каждом узле – обеспечивает присутствие локального средства с помощью которого клиент может осуществить все операции поиска. Создается автоматически.

OU (Organization Unit) поддерживает иерархическую систему имен , используя описательные имена. Использование этих объектов – расширяет функции администрирования в W2K либо во всем домене либо в дереве всех подразделений. AD дает возможность назначить единые права для отдельного продукта, только если он один входит в OU. Права не могут быть для нескольких доменов – AD администрируется как несколько активных доменов, а не как единое дерево.

Еще одним ключевым элементом AD является **Directory Schema** (DS) – описывает способ сохранения объектов в каталоге - позволяет создавать новые поля в уже существующих объектах и создавать новые типы объектов. В AD используется упрощенная версия DS из X500.

Права доступа и наследования в AD осуществляются по правилам:

- Все изменения в AD в DS каталога вступают в силу автоматически. Для уровня дерева, куда они были внесены, а также для всех подчиненных ему уровней наследование в AD статистическое. Изменения будут внесены во все объекты, на которые оно распространяется. При статистическом наследовании для большого количества объектов необходим больший объем данных в реплицировании, но за счет этого AD работает быстрее.
- AD не использует объекты OU в качестве базиса для назначения прав доступа.
- Возможно назначение прав по всей организации. В AD нет различий между локальными и глобальными группами.

2.11. Реестр (registry) Windows NT

Реестр (registry) Windows NT — это централизованная база данных, уникальная для каждого компьютера с данной операционной системой. В нем хранятся конфигурационные параметры для всех компонентов системы, включая установки оборудования, драйверов устройств, сетевых протоколов и плат адаптеров. Там же содержится информация об установленных в системе приложениях и пользователях Windows NT.

2.11.1. Структура реестра

Управление более старыми системами фирмы Microsoft (вроде Windows 3.1 или Windows for Workgroups) и работающими в них приложениями осуществлялось обычно установкой значений для параметров, хранящихся в текстовых файлах. Такие файлы с расширением .INI создавала практически каждая программа на компьютере. Следить за этими файлами и их модифицировать для системного администратора было весьма непросто. Поэтому разработчики операционной системы Windows NT решили отказаться от INI-файлов и создать единую унифицированную структуру данных для хранения параметров и самой операционной системы, и ее приложений. Эта структура и получила название реестра.

Каждый компонент Windows NT (служба, драйвер или определенная программа) сохраняет все необходимые для его нормальной работы параметры и установки в отдельной части реестра. Такие части называются разделами (keys), и в целом они аналогичны отдельным секциям (т. е. частям, которые начинаются с ключевого слова в квадратных скобках) INI-файлов системы Windows 3.1. В раздел записываются параметры (values), различающиеся своими названиями. Каждый из параметров имеет тип (value type), в соответствии с которым может принимать то или иное значение (value data). В языках программирования параметры реестра аналогичны переменным программы, также имеющим имя, тип и значение.

Секции INI-файлов не могли включать в себя вложенные секции. А вот разделы реестра Windows NT могут иметь подразделы (subkeys). Поэтому реестр представляет собой иерархическую древовидную структуру. На ее верхнем уровне располагаются так называемые ветви (subtrees). В версии 4.0 этих ветвей пять:

- HKEY_LOCAL_MACHINE;
- HKEY_USERS;
- HKEY_CLASSES_ROOT;
- HKEY_CURRENT_CONFIG;
- HKEY_CURRENT_USER.

Однако не все из них независимы друг от друга. На самом деле основными ветвями являются лишь первые две — остальные представляют собой их подразделы и служат для более быстрого доступа к содержащимся в них параметрам.

2.11.2. Управление системой через реестр

Изменения в настройках драйверов, сетевых протоколов, служб или установленных в системе приложениях приводят к модификации параметров тех разделов реестра, которые относятся к соответствующему аппаратному или программному компоненту. Например, если администратор Windows NT в диалоговом окне Network из Панели управления поменяет порядок привязки сетевых протоколов к

службе сервера, то эти изменения будут сохранены в параметрах раздела CurrentControlSetX\Services\lanmanServer\Linkage ветви HKEY_LOCAL_MACHINE. А если пользователь с помощью программы System из той же Панели управления захочет установить значение какой-либо переменной окружения (environment variable), то соответствующий этой переменной параметр появится в разделе Environment ветви HKEY_CURRENT_USER. Таким образом, управление системой Windows NT осуществляется путем изменения значений тех или иных параметров реестра.

Чаще всего реестр модифицируют косвенно, поскольку это не требует от системного администратора дополнительных знаний о конкретных параметрах: как они должны называться, в какой раздел помещены и какие значения могут принимать. Примером косвенной работы с реестром могут служить изменения настроек в программах Панели управления или в Редакторе системной политики POLEDIT (в режиме редактирования реестра). Какие параметры реестра изменятся при использовании Редактора системной политики зависит от его настройки, а точнее, от содержимого текстовых файлов WINNT.ADM и COMMON.ADM.

Программа REGEDT32 (и близкая к ней по назначению REGEDIT) позволяет получить практически неограниченный доступ к любой части реестра. В этой программе системный администратор имеет дело с разделами и параметрами реестра в том виде, в каком они хранятся и применяются операционной системой или приложениями. Поэтому пользоваться Редактором реестра рекомендуется с большой осторожностью.

2.11.3. Основные кусты реестра

Реестр формируется в памяти компьютера при запуске системы Windows NT. При этом используются несколько файлов из папки \winnt_root\System32\Config (winnt_root — название папки, где была установлена операционная система, например WINNT). Разделы реестра, которым соответствуют эти файлы, называются кустами (hives). Основные кусты реестра находятся в ветви HKEY_LOCAL_MACHINE и называются SAM, SECURITY, SOFTWARE и SYSTEM. Первые два используются системой безопасности Windows NT: раздел SAM — не что иное, как база данных Диспетчера учетных записей, а SECURITY хранит информацию, используемую локальным администратором безопасности (LSA). В кусте SOFTWARE хранятся настройки программного обеспечения того или иного производителя, а в SYSTEM — конфигурационная информация (параметры драйверов и служб), необходимая для загрузки операционной системы.

Раздел HARDWARE ветви HKEY_LOCAL_MACHINE не является кустом, поскольку находящаяся в нем информация не сохраняется в каком-либо файле. При каждом запуске Windows NT данные в этот раздел записываются заново. Они либо извлекаются из памяти аппаратных компонентов (firmware) компьютеров с RISC-процессорами, либо собираются программой NTDETECT.COM для компьютеров с x86-процессорами.

При редактировании параметров реестра (любым из рассмотренных выше способов) новые значения сохраняются и в памяти, и в файле на магнитном диске. Целостность данных реестра в процессе их модификации обеспечивает механизм, основанный на применении журналов транзакций. Любое изменение, вносимое в реестр, вначале фиксируется в журнале (для этого у каждого из кустов существует свой отдельный файл с расширением .LOG) и только затем переносится в файл соответствующего куста. Такой механизм позволяет предотвратить повреждение информации, если в момент ее модификации происходит аппаратный сбой. При следующем запуске системы Windows NT на основе анализа журналов транзакций определяется, какие изменения на момент сбоя были завершены, а какие — нет. Первые записываются в файл, соответствующий нужному кусту реестра, вторые просто удаляются из журнала.

Кроме ветви HKEY_LOCAL_MACHINE, в которой находится информация, относящаяся ко всему компьютеру с операционной системой Windows NT в целом, в реестре есть ветвь HKEY_USERS. Здесь располагаются разделы и параметры, определяющие настройки программного обеспечения для отдельных пользователей Windows NT (т. е. профили пользователей). Обычно в данной ветви реестра хранятся только Профили пользователей, в данный момент зарегистрированных в системе (в том числе и в качестве службы), а также профиль по умолчанию (DEFAULT).

Для функционирования операционной системы Windows NT и дополнительно установленных приложений, для нормальной работы пользователей важно, чтобы все вышеупомянутые разделы реестра содержали правильную информацию. Это в первую очередь относится к разделам ветви HKEY_LOCAL_MACHINE. Так, например, ошибочные значения параметров в разделе SYSTEM могут привести к тому, что какой-либо драйвер или служба Windows NT перестанет загружаться, а это может

привести к невозможности успешной загрузки всей системы. Модификация параметров раздела SOFTWARE способна вызвать ошибки в работе тех или иных программ, установленных на компьютере. А при неправильных изменениях в разделах SAM и SECURITY пользователи не смогут войти в систему для работы на данном компьютере или в домене.

2.11.4. Информация о безопасности реестра

Ясно, что в многопользовательской операционной системе, такой как Windows NT, доступ разных пользователей к параметрам реестра необходимо строго разграничивать и контролировать. Для этого разделы и подразделы реестра защищаются в системе так же, как, например, папки и вложенные папки на дисках, отформатированных с файловой системой NTFS. Настройка параметров системы безопасности для разделов реестра осуществляется с помощью программы REGEDT32. Упоминавшаяся ранее программа REGEDIT из комплекта Windows NT версии 4.0, хоть и позволяет манипулировать системным реестром, средств работы с информацией о безопасности не имеет. С другой стороны, в эту программу включены гораздо более развитые средства поиска. Используя ее, можно осуществлять поиск нужной последовательности символов не только в названиях разделов и подразделов, но и в именах и значениях параметров реестра. REGEDIT (в отличие от REGEDT32) также позволяет изменять названия разделов, что иногда просто необходимо.

Уже говорилось, что реестр строится в оперативной памяти при загрузке системы Windows NT. При этом на основании информации, содержащейся в файлах папки \wint_root\System32\Config, для каждого раздела и подраздела создается отдельный объект. Доступ к этим объектам контролируется операционной системой, так же как и доступ к любым другим объектам. Кроме данных, хранящихся в соответствующем разделе или подразделе, у каждого такого объекта имеется свой отдельный список прав доступа, который определяет, какие разрешения пользователи и группы будут иметь при доступе к параметрам данного раздела и, соответственно, какие действия с этими параметрами они могут выполнять. Сюда также можно поместить записи, которые задают режим регистрации действий, выполнявшиеся соответствующим разделом реестра. И, наконец, у каждого раздела реестра есть владелец (owner). Как и в случае файлов и папок на диске с NTFS, владельцем может быть либо конкретный пользователь компьютера или домена, либо группа Администраторы, если раздел создан пользователем, членом данной группы. Кроме того, в качестве владельца (например раздела HKEY_LOCAL_MACHINE\SAM\SAM) может выступать и операционная система (Владелец: SYSTEM).

Еще раз отметим, что объекты реестра в оперативной памяти создаются для разделов и подразделов, но не для отдельных параметров. Именно поэтому в отличие от NTFS (где разрешения можно установить и для папок, и, отдельно, для файлов, находящихся в них) при работе с реестром Windows NT разрешения назначаются только на уровне раздела. Они распространяются на все параметры, которые находятся в соответствующем разделе. Отдельные разрешения на доступ к тому или иному параметру раздела установить нельзя, однако для подразделов можно установить собственные разрешения.

2.11.5. Разрешения на доступ к разделам реестра

Как уже говорилось, разрешения на доступ к тому или иному разделу реестра (т. е. для модификации дискреционного списка прав доступа) обычно изменяются с помощью программы REGEDT32. Установив в ней в качестве текущего нужный раздел, выберите затем в меню Security команду Permissions, и на экране появится диалоговое окно со списком прав доступа к данному разделу.

Окно Registry Key Permissions сильно напоминает окно управления списком прав доступа к папке или файлу на диске с файловой системой NTFS. Разрешения на доступ к разделу, которые можно дать пользователю или группе, в этом окне обозначены как Read, Full Control и Special Access (однако разрешения No Access, как в случае NTFS, нет). Выбор в меню команды Special Access вызывает одноименное диалоговое окно, где можно выборочно установить нужные права доступа к соответствующему разделу. Список этих прав и их краткое описание приведены в табл. 2.5.

Тип доступа к разделу, обозначенный в редакторе реестра как Read, соответствует набору прав Q + E + N + R, тип доступа Full Control позволяет выполнять любые действия с данным разделом. Довольно часто в списке присутствуют записи с набором прав Q + S + C + E + N + D + R. Этот набор примерно соответствует типу доступа Change в случае файловой системы NTFS.

Для просмотра значений параметров тех или иных разделов реестра и списков прав доступа к разделам системный администратор может использовать программу REGEDT32. Однако некоторые про-

граммы независимых поставщиков существенно облегчают эту работу и позволяют выводить нужную информацию в более удобном для анализа виде. Из числа таких программ отметим уже упоминавшуюся ранее DUMPACL фирмы Somarsoft и DUMPREG этой же фирмы.

Таблица 2.5

Права доступа к разделу реестра

Право доступа	Дает возможность...
Query Value (Q)	...прочесть значения параметров раздела, а также узнать время последнего изменения параметров раздела
Set Value (S)	... записать в раздел новые параметры и изменить значения уже существующих
Create Subkey (C)	... создать подраздел в данном разделе
Enumerate Subkeys (E)	... просмотреть список подразделов
Notify (N)	... получить оповещение об изменениях в данном разделе
Create Link (L)	... создать в разделе символическую ссылку (symbolic link) на другой раздел
Delete (D)	... удалить данный раздел целиком и/или отдельные его параметры
Write DAC(W)	... изменить список прав доступа к разделу
Write Owner (O)	... стать владельцем раздела
Read Control (R)	...просмотреть информацию о разрешениях на доступ к разделу

В Наборе Resource Kit для Windows NT также имеется ряд программ (и с графическим интерфейсом, и запускаемых из командной строки) для работы с системным реестром. Например, запускаемая из командной строки программа SECADD позволяет удалить группу Everyone из списков прав доступа выбранного раздела реестра локального или удаленного компьютера. С ее помощью можно также разрешить пользователю или группе Windows NT доступ на чтение к указанному в командной строке разделу.

2.11.6. Права доступа по умолчанию

Разрешения на доступ к разделам реестра, установленные в системе Windows NT по умолчанию, не позволяют обычным пользователям модифицировать его части, наиболее важные для функционирования самой операционной системы, ее системы безопасности и большинства приложений. Некоторые разделы ветви HKEY_LOCAL_MACHINE, в частности SAM и SECURITY, по умолчанию недоступны для просмотра и модификации даже администратору (хотя последний может просмотреть и изменить список прав доступа к ним).

Однако для ряда разделов реестра разрешения, с точки зрения безопасности, недостаточно жестки. В первую очередь это относится к разделам, в списках прав доступа которых наличествует группа Everyone [часто с типом доступа Full Control или набором прав Q + S + C + E + N + D + R, включающим права на модификацию (S) и удаление (D) параметров или всего раздела. Такие разрешения дают взломщику возможность получить доступ к отдельным частям реестра локального или удаленного компьютера как для чтения находящейся в них информации, так и для ее модификации. Причем удаленное подключение такого рода можно осуществить и применив учетную запись пользователя Guest (если она не заблокирована), и с помощью анонимного входа. Необходимо также учитывать наличие в списках прав доступа к определенным разделам реестра и записей для группы INTERACTIVE. Напомним: в эту специальную группу автоматически попадает любой пользователь, интерактивно зарегистрировавшийся на данном компьютере с системой Windows NT. По умолчанию группа INTERACTIVE присутствует в списках прав доступа к разделам ветви HKEY_CLASSES_ROOT (или, что то же самое, к подразделам раздела HKEY_LOCAL_MACHINE\Software\Classes) с тем же самым набором прав Q + S + C + E + N + D + R. Это позволяет его членам модифицировать и удалять параметры указанных разделов.

2.11.7. Защита от локального доступа

Защита реестра от локального доступа позволяет усилить безопасности операционной системы Windows NT. Рассмотрим способы реализации такой защиты.

2.11.7.1. Ограничение прав группы Everyone

Поскольку отдельные разделы реестра системы Windows NT доступны членам группы Everyone, имеет смысл предпринять ряд мер, позволяющих более надежно защитить эту базу данных конфигурационной информации от попыток модификации со стороны неправомочных пользователей отдельного компьютера или домена.

С этой целью фирма Microsoft рекомендует после установки системы изменить разрешения группы Everyone на Read (Q + E + N + R) для разделов, перечисленных ниже (с подразделами, если это указано явно):

- в ветви HKEY_LOCAL_MACHINE
  - Software
  - Software\Microsoft\RPC
  - Software\Microsoft\Windows\CurentVersion\Run
  - Software\Microsoft\Windows\CurentVersion\RunOnce

    Особо обращаем ваше внимание на эти два раздела: перечисленные в них приложения выполняются (по крайней мере один раз) при запуске операционной системы Windows NT, поэтому они работают в контексте безопасности ОС и, естественно, имеют доступ ко всем ресурсам компьютера.
  - Software\Microsoft\Windows\CurentVersion\Uninstall. Здесь находится список программ, позволяющих убрать те или иные из ранее установленных на компьютере приложений.
  - Software\Microsoft\Windows\CurentVersion\AeDebu
  - Software\Microsoft\Windows\CurentVersion\Compatibility
  - Software\Microsoft\Windows\CurentVersion\Drivers
  - Software\Microsoft\Windows\CurentVersion\Embedding
  - Software\Microsoft\Windows\CurentVersion\Fonts
  - Software\Microsoft\Windows\CurentVersion\FontSubstitutes
  - Software\Microsoft\Windows\CurentVersion\Font Drivers
  - Software\Microsoft\Windows\CurentVersion\Font Mapper
  - Software\Microsoft\Windows\CurentVersion\Font Cache
  - Software\Microsoft\Windows\CurentVersion\GRE_Initialize
  - Software\Microsoft\Windows\CurentVersion\MCI
  - Software\Microsoft\Windows\CurentVersion\MCI_Extensions
  - Software\Microsoft\Windows\CurentVersion\Perflib
    Можно даже убрать группу Everyone из списка прав доступа к этому разделу, что не позволит ее членам получать сведения о производительности вашего компьютера.
  - Software\Microsoft\Windows\CurentVersion\Potrs (и подразделы)
  - Software\Microsoft\Windows\CurentVersion\ProfileList
  - Software\Microsoft\Windows\CurentVersion\Type 1 Installer
  - Software\Microsoft\Windows\CurentVersion\(и подразделы)
  - Software\Microsoft\Windows\CurentVersion\Windows3.1MigrationStatus (и подразделы)
  - System\CurrentContolSet\Services\LanmanServer\Shares
  - System\CurrentContolSet\Services\UPS
- ветвь HKEY_CLASSES_ROOT и все ее подразделы
- раздел HKEY_USERS\DEFAULT (и подразделы).

2.11.7.2. Права группы INTERACTIVE

Члены группы INTERACTIVE обладают достаточно большими правами на модификацию разделов ветви HKEY_CLASSES_ROOT, в которой хранится информация об ассоциациях файлов по расширениям и сведения, относящиеся к функционированию механизмов связывания и внедрения объектов (Object Linking and Embedding, OLE). Данная информации необходима для нормальной работы в Windows NT большинства приложений, в том числе и тех, что входят в состав самой операционной системы.

Например, если вы попробуете удалить из реестра раздел, относящийся к файлам с расширением .COM или .EXE, вы тем самым потеряете способность, работая в Windows NT, запускать соответствующие исполняемые файлы двойным щелчком мыши. Убрав из реестра раздел с именем .Ink, вы лишите пользователей возможности запуска приложений через меню Start.

Фирма Microsoft не дает никаких рекомендаций относительно того, нужно ли ограничивать права доступа членов группы INTERACTIVE к реестру Windows NT. В связи с этим нужно жестко следить за тем, каким пользователям необходимо иметь право входить в систему интерактивно на том или другом компьютере. Это особенно касается контроллеров доменов, поскольку, работая на них, системный администратор обычно управляет пользователями и ресурсами своего домена. Напомним, что по умолчанию правом входа в систему на контроллерах домена обладают только члены группы АДМИНИСТРАТОРЫ и нескольких групп операторов. Учитывая изложенные выше соображения, администратор должен по возможности ограничивать количество членов указанных групп.

2.11.8. Защита от удаленного доступа

Защита реестра Windows NT от удаленного доступа (т.е. от просмотра и модификации при подключении по сети) также позволяет усилить безопасность этой операционной системы.

2.11.8.1. Использование раздела winreg

Одним из методов ограничения сетевого доступа к реестру является использование специального раздела, появившегося в версии 4.0 операционной системы Windows NT. Это раздел SYSTEM\CurrentControlSet\Control\ SecurePipeServers\winreg в ветви HKEY_LOCAL_MACHINE.

Регулируя разрешения на доступ к данному разделу, администратор может четко определить круг пользователей, имеющих право удаленного доступа к реестру данного компьютера. По умолчанию в системе Windows NT Server такое право есть только у членов локальной группы Administrators. В системе Windows NT Workstation такой раздел по умолчанию отсутствует, но может (вернее, даже должен) быть создан после установки. Изменения в списке прав доступа раздела winreg, а также изменения в параметрах его подразделов (см. далее) вступают в силу после перезагрузки системы.

Еще раз подчеркнем: право удаленного доступа к реестру получают только пользователи или группы, перечисленные в списке прав доступа к указанному разделу, а не в его подразделах или параметрах. Остальные пользователи Windows NT и члены других групп такой возможности иметь не будут. Тем не менее, чтобы разрешить последним доступ по сети к определенным разделам реестра, эти разделы можно перечислить в параметрах Machine и Users подраздела winreg\AllowedPaths. Указанные параметры должны иметь тип REG_MULTI_SZ. В первый из них заносятся названия подразделов ветви HKEY_LOCAL_MACHINE (например, System\CurrentControlSet\ Control\Print\Printers — для обеспечения доступа к информации об общих принтерах данного компьютера или System\CurrentControlSet\Services\Replicator — для нормальной работы службы репликации). Второй может содержать сведения о подразделах ветви HKEY_USERS. Внесение в тот или иной параметр названия какого-либо раздела разрешает и сетевой доступ к его подразделам. При этом проверка удаленного доступа к таким разделам реестра осуществляется на основе установленных для них локальных разрешений.

Однако, несмотря на ограничения, накладываемые рассмотренным выше способом, просмотр определенных областей реестра (в частности, раздела .DEFAULT ветви HKEY_USERS) при анонимном сетевом подключении все же возможен.

2.11.8.2. Ограничение доступа через анонимные подключения

С целью защиты реестра Windows NT от удаленного доступа через анонимный вход можно заменить группу Everyone в списках прав доступа к разделам на группу, в которую администратор внесет всех

пользователей компьютера (или домена). В качестве такой группы можно указать, например, группы Users или Authenticated Users. Последняя создается в Windows NT версии 4.0 в процессе установки Service Pack 3 и отличается от Everyone только тем, что ее членами не являются пользователи, подключившиеся к компьютеру анонимно.

При выполнении процедуры замены одной группы в списках прав доступа на другую большую помощь может оказать программа REGADMIN фирмы Midwestern Commerce. В отличие от REGEDT32 она позволяет не только заменять списки прав доступа к разделам реестра, но и редактировать их (примерно так, как это делает программа CACLS при запуске с ключом /E в случае файлов и каталогов).

Другим способом полностью запретить доступ к реестру через анонимные подключения к службе сервера Windows NT является установка Service Pack 3 для версии 4.0 или соответствующей «заплаты» (sec-fix) для версии 3.51.

2.11.9. Аудит реестра

Кроме защиты реестра Windows NT, системный администратор может установить режим регистрации событий, связанных с доступом к тому или иному разделу реестра. Как и в случае других объектов этой операционной системы, для этого надо внести соответствующие записи в системный список прав доступа к нужному разделу. В первую очередь это относится к тем разделам, в которых хранится информация, необходимая Локальному администратору безопасности (HKEY_LOCAL_ MACHINE\SECURITY) и Диспетчеру учетных записей (HKEY_ LOCAL_MACHINE\ SAM).

2.11.9.1. Настройка аудита реестра

Вначале надо проверить, включен ли в программе User Manager for Domains режим аудита событий, связанных с доступом к файлам и объектам (File and Object Access).

Для указанных выше разделов, связанных с системой безопасности, рекомендуется установить аудит на успешное или неуспешное выполнение таких действий, как Query Value, Set Value, Write DAC и Read Control для всех пользователей, обладающих административными полномочиями в системе. Можно это сделать и для группы Everyone, но тогда количество записей аудита в журнале безопасности будет больше. Чтобы отслеживать только изменения, можно не следить за событиями типов Query Value и Read Control.

Установить параметры аудита администратор может в диалоговом окне Registry Key Auditing, доступ к которому в программе REGEDT32 осуществляется выбором команды Auditing из меню Security. В качестве стартового раздела при выполнении этой операции лучше выбрать SECURITY, поскольку он, кроме всего прочего, включает символическую ссылку на раздел SAM. Таким образом, администратор может проставить нужные параметры аудита для двух указанных разделов одновременно (обратите внимание на установленный флажок Audit Permission on Existing Subkeys)

При желании системный администратор может подобным образом установить режим аудита и для других разделов реестра системы Windows NT. Поскольку доступ к разным разделам (и для чтения, и для записи информации) может осуществляться довольно часто, делать это нужно только в случае действительной необходимости.

2.11.9.2. Анализ записей аудита

После настройки аудита реестра информация о чтении и модификации параметров соответствующих разделов будет появляться в журнале безопасности Windows NT. При этом следует учитывать, что количество записей о событиях категории Object Access может быть довольно велико. В таком случае администратору может потребоваться увеличить размер журнала безопасности или предпринять другие меры для сохранения записываемой в него информации.

Системный администратор должен периодически просматривать и анализировать записи аудита, в том числе те, что относятся к событиям доступа к тому или иному разделу реестра. Отметим, что имеющейся в этих записях информации не всегда достаточно, чтобы однозначно определить, какой пользователь выполнил то или иное действие.

3. Архитектуры подсистем безопасности сетевых операционных систем

В современных условиях ОС должны обеспечивать безопасные службы передачи сообщений, поддержку серверных (многопользовательских) процессов, таких, как системы управления базами данных, Web-серверы, мониторы транзакций и т.д.

Рассмотрим архитектуры подсистем безопасности сетевых ОС в сравнении Microsoft Windows NT Server 4.0 и Novell IntranetWare 4.11 с точек зрения:

- сетевого клиента;
- сервера файлов;
- сервера приложений.

Каждый из подразделов построен следующим образом: вначале дается общее описание некоторого механизма подсистемы безопасности сетевой операционной системы, а затем приводится реализация этой функции в сравниваемых операционных системах.

3.1. Обзор архитектур операционных систем Microsoft Windows NT Server 4.0 и Novell IntranetWare 4.11

Windows NT

Windows NT создавалась как операционная система общего применения, в которую, помимо средств совместного использования файлов и принтеров, были включены службы передачи сообщении и поддержки сетевых приложений. И Windows NT Server, и Windows NT Workstation имеют одну и ту же архитектуру подсистемы безопасности и, следовательно, весьма похожие средства защиты информации. Ввиду этого сеть на основе Windows NT (в которой присутствуют и серверы, и рабочие станции) - это сеть равных. В большинстве случаев функциональные возможности, доступные серверным приложениям, в не меньшей степени доступны и на рабочих станциях Windows NT Workstation.

Централизованная модель администрирования домена Windows NT Server предпочтительнее при создании систем клиент-сервер. Применение одноранговых свойств Windows NT Workstation не рекомендуется, так как с ростом числа компьютеров управление такой системой резко усложняется.

Приложения имеют доступ к некоторым службам подсистемы безопасности Windows NT, например, к таким, как механизмы аутентификации. Вне зависимости от того, осуществляется ли доступ к локальным ресурсам или к сетевым, процесс получит к ним доступ только после аутентификации и проверки прав на доступ операционной системой. Такая проверка осуществляется прозрачным для пользователя способом.

Как для рабочей станции, так и для сервера реализованы средства аудита системных событий. Приложения могут использовать эти же службы для аудита собственных событий.

IntranetWare

IntranetWare реализует классическую архитектуру «клиент-сервер»: клиент посылает запрос серверу, сервер его обрабатывает и возвращает ответ клиенту. В архитектуре IntranetWare предполагается, что клиент и сервер - разные компьютеры. К моменту выхода IntranetWare приложения обычно выполнялись на клиентских машинах, а сервер предоставлял безопасные средства совместного использования сетевых ресурсов, таких как файлы и принтеры. Приложения на серверах IntranetWare обычно не размещались.

IntranetWare оптимизирована для работы в такой среде и поэтому выполняет функции файл- и принт-сервера очень хорошо.

IntranetWare - серверная, а не клиентская операционная система, а функционалы сервера и рабочей станции сильно различаются. Средства обеспечения информационной безопасности со стороны клиента, естественно, зависят от того программного и аппаратного обеспечения, которое на нем установлено.

3.2. Архитектура сетевого клиента

На сетевом клиенте обычно выполняются приложения, которым необходим доступ к совместно используемым данным и ресурсам, управляемым серверами сети. Такие приложения должны быть защищены друг от друга и в состоянии ограничить или запретить доступ к собственным данным со стороны других таких же программ. Ядро безопасности (подсистема ОС), в свою очередь, должно быть изолировано от таких приложений, чтобы имеющие ошибки или злонамеренные программы не могли нанести вреда самой операционной системе или повлиять на работу механизмов безопасности.

Помимо этого сетевой клиент ответствен за идентификацию и аутентификацию пользователя - получая от него соответствующую информацию (например имя и пароль), сетевой клиент должен обеспечить ее защиту от компрометации как при хранении на рабочей станции, так и при передаче такой информации по сети.

Для выявления попыток несанкционированного вторжения в систему или определения причин происшедших сбоев необходимо вести журнал действий работающих за компьютером пользователей, в котором фиксируются такие события, как запуск и завершение программ. Так как сетевые атаки редко используют какое-либо одно средство или службу операционной системы, то администратор безопасности должен иметь возможность проанализировать все системные события в их взаимосвязи, чтобы понять, кем, когда и как была совершена попытка обойти службы защиты информации.

Это требование диктует необходимость соблюдения последовательности и четкой согласованности протоколируемой информации о событиях, произошедших в операционной системе, службах защиты информации и поддержки сети.

Windows NT

Windows NT Workstation существенно использует код и программное обеспечение Windows NT Server. Это приводит к тому, что средства защиты информации этих операционных систем похожи. До предоставления доступа к любым ресурсам (как локальным, так и сетевым) пользователь должен быть идентифицирован и должен успешно пройти процедуру аутентификации.

Последующие обращения к ресурсам управляются их списками контроля доступа, в которых владелец ресурса четко указывает, кто и с каким уровнем полномочий может получить к ним доступ. Каждое обращение к ресурсу может быть подвергнуто аудиту, а каждая запись журнала имеет четкое указание на уникальный в системе идентификатор пользователя.

В среде Windows NT можно запускать программы, не вызывающие доверия, без риска повреждения операционной системы или других приложений. Такие программы запускаются в собственном адресном пространстве и не могут получить доступ к коду или данным других приложений и операционной системы в обход четко определенных (и контролируемых ядром и подсистемой безопасности) прикладных интерфейсов программирования.

Ядро Windows NT работает в привилегированном режиме - режиме ядра. Любые программы не могут «уравнять» себя в правах с ядром, перейдя в тот же режим работы, и не могут прямо воспользоваться низкоуровневыми функциями и механизмами операционной системы. Вместо этого пользовательские программы и службы обязаны обращаться к четко определенному набору интерфейсов прикладного программирования, доступ к которым контролируется ядром.

Для нужд безопасной межпрограммной коммуникации в состав Windows NT включена поддержка протоколов Secure Distributed Component Object Model (Secure DCOM) и Secure Sockets Layer (SSL).

IntranetWare

IntranetWare является серверной операционной системой и сама по себе не может служить в качестве рабочей станции - сетевого клиента. Фирма Novell не производит собственных клиентских операционных систем. Таким образом, ответственность за выбор действительно безопасной при использовании совместно с IntranetWare клиентской ОС полностью ложится на проектировщика сети.

Разработка безопасного сетевого клиента является далеко не тривиальной задачей: как уже отмечалось ранее, такой клиент должен обеспечивать аутентификацию пользователей, защиту паролей, контроль доступа к локальным ресурсам рабочей станции, целостность ядра безопасности, предоставлять защиту приложений от вредоносного воздействия других программ и гарантировать возможность ревизии действий субъектов системы. В опубликованных фирмой Novell материалах можно найти несколько

рекомендуемых ею подходов к решению этого комплекса проблем: некоторые из них основываются на ограничении функциональности сетевого клиента как такового, другие рекомендуют использование специализированных аппаратных средств.

Для повышения уровня безопасности фирма Novell рекомендует использовать дополнительно продукты стороннего разработчика - например систему Assure EC 4.11 производства компании Sistex.

Assure EC 4.11 является основывающейся на специальной дополнительной плате с процессором AMD 386SX однопользовательской системой, работающей под управлением операционной системы MS-DOS.

Приемлемый уровень информационной безопасности сетевого клиента Sistex достигается тем, что устанавливаемое в персональный компьютер дополнительное аппаратное обеспечение служит ядром безопасности - им перехватываются все обращения к файлам и системным устройствам, а значит, имеется и возможность ограничения доступа к таким ресурсам. При включении компьютера аппаратура Assure EC перехватывает управление системой, проводит аутентификацию пользователя, а затем производит запуск операционной системы. Операционная система реально выполняется как приложение поверх ядра Assure EC в том же адресном пространстве, что и другие программы. Поэтому данный программно-аппаратный комплекс не в состоянии обеспечить ни защиту ОС от злонамеренных или имеющих ошибки программ, ни защиту программ от деструктивного влияния друг на друга, ни обеспечить контроль доступа к объектам операционной системы. Ядро безопасности, однако, является защищенным, так как оно работает исключительно в рамках дополнительной платы Sistex и недоступно другим программам.

3.3. Сравнение архитектур безопасности сетевых клиентов

Ниже приводятся основные требования к подсистеме обеспечения информационной безопасности сетевого клиента. После краткого описания того или иного принципа резюмируется его реализация в Windows NT 4.0 и IntranetWare 4.11. Так как IntranetWare не является клиентской операционной системой, в сравнении этих характеристик использовался клиент Sistex Assure EC 4.11.

3.3.1. Аутентификация

Клиентская операционная система ответственна за проведение идентификации пользователя и проверку достоверности введенных идентификационных данных. Обычно такая процедура реализуется посредством запроса имени (идентификация) и пароля пользователя (аутентификация), пытающегося получить доступ к системе, хотя возможны и иногда применяются альтернативные способы "установления личности", например, цифровые сертификаты или биометрические системы.

Данные, используемые процедурами аутентификации, должны быть защищены от несанкционированного доступа и модификации как во время нахождения под управлением операционной системы, так и в процессе передачи по сети. Система аутентификации должна обладать средствами усиления парольной дисциплины и контроля устаревших паролей, а также обладать функциями определения и предотвращения вторжений в систему - такими, как, например, блокировка бюджетов пользователей и привязка к конкретным рабочим станциям.

Windows NT

До того как пользователь сможет получить доступ к любым системным ресурсам, операционная система Microsoft Windows NT требует прохождения им обязательной процедуры аутентификации на основе запроса его имени и пароля. Результатом этого является то, что пользователь может получить доступ к сетевым данным и приложениям, а также к локальным ресурсам своей рабочей станции, пройдя такую процедуру только один раз. Кроме того, Windows NT как на сервере, так и на рабочей станции предоставляет стандартные интерфейсы программирования для интеграции альтернативных механизмов аутентификации пользователей (например на основе смарт-карт или биометрических систем), заказных средств поддержания парольной дисциплины, аутентификации удаленного доступа.

Пароли хранятся в зашифрованном виде. В сетевых процедурах аутентификации используется механизм "запрос-ответ" таким образом, что парольная информация никогда не циркулирует в сети в открытом виде.

В Windows NT включены мощные средства администрирования парольной дисциплины, включая средства управления периодом их устаревания, минимальной длиной, требованиями к входящим в них символам, хранением парольной истории пользователя. Сетевой клиент Windows NT может быть настроен на полное запрещение доступа к сетевым ресурсам указанным пользователям или на ограничение такого доступа указанными временными интервалами. Каждый пользователь Windows NT может обладать разным уровнем прав и привилегий в системе.

IntranetWare

Сетевой клиент Sistex Assure EC 4.11 проводит аутентификацию на основе запроса имени и пароля пользователя. Введенный пользователем пароль используется для генерации криптографического сеансового ключа, который для проведения аутентификации передается по сети сетевому серверу. Парольная информация не защищена от компрометации во время нахождения в оперативной памяти рабочей станции, так как доступ к системной памяти не контролируется и не ограничивается операционной системой. В качестве решения этой проблемы клиент Sistex предоставляет функции явного удаления такой информации из оперативной памяти компьютера.

Сама по себе рабочая станция не обладает средствами и усиления парольной дисциплины, и ее контроля, не имеет функций предотвращения несанкционированного вторжения в вычислительную сеть и т.д. Эти задачи возложены на соответствующие средства операционной системы Novell IntranetWare.

3.3.2. Контроль доступа

Все системные объекты безопасного сетевого клиента, такие, как приложения, файлы, процессы, системные устройства и т.д. (список определяется операционной системой) должны быть защищены от несанкционированного использования не только механизмами аутентификации, но и специальными средствами контроля доступа. Такие средства должны гарантировать, что владелец объекта будет иметь возможность самостоятельного определения, какие из субъектов системы смогут получить доступ к такому объекту и с каким уровнем привилегий (например, доступ только на чтение без возможности удаления или модификации). Доступ к ресурсам рабочей станции должен управляться с точностью до отдельного пользователя. Владелец ресурса должен иметь возможность предоставить или запретить доступ к определенному объекту каждому конкретному пользователю.

Windows NT

Подсистема безопасности Windows NT дает возможность каждому владельцу некоторого ресурса задать конкретные права доступа к нему при помощи графического интерфейса, в котором субъекты системы идентифицируются своими именами. Контроль доступа не ограничивается только файлами и системными устройствами, этой обязательной для Windows NT процедуре подлежит также доступ к процессам, памяти, рабочему столу, именованным каналам, таймерам, разделяемым ресурсам, системным службам, ключам реестра и многим другим объектам операционной системы.

Приложения Windows NT могут самостоятельно задавать права доступа к собственным объектам как в локальной, так и в клиент-серверной среде.

IntranetWare

Аппаратные средства клиента Sistex обеспечивают средства разграничения доступа к ресурсам системы, перехватывая трафик шины персонального компьютера и, следовательно, ограничены в своих возможностях управления доступом объектами, связанными с процедурами ввода-вывода, а именно, файлами и устройствами ввода-вывода. Память, процессы, таймеры и прочие системные объекты управлению доступом не подвержены. Любая программа может получить прямой доступ к любому участку оперативной памяти компьютера. Операционная система может быть легко повреждена или модифицирована злонамеренным или имеющим ошибки приложением.

Однако ядро безопасности располагается на плате расширения Assure EC и не может быть модифицировано пользовательскими программами.

3.3.3. Аудит

Следующим важным требованием к безопасному сетевому клиенту является реализация им средств аудита (ревизии) системных событий. Все важные системные события должны протоколироваться в виде, пригодном для последующего анализа.

Журнал аудита системных событий является важным средством в процессе обнаружения и предотвращения попыток несанкционированного доступа к системе. Поэтому записи такого журнала не могут ограничиваться только регистрацией попыток входа в систему и доступом к файлам. Необходимо также иметь возможность отслеживания доступа к объектам, расположенным в системной памяти, запуска и остановки приложений, загрузки и выгрузки драйверов и всех прочих системных событий, которые потенциально могут возникать в процессе "взлома" системы безопасности.

Журнал системных событий, используемый при ревизии системы, должен быть, в свою очередь, защищен от доступа со стороны неавторизованного персонала. Операционная система должна включать в свой состав инструменты ревизии системы в целом и действий отдельных пользователей.

Windows NT

Подсистема аудита Microsoft Windows NT в состоянии протоколировать попытки обращения к любому из объектов операционной системы. Средства аудита в любой момент могут быть отключены или вновь активизированы администратором. В отличие от решения Novell подсистемы аудита серверного и клиентского вариантов Windows NT совместимы друг с другом как по составу протоколируемых событий, так и в части формата хранимых данных.

Системный администратор заранее определяет размер файла журнала событий и то, каким образом должна поступать операционная система в случае его заполнения: перезаписывать наиболее старые системные события новыми или производить остановку ОС.

В операционную систему включены средства просмотра ревизионного журнала и его сохранения во внешних файлах. Защита от несанкционированного доступа к журналу событий обеспечивается посредством определения списков контроля доступа к нему, которыми определяется список авторизованных пользователей и их права.

IntranetWare

Из-за того что средства обеспечения информационной безопасности Sistex Assure EC основываются только на аутентификации пользователя и перехвате событии ввода-вывода, подсистема аудита ограничена регистрацией только этих событий. События исключительно этого рода могут в полной мере контролироваться подсистемой безопасности. Доступ к оперативной памяти, запуск и завершение пользовательских процессов, загрузка и выгрузка драйверов и даже перезапись системных областей оперативной памяти не подвержены регистрации, что делает задачу анализа журнала событий с целью определения попыток несанкционированного вторжения в систему трудноразрешимой,

Кроме того, генерируемый Assure EC журнал не совместим с аналогичными средствами IntranetWare, хотя и располагается на сервере. Защита от несанкционированного доступа к журналу событий обеспечивается посредством задания списков контроля доступа к нему, которыми определяется список авторизованных пользователей и их права. Для этого используются собственные средства Novell IntranetWare 4.11.

3.3.4. Изоляция подсистемы безопасности

Следующим требованием к безопасному сетевому клиенту является четкая изоляция средств обеспечения информационной безопасности от внешних программных воздействий - обеспечение целостности подсистемы безопасности. Операционная система или аппаратные средства клиента сети должны защищать приложения, системный код и данные от всех попыток модификации злонамеренными или имеющими ошибки приложениями. Эти меры призваны обеспечить невозможность обхода подсистемы безопасности. Код и данные пользовательских приложений также должны быть защищены от несанкционированного воздействия на них.

Windows NT

Ядро безопасности Windows NT защищено от воздействия пользовательских процессов концепцией домена исполнения. Приложения работают в пользовательском режиме, а операционная система и подсистема безопасности – в режиме ядра. "Охрана" границы между этими режимами и невозможность ее нарушения обеспечивается аппаратными средствами. Ядро Windows NT имеет доступ ко всем ресурсам всех доменов исполнения, тогда как приложения пользовательского режима не имею г доступа к ресурсам ядра; таким образом, плохо написанные программы или программные "бомбы" не могут разрушить, повредить или обойти службы операционной системы, и в частности подсистему безопасности.

Кроме того, каждое приложение обладает своим адресным пространством, изолированным от адресных пространств других программ, что обеспечивает защиту программ от внешних воздействий.

IntranetWare

В архитектуре безопасного сетевого клиента Sistex защита подсистемы безопасности обеспечивается дополнительными аппаратными средствами, устанавливаемыми в обычный персональный компьютер IBM PC. Подсистема обеспечения информационной безопасности физически отделена от операционной системы и недоступна ни ей, ни исполняемым приложениям.

В такой архитектуре службы информационной безопасности защищены от вредоносных программных воздействий, но целостность ОС и пользовательских приложений не контролируется. Кроме того, как уже отмечалось выше, исполняемая поверх Assure EC операционная система не защищена от пользовательских приложений, а приложения - от вредоносного воздействия друг на друга.

3.3.5. Аутентификация рабочих станций

Клиентские рабочие станции должны присоединяться к вычислительной сети безопасным образом. Эта функция необходима для предотвращения вторжения в сеть при помощи портативного или "чужого" компьютера.

Windows NT

Рабочие станции, работающие под управлением Windows NT Workstation, при интеграции в сеть Windows NT должны быть явно определены на контроллере домена и обязаны успешно пройти процедуру собственной аутентификации. Только после этого пользователям, работающим за этим компьютером, будет предоставлена попытка пройти процедуру аутентификации.

IntranetWare

Операционная система Novell IntranetWare не имеет аналогичных средств и не может аутентифицировать рабочие станции. Для попытки "взлома" сети IntranetWare не требуется доступ к какому-то специальному компьютеру — злоумышленник может использовать свой собственный ПК.

Попытку регистрации в сети Novell IntranetWare можно предпринять сразу же после установки клиентского программного обеспечения, например Client32. Защищенный клиент Sistex Assure EC 4.11 средствами аутентификации рабочих станций не обладает в силу того, что такая функция не поддерживается серверной операционной системой, для совместной работы с которой он предназначен.

3.3.6. Безопасные коммуникации

Рабочие стации должны иметь возможность безопасного обмена информацией с сетевыми серверами и между собой.

Windows NT

Windows NT имеет встроенные криптографические средства, доступные для использования пользовательскими приложениями и допускающими расширение за счет продуктов сторонних разработчиков.

Кроме того, можно использовать "подпись"' сетевых пакетов, аналогично описанной ниже реализации того же принципа в Novell IntranetWare.

IntranetWare

В сети IntranetWare имеется возможность использования процедур "подписи" сетевых пакетов. Каждое сетевое сообщение может быть снабжено трудноподделаевым "ярлыком", состоящим из комбинации "подписи" рабочей станции и случайного числа.

Сервер IntranetWare проверяет "подпись" полученного по сети пакета и, если она не верна, отбрасывает его.

Использование подписи пакетов позволяет защититься от попыток несанкционированного получения доступа к сети путем симуляции злоумышленником сетевого графика легального пользователя.

3.3.7. Управление безопасностью

Последним требованием к безопасному клиенту вычислительной сети является предоставление инструментов эффективного управления подсистемой безопасности. Минимальный набор таких инструментов должен включать в себя средства управления бюджетами пользователей, паролями и списками контроля доступа к защищаемым ресурсам.

Желательно, чтобы интерфейс таких средств позволял администратору управлять безопасностью в масштабах всей сети в целом.

Windows NT

В состав Windows NT входит ряд средств управления безопасностью, среди которых можно упомянуть редактор системных правил (System Policy Editor), редактор конфигурации средств безопасности (Security Configuration Editor) и консоль управления (Microsoft Management Console). Все эти средства используют графический интерфейс Windows.

IntranetWare

В реализации Novell управление безопасностью рабочих станций и сервера четко разделяется. Для решения этих задач используются различные средства.

Администрирование бюджетов пользователей и настройка средств безопасности сети Novell IntranetWare может производиться как с консоли управления сервером, так и удаленно, при помощи программы Remote Console (RCONSOLE).

Консоль управления сервером, в отличие от Windows NT, не защищена процедурами аутентификации - любой, имеющий к ней физический доступ, может исполнить любые допустимые команды управления сервером. По этой причине часто серверы Novell помещаются в отдельной комнате (иногда от них отключают клавиатуру и монитор), а все администрирование производится удаленно. Программа удаленного управления сервером IntranetWare предоставляет те же возможности управления сервером, что и доступные с его консоли.

Отрицательной стороной использования средств удаленного управления серверами Novell IntranetWare является то, что несанкционированное использование RCONSOLE предотвращается только паролем, а не комбинацией "имя пользователя/пароль". Аутентификация только на основе введенного пароля не дает возможности отследить пользователя, выдавшего команду управления сервером в журнале системных событий, что сильно затрудняет попытки отследить злоумышленника или хотя бы определить, какой из сетевых администраторов компании выдал конкретную команду управления сервером.

Приводимая ниже табл. 3.1 резюмирует подходы Microsoft и Novell к реализации безопасного клиента сети на основе Windows NT Server 4.0 и IntranetWare 4.11 соответственно.

Таблица 3.1

Сравнение архитектур сетевых клиентов

Требования	Функции	Windows NT 4.0	Sistex Assure EC 4.11
Аутентификация	Возможность определения прав и привилегий для каждого пользователя	Да	Да
	Имя пользователя / пароль	Да	Да
	Шифрование парольной информации	Да	Да
	Средства поддержания парольной дисциплины	Да	Да
	Ограничение возможности работы указанными компьютерами	Да	Да
	Ограничение возможности работы указанными временными интервалами	Да	Да
	Возможность замены процедур аутентификации пользователей	Да	Нет
Контроль доступа	Списки контроля доступа к файлам и системным устройствам	Да	Да
	Списки контроля доступа к объектам системной памяти	Да	Нет
Аудит	Аудит событий аутентификации	Да	Да
	Аудит попыток доступа к файлам и системным устройствам	Да	Да
	Аудит событий операционной системы	Да	Нет
	Средства анализа журнала событий с графическим интерфейсом	Да	Нет
Изоляция подсистемы безопасности	Защита операционной системы	Да	Нет
	Защита приложений	Да	Нет
Аутентификация рабочих станций	Функция безопасного присоединения к сети	Да	Нет
Безопасные коммуникации	Встроенные средства безопасной передачи данных в сетевой среде	Да	Да
Управление безопасностью	Средства управления с графическим интерфейсом	Да	Нет
	Одинаковые инструменты управления клиентом и сервером	Да	Нет
Доступность	Работа на стандартном ПК	Да	Нет

3.4. Сравнение архитектур безопасности серверов файлов

Функцией сервера файлов является предоставление контролируемого доступа к файлам, принтерам, приложениям, выполняющимся на рабочих станциях - клиентах сервера. Следовательно, файловый сервер обязан обеспечивать развитые средства защиты контролируемых им ресурсов посредством развитой системы контроля доступа. Не менее необходимо наличие служб ревизии системных событий для обнаружения и предотвращения попыток несанкционированного доступа к нему. Далее приводятся основные требования к подсистеме обеспечения информационной безопасности сервера файлов.

3.4.1. Аутентификация

Windows NT

Как во время хранения на сервере, так и в процессе передачи по сетевым каналам парольная информация, используемая в процедурах аутентификации Windows NT, защищена криптографическими средствами.

Аутентификация клиентов сервера Windows NT производится всегда. Операционная система Windows NT может быть настроена на запрещение любого доступа к сети либо на его ограничение указанными промежутками времени и заданными параметрами учетных записей пользователей.

ОС Windows NT использует концепцию безопасного запуска, которая обеспечивает невозможность проникновения хакера в систему с помощью «троянского коня».

Системы, работающие под управление как Windows NT Workstation, так и Windows NT Server, могут быть заблокированы - находиться в состоянии, когда пользователь не сможет выключить работающий компьютер с консоли. Последовательность загрузки может быть настроена таким образом, чтобы запуск системы производился только с жесткого диска, обеспечивая невозможность старта компьютера с альтернативной операционной системой.

IntranetWare

Как во время хранения на сервере, так и в процессе передачи по сетевым каналам парольная информация, используемая в процедурах аутентификации IntranetWare, защищена криптографическими средствами.

На консоли управления сервером IntranetWare не требует in/ идентификации, ни аутентификации пользователя. Любой, получивший физический доступ к консоли управления сервером, сможет выполнить любую команду управления им. Это приводит к тому, что требования к физической защите консоли управления сервером Novell IntranetWare намного строже, чем аналогичные требования Microsoft Windows NT.

IntranetWare также обладает полным набором функций по ограничению прав использования сетевых ресурсов определенными бюджетными записями пользователей сети, конкретными временными промежутками или конкретными рабочими станциями.

3.4.2. Контроль доступа

Windows NT

Операционная система Microsoft Windows NT обладает полным набором средств, обеспечивающих контроль доступа к объектам сервера. Владелец определенного ресурса или пользователь, обладающий соответствующими правами, в состоянии ограничить или запретить чтение, запись, удаление или модификацию таких объектов.

В Windows NT доступ к любому защищенному объекту определяется одной и той же структурой данных (SECURITY_INFO) и контролируется одним и тем же механизмом (Security Reference Monitor). Такой подход существенно упрощает разработку прикладного программного обеспечения, использующего службы информационной безопасности Windows NT, и способствует формированию надежной программной инфраструктуры предприятия.

IntranetWare

Операционная система Novell IntranetWare обладает полным набором средств, обеспечивающих контроль доступа к объектам сервера. Владелец определенного ресурса или пользователь, обладающий соответствующими правами, в состоянии ограничить или запретить чтение, запись, удаление или модификацию таких объектов.

В Novell IntranetWare, с точки зрения служб информационной безопасности, существуют два совершенно различных типа объектов: объекты NetWare или Novell Directory Services и объекты файловой системы, которые были оставлены в качестве отдельного класса из соображений обратной совместимости. Решение о предоставлении доступа конкретному субъекту системы к объектам разных типов принимается различными подсистемами Novell IntranetWare, что без нужды усложняет подсистему обеспечения информационной безопасности.

3.4.3. Ревизия

Windows NT

Журналы системных событий Windows NT Server и Windows NT Workstation совместимы друг с другом. Такой журнал может быть локально проанализирован любым клиентом или сервером NT. Для этого достаточно воспользоваться программой **Просмотр событий** (Event Log), работающей не только на Windows NT, но и на платформе Windows 9x.

Доступ к такому журналу ревизии системных событий защищается стандартными средствами избирательного доступа к ресурсам Windows NT.

IntranetWare

Несмотря на то, что обе рассматриваемые платформы требуют принятия мер по физическому ограничению доступа к консоли управления сервером (система не может быть достаточно защищена, если не контролируется физический доступ к компьютеру, на котором она работает), в случае использования Novell IntranetWare эти ограничительные меры должны носить более жесткий характер.

Дело в том, что, как уже упоминалось ранее, консоль управления сервером IntranetWare не защищается процедурами идентификации и аутентификации, и поэтому система протоколирования системных событий Novell IntranetWare не в состоянии определить, кто именно выдал ту или иную команду управления сервером. Средства безопасности управляющих инструментов IntranetWare в основной степени полагаются на меры физической безопасности консоли управления.

Серверных утилит анализа или просмотра журнала ревизии в IntranetWare не предусмотрено, вместо них предлагается пользоваться программами, исполняемыми на клиентских рабочих местах, например приложением AUDITCON. Данная программа не имеет графического интерфейса и требует использования в режиме командной строки. В частности, это означает, что системный администратор обязан помнить набор ее специфичных команд, что приводит к дополнительным затратам времени и финансов на обучение персонала.

Доступ к журналу ревизии системных событий защищается стандартными средствами избирательного доступа к ресурсам IntranetWare.

3.4.4. Изоляция подсистемы безопасности

Windows NT

Microsoft Windows NT для собственной работы использует специальный режим работы - режим ядра. Пользовательские же приложения исполняются в другом режиме - режиме пользователя. В этом режиме не существует способа получения доступа к программам привилегированного режима, кроме как посредством четко определенных (и защищаемых) интерфейсов прикладного программирования.

IntranetWare

В случае IntranetWare пользовательские приложения исполняются на рабочих станциях клиентов сети, а не на сервере. Таким образом, серверная операционная система физически изолирована от неблагоприятного или злонамеренного влияния пользовательских программ. Архитектура IntranetWare усиливает защищенность операционной системы за счет ее гибкости.

Приводимая ниже табл. 3.2 резюмирует подходы Microsoft и Novell к реализации сервера файлов Windows NT Server 4.0 и IntranetWare 4.11 соответственно.

Таблица 3.2

Сравнение архитектур серверов файлов

Требования	Функции	Windows NT 4.0	Novell Intra-netWare 4.11
Аутентификация	Имя пользователя / пароль	Да	Не на консоли
	Шифрование парольной информации	Да	Да
	Криптографическая защита парольной информации	Да	Да
	Усиление парольной дисциплины	Да	Да
Контроль доступа	Списки контроля доступа к файлам и устройствам	Да	Да
Аудит	Аудит доступа к файлам и устройствам	Да	Да
	Аудит административных операций	Да	Да
	Идентификация пользователя в журнале ревизии	Да	Не на консоли
	Просмотр журнала событий на сервере	Да	Нет
	Средства анализа журнала ревизии с графическим интерфейсом	Да	Нет
	Ограничение доступа к ревизионному журналу списками контроля доступа	Да	Да
Изоляция подсистемы безопасности	Защита операционной системы	Да	Да
Управление безопасностью	Средства управления с графическим интерфейсом	Да	Да
	Одинаковые инструменты управления клиентом и сервером	Да	Нет

3.5. Сравнение архитектур безопасности серверов приложений

Работа операционной системы в качестве сервера приложений масштаба предприятия выдвигает дополнительные требования к подсистеме обеспечения информационной безопасности. В отличие от уже рассмотренных случаев сетевого клиента и сервера файлов требуется как минимум обеспечить следующие возможности:

- дополнительной защиты операционной системы и приложений друг от друга через усиление средств изоляции подсистем;
- минимизации риска неправильного администрирования системы -- привилегии, предназначенные для использования пользовательскими приложениями, должны быть спроектированы так, чтобы обеспечить достаточную управляемость правами серверных программ по доступу к системным ресурсам, и в то же время набор допустимых привилегий должен быть разумно минимален во избежание ошибок при их предоставлении.

3.5.1. Изоляция подсистемы безопасности

Серверная операционная система обязана защищать себя от несанкционированного воздействия других программ, а также защищать приложения от воздействия других программ, реализуя и четко контролируя принцип изоляции различных подсистем от возможных злонамеренных действий. Зачастую весь бизнес предприятия зависит от данных, хранимых и / или обрабатываемых сервером приложений, поэтому задача изоляции объектов операционной системы от несанкционированных действий начинает играть наипервейшую роль.

Windows NT

Microsoft Windows NT использует несколько режимов работы - режим ядра и режим пользователя. Приложения, исполняющиеся в пользовательском режиме, не в состоянии получить прямой доступ к

данным или исполняемому коду режима ядра, минуя четко контролируемый специальный интерфейс прикладного программирования.

Аварийное завершение пользовательского приложения не влияет на операционную систему. Программы не могут повредить ОС или другие приложения. Парольная информация и другие важные системные данные хранятся и обрабатываются исключительно в режиме ядра.

Из-за такого архитектурного решения заключением о соответствии Windows NT классу защищенности C2 допускается выполнение непроверенных приложений с сохранением присвоенного Агентством национальной безопасности США (National Security Agency) класса защищенности.

IntranetWare

Несмотря на то, что средства защиты Novell IntranetWare 4.11 вполне адекватны при ее использовании в качестве файлового сервера (приложения исполняются на клиентских рабочих станциях), их архитектура совершенно не удовлетворяет требованиям к подсистеме безопасности сервера приложений.

Основной проблемой является то, что в IntranetWare приложения пользуются тем же адресным пространством, что и операционная система. (Это архитектурное решение вызвано используемым IntranetWare принципом: приложения должны исполняться на рабочих местах клиентов сети). В отличие от Windows NT, серверные приложения Novell IntranetWare могут рассматриваться как драйверы устройств, что означает их фактическое превращение из пользовательских программ в равноправную часть операционной системы. Очевидным следствием этого факта является то, что расположенные на сервере IntranetWare приложения обладают теми же правами по доступу к ресурсам, что и сама ОС.

Отсутствие средств изоляции подсистемы безопасности Novell IntranetWare от серверных приложений означает, что злонамеренная или имеющая ошибки программа может повредить или обойти службы защиты операционной системы и, следовательно, скомпрометировать данные, находящиеся под защитой ОС.

Серверные приложения Novell IntranetWare по той же причине уязвимы к атакам со стороны других аналогичных программ. Все серверные приложения IntranetWare делят одно адресное пространство и уязвимы к атакам посредством «троянских коней», вирусов и сетевых «червяков».

3.5.2. Управление привилегиями

Важным требованием к защищенной операционной системе является следующее: такая система должна предоставлять приложениям привилегии уровня операционной системы контролируемым и ограниченным образом. Управление привилегиями - это возможность регулирования объема прав по выполнению системных операций, предоставляемых пользовательским приложениям. Например, в Unix-системах существует понятие «суперправ» - привилегии «root». Пользователь или программа, обладающая таким уровнем привилегий, может делать с системой практически что угодно: работать в привилегированном режиме с аппаратными средствами компьютера, модифицировать любой участок оперативной памяти, производить любые действия с файловыми системами и т.д. В подавляющем большинстве случаев прикладной программе для работы не требуется полный набор привилегий уровня операционной системы, и поэтому необходимо иметь средства удобного управления предоставлением приложениям тех и только тех привилегий, которые им действительно необходимы для нормальной работы. В этом случае будет достигаться более безопасная и стабильная конфигурация сетевого сервера.

Windows NT

В операционной системе Microsoft Windows NT управление привилегиями реализуется посредством нескольких механизмов:

- Через изоляцию подсистем. Приложения исполняются в пользовательском режиме, а операционная система - в режиме ядра.
- Приложения могут исполняться в контексте безопасности указанного пользователя Windows NT, в этом случае привилегии этого пользователя наследуются исполняемой программой.
- Возможно предоставление программе системной привилегии, позволяющей ей использовать привилегии существующих пользователей и / или групп Windows NT. Права приложения в этом случае управляемы опосредованно, через администрирование привилегий пользователей и / или групп.

- Модель служб безопасности Windows NT позволяет серверным приложениям заимствовать права своих клиентов при помощи процедуры, называемой обезличиванием (impersonation). В этом случае серверное приложение при выполнении некоторого действия будет обладать правами того из своих пользователей, кто его запросил. Такая архитектура подсистемы управления системными привилегиями обеспечивает достаточную точность администрирования, минимизируя риск нарушения защиты со стороны злонамеренных или имеющих ошибки приложений.

IntranetWare

В операционной системе Novell IntranetWare отсутствует понятие системных привилегий и фактические возможности всех серверных приложений одинаковы. Даже простейшая программа IntranetWare обладает теми же правами, что и операционная система.

3.5.3. Расширяемость

На сервере приложений уровня предприятия могут выполняться самые разнообразные программы: например, системы управления базами данных или серверы Web. Как уже неоднократно отмечалось выше, операционная система должна обладать полным спектром защитных механизмов, чтобы гарантировать контролируемый и ограниченный доступ к ресурсам сервера. Однако сервер приложений должен дополнительно предоставлять возможность интеграции собственных служб обеспечения информационной безопасности тем из прикладных программ, которые в них нуждаются. Разработчики прикладного ПО должны иметь возможность встраивания серверных механизмов защиты информации в собственные программы. Чем больше функций защиты информации будет доступно программистам, тем больше из них будет реально реализовано в заказных разработках, и архитектура средств защиты останется целостной и непротиворечивой. Системные интеграторы, к примеру, будут иметь более высокую уверенность в надежности защитных механизмов таких программ, а открытые интерфейсы прикладного программирования сэкономят время разработки и тестирования нового серверного ПО, администраторы защиты выиграют от функций централизованного управления такими средствами и возможности согласованного внедрения политики безопасности организации.

Windows NT

Службы информационной безопасности Microsoft Windows NT проектировались с целью обеспечения расширяемости, переносимости и согласованности друг с другом. Независимые разработчики программного обеспечения могут использовать открытые интерфейсы прикладного программирования Windows NT для интеграции служб аутентификации субъектов, контроля доступа к объектам системы, обеспечения аутентифицированных безопасных средств обмена данными в сетевой среде в собственные приложения. Программистам нет необходимости разрабатывать собственные решения для этих задач.

Некоторые из доступных разработчику служб информационной безопасности Windows NT перечислены ниже.

Security Support Provider Interface (SSPI). При помощи этого интерфейса прикладного программирования заказное приложение может получить доступ к интегрированным службам аутентификации, обеспечения целостности и конфиденциальности сообщений, а также к средствам обеспечения гарантированного качества услуг для любого распределенного прикладного протокола. Разработчик может использовать различные подмножества перечисленных функций без модификации такого протокола. Этот интерфейс в основном используется для задач аутентификации доступа субъектов сети к различным службам прикладной программы.

Graphical Identification and Authentication (GINA). Помимо стандартных средств аутентификации пользователей на основе запроса имени и пароля Windows NT предоставляет сторонним разработчикам, заинтересованным в усилении этих средств, интерфейс прикладного программирования GINA, позволяющий заменить эти средства аутентификации любыми другими: например, на основе использования цифровых сертификатов, смарт-карт, биометрических данных пользователя и т.д.

Обезличивание (Impersonation). Запущенная пользователем программа не должна обладать большим набором прав по доступу к объектам операционной системы, чем предоставленный этому пользователю. Обезличивание дает возможность приложениям пользователя выполняться в его контексте безопасности. Контекст безопасности определяет набор прав и привилегий пользователя по доступу к объектам и службам операционной системы.

Операционная система Windows NT, предоставляя возможность одному процессу обезличить другой, гарантирует, что пользователь-клиент сервера имеет достаточно прав на выполнение действий, запрошенных им у сервера.

Аутентификация удаленного вызова процедур (Authenticated RPC). Средства технологии аутентифицированного вызова удаленных процедур активно используются приложениями «клиент-сервер». Когда клиент пытается выполнить некоторую функцию на удаленной машине, прежде всего такая попытка потребует аутентификации, как самого клиента, так и сервера.

Подсистема поддержки удаленного вызова процедур Windows NT использует специальный протокол аутентификации, подтверждающий подлинность как вызывающей (клиента), так и отвечающей (сервера) стороны. Дополнительной возможностью этого средства операционной системы Windows NT является шифрование сетевого трафика, генерируемого удаленными вызовами процедур.

Контроль доступа. Доступ к объектам Windows NT управляется с помощью специального описателя (handle), ассоциируемого с каждым таким объектом. Описатель объекта генерируется при попытке доступа к нему. Для дальнейших ссылок на объект Windows NT использует этот описатель.

Разработчик программного обеспечения может определить свой собственный тип объектов, которые не присутствуют в стандартном комплекте поставки операционной системы, но доступ к которым должен быть защищен. Предоставив Windows NT описание такого объекта, разработчик добьется того, что подсистема обеспечения информационной безопасности операционной системы будет контролировать доступ к нему так же, как это производится со стандартными защищаемыми объектами Windows NT, такими, как файлы, принтеры или именованные каналы.

Криптографические службы (CryptoAPl). В состав операционной системы Windows NT входит интерфейс прикладного программирования CryptoAPI, предоставляющий приложениям доступ к криптографическим службам на основе технологии открытых ключей RSA Data Security, а также поддерживающий шифрование, хеширование, цифровую подпись и работу с цифровыми сертификатами.

В комплект поставки Windows NT входят криптографические модули, реализующие алгоритмы компании RSA Data Security. Дополнительные модули могут быть разработаны сторонними производителями и легко интегрируются в общую инфраструктуру криптографических служб Windows NT.

IntranetWare

Операционная система Novell IntranetWare проектировалась с целью предоставления своих служб для использования приложениями, расположенными на рабочих станциях - клиентах сети. Серверным приложениям никакие из встроенных служб обеспечения информационной безопасности IntranetWare не доступны.

Приводимая ниже табл. 3.3 резюмирует подходы Microsoft и Novell к реализации сервера приложений на основе Windows NT Server 4.0 и IntranetWare 4.11 соответственно.

Таблица 3.3

Сравнение архитектур серверов приложений

Требования	Функции	Windows NT 4.0	Novell IntranetWare 4.11
Изоляция подсистемы безопасности	Защита подсистемы безопасности от злонамеренных и имеющих ошибки приложений	Да	Нет
	Защита приложений от влияния других приложений	Да	Нет
Управление привилегиями	Функции управления привилегиями уровня операционной системы	Да	Нет
Аудит	Идентификация пользователя в журнале аудита	Да	Не на консоли
Аутентификация	Проводится всегда	Да	Нет
Расширяемость	Выполнение прикладных программ не вызывает нарушения защиты системы	Да	Нет

4. Безопасность и межсетевые экраны

4.1. Основы и цель использования

Многие организации присоединяют или хотят присоединить свои локальные вычислительные сети (ЛВС) к Интернету, чтобы их пользователи имели легкий доступ к сервисам Интернета. Так как Интернет в целом не является безопасным, машины в этих ЛВС уязвимы к неавторизованному использованию и внешним атакам.

Для управления доступом между небезопасным Интернетом и локальной сетью используется межсетевой экран. Он выполняет роль стража между Интернетом и внутренними сетями. Межсетевой экран - это не одна компонента, а стратегия защиты ресурсов организации, доступных из Интернета.

Основная функция межсетевого экрана - централизация управления доступом. Если удаленные пользователи могут получить доступ к внутренним сетям в обход межсетевого экрана, его эффективность близка к нулю. Например, если менеджер, находящийся в командировке, имеет модем, присоединенный к его ПЭВМ в офисе, то он может дозвониться до своего компьютера из командировки, а так как эта ПЭВМ также находится во внутренней защищенной сети, то атакующий, имеющий возможность установить коммутируемое соединение с этой ПЭВМ, может обойти защиту межсетевого экрана. Если пользователь имеет подключение к Интернету у какого-нибудь провайдера Интернета, и часто соединяется с Интернетом со своей рабочей машины с помощью модема, то он устанавливает небезопасное соединение с Интернетом в обход защиты межсетевого экрана.

Межсетевые экраны часто могут быть использованы для защиты сегментов Интранета организации.

Более подробная информация о межсетевых экранах содержится в "NIST Special Publication 800-10 "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls."

Межсетевые экраны обеспечивают несколько типов защиты, они могут:

- блокировать нежелательный трафик;
- направлять входной трафик только к надежным внутренним системам;
- скрыть уязвимые системы, которые нельзя обезопасить от атак из Интернета другим способом;
- протоколировать трафик в и из внутренней сети;
- скрывать информацию, такую как имена систем, топологию сети, типы сетевых устройств и внутренние идентификаторы пользователей, от Интернета;
- обеспечить более надежную аутентификацию, чем та, которую представляют стандартные приложения.

Каждая из этих функций будет описана далее.

Как и для любого средства защиты, нужны определенные компромиссы между удобством работы и безопасностью. Прозрачность - это видимость межсетевого экрана как внутренним пользователям, так и внешним, осуществляющим взаимодействие через межсетевой экран. Межсетевой экран прозрачен для пользователей, если он не мешает им получить доступ к сети. Обычно межсетевые экраны конфигурируются так, чтобы быть прозрачными для внутренних пользователей сети (посылающих пакеты наружу за межсетевой экран); и с другой стороны, межсетевой экран конфигурируется так, чтобы быть непрозрачным для внешних пользователей, пытающихся получить доступ к внутренней сети извне. Это обычно обеспечивает высокий уровень безопасности и не мешает внутренним пользователям.

4.2. Аутентификация

Межсетевые экраны на основе маршрутизаторов не обеспечивают аутентификацию пользователей. В межсетевых экранах, в состав которых входят прокси-сервера, аутентификация осуществляется на основе:

- **Имени / пароля.** Это самый плохой вариант, так как в этом случае аутентификационная информация может быть перехвачена в сети или получена путем подглядывания за ее вводом и еще множеством других способов.

- **Одноразовых паролей.** В этом случае используют программы или специальные устройства для генерации нового пароля для каждого сеанса. Это означает, что старые пароли не могут быть повторно использованы, если они были перехвачены в сети или украдены другим способом.
- **Электронных сертификатов.** В этом случае используется шифрование с открытыми ключами.

4.3. Анализ возможностей маршрутизации и прокси-серверов

В политике информационной безопасности должно быть определено, может ли межсетевой экран маршрутизировать пакеты или они должны передаваться прокси-серверам. Простейшим межсетевым экраном является маршрутизатор, который может выступать в роли устройства для фильтрации пакетов. Все, что он может - только перенаправлять пакеты. А прикладные шлюзы наоборот не могут быть сконфигурированы для маршрутизации трафика между внутренним и внешним интерфейсами межсетевого экрана, так как это может привести к обходу средств защиты. Все соединения между внешними и внутренними сетями должны проходить через прикладные шлюзы (прокси-сервер).

Маршрутизация источника

Это механизм, посредством которого путь к машине-получателю пакета определяется отправителем, а не промежуточными маршрутизаторами. Маршрутизация источника в основном используется для устранения проблем в сетях, но также может быть использована для атаки на хост. Если атакующий знает, что ваш хост доверяет какому-нибудь другому хосту, то маршрутизация источника может быть использована для создания впечатления, что пакеты атакующего приходят от доверенного хоста. Ввиду такой угрозы безопасности маршрутизаторы с фильтрацией пакетов обычно конфигурируются так, чтобы отвергать пакеты с опцией маршрутизации источника. Поэтому владелец сайта, желающий избежать проблем с маршрутизацией источника, обычно определяет политику, в которой такая маршрутизация запрещена.

Фальсификация IP-адреса

Это имеет место, когда атакующий маскирует свою машину под хост в сети объекта атаки (то есть пытается заставить цель атаки думать, что пакеты приходят от доверенной машины во внутренней сети). Политика в отношении маршрутизации пакетов должна быть четкой, чтобы можно было корректно построить обработку пакетов, если есть проблемы с безопасностью. Необходимо объединить аутентификацию на основе адреса отправителя с другими способами защиты, чтобы защитить вашу сеть от атак подобного рода.

4.4. Типы межсетевых экранов

Существует несколько различных реализаций межсетевых экранов, которые могут быть созданы разными путями. В табл. 4.1 кратко характеризуются несколько архитектур межсетевых экранов и их применимость к средам с низким, средним и высоким рискам.

Таблица 4.1

Риски безопасности межсетевого экрана. Варианты архитектур межсетевых экранов

Архитектура межсетевого экрана (если один из типов, указанных ниже, реализован)	Среда с высоким риском, например банк	Среда со средним риском, например университет	Среда с низким риском, например мелкий магазин
Фильтрация пакетов	Неприемлемо	Минимальная безопасность	Рекомендованный вариант
Прикладные шлюзы	Эффективный вариант	Рекомендованный вариант	Допустимый вариант
Гибридные шлюзы	Рекомендованный вариант	Эффективный вариант	Допустимый вариант

4.4.1. Шлюзы с фильтрацией пакетов

Межсетевые экраны с фильтрацией пакетов используют маршрутизаторы с правилами фильтрации пакетов для предоставления или запрещения доступа на основе адреса отправителя, адреса получателя и порта. Они обеспечивают минимальную безопасность за низкую цену, и это может оказаться приемлемым для среды с низким риском. Они являются быстрыми, гибкими и прозрачными. Правила фильтрации часто нелегко администрировать, но имеется ряд средств для упрощения задачи создания и поддержания правил.

Шлюзы с фильтрацией имеют свои недостатки, включая следующие:

- Адреса и порты отправителя и получателя, содержащиеся в заголовке IP-пакета, - единственная информация, доступная маршрутизатору при принятии решения о том, разрешать или запрещать доступ трафика во внутреннюю сеть.
- Не защищают от фальсификации IP и DNS-адресов.
- Атакующий получит доступ ко всем хостам во внутренней сети после того, как ему был предоставлен доступ межсетевым экраном.
- Усиленная аутентификация пользователя не поддерживается некоторыми шлюзами с фильтрацией пакетов.
- Практически отсутствуют средства протоколирования доступа к сети.

Прикладные шлюзы

Прикладной шлюз использует программы (называемые прокси-серверами), запускаемые на межсетевом экране. Эти прокси-серверы принимают запросы извне, анализируют их и передают безопасные запросы внутренним хостам, которые предоставляют соответствующие сервисы. Прикладные шлюзы могут обеспечивать такие функции, как аутентификация пользователей и протоколирование их действий.

Так как прикладной шлюз считается самым безопасным типом межсетевого экрана, эта конфигурация имеет ряд преимуществ с точки зрения сайта со средним уровнем риска:

- Межсетевой экран может быть сконфигурирован как единственный хост, видимый из внешней сети, что будет требовать проходить все соединения с внешней сетью через него.
- Использование прокси-серверов для различных сервисов предотвращает прямой доступ к этим сервисам, защищая организацию от небезопасных или плохо сконфигурированных внутренних хостов
- С помощью прикладных шлюзов может быть реализована усиленная аутентификация.
- Прокси-серверы могут обеспечивать детальное протоколирование на прикладном уровне.

Межсетевые экраны прикладного уровня должны конфигурироваться так, чтобы весь выходящий трафик казался исходящим от межсетевого экрана (то есть чтобы только межсетевой экран был виден внешним сетям). Таким образом будет запрещен прямой доступ ко внутренним ресурсам сети. Все входящие запросы различных сетевых сервисов, таких как Telnet, FTP, HTTP, RLOGIN, и т.д., независимо от того, какой внутренний хост запрашивается, должны проходить через соответствующий прокси-сервер на межсетевом экране.

Прикладные шлюзы требуют прокси-сервера для каждого сервиса, такого, как FTP, HTTP и т.д., поддерживаемого межсетевым экраном. Когда требуемый сервис не поддерживается прокси, у организации имеется три варианта действий:

1. Отказаться от использования этого сервиса, пока производитель межсетевого экрана не разработает для него безопасный прокси-сервер - это предпочтительный подход, так как многие новые сервисы имеют большое число уязвимых мест.
2. Разработать свой прокси-сервер - это достаточно сложная задача и должна решаться только техническими организациями, имеющими соответствующих специалистов.
3. Пропустить сервис через межсетевой экран - использование того, что обычно называется "заглушками", большинство межсетевых экранов с прикладными шлюзами позволяет пропускать большинство сервисов через межсетевой экран с минимальной фильтрацией пакетов. Это может ограничить число уязвимых мест, но привести к компрометации систем за межсетевым экраном.

Низкий риск

Когда для входящих Интернет сервисов нет прокси-сервера, но требуется пропускать его через межсетевой экран, администратор межсетевого экрана должен использовать конфигурацию или "заплатку",

которая позволит использовать требуемый сервис. Когда прокси-сервер разрабатывается производителем, то "заплатка" должна быть отключена.

Средний-высокий

Все входящие Интернет сервисы должны обрабатываться прокси-сервером на межсетевом экране. Если требуется использование нового сервиса, то оно должно быть запрещено до тех пор, пока производитель межсетевого экрана не разработает для него прокси-сервер, и он не будет протестирован администратором межсетевого экрана. Только по специальному разрешению руководства можно разрабатывать свой прокси-сервер или закупать его у других производителей.

Гибридные или сложные шлюзы

Гибридные шлюзы объединяют в себе два описанных выше типа межсетевых экранов и реализуют их последовательно, а не параллельно. Если они соединены последовательно, то общая безопасность увеличивается, с другой стороны, если их использовать параллельно, то общая безопасность системы будет равна наименее безопасному из используемых методов. В средах со средним и высоким риском, гибридные шлюзы могут оказаться идеальной реализацией межсетевых экранов.

4.5. Архитектуры межсетевых экранов

Межсетевые экраны могут быть сконфигурированы в виде одной из нескольких архитектур, что обеспечивает различные уровни безопасности при различных затратах на установку и поддержание работоспособности. Организации должны проанализировать свой профиль риска и выбрать соответствующую архитектуру. Следующие разделы описывают типичные архитектуры межсетевых экранов и приводят примеры политик безопасности для них.

4.5.1. Хост, подключенный к двум сегментам сети

Это такой хост, который имеет более одного интерфейса с сетью, причем каждый интерфейс с сетью подключен физически к отдельному сегменту сети. Самым распространенным примером является хост, подключенный к двум сегментам.

Межсетевой экран на основе хоста, подключенного к двум сегментам сети, – это межсетевой экран с двумя сетевыми платами, каждая из которых подключена к отдельной сети. Например, одна сетевая плата соединена с внешней или небезопасной сетью, а другая - с внутренней или безопасной сетью. В этой конфигурации ключевым принципом обеспечения безопасности является запрет прямой маршрутизации трафика из недоверенной сети в доверенную - межсетевой экран всегда должен быть при этом промежуточным звеном.

Маршрутизация должна быть отключена на межсетевом экране такого типа, чтобы IP-пакеты из одной сети не могли пройти в другую сеть.

Такая конфигурация, наверное, является одной из самых дешевых и распространенных при коммутируемом подключении ЛВС организации к Интернету. Например, берется машина, на которую устанавливается FreeBSD, и на ней запрещается маршрутизация, кроме того соответствующим образом конфигурируется встроенный в ядро пакетный фильтр.

4.5.2. Экранированный хост

При архитектуре типа «экранированный хост» используется хост (называемый хостом-бастионом), с которым может установить соединение любой внешний хост, но запрещен доступ ко всем другим внутренним, менее безопасным хостам. Для этого фильтрующий маршрутизатор конфигурируется так, что все соединения с внутренней сетью из внешних сетей направляются к хосту-бастиону.

Если шлюз с пакетной фильтрацией установлен, то хост-бастион должен быть сконфигурирован так, чтобы все соединения из внешних сетей проходили через него, чтобы предотвратить прямое соединение между сетью организации и Интернетом.

4.5.3. Экранированная подсеть

Архитектура экранированной сети по существу совпадает с архитектурой экранированного хоста, но добавляет еще одну линию защиты с помощью создания сети, в которой находится хост-бастион, отделенный от внутренней сети.

Экранированная подсеть должна внедряться с помощью добавления сети-периметра, для того чтобы отделить внутреннюю сеть от внешней. Это гарантирует, что даже при успехе атаки на хост-бастион атакующий не сможет пройти дальше сети-периметра из-за того, что между внутренней сетью и сетью-периметром находится еще один экранирующий маршрутизатор.

5. Всемирная паутина - World Wide Web (WWW)

Интернет - это сеть сетей, обеспечивающая инфраструктуру для взаимодействия и совместного использования информации. Он обеспечивает ряд сервисов, таких, как электронная почта, передача файлов, подключение в режиме удаленного терминала, интерактивные конференции, группы новостей, и WWW.

World Wide Web (называется "WWW', "Web" или "W3") - это вселенная информации, доступной из Интернета. WWW появился как сетевой информационный проект в CERN, европейской физической лаборатории. WWW состоит из программ, набора протоколов и соглашений, используемых для получения доступа к информации и ее поиска в Интернете. С помощью использования гипертекстовых и мультимедийных технологий WWW позволяет любому пользователю легко добавлять новую информацию, просматривать ее и искать.

Web-клиенты, также известные как веб-браузеры, обеспечивают пользовательский интерфейс для навигации среди информации с помощью метода указания и щелкания мышью. Веб-серверы предоставляют браузерам HTML и другие средства для получения информации с помощью протокола HTTP. Браузеры интерпретируют, форматируют и отображают документы пользователям. Конечным результатом является мультимедийное представление Интернета.

Веб-серверы могут быть атакованы или использованы как место, с которого будут атакованы внутренние сети организации. Необходимо обеспечить безопасность ряд областей в веб-серверах - самой операционной системы, программы веб-сервера, скриптов сервера и ряда других программ.

Браузеры также приводят к появлению уязвимых мест, хотя эти уязвимые места гораздо менее серьезны, чем те, которые могут возникнуть из-за веб-сервера. В следующих разделах описываются примеры политик для использования WWW-браузеров, серверов, и публикации информации на домашних страницах WWW.

5.1. Поиск информации в Интернете с помощью браузера

Существует ряд рисков, связанных с использованием WWW-браузеров для поиска и получения информации из Интернета. Программы веб-браузеров являются очень сложными и станут еще сложнее. Ошибки в них могут использоваться для сетевых атак.

5.1.1. Примеры политик безопасности при поиске информации

Низкий риск

Пользователь

- Программы для поиска и просмотра информации в Интернете, такие, как WWW, Gopher, WAIS и т.д. предоставляются сотрудникам в основном для более лучшего исполнения ими своих должностных обязанностей.
- Любое использование их в личных целях не должно мешать обычной трудовой деятельности сотрудников организации, не должно быть связано с ведением коммерческой деятельности в личных интересах, выходящих за рамки обязанностей сотрудника, и не должно потенциально угрожать организации.
- Сотрудникам организации, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским.
- Пользователям WWW напоминается, что веб-браузеры оставляют "отпечатки пальцев" на сайтах, позволяющие установить, кто и когда посещал эти сайты.

Менеджер

- Пользователям должны быть известны и доступны места, где можно взять лицензионные программы для WWW.

Сотрудник отдела автоматизации

- Должно иметься и поддерживаться локальное хранилище полезных веб-браузеров, приложений для отображения различных форматов документов и плагинов. Оно должно быть доступно для сотрудников организации .

Средний риск

Пользователь

- Служащие пользуются программами для поиска информации в WWW только для более лучшего выполнения ими своих должностных обязанностей.
- Все программы, используемые для доступа к WWW, должны быть утверждены сетевым администратором и на них должны быть установлены все доработки производителя(patch), связанные с безопасностью.
- Все файлы, загружаемые с помощью WWW, должны проверяться на вирусы с помощью утвержденных руководством антивирусных программ.
- Во всех браузерах должна быть запрещена обработка Java, Javascript и ActiveX из-за небезопасности данных технологий.
- Могут использоваться или загружаться только версии браузеров, использование которых разрешено в организациит. Другие версии могут содержать вирусы или ошибки.
- Все веб-браузеры должны быть сконфигурированы так, чтобы использовать прокси-сервер для WWW из состава межсетевого экрана.
- При посылке данных на веб-сервер с помощью форм HTML из браузера удостоверьтесь, что установлен механизм, такой как SSL (Secure Sockets Layer), для шифрования сообщения при посылке его.

Высокий риск

Пользователь

- Пользователи могут производить поиск информации в Интернете с помощью World Wide Web (WWW), Gopher, WAIS и т.д. только, если этого явно требуют их должностные обязанности.
- Не должны посещаться сайты, про которые, что они содержат оскорбительную или другую вредную информацию.
- Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему санкций.
- Адреса сайтов, содержащих вредную информацию, должны сообщаться ответственному в организации за безопасность использования Интернета.

Менеджер

- В организации должен вестись список запрещенных сайтов. Программы для работы с WWW должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.
- Сайты, о которых стало известно, что они содержат вредную информацию, должны сразу же блокироваться сетевыми администраторами.
- Сотрудники, нанятые по контракту, должны соблюдать эту политику после предоставления им доступа к Интернету в письменном виде.

Сотрудник отдела автоматизации

- Все посещаемые сайты должны протоколироваться.
- Веб-браузеры должны быть сконфигурированы так, чтобы выполнялись следующие правила:
  - доступ к Интернету должен осуществляться только через HTTP-прокси;
  - каждый загружаемый файл должен проверяться на вирусы или РПС;
  - могут загружаться только те программы на ActiveX, использование которых разрешено организацией;
  - могут загружаться только те программы на Java, использование которых разрешено организацией;
  - могут загружаться только те программы на Javascript, использование которых разрешено организацией.

Веб-страницы часто включают формы. Как и электронная почта, данные, посылаемые веб-браузером на веб-сервер, проходят через большое число промежуточных компьютеров и сетей до того, как дос-

тигнут своего конечного назначения. Любая важная информация, посылаемая с помощью ввода данных на веб-странице, может быть перехвачена.

5.2. Защита веб-сервера

Многие организации сейчас поддерживают внешние WWW-сайты, описывающие их компанию или сервисы. По причинам безопасности эти серверы размещаются за межсетевым экраном компании.

Должны быть назначены ответственные за создание, управление и администрирование внешнего веб-сайта компании. В больших компаниях это может входить в обязанности нескольких должностей. Например, коммерческий директор может отвечать за выявление и реализацию новых способов продвижения товаров и услуг, а администратор веб-сайта - за соблюдение на нем общей стратегии, включая координированную подготовку его содержимого и контроль за его бюджетом. Начальник отдела продаж может отвечать за представление отчетов о доходах, связанных с ведением веб-сайта. А веб-мастер будет отвечать за технические аспекты веб-сайта, включая разработку, поддержание связи с ним, интранет, электронную почту, и безопасность брандмауэра. Скорее всего программисты будут отвечать за работоспособность веб-сайта, включая его установку, разработку программ для него, их отладку и документирование. Веб-художник может заниматься созданием графических образов для него.

В более маленьких организациях программист или веб-мастер может выполнять большую часть описанных выше обязанностей и предоставлять доклады пресс-службе или начальнику отдела продаж. Наконец, в очень маленькой организации эти обязанности могут стать дополнительными обязанностями системного аналитика или администратора ЛВС. Независимо от того, как администрируется веб-сайт, все люди, исполняющие эти обязанности должны претворять в жизнь политику компании, разработанную ее руководством. Верхнее звено руководства организацией может отвечать за утверждение создания новых веб-сайтов или переработку имеющихся.

Каждый может создать веб-сайт для распространения информации по любым вопросам, не связанным с организацией. Организация должна принять решение о том, стоит ли разрешать сотрудникам делать это на чужих веб-сайтах.

Большинство организаций используют Интернет для распространения информации о себе и своих сервисах. Так как они представляют информацию, а не скрывают ее, они описывают веб-сайт как "публичный", на котором не содержится никакой конфиденциальной информации, и оттуда не может исходить никакой угрозы. Проблема заключается в том, что хотя эта информация может быть публично доступной, веб-сайт является частью организации, и должен быть защищен от вандализма.

5.2.1. Примеры политик веб-серверов

Низкий риск

Пользователь
- На веб-сайтах организации не должен размещаться оскорбительный или нудный материал.
- На веб-сайтах организации не должен размещаться персональные рекламные объявления

Менеджер
- Менеджерам и пользователям разрешено иметь веб-сайт.
- Материалы о сотрудниках на веб-сайтах или доступные с их помощью должны быть минимальны.
- На веб-сайтах организации не должен размещаться оскорбительный или нудный материал.
- Конфиденциальная информация не должна делаться доступной.

Сотрудник отдела автоматизации
- Должен поддерживаться и быть доступен для внутреннего пользования локальный архив программ веб-серверов и средств публикации информации на них.

Средний риск

Пользователь
- Пользователям запрещено устанавливать или запускать веб-серверы.

- В отношении веб-страниц должен соблюдаться установленный в организации порядок утверждения документов, отчетов, маркетинговой информации и т.д.

Менеджер
- Менеджерам и пользователям разрешено иметь веб-страницы для участия в проекте или выполнения своих должностных обязанностей

Сотрудник отдела автоматизации
- Веб-сервер и любые данные, являющиеся публично доступными, должны быть размещены за пределами брандмауэра организации.
- Веб-серверы должны быть сконфигурированы так, чтобы пользователи не могли устанавливать CGI-скрипты.
- Все сетевые приложения, кроме HTTP, должны быть отключены (например SMTP, FTP и т.д.)

Информационные серверы должны быть размещены в защищенной подсети для изоляции их от других систем организации. Это уменьшает вероятность того, что информационный сервер будет скомпрометирован и использован для атаки на другие системы организации.

При использования средств администрирования с помощью WWW ограничьте доступ к нему только авторизованных систем (с помощью IP-адресов, а не имен хостов). Всегда меняйте пароли по умолчанию.

Высокий риск

Пользователь
- Пользователям запрещено загружать, устанавливать или запускать программы веб-серверов.
- Должен производиться контроль сетевого трафика для выявления неавторизованных веб-серверов. Операторы этих серверов будут подвергаться дисциплинарным наказаниям.

Менеджер
- Руководство организации должно дать в письменном виде разрешение на работу веб-сервера, подключенного к Интернету.
- Все содержимое веб-серверов компании, присоединенных к Интернету, должно быть утверждено и установлено веб-мастером.
- Конфиденциальная информация не должна быть доступна с помощью веб-сайта.
- К информации, размещенной на веб-сервере, применимы все законы о защите информации. Поэтому перед размещением информации в Интернете она должна быть просмотрена и утверждена так же, как утверждаются официальные бумажные документы организации. Должны быть защищены авторские права, и получено разрешение о публикации информации на веб-сайте.
- Все публично доступные веб-сайты должны регулярно тестироваться на предмет корректности ссылок, и не должны находиться в состоянии "under construction". При реконструкции областей они должны делаться недоступными.

Сотрудник отдела автоматизации
- Не должно иметься средств удаленного управления веб-сервером (то есть с мест, отличных от консоли). Все действия администратора должны делаться только с консоли. Вход в систему с удаленного терминала с правами суперпользователя должен быть запрещен.
- Программы веб-серверов и операционной системы, под управлением которой работает веб-сервер, должны содержать все исправления, рекомендованные производителем для этой версии.
- Входящий трафик HTTP должен сканироваться, и о случаях появления неавторизованных веб-серверов должно докладываться
- Ограничение доступа к информации пользователями, адрес которых заканчивается на .GOV или .COM, обеспечивает минимальную защиту для информации, не разрешенной для показа всем. Может использоваться отдельный сервер или отдельная часть для информации с ограниченным доступом.
- За всеми веб-сайтами должен осуществляться контроль как составная часть администрирования сети. Действия всех пользователей, заподозренных в некорректном использовании Интернете, могут быть запротоколированы для обоснования применения к ним в дальнейшем административных санкций.
- На UNIX-системах веб-серверы не должны запускаться с правами суперпользователя.

- Разработка и использование CGI-скриптов должны контролироваться. CGI-скрипты не должны обрабатывать входные данные без их проверки. Любые внешние программы, запускаемые с параметрами в командной строке, не должны содержать метасимволов. Разработчики отвечают за использование правильных регулярных выражений для сканирования метасимволов командного процессора и их удаление перед передачей входных данных программа на сервере и операционной системе.
- Все WWW-серверы организации, подключенные к Интернету, должны находиться между брандмауэром и внутренней сетью организации. Любые внутренние WWW-серверы организации, обеспечивающие работу критических приложений организации, должны быть защищены внутренними брандмауэрами. Критическая, конфиденциальная и персональная информация никогда не должна храниться на внешнем WWW-сервере.

6. Электронная почта

6.1. Использование электронной почты

6.1.1. Опасности ЭП

Помимо взаимодействия один-один, e-mail может поддерживать списки электронных адресов для рассылки, поэтому человек или организация может послать e-mail всему этому списку адресов людей или организаций. Иногда списки рассылки e-mail имеют элементы, являющиеся указателями на другие списки рассылки, поэтому одно письмо может быть в конце концов доставлено тысячам людей.

Организациям нужны политики для электронной почты, чтобы помочь сотрудникам правильно ее использовать, уменьшить риск умышленного или неумышленного неправильного ее использования, и чтобы гарантировать, что официальные документы, передаваемые с помощью электронной почты, правильно обрабатываются. Аналогично политике использования телефона, организациям нужно разработать политику для правильного использования электронной почты.

Политика должна давать общие рекомендации в таких областях:

- Использование электронной почты для ведения деловой деятельности.
- Использование электронной почты для ведения личных дел.
- Управление доступом и сохранение конфиденциальности сообщений.
- Администрирование и хранение электронных писем.

6.2. Основы электронной почты

ЭП – средство обмена и базируется на основе некоторых протоколов. Основными почтовыми протоколами в Интернете являются SMTP (Simple Mail Transport Protocol), POP (Post Office Protocol) и IMAP (Internet Mail Access Protocol).

6.2.1. SMTP

SMTP - это почтовый протокол хост-хост. SMTP-сервер принимает письма от других систем и сохраняет их в почтовых ящиках пользователей. Сохраненные письма могут быть прочитаны несколькими способами. Пользователи с интерактивным доступом на почтовом сервере могут читать почту с помощью локальных почтовых приложений. Пользователи на других системах могут загрузить свои письма с помощью программ – почтовых клиентов по протоколам POP3 и IMAP.

UNIX-хосты сделали самым популярным SMTP. Широко используемыми SMTP-серверами являются Sendmail, Smail, MMDF и PP. Самым популярным SMTP-сервером в Unixe является Sendmail, написанный Брайаном Эллманом. Он поддерживает создание очередей сообщений, переписывание заголовков писем, списки рассылки и т.д. Обычно он конфигурируется так, что должен работать как привилегированный процесс. Это означает, что если его защиту можно будет обойти каким-нибудь способом, атакующий сможет нанести вред, значительно превышающий удаление электронных писем.

6.2.2. POP

POP - это самый популярный протокол приема электронной почты. POP-сервер позволяет POP-клиенту загрузить письма, которые были получены им от другого почтового сервера. Клиенты могут загрузить все сообщения или только те, которые они еще не читали. Он не поддерживает удаление сообщений перед загрузкой на основе атрибутов сообщения, таких как адрес отправителя или получателя. POP версии 2 поддерживает аутентификацию пользователя с помощью пароля, но пароль передается серверу в открытом (незашифрованном) виде.

POP версии 3 предоставляет дополнительный метод аутентификации, называемый APOP, который прячет пароль. Некоторые реализации POP могут использовать Kerberos для аутентификации.

6.2.3. IMAP

IMAP4rev1 поддерживает операции создания, удаления, переименования почтовых ящиков; проверки поступления новых писем; оперативное удаление писем; установку и сброс флагов операций; разбор заголовков в формате RFC-822 и MIME-IMB; поиск среди писем; выборочное чтение писем.

IMAP более удобен для чтения почты в путешествии, чем POP, так как сообщения могут быть оставлены на сервере, что избавляет от необходимости синхронизировать списки прочитанных писем на локальном хосте и на сервере.

6.2.4. MIME

MIME - это сокращение для многоцелевых расширений Интернет-почты (Multipurpose Internet Mail Extensions). Как сказано в RFC 2045, он переопределяет формат сообщений электронной почты, чтобы позволить:

- передачу текстов в кодировке, отличной от US-ASCII;
- передачу в письме нетекстовой информации в различных форматах;
- сообщения из нескольких частей;
- передачу в заголовке письма информации в кодировке, отличной от US-ASCII.

Он может использоваться для поддержки таких средств безопасности, как цифровые подписи и шифрованные сообщения. Он также позволяет посылать по почте выполняемые файлы, зараженные вирусами, или письма с РПС.

Как и веб-браузеры, программы чтения почты могут быть сконфигурированы для автоматического запуска приложения-помощника для обработки определенных типов MIME-сообщений.

6.3. Потенциальные проблемы с электронной почтой

6.3.1. Случайные ошибки

Можно легко допустить ошибку при работе с электронной почтой. Письмо может быть послано случайно. Простое нажатие клавиши или щелчок мышью может послать письмо по неправильному адресу. Почтовые сообщения хранятся годами, поэтому некорректное выражение может «аукнуться» через много времени. Архивы писем могут возрасти до такой степени, что система будет аварийно завершаться. Неправильно настроенная программа чтения групп новостей может привести к посылке сообщения не в те группы. Ошибки в списках рассылки могут привести к долгому блужданию писем между почтовыми серверами, причем число писем может увеличиться до такой степени, что почтовые серверы аварийно завершатся.

Когда почтовая система организации присоединена к Интернету, последствия ошибок могут оказаться в тысячу раз хуже.

Вот некоторые из способов предотвратить ошибки:

- Учить пользователей что делать, если они совершили ошибку, и как правильно работать с электронной почтой.
- Конфигурировать программы электронной почты так, чтобы стандартные действия пользователя, использующие установки по умолчанию, были бы самыми безопасными.
- Использовать программы, которые строго реализуют протоколы и соглашения Интернета.

6.3.2. Персональное использование

Так как письмо обычно используется для обеспечения деятельности организации, как телефон и факс, использование его в личных целях должно быть ограничено или запрещено (это зависит от организации).

Хотя все понимают, что электронная почта используется прежде всего для решения задач организации, такую политику тяжело претворить в жизнь. Если политика не может быть согласованно внедрена, неизбежно ее несоблюдение и тогда политика не сможет использоваться в качестве основы для наказания. Гораздо более мудрым будет создать политику, которая устанавливает четкие границы использования e-mail в личных целях, аналогично тому, как устанавливаются рамки использования служебного телефона в личных целях.

Если вы используете служебный телефон для того, чтобы позвонить в химчистку, то маловероятно, что ваш звонок будет восприниматься как официальный запрос компании. Но посылка электронного письма с электронным почтовым адресом, содержащим адрес организации, будет похожа на посылку бумажного письма на фирменном бланке компании. Если отправитель использует свой почтовый ящик в компании для посылки электронной почты в группу новостей, может показаться, что компания одобряет мнение, высказываемое им в письме.

6.3.3. Маркетинг

В прошлом, когда Интернет был исследовательской сетью, его коммерческое использование было запрещено. Кроме того, слишком мало компаний и людей имели доступ к интернетовской почте, поэтому было нецелесообразно использовать ее для коммерческих целей. Сейчас Интернет расширился и разрешается использовать его в коммерческих целях, поэтому компании стали поддерживать списки рассылки для обмена информацией со своими клиентами. Как правило, клиенты должны послать запрос для того, чтобы попасть в список рассылки. Таким образом можно передать информацию значительной аудитории. Так родился маркетинг в Интернете с помощью посылки отдельных почтовых сообщений.

Люди написали программы для автоматизации поддержания списков рассылки и образовали компании для сбора и продажи списков электронных почтовых адресов организациям, занимающимся маркетингом. Конгресс США принял билль, согласно которому прямой маркетинг с помощью электронной почты должен осуществляться в соответствии с теми же правилами, которыми ограничивается использование массовой посылки писем. Необходимо, чтобы лица, занимающиеся таким маркетингом, вели списки адресов, владельцы которых не желают получать рекламу в электронных письмах.

6.4. Угрозы, связанные с электронной почтой

Основные протоколы передачи почты обычно не осуществляют надежной аутентификации, что позволяет легко создать письма с фальшивыми адресами. Ни один из этих протоколов не использует криптографию, которая могла бы гарантировать конфиденциальность электронных писем. Хотя существуют расширения этих протоколов, решение использовать их должно быть явно принято как составная часть политики администрации почтового сервера. Некоторые такие расширения используют уже имеющиеся средства аутентификации, а другие позволяют клиенту и серверу согласовать тип аутентификации, который будет использоваться в данном соединении.

6.4.1. Фальшивые адреса отправителя

Адресу отправителя в электронной почте Интернета нельзя доверять, так как отправитель может указать фальшивый обратный адрес или заголовок может быть модифицирован в ходе передачи письма, или отправитель может сам соединиться с SMTP-портом на машине, от имени которой он хочет отправить письмо, и ввести текст письма.

6.4.2. Перехват письма

Заголовки и содержимое электронных писем передаются в чистом виде. В результате содержимое сообщения может быть прочитано или изменено в процессе передачи его по Интернету. Заголовок может

быть модифицирован, чтобы скрыть или изменить отправителя или для того чтобы перенаправить сообщение.

6.4.3. Почтовые бомбы

Почтовая бомба - это атака с помощью электронной почты. Атакуемая система переполняется письмами до тех пор, пока она не выйдет из строя. Как это может произойти, зависит от типа почтового сервера и того, как он сконфигурирован.

Некоторые провайдеры Интернета дают временные логины любому для тестирования подключения к Интернету, и эти логины могут быть использованы для начала подобных атак.

Типовые варианты выхода почтового сервера из строя:

- Почтовые сообщения принимаются до тех пор, пока диск, на котором они размещаются, не переполнится. Следующие письма не принимаются. Если этот диск – основной системный диск, то вся система может аварийно завершиться.
- Входная очередь переполняется сообщениями, которые нужно обработать и передать дальше, до тех пор, пока не будет достигнут предельный размер очереди. Последующие сообщения не попадут в очередь.
- В некоторых почтовых системах можно установить максимальное число почтовых сообщений или максимальный общий размер сообщений, которые пользователь может принять за один раз. Последующие сообщения будут отвергнуты или уничтожены.
- Может быть превышена квота диска для данного пользователя. Это помешает принять последующие письма, и может помешать ему выполнять другие действия. Восстановление может оказаться трудным для пользователя, так как ему может понадобиться дополнительное дисковое пространство для удаления писем.
- Большой размер почтового ящика может сделать трудным для системного администратора получение системных предупреждений и сообщений об ошибках
- Посылка почтовых бомб в список рассылки может привести к тому, что его члены могут отказаться от рассылки.

6.4.4. Угрожающие письма

Любой человек в мире может послать вам письмо, поэтому может оказаться трудным заставить его прекратить посылать их вам. Люди могут узнать ваш адрес из списка адресов организации, списка лиц, подписавшихся на список рассылки, или писем в Usenet. Если вы указали ваш почтовый адрес какому-нибудь веб-сайту, от он может продать ваш адрес "почтовым мусорщикам". Некоторые веб-браузеры сами указывают ваш почтовый адрес, когда вы посещаете веб-сайт, поэтому вы можете даже не понять, что вы его дали. Много почтовых систем имеют возможность фильтрации почты, то есть поиска указанных слов или словосочетаний в заголовке письма или его теле, и последующего помещения его в определенный почтовый ящик или удаления. Но большинство пользователей не знает, как использовать механизм фильтрации. Кроме того, фильтрация у клиента происходит после того, как письмо уже получено или загружено, поэтому таким образом удалить большие объемы писем тяжело.

Для безопасной атаки может использоваться анонимный ремэйлер. Когда кто-то хочет послать оскорбительное или угрожающее письмо и при этом скрыть свою личность, он может воспользоваться анонимным ремэйлером. Если человек хочет послать электронное письмо, не раскрывая свой домашний адрес тем, кто может угрожать ему, он может тоже использовать анонимный ремэйлер. Если он начнет вдруг получать нежелательные письма по своему текущему адресу, он может отказаться от него и взять новый.

Одним часто используемым средством защиты, применяемым некоторыми пользователями Usenet, является конфигурирование своих клиентов для чтения новостей таким образом, что в поле обратного адреса письма, посылаемого ими в группу новостей, помещается фальшивый адрес, а реальный адрес помещается в сигнатуре или в теле сообщения. Таким образом, программы сбора почтовых адресов, собирающие адреса из поля обратного адреса, окажутся бесполезными.

В конгрессе США были рассмотрены несколько биллей об ограничениях на работу таких программ-мусорщиков. В одном предлагалось создать списки стоп-слов и помещать слово "реклама" в строку темы письма. В другом предлагалось считать их просто незаконными.

6.5. Защита электронной почты

6.5.1. Корректное использование электронной почты

Все служащие должны использовать электронную почту так же, как и любое другое официальное средство организации. Из этого следует, что когда письмо посылается, как отправитель, так и получатель, должен гарантировать, что взаимодействие между ними осуществляется согласно принятым правилам взаимодействия. Взаимодействие с помощью почты не должно быть неэтичным, не должно восприниматься как конфликтная ситуация или содержать конфиденциальную информацию.

6.5.2. Защита от фальшивых адресов

От этого можно защититься с помощью использования шифрования для присоединения к письмам электронных подписей. Одним популярным методом является использование шифрования с открытыми ключами. Однонаправленная хэш-функция письма шифруется, используя секретный ключ отправителя. Получатель использует открытый ключ отправителя для расшифровки хэш-функции и сравнивает его с хэш-функцией, рассчитанной по полученному сообщению. Это гарантирует, что сообщение на самом деле написано отправителем, и не было изменено в пути. Правительство США требует использования алгоритма Secure Hash Algorithm (SHA) и Digital Signature Standard, там где это возможно. А самые популярные коммерческие программы используют алгоритмы RC2, RC4 или RC5 фирмы RSA.

6.5.3. Защита от перехвата

От него можно защититься с помощью шифрования содержимого сообщения или канала, по которому он передается. Если канал связи зашифрован, то системные администраторы на обоих его концах все-таки могут читать или изменять сообщения. Было предложено много различных схем шифрования электронной почты, но ни одна из них не стала массовой. Одним из самых популярных приложений является PGP. В прошлом использование PGP было проблематичным, так как в ней применялось шифрование, подпадавшее под запрет на экспорт из США. Коммерческая версия PGP включает в себя плагины для нескольких популярных почтовых программ, что делает ее особенно удобной для включения в письмо электронной подписи и шифрования письма клиентом. Последние версии PGP используют лицензированную версию алгоритма шифрования с открытыми ключами RSA.

6.6. Примеры политик безопасности для электронной почты

Защита писем, почтовых серверов и программ должна соответствовать важности информации, передаваемой по сетям. Как правило, должно осуществляться централизованное управление сервисами электронной почты. Должна быть разработана политика, в которой указывался бы нужный уровень защиты.

Низкий риск

Пользователь

- Использование служб электронной почты для целей, явно противоречащих интересам организации или противоречащих политикам безопасности организации, запрещено, так же как и чрезмерное использование ее в личных целях.
- Использование адресов организации в письмах-пирамидах запрещено.
- Организация предоставляет своим сотрудникам электронную почту для выполнения ими своих обязанностей. Ограниченное использование ее в личных целях разрешается, если оно не угрожает организации.
- Использование электронной почты таким образом, что это помогает получать личную коммерческую выгоду, запрещено.

Менеджер

- Все сотрудники должны иметь адреса электронной почты.
- Справочники электронных адресов должны быть открыты для общего доступа.

- Если организация обеспечивает доступ к электронной почте внешних пользователей, таких, как консультанты, контрактные служащие или партнеры, они должны прочитать политику доступа к электронной почте и расписаться за это.
- Содержимое почтовых сообщений считается конфиденциальным, за исключением случая проведения расследований органами внутренних дел.

Сотрудник отдела автоматизации
- POP-сервер должен быть сконфигурирован так, чтобы исключать использование незашифрованных паролей с локальных машин.

Средний риск

Пользователь
- Электронная почта предоставляется сотрудникам организации только для выполнения ими своих служебных обязанностей. Использование ее в личных целях запрещено.
- Конфиденциальная информация или информация, являющаяся собственностью организации, не может быть послана с помощью электронной почты.
- Могут использоваться только утвержденные почтовые программы.
- Нельзя устанавливать анонимные ремэйлеры.
- Служащим запрещено использовать анонимные ремэйлеры.

Менеджер
- Конфиденциальная информация или информация, являющаяся собственностью организации, не может быть послана с помощью электронной почты.
- Если будет установлено, что сотрудник использует электронную почту с умыслом, он будет наказан.

Сотрудник отдела автоматизации
- Почтовая система должна обеспечивать только один внешний электронный адрес для каждого сотрудника. Этот адрес не должен содержать имени внутренней системы или должности.
- Должен вестись локальный архив MIME-совместимых программ для просмотра специальных форматов и быть доступен для внутреннего использования.

Высокий риск

Пользователь
- Электронная почта предоставляется сотрудникам организации только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.
- Все электронные письма, создаваемые и хранимые на компьютерах организации, являются собственностью организации и не считаются персональными.
- Организация оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.
- Пользователи не должны позволять кому-либо посылать письма, используя их идентификаторы. Это касается их начальников, секретарей, ассистентов или др.
- Организация оставляет за собой право осуществлять наблюдение за почтовыми отправлениями сотрудников. Электронные письма могут быть прочитаны организацией даже если они были удалены и отправителем, и получателем. Такие сообщения могут использоваться для обоснования наказания.

Менеджер
- Справочники электронных адресов сотрудников не могут быть сделаны доступными для всех.
- Если с помощью электронного письма должна быть послана конфиденциальная информация или информация, являющаяся собственностью организации, она должна быть зашифрована так, чтобы ее мог прочитать только тот, кому она предназначена, с использованием утвержденных в организации программ и алгоритмов.
- Никто из посетителей, контрактников или временных служащих не имеет права пользоваться электронной почтой организации.
- Должно использоваться шифрование всей информации, классифицированной как критическая или коммерческая тайна, при передаче ее через открытые сети, такие как Интернет.

- Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики.

Сотрудник отдела автоматизации

- Входящие письма должны проверяться на вирусы или другие РПС.
- Почтовые серверы должны быть сконфигурированы так, чтобы отвергать письма, адресованные не на компьютеры организации.
- Журналы почтовых серверов должны проверяться на предмет выявления использования неутвержденных почтовых клиентов сотрудниками организации, и о таких случаях должно докладываться.
- Почтовые клиенты должны быть сконфигурированы так, чтобы каждое сообщение содержало цифровую подпись отправителя.

6.7. Хранение электронных писем

Официальные документы организации, передаваемые с помощью электронной почты, должны быть идентифицированы и должны администрироваться, защищаться и сопровождаться настолько долго, насколько это нужно для деятельности организации, аудита, юристов или других целей. Когда электронная почта - это единственный способ передачи официальных документов компании, то к ним применяются те же самые процедуры, как если бы они передавались на бумаге.

Для предотвращения случайного удаления писем сотрудники должны направлять копии таких сообщений в официальный файл или архив. Должны храниться как входящие, так и выходящие сообщения с приложениями. Любое письмо, содержащее формальное разрешение или выражающее соглашение организации с другой организацией, должно копироваться в соответствующий файл (или должна делаться его печатная копия) для протоколируемости и аудита.

Период хранения всех писем определяется юристами. Если сообщения хранятся слишком долго, организация может по решению суда сделать такую информацию публичной.

7. Безопасность рабочей станции под управлением ОС Linux

Безопасность Linux окружения начинается с рабочей станции. Защищаете ли вы отдельный персональный компьютер (ПК) или обеспечиваете безопасность системы организации, безопасность начинается с ПК.

7.1. Оценка безопасности рабочей станции

Когда проводится оценка безопасности рабочей станции, пользователь должен обратить внимание на следующее:

- Безопасность BIOS и загрузчика операционной системы – имеет ли неавторизованный пользователь физический доступ к машине и может ли он загрузиться в однопользовательском или безопасном режиме без пароля.
- Безопасность паролей – каким образом обеспечивается безопасность паролей пользователей на машине.
- Административное управление – какие учетные записи и какое количество из них имеют административные права.
- Доступные сетевые сервисы – какие сервисы прослушивают запросы из сети, а также какие могут быть запущены.
- Персональный файервол – какой тип файервола необходимо использовать.
- Инструменты, повышающие безопасность соединений – какие инструменты используются для связи между компьютерами и какие должны быть удалены.

7.1.1. Безопасность BIOS и загрузчика операционной системы

Парольная защита для BIOS и загрузчика операционной системы может предотвратить получение прав администратора (root) неавторизованными пользователями в вашей системе, имеющими физический либо удаленный доступ к ней, а также получения прав администратора (root) посредством загрузки в однопользовательском режиме. При разработке правил защиты необходимо учитывать, какая информация находится на машине, а также месторасположение рабочей станции. Например, если машина используется для торговых презентаций и не содержит важной информации, то она может быть некритична для некоторых видов атак. Однако, если личные рабочие станции (домашние ПК, laptop) служащих имеют беспарольную защиту SSH ключей, с помощью которых осуществляется доступ к корпоративной сети, то это может создать значительную брешь в защите.

С другой стороны, если рабочая станция установлена в месте, куда имеют доступ только авторизованные и надежные люди, то необходимость в защите BIOS и загрузчика операционной системы может возникать не всегда.

7.1.2. Парольная защита BIOS

Следует привести два главных аргумента в пользу парольной защиты BIOS:

1. Предупреждение изменения настроек BIOS – если вторгшийся в вашу систему имеет доступ к BIOS, он может загрузиться с дискеты или с CD-ROM. Это дает ему возможность войдя в систему в безопасном или однопользовательском режиме запустить различные программы или скопировать данные.
2. Предупреждение загрузки системы – некоторые BIOS могут обеспечить парольную защиту процесса их загрузки. При активации системы атакующему необходимо будет ввести пароль BIOS для продолжения загрузки.

Так как методы установки BIOS у различных производителей отличаются, то необходимо изучить руководство для вашего компьютера.

Если вы забыли пароль BIOS, вы можете обнулить его перемычками на материнской плате или разомкнуть контакты CMOS батареи. Однако перед выполнением этих действий необходимо обратиться к руководству по обслуживанию вашей рабочей станции.

Внимание! Некоторые системы BIOS **не поддерживают** парольную защиту.

7.1.3. Парольная защита загрузчика операционной системы

Следующие аргументы служат для обоснования парольной защиты загрузчика ОС Linux:

1) предотвращение доступа к загрузке в однопользовательском режиме – если атакующий может загрузиться в однопользовательском режиме, то он становится пользователем с правами администратора (root);
2) предотвращение доступа к консоли GRUB – если на машине в качестве загрузчика используется GRUB, атакующий может используя интерфейс командного редактора изменить ее конфигурацию или собрать информацию используя команду cat;
3) предотвращение доступа к небезопасным операционным системам – если в системе установлена возможность загрузки двух ОС, атакующий может выбрать, например DOS, которая игнорирует управление доступом и защиту файлов.

В настоящее время при работе с ОС Linux наиболее распространенными являются загрузчики GRUB и LILO. Следующие два раздела описывают, как осуществить парольную защиту этих приложений.

7.1.4. Парольная защита GRUB

Вы можете сконфигурировать GRUB, добавив директиву **password** в конфигурационный файл. Это первое решение по поводу парольной защиты, затем откройте командный интерпретатор с правами администратора (root) и введите следующее:

/sbin/grub-md5-crypt.

Запустите модуль. Это позволит модулю MD5 хешировать пароли.

Отредактируйте конфигурационный файл GRUB:

/boot/grub/grub.conf.

Откройте файл.

Ниже последней строчки основного документа добавьте следующее:

password-md5 password-hash

Переместите password hash со значениями в:

/sbin/grub-md5-crypt (GRUB также допускает простой текст паролей, но рекомендуется использовать md5, потому что /boot/grub/grub.conf при установке по умолчанию, в некоторых дистрибутивах Linux, может быть прочитан.)

Загрузите систему.

GRUB меню не позволит вам доступ к редактору или командному интерфейсу без первоначального нажатия [p] ведущего к паролю GRUB.

К сожалению, это решение не предотвратит атаки от загрузки небезопасной ОС в двойном boot окружении, то есть если на машине установлена кроме Linux еще и небезопасная ОС.

Чтобы убрать данную уязвимость, необходимо отредактировать различные части /boot/grub/grub.conf файла. Просмотрите файл и найдите строчки с заголовками небезопасных ОС. Добавьте прямо под ними lock. Для DOS системы это выглядит следующим образом:

```
title DOS
lock
```

Внимание! Вы должны хранить парольную строку в основном разделе /boot/grub/grub.conf файла, для чего необходимо проделать соответствующую работу. В противном случае атакующий будет способен получить доступ к редактору и удалить строку lock.

Если вы имеете различные пароли к определенному ядру или ОС, добавьте строку lock и следом строку password. Таким образом, вы защитите каждый уникальный пароль. Пример:

```
title DOS
lock
password –md5 password hash
```

Запомните, что файл /boot/grub/grub.conf в некоторых дистрибутивах Linux по умолчанию читаем. Хорошим решением будет изменить это, так как данное изменение не отразится на функциональности GRUB. Для этого выполните с правами администратора (root) следующую команду:

chmod600 /boot/grub/grub.conf.

7.1.5. Парольная защита LILO

LILO более простой загрузчик, чем GRUB, и не предоставляет командный интерфейс. Поэтому вы можете не беспокоиться, что атакующий получит доступ к системе перед тем, как будет загружено ядро. Однако остается опасность загрузки в однопользовательском режиме или загрузки небезопасной ОС.

Вы можете сконфигурировать LILO таким образом, чтобы он запрашивал пароль перед загрузкой любой ОС или ядра. Добавьте парольную директиву. Для этого откройте терминал с правами администратора (root) и отредактируйте файл /etc/lilo.conf.

Первоначально добавьте парольную директиву следующим образом (в таком виде она будет действовать на все ОС в системе):

pssword=*password*

В вышеобозначенной директиве вместо второго слова *password* проставьте свой пароль.

Важное: В любое время при редактировании /etc/lilo.conf можно запустить команду /sbin/lilo-v-v для того, чтобы изменения вступили в силу.

Если вы не хотите иметь общий пароль, вы можете добавить парольную директиву в список файла /etc/lilo.conf для любого ядра или ОС, для которой вы хотите ограничить доступ. Для этого сделайте следующее, добавьте парольную директиву непосредственно под строкой image. После окончания редактирования вы увидите примерно следующее:

image= /boot/vmlinuz- version
password=*password*

Если вы хотите позволить загрузку ядра или ОС без парольной верификации, но не хотите позволять пользователям вносить изменения без пароля, вы можете добавить ограничительную директиву в строку после password. Это будет выглядеть примерно так:

image= /boot/vmlinuz- version
password=*password*
restricted

Если вы используете команду restricted, то вы должны иметь строку password.

Внимание! Файл /etc/lilo.conf в некоторых дистрибутивах Linux по умолчанию читаем. Если вы защищаете паролем LILO, необходимо чтобы только администратор (root) мог читать и редактировать файл со всеми паролями в виде обычного текста. Для этого выполните с правами root следующую команду:

chmod600 /etc/lilo.conf

7.1.6. Безопасность пароля

Пароли – это первый шаг верификации, который требует Linux при входе пользователя в систему. Поэтому безопасность пароля имеет огромное значение для защиты пользователя, рабочей станции и сети.

В целях безопасности инсталляционная программа Linux по умолчанию использует Message – Digest Algoritm (MD5) и “теневые” пароли. Убедительно рекомендуется не изменять данные настройки. Если вы исключите MD5 в процессе инсталляции, то будет использоваться старый формат DES. Этот формат ограничивает длину пароля 8 символами (не предусмотрен ввод пунктуации и специальных символов) и предлагает 56-битовый уровень шифрования.

Если вы исключите затенение паролей, то все пользовательские пароли в виде однонаправленного хеша будут находиться в читаемом файле /etc/passwd. Это откроет путь взлома паролей вашей системы в режиме offline. Если злоумышленник может получить доступ к машине как легальный пользователь, он может просмотреть файл /etc/passwd и затем, запустив программы - взломщики паролей, взломать их. И если в файле находятся небезопасные пароли, то только вопрос времени, когда они будут взломаны.

Затенение паролей устраняет этот тип атак, так как хранит хеши паролей в файле /etc/shadow, который читаем только с правами администратора (root).

Это исключит удаленный взлом паролей, если злоумышленник использует такие сетевые сервисы, как SSH и FTP. Этот вид атак “грубой силы” очень тихий и не оставляет сотен записей в log файлах о попытках входа в систему. Конечно, если злоумышленник начал атаку среди ночи и у вас слабые пароли, то он может получить доступ до того, как вы это заметите. Поэтому необходимо учитывать формат и условия хранения паролей. Самое простое и наиболее важное, что может сделать для своей защиты пользователь – это создание сложных паролей, что делает атаки по взлому паролей менее чувствительными для системы.

7.2. Обеспечение целостности файловой системы ОС Linux

При обеспечении целостности файловой системы ОС Linux очень важно сохранить моментальный снимок состояния системы сразу после установки, поскольку наиболее надежным методом определения целостности является сравнение объектов. При *сравнении объектов* целью является получение ответа на вопрос: "Все ли сохранилось в прежнем виде?". *Объектами* могут быть файлы, каталоги, устройства и т.п. Они *сравниваются* с этими же объектами в прежнем состоянии.

Существует несколько подходов к сравнению объектов, но все они основаны на выявлении изменений в информации о состоянии файлов. Например, очень примитивный подход состоит в создании контрольного списка всех файлов и последующем поиске в нем изменений таких параметров, как:

- дата последнего изменения;
- дата создания;
- размер файла.

К сожалению, этого недостаточно, поскольку эти значения (дата и время) можно легко изменить.

Еще один подход состоит в использовании простых контрольных сумм. Контрольные суммы — это числовые значения, сформированные на базе сумм битов данных файла, и часто используемые программами, выполняющими передачу данных по сети. При передаче данных из пункта А в пункт Б клиент и сервер запоминают контрольную сумму для каждого блока данных. В пункте приема контрольная сумма сравнивается с полученными данными. Если два значения совпадают, значит, данные переданы успешно и без искажений. Если же сравниваемые значения не совпадают, значит, данные были повреждены при передаче — генерируется соответствующее сообщение об ошибке.

Генерировать контрольные суммы статических файлов можно с помощью различных утилит, включая **sum** (или, на некоторых платформах, cksum).

Утилита **sum** вычисляет и выдает 16-битовую контрольную сумму для указанного файла, а также выдает количество блоков в файле. Пустые (NULL) символы (с нулевым кодом ASCII) при вычислении контрольной суммы игнорируются. Утилита sum обычно используется для поиска дефектов или для проверки файла, переданного по линии связи.

Для простой и грубой проверки целостности файлов (без особых гарантий) можно сгенерировать моментальный снимок всей файловой системы при помощи следующей команды:

 # sum 'find / ***каталог .*** **-print' >** <файл_контрольной_суммы.txt>

Эта команда сгенерирует 16-битовую контрольную сумму для каждого файла на жестком диске и поместит результат в файл **файл_контрольной_суммы.txt.** Затем можно написать сценарий для периодического сравнения этих значений с текущими значениями в системе. Он предупредит вас об изменении состояния и нарушении целостности файлов.

Для сравнения двух файлов воспользуйтесь командой **diff**.

Созданный файл **файл_контрольной_суммы.txt** необходимо сохранить в безопасном месте, возможно, даже в файловой системе, смонтированной только для чтения.

Этот подход, несомненно, предпочтительнее сравнения времени, даты создания или даты последнего изменения. Однако 16-разрядных контрольных сумм недостаточно. Поэтому желательно использовать алгоритмы типа MD5. Алгоритм MD5 принадлежит к семейству односторонних хеш-функций под общим названием "алгоритм резюмирования сообщений" (message digest algorithms) и первоначально определен в стандарте RFC 1321.

Алгоритм [MD5] воспринимает в качестве входных данных сообщение произвольной длины и выдает в результате 128-разрядных "отпечатков" или "резюме сообщения" для входных данных. Предполагается, что невозможно создать два различных сообщения с одинаковыми резюме или за приемлемое время создать сообщение с определенным, заранее известным резюме.

Алгоритмы резюмирования сообщений обеспечивают высокую степень надежности, особенно хорошо они подходят для проверки целостности файлов. Важно использовать средства, которые могут автоматически создавать моментальный снимок исходной операционной системы и генерировать по алгоритму MD5 (или аналогичному) значения для последующих сравнений. Наиболее известным и широко используемым средством такого рода является Tripwire.

8. Tripwire

Tripwire — гибкое и удобное средство проверки целостности файлов, использующее различные алгоритмы.

Tripwire гарантирует первичную целостность файловой системы. Вот некоторые из более интересных возможностей этой программы.

- Tripwire может работать с удаленными компьютерами по сети. Поэтому можно сгенерировать базу данных цифровых "отпечатков" для всей сети сразу после ее установки.
- Tripwire написана на языке C с целью обеспечения переносимости. Она будет компилироваться и собираться на любой платформе без изменений в исходном коде.
- Tripwire поставляется вместе с макроязыком, позволяющим автоматизировать выполнение определенных действий.

Tripwire — превосходное инструментальное средство, но только при совместном использовании с другими мерами защиты. Например, Tripwire никак не поможет, если не защитить первоначальный моментальный снимок файловой системы и базу данных "отпечатков". База данных, используемая средством проверки целостности, должна быть защищена от неавторизованного изменения; если посторонний сможет изменить базу данных вся схема проверки целостности будет разрушена.

Перед первоначальным запуском Tripwire необходимо настроить два файла:

- файл конфигурации Tripwire;
- файл политики Tripwire.

8.1. Файл конфигурации Tripwire

В файле конфигурации хранится информация о системе (в основном о месте установки утилит и файлов конфигурации Tripwire). Стандартный файл конфигурации **(twcfg.txt)** находится в каталоге **/etc/tripwire**. Однако программа Tripwire использует не этот файл. Действительный файл конфигурации зашифрован и блокирован. Для загрузки незашифрованного файла в качестве файла конфигурации можно воспользоваться командой **twadmin — create-cfgfile**

[root@pointy tripwire-2.3]# more /etc/tripwire/ twcfq.txt

8.2. Файл политики Tripwire

Просмотрите файл политики Tripwire. В файле политики хранятся спецификации объектов (файлов, каталогов и т.п.), которые должна отслеживать программа Tripwire, а также их местонахождение.

Tripwire поставляется с файлом-образцом /etc/tripwire/twpol.txt, который оптимизирован для Red Hat Linux 7.x. Необходимо просмотреть его перед первым запуском Tripwire. Вы сможете обнаружить и удалить ошибочные пути, а также прописать по необходимости новые.

Если изменения в файле политики сделаны или не требуются, можно приступать к конфигурированию и запуску Tripwire.

Кроме Tripwire существует ряд других средств проверки целостности файлов (Aide, ATP, Distributed L6 и т.п.,причем некоторые поставляются с исходным кодом). Все они компилируются в той или иной версии UNIX, но ни одно не предназначено специально для Linux.

8.3. Административное управление

При администрировании персональной машины пользователь выполняет некоторые задачи с правами администратора (root) или достигает использования прав root при помощи таких программ, как sudo или su.

Однако для системного администратора необходимо сделать выбор, сколько людей в организации могут иметь административный доступ к данной машине. Через модуль PAM, вызываемый

pam_console.so, некоторые действия, которые обычно зарезервированы за пользователем с правами администратора (root), могут быть выполнены обычным пользователем.

Однако другие важные задачи по системному администрированию, такие, как изменение сетевых настроек, конфигурирование новой мыши или мониторинг сетевых устройств будут невозможны без административного доступа. Как результат системный администратор может определить, сколько доверенных пользователей в его сети.

8.3.1. Подгружаемые модули аутентификации

PAM (Pluggable Authentication Modules), означает подгружаемые модули аутентификации (ПМА).

Теперь если программа (в частности login) желает произвести аутентификацию пользователя, она больше не занимается этим, а обращается к модулю PAM с соответствующей просьбой. PAM выполняет все проверки и отправляет вызвавшей его программе результат процесса аутентификации. Выбор алгоритма и особенности аутентификации теперь относятся к компетенции модуля PAM.

Формально PAM выполнен в виде разделяемых библиотек-модулей, расположенных в каталоге /lib/security/. Каждый модуль по-особому пропускает через себя пользователя, реализуя свой особенный механизм аутентификации. То есть, запуская тот или иной набор модулей, можно реализовывать свои собственные сценарии аутентификации.

Информация о том, каким программам какой сценарий использовать, расположена в каталоге /etc/pam.d. Имя каждого сценария в этом каталоге совпадает с именем программы, для которого он предназначен. Например, сценарий для login находится по адресу /etc/pam.d/login.

Содержимое данного файла может выглядить, например, так:

```
#%PAM-1.0
auth     requisite     /lib/security/pam_unix.so      nullok #set_secrpc
auth     required      /lib/security/pam_securetty.so
auth     required      /lib/security/pam_env.so
auth     required      /lib/security/pam_mail.so
account  required      /lib/security/pam_unix.so
password required      /lib/security/pam_unix.so      strict=false
session  required      /lib/security/pam_unix.so      none # debug or trace
session  required      /lib/security/pam_limits.so
```

Каждая строчка означает, что для удачной аутентификации пользователь должен пройти через указанный модуль.

Формат записи данного файла содержит:

- тип-модуля;
- флаг-контроля;
- путь-к-модулю;
- параметры-модуля.

Тип-модуля должен быть одним из:

- **auth:**Такой модуль проверяет наличие пользователя в системе, спрашивает его имя, разрешает или нет доступ в ту или иную группу (независимо от записей в файле /etc/groups) и вообще способен давать привилегии (конечно, специально предназначенные для этого);
- **account**: Этот модуль не занимается аутентификацией, а позволяет контролировать распределение ресурсов системы для тех или иных пользовательских бюджетов;
- **session**: Модуль связан с процессами, которые могут происходить, перед тем как пользователь получит доступ к той или иной службе. Например, ведение записей в системных журналах;
- **password**:Модуль, как следует из названия, занимающийся непосредственно проверкой паролей на подлинность, слабость и т.д.

Флаг-контроля указывает, как система будет реагировать при удачном или неудачном прохождении соответствующего модуля. Поскольку модули запускаются последовательно один за другим, то специальной расстановкой флагов можно определить значимость каждого из них. Возможна простая и слож-

ная форма записи подобных флагов. В качестве флагов могут быть использованы следующие ключевые слова:

- **required**: Успех этого модуля требуется для всей аутентификации в целом. Неудача модуля с подобным флагом не проявится для пользователя, пока не выполнятся все оставшиеся модули;
- **requisite**: То же самое, но только в случае провала управление тут же будет возвращено приложению;
- **sufficient**: Удачное прохождение подобного модуля считается достаточным для признания всей аутентификации удачной, если не провалилась проверка на предшествующих модулях с флагом required. Неудача же этого модуля не считается фатальной для всей последующей аутентификации;
- **optional:** Этот модуль не критичен для аутентификации и используется как дополнительный. То есть, например, может ограничиться выводом на экран предупреждения о слабости вашего пароля.

Путь-к-модулю должен указывать полный адрес выбранного модуля на диске, а **параметры-модуля** зависят от его выбора.

Помимо файлов-сценариев для некоторых модулей могут использоваться дополнительные файлы конфигурации. Все они расположены в каталоге /etc/security и каждый файл предназначен для конкретной группы настроек.

time.conf - Здесь вы сможете ограничить время доступа пользователей с различных терминалов к различным сервисам. Например, запретить входить в систему с первой виртуальной консоли администратору во время выходных. Эти настройки обслуживает модуль pam_time и соответственно, если вы хотите, чтобы ваши ограничения возымели действие, модуль должен быть прописан в соответствующем сценарии.
pam_env.conf - С помощью данного файла можно ограничить возможности в изменении отдельных переменных среды пользователями. Работает под руководством модуля pam_env.
limits.conf - В данном файле можно индивидуально или для группы ограничить: размер core-файла, максимальный допустимый размер файла, максимальное количество открытых файлов, запущенных процессов, сколько раз можно одновременно зайти в систему и т.д. Руководящий модуль pam_limits.
access.conf - Так как PAM имеет средства аутентификации по сети, то подобные настройки являются полезными, ибо контролируется не только кто может войти, но и откуда. Контролируется pam_access.
group.conf - Можно указать, какой группе будет принадлежать служба, запущенная определенным пользователем, в определенное время с определенного терминала. Руководящие модули pam_time и pam_group.
console.perms - В этом файле определяются права, получаемые привилегированными пользователями к консоли во время входа в систему и возвращаемые при выходе. Модуль pam_console.

Итак, логика действий проста и понятна, осталось только разобраться, какие могут быть модули.

- **pam_cracklib**: Тип password. Проверяет ваш пароль на стойкость, не является ли он, например, палиндромом (это необязательно при использовании модуля pam_unix). Полезен для программ, задающих пароли. Полезные параметры: retry=N – дается N попыток на исправление ошибки, diffok=N-должно быть изменено минимум N символов при смене пароля,minlen=N -минимальный размер пароля, dcredit=N ucredit=N lcredit=N ocredit=N - в пароле должно присутствовать минимум N цифр, строчных, прописных букв и других символов.
- **pam_deny**:Тип любой. Всегда перекрывает доступ.
- **pam_env**: Тип auth. Контролирует сохранность переменных среды. Полезный параметр conffile=S - задает альтернативное название файла конфигурации.
- **pam_ftp**: Тип auth. Предназначен для организации анонимного доступа. То есть, получив имя пользователя «anonymous», ждет в качестве пароля что-то похожее на его почтовый адрес. Полезные параметры: ignore – не обращать внимание, похож ли пароль на почтовый адрес, users=XXX,YYY -позволяет анонимный вход для пользователей из этого списка.
- **pam_group**: Тип auth. Предназначение ясно из описания конфигурационного файла group.conf.
- **pam_lastlog**: Тип auth. Сообщает о времени и месте входа в систему. Обновляет /var/log/wtmp файл. Полезные параметры: nodate, noterm, nohost, silent – не выводить в сообщении даты, терминала, машины или вообще ничего, never – если пользователь никогда ранее не появлялся, то его приветствуют.
- **pam_limits**: Тип session. Предназначение указано выше при описании файла limits.conf. Полезный параметр: conf=S – альтернативное имя конфигурационного файла.
- **pam_listfile**: Тип auth. Предназначен для организации доступа на основе конфигурационных файлов-списков, например /etc/ftpaccess. Для примера смотрите соответствующие файлы сценариев. Возможные параметры: onerr=succeed|fail; sence=allow|deny; file=filename; item=user|tty|rhost|ruser|group|shell apply=user|@group. Первый параметр задает возвращаемое

значение в случае неудачного поиска. Второй - в случае удачного поиска. Третий – имя файла со списком. Четвертый –тип элемента в списке. Последний вносит дополнительный ограничения, если тип объявлен tty, rhost или shell.

- **pam_mail**: Тип auth. Сообщается о наличии почты, если таковая имеется. Полезные параметры: dir=S – путь к каталогу почтовых очередей, noenv - не устанавливать переменную среды MAIL, close – сообщать, если есть почта у пользователей с аннулированными бюджетами, nopen – не печатать какой-либо почтовой информации, если пользовательский бюджет только-что заведен.
- **pam_nologin**: Тип auth. Стандартная реакция на наличие файла /etc/nologin. Когда он присутствует, в систему может зайти только root, а остальным будет выдано на экран содержимое этого файла.
- **pam_permit**: Тип любой. Использование данного модуля ОПАСНО и применимо только в критических ситуациях. Всегда дает допуск.
- **pam_pwdb**: Тип любой. Замещает модули серии pam_unix.... . Использует интерфейс библиотеки libpwdb (пользовательские базы данных), что повышает независимость системы аутентификации от способа хранения пользовательских данных (NIS или passwd или shadow). Полезные параметры: nullok – можно использовать пустые пароли, md5, shadow, bigcrypt – различные способы шифрования пароля.
- **pam_radius**: Тип session. Позволяет осуществлять аутентификацию через RADIUS сервер.
- **pam_rhosts_auth**: Тип auth. Механизм работы этого модуля основывается на анализе содержимого файлов hosts.equiv и .rhosts используемых для аутентификации таких служб, как rlogin и rsh. Полезные параметры: no_hosts_equiv – игнорировать содержимое файла hosts.equiv, no_rhosts – игнорировать содержимое файлов .rhosts, suppress – охраняет системные журналы от потока малозначимых сообщений в частности, когда используется контрольный флаг sufficient.
- **pam_root_ok**: Тип auth. Используется в случае, когда администратору необходимо получать доступ к сервису без введения пароля. Этот модуль допускает пользователя к сервису, только если его uid равен 0.
- **pam_securetty**: Включает в проверку файл /etc/securetty. Суперпользователь сможет зайти только на указанных там терминалах.
- **pam_time**: Тип account. Принцип работы ясен из описания устройства конфигурационного файла time.conf.
- **pam_warn**: Тип auth и password. Просто ведет записи в системных журналах например при смене пароля.
- **pam_weel**: Тип auth. Для любителей BSD, где получить права суперпользователя может только пользователь группы wheel (группа root в Linux). Полезные параметры: group=XXX – использовать указанную группу вместо стандартной нулевой, deny – инвертирование действия алгоритма, запрещается получать права суперпользователя пользователям указанной группы, используется вместе с предыдущим параметром, trust – избавляет пользователей группы wheel от необходимости вводить пароль при смене uid на 0.

8.3.2. Предоставление доступа с правами администратора

Если среди сотрудников организации есть доверенные люди, то возможность предоставления им прав администратора (root) может быть неплохим намерением с вашей стороны.

Добавление прав доступа пользователям означает, что добавление устройств и конфигурирование сетевого интерфейса может быть выполнено индивидуальным пользователем.

С другой стороны, предоставление административных прав доступа индивидуальным пользователям может привести к следующему (перечислены только некоторые события):

- Микроконфигурирование машины – пользователи с правами root могут микроконфигурировать машину и попросить помощи для восстановления работоспособности или, что еще хуже, открыть уязвимости в системе безопасности, не зная об этом;
- Запуск небезопасных сервисов – пользователи с правами root могут запустить на своих машинах небезопасные сервисы, такие, как FTP или telnet, потенциально подвергающие имена пользователей и их пароли риску, так как они передаются по сети в открытом виде;
- Запуск почтовых сообщений с правами root – почтовые вирусы представляют наибольшую угрозу, если выполняются с правами root.

8.3.3. Запрещение доступа с правами администратора

Если администратору нежелательно предоставлять пользователям права root по тем или иным причинам, пароль root должен быть сохранен в секрете и доступ к уровню выполнения или простому пользовательскому режиму может быть ограничен через парольную защиту загрузчика прав root.

В табл. 8.1 показаны пути, по которым администратор может дополнительно обеспечить запрещение доступа к правам root.

Таблица 8.1

Запрещение доступа с правами администратора

Метод	Описание	Достоинства	Недостатки
Запрещение входа в систему с правами администратора, используя SSH	Отредактировать файл **/etc/ssh/sshd_config** и установить параметр PermitRootLogin в **no**	Предупреждение входа в систему с правами администратора, используя инструменты OpenSSH. Предупреждают доступ следующие программы**: ssh, scp, sftp**	Эффективна только для инструментов OpenSSH, на другие программы данная установка не действует
Изменение командного интерпретатора администратора	Отредактируйте файл **/etc/passwd** и измените оболочку с **/bin/bash/** на **/sbin/nologin**	Предупреждает попытки доступа к оболочке администратора и попытки входа. Следующие программы предупреждают доступ к правам администратора: **login, gdm, kdm, xdm, su, ssh, scp, sftp**	Не действует на программы, которые не требуют оболочки, такие, как FTP клиенты, почтовые клиенты и другие setuid программы. Следующие программы не предотвращают доступ к оболочке с правами администратора: **sudo, ftp clients, e-mail clients**
Запрещение доступа с правами администратора к любому устройству консоли (**tty**)	Файл **/etc/securetty** предотвращает вход с правами администратора на любое устройство, подключенное к компьютеру	Предотвращение доступа к виртуальной консоли или сети. Следующие программы предотвращают доступ с правами администратора: **login, gdm, kdm, xdm,** другие сетевые сервисы, которые открывает **tty**	Программы, которые не требуют входа с правами администратора, но решают административные задачи через setuid механизмы. Следующие программы не предотвращают доступа к правам администратора: **su, sudo, ssh, scp, sftp**.
Использование PAM для ограничения прав доступа к сервисам, использующие права администратора	Отредактируйте файл целевого сервиса в директории **/etc/pam.d/** Сделайте pam_listfile.so, требующим аутентификации. Для большей информации смотри раздел ”Подгружаемые модули аутентификации”	Предотвращение доступа к сетевым сервисам использующих права администратора, которые поддерживает PAM	Программы и сервисы которые не поддерживает PAM

8.3.4. Запрещение прав доступа к командному интерпретатору с правами администратора

Если администратор не хочет предоставлять пользователям доступ к командному интерпретатору с правами root, он может установить пароль для /sbin/nologin в файле /etc/passwd. Это предотвратит доступ к системе с правами администратора через команды оболочки, такие, как su и ssh.

Важное: Программы, которые не требуют доступа к оболочке shell, такие, как e-mail клиенты или команда sudo, в данном случае могут получить доступ к правам администратора.

8.3.5. Запрещение доступа к регистрации с правами администратора

Дальнейшее запрещение прав доступа заключается в отключении возможности регистрации в системе с правами администратора, осуществляя редактирование через консоль файл /etc/securetty. Этот файл содержит все устройства, с которых может регистрироваться администратор. Если файла не существует вообще, то пользователь с правами администратора может войти в систему через любое коммуникационное устройство, будь то консоль или сетевой интерфейс. Это опасно, потому что при конфигурации данным образом пользователь может, используя telnet на своей машине с правами администратора, послать пароль в простом виде через сеть. По умолчанию многие дистрибутивы ОС Linux к файлу /etc/securetty допускают только пользователя с правами администратора зарегистрированного на консоли физически прикрепленной к машине (не виртуальной). Предотвращение удаления содержимого этого файла пользователем с правами администратора осуществляется следующей командой:

```
echo> /etc/securetty
```

Внимание! Данное решение по поводу файла /etc/securetty будет бессмысленно для предотвращения действий пользователя с правами администратора, зарегистрировавшегося удаленно при помощи OpenSSH, потому что консоль не будет открыта до тех пор, пока не будет проведена аутентификация.

8.3.6. Запрещение доступа к регистрации с правами администратора при помощи SSH

Для предотвращения входа в систему пользователя с правами при помощи SSH вам необходимо отредактировать конфигурационный файл демона SSH: /etc/ssh/sshd_config. Измените строку содержащую: #PermitRootLogin yes

на

```
PermitRootLogin no
```

8.3.7. Запрещение доступа к регистрации с правами администратора при помощи PAM

Модуль PAM, /lib/security/pam_listfile.so, предоставляет большую гибкость для специфических ограничений доступа. Он предоставляет администратору распечатку пользователей, которым не позволен доступ. Ниже показано, как модуль используется для FTP сервиса в /etc/pamd/ftp, конфигурационном файле PAM (\ в последнем символе первой строки нет необходимости, если для управления используется только одна строка):

```
auth required /lib/security/pam_listfile.so item=user\
sense=denyfile=/etc/ftpusers onerr=succed
```

Это говорит о том, что PAM учитывает файл /etc/ftpusers и запрещает любому прописанному там пользователю доступ к сервису. Администратор свободно изменяет название этого файла и может сохранять отдельные списки для каждого сервиса или использовать один общий список для запрещения доступа ко множеству сервисов.

Если администратор хочет запретить доступ ко множеству сервисов, он может добавить похожую строку в PAM конфигурируемые сервисы, такие, как /etc/pam.d/pop и /etc/pam.d/imap для почтовых клиентов или /etc/pam.d/ssh для SSH клиентов.

8.3.8. Ограничение доступа к регистрации с правами администратора

Часто администратор может предоставлять доступ к root пользователю только setuid программам, таким как su или sudo.

8.3.9. Команда su

Когда пользователь вызывает команду su, она немедленно требует ввода пароля администратора и после аутентификации предоставляет оболочку с правами администратора. Раз зарегистрировавшись su командой, пользователь станет администратором и будет иметь абсолютный административный

доступ к системе. Кроме того, если пользователь имеет права администратора, это делает возможным в некоторых случаях при использовании команды su изменить права любого другого пользователя в системе без предъявления пароля. Так как эта программа очень мощная, администратор может ограничить доступ к данной команде. Один из простых способов сделать это – добавить пользователей, имеющих доступ к команде su в специальную административную группу wheel. Для этого с правами root надо выполнить следующую команду:

usermod- G wheel username .

Затем откройте конфигурационный файл PAM для команды su, /etc/pam.d/su в режиме редактора и удалите коментарий [#] из следующей строчки:

auth required/lib/security/pam_wheel.so use_uid

Делать это допускается только членам административной группы wheel.

Примечание: Администратор принадлежит группе wheel по умолчанию.

8.3.10. Команда sudo

Команда sudo предлагает другой подход к предоставлению доверенным пользователям административного доступа. Когда доверенный пользователь выполняет какую-либо административную команду с помощью sudo, он повторяет **свой** пароль. Затем после успешной аутентификации и предположения, что команда допустима, она будет выполнена так, как если бы ее запускал администратор.

Основной формат команды sudo следующий:

sudo command

В вышеприведенном примере слово command заменяется командой, обычно предназначенной для выполнения только администратором, такой как mount.

Важное: Пользователи команды sudo должны быть внимательны, если отлучаются от своей машины, так как sudo может выполнять команды без запроса пароля в течение 5 минут. Эта установка может быть изменена в конфигурационном файле: /etc/sudoers.

Команда sudo предоставляет высокую степень гибкости. Например, только пользователи, прописанные в конфигурационном файле /etc/sudoers, могут использовать команду sudo и команда выполняется в их оболочке, а не в оболочке администратора. Это говорит о том, что оболочка администратора может быть достаточно полно защищена.

Команда sudo также предлагает понятный аудит. При каждой успешной аутентификации посылается сообщение в файл /var/log и команда, которая проводила вход пользователя, посылает его имя в файл безопасности /var/log.

Еще одним достоинством команды sudo является то, что администратор может предоставить различным пользователям доступ только к тем командам, которые им нужны.

Все команды, выполненные при помощи sudo, записываются в файл /var/log/secure, так же как и все попытки использования команды sudo.

Администраторам для редактирования конфигурационного файла sudo, /etc/sudoers необходимо использовать visudo.

Для предоставления некоторым пользователям полных административных привилегий запустите visudo и добавьте строку содержащую в разделе спецификаций привилегий пользователя следующее:

Juan ALL=(ALL)ALL

Этот пример говорит о том, что пользователь Juan может использовать sudo на любом хосте и выполнять любую команду.

Приведенный ниже пример показывает возможность детализации при конфигурировании sudo:

%userslocalhost=/sbin/shutdown-h now

А также то, что любой пользователь может в любое время выйти из консоли командой /sbin/shutdown-h now.

Страница man для sudores содержит детализированный список опций для этого файла.

8.3.11. Доступные сетевые сервисы

Многие сервисы под Linux работают как сетевые серверы. Если сетевой сервис запущен на машине, то серверное приложение вызывает демон, прослушивающий один или более сетевых портов. Каждый из этих серверов потенциально представляет угрозу и является дорогой для проведения атак.

8.3.12. Риски сервисов

Сетевые сервисы могут представлять различные риски для Linux систем. Ниже приведены некоторые важнейшие из них:

- Атаки переполнения буфера – сервисы, которые подсоединяются к портам от 0 до 1023, должны запускаться с правами администратора. Если при эксплуатации приложения возможно переполнение буфера, атакующий может достичь доступа к системе как пользователь запустивший демона. Так как приложения, у которых возможно переполнение буфера существуют, взломщики будут использовать автоматические инструменты для идентификации систем с такими уязвимостями, и раз они могут получить доступ, они будут использовать автоматические инструменты администратора, для сохранения своего доступа к системе.
- Атака «отказ в обслуживании» – заполняющая сервис запросами, она может привести систему к остановке, так как система будет пытаться завершить процесс входа и ответить на каждый запрос.
- Атаки с помощью уязвимых скриптов – если сервер использует скрипты, выполняющие действия на серверной стороне, взломщик может для атаки вставить неправильно написанные скрипты. Эти уязвимые к атакам скрипты могут привести к состоянию переполнения буфера или предоставить атакующему возможность изменения файлов в системе.

Ограничением для атак, использующих сеть, является отключение всех неиспользуемых сервисов.

8.3.13. Идентификационные и конфигурационные сервисы

Для увеличения безопасности большинство сетевых сервисов при инсталляции многих дистрибутивов ОС Linux по умолчанию отключены. Однако есть некоторые исключения:

- lpd – сервер печати, требующий команду lpr.
- portmap – необходимый компонент для NFS, NIS и других RFC протоколов.
- xinetd – суперсервер, который управляет соединениями с серверами подчиненными хосту, такими, как wuftp, vsftpd, telnet и sgi-fam (которые необходимы для файлового менеджера Nautilus).
- sendmail – агент передачи почтовых сообщений по умолчанию включен, но только в режиме прослушивания портов для соединения на локальной машине.
- sshd – сервер OpenSSH, который является безопасной заменой telnet.

Когда решается вопрос об использовании того или иного сервиса, лучше быть более осторожным. Например, если у вас нет принтера, не оставляйте запущенным сервис lpd в надежде, что скоро вы его приобретете. То же справедливо и для portmap, если вы не монтируете разделы NFS (ypbind сервис), то отключите portmap. ОС Linux содержит различные программы, предназначенные для включения или отключения сервисов. Это такие программы, как Services Configuration Tool, ntsysv и chkconfig.

Но проверять, какие сетевые сервисы сконфигурированы для запуска при старте системы, недостаточно. Системный администратор должен также проверять, какие порты открыты или прослушиваются.

8.3.14. Небезопасные сервисы

Потенциально любой сетевой сервис небезопасен. Поэтому так важно отключать все неиспользуемые сервисы. Периодически проверяйте и отключайте такие сервисы. Некоторые сетевые протоколы более опасны, чем другие. К ним относятся такие протоколы, сервисы которых позволяют следующее:

Посылают имена пользователей и пароли в простом виде и не шифруют сессию аутентификации – многие старые протоколы, такие как telnet и FTP.

Посылают важную информацию в простом виде – протоколы, которые посылают имя пользователя и пароль в простом виде, в таком же виде посылают и всю другую информацию между сервером и клиентом. Это такие протоколы, как telnet, FTP,HTTP (httpd) и SMTP (sendmail).

Многие сетевые файловые системы, такие как NFS и SMB, также посылают информацию через сеть в простом виде. Это возлагает на пользователя ответственность при передаче некоторых видов информации, когда он использует эти протоколы.

Сервисы удаленной подкачки памяти, подобные netdump, передают содержимое памяти через сеть. Подключаемая память может содержать пароли, базы данных либо другую важную информацию.

Другие сервисы подобные finger и rwhod предоставляют информацию о пользователях системы.

Примерами опасных сервисов являются: **rlogin, rsh, telnet, vsftpd, wu-ftpd**.

Все программы удаленного входа и программы оболочки (rlogin, rsh, telnet) были бы безопасны при исполнении в SSH.

FTP сервис не представляет такую опасность для системы, как удаленные оболочки, но FTP серверы должны быть внимательно сконфигурированы и периодически проверяться для устранения проблем.

Сервисы, которые должны быть внимательно сконфигурированы, а после контролироваться файерволом, следующие: finger, identd, netdump, netdump-server, nfs, portmap, rwhod, sendmail, smb (Samba), yppasswdd, ypserv, ypxfrd.

8.4. Персональный защитный экран (firewall)

Если есть необходимость в использовании сетевых сервисов, то очень важно использовать файервол (firewall). Файервол предотвращает доступ сетевых пакетов к сетевому интерфейсу системы. Если запрос поступил на порт, который заблокирован файерволом, он будет игнорирован. Если сервис прослушивает один из заблокированных портов, он не получит пакеты и будет эффективно отключен. По этой причине надо быть внимательным при конфигурировании блокирования доступа к неиспользуемым портам, для того чтобы не заблокировать доступ к портам, используемым конфигурационными сервисами.

Конфигурирование файервола осуществляется при помощи утилиты iptables.

8.5. Коммуникационные инструменты, повышающие безопасность

В связи с ростом популярности Интернета возникает угроза перехвата и прослушивания передаваемых данных. В последние годы были разработаны инструменты для криптографической передачи данных через сеть.

ОС Linux представляет следующие инструменты, использующие высокий уровень для защиты информации передаваемой по сети, – алгоритмы шифрования с открытым ключом.

- OpenSSH – бесплатный инструмент к SSH протоколу для шифрования сетевых соединений.
- Gnu Privacy Guard (GPG) – бесплатный инструмент к PGP (Pretty Good Privacy) криптографического приложения для шифрования данных.

OpenSSH – безопасный путь для удаленного доступа к машине, кроме того, заменяет старые нешифрующие сервисы, подобные telnet и rsh. OpenSSH включает в себя сетевой сервис sshd и три клиентских приложения:

- ssh – клиент безопасного удаленного доступа к консоли;
- scp – команда безопасного удаленного копирования;
- sftp – безопасный ftp клиент, который представляет интерактивные сессии передачи файлов.

Убедительно рекомендуется, чтобы любое удаленное соединение с Linux системами происходило с использованием SSH протокола.

Важное: Хотя сервис sshd достаточно безопасен, необходимо не забывать о своевременном его обновлении.

GPG – мощный инструмент, предназначенный для сохранения конфиденциальности личной информации. Он может использоваться для передачи по сетям общего назначения личной информации, а также для ее защиты на жестком диске компьютера.

9. Безопасность сервера под управлением ОС Linux

Когда ОС Linux используется как сервер в сети общего назначения, она становится потенциальной целью для различного рода атак. По этой причине усиление безопасности системы и блокирование неиспользуемых сервисов очень важны для системного администратора.

Для увеличения безопасности сервера необходимо обратить внимание на следующие основные пункты:

- проводить своевременное обновление всех сервисов для защиты от недавно обнаруженных уязвимостей;
- использовать безопасные протоколы всегда, как только это возможно;
- использовать только один тип сервиса всегда, как только это возможно;
- внимательно отслеживать подозрительную активность всех сервисов.

9.1. Безопасность сервисов с TCP Wrappers и xinetd

TCP Wrappers предоставляет управление доступом ко множеству сервисов. Большинство современных сетевых сервисов, таких как SSH, telnet, FTP, используют TCP Wrappers, программу, которая разработана для того, чтобы стоять на страже между поступающим запросом и запрашиваемым сервисом.

9.1.1. Повышение безопасности с TCP Wrappers

TCP Wrappers способен на много больше, чем только отказ в доступе к сервисам. Ниже показано, как он может использоваться для посылки флагов на соединение, для предостережения от атак с отдельных хостов, и повышения функциональности механизма входа в систему. Для перечисления функциональности и управления языком TCP Wrappers можно воспользоваться руководством man, опция хосты.

Посылка запугивающего сообщения клиенту, пытающемуся подключиться к сервису, является хорошим путем к маскировке, которую выполняет системный сервер, давая знать потенциальному нарушителю то, что системный администратор заботится о безопасности. TCP Wrappers использует опцию посылки сообщений при подключении к сервису. Например, инструмент посылки сообщений для wu-ftpd. Для начала вам необходимо создать посылаемый файл. Он может быть расположен в любом месте системы, но он должен иметь отношение некоторого имени как демон. Например: /etc/banners/in.ftpd. Содержимое файла может выглядеть примерно так:

220-Hello,%c

220-Вся активность на ftp.example.com регистрируется

220-Соединение будет продолжено и вы предупреждены

Символ % предоставляет информацию о клиенте, такую, как имя пользователя и имя машины или имя пользователя и IP-адрес, делающие соединение еще более запугивающим.

Для того чтобы вышеназванное сообщение выдавалось при входящих соединениях, добавьте в файл /etc/hosts.allow следующее:

in.ftpd:All:banners/etc/banners/

Если отдельные хосты или сеть имеют намерение атаковать сервер, TCP Wrappers может быть использован для предотвращения последующих атак из этих хостов или сетей директивой spawn.

В приведенном ниже примере показано, что взломщик из сети 206.182.68.0/24 предпринимает атаки на сервер. При размещении следующей строки в файле /etc/hosts.deny попытки удачных и неудачных соединений будут зафиксированы в специальном файле:

ALL:206.182.68.0:spawn/bin/'date'%c%d>>/var/log/intruder_alert

Символ %d предоставляет имя сервиса, что затруднит атакующему доступ.

Для предоставления возможности соединения и входа в систему директива spawn помещается в файл /etc/hosts.allow.

На заметку: С директивой spawn выполняется любая shell команда, вы можете создать скрипт, уведомляющий вас или выполняющий определенную цепочку команд в случае, когда некоторые клиенты пытаются подключиться к вашему серверу.

Если некоторые типы соединений более интересны, чем другие, уровень входа для этих сервисов может быть повышен опцией severity.

В приведенном ниже примере предполагается, что любой пытающийся подключиться к порту 23 (порт telnet) вашего FTP сервера – взломщик.

Обозначьте это, разместите флаг warning в log файлах вместо установленного по умолчанию флага info, и откажите в соединении.

Для этого в файл /etc/hosts.deny поместите следующую строку:
in.telnetd : ALL : severity warning

При этом будет использоваться регистрация authpriv, установленная по умолчанию, но повышен приоритет от установленного значения по умолчанию info до warning.

9.1.2. Повышение безопасности с xinetd

Другим мощным инструментом для управления доступом к подчиненным сервисам является xinetd. В этом разделе показано, как xinetd может быть использован для установки сервиса trap и управления любым количеством ресурсов данным xinetd сервису. xinetd может использоваться при генерации отчетов для предотвращения атак типа отказ в обслуживании. Для большей информации о возможностях данной опции можно воспользоваться руководством man для xinetd и xinetd.conf.

Одной из главных черт xinetd является ее способность добавлять хосты в глобальный список no_access. Хостам из этого списка не позволяется в дальнейшем подключаться к сервисам, управляемым xinetd в течение точно определенного промежутка времени или до тех пор пока xinetd будет перезапущен. Это выполняется при помощи атрибута sensor. Этот метод является достаточно легким для блокирования хостов, пытающихся сканировать порты сервера.

Первым шагом в установке sensor является выбор сервиса, с которым вы планируете его использование. Для примера возьмем сервис telnet.

Отредактируйте файл /etc/xinetd.d/telnet и измените строку флаги следующим образом:
flags = SENSOR.

Добавьте строку со следующей связкой:
deny_time=30

Это не позволит хосту, который пытался подключиться к порту, повторное подключение в течение 30 минут. Другим приемлемым значением для временного отказа является атрибут FOREVER, который сохраняет запрет на подключение до тех пор, пока xinetd не будет перезапущен, и атрибут NEVER, который предоставляет подключение и вход в систему. Последняя строка вышеобозначенного файла должна читаться как
disable=no

Несмотря на то что использование SENSOR является хорошей мерой для выявления и остановки подключений из неблагонадежных хостов, он имеет два недостатка:

- Не работает против сканеров-невидимок (stealth);
- Атакующий, который знает, что Вы запустили SENSOR, может организовать атаку против некоторых хостов, подделывая их IP-адреса и подсоединяясь к запрещенным портам.

9.2. Ресурсы управляемые сервером

Другой важной чертой xinetd является ее способность управлять многочисленными ресурсами сервисов, а также управлять процессом утилизации. Это может быть выполнено при помощи следующих директив:

- cps = <number_of_connections> <wait_period>- предписывает количество соединений, предоставляемых сервисом в секунду. Эта директива может принимать только целочисленное значение;
- instances = <number_of_connections> - предписывает общее количество соединений, доступных к сервису. Эта директива может принимать как целочисленное значение, так и значение UNLIMITED;
- per_source = <number_of_connections> - предписывает количество соединений, предоставляемых сервисом к каждому хосту. Эта директива может принимать как целочисленное значение, так и значение UNLIMITED;
- rlimit_as = <number[K|M]> - предписывает количество адресного пространства памяти, которое сервис может занять в килобайтах или магабайтах. Эта директива может принимать как целочисленное значение, так и значение UNLIMITED;
- rlimit_cpu = <number_of_seconds> - предписывает количество времени в секундах, на которое сервис может занять процессор. Эта директива может принимать как целочисленное значение, так и значение UNLIMITED;

Использование этих директив может помочь предотвратить отказ в обслуживании любого xinetd сервиса в системе.

9.3. Безопасность Portmap

Portmap сервис – это динамический порт, назначаемый демону для сервисов RPC, таких как NIS и NFS. RPC – это сокращение от Remote Procedure Call (удаленный вызов процедур). Он имеет слабые механизмы аутентификации и возможность назначать широкие полномочия портам сервисов по их управлению. Поэтому обеспечение его безопасности является трудной задачей.

Если вы запустили RPC сервисы, вы должны выполнять некоторые основные правила.

9.3.1. Защита portmap при помощи TCP Wrappers

Важно использовать TCP Wrappers для ограничения сетей или хостов, имеющих доступ к portmap сервису, но не имеющих надежных средств аутентификации. Затем используйте только IP-адреса, для которых ограничивается доступ к сервису. Следует помнить: чем меньше хостов имеют доступ к portmap, тем лучше.

9.3.2. Защита portmap при помощи iptables

Дальнейшее ограничение доступа к portmap сервису можно обеспечить установкой правил iptables, ограничивающих доступ специфических сетей. Ниже в примере показана iptables команда, которая предоставляет только TCP-подключения к portmap, прослушивающий 111 порт, только из сети 192.168.0/24. Все другие пакеты будут отвергнуты.

```
iptables -A INPUT -p tcp -s! 192.168.0.0/24  --dport 111 -j DROP
```

Похожим образом ограничивается и UDP трафик, для этого используйте следующую команду:

```
iptables -A INPUT -p udp -s! 192.168.0.0/24  --dport 111 -j DROP
```

9.4. Безопасность NIS

NIS (Network Information Service) – сетевой информационный сервис. Это RPC сервис, называемый ypserv, который использовался совместно с portmap и другими родственными сервисами, передающими карты имен пользователей, пароли и другую важную информацию любому компьютеру, претендующему быть включенным в этот домен.

NIS охватывает несколько приложений, таких как:

- /usr/sbin/rpc.yppasswdd – также называемый yppasswdd сервисом, этот демон предоставляет пользователям возможность изменения их NIS паролей.
- /usr/sbin/rpc.ypxfrd – также называемый ypxfrd сервис, этот демон ответственный за передачу NIS карты через сеть.
- /usr/sbin/yppush – это приложение изменяет базу данных NIS при увеличении NIS серверов.
- /usr/sbin/ypserv – это демон NIS сервера.

NIS на сегодняшний день является не совсем безопасным стандартом. Он не имеет механизмов аутентификации хостов и передает всю информацию в простом виде, включая хэши паролей. Поэтому крайне внимательно должна быть построена сеть, которая использует NIS. Далее ситуация осложняется тем, что по умолчанию конфигурация NIS небезопасна. Рекомендуется при любом планировании использования NIS сервера, в первую очередь для того, чтобы обезопасить сервис portmap, а затем выполнить следующие рекомендации.

9.4.1. Внимательное планирование сети

Так как NIS передает незашифрованную информацию через сеть, то очень важно, чтобы сервис был запущен позади файервола (firewall) и включен в безопасные сегменты сети. В любое время информация, переданная NIS через небезопасную сеть, имеет риск быть перехваченной. Внимательное проектирование сети, касающееся этих вопросов, может помочь в предотвращении грубых нарушений безопасности.

9.4.2. Использование сложного имени NIS домена и имени хоста

Любая машина из NIS домена может выполнять команду для получения информации из сервера без процедуры аутентификации так долго, сколько пользователь будет знать NIS серверы, имя хоста DNS и имя домена NIS.

Например, если кто-либо подключит переносной компьютер в сеть или взломает сеть с внешней стороны (и имеет возможность подмены IP-адреса внутренней сети), то приведенная ниже команда позволит выдать карту /etc/passwd

ypcat -d <*NIS_domain*> -h <*DNS_hostname*> passwd

Если атакующий имеет права администратора (root), он может получить файл /etc/shadow, выполнив следующую команду:

ypcat -d <*NIS_domain*> -h <*DNS_hostname*> shadow

Замечание: Если используется Kerberos, то файл /etc/shadow не хранится внутри карты NIS.

Сделайте доступ к картам NIS более трудным для атакующего. Создайте случайным образом строчку для хостового имени DNS, например такую как o7hfawtgmhwg.domain.com. Похожим образом, создайте другое случайное имя домена NIS. Это сделает намного более сложным для атакующего доступ к NIS серверу.

9.4.3. Редактирование файла /var/yp/securenets

NIS прослушивает все сети, если файл /var/yp/securenets не существует, как происходит в случае при инсталляции по умолчанию или если он пустой. Первое, что необходимо сделать, это прописать в файл пары netmask/network, для того чтобы ypserv отвечал на запросы, приходящие только из собственной сети.

Внимание: Никогда не запускайте NIS сервер без создания файла /var/yp/securenets. Ниже приведен пример, взятый из файла /var/yp/securenets:
255.255.255.0 192.168.0.0

Эти действия не предлагают защиту от атак, направленных на подмену IP-адресов, но они ограничивают сети, которые будет обслуживать NIS сервер.

9.4.4. Назначение и использование статических портов

Всем серверам, имеющим отношение к NIS, могут быть назначены специфические порты, кроме rpc.yppasswdd – демона, который предоставляет пользователям возможность изменения их паролей. Назначение портов к двум другим демонам NIS сервера, rpc.ypxfrd и ypserv предлагает вам создать правила, применяемые в файерволе (firewall) для дальнейшей защиты демонов сервера NIS от вторжения.

Для этого необходимо сделать следующее, добавьте в файл /etc/sysconfig/network такие строки:
YPSERV_ARGS="-p 834"
YPXFRD_ARGS="-p 835"

Литература
(с краткой аннотацией)

1. Брагг Р. Система безопасности Windows 2000.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001.

   Пособие для профессионалов, в котором излагаются основы стратегии безопасности для систем, работающих под управлением Windows 2000. Позволяет читателю понять основные концепции безопасности, освоить методы управления доступом к Windows с помощью инструментов безопасности, настроить систему защиты удаленного доступа, установить или обновить операционную систему с учетом требований безопасности.

2. Гайкович В., Лершин А. Безопасность электронных банковских систем. – М.,1993.

   Компьютерные системы – одна из наиболее уязвимых сторон современных банков и финансовых организаций, притягивающих злоумышленников. Они нуждаются в защите. Как защищать свои системы? От кого? Сколько это будет стоить? Как вести себя в критических ситуациях.

3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2 кн. Кн. 1. – М.: Энергоатомиздат, 1994.

   В книге с позиций системно-концептуального подхода рассмотрен широкий круг вопросов, относящихся к защите информации, накапливаемой, хранимой и обрабатываемой в современных автоматизированных системах и сетях.

4. Герасименко В.А., Малюк А.А. Основы защиты информации. – М., 1997.

   Рекомендовано Министерством общего и профессионального образования РФ в качестве учебника для вузов.

5. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. Серия «Информатизация России на пороге XXI века». – М.: СИНТЕГ, 1999.

   Впервые в отечественной литературе рассматривается концепция информационной войны. Показан размах, который приобрела эта концепция на Западе, в частности, приводятся взгляды Министерства обороны США на проблему ведения информационной войны. Анализируются средства и методы ведения информационной войны, возможные объекты атаки и средства их защиты.

6. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему / Под науч. ред. Д.П. Зегжды, В.В. Платонова. – СПб.: Мир и семья-95, 1997.

   Это первое отечественное издание, посвященное уникальной технологии создания защищенных систем обработки информации, где рассмотрены проблемы практической реализации моделей безопасности. В книге дается представление о защищенной информационной системе, анализируется существующий опыт разработки подобных систем и причины нарушения их безопасности, что позволяет предложить качественно новые методы и средства их защиты.

7. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб.: БХВ-Петербург, 2001.

   Рассматриваются технологические основы защиты информационного взаимодействия в компьютерных сетях при их подключении к открытым коммуникациям, методы и средства межсетевого экранирования для зашиты локальных сетей от несанкционированных воздействий со стороны открытых коммуникаций, базовые протоколы и средства построения защищенных виртуальных сетей на различных уровнях эталонной модели сетевого взаимодействия.

8. Зубанов Ф. Windows NT – выбор «профи». 2-е изд., испр. и доп. – М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd.», 1997.

   Основное внимание в книге уделяется вопросам планирования, установки, защиты и администрирования, обеспечивающих безотказную работу вычислительной системы. В частности, рассматриваются доменная структура сетей Microsoft, учетные записи пользователей и групп, управление политикой ведения учетных записей, вопросы отказоустойчивой работы с дисками, кластерные технологии, файловые системы, безопасная работа в глобальных сетях и при подключении к Internet. Кроме того, описываются особенности новой, 4 версии Windows NT.

9. Каплан А., Нильсен М.Ш. Windows 2000 изнутри: Пер. с англ. – М.: ДМК, 2000.

Большую часть книги занимает критический обзор архитектуры Windows 2000 в сравнении с Windows NT 4.0 и другими сетевыми ОС, например UNIX и NetWare, а также Windows 95/98. Подробно описываются достоинства и недостатки нового пользовательского интерфейса, средств администрирования на основе MMC, службы каталогов Active Directory, технологии кластеризации. Много внимания уделяется реализации сетевого протокола TCP/IP, который полностью заменил устаревший NetBIOS, а также файловой системе NTFS 5.

10. Кастер Х. Основы Windows NT и NTFS: / Пер. с англ. – М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd.», 1996.

Взгляд изнутри на проект, философию, архитектуру и будущее операционной системы Microsoft Windows NT.

11. Компьютерная преступность и информационная безопасность / Под общ. ред. А.П. Леонова. – Мн.: АРИЛ, 2000. – 552 с.

В рамках междисциплинарного подхода к исследованию проблемы информационной безопасности рассмотрены актуальные вопросы обеспечения гарантированной защиты информации в компьютерных системах и сетях.

12. Леонов А.П., Леонов К.А., Фролов Г.В. Безопасность автоматизированных банковских и офисных систем. – Мн.: НКП Беларуси, 1996.

Монография посвящена проблеме комплексной защиты информационной безопасности автоматизированных банковских и офисных систем. Рассматриваются системная методология защиты информационной безопасности, эволюция аппаратно-программных платформ автоматизации банков и офисов, методы и средства комплексной зашиты информации в автоматизированных банковских и офисных системах.

13. Люцарев В.С., Ермаков К.В., Рудный Е.Б., Ермаков И.В. Безопасность компьютерных сетей на основе Windows NT. – М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd.», 1998.

В книге изложен взгляд независимых специалистов на проблемы функционирования и защиты компонентов операционной системы Microsoft Windows NT.

14. Петренко С.А., Петренко А.А. Аудит безопасности Intranet. – М.: ДМК Пресс, 2002. – 416 с.

В книге содержится комплексное описание всех основных вопросов аудита безопасности корпоративных систем Internet/Intranet в соответствии с требованиями международных стандартов ISO 15408, ISO 17799 (BS7799), BSI и COBIT.

15. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов / В.Г. Проскурин, С.В. Крутов, И.В. Мацкевич – М.: Радио и связь, 2000. – 168 с.

Рассматривается общая концепция защиты информации в операционных системах, аппаратное и программное обеспечение защитных функций ОС.

16. Штребе М., Перкинс Ч., Монкур М. Безопасность сетей NT4: Пер. с англ. В 2 т. Т. 1. – М.: Мир, 1999.

В томе 1 рассмотрены концепция и модель безопасности сети, вопросы системной политики, а также защита от персонала, шифрование, удаленный доступ.

17. Штребе М., Перкинс Ч., Монкур М. Безопасность сетей NT4: Пер. с англ. В 2 т. Т. 2. – М.: Мир, 1999.

В томе 2 подробно рассмотрены вопросы защиты компонентов сети, а также использование брандмауэров, серверов полномочий и пакетной фильтрации. В конце книги описана система безопасности Windows NT5 и приведен обширный толковый словарь терминов по компьютерной безопасности.

18. Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издатель Молгачева С.В., 2001.

Книга посвящена рассмотрению широкого круга проблем компьютерной безопасности. Наряду с теоретическим и нормативно-методическим материалом содержит описание практических подходов к реализации систем безопасности.

Св. план 2004, поз. 32

Учебное издание

Иванченко Юрий Иванович,
Деев Алексей Юрьевич,
Заговалко Алексей Владимирович

ИНТЕЛЛЕКТУАЛЬНЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

Учебное пособие
для студентов специальности «Искусственный интеллект»
специализации «Интеллектуальные компьютерные технологии
защиты информации»

В 3-х частях

Часть 2
Защита информации на уровне операционной системы

Редактор Е.Н. Батурчик
Компьютерная верстка: А.Ю. Деев, А.В. Заговалко

Подписано в печать
Гарнитура «Таймс».
Уч.-изд. л.

Формат 60х84 1/8.
Печать ризографическая.
Тираж 100 экз.

Бумага офсетная.
Усл. печ. л.
Заказ

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
Лицензия на осуществление издательской деятельности №02330/0056964 от 01.04.2004.
Лицензия на осуществление полиграфической деятельности №02330/0133108 от 30.04.2004.
220013, Минск, П. Бровки, 6