Министерство образования РФ

**НГТУ**



Курсовой проект по «Администрированию сетей»

на тему: «Безопасность файловых ресурсов сети

Windows 2000»

Факультет: АВТ

Группа: АС-812

Студент: Баторова С.М**.**

Преподаватель: Шахмаметов Р.Г.

Новосибирск

2002

# СОДЕРЖАНИЕ

ВВЕДЕНИЕ…………………………………………………………….3

1. ФАЙЛОВАЯ СИСТЕМА………………………………………….4

1.1.Система FAT…………………………………………………….4

1.2.Система FAT32………………………………………………….5

1.3. Система NTFS…………………………………………………..5

1. ЗАЩИТА ФАЙЛОВ………………………………………………..9

2.1. Разрешения для файлов………………………………………10

2.2. Устранение конфликта с разрешениями……………………13

1. ЗАЩИТА ПАПОК………………………………………………...14

3.1. Изменение разрешений для файлов и папок………………..15

1. ПРИСВОЕНИЕ ФАЙЛА ИЛИ ПАПКИ…………………………17
2. НАСТРОЙКА БЕЗОПАСНОСТИ ДЛЯ НОВЫХ ФАЙЛОВ

И ПАПОК………………………………………………………….18

1. ИСПОЛЬЗОВАНИЕ ШИФРОВАНИЯ ФАЙЛОВ………………19
2. УСТАНОВЛЕНИЕ ДИСКОВЫХ КВОТ………………………...20

7.1. Управление дисковыми квотами…………………………….21

7.2. Создание новой записи квот…………………………………22

7.3. Удаление записи квоты………………………………………22

ЗАКЛЮЧЕНИЕ………………………………………………………23

ЛИТЕРАТУРА………………………………………………………..24

# ВВЕДЕНИЕ

При создании системы безопасности новой ОС Windows 2000 разработчики фирмы Microsoft постарались учесть как существующий опыт использования системы безопасности Windows NT 4.0, так и реализовать новые наборы механизмов и протоколов безопасной работы с информацией. Windows NT 4.0 выбрана не случайно: она позиционируется как ОС для предприятий, обладает встроенными возможностями разграничения доступа к ресурсам и за 6 лет экс-плуатации хорошо зарекомендовала свои существующие и потенциальные возможности безопасности. Но если заглянуть в Windows 2000, то, очевидно, что, несмотря на большое количество механизмов безопасности, внесенных в новую ОС из Windows NT 4.0, все они претерпели существенные изменения в сторону увеличения удобства, надежности и функциональности.

Система Windows 2000 компании Microsoft обеспечивает возможность безопасного доступа к ресурсам системы. Если для вас, самым важным ресурсом, подлежащим защите, являются файлы, можно настроить систему так, чтобы иметь возможность контролировать то, как другие пользователи читают, записывают, создают и изменяют файлы и папки на вашем компьютере.

Это возможно только при использовании системы NTFS. Система была создана для Windows NT, предшественника Windows 2000, и является одной из трех систем, которые можно использовать на жестком диске компьютера.

# 1. Файловая система

Файловая система – это структура, в которую организованы файлы, где они проименованы и сохранены на жестком диске. В Windows 2000 применяется иерархическая файловая система. На каждом диске создается так называемый корневой каталог, который может включать в себя файлы и другие каталоги (подкаталоги). Таким образом, создается связанная древовидная иерархия файлов и каталогов.[1]

Все файловые системы, поддерживаемые Windows 2000, являются иерархическими, хотя существенно отличаются между собой способами записи файлов на носителях информации. Windows 2000 поддерживает следующие файловые системы:

▪ **FAT:** применяется в MS-DOS.

▪ **FAT32:** применяется вWindows 95/98.

▪ **NTFS:** применяется в Windows 2000.

Используя любую файловую систему, можно использовать разрешения для доступа к общим папкам, чтобы их контролировать. Можно указать, какие пользователи могут читать, записывать, создавать или изменять файлы и папки внутри папок, предоставленных в общее пользование.[2]

* 1. **Система FAT**

Эта файловая система разработана вместе с операционной системой MS-DOS в начале 80-х годов. Первоначально эта файловая система предназначалась для работы с дискетами. После появления на персональных компьютерах накопителей на жестких магнитных дисках большой емкости она начала использоваться и для них.

Особенности FAT:

▪ Длина имени файла – не более 8 символов, расширение имени - не более 3 символов.

▪ Имя файла и расширение разделяются точкой.

▪ Нельзя использовать в имени файла некоторые специальные символы и пробел.

▪ FAT (File Allocation Table – таблица размещения файлов) содержит информацию о расположении данных на носителе.

▪ Относительно медленный доступ к информации из-за разделения места хранения сведений о файлах (FAT) и самих файлов.

▪ В процессе записи и удаления информации на дисках происходит дробление свободной области хранения данных на небольшие участки (фрагментация).

**1.2 Система FAT32**

Файловая система FAT32 разработана для эффективного использования устройств хранения информации большой емкости (от 512Мб до 2 Тб). Эта система используется в Windows 95/98 и Windows 2000. Технические недостатки файловой системы FAT MS-DOS в системе FAT32 в значителльной степени были устранены.

Особенности FAT32:

▪ Поддерживается только на жестких магнитных дисках.

▪ Имена файлов вместе с расширением могут иметь длину до 215 символов.

▪ В имени файла допускается использование пробелов.

▪ В имени файла не разрешено использование лишь некоторых специальных символов.

▪ Эффективность использования дискового пространства на накопителях больших размеров на 10%…15% выше, чем при использовании FAT и особенно ярко проявляется при хранении большого числа файлов мелкого размера.

▪ Надежность хранения данных повышена за счет возможности свободного размещения корневого каталога и использования резервной копии таблицы размещения файлов.

▪ Предусмотрена возможность динамического изменения размера разделов на накопителе.[2]

**1.3 Система NTFS**

Обозначение файловой системы NTFS представляет собой аббревиатуру от New Technology File System (файловая система операционной системы NT).

NTFS представляет собой новую файловую систему, используемую в операционной системе Windows 2000. Ограничения, которые имелись в FAT32, в NTFS были в значительной степени устранены.

Для томов NTFS система Windows 2000 предлагает дополнительные параметры защиты. Кроме контроля за папками, предоставленными в общее пользование, можно следить за безопасностью файлов и папок локальных пользователей (тех, что входят в систему с вашей рабочей станции). Можно налагать ограничения на любые папки и файлы; в томах FAT можно выдавать разрешения только на уровне папки (и только для пользователей, что вошли через сеть).

У файловой системы NTFS имеется и ряд других преимуществ:

▪ Поддерживается только на жестких дисках.

▪ Система NTFS более экономно размещает информацию на очень больших жестких дисках (поддерживает 64-разрядную адресацию данных).

▪ При записи имен файлов используется уникальный код (Unicod). Такая кодировка символов пришла на смену кодировке ANSI. В Unicode используется 16-разрядное представление символов. Поэтому в таблице кодирования может содержаться до 65536 символов.

▪ Система обеспечивает лучшее восстановление информации в случае проблем с жестким диском.

▪ Поддерживает сжатие файлов. (Программы для компрессии, написанные на базе MS-DOS (DriveSpase, Doublespase, Stacker) не работают в системе Windows 2000.)

▪ Система поддерживает дисковые квоты – ограничение дискового пространства, которые можно установить для каждого пользователя.

▪ Система NTFS поддерживает шифрование файлов для повышения безопасности.

Недостатком файловой системы NTFS является невозможность для других систем (Windows 9x, Linux, MS-DOS и OS/2) читать тома NTFS. Если используется система, отличная от Windows 2000, прочесть информацию из томов NTFS будет невозможно.[1]

**Примечания:**

1. Учитывая, что файловые системы FAT32 и NTFS не поддерживаются на гибких дисках, при передаче данных лучше всего использовать сеть, так как при этом файлы сохраняют длинные имена.
2. При задании имен файлов и каталогов в файлофой системе NTFS допускается:

▪ Длина имен до 215 символов (включая расширение имени).

▪ Использование больших и малых букв, т. е. прописное и строчное написание символов различается.

▪ Использование всех символов, за исключением ? “ / \ < > \* | : .

▪ Для систем, использующих MS-DOS, при задании NTFS-имени файла автоматически создается MS-DOS-имя файла.

При этом выполняются следующие действия:

* Символы пробела исключаются.
* Спецсимволы исключаются. Windows 2000 интерпретирует последний специальный символ имени как разделитель между именем файла и его расширением.
* Символы, не поддерживаемые в MS-DOS, преобразуются в символ подчеркивания “\_”.
* Имя файла сокращается до 6 символов, за которыми следует символ ~ (тильда) и одна цифра.
* Расширение имени сокращается до трех символов.

1. В качестве имен файлов или каталогов запрещено использование имен, зарезервированных операционной системой:

AUX, COM1…COM4, LPT1…LPT4, NUL, PRN.

1. Функции защиты данных от несанкционированного доступа со всеми их возможностями могут использоваться при установке файловой системы NTFS.[2]

Файловая система NTFS 5.0. Эта версия файловой системы является объектно-ориентированным хранилищем данных, представляемых в виде привычных для пользователя объектов — файлов и каталогов. В NTFS 5.0 теперь можно хранить потенциально любую информацию и в любых форматах представления. Реализуются эти возможности за счет появления в файловой системе нового механизма Reparse points (повторный грамматический анализ). Reparse points  — это объекты, которые могут быть связаны с файлами или каталогами, и описывают правила хранения и обработки информации, хранящейся в нестандартном для файловой системы виде. С использованием этого механизма в NTFS уже реализованы механизмы шифрации данных и механизмы монтирования томов (представление любого тома в виде каталога на другом диске — возможность создания виртуальной файловой системы, состоящей только из файлов и каталогов на любой рабочей станции или сервере). А разработчики получили мощный инструмент для создания приложений, способных хранить данные в своем уникальном формате (включая и собственные алгоритмы шифрации) для обеспечения необходимого уровня производительности и безопасности работы с данными.

Рассмотрим принципы работы механизма Reparse points. Любое приложение, работающее с файловой системой, при обращении к дискам отображает информацию в виде привычных файлов и каталогов, хранящихся в NTFS. При попытке открытия выбранного пользователем файла (или каталога), запрос на чтение данных передается приложением ядру ОС. Ядро, анализируя свойства выбранного файла и обнаруживая связанный с ним объект Reparse points, анализирует хранящуюся в этом объекте информацию (в этом и состоит суть названия механизма — повторный грамматический анализ). Объект Reparse points, по сути, содержит ссылку на специальный драйвер, создаваемый любым разработчиком. Этот драйвер и определяет реальный формат хранения данных на томах NTFS. При попытке открытия файла управление передается созданному разработчиком модулю, который и считывает данные с диска в известном ему формате. Поэтому с появлением этого нового механизма любой разработчик имеет возможность обеспечить безопасность и удобство хранения данных для своего специфического приложения. [5]

Еще одним новшеством файловой системы NTFS 5.0 стали обновленные механизмы разграничения прав доступа и появившиеся средства квотирования дискового пространства. Отныне система прав доступа обладает встроенными механизмами наследования, позволяющими с большой степенью удобства выполнять разграничение полномочий в файловых системах с большим количеством уровней вложенности каталогов. Из приятных нововведений также можно назвать появившийся инструментарий (в отличие от Windows NT 4.0 он поставляется в составе Windows 2000), позволяющий описывать маски наследуемых прав для любых комбинаций каталогов, файлов и целых ветвей файловой системы. Сами права доступа стали обладать существенно большей гибкостью, не создающей путаницу из-за обилия вариантов разграничения прав.

Интерфейсы прикладного программирования (API) сетевой аутентификации Windows, являющиеся частью SSPI (Security Support Provider Interface). Приложения и службы Windows 2000 используют SSPI для изоляции протоколов прикладного уровня от деталей протоколов сетевой безопасности. Windows 2000 поддерживает интерфейс SSPI в целях сокращения кода уровня приложений, необходимого для работы с многочисленными протоколами аутентификации. Интерфейс SSPI представляет уровень, поддерживающий различные механизмы аутентификации и шифрации, использующие протоколы с симметричными или асимметричными ключами.

SSPI — это инструмент, с помощью которого реализована вся внутренняя система безопасности Windows 2000 и ее сервисов. SSPI обеспечивает существование 3 основных механизмов сетевой безопасности: аутентификацию, гарантию целостности и конфиденциальность. Под аутентификацией понимается возможность проверки того, что полученные вами данные пришли действительно от того, чей адрес стоит в поле отправителя. Гарантия целостности подразумевает наличие набора средств, позволяющих проверить получение тех данных, которые были посланы вам. Соблюдение конфиденциальности требует, чтобы сообщение было получено и прочитано только тем пользователем, кому оно адресовано.

С использованием SSPI разработчики получают возможность создания приложений со встроенными средствами сетевой безопасности и соблюдением открытых стандартов. Это позволяет гарантировать безопасный обмен данными с любыми организациями — партнерами, заказами, поставщиками по общедоступным каналам связи, например, Интернет.[4]

В Windows 2000 каждый пользователь должен зарегистрироваться в системе перед началом работы. Это необходимо как на локальной рабочей станции без подключения к сети, так и на станции в компьютерной сети. Внутри системы каждый пользовательл имеет свой ID (идентификатор или уникальное имяпользователя, состоящее из имени и пароля). Каждый пользователь также может войти в систему в качестве гостя (Guest). В этом случае ему предоставляется возможность обращения к файлам других компьютеров сети, которрые разрешены для совместного использования, но не к файлам, расположенным на NT-сервере.

Каждый пользователь должен зарегистрироваться в системе индивидуально. Это позволяет организовать защиту файлов таким образом, что некоторые каталоги или диски для одних пользователей могут быть закрыты, а для других – открыты. Это относится к предоставлению всех прав доступа.

Пользователю, обладающему правами админитсратора, доступны все ресурсы, имеющиеся в данной системе. И если он однажды забудет свой пароль, то это приведет к необходимости форматирования диска и переустановки операционной системы. Следует, однако, отметить, что полный ассортимент средств защиты доступен лишь тогда, когда установлена файловая система NTFS.

Без проблем можно подключить несколько рабочих станций Windows 2000 к Peer-to-peer-сети (одноранговая сеть). Для этого нужно вставить в компьютер сетевую плату и с помощью Панели управления настроить параметры кабельного соединения. Необходимо также запустить Сервер обслуживания. В такой сети тоже можно предоставить отдельным пользователям праава доступа к ресурсам со всеми или ограниченными возможностями, а также организовать коллективное использование принтера. В одноранговую сеть могут объединяться компьютеры с другими операционными системамми, такими как Windows for Workgroups, Windows 95/98 и Novell-клиент.

Сеть может обладать дополнительной возможностью обеспечения лоступа посредством RAS (Remote Acces Service-служба удаленного доступа). С помощью RAS из Windows 2000-компьютера можно обращаться к сети через модем по телефону и работать в ней как обычный клиент.[2]

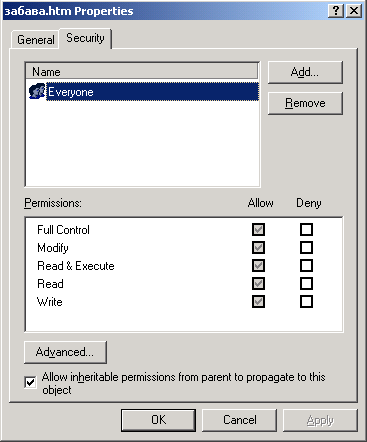
**2. Защита файлов**

Файловая система FAT для каждого файла в томе сохраняет имя файла, его размер, дату последнего изменения и собственно информацию. Система NTFS , кроме перечисленного, также выдает список контроля доступа (access control list, ACL), который определяет степень доступа к файлам и папкам системы, имеющуюся у пользователя. Каждый файл и папка в томе NTFS имеют свой ACL.

Защитой файлов в томе NTFS можно управлять с помощью вкладки Security (Безопасность) в диалоговом окне свойств файла:

1. Щелкнуть правой кнопкой мыши на файле в Проводнике.
2. Выбрать во всплывающем меню пункт Properties (Свойства).
3. Щелкнуть на вкладке Security (Безопасность), чтобы открыть диалоговое окно, изображенное на рис.1.

Если выделенный файл не хранится в томе NTFS, вкладка Security(Безопасность) не появится, поскольку защита файла возможна только в томе NTFS.



**Рис.1.** На вкладке Безопасность отображены пользователи, имеющие разрешения на доступ к файлу

Диалоговое окно используется для просмотра и изменения степени доступа пользователя к файлу. При выделении имени в поле Name (Имя) в поле Permissions (Разрешения) в нижней части диалогового окна отображается степень доступа данного пользователя или группы к данному файлу. Затененные флажки определяют наличие разрешения «по наследству». Это значит, что разрешение было предоставлено родительским объектом. Например, родительский объект для файла – папка, в которой он содержится. Затененный флажок дает знать, что разрешение дано по умолчанию, поскольку файл создан в папке, у которой помечен соответствующий флажок.[1]

## 2.1 Разрешения для файлов

Поле Permissions (Разрешения) включает список основных разрешений, и использовать их можно в различных сочетаниях, чтобы они подходили именно вам. По сути, каждое разрешение из списка представляет собой установленный набор разрешений. В табл. 1 показано, что именно включено в то или иное разрешение из списка в поле Permissions (Разрешения).

*Таблица 1.*

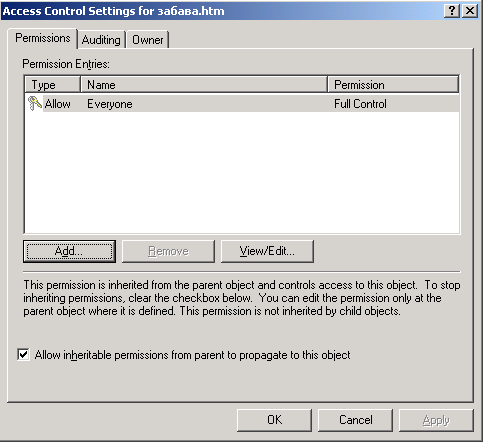
##### Основные разрешения для файла

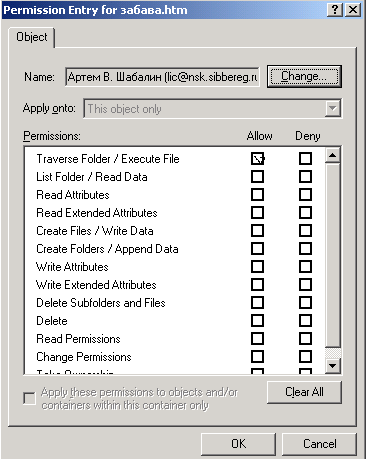
|  |  |  |
| --- | --- | --- |
| **Разрешение** | Описание | Индивидуальные разрешения |
| Read (Чтение) | Позволяет пользовате-  лю просматривать  информацию файла | - List Folder/Read Data (Содержание папки/  Чтение данных)  - Read Attributes (Чтение атрибутов)  - Read Extended Attributes (Чтение дополни-  тельных атрибутов)  - Read Permissions (Чтение разрешений )  - Synchronize (Синхронизация) |
| Read & Execute  ( Чтение  и выполнение) | Позволяет запускать  Программы | - Все разрешения, перечисленные выше  - Traverse Folder/Execute Files (Обзор папок  Выполнение файлов) |
| Write (Запись),  Содержимое  Файла | Позволяет изменять  Файлы | - Creates Files/Write Data (Создание файлов/  Запись данных)  - Creates Folders/Append Data (Создание па-  пок/Дозапись данных)  - Write Attributes (Запись атрибутов)  - Write Extended Attributes (Запись дополни-  тельных атрибутов)  - Read Permissions (Чтение разрешений)  - Synchronize (Синхронизация) |
| Modify  (Изменить) | Позволяет читать,  изменять и удалять  файл | - Все перечисленные выше разрешения  - Delete (Удаление) |
| Full Control  ( Полный  доступ) | Позволяет осущест-  влять полный контроль над файлом | - Все перечисленные выше разрешения  - Delete Subfolders and Files ( Удаление  подпапок и файлов)  - Change Permissions ( Смена разрешений)  - Take Ownership (Смена владельца) |

В некоторых случаях установленный набор разрешений не обеспечивает контроль над доступом пользователей или групп к файлу. В таких ситуациях следует присваивать разрешения в индивидуальном порядке. Для этого необходимо выполнить следующие действия:

1. На вкладке Security (Безопасность) в диалоговом окне свойств файла щелкнуть на кнопке Advansed (Дополнительно).
2. На вкладке Permissions (Разрешения) появившегося диалогового окна Access Control Settings (Параметры управления доступом) выделить нужную группу или пользователя и щелкнуть на кнопке View/Edit (Показать).

Как показано на рис.2, появляется список разрешений, похожий на список со

вкладки Security (Безопасность) из диалогового окна свойств, но в этом списке можно устанавливать индивидуальные разрешения.[3]



**Рис.2.** Щелчок на вкладке Дополнительно и далее на кнопке Показать приводит в диалоговое окно, где можно выбрать комбинацию разрешений

* 1. Как устранить конфликт с разрешениями

Использование групп позволяет легко разрешать или запрещать доступ к файлам и папкам сразу многим пользователям. Однако добавление или удаление разрешения для группы часто создает проблемы. Одна из проблем – дать разрешение группе, тогда как некоторым ее участникам доступ должен быть запрещен.

При изменении степеней защиты следует помнить, что разрешения накапливаются. Следует просматривать список членов группы, чтобы быть уверенным, что разрешение получат только те, кому следует.

**Использование групп для настройки разрешений.** Поскольку разрешения накапливаются, следует проявлять осторожность при осуществлении защиты. Проще дать разрешение группе в целом, а не присваивать его в индивидуальном порядке каждому члену группы. Следует однажды дать разрешение группе, а затем добавлять или исключать пользователей из списка. Допустим, что группа Бухгалтерский отдел имеет степень доступа к файлам со счетами Modify (Изменить). Мария Ивановна работает в бухгалтерии и соответственно имеет разрешение на изменение файлов со счетами. Существует также группа пользователей Контролеры бухгалтерского отдела, у которой имеется разрешение на полный доступ. Если Марию Ивановну повысят, и она станет контролером, ее будет необходимо переместить из группы с разрешением изменять файлы в группу полного контроля. Если прямо изменить ее степень доступа, она не сможет автоматически получить все нужные ей разрешения. Более того, менять разрешения для отдельных пользователей в большой организации – занятие весьма трудоемкое.

Например, Юрий Петрович является членом группы Кадры и имеет разрешение Read (Чтение) для файла Январь.xls в папке Платежные ведомости. Если группе будет дано разрешение Write (Запись), Юрий Петрович получит его как член группы, а поскольку разрешения накапливаются, то разрешение читать файл также останется, и он сможет пользоваться двумя степенями доступа.

Запрещение определенного разрешения превосходит *все* выданные разрешения. Например, если группа Кадры имеет флажок в столбце Deny (Запретить) для каждого разрешения, Юрию Петровичу будет запрещен доступ к файлу даже в том случае, если для его учетной записи разрешен полный контроль.

Прежде чем использовать запрещение, следует понять, кого именно оно затронет. Например, у вас имеется секретный файл, который вы хотите предоставить своей группе с разрешением полного доступа, однако для повышения безопасности устанавливаете флажки Deny (Запретить) группы Everyone (Все). Поскольку ваша учетная запись входит в группу Everyone (Все), получается, что вы лишаете себя самого доступа к файлу. Теперь использовать файл не сможет даже его владелец (тот, кто его создал), однако он сможет изменить настройки.[1]

1. **Защита папок**

Установление разрешений для папок похоже на установление разрешений для доступа к файлам, однако существуют и отличия.

Одно из них состоит в том, что вкладка Security (Безопасность) в диалоговом окне свойств папки включает дополнительное разрешение List Folder Content (Список содержимого папки). В это разрешение включены те же пункты, что и в разрешение Read & Execute (Чтение и выполнение). Разница между этими разрешениями состоит в способе наследования. Разрешение List Folder Content (Список содержимого папки) наследуется папками, но не файлами, тогда как разрешение Read & Execute (Чтение и выполнение) наследуется и папками, и файлами. Наследование является наиболее значимой разницей между разрешениями для файлов и для папок.

Если оставлен установленный по умолчанию флажок Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект) со вкладки Security (Безопасность) в диалоговом окне файла или папки, разрешение передается от родительского объекта (папки, содержащей данную папку или файл) «по наследству». Если сам родительский объект имеет такую пометку, разрешение передается от его родительского объекта и т. д. У объекта может быть огромная коллекция наследованных и явно указанных разрешений (тех, у которых разрешения были изменены или добавлены). Наследованные разрешения обозначены в затененных полях столбцов Allow (Разрешить) и Deny (Запретить), остальные разрешения помещены в обычных полях.[4]

**Однако, каждый пользователь** или член группы, имеющий разрешение на полный контроль папки, может удалять любые файлы из этой папки независимо от разрешений для этих файлов.

Преимущество такой настройки состоит в том, что она позволяет изменять разрешения для одной папки и распространять их на все ее дочерние объекты, не изменяя разрешения в индивидуальном порядке. При изменении степени доступа пользователя к папке меняется и разрешение к файлам этой папки.

Изменить или перекрыть наследуемые разрешения можно следующими способами:

►Проведение изменений для родительского объекта данного объекта изменяет наследуемые разрешения данного объекта.

►Выбор противоположной настройки (Allow (Разрешить) или Deny(Запретить)) перекрывает разрешение, переданное по наследству.

► При снятии флажка Allow Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект) появляется диалоговое окно «Безопасность».

Дальше имеется три пути:

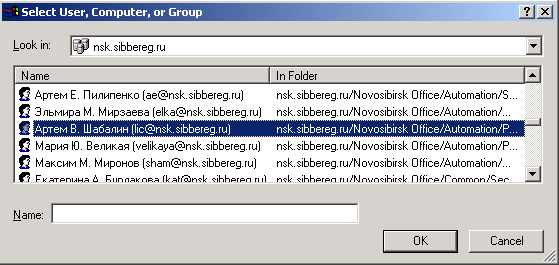
* Щелчок на кнопке Copy (Копировать) позволяет копировать все унаследованные разрешения объекта, что превращает их в собственные разрешения. Разрешение остается, но оно не изменяется при изменении разрешения родительского объекта.
* Щелчок на кнопке Remove (Удалить) удаляет все унаследованные разрешения, остаются только установленные явно указанные разрешения.
* Щелчок на кнопке Cancel (Отмена) закрывает диалоговое окно без всяких изменений.
  1. **Изменение разрешений для файлов или папок**

Несмотря на то, что гораздо удобнее давать разрешения пользователям, добавляя их к группе, у которой имеется определенная степень доступа, иногда некоторые пользователи нуждаются в особых разрешениях, которых нет ни у одной группы. В таких случаях следует вручную присваивать разрешение. Во всех остальных ситуациях следует обновлять разрешения всей группы.

Прежде чем изменять степень доступа всей группы, следует уточнить, кто именно в нее входит.

Для присвоения разрешения для файла или папки необходимо выполнить следующее:

1. Щелкнуть правой кнопкой мыши на папке или файле в Проводнике и выбрать пункт Properties (Свойства).
2. Щелкнуть на вкладке Security(Безопасность).
3. Если следует присвоить разрешение пользователю или группе, которые отсутствуют в списке Name (Имя), следует щелкнуть на кнопке Add (Добавить), чтобы появилось диалоговое окно Select Users, Computers, Or Groups (Выбор: Пользователи, Компьютеры или группы). Затем выделить нужного пользователя или группу, щелкнуть на кнопках Add (Добавить) и ОК(см.рис.3).
4. Для удаления пользователя или группы следует выделить их в списке Name (Имя) и щелкнуть на кнопке Remove (Удалить). В этом случае у пользователя или группы не останется разрешения на объект, если только пользователь или группа не являются участниками другой группы, которая остается в списке. Такие пользователи сохранят доступ к файлу или папке. (если следует запретить доступ, лучше не удалять пользователей из списка, а изменить разрешение на запрещение).



**Рис.3**

1. Выделить имя каждого пользователя в списке Name (Имя) и щелкнуть на Allow (Разрешить) или Deny (Запретить), чтобы вызвать соответствующее действие.

Если пользователю или группе необходимо присвоить особый набор разрешений, следует щелкнуть на вкладке Advanced (Дополнительно), чтобы открыть диалоговое окно «Элемент разрешения», а затем щелкнуть на кнопке View/Edit (Показать), чтобы указать индивидуальные настройки.

Если перед тем, как щелкнуть правой кнопкой мыши и выбрать пункт Properties (Свойства), вы выделили несколько папок или файлов, изменения повлияют на все выделенные объекты. Если существующие разрешения не одинаковы для всех выделенных объектов, появится соответствующее сообщение. Если щелкнуть на кнопке Yes (Да) в этом сообщении, система изменит разрешения для всех выделенных объектов на наследованные и удалит все явно указанные разрешения сделанные до того.

Именно здесь можно извлечь пользу из разрешений, полученных по наследству. Чтобы изменить разрешения для папки и всех папок и файлов, которые она содержит, необходимо выполнить следующие действия:

1. Вывести на экран вкладку Security (Безопасность) для папки и установить разрешения для всех пользователей, как было описано выше. Не следует щелкать на кнопке OK , чтобы не закрыть окно.
2. Щелкнуть на кнопке Advanced (Дополнительно).
3. На вкладке Permissions (Разрешения) в диалоговом окне Access Control Settings Reset Permissions On All Child Objects And Enable Propagation Of Inheritable Permissions (Установить разрешения для всех дочерних объектов и разрешить их наследование) и щелкнуть на кнопке ОК.

После получения вашего подтверждения настройки в окне сообщения, система проследит все файлы в папке, все подпапки и все файлы во всех подпапках. Для всех этих объектов будут удалены указанные выше разрешения и присвоены “наследуемые” разрешения. Таким образом, у всех объектов окажутся те же разрешения, что и у родительской папки.[2]

1. **Присвоение файла или папки**

Каждый файл или папка в томе NTFS имеет владельца, то есть человека, который осуществляет контроль за разрешениями для объектов и присваивает их другим пользователям. Создатель нового файла является его началльным владельцем.

Для обнаружения того, кто является владельцем файла или папки, следует выполнить такие действия:

1. Щелкнуть правой кнопкой мыши на файле или папке в Проводнике и выбрать пункт Properties (Свойства).
2. Щелкнуть на вкладке Security (Безопасность) и щелкнуть на Advanced (Дополнительно).
3. Щелкнуть на вкладке Owner (Владелец), чтобы открыть диалоговое окно «Параметры управления доступом для НР\_file на DRIVE ». В поле Current Owner Of This Item (Текущиц владелец этого элемента) будет указано имя владельца.

Иногда приходится присваивать «чужой » файл или папку. Например, если владелец файла больше не хочет им заниматься, системный администратор может присвоить файл себе или другому пользователю, или другой пользователь может присвоить файл напрямую.

Для присвоения файла или папки необходимо иметь разрешение Take Ownership (Смена владельца), которое включено в разрешение Full Control (Полный доступ). Чтобы получить такое разрешение, необходимо получить разрешение на полный доступ у администратора или владельца файла, который также обладает полным доступом.

Для присвоения файла или папки необходимо:

1. Вывести на экран вкладку Owner (Владелец) диалогового окна Access Controll Settings (Параметры управления доступом).
2. Выделить в списке Change Owner To (Изменить владельца на ) имя (список включает имя учетной записи и группы, к которой вы принадлежите).
3. Если при присвоении папки вы хотите получить ее содержимое, следует установить флажок Replace Owner On Subcontainers And Objects (Сменить владельца содержимого).

Файл может принадлежать только одному пользователю. Если вы получаете его в собственность, другой пользователь уже не является его владельцем. Однако группа может владеть файлом. В этом случае все участники группы получают степень доступа создателя-владельца.

Все создатели файлов являются их владельцами, если только объекты не были присвоены другим. Несмотря на право администратора получать файл во владение, при присвоении степеней доступа к файлу последнее слово остается за его владельцем.

**Защита для пользователя.**

Выше обсуждались функции для присвоения администраторами и владельцами файлов степеней доступа. Какое же отношение имеет защита к простому пользователю?

При попытке пользователя произвести операцию с защищенным файлом, система Windows сверяется со списком контроля доступа. Если ACL позволяет доступ, пользователь получает его. Если нет – не получает. Окно с сообщением об ошибке, появляющееся в таких случаях, зависит от системы и от того, что именно хотел сделать пользователь.[4]

## 5.Настройка безопасности для новых файлов и папок

До сих пор речь шла о настройках для защиты уже существующих файлов и папок. Теперь следует рассказать о защите вновь созданных объектов.

Правило простое: новые файлы и папки получают разрешение той папки, в которой они были созданы. Если создать файл в папке, для которой у бухгалтерского отдела имеется разрешение Modify (Изменить), а у отдела кадров – Full Control (Полный доступ), то отделы останутся при своих разрешениях, если в папке появится новый файл.

Точно так же, если скопировать существующий файл или папку в другую папку или переместить файлы и папки в другой том, копии будут иметь то же разрешение, что и оригинал, поскольку, по сути при копировании и перемещении создаются новые файлы и папки. С другой стороны, если перемещать существующие папки и файлы в другую папку в том же томе, папки и файлы сохраняют свои разрешения, они не будут наследовать разрешения их нового хранилища.[5]

## 6. Использование шифрования файлов

Система шифровки файлов (EES)- новая в системе Windows 2000. Она позволяет зашифровать файлы в томах NTFS так, чтобы их мог использовать только владелец. При шифровке файла или папки система использует ваш сертификат шифровки и его частный ключ для кодирования информации. Когда бы вы ни использовали файл (при условии, что вы используете одну и ту же учетную запись пользователя при шифровке и при последующих вхождениях), система использует тот же сертификат для расшифровки. (Это происходит вне предела видимости, поэтому использование зашифрованного файла ничем не отличается от обычного.) Ели файл попробует открыть, копировать, переместить, переименовать кто-нибудь другой, он получит сообщение об отсутствии доступа к файлу.

При этом любой пользователь, имеющий разрешение на удаление файла, входящее в разрешение Modify(Изменить) и Full Control(Полный доступ), может удалить зашифрованный файл.

При кодировании папки все файлы и подпапки также оказываются зашифрованы, включая временные файлы, которые создаются некоторые программы при редактировании документа. Если вы храните все документы в папке My Documents (Мои документы), она является первым кандидатом.

Для кодирования папки необходимо выполнить следующие действия:

1. Щелкнуть правой кнопкой мыши на папке (или файле, если необходимо закодировать отдельный файл) в проводнике Windows и выбрать в меню пункт Properties (Свойства).
2. На вкладке General (Общие) щелкнуть на Advanced (Дополнительно), чтобы показать диалоговое окно Advanced Attributes (Дополнительные атрибуты).
3. Установить флажок Encrypt Contents To Secure Date (Шифровать содержимое для защиты данных).

Сжатый файлы зашифровать нельзя. Если подлежащие кодированию файлы уже сжаты, система Windows уберет атрибут Compressed (Сжатый).

1. Щелкнуть на кнопке OK, чтобы закрыть диалоговое окно Advanced Attributes (Дополнительные атрибуты), и щелкнуть на ОК еще раз, чтобы закрыть диалоговое окно свойств. При кодировании папки система запросит подтверждение.
2. Выбрать параметр и щелкнуть на кнопке ОК

▪ При выборе Apply Changes To This Folder Only (Только в этой папке) система не станет шифровать уже существующие файлы (включая те, что были скопированы или перемещены в папку).

▪ При выборе Apply Changes To This Folder, Subfolders And Files (К этой папке и ко всем вложенным файлам и папкам) система немедленно зашифрует все, что содержится в папке.

Использовать зашифрованные файлы можно только при данной учетной записи и сертификате. Зашифрованные файлы нельзя предоставлять в общее пользование по сети или на той же рабочей станции.

### Создание страховочной копии сертификата для шифровки

Сертификат для шифровки следует скопировать на дискету и хранить в надежном месте. Если вы потеряете сертификат (что может произойти, например, при повреждении диска), его будет можно восстановить для расшифровки файлов.

Для создания страховочной копии сертификата необходимо:

1. Открыть User And Passwords (Пользователи и Пороли) на панели управления.
2. Щелкнуть на вкладке Advanced (Дополнительные) и щелкнуть на Certificates (Сертификаты).
3. В диалоговом окне Certificates (Сертификаты) щелкнуть на вкладке Personal (Личный) и выбрать сертификат с именем вашей учетной записи.
4. Щелкнуть на Export (Экспортировать), чтобы загрузился мастер экспортирования сертификата, а затем выполнить его требования.[4]

## 7. Установка дисковых квот

Другой новой функцией системы Windows 2000 является возможность распределять и ограничивать дисковое пространство для пользователей в томах NTFS. Это особенно полезно для сервера, однако может пригодиться и для одиночной рабочей станции, где имеется несколько пользователей.

Чтобы установить дисковые квоты, необходимо обладать полномочиями администратора. Чтобы использовать квоты, необходимо выполнять следующие действия:

1. Щелкнуть правой кнопкой мыши на диске в папке My Computer (Мой Компьютер) и выбрать пункт Properties (Свойства).
2. Щелкнуть на вкладке Quota (Квота) и установить флажок Enable Quota Management (Включить Управление квотами), чтобы на вкладке появились другие элементы.
3. Установите прочие параметры на вкладке Quota (Квота)

▪ Выбор Deny Disk Space To Users Exceeding Quota Limit (Не выделять пространство на диске при превышении квоты) не позволяет сохранять файлы после превышения выделенной квоты. (Появится сообщение с нехватке места диске.) Если не установить этот флажок, система не будет обращать внимание на используемый объем диска, но позволит закрепить часть диска за пользователем.

▪ Чтобы установить принятые по умолчанию ограничения дискового пространства для новых пользователей (тех, к которых нет записи в окне квот), следует установить переключатель Limit Disk Space To (Выделять на диске не более) и указывать ограничения и критический уровень. (Критический уровень указывается не для пользователя, а для администратора, который может наблюдать за пользователями, приближающимися к ограничению.) Если для новых пользователей не стоит ограничивать дискового пространства, следует поставить переключатель в положение Do Not Limit Disk Usage (Не ограничивать выделение места на диске).

▪ Если вы хотите, чтобы система протоколировала, когда пользователь превышает ограничения или критический уровень, следует установить соответствующие флажки.[1]

## 7.1 Управление дисковыми квотами

При использовании квот в системе, где уже существует файлы, система Windows подсчитывает дисковое пространство, использующееся каждым, кто создавал, копировал или присваивал существующие файлы. Принятые по умолчанию ограничения и критические уровни распространяются на старых и новых пользователей, сохраняющих файлы. Чтобы просматривать и изменять записи квот, следует открыть диалоговое окно свойств диска, щелкнуть на вкладке Quota (Квота) и щелкнуть на Quota Entries (Записи квот). В результате появится окно Quota Entries (Записи квот). Прежде чем щелкнуть на Quota Entries (Записи квот) в первый раз, следует щелкнуть на ОК или Apply (Применить). Если этого не сделать, в окне будет показан 0 байт использованного места.

Для каждого пользователя окно записи квот показывает следующую информацию:

▪ Указатель состояния (ОК для тех, кто далек от критического уровня, и Warring (Предупреждение) для тех, кто близок к нему, а также Above Limits (превышение ограничений) для тех, кто вышел за пределы).

▪ Имя пользователя и имя учетной записи.

▪ Количество дискового пространства, занимаемого файлами пользователя.

▪ Ограничения и критический уровень.

▪ Процент квоты, который уже использован.

Чтобы изменить ограничения пользователя, следует дважды щелкнуть на его имени. Появится диалоговое окно с вариантами выбора, похожими на те, что имеются на вкладке Quota (Квота) для новых пользователей.[2]

## 7.2 Создание новой записи квот

Для установления ограничений для пользователя, у которого еще нет записи, следует открыть окно Quota Entries (Записи квот) и выбрать в меню Quota (Квота) пункт New Quota Entry (Создание записи квоты). Появится диалоговое окно Select Users (Выбор пользователей), где можно выбрать локальную запись пользователя или учетные записи домена, которому следует установить ограничения. После выбора одной или нескольких учетных записей пользователя следует указать ограничения в появившемся диалоговом окне Add New Quota Entry (Добавить новую запись квоты).

## 7.3 Удаление записи квоты

Если у пользователя больше нет файлов в вашем томе NTFS, можно удалить его записи квоты, щелкнув на ней правой кнопкой мыши и выбрав пункт Delete (Удалить). Удалить записи пользователя, который имеет файлы на диске нельзя.

Можно использовать команду Delete (Удалить), чтобы точно определить, какие файлы принадлежат пользователю, а потом, если следует удалить запись квоты, можно удалить, сменить владельца или переместить файлы пользователя. Файл следует выделить и использовать кнопки Delete (Удалить), Take Ownership (Смена владельца) или Move (Переместить) для совершения соответствующих действий. Когда все файлы будут распределены тем или иным способом, следует щелкнуть на кнопке Close(Закрыть), чтобы завершить удаление записи квоты пользователя.[1]

**ЗАКЛЮЧЕНИЕ**

Система безопасности Windows 2000 состоит из множества компонентов, предоставляющих возможность обеспечения безопасности работы с данными в любой точке сети, начиная с хранения информации в файлах на дисках серверов и рабочих станций и заканчивая средствами обеспечения гарантированного уровня безопасности при передаче данных по сети путем использования механизмов виртуальных частных сетей (VPN). Сейчас Windows 2000 содержит более 40 различных интегрированных между собой механизмов безопасности, каждый из которых может быть расширен разработчиками для учета особенностей применения этой ОС в сети своего предприятия.

**ЛИТЕРАТУРА**

1. Стинсон К., Зихерт К.

Эффективная работа с Microsoft Windows 2000 Professional,

СПб, 2001.

1. Штайнер Г.

Windows 2000 Справочник, М, 2000.

1. Под редакцией Чекмарева А.

Новые технологии Windows 2000, СПб, 1999.

1. Самоучитель.

Технология Windows NT Microsoft Windows 2000 Professional,

М, 2000.

1. Джойс Дж., Мун М.

Windows 2000 Professional, М, 2001.