**Лабораторная работа № 2**

**Тема: «Парольная защита баз данных в *Microsoft Access». «*Парольная защита и разграничение доступа в Windows XP»**

# Цель:

Частичную защиту базы данных обеспечивает добавление пароля, ограничивающего пользователей, которые могут открывать базу данных. *Microsoft Access* хранит пароль базы данных в незашифрованном виде. Если это нарушает безопасность защищаемой паролем базы данных, не следует использовать пароль. Вместо этого необходимо определить ***защиту на уровне пользователей*** (см. с. 33). Защита на уровне пользователей предполагает задание администратором базы данных определенных разрешений отдельным пользователям и группам пользователей на следующие объекты: таблицы, запросы, формы, отчеты и макросы.



Внимание!!!

Если Вы потеряли или забыли пароль, восстановить его будет невозможно, и вы не сможете открыть базу данных.

Нельзя установить пароль базы данных, если для базы данных была определена защита на уровне пользователей, а у Вас нет разрешений администратора для базы данных. Кроме того, пароль базы данных определяется дополнительно к защите на уровне пользователей. Если была определена защита на уровне пользователей, то любые ограничения, основанные на разрешениях на доступ на уровне пользователей, остаются в силе.

1. Закройте базу данных. Если база данных открыта для общего доступа в сети, убедитесь, что все остальные пользователи закрыли ее.
2. Сделайте резервную копию базы данных и сохраните ее в надежном месте.
3. В меню **Файл** выберите команду **Открыть**.
4. Щелкните стрелку справа от поля **Папка**, выберите диск и папку, в которой расположен файл базы данных *Microsoft Access* , и щелкните значок этого файла.
5. Щелкните стрелку справа от кнопки **Открыть**, выберите вариант

**Монопольно** и откройте базу данных.

1. В меню **Сервис** выберите команду **Защита** и подкоманду **Задать пароль базы данных**.
2. Введите пароль в поле ***Password***.

# Соглашения о паролях

Имена учетных записей могут иметь длину от 1 до 20 знаков и могут состоять из букв, цифр, пробелов и символов из расширенных наборов, за исключением следующих:

 знаки " \ [ ] : | < > + = ; , . ? \*  пробелы в начале имени;

 управляющие знаки (с кодами ASCII от 10 до 31).

***Примечание***. В паролях учитывается регистр знаков.

1. Для подтверждения пароля введите его еще раз в поле

**Подтверждение**, а затем нажмите кнопку **OK**.

Теперь пароль задан. При следующем открытии базы данных появляется диалоговое окно, в которое необходимо ввести пароль.

## Примечания

 Пароль базы данных сохраняется в базе данных, а не в файле рабочей группы. Файл рабочей группы – это файл, который *Microsoft Access* считывает при запуске, содержащий сведения о пользователях, входящих в рабочую группу. Эти сведения включают имена учетных записей пользователей, их пароли и имена групп, в которые входят пользователи.

 Если таблица из защищенной паролем базы данных является ***связанной***, то при установлении связи пароль сохраняется (помещается во временный буфер) в базе данных, с которой связывается таблица. Это позволит любому пользователю видеть ваши данные.

## Задание 1

Закройте паролем Вашу базу данных.

## Задание 2

# Отображение и скрытие объектов базы данных в окне базы данных

*Указание отображения или скрытия объекта базы данных*

1. В списке **Объекты** окна базы данных (Окно базы данных. Окно, которое открывается при открытии базы данных *Microsoft Access* или проекта Microsoft Access. В окне базы данных выводятся ярлыки для создания новых объектов базы данных и открытия существующих объектов.) выберите тип объекта базы данных, свойства которого нужно изменить.
2. Нажмите кнопку **Свойства** на панели инструментов **База данных**.
3. Установите или снимите флажок **скрытый**.

## Задание 3

# Отображение или скрытие объектов, скрытых по умолчанию

Если нужно выполнить какие-либо действия с объектами, которые были определены как скрытые, можно отобразить эти объекты в окне базы данных , не отменяя их атрибута скрытия.

1. В меню **Сервис** выберите команду **Параметры**.
2. Выберите вкладку **Вид**.
3. Установите или снимите флажок **скрытые объекты** в группе **Отображать**. Чтобы показать различие между скрытыми и остальными объектами, скрытые объекты отображаются в виде серых значков.

# Использование параметров запуска

Для указания, например, отображаемой формы, возможности изменения панелей инструментов, а также контекстных меню , доступных в, можно воспользоваться параметрами запуска. Кроме того, специальный макрос *AutoExec* позволяет автоматически выполнить или набор макрокоманд при открытии базы данных. В процессе открытия базы данных *Microsoft Access* выполняет поиск макроса с этим именем и, если такой макрос существует, автоматически запускает его.

# Настройка параметров запуска

1. В меню **Сервис** выберите команду **Параметры запуска**.
2. Выберите нужные параметры или введите нужные значения.

Для получения дополнительных сведений об определенном элементе диалогового окна нажмите кнопку контекстной справки в верхнем углу окна и выберите соответствующий элемент.

## Задание 4

# Создание макроса, который запускается при первом открытии файла

## Microsoft Access

1. Создайте макрос, содержащий макрокоманды, которые требуется выполнить при открытии базы данных.
2. Сохраните макрос под именем *AutoExec*.

При следующем открытии базы данных *Microsoft Access* автоматически запустит этот макрос.

## Примечание

Если требуется открыть базу данных, не выполняя при этом макрос

*AutoExec*, открывайте базу данных при нажатой клавише *SHIFT*.

## Задание 5

**Удаление пароля в базе данных *Microsoft Access (.mdb)***

1. В меню **Файл** выберите команду **Открыть**.
2. Щелкните стрелку справа от кнопки **Открыть**, выберите команду

**Монопольно** и откройте базу данных.

1. В диалоговом окне **Необходимо ввести пароль** введите пароль базы данных и нажмите кнопку *OK*. Пароли учитывают регистр знаков (учет регистра – это учет различия между строчными и прописными буквами. При поиске с учетом регистра требуется совпадение с образцом с точностью до прописных и строчных букв).
2. В меню **Сервис** выберите команды **Защита** и **Удалить пароль базы данных**. Эта команда доступна, когда пароль базы данных уже установлен.
3. В диалоговом окне **Удаление пароля базы данных** введите текущий пароль.

## Задание 6

# Создание или изменение пароля учетной записи пользователя в базе данных *Microsoft Access*

Пароль учетной записи пользователя определяется для того, чтобы запретить пользователю подключение под учетной записью другого пользователя. *Microsoft Access* по умолчанию присваивает учетной записи пользователя «*Admin*» и любым новым учетным записям пользователя , создаваемым в рабочей группе, пустые пароли.

**Внимание!** Если пароль потерян или забыт, то восстановить его будет невозможно. Поэтому следует хранить его в надежном месте. Чтобы получить доступ к базе данных пользователь, потерявший пароль, должен обратиться к администратору (члену группы «*Admins*» той рабочей группы, в которой были созданы учетная запись и пароль), чтобы тот снял пароль.

1. Запустите *Microsoft Access* с использованием той рабочей группы, в которой хранится учетная запись пользователя, и войдите в него по той учетной записи, для которой нужно создать или изменить пароль.

Для проверки имени текущей рабочей группы или для изменения рабочей группы используйте служебную программу «Администратор рабочих групп».

1. Откройте базу данных.
2. В меню **Сервис** выберите команду **Защита**, а затем команду

# Пользователи и группы.

1. На вкладке **Изменение пароля** оставьте поле **Текущий пароль** пустым, если учетная запись ранее не имела пароля. В противном случае введите в поле **Текущий пароль** старый пароль.
2. Введите новый пароль в поле **Новый пароль**.

# Соглашения о паролях

Имена учетных записей могут иметь длину от 1 до 20 знаков и могут состоять из букв, цифр, пробелов и символов из расширенных наборов, за исключением следующих:

 знаки " \ [ ] : | < > + = ; , . ? \*  пробелы в начале имени;

 управляющие знаки (с кодами *ASCII* от 10 до 31).

**Примечание**. В паролях учитывается регистр знаков.

1. Повторно введите новый пароль в поле **Подтверждение** и нажмите кнопку *OK*.

## Задание 7

# Снятие пароля учетной записи пользователя

Для выполнения данной процедуры необходимо войти в базу по учетной записи члена группы «*Admins*».

1. Запустите *Microsoft Access* с использованием файла рабочей группы, в котором хранится учетная запись пользователя .

Узнать имя текущего файла рабочей группы или изменить рабочую группу

можно с помощью администратора рабочих групп.

1. Откройте базу данных.
2. В меню **Сервис** выберите команду **Защита**, а затем команду

# Пользователи и группы.

1. На вкладке **Пользователи** введите имя учетной записи пользователя в поле **Имя**.
2. Нажмите кнопку **Снять пароль**.
3. Повторите шаги 4 и 5 для снятия других паролей, затем нажмите кнопку ***OK***.

## Задание 8

# Защита на уровне пользователей

При активизации защиты на уровне пользователей в базе данных *Microsoft Access* администратор базы данных или владелец объекта предоставляет определенные разрешения отдельным пользователям и группам пользователей на следующие объекты: таблицы, запросы, формы, отчеты и макросы. *Microsoft Access* напоминает механизмы безопасности, используемые на серверах и больших компьютерах. С помощью паролей и разрешений (набора атрибутов, определяющих права пользователя на данные или объекты в базе данных) предоставляется или ограничивается доступ пользователей или групп к объектам базы данных. Учетные записи системы безопасности определяют пользователей и группы, которым разрешен доступ к объектам. Эта информация, которую называют сведениями о рабочей группе (рабочая группа это группа пользователей сети, которые работают с данными в режиме общего доступа и имеют общий файл рабочей группы.), сохраняется в файле рабочей группы (Файл рабочей группы. Файл, который *Microsoft Access* считывает при запуске, содержащий сведения о пользователях, входящих в рабочую группу. Эти сведения включают имена учетных записей пользователей, их пароли и имена групп, в которые входят пользователи.).

# Общие сведения о защите на уровне пользователей

Наиболее гибкий и распространенный способ защиты базы данных называют защитой на уровне пользователей. Двумя основными причинами использования защиты на уровне пользователей являются:

 защита приложения от повреждения из-за неумышленного изменения пользователями таблиц, запросов, форм, отчетов и макросов, от которых зависит работа приложения;

 защита конфиденциальных сведений в базе данных.

При использовании этого типа защиты пользователь должен ввести пароль при запуске *Microsoft Access*. Затем *Access* читает файл рабочей группы, в котором каждый пользователь идентифицируется уникальным кодом. В файле рабочей группы пользователи по их личным кодам и паролям идентифицируются как авторизованные индивидуальные пользователи и как члены конкретных групп. В *Microsoft Access* определены две стандартные группы: администраторы – группа «*Admins*» (учетная запись группы системных администраторов, имеющих полные разрешения на все базы данных, используемые рабочей группой. Программа установки автоматически добавляет в группу «Admins» стандартную учетную запись пользователя

«*Admin*».) и пользователи – группа «*Users*» (учетная запись группы, в которую включаются все учетные записи пользователей. *Microsoft Access* автоматически добавляет создаваемые учетные записи пользователей в группу «*Users*»), но допускается определение дополнительных групп.

Хотя установка защиты на уровне пользователей для большинства баз данных является сложной задачей, мастер защиты позволит быстро и легко защитить базу данных. Более того, благодаря использованию общих схем защиты, мастер позволяет уменьшить или даже вообще исключить необходимость использования команды **Защита** в меню **Сервис**.

Мастер защиты помогает назначить разрешения и создать учетные записи пользователей (учетная запись пользователя, определяемая именем и личным

кодом (*PID*), которая создается для управления разрешениями пользователя на доступ к объектам базы данных в рабочей группе *Microsoft Access*) и учетные записи групп (совокупность учетных записей пользователей, входящих в рабочую группу, имеющая собственные групповое имя и личный код (*PID*). Разрешения, назначенные группе, автоматически получает каждый пользователь, входящий в группу). Однако после запуска мастера для базы данных и существующих в ней таблиц, запросов, форм, отчетов и макросов имеется возможность вручную назначить или удалить разрешения на доступ для учетных записей пользователей и групп в рабочей группе. Также могут быть установлены разрешения на доступ, по умолчанию присваиваемые вновь создаваемым объектам базы данных.

Группам и пользователям предоставляются разрешения, определяющие возможность их доступа к каждому объекту базы данных. Например, члены группы «*Users*» могут иметь разрешения на просмотр, ввод или изменение данных в таблице «Клиенты», но им не будет разрешено изменять структуру этой таблицы. Члены группы «*Users*» могут быть допущены только к просмотру данных в таблице, содержащей сведения о заказах, и не иметь доступа к таблице «Платежная ведомость». Члены группы «*Admins*» имеют разрешения на доступ ко всем объектам базы данных. Имеется возможность установить более разветвленную структуру управления, создавая собственные учетные записи групп, предоставляя этим группам соответствующие разрешения и добавляя пользователей в группы.

Если для системы защиты достаточно группы администраторов и группы пользователей, то нет необходимости создавать другие группы. Можно воспользоваться стандартными группами «*Admins*» и «*Users*». В этом случае необходимо присвоить соответствующие разрешения на доступ стандартной группе «*Users*» и добавить дополнительных администраторов в стандартную группу «*Admins*». Каждый новый пользователь автоматически добавляется в группу «*Users»*. Типовые разрешения на доступ для группы «*Users*» могут

включать «Чтение данных» и «Обновление данных» для таблиц и запросов и

«Открытие/запуск» для форм и отчетов

В случае необходимости более разветвленной структуры управления для различных групп пользователей, имеется возможность создания новых групп, присвоения группам различных наборов разрешений на доступ и добавления новых пользователей в соответствующие группы. Для упрощения управления разрешениями на доступ рекомендуется присваивать разрешения только группам (а не отдельным пользователям), а затем добавлять пользователей в соответствующие группы.

Например, можно организовать защиту базы данных «Заказы» с помощью создания учетных записей «Управляющие» для руководства фирмы,

«Представители» для торговых представителей и «Персонал» для административного персонала. После этого следует присвоить наибольшее количество разрешений группе «Управляющие», промежуточное количество группе «Представители» и минимальное группе «Персонал». При создании учетной записи для нового сотрудника эта запись будет добавляться в одну из групп, и сотрудник автоматически получит разрешения, принадлежащие этой группе.

# Рабочие группы и файлы рабочих групп

Рабочая группа *Microsoft Access* – это группа пользователей, которые совместно используют данные в многопользовательской среде. Если определена защита на уровне пользователей, члены рабочей группы регистрируются с помощью, которые сохраняются в файле рабочей группы *Microsoft Access*. Пароли пользователей также запоминаются в файле рабочей группы. Этим учетным записям системы защиты могут быть предоставлены разрешения на доступ к базе данных и ее таблицам, запросам, формам, отчетам и макросам. Сами разрешения сохраняются в защищенной базе данных.

Когда пользователь в первый раз запускает *Microsoft Access* после установки *Microsoft Office*, *Access* автоматически создает файл рабочей группы

*Microsoft Access*, который идентифицируется по указанными пользователем имени и названию организации. Относительное расположение файла рабочей группы записывается в следующие параметры реестра:

HKEY\_CURRENT\_USER\Software\Microsoft\Office\10.0\Access\Jet\4.0\Eng ines\SystemDB

и HKEY\_USERS\.DEFAULT\Software\Microsoft\Office\10.0\Access\Jet\4.0\En

gines\SystemDB

Следующие пользователи наследуют стандартный путь к файлу рабочей группы из раздела реестра *HKEY\_USERS*. Так как получение этой информации часто не представляет особого труда, существует вероятность того, что кто-то сможет создать другую версию этого файла и приобрести неотъемлемые разрешения на доступ учетной записи администратора в рабочей группе, определяемой этим файлом рабочей группы. Чтобы избежать этого, создайте новый файл рабочей группы и укажите код рабочей группы (*WID* – код рабочей группы представляет набор от 4 до 20 алфавитно-цифровых символов (с учетом регистра), который вводится при создании нового файла рабочей группы с помощью администратора рабочих групп. Этот код однозначно определяет группу «*Admins*» в файле рабочей группы.). Только тот, кто знает этот код, сможет создать копию файла рабочей группы.

Любые создаваемые учетные записи пользователей и групп и пароли сохраняются в этом файле рабочей группы до тех пор, пока пользователь не присоединится к другой рабочей группе с помощью администратора рабочих групп.

**Примечание**. В *Access* 2002 программу «Администратор рабочих групп» можно запустить из подменю **Защита** меню **Сервис**.

Обязательно запишите введенное имя, название организации и код рабочей группы с учетом регистра (для всех трех элементов) и храните их в надежном месте. Если потребуется заново создать файл рабочей группы,

необходимо будет ввести точно эти же сведения. Если они забыты или потеряны, восстановить их и получить доступ к базам данных будет невозможно.

# Разрешения на доступ: как они работают и кто может их назначать

Существуют два типа ***разрешений на доступ***: явные и неявные. Разрешения называются явными, если они непосредственно присвоены ***учетной записи пользователя***; такие разрешения не влияют на разрешения других пользователей. Неявными называются разрешения на доступ, присвоенные учетной записи группы . Пользователь, включенный в такую группу, получает все разрешения, предоставленные группе; удаление пользователя из этой группы лишает его всех разрешений, присвоенных данной группе.

При попытке пользователя выполнить какую-либо операцию с защищенным объектом базы данных его текущие разрешения определяются комбинацией явных и неявных разрешений на доступ. На уровне пользователей всегда действуют минимальные ограничения из налагаемых явными разрешениями для пользователя и для всех групп, к которым принадлежит данный пользователь. Поэтому простейшим способом управления рабочей группой является создание новых групп и определение разрешений на доступ для этих групп, а не для индивидуальных пользователей. После этого изменение разрешений для отдельных пользователей осуществляется путем добавления пользователей в группы или удаления их из групп. Кроме того, при необходимости предоставить новые разрешения, они предоставляются сразу всем членам группы в одной операции.

Изменять разрешения других пользователей на отдельные объекты базы данных могут следующие пользователи:

 члены ***группы «Admins»***, определенной в файле рабочей группы, который использовался при создании конкретной базы данных;

 ***владелец*** (при активизированной системе защиты это учетная запись пользователя, которая осуществляет управление базой данных или ее объектом. По умолчанию разрешения владельца имеет учетная запись пользователя, создавшего базу данных или ее объект.) объекта;

 любой пользователь, получивший на этот объект разрешения администратора.

В ряде случаев пользователи, не имеющие разрешения на выполнение какого-либо действия, имеют возможность присвоить их себе. Такая ситуация имеет место для пользователя, являющегося членом группы «*Admins*» или владельцем объекта.

Пользователь, создавший таблицу, запрос, форму, отчет или макрос, является владельцем этого объекта. Кроме того, группа пользователей, которые могут изменять разрешения в базе данных, может также сменить владельца объектов или заново создать эти объекты, что является альтернативным способом смены владельца объектов. Для создания объекта заново достаточно импортировать или экспортировать этот объект в другую базу данных или сделать копию объекта. Этот прием является простейшим способом смены владельца объектов, в том числе и всей базы данных.

## Примечание

Копирование, импорт или экспорт не приводит к изменению прав владельца для запросов, у которых свойство **При запуске предоставляются права (*RunPermissions*)** имеет значение **Владельца**. Изменение владельца допускается только для запросов, у которых свойство **При запуске предоставляются права (*RunPermissions*)** имеет значение **Пользователя**.

# Организация учетных записей

Файл рабочей группы *Microsoft Access* содержит следующие встроенные учетные записи (табл. 2).

Таблица 2

|  |  |
| --- | --- |
| **Учетная запись** | **Функция** |
| *Admin* | Стандартная. Данные записи являются одинаковыми для  всех экземпляров *Microsoft Access* и других приложений. |
| *Admins* | Учетная запись группы администраторов. Данная запись является уникальной в каждом файле рабочей группы. По умолчанию пользователь «*Admin*» является членом группы  «*Admins*». В каждый момент в группу «*Admins*» должен  входить по крайней мере один пользователь. |
| *Users* | Учетная запись группы, содержащая все учетные записи пользователей. *Microsoft Access* автоматически добавляет учетные записи пользователей в группу «*Users*» при их создании членом группы «*Admins*». Данные записи являются одинаковыми в каждом файле рабочей группы, однако этот файл содержит только учетные записи пользователей, созданные членами группы «*Admins*», входящими в данную рабочую группу. По умолчанию данная учетная запись имеет все разрешения на все новые объекты. Единственным способом удаления учетной записи из группы «*Users*» является удаление пользователя членом  группы «*Admins*». |

В действительности, система защиты *Microsoft Access* всегда включена. До активизации пользователем процедуры подключения для рабочей группы *Microsoft Access* при запуске автоматически подключает всех пользователей с

помощью встроенной ***учетной записи пользователя «Admin»*** с пустым паролем. Неявно *Microsoft Access* использует учетную запись «*Admin*» как учетную запись администратора рабочей группы, а также как ***владельца*** всех создаваемых баз данных и таблиц, форм, отчетов и макросов.

Наличие администраторов и владельцев является необходимым, поскольку им предоставляются разрешения, которые невозможно отобрать.

1. Администраторы (члены группы «*Admins*») всегда могут получить все разрешения на объекты, созданные в рабочей группе.
2. Учетные записи, являющиеся владельцами таблиц, запросов, форм, отчетов или макросов всегда могут получить все разрешения на доступ к этим объектам.
3. Учетная запись, являющаяся владельцем базы данных, всегда может открыть базу данных.

Поскольку учетные записи пользователя «*Admin*» совершенно одинаковы для всех экземпляров *Microsoft Access*, то первым шагом при организации системы защиты является определение учетных записей администратора и владельца (или единой учетной записи, являющейся записью и администратора, и владельца). После этого следует удалить учетную запись пользователя

«*Admin*» из группы «*Admins*». Если этого не сделать, любой пользователь *Microsoft Access* сможет подключиться к рабочей группе с помощью учетной записи «*Admin*» и получить все разрешения на доступ к таблицам, запросам, формам, отчетам и макросам рабочей группы.

В группу «*Admins*» разрешается добавлять произвольное число учетных записей, однако владельцем базы данных может быть только одна учетная запись ‒ та, что была активной при создании базы данных, либо та, что была активной при передаче права владельца путем создания новой базы данных и импорта в нее всех объектов из исходной базы данных. Однако учетные записи групп могут являться владельцами таблиц, запросов, форм, отчетов и макросов базы данных.

# Соображения при организации учетных записей

 Для входа в *Microsoft Access* могут быть использованы только учетные записи пользователя; вход с помощью учетной записи группы невозможен.

 Учетные записи, создаваемые для пользователей базы данных, должны сохраняться в файле той рабочей группы, к которой пользователи будут присоединяться для работы с базой данных. Если для создания базы данных используется другой файл рабочей группы, перед созданием учетных записей его необходимо сменить.

 Необходимо создать уникальные пароли для учетных записей администратора и пользователей. Пользователь, подключившийся с помощью учетной записи администратора, всегда сможет получить все разрешения на доступ ко всем таблицам, запросам, формам, отчетам и макросам, созданным в рабочей группе. Пользователь, подключившийся с помощью учетной записи владельца, всегда сможет получить все разрешения на доступ к объектам, принадлежащим данному владельцу.

После создания учетных записей пользователей и групп можно просматривать и печатать их схемы. *Microsoft Access* печатает отчет по учетным записям в рабочей группе, демонстрирующий группы, к которым принадлежит каждый пользователь, и всех пользователей, входящих в каждую группу.

## Примечание

Для печати сведений об учетных записях пользователей и групп при использовании файла рабочей группы, созданного в *Microsoft Access* версии 2.0, необходимо подключиться как член группы «*Admins*». Если файл рабочей группы был создан в *Microsoft Access* версии 7.0 или более поздней, то печатать сведения о защите могут все пользователи, входящие в рабочую группу.

## Задание

Назначьте разрешения на доступ к объектам вашей базы данных для:

* каждой из групп пользователей на Вашем компьютере;
* для каждого пользователя на Вашем компьютере.

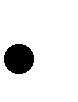
**Задание 9**

**Защита паролем компьютера в ждущем и спящем режимах**

1. Откройте на панели управления компонент **Электропитание**.
2. Выберите вкладку **Дополнительно** и установите флажок **Запрашивать пароль при выходе из спящего режима**. При выходе компьютера из спящего режима будет запрашиваться пароль учетной записи, с которой был осуществлен вход в систему.

## Примечания

 Чтобы открыть компонент «Электропитание», нажмите кнопку **Пуск**, выберите команды **Настройка** и **Панель управления**, а затем дважды щелкните значок **Электропитание**.

 Пароль *Windows* используется и для ждущего, и для спящего

режимов.

# Общие сведения об управлении доступом

Управление доступом заключается в предоставлении пользователям, группам и компьютерам определенных прав на доступ к объектам по сети. Ниже перечислены основные понятия, связанные с управлением доступом.

# Разрешения

Разрешения определяют тип доступа к объекту или его свойству, допустимый для пользователя или группы. Например, группе пользователей финансового отдела можно предоставить разрешения на чтение и запись для файла платежной ведомости *payroll.dat*.

Разрешения применяются к защищенным объектам, таким как файлы, объекты *Active Directory* или объекты реестра. Разрешения могут быть предоставлены любому пользователю, группе или компьютеру. Рекомендуется назначать разрешения группам.

Разрешения на доступ к объектам могут назначаться:

 группам, пользователям и специальным группам домена;

 группам и пользователям данного или любого доверенного домена;  локальным группам и пользователям компьютера, на котором

находится объект.

Разрешения, назначаемые объекту, зависят от его типа. Например, разрешения, которые могут быть назначены для файла, отличаются от разрешений, допустимых для раздела реестра. Однако некоторые разрешения являются общими для большинства типов объектов. Эти общие разрешения перечислены ниже:

 чтение разрешений;  смена разрешений;  смена владельца;

 удаление.

При установке разрешений необходимо определить уровень доступа для групп и пользователей. Например, одному пользователю можно разрешить читать содержимое некоторого файла, другому – вносить изменения в файл, а всем остальным пользователям вообще запретить доступ к этому файлу. Также можно устанавливать разрешения на доступ к принтерам, чтобы одни пользователи могли настраивать принтер, а другие – только печатать на них.

Если требуется изменить разрешения для отдельного объекта, можно просто запустить нужную программу и внести изменения в свойства объекта. Например, чтобы изменить разрешения на доступ к файлу, запустите проводник, щелкните имя файла правой кнопкой мыши и выберите команду **Свойства**. На вкладке **Безопасность** можно изменить разрешения для файла.

# Владение объектами

При создании объекта ему назначается владелец. По умолчанию владельцем объекта становится его создатель. Какие разрешения ни были бы

установлены для объекта, владелец объекта всегда может изменить эти разрешения.

# Наследование разрешений

Механизм наследования облегчает администраторам задачи назначения разрешений и управления ими. Благодаря этому механизму разрешения, установленные для контейнера, автоматически распространяются на все объекты этого контейнера. Например, файлы, создаваемые в папке, наследуют разрешения этой папки.

# Аудит объектов

Доступ пользователей к объектам можно подвергнуть аудиту. События, связанные с безопасностью, можно просматривать в журнале безопасности, используя программу просмотра событий. Дополнительные сведения см. в разделе «Аудит».

# Пароли и учетные записи пользователей

*Чтобы добавить на компьютер нового пользователя*

При добавлении на компьютер нового пользователя ему предоставляется доступ к файлам и программам на этом компьютере.

Последовательность шагов для выполнения этой задачи зависит от того, входит ли компьютер в сетевой домен или является частью рабочей группы (или является автономным компьютером).

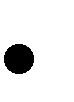
**Задание 10**

*Компьютер подключен к домену*

Для выполнения этой процедуры необходимо войти в систему с учетной записью «Администратор» или члена группы «Администраторы». Если компьютер подключен к сети, то параметры сетевой политики могут запретить выполнение данной процедуры.

1. Откройте на панели управления компонент **Учетные записи пользователей**.
2. На вкладке **Пользователи** нажмите кнопку **Добавить**.
3. Выполняйте указания на экране для добавления нового пользователя.

## Примечания

 Диалоговое окно **Добавление нового пользователя** предоставляет существующему пользователю домена возможность пользоваться компьютером.  С помощью учетных записей пользователей можно только добавлять существующих пользователей домена. Чтобы добавить нового локального пользователя, на вкладке **Дополнительно** нажмите кнопку **Дополнительно**. В оснастке **Локальные пользователи и группы** нажмите кнопку **Пользователи**, а затем в меню **Действие** выберите команду **Новый**

# пользователь.

 Если новый пользователь будет выполнять не только административные задачи, его не следует добавлять в группу

«Администраторы».

**Задание 11**

*Компьютер не подключен к домену*

Необходимо иметь учетную запись администратора компьютера, чтобы добавлять на компьютер нового пользователя.

1. Откройте на панели управления компонент **Учетные записи пользователей**.
2. Щелкните ссылку **Создать учетную запись**.
3. Введите имя новой учетной записи и нажмите кнопку **Далее**.
4. Щелкните переключатель **Администратор компьютера** или **Ограниченная запись** в зависимости от нужной учетной записи, а затем нажмите кнопку **Создать учетную запись**.

## Примечания

 Имя, назначенное учетной записи, будет выводиться на экране приветствия и в меню **Пуск**.

 Первый пользователь компьютера должен иметь учетную запись администратора компьютера.

## Примечание

 Чтобы открыть компонент «Учетные записи», нажмите кнопку **Пуск**, выберите команды **Настройка** и **Панель управления**, затем дважды щелкните значок **Учетные записи пользователей**.

# Советы и рекомендации Разрешения

 Старайтесь устанавливать разрешения для групп, а не для отдельных пользователей.

Поскольку непосредственное сопровождение учетных записей пользователей, как правило, неэффективно, назначать разрешения отдельным пользователям следует лишь в исключительных случаях.

 Устанавливайте разрешения, которые могли бы наследоваться дочерним объектам.

 Лучше назначать не индивидуальные разрешения, а разрешения

**Полный доступ**, если это допустимо.

 Запретить доступ может потребоваться в следующих случаях:

* чтобы исключить каких-либо пользователей из группы, которой предоставлены определенные разрешения;
* чтобы отменить какое-либо особое разрешение, если пользователю или группе уже предоставлен полный доступ.

# Права пользователей

 Назначайте права на максимально высоком уровне дерева контейнера, насколько это возможно. Таким образом достигается наиболее широкий охват действующими правами. Назначаемые права должны подходить большинству участников безопасности.

 Для распространения прав в дереве используйте механизм наследования. Параметры управления доступом будут быстро и эффективно применены ко всем дочерним объектам или в поддереве родительского объекта.

 Администраторам рекомендуется использовать учетную запись с ограниченными разрешениями для выполнения повседневных задач, не связанных с администрированием, и учетную запись с более широкими правами только для выполнения отдельных административных задач. Чтобы для этого не требовалось каждый раз выходить из системы и затем входить повторно, войдите с обычной учетной записью и затем с помощью команды **Запустить как** запускайте программы, требующие более широких прав.

**Задание 12**

*Чтобы установить, просмотреть, сменить или удалить разрешения для файлов и папок*

1. Откройте проводник и найдите файл или папку, для которой требуется установить разрешения.
2. Щелкните файл или папку правой кнопкой мыши, выберите команду **Свойства** и перейдите на вкладку **Безопасность**.
3. Выполните одно из следующих действий.
   * Чтобы установить разрешения для группы или пользователя, которого нет в списке **Группы или пользователи**, нажмите кнопку **Добавить**. Введите имя группы или пользователя, для которого устанавливаются разрешения, и нажмите кнопку **ОК**.
   * Чтобы сменить или удалить разрешения на доступ для существующей группы или пользователя, выберите имя этой группы или пользователя.
4. Выполните одно из следующих действий:
   * Чтобы предоставить или отменить разрешение, в списке **Разрешения для *Имя пользователя или группы*** установите соответственно флажок **Разрешить** или **Запретить**.
   * Чтобы удалить группу или пользователя из списка **Группы или пользователи**, нажмите кнопку **Удалить**.

# Примечания

 Чтобы открыть проводник, нажмите кнопку **Пуск** и выберите команды **Программы**, **Стандартные** и **Проводник**.

 В *Windows XP Professional* группа «Все» больше не включает в себя группу «Анонимный вход».

 Разрешения на доступ к файлам и папкам можно устанавливать только на дисках, отформатированных для файловой системы *NTFS*.

 Изменять разрешения может только владелец объекта или те пользователи, которым он предоставил соответствующие разрешения.

 Группы и пользователи, которым предоставлен полный доступ к папке, могут удалять из нее файлы и подпапки независимо от имеющихся разрешений на доступ к этим файлам и подпапкам.

 Если флажки в списке **Разрешения для *Имя пользователя или группы*** затенены или кнопка **Удалить** недоступна, значит, данный объект унаследовал разрешения от родительской папки. Для получения дополнительных сведений о наследовании свойств файлами и папками щелкните ссылку «См. также».

 При добавлении нового пользователя или группы им по умолчанию назначаются разрешения **Чтение и выполнение**, **Список содержимого папки** и **Чтение**.

**Задание 13**

*Чтобы стать владельцем файла или папки*

1. Откройте Проводник и найдите файл или папку, владельцем которой хотите стать.
2. Щелкните файл или папку правой кнопкой мыши, выберите команду **Свойства** и перейдите на вкладку **Безопасность**.
3. Нажмите кнопку **Дополнительно** и перейдите на вкладку

# Владелец.

1. В списке **Изменить владельца на** выберите нового владельца.

## Примечания

 Чтобы открыть проводник, нажмите кнопку **Пуск** и выберите команды **Программы**, **Стандартные** и **Проводник**.

Передать права владения можно двумя способами.

* + Текущий владелец может наделить других пользователей разрешением **Смена владельца**, после чего они смогут в любой момент стать владельцем объекта.
  + Администратор может стать владельцем любого файла на компьютере. Однако он не может передать право владения другим пользователям. Такое ограничение необходимо для того, чтобы администратор нес ответственность за свои действия.

 В *Windows XP Professional* группа «Все» больше не включает в себя группу «Анонимный вход».

**Задание 14**

*Чтобы скрыть файл или папку*

1. Откройте папку **Мои документы**.

Если в папке «Мои документы» или ее подпапках нет файла или папки, которые требуется скрыть, найдите этот файл или папку, нажав кнопку

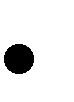
«Поиск». Чтобы запустить средство поиска, нажмите кнопку **Пуск**, выберите команду **Найти**, а затем выберите команду **Файлы и папки**.

1. Щелкните файл или папку правой кнопкой мыши и выберите команду **Свойства**.
2. На вкладке **Общие** установите флажок **Скрытый**.

## Примечания

 Чтобы открыть папку «Мои документы», дважды щелкните значок

**Мои документы** на рабочем столе.

 Для просмотра скрытых файлов выберите в меню **Сервис** в окне любой папки команду **Свойства папки**. На вкладке **Вид** в группе **Дополнительные параметры** выберите вариант **Показывать скрытые файлы и папки**.