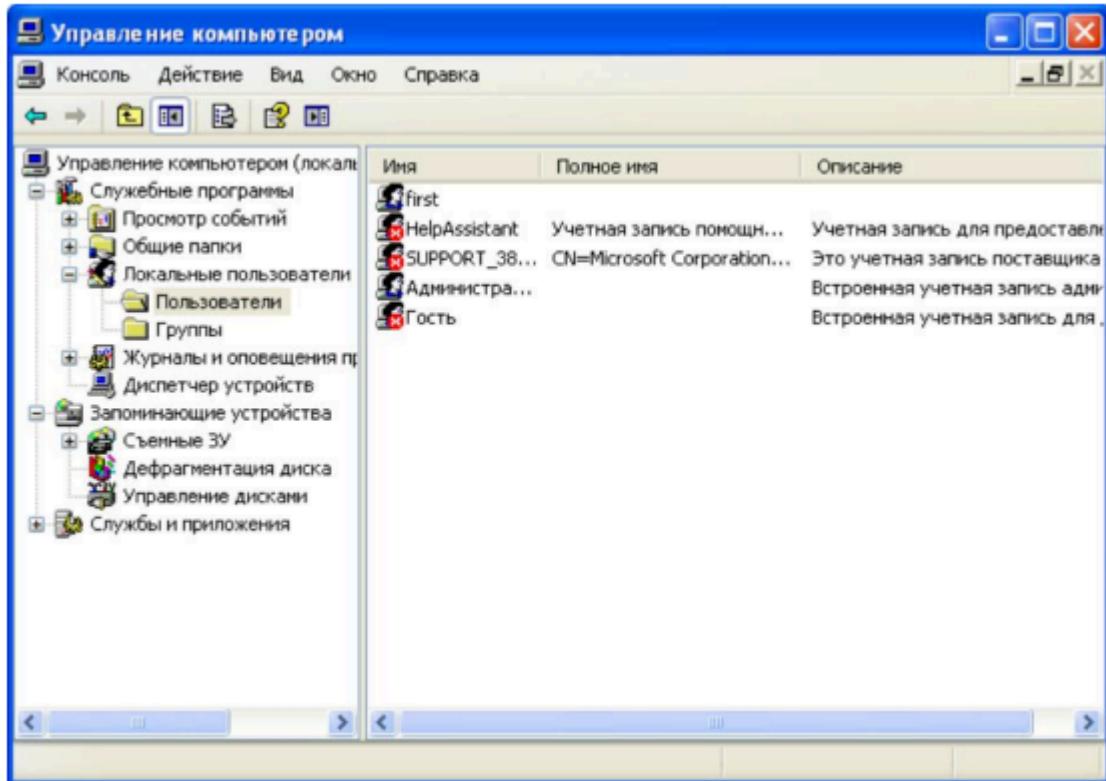


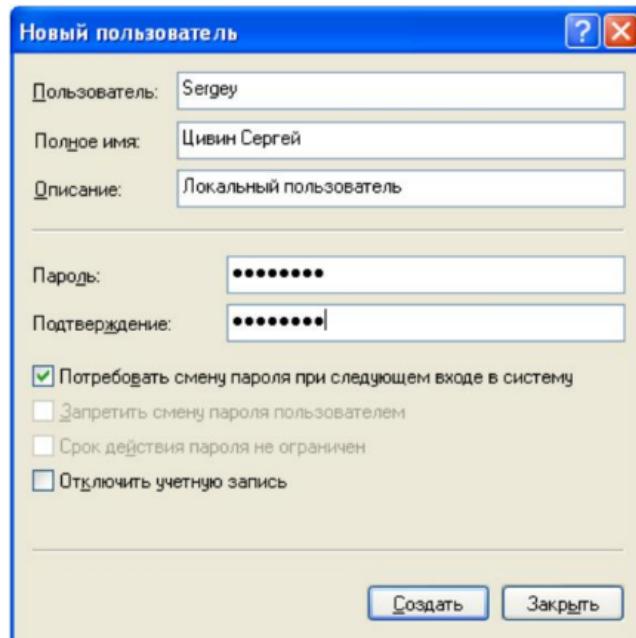
# 1) Windows

## Создание учетной записи пользователя

Открыть меню Пуск, правой кнопкой мыши щелкнуть на записи «Мой компьютер» и в контекстном меню выбрать «Управление». Откроется консоль «Управление компьютером»

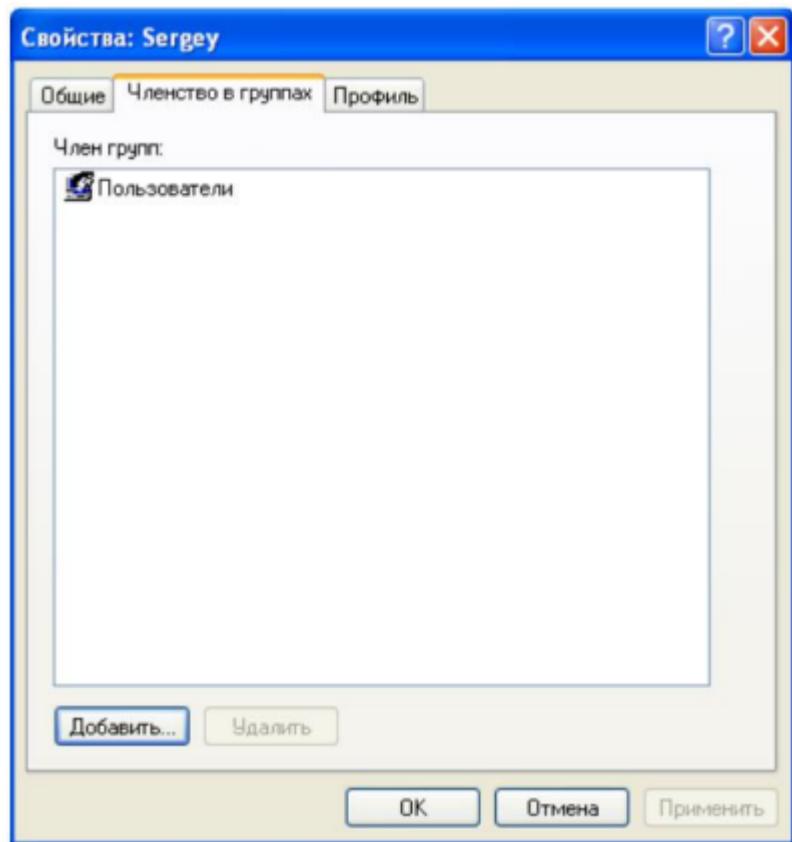


В левой части окна перейти в папку «Локальные пользователи и группы», подпапка «Пользователи». В меню «Действие» выбрать пункт меню «Новый пользователь...». Откроется диалоговое окно создания нового пользователя



Ввести имя входа и полное имя пользователя.

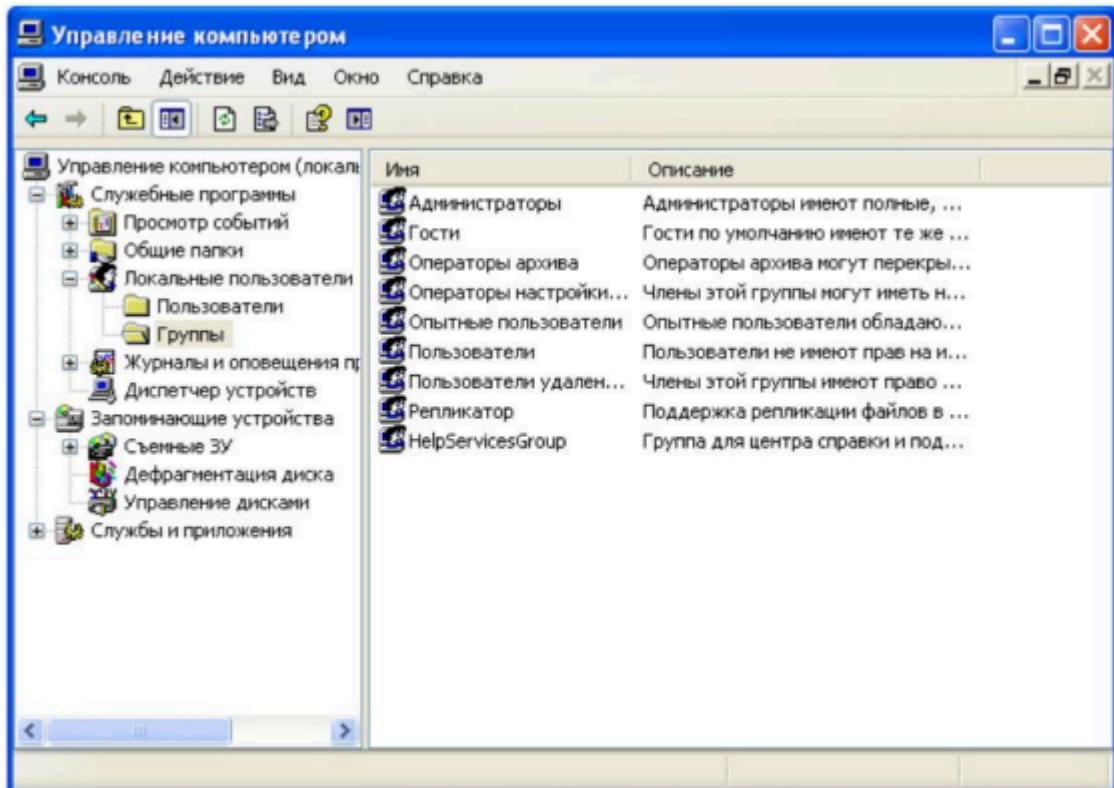
С помощью консоли «Управление компьютером» можно не только создавать новые элементы, но и управлять существующими пользователями: задать пароль пользователя, изменять полное имя и описание пользователя(изменять имя входа нельзя), удалять пользователей. Каждая вновь созданная учетная запись по умолчанию становится членом группы «Пользователи». Для того, чтобы посмотреть, членом каких групп является пользователь, в консоли «Управление компьютером» нужно щелкнуть правой кнопкой мыши по записи о пользователе и в контекстном меню выбрать «Свойства». В открывшемся диалоговом окне перейти на вкладку «Членство в группах»



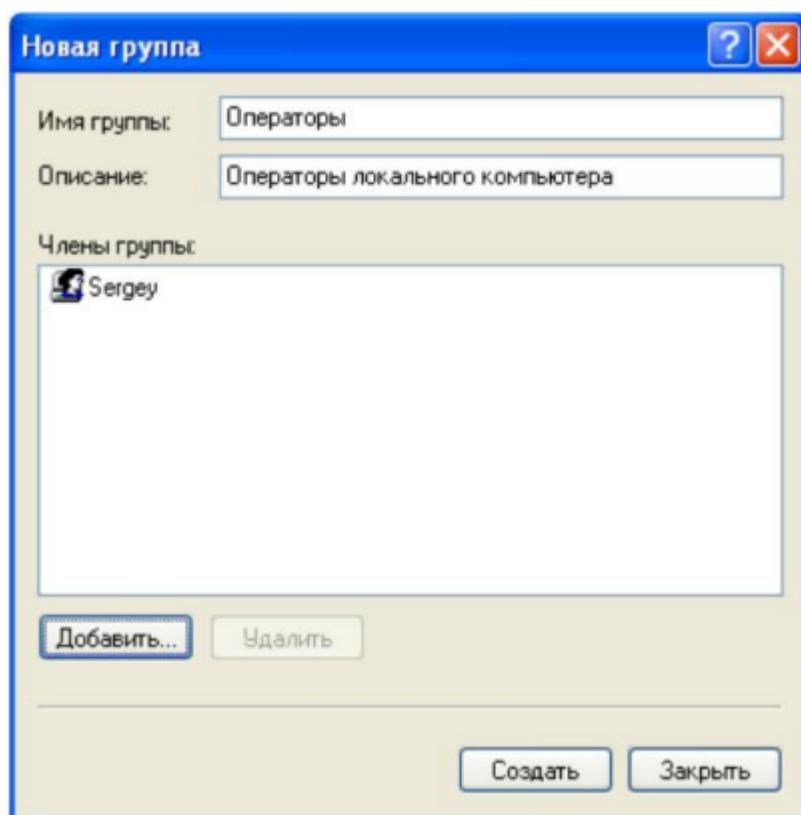
Для того, чтобы проверить новую учетную запись, нужно завершить сеанс локального администратора, и начать сеанс с помощью новой учетной записи.

### **Создание группы пользователей**

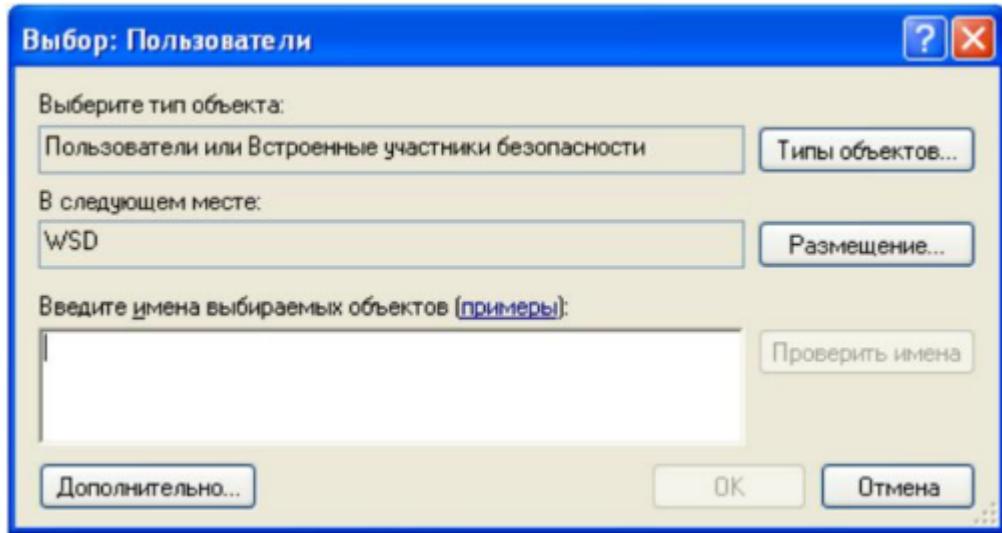
Для создания новой группы следует в сеансе администратора открыть консоль «Управление компьютером» и перейти в папку «Локальные пользователи и группы», подпапку «Группы»



В меню «Действие» выбрать пункт меню «Создать группу...». Откроется окно создания новой группы



Ввести имя группы и ее описание. Нажать кнопку «Добавить...». Откроется окно для выбора пользователей

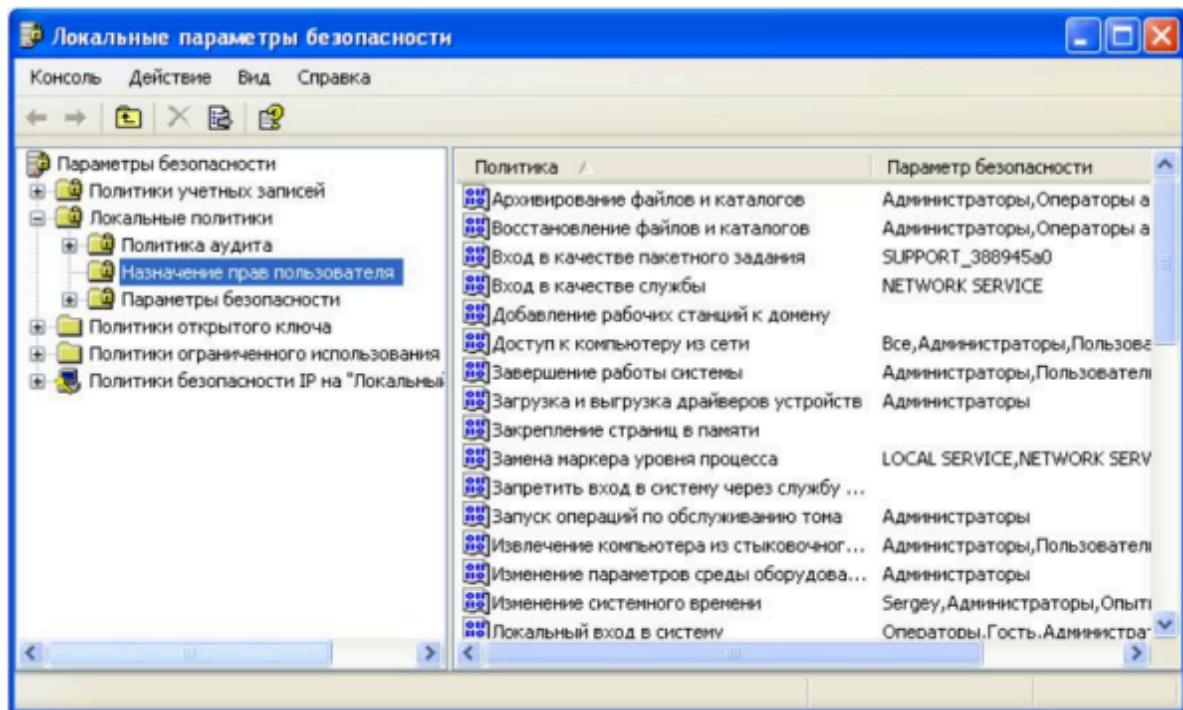


Ввести имена пользователей (если необходимо ввести более одного пользователя, имена должны разделяться точкой с запятой). Нажать кнопку «Проверить имена». Система выполнит поиск имен пользователей в базе данных учетных записей. Корректные имена пользователей будут выделены подчеркиванием. Если имя пользователя написано с ошибкой, система отобразит сообщение об ошибке. Нажать кнопку «OK». Окно выбора пользователей закроется. В окне «Новая группа» нажать кнопку «Создать», будет создана новая группа.

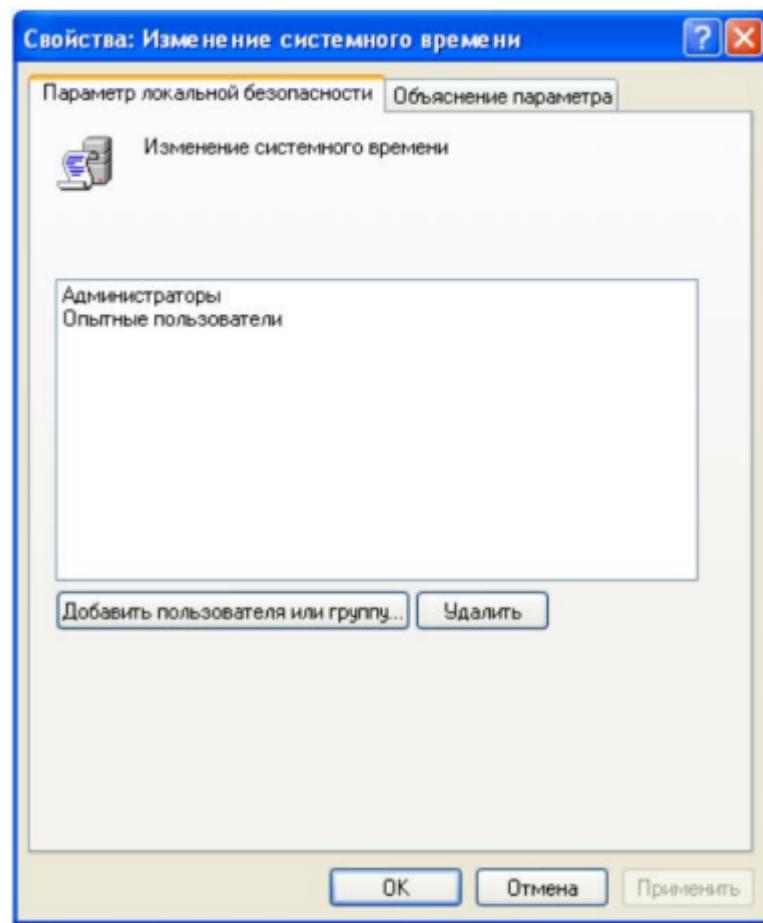
### Управление локальной политикой безопасности

Управление локальной политикой безопасности будет рассмотрено на примере назначения привилегий пользователям.

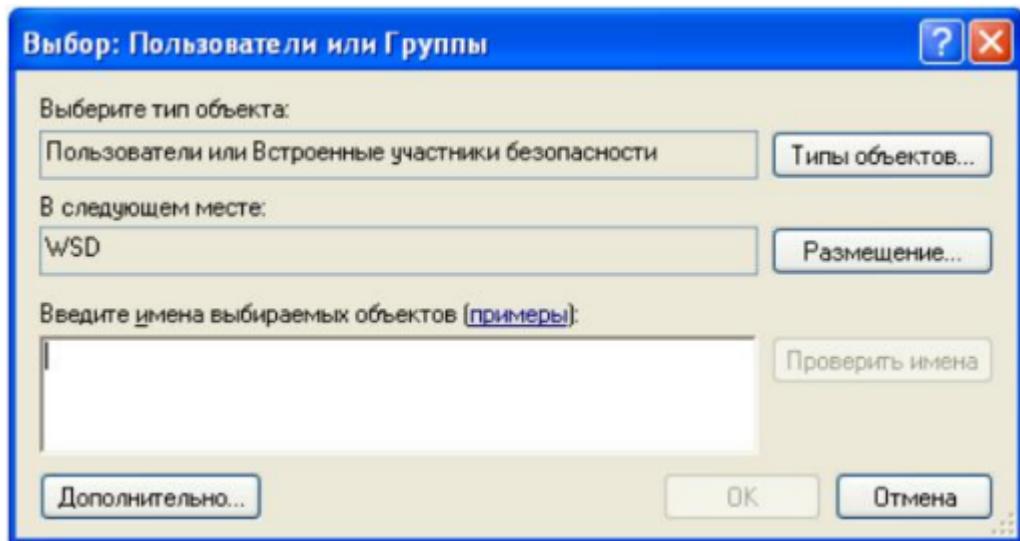
В меню «Пуск» нужно выбрать «Панель управления», в левой части окна щелкнуть на ссылку «Переключение к классическому виду», выбрать «Администрирование», а затем «Локальная политика безопасности». Откроется консоль «Локальные параметры безопасности»



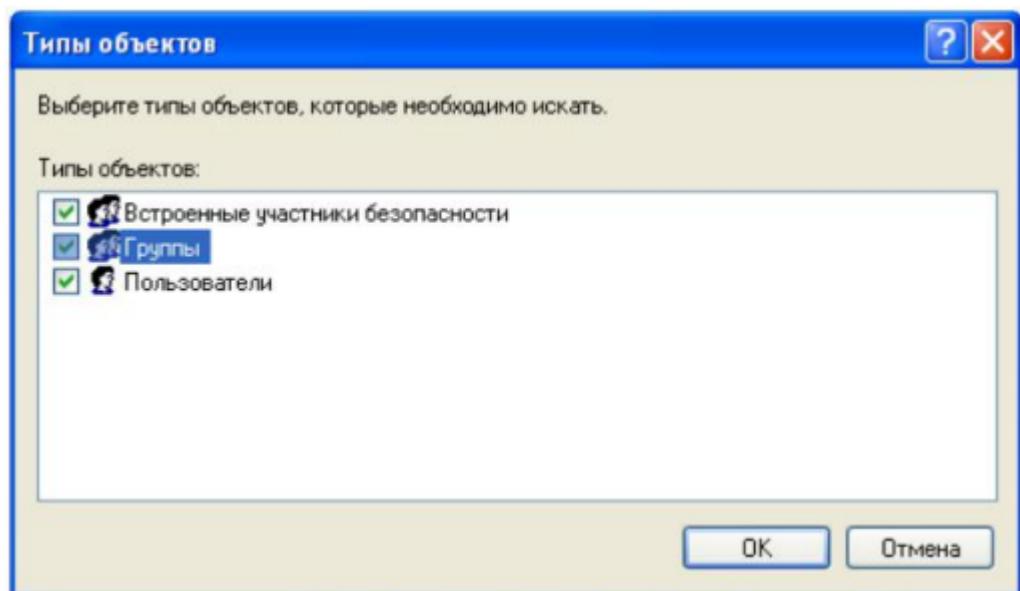
Выбрать папку «Локальные политики», раздел «Назначение прав пользователя». В правой части окна двойным щелчком мыши открыть запись «Изменение системного времени», откроется диалоговое окно для изменения значения данного параметра



По умолчанию только члены групп «Администраторы» и «Опытные пользователи» имеют привилегию изменять системное время. Нажать кнопку «Добавить пользователя или группу...», откроется диалоговое окно



Нажать на кнопку «Типы объектов» и установить флажок для элемента «Группы»

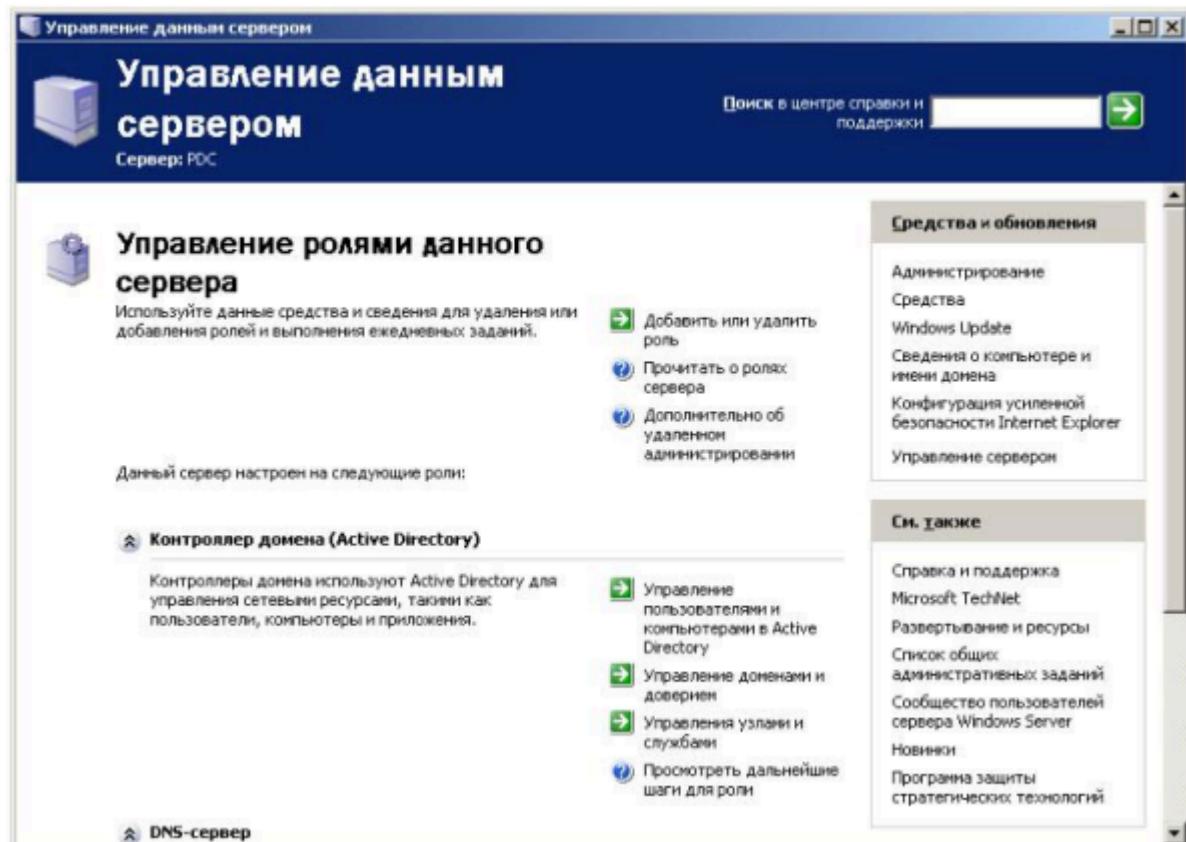


Нажать «OK». Ввести имя группы «Операторы» и нажать «OK» два раза. Параметр безопасности будет изменен.

### Работа с доменом

Для управления доменными учетными записями необходимо войти в систему на контроллере домена с учетной записью администратора.

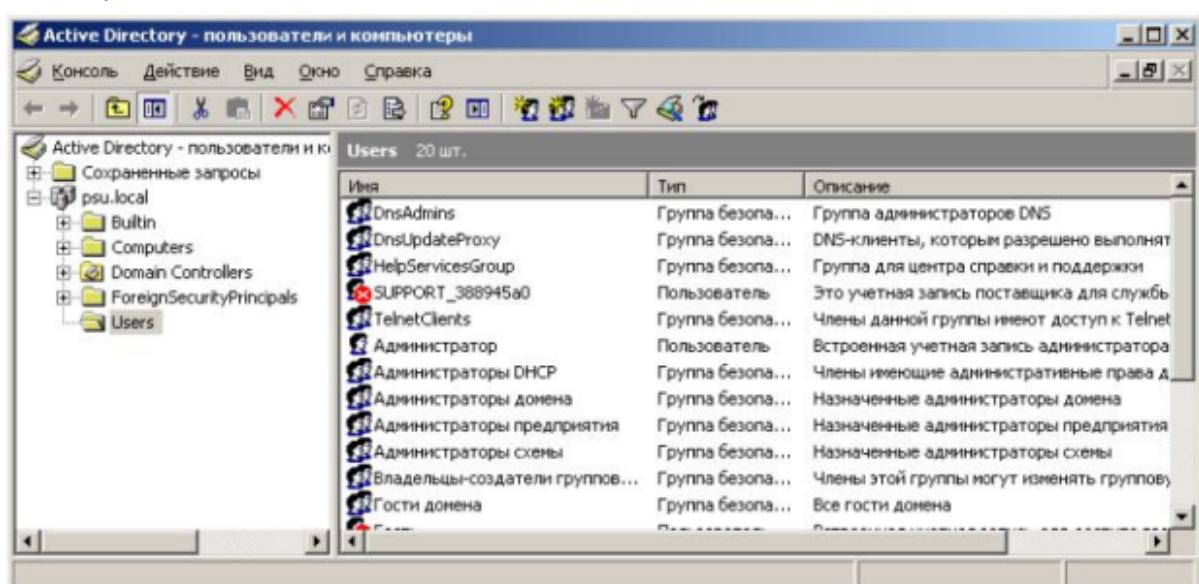
Важно убедиться, что в поле «Вход в» выбрано имя домена. Если данное поле не отображается, нужно нажать на кнопку «Параметры», чтобы отобразить дополнительные поля. Нажать кнопку «OK». Откроется рабочий стол пользователя. Также автоматически запускается утилита «Управление данным сервером»



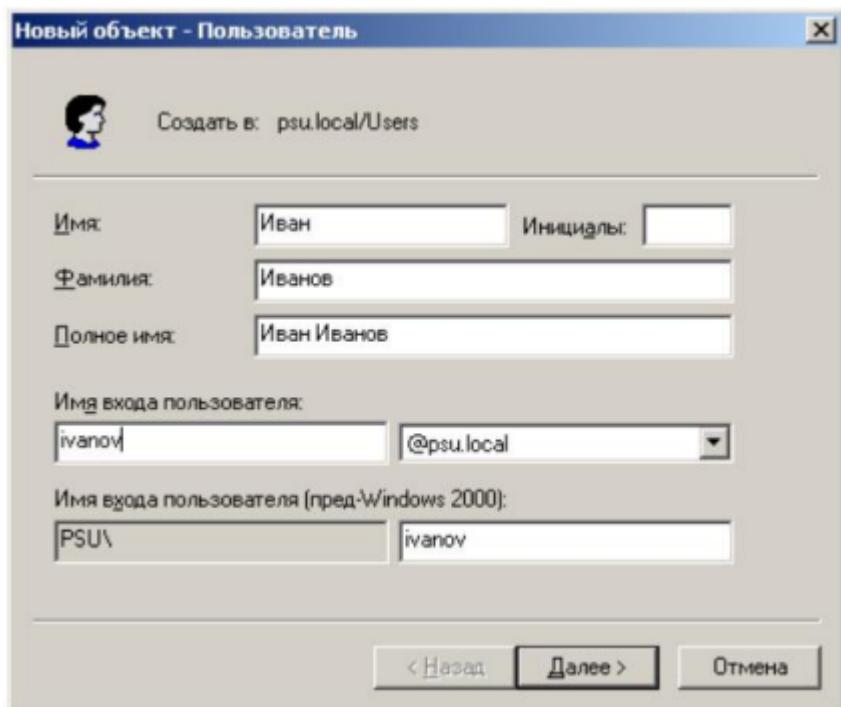
Если данная программа не запускается автоматически, ее можно запустить из меню «Пуск», подменю «Администрирование».

### Создание учетной записи пользователя в домене

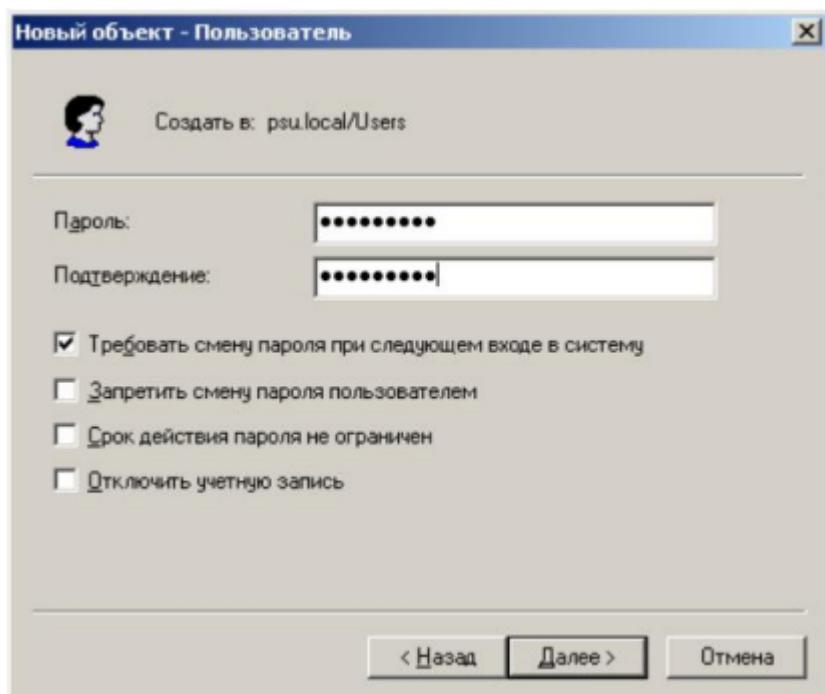
В утилите «Управление данным сервером» щелкнуть по ссылке «Управление пользователями и компьютерами в Active Directory». Откроется консоль «Active Directory – пользователи и компьютеры»



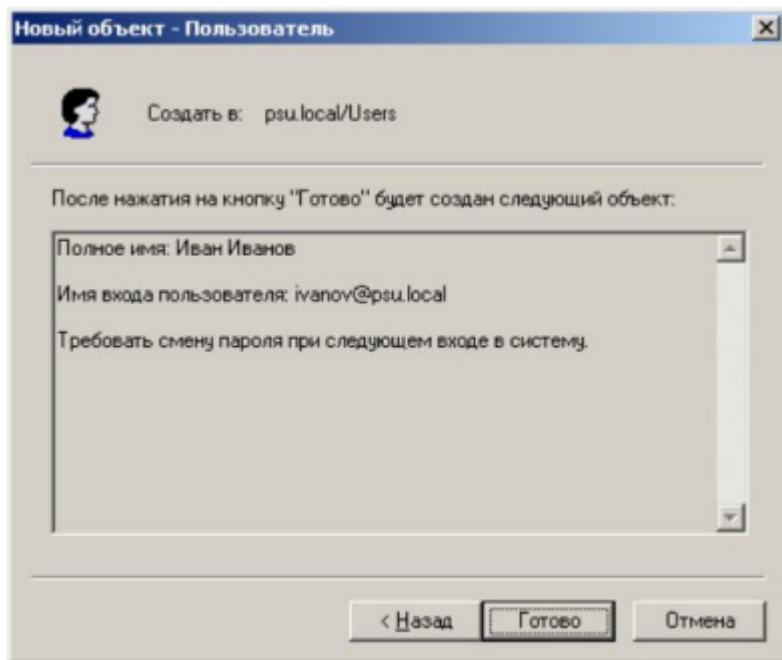
Для того, чтобы создать учетную запись пользователя домена, в левой части окна нужно перейти в папку «Users», нажатием правой кнопки мыши вызвать контекстное меню и выбрать «Создать» > «Пользователь». Откроется мастер создания нового пользователя



Ввести имя и фамилию пользователя, ввести имя входа. Нажать кнопку «Далее». Откроется второй шаг мастера



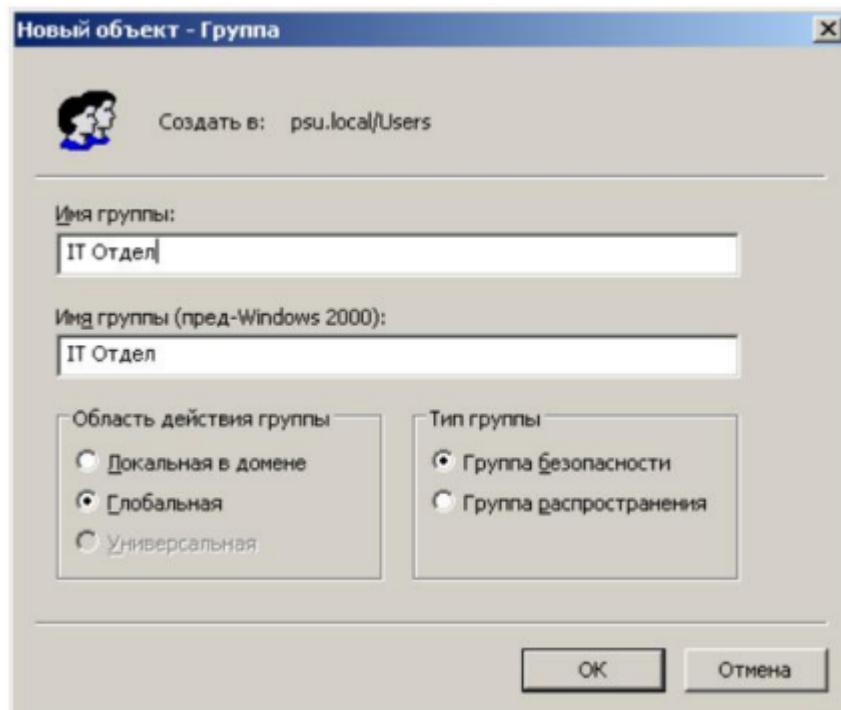
Ввести пароль и подтверждение пароля. Нажать кнопку «Далее». Откроется последний шаг мастера



Нажать кнопку «Готово». Учетная запись пользователя создана

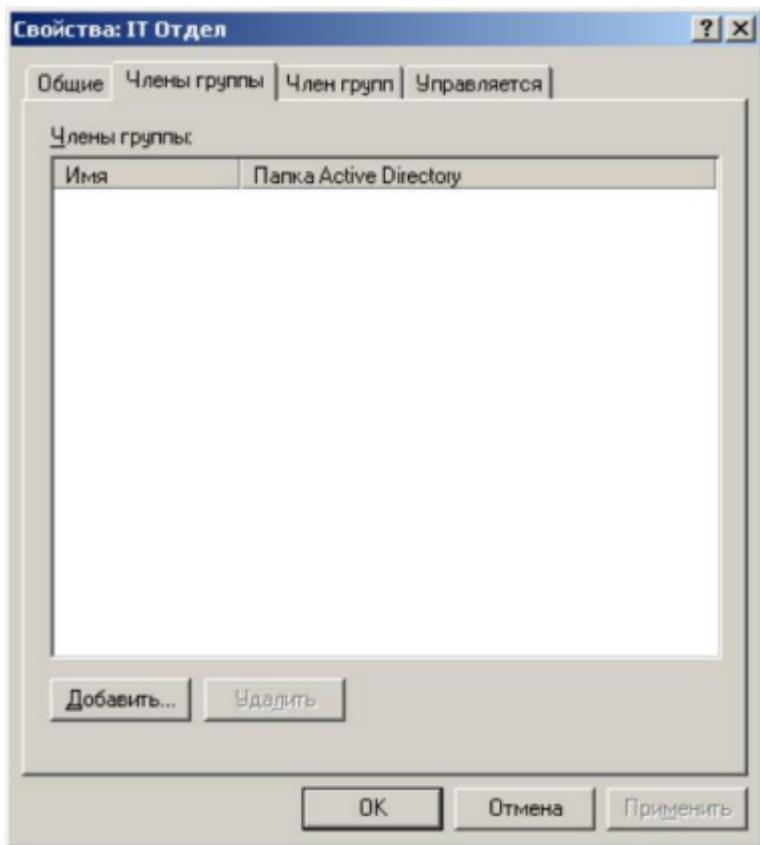
### Создание группы в домене

Группы располагаются в том же контейнере, что и пользователи домена. Для создания группы в контекстном меню необходимо выбрать «Создать» > «Группа»



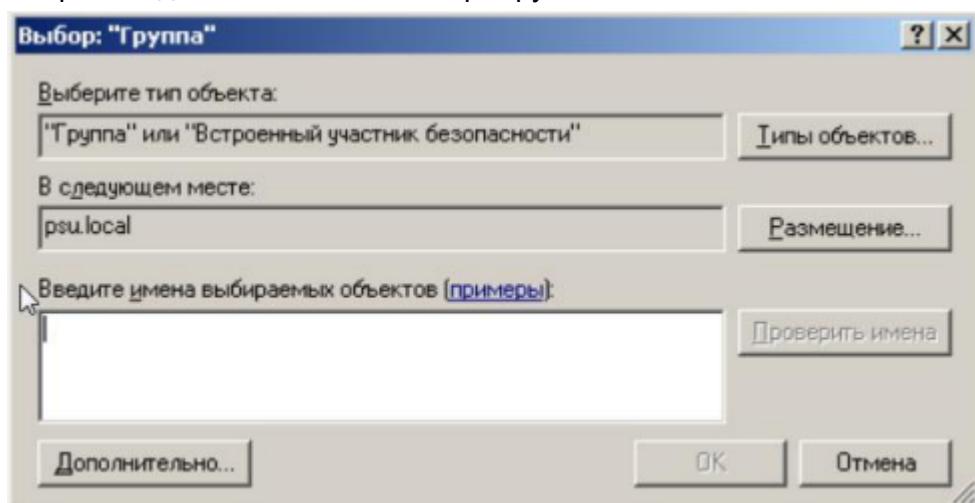
Ввести имя группы. Поле «Имя группы (пред-Windows2000)» заполнится автоматически, нет необходимости менять его значение. Выбрать тип группы «Группа безопасности», область действия группы «Глобальная». Глобальные группы используются для объединения пользователей по функциональному или географическому признаку, локальные группы – для назначения доступа к ресурсам.

Нажать «OK». Создана новая группа. Изначально новая группа пуста. Щелкнуть правой кнопкой мыши по имени группы в списке и в контекстном меню выбрать «Свойства». В открывшемся окне свойств группы переключиться на вкладку «Члены группы»



Нажать кнопку «Добавить...» и в появившемся окне выбрать пользователей, которых необходимо добавить в группу. Нажать «OK» два раза.

Альтернативный способ добавления пользователя в группу: щелкнуть правой кнопкой мыши на имени пользователя в списке и в контекстном меню выбрать «Добавить в группу». Откроется диалоговое окно выбора группы



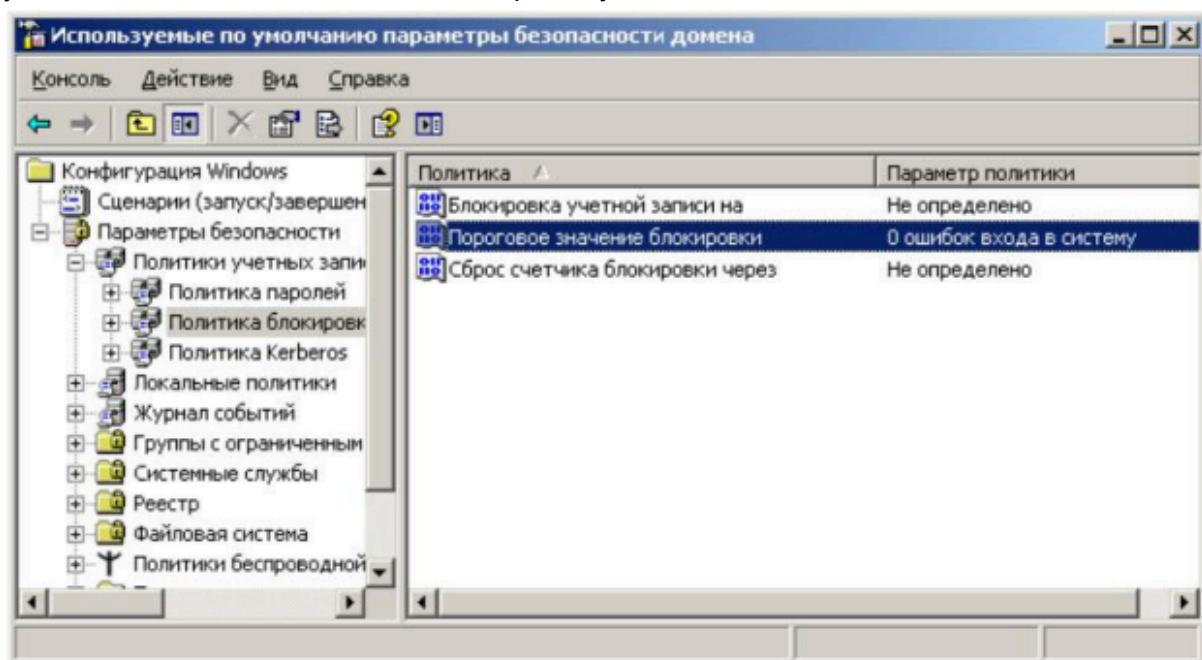
Ввести имя группы, нажать кнопку «Проверить имена». Затем нажать кнопку «OK». В отличие от локальных групп пользователей, группы домена могут быть членами других групп.

## Управление политикой безопасности домена

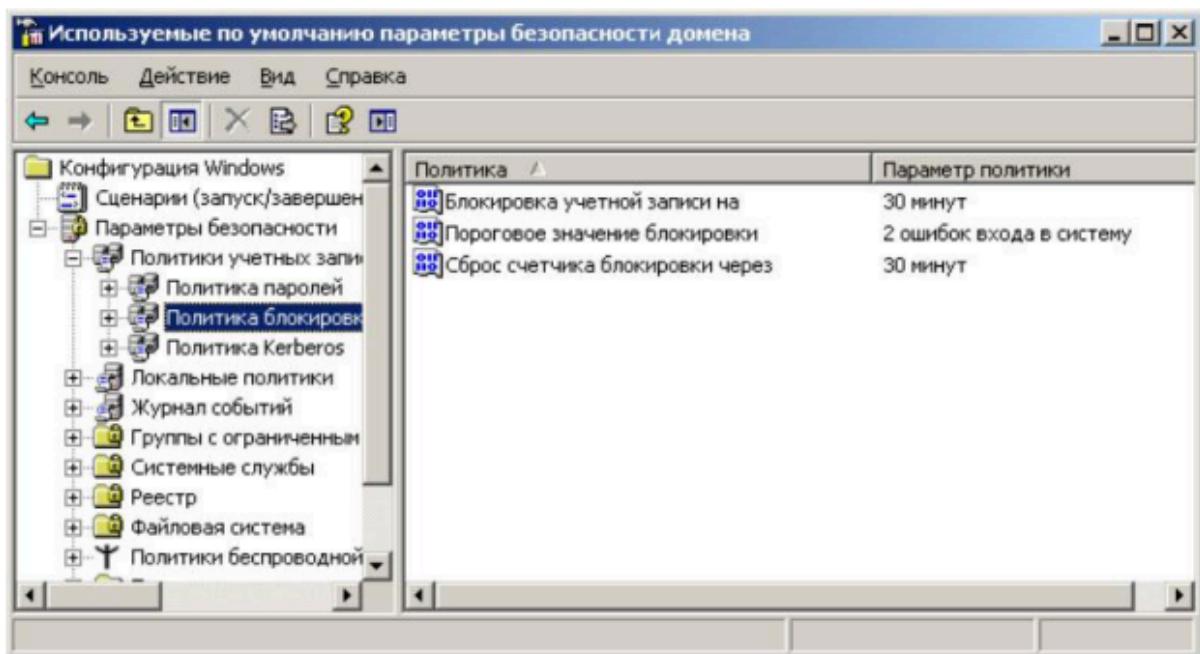
Управление политикой безопасности домена будет рассмотрено на примере настройки параметров автоматической блокировки учетных записей.

Блокировка учетных записей — это средство защиты учетной записи от подбора пароля по словарю или методом грубой силы.

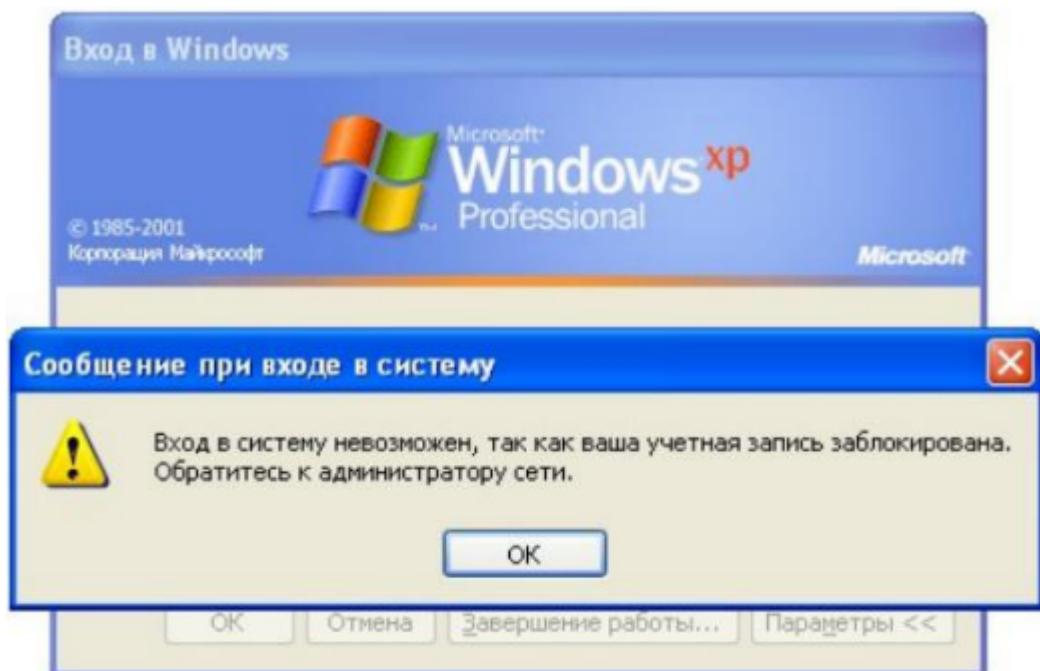
Множественные неудачные попытки входа пользователя могут сигнализировать об атаке подбора пароля пользователя. Чтобы предотвратить реализацию этой атаки, учетная запись пользователя блокируется после некоторого количества неудачных попыток. Через заданный интервал времени учетная запись будет автоматически разблокирована. До истечения этого времени учетную запись может разблокировать администратор. Для настройки параметров блокировки учетных записей домена в меню «Пуск» следует выбрать пункт «Администрирование», подпункт «Политика безопасности домена». Перейти в папку «Параметры безопасности» > «Политики учетных записей» > «Политика блокировки учетной записи»



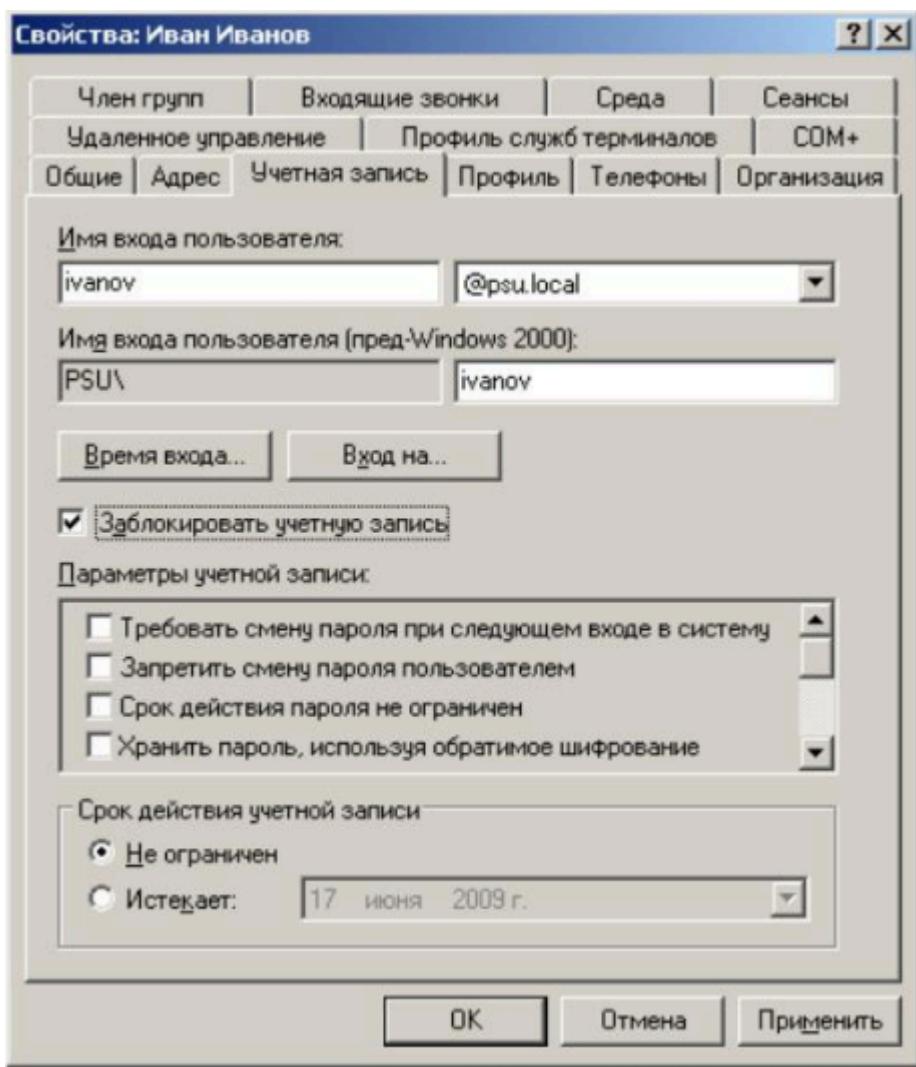
Изначально блокировка учетных записей отключена. Двойным щелчком мыши по названию параметра можно открыть окно для изменения его значения. Установить пороговое значение блокировки равное двум, а два остальных параметра равные 30 минутам. Параметры примут вид



Теперь после двух неудачных попыток войти в систему учетная запись пользователя будет заблокирована, и система не разрешит войти в систему даже с правильным паролем. При попытке войти в систему отобразится сообщение



Учетная запись будет автоматически разблокирована через 30 минут .Администратор домена может вручную разблокировать учетную запись до истечения этого времени. Для этого нужно открыть консоль «ActiveDirectory– пользователи и компьютеры», перейти в папку «Users», двойным щелчком по имени пользователя в списке открыть свойства пользователя и перейти на вкладку «Учетная запись». Снять флагок «Заблокировать учетную запись»



### Разрешения для папок NTFS

Таблица 2.1 – Разрешения для папок NTFS

Разрешения для	Права пользователя

папок в NTFS	
Чтение (Read)	Просматривать файлы и папки, а также список владельцев, разрешения и атрибуты папки (такие, как «Только чтение», «Скрытый», «Архивный» и «Системный»).
Запись (Write)	Создавать новые файлы и папки внутри папки, изменять атрибуты папки и просматривать владельцев и разрешения для папки.
Список содержимого папки (List Folder Contents)	Просматривать имена файлов и папок.
Чтение и выполнение (Read & Execute)	Перемещаться по структуре папок в поисках других файлов или папок, даже если пользователь не обладает разрешением на доступ к просматриваемым папкам. Выполнять все действия, право на которые дают разрешения «Чтение» и «Список содержимого папки».
Изменить (Modify)	Удалять папки и выполнять все действия, право на которые дают разрешения «Запись» и «Чтение и выполнение».
Полный доступ (Full Control)	Изменять разрешения, менять владельца, удалять папки и файлы и выполнять действия, право на которые дают все остальные разрешения NTFS для папок.

Таблица 2.2 – Разрешения для файлов NTFS

Разрешения для файлов в NTFS	Права пользователя
Чтение (Read)	Просматривать файл, а также список владельцев, разрешения и атрибуты файла.
Запись (Write)	Перезаписывать файл, изменять атрибуты файлов и просматривать владельцев и разрешения.
Чтение и выполнение (Read & Execute)	Запускать приложения и выполнять все действия, право на которые дает разрешение «Чтение».
Изменить (Modify)	Изменять и удалять файл, а также выполнять все действия, право на которые дают разрешения «Запись» и «Чтение и выполнение».
Полный доступ (Full Control)	Изменять разрешения, менять владельца и выполнять действия, право на которые дают все остальные разрешения NTFS для файлов.

### Подсистема аудита в ОС Windows 2000/XP

Подсистема аудита (Auditing) — это инструмент, предназначенный для поддержания безопасности в сети и позволяющий отслеживать действия пользователей, а также системные события. Он является одной из функций групповой политики Windows 2000/XP.

Аудит позволяет отслеживать на компьютере как действия пользователей, так и действия ОС Windows XP, называемые событиями(Events). Средствами аудита можно задать режим, при котором WindowsXP регистрирует события в журнале безопасности

(Security Log). В нем хранятся записи об успешных и неудачных попытках входа в систему и о таких событиях, как создание, открытие и закрытие файлов или других объектов.

Запись аудита в журнале безопасности содержит данные о:

- выполненных операциях;
- пользователях, выполнивших операцию;
- успешном или неуспешном результате операции;
- времени, когда произошло данное событие.

Политика аудита (Audit Policy) задает типы событий системы безопасности, которые Windows XP регистрирует в журнале безопасности каждого компьютера. Система Windows XP регистрирует событие в журнале безопасности того компьютера, на котором событие происходит. Так, каждый раз, когда кто-нибудь пытается войти в систему и попытка входа оказывается неудачной, Windows XP регистрирует событие в журнале безопасности данного компьютера. Можно настроить политику аудита для данного компьютера на выполнение следующих операций:

- выявление успешных или неудачных действий, например, попыток входа пользователей в систему или попытки отдельного пользователя прочитать указанный файл, попытки изменения учетной записи пользователя или принадлежности к группе, попытки изменение параметров безопасности;
- исключение или минимизация риска неавторизованного использования ресурсов.

Для просмотра событий, зарегистрированных системой Windows XP в журнале безопасности, используется утилита «Просмотр событий» (Event Viewer). Можно также сохранять файлы журнала в архиве для выяснения закономерностей за указанный период времени — например, чтобы определить частоту использования принтеров или файлов или выявление попыток неавторизованного использования ресурсов.

### **Определение событий, подлежащих регистрации**

При планировании политики аудита нужно определить, какие события следует регистрировать и на каких компьютерах надо установить аудит. По умолчанию аудит отключен. Когда известно, на каких компьютерах он требуется, нужно также определить, какие события регистрировать на каждом из них. Windows XP регистрирует события, подлежащие аудиту, отдельно на каждом компьютере. Можно регистрировать следующие типы событий:

- попытки доступа к файлам и папкам;
- начало и завершение сеанса пользователя;
- выключение компьютера с Windows XP;
- запуск компьютера с Windows XP;
- изменения учетных записей пользователей и групп;
- попытки изменения объектов AD (только если компьютер с Windows XP является частью домена).

После того как типы регистрируемых событий заданы, нужно определить, регистрировать ли успешные действия, неудавшиеся попытки или оба вида событий. Отслеживание успешных действий дает информацию о том, как часто система Windows XP или пользователи обращаются к конкретным файлам, принтерам или другим объектам; эта информация пригодится для планирования ресурсов.

Регистрация неудачных попыток позволяет выявить слабые места в защите системы.

Так, если зафиксировано несколько неудачных попыток входа в систему под определенным именем пользователя, особенно в нерабочее время, можно предположить, что неавторизованный пользователь пытается атаковать систему. Кроме того, при выборе политики аудита следует руководствоваться правилами, описанными далее:

- следует определить, нужно ли отслеживать закономерности загрузки системы. Если да, то предусмотреть сохранение журналов событий в архиве. Это позволит контролировать распределение загрузки по времени и заранее планировать увеличение ресурсов системы;
- часто просматривать журналы безопасности. Обязательно установить расписание и регулярно просматривать журналы безопасности, так как выполнение аудита сама по себе не предупреждает о слабых местах в защите системы;
- задать информативную и работоспособную политику аудита. Всегда регистрировать попытки доступа к важным данным. Регистрировать только те события, которые дают существенную информацию. Это снижает потребление ресурсов компьютера до минимума и упрощает поиск нужной информации. Регистрация большого числа событий может привести к чрезмерной трате системных ресурсов ОС.

### **Реализация политики аудита**

Для установки и администрирования аудита необходимо:

- иметь право пользователя «Управление аудитом и журналом безопасности» на том компьютере, на котором планируется установить политику аудита или просмотреть журнал безопасности. По умолчанию в Windows XP такие права имеет группа «Администраторы»;
  - разместить файлы и папки, аудит которых планируется, на томах с файловой системой NT (NTFS).
- Настройка аудита выполняется в два этапа, описанных далее.
- 1) Задание политики аудита. Политика аудита разрешает аудит объектов, но не инициирует аудит заданных объектов.
  - 2) Разрешения аудита заданных ресурсов. Для файлов, папок, принтеров и объектов AD назначаются конкретные события, подлежащие регистрации. После этого Windows XP начинает отслеживать заданные события и регистрировать их в журнале.

### **Примеры**

#### **Изменение разрешений NTFS**

Администраторы, пользователи с разрешением «Полный доступ» и владельцы файлов и папок могут устанавливать разрешения для отдельных пользователей и групп. Для установки или изменения разрешения NTFS для файла или папки на вкладке Безопасность (Security) диалогового окна свойств файла или папки необходимо настроить параметры

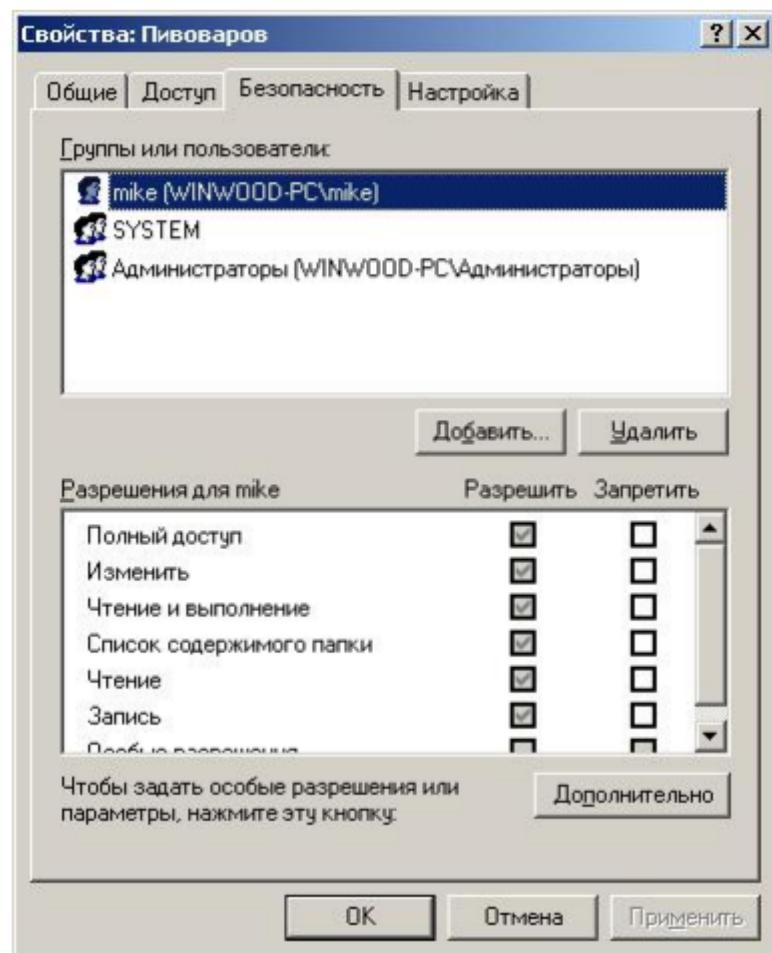


Таблица 2.3 – Опции вкладки Безопасность

Параметр	Назначение
Группы или пользователи (Group Or User Name)	Позволяет выделить пользователя или группу, для которой нужно изменить разрешения, или которых нужно удалить из списка.
Разрешения для ... (Permissions For)	Устанавливает и запрещает разрешения. Нужно отметить флажок «Разрешить» для назначения разрешения или флажок «Запретить» для запрета разрешения.
Добавить (Add)	Открывает диалоговое окно «Выбор: пользователи или группы», в котором можно выбрать пользователей или группы для добавления их к списку «Группы или пользователи», показанному на рисунке 2.2.
Удалить (Remove)	Удаляет выделенного пользователя или группу и соответствующие разрешения для файла или папки.
Дополнительно (Advanced)	Открывает диалоговое окно «Дополнительные параметры безопасности» для выделенной папки. В открывшемся окне можно назначать или запрещать особые разрешения, как показано на рисунке 2.3.

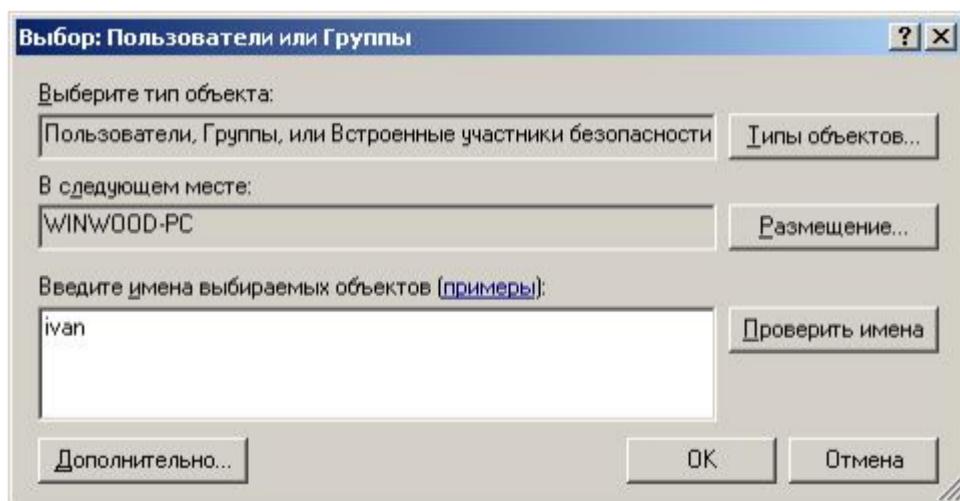
## Добавление пользователей или групп в список управления доступом

Нажать кнопку «Добавить» для открытия диалогового окна «Выбор: пользователи или группы», показанного на рисунке 2.2. Это диалоговое окно используется для добавления пользователей или групп, для которых необходимо назначать разрешения на доступ к папке или файлу. Параметры, доступные в диалоговом окне «Выбор: пользователи или группы», описаны в таблице 2.4

Таблица 2.4 – Параметры диалогового окна «Выбор: пользователи или группы»

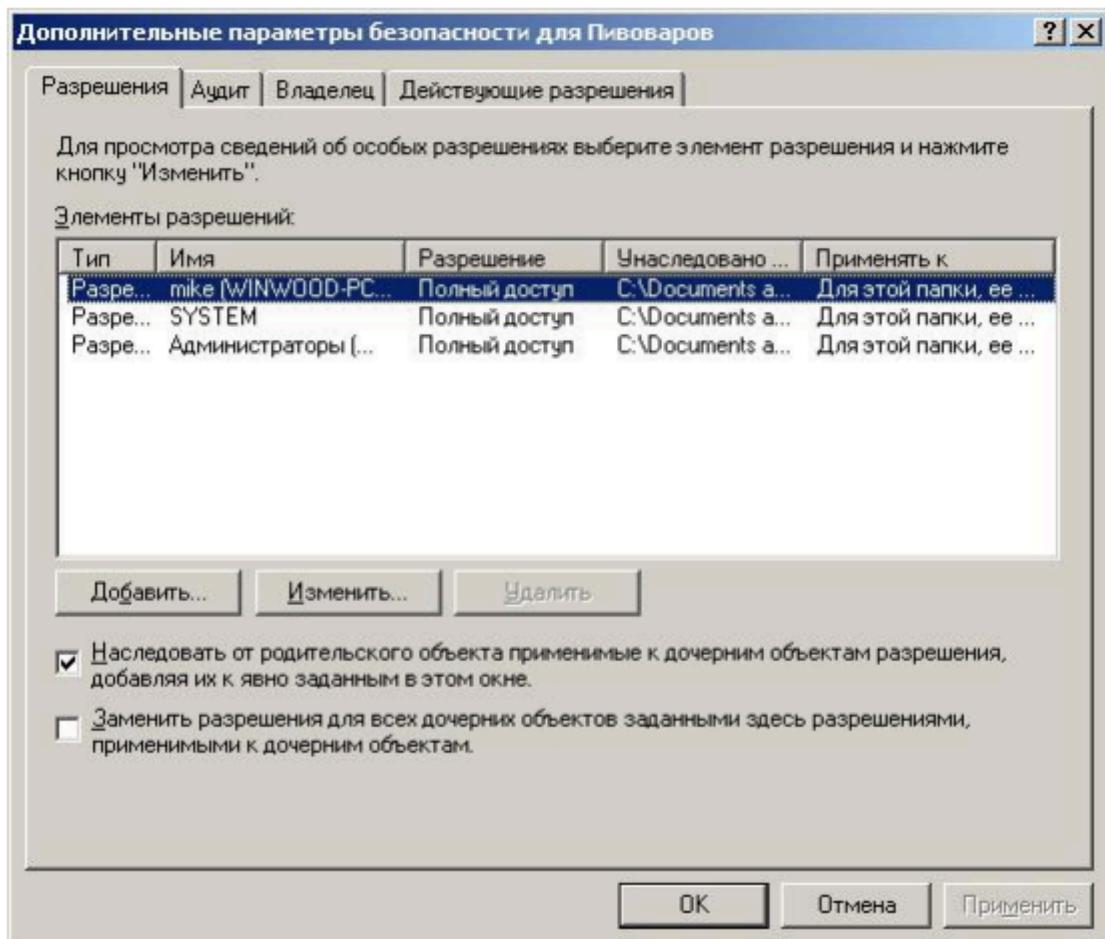
Параметр	Назначение
Выберите тип объектов (Select The Object Type)	Позволяет выбрать тип объекта, например встроенные участники безопасности (пользователи, группы и учетные записи отдельных компьютеров), пользователи или группы.
В следующем месте (From This Location)	Указывает текущую область поиска, например в домене или на локальном компьютере.
Размещение (Locations)	Позволяет выбрать область поиска, например в домене или на локальном компьютере.
Введите имена выбираемых объектов (Enter The Object	Позволяет ввести список тех встроенных участников безопасности, пользователей и групп, которых необходимо добавить.

Names To Select)	
Проверить имена (Check Names)	Проверяет выделенный список встроенных участников безопасности, пользователей и групп, которых необходимо добавить.
Дополнительно (Advanced)	Позволяет получить доступ к дополнительным возможностям поиска, включая возможность поиска удаленных учетных записей пользователей, учетных записей с неустаревшими паролями и учетных записей, по которым не подключались определенное количество дней.

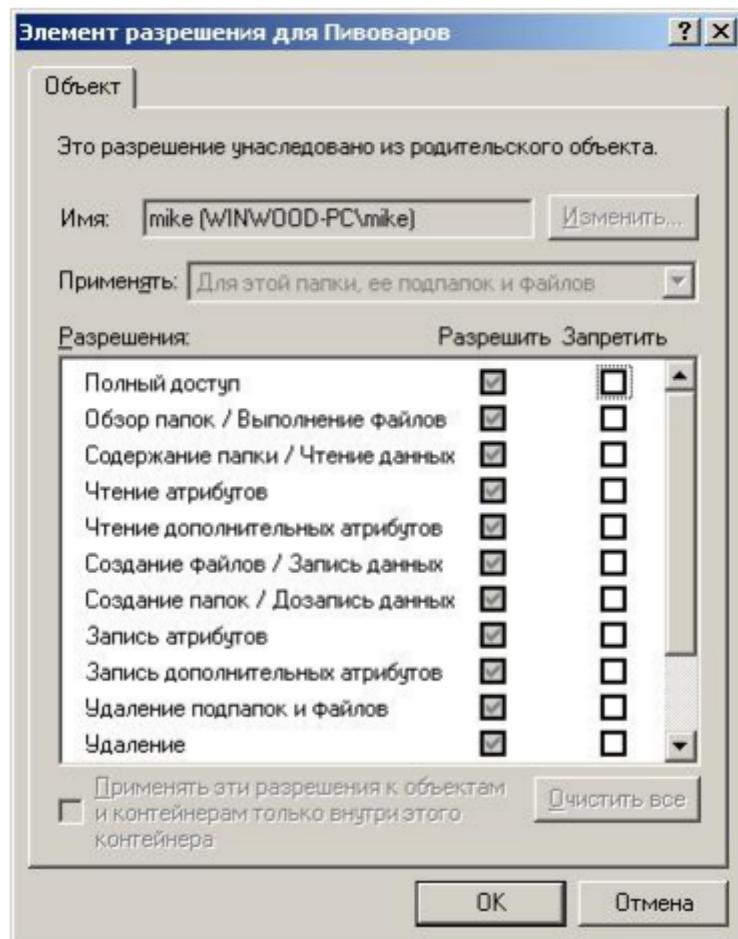


## Назначение или запрещение особых разрешений

Нажать кнопку «Дополнительно», чтобы открыть диалоговое окно «Дополнительные параметры безопасности», показанное на рисунке 2.3, где перечислены группы и пользователи и установленные для них разрешения для этого объекта. В поле «Элементы разрешений» также указано, от какого объекта разрешения унаследованы и к каким объектам применимы



Также можно воспользоваться диалоговым окном «Дополнительные параметры безопасности» для изменения разрешений, установленных для пользователя или группы. Для изменения разрешений, установленных для пользователя или группы, необходимо выделить пользователя и нажать кнопку «Изменить». Откроется диалоговое окно «Элемент разрешения для ...», показанное на рисунке 2.4. Затем выделить или отменить определенные разрешения



## Смена владельца объекта

Разрешается передавать право владельца файлов и папок от одного пользователя к другому. Администратор может предоставить кому-либо право смены владельца или самостоятельно сменить владельца файла или папки.

Для смены владельца файла или папки действуют определенные правила:

- текущий владелец или любой пользователь с разрешением «Полный доступ» может установить стандартное разрешение «Полный доступ» или особое разрешение доступа «Смена владельца» для другого пользователя или группы, позволяя пользователю или любому члену группы стать владельцем;
- администратор имеет право сменить владельца папки или файла независимо от назначенных разрешений. Если администратор становится владельцем, группа «Администраторы» также становится владельцем, и любой из членов группы «Администраторы» может изменять разрешения для файла или папки и назначать разрешение «Смена владельца» другому пользователю или группе.

Например, если сотрудник уволился из организации, то администратор может изменить владельца для файлов данного сотрудника и назначить разрешение «Смена владельца» другому сотруднику, который и станет владельцем этих файлов.

Чтобы сменить владельца файла или папки, пользователь или член группы с разрешением «Смена владельца» должен явно назначить нового владельца. Для этого необходимо выполнить действия, описанные далее.

- 1) На вкладке «Безопасность» диалогового окна свойств файла или папки нажать кнопку «Дополнительно».
- 2) В открывшемся диалоговом окне «Дополнительные параметры безопасности», на вкладке «Владелец», в списке «Изменить владельца на», выбрать нужное имя.
- 3) Установить флажок «Заменить владельца субконтейнеров и объектов» для того, чтобы стать владельцем всех подпапок файлов, содержащихся в папке. Затем нажать кнопку «OK».

### **Предотвращение наследования разрешений**

По умолчанию подпапки и файлы наследуют разрешения, установленные для родительской папки. Признаком этого служит установленный флажок «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне». В диалоговом окне «Дополнительные параметры безопасности». Для предотвращения наследования разрешений от родительской папки следует снять этот флажок. При этом необходимо выбрать один из вариантов, описанных в таблице 2.6.

**Таблица 2.6 – Параметры предотвращения наследования разрешений**

Параметр	Назначение
Копировать (Copy)	Копирует разрешения, которые были ранее переданы от родительского объекта к дочерним объектам, затем запрещает последующее наследование разрешений от родительской папки.
Удалить (Remove)	Удаляет разрешения, которые были ранее переданы от родительского объекта к дочерним объектам, и сохраняет только те разрешения, которые явно установлены здесь.
Отмена (Cancel)	Закрывает диалоговое окно.

### **Установка политики аудита**

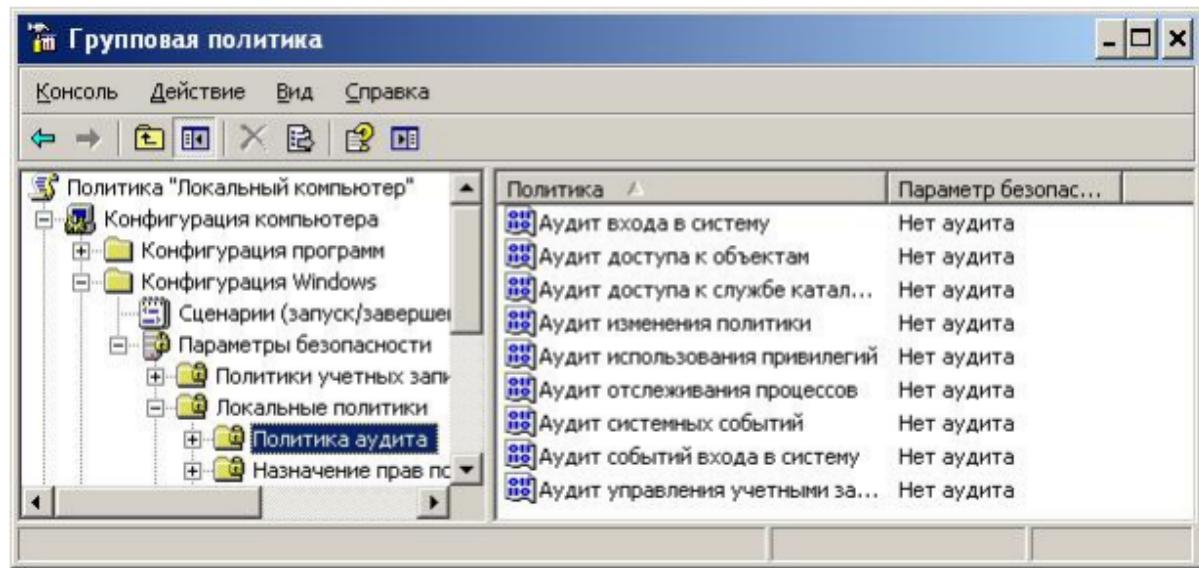
На первом этапе установки политики аудита в Windows XP необходимо выбрать типы событий, подлежащих регистрации. Для каждого регистрируемого события в параметрах указывается, какие попытки следует отслеживать — успешные или неудачные. Политика аудита на локальном компьютере устанавливается средствами оснастки «Групповая политика», которую можно запустить, используя консоль управления MMC (Microsoft Management Console) и добавив в консоль оснастку «Групповая политика». Кроме того, для локального компьютера уже есть предустановленная консоль управления групповой политикой локального компьютера — gpedit.msc. В таблице 2.7 перечислены типы событий, регистрируемые в Windows XP

Таблица 2.7 – Типы событий, регистрируемых Windows XP

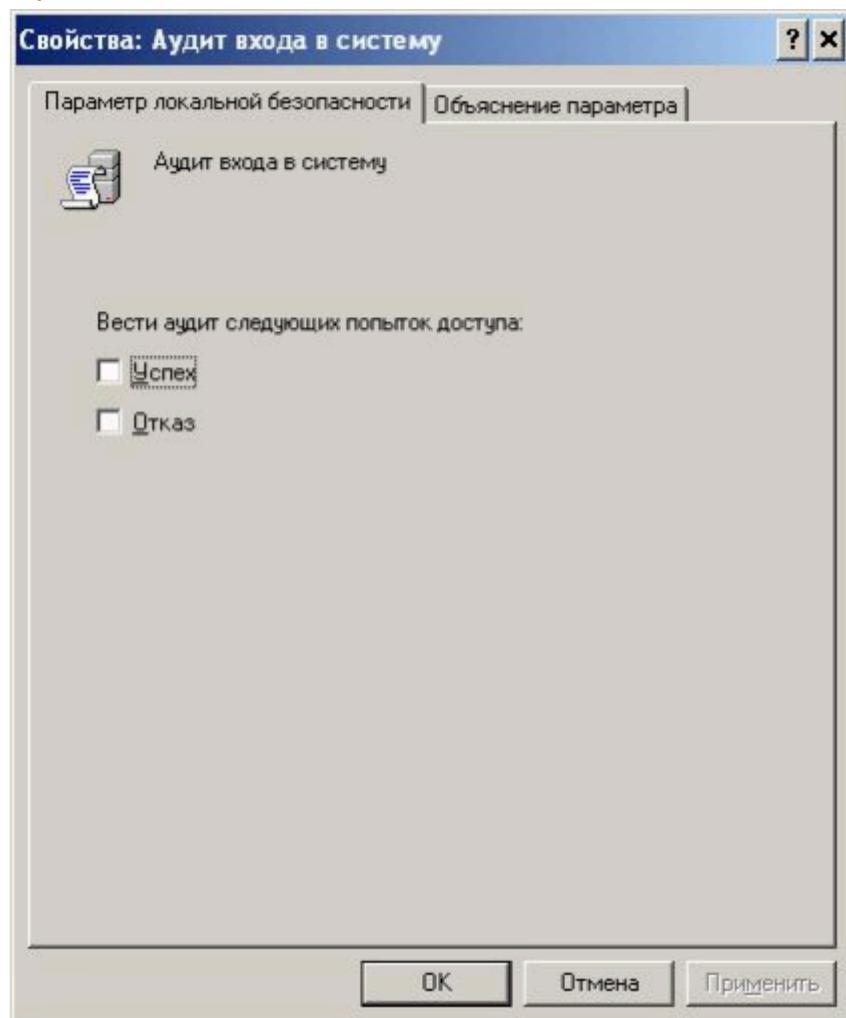
Событие	Описание
Вход в систему под заданной учетной записью	Контроллер домена получил запрос на проверку учетной записи пользователя (применяется только в тех случаях, когда компьютер с Windows XP входит в домен Microsoft Windows 2000).
Управление учетными записями	Администратор создал, изменил или удалил учетную запись пользователя или группу. Некоторая учетная запись была переименована, отключена или включена, или для нее был назначен или изменен пароль.
Доступ к службе каталогов	Пользователь получил доступ к объекту AD. Для регистрации событий этого типа нужно сконфигурировать аудит для определенных объектов AD (Только если компьютер с Windows XP входит в домен Microsoft Windows 2000).
Вход в систему	Пользователь локально вошел в систему, или вышел из нее, или подключился к компьютеру через сеть (или отключился от него).
Доступ к объектам	Пользователь получил доступ к файлу, папке или принтеру. Определенные файлы, папки или принтеры должны быть настроены для аудита. В этом случае регистрируется доступ пользователей к файлам, папкам и принтерам.
Изменение системной политики	Изменены пользовательские параметры безопасности, права пользователя или политика аудита.
Использование привилегий	Пользователь применил права, например, изменил системное время (в этом случае не подразумеваются права, связанные с регистрацией в системе или с завершением сеанса).
Отслеживание процесса	Программа выполнила действие. Эта информация важна главным образом для программистов, которым нужно детально проследить выполнение программы.
Системные события	Пользователь перезапустил или выключил компьютер, или произошло событие, повлиявшее на безопасность Windows XP или на журнал безопасности. Например, журнал аудита переполнился и Windows XP начинает игнорировать поступающие сообщения о событиях.

Для установки политики аудита на компьютере с Windows XP следует запустить оснастку «Групповая политика», как описано далее.

- 1) Войти в систему, используя учетную запись пользователя, входящего в группу «Администраторы».
- 2) Открыть меню «Пуск», выбрать пункт «Выполнить». В открывшемся окне ввести команду «gpedit.msc» и нажать «OK».
- 3) Двойным щелчком открыть пункт «Конфигурация компьютера», затем «Конфигурация Windows».
- 4) Двойным щелчком открыть «Параметры безопасности», затем «Локальные политики».
- 5) Двойным щелчком открыть папку «Политика аудита». В правой панели консоли отобразятся текущие параметры политики аудита, как показано на рисунке 2.5.



6) Выбрать тип события для аудита, затем в меню «Действие» выбрать пункт «Свойства». Так, если в списке указать «Аудит входа в систему» и в меню «Действие» выбрать пункт «Свойства», появится окно «Свойства: аудит входа в систему», как показано на рисунке 2.6.



7) Установить флажок «Успех», флажок «Отказ» или оба флажка. Если выбран флажок «Успех», то включен аудит успешных попыток. Если выбран флажок «Отказ», то включен аудит неудачных попыток.

8) Нажать кнопку «OK».

9) Перезапустить компьютер. После настройки параметров политики аудита следует иметь в виду, что изменения в политике аудита компьютера вступают в силу только после перезагрузки.

Для введения политики в действие без перезагрузки компьютера можно использовать команду gpupdate.

### **Аудит доступа к файлам и папкам**

Если требуется выявить слабые места в защите локальной сети, можно установить аудит файлов и папок, расположенных на разделах NTFS. Для аудита доступа пользователей к файлам и папкам прежде всего следует настроить политику аудита на регистрацию доступа к объектам, в том числе файлов и папок.

При настройке политики аудита на регистрацию доступа к объектам включается аудит конкретных файлов и папок. При этом также указывается, какие виды доступа, пользователи и группы подлежат аудиту.

Чтобы включить аудит конкретных файлов или папок, нужно выполнить действия, описанные далее

- 1) В меню «Пуск» щелкнуть правой клавишей мыши элемент «Мой компьютер» и выбрать в контекстном меню пункт «Проводник».
- 2) Щелкнуть правой клавишей мыши по файлу или папке, для которой нужно включить аудит, и выбрать пункт контекстного меню «Свойства».
- 3) На вкладке «Безопасность» диалогового окна «Свойства» нажать кнопку «Дополнительно».
- 4) На вкладке «Аудит» в диалоговом окне «Дополнительные параметры безопасности» нажать кнопку «Добавить», выбрать пользователей, для которых требуется включить аудит доступа к файлами папкам, и нажать кнопку «OK».
- 5) В диалоговом окне «Элемент аудита для ...» установить флажок «Успех», флажок «Отказ» или оба флажка, чтобы указать тип событий для аудита. На рисунке 2.7 показан список событий, аудит которых возможен для папок. В таблице 2.8 перечислены действия пользователей, вызывающие соответствующие события, что поможет определить, в каких случаях следует включать аудит этих событий.

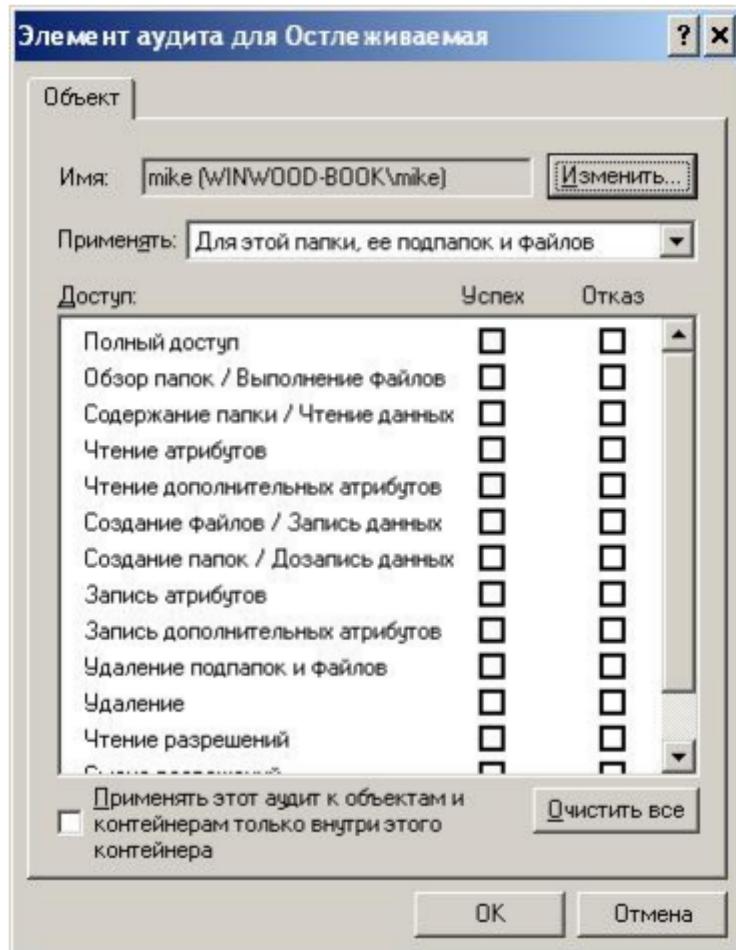


Таблица 2.8 – События для файлов и папок, вызываемые действиями пользователей

Событие	Действие пользователя, вызвавшее событие
Переход в папку / Выполнение файла	Запуск программы или получение доступа к папке при смене текущей папки.
Получение списка файлов / Чтение данных	Просмотр содержимого файла или папки.
Чтение атрибутов	Просмотр атрибутов файла или папки.
Чтение расширенных атрибутов	Просмотр атрибутов файла или папки.
Создание файлов / Запись данных	Изменение содержимого файла или создание новых файлов в папке.
Создание папок / Добавление данных	Создание папок внутри папок.
Запись атрибутов	Изменение атрибутов файла или папки.
Запись расширенных атрибутов	Изменение атрибутов файла или папки.
Удаление вложенных папок и файлов	Удаление файла или папки внутри папки.
Удаление	Удаление файла или папки.
Чтение разрешений	Просмотр прав владельца файла на файл или папку.
Смена разрешений	Изменение прав доступа к файлу или папке.

**Смена владельца**

**Изменить право владельца на файл или папку.**

- 6) Нажать кнопку «OK», чтобы вернуться в диалоговое окно «Дополнительные параметры безопасности». По умолчанию все изменения параметров аудита, выполненные для родительской папки, относятся также и ко всем дочерним папкам и всем файлам в родительской и дочерних папках.
- 7) Чтобы запретить изменения параметров аудита для текущей папки при изменении параметров родительской папки, необходимо снять флажок «Наследовать от родительского объекта: Параметры аудита, применимые к дочерним объектам».
- 8) Нажать кнопку «OK».

### **Просмотр журнала безопасности**

В журнале безопасности хранится информация о событиях, которые отслеживаются политикой аудита, например, неудачные и успешные попытки регистрации в системе. Чтобы просмотреть журнал безопасности, необходимо выполнить действия, описанные далее.

- 1) Нажать кнопку «Пуск», затем «Выполнить». В открывшемся окне ввести команду «eventvwr.msc» и нажать кнопку «OK».
- 2) В дереве консоли утилиты просмотра событий выбрать пункт «Безопасность». В правой панели отобразится список элементов журнала с кратким описанием каждого элемента, как показано на рисунке 2.8. Успешные попытки условно обозначены значком ключа, а неудачные—значком замка. Кроме того, указаны дата и время события, категория события и пользователь, действие которого вызвало данное событие. В колонке «Категория» отображается тип события, например, доступ к объекту управления учетными записями, доступ к службе каталогов или попытка регистрации в системе.

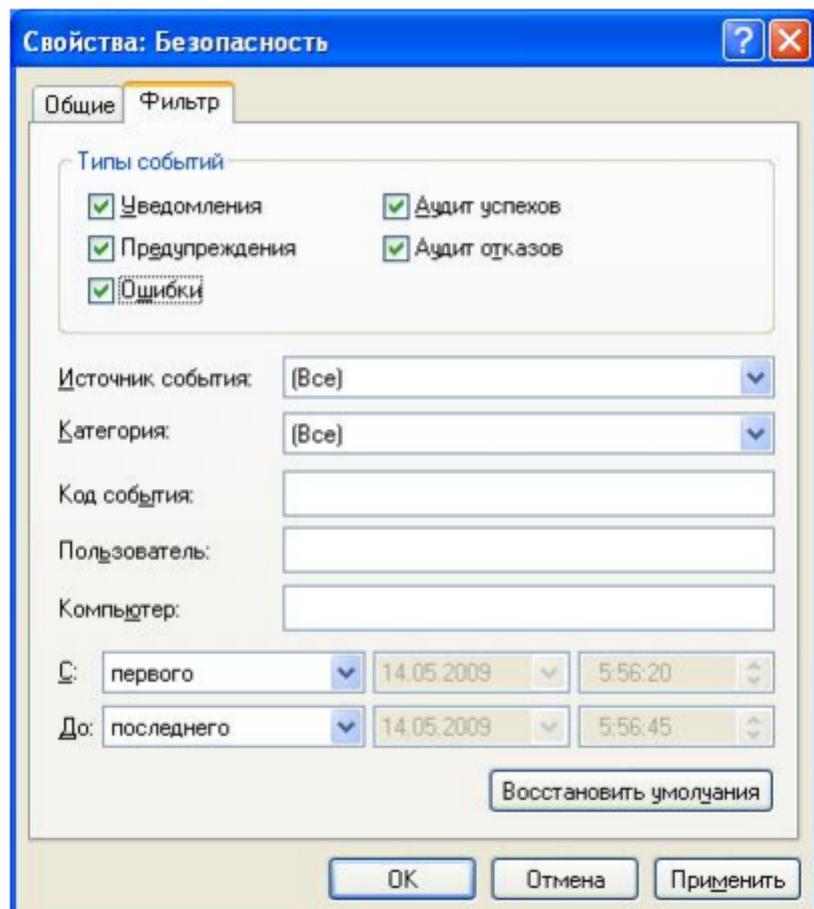
Безопасность 6 событий							
Тип	Дата	Время	Источник	Категория	Соб...	Пользователь	Компью...
Аудит успехов	14.05.2009	5:56:45	Security	Использование прав	576	Администратор	XP-1
Аудит успехов	14.05.2009	5:56:45	Security	Вход/выход	528	Администратор	XP-1
Аудит отказов	14.05.2009	5:56:39	Security	Вход/выход	529	SYSTEM	XP-1
Аудит отказов	14.05.2009	5:56:35	Security	Вход/выход	529	SYSTEM	XP-1
Аудит успехов	14.05.2009	5:56:27	Security	Вход/выход	551	Администратор	XP-1
Аудит успехов	14.05.2009	5:56:20	Security	Изменение политики	612	Администратор	XP-1

- 3) Чтобы просмотреть дополнительную информацию о любом событии, выделить событие и в меню «Действие» выбрать пункт «Свойства». Windows XP регистрирует события в журнале безопасности того компьютера, на котором событие произошло. Эти события можно просматривать с любого компьютера при наличии прав администратора на компьютере, на котором произошло событие. Чтобы просмотреть журнал безопасности удаленного компьютера, необходимо открыть консоль MMC и выбрать просмотр событий удаленного компьютера.

### **Поиск событий**

При первом запуске утилиты «Просмотр событий» автоматически отображаются все события, зарегистрированные в выбранном журнале. Чтобы показать нужные события, можно использовать команду «Фильтр». Кроме того, для поиска конкретных событий применяют команду «Найти».

Чтобы выполнить отбор или поиск событий, следует запустить утилиту «Просмотр событий», затем в меню «Вид» выбрать пункт «Фильтр» или «Найти». Параметры в окнах фильтра и поиска практически не отличаются.



В таблице 2.9 перечислены параметры вкладки «Фильтр», используемые для отбора нужных событий, и команды «Найти», применяемые для поиска нужных событий.

Таблица 2.9 – Параметры для фильтрации и поиска событий

Параметр	Описание
Типы событий	Типы событий для просмотра.
Источник события	Программа или драйвер компонента, вызвавшие событие.
Категория	Тип события, например, попытка начала и завершения сеанса или системное событие.
Код события	Идентификационный номер события. Он упрощает сотрудникам службы технической поддержки контроль событий.
Пользователь	Имя учетной записи пользователя.
Компьютер	Имя компьютера.
«С» и «До»	Интервал времени, за который необходимо просмотреть события (только на вкладке «Фильтр»).
Восстановить значения по умолчанию	Отменяет все изменения на этой вкладке и восстанавливает значения по умолчанию.
Описание	Текстовый фрагмент в описании события (только в диалоговом окне «Найти»).
Направление поиска	Направление, в котором программа поиска будет просматривать журнал (вверх или вниз; только в диалоговом окне «Найти»).
Найти далее	Программа поиска находит и отображает следующую запись, удовлетворяющую условиям поиска.

### Управление журналами аудита

Сравнивая данные журналов, записанные в разное время, можно выявлять закономерности в работе Windows XP. Их анализ позволяет определять загруженность ресурсов и планировать их расширение. Кроме того, в журналах фиксируются попытки неавторизованного использования ресурсов. Windows XP позволяет изменять размер файлов журнала и задавать действия системы при переполнении журнала.

Параметры каждого журнала аудита можно настраивать в отдельности. Чтобы изменить параметры журнала, нужно выбрать его название в окне утилиты «Просмотр событий», а затем в меню «Действие» выбрать пункт «Свойства». Появится диалоговое окно «Свойства» для выбранного журнала. В диалоговом окне «Свойства» для каждого типа журнала аудита настраиваются следующие параметры:

- предельный размер каждого журнала, который может изменяться от 64 кбайт до 4194240 кбайт (4 Гбайт). По умолчанию размер журнала составляет 512 кбайт;
- действия Windows XP при достижении файлом журнала предельного размера. Чтобы настроить эти действия, следует выбрать один из вариантов, перечисленных в таблице 2.10.

Таблица 2.10 – Варианты обработки заполненных файлов журнала аудита

Параметр	Описание
Удалять старые события по необходимости	Если установлен этот параметр, можно потерять информацию при переполнении журнала до того, как его сохранят. Однако при этом не требуется обслуживания.
Удалять события, произошедшие более, чем X дней назад	Если установлен этот параметр, можно потерять информацию при переполнении журнала до того, как его сохранят. Будет утрачена только та информация, которая поступила более X дней назад. При применении этого параметра необходимо указать число дней (по умолчанию 7).
Не удалять события	Если установлен этот параметр, нужно очищать журнал вручную. При заполнении журнала Windows XP прекращает регистрацию событий, сохраняя уже имеющиеся записи журнала безопасности.

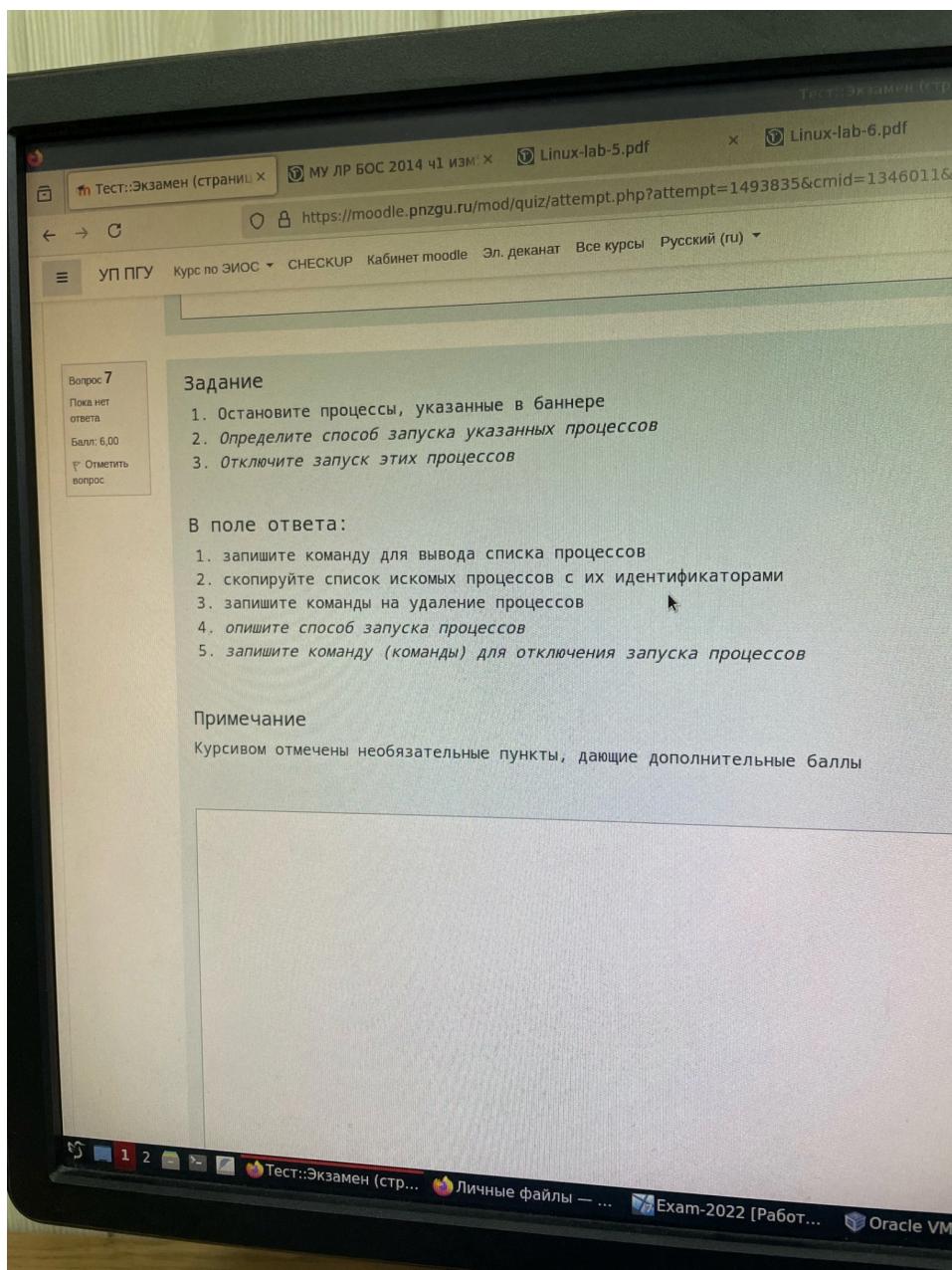
### Архивация журналов

Архивация журналов безопасности позволяет вести учет событий, связанных с безопасностью. На многих предприятиях принято сохранять архивированные журналы в течение некоторого времени, чтобы иметь возможность просмотреть информацию по безопасности за требуемый период.

Чтобы сохранить, очистить или просмотреть архивированный журнал, необходимо выбрать нужный журнал в окне утилиты «Просмотр событий» и выполните одно из действий, перечисленных в таблице 2.11.

Таблица 2.11 – Действия для архивации, очистки или просмотра файла журнала

Цель	Действия
Сохранить журнал в архиве	Выбрать «Сохранить файл журнала как», затем ввести имя файла.
Очистить журнал	Для очистки журнала выбрать «Стереть все события». При этом Windows XP генерирует запись в журнале безопасности о том, что журнал очищен.
Просмотреть архивированный журнал	Выбрать «Открыть файл журнала», выбрать журнал и указать вид выбранного журнала.



Для выполнения задания по управлению процессами в Linux вам нужно использовать команды, которые позволяют:

1. Вывести список процессов.
2. Найти нужные процессы (указанные в баннере).
3. Удалить или остановить эти процессы.
4. Определить способ запуска этих процессов.
5. Отключить их запуск.

### **Шаги выполнения:**

1. **Вывести список процессов:**

ps aux

или:

```
top
```

Чтобы сохранить список процессов в файл, используйте:

```
ps aux > processes.txt
```

1. Найти нужные процессы: Для поиска конкретного процесса по имени:

```
ps aux | grep "имя_процесса"
```

1. Остановить процессы: Для завершения процесса используйте команду `kill`:

```
kill PID
```

где `PID` — идентификатор процесса. Если процесс не завершился, используйте принудительное завершение:

```
kill -9 PID
```

**Определить способ запуска:** Для проверки способа запуска процесса посмотрите системные файлы, например:

- `/etc/init.d/`
- `/etc/systemd/system/`

Для процессов, управляемых systemd:

```
systemctl status имя_сервиса
```

**Отключить запуск процессов:** Если процесс запускается через systemd, отключите его:

```
systemctl disable имя_сервиса
```

Если процесс находится в автозагрузке, проверьте папки:

- `/etc/rc.local`
- `~/.bashrc`
- `~/.config/autostart/`

Для удаления записи из автозагрузки отредактируйте соответствующие файлы.

**1. Запустите системный сервис `iperf`:**

```
systemctl start iperf
```

**2. Включите автозапуск сервиса `iperf`:**

```
systemctl enable iperf
```

**3. Найдите в журнале записи, относящиеся к этому сервису:**

Используйте `journalctl` для фильтрации записей:

```
journalctl -u iperf
```

Чтобы сохранить фрагмент в файл:

```
journalctl -u iperf > iperf_logs.txt
```

**4. Найдите сервис, использующий порт 13:**

Просмотрите список активных соединений и процессов:

```
netstat -tulnp | grep :13
```

или с использованием `ss`:

```
ss -tulnp | grep :13
```

**5. Остановите этот сервис:**

Найдите PID процесса (если это не системный сервис):

```
ps aux | grep имя_процесса  
kill PID
```

Если это системный сервис:

```
systemctl stop имя_сервиса
```

**6. Отключите автозапуск сервиса, использующего порт 13:**

```
systemctl disable имя_сервиса
```

**7. Найдите в журнале записи, относящиеся к этому сервису:**

Используйте `journalctl` с именем или портом:

```
journalctl -u имя_сервиса
```

или:

`journalctl | grep порт_или_имя_процесса`

## 2) Линукс

### *Подключение к серверу SSH*

Подключение к серверу выполняется с помощью программы *ssh*. Для интерактивного сеанса в команде необходимо указать имя пользователя и хост, а также при необходимости еще и порт для соединения с сервером:

2

```
ssh -p 20022 user@localhost
```

### 3.3 Примеры

#### 3.3.1 Команды манипуляции учетными записями пользователей

Для управления паролями пользователей используется команда *passwd*, варианты применения которой показаны в таблице 3.1.

Таблица 3.1 – Примеры использования команды *passwd*

Команда	Описание
<i>passwd ivanov</i>	Назначение пароля пользователю ivanov.
<i>passwd -d petrov</i>	Сброс пароля, блокировка пользователя petrov.

Для добавления новой учетной записи пользователя используются команды *useradd* и *adduser*, варианты применения которых показаны в таблице 3.2. Важно отметить, что по умолчанию команда *useradd* создает учетную запись пользователя без пароля, то есть пользователь не может регистрироваться в системе.

Таблица 3.2 – Примеры использования команд *useradd* и *adduser*

Команда	Описание
<i>useradd ivanov</i>	Добавление учетной записи пользователя без создания домашнего каталога.

useradd -m petrov	Добавление учетной записи пользователя и создание домашнего каталога.
useradd -m -s/bin/bash sidorov	Добавление учетной записи пользователя, создание домашнего каталога и установка программы-оболочки /bin/bash.
useradd -D	Просмотр значений по умолчанию.
adduser ivanov	Добавление учетной записи пользователя, создание домашнего каталога, установка пароля и дополнительных сведений в интерактивном режиме.

Для удаления учетных записей пользователей используются команды userdel и deluser, варианты применения которых показаны в таблице 3.3.

Таблица 3.3 – Примеры использования команд userdel и deluser

Команда	Описание
userdel ivanov	Удаление учетной записи пользователя ivanov.
userdel -r petrov	Удаление учетной записи пользователя petrov и его домашнего каталога.
deluser ivanov	Удаление учетной записи пользователя ivanov.
deluser --remove-home petrov	Удаление учетной записи пользователя petrov и его домашнего каталога.
deluser --remove-all-files sidorov	Удаление учетной записи пользователя sidorov и всех принадлежащих файлов (выполняется длительное время).

Для изменения пользовательских данных используются команды adduser и usermod, варианты применения которых показаны в таблице 3.4.

Таблица 3.4 – Примеры использования команд userdel и deluser

Команда	Описание
adduser ivanov wireless	Добавление учетной записи пользователя ivanov в группу wireless.
usermod -a -G wireless,vboxusers ivanov	Добавление учетной записи пользователя ivanov в группы wireless, vboxusers.
usermod -c Иванов ivanov	Добавление комментария Иванов в учетную запись ivanov.
usermod -d /var/samba/ivanov ivanov	Установка пользователю ivanov домашнего каталога /var/samba/ivanov.
usermod -s ivanov	Установка пользователю ivanov программы-оболочки /bin/bash.

Для управления группами учетных записей пользователей используются команды, приведенные в таблице 3.5.

Таблица 3.5 – Применение команд управления группами

Команда	Описание
addgroup administrators	Создание группы administrators.
groupadd administrators	Создание группы administrators.
delgroup administrators	Удаление группы administrators.
groupdel administrators	Удаление группы administrators.
group ivanov	Просмотр сведений о членстве в группах пользователя ivanov.

Для смены идентификатора пользователя, например, для проверки прав доступа, используется команда su:

**su имя-пользователя**

---

### 3.3.3 Команды манипуляции правами пользователей на файлы и каталоги

Получить информацию о владельцах и правах файлов можно, используя команду ls с параметром -l. Формат команды следующий:

*ls -l имя\_файла*

В результате выводится следующая информация о файлах: тип файла, права доступа к файлу, количество ссылок на файл, имя владельца, имя группы, размер файла (в байтах), временной штамп и имя файла.

Для смены прав доступа на файл используется команда chmod, имеющая следующий формат:

*chmod wXr имя-файла*

67

Вместо символа w подставляется:

- либо символ u (т.е. пользователь, который является владельцем);
- либо g (группа);
- либо o (все пользователи, не входящие в группу, которой принадлежит данный файл);
- либо a (все пользователи системы, т.е. и владелец, и группа, и все остальные).

Вместо X ставится:

- либо + (предоставляется право);
- либо – (лишается соответствующего права);
- либо = (установить указанные права вместо имеющихся).

Вместо r — символ, обозначающий соответствующее право:

- r (чтение);
- w (запись);
- x (выполнение).

Если опустить указание на то, кому предоставляется данное право, то подразумевается, что речь идет вообще обо всех пользователях.

Второй вариант использования команды chmod основан на цифровом представлении прав. Для этого символ г кодируется цифрой 4, символ w — цифрой 2, а символ x — цифрой 1. Для того, чтобы предоставить пользователям какой-то набор прав, нужно сложить соответствующие цифры. Получив, таким образом, нужные цифровые значения для владельца файла, для группы файла и для всех остальных пользователей, эти три цифры задаются в качестве аргумента команды chmod (эти цифры ставятся после имени команды перед вторым аргументом, который задает имя файла).

Примеры использования команды chmod приведены в таблице 3.9.

Таблица 3.9 – Примеры использования команды chmod

Команда	Описание
chmod a+x file.txt	Предоставление всем пользователям права на выполнение файла file.txt.
chmod +w file.txt	Предоставление всем пользователям права на запись файла file.txt.

68

chmod go-rw file.txt	Удаление прав на чтение и запись для всех пользователей, кроме владельца файла file.txt.
chmod ugo+rwx file.txt	Предоставление всем пользователям прав на чтение, запись и выполнение файла file.txt.
chmod 760 file.txt	Предоставление всех прав ( $4+2+1=7$ ) владельцу файла file.txt, предоставление прав на чтение и запись группе ( $4+2=6$ ), отказ в правах всем остальным пользователям (0).

Команды chown и chgrp служат для смены владельца файла и группы файла. Выполнять смену владельца может только суперпользователь, смену группы может выполнить сам владелец файла или суперпользователь. Для того, чтобы иметь право сменить группу, владелец должен дополнительно быть членом той группы, которой он хочет дать права на данный файл. Формат этих двух команд аналогичен:

*chown имя-пользователя имя-файла*

*chgrp имя-группы имя-файла*

Возможна смена одновременно владельца и группы:

*chown имя-пользователя:имя-группы имя-файла*

### 3.3.4 Команды манипуляции POSIX ACL

Для работы со списками контроля доступа поддержка ACL должна быть включена в ядре системы при компиляции (как правило, по умолчанию) и в файловой системе при монтировании (показано в последней строке таблицы 3.8).

При помощи программы getfacl можно посмотреть список текущих ACL:

```
getfacl [параметры] файлы
```

Для установки и удаления ACL используется программа setfacl:

```
setfacl [параметры] [{-m|-x} ACL] файлы
```

Установка ACL из файла:

```
setfacl [параметры] [{-M|-X} файл] файлы
```

Для добавления и изменения ACL используется параметр `-m`. Например, чтобы добавить права доступа для пользователя `user1`, необходимо выполнить следующую команду:

```
setfacl -m u:user1:r test
```

После `-m` записывается ACL. Формат записи достаточно простой. Если первый символ `u`, то добавляются права для указанного после двоеточия пользователя. Если первый символ `g` — определяются права для группы. Если `m` — определяется маска. Сами права записываются в символьном виде (`rwx`).

Для добавления в ACL файла `test` группы `bin` с правами `rwx`:

```
setfacl -m g:bin:rwx test
```

Для удаления всех прав на файл `test` для пользователя `user1` используется параметр `-x`:

```
setfacl -x u:user1 test
```

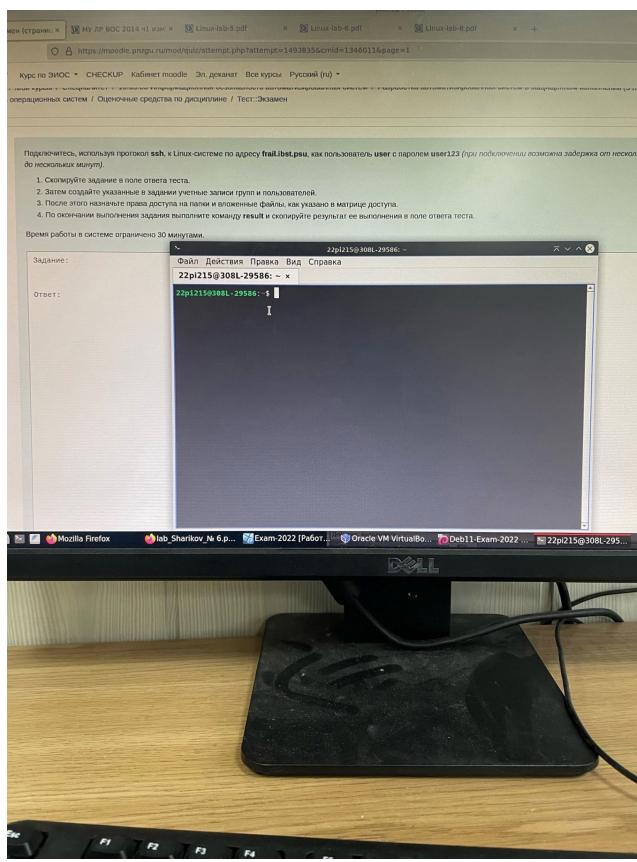
Возможные форматы записи ACL:

```
[default]:[u[ser]:][пользователь][:[+|^]права]
[default]: g[group]:[группа][:[+|^]права]
[default]: m[mask][:[+|^]права]
[default]: o[ther][:[+|^]права]
```

где:

- `default` – устанавливает ACL по умолчанию. Имеет смысл только для каталога. При создании файлов в каталоге, у которого установлен ACL по умолчанию, значения ACL копируются во вновь создаваемые файлы;
- `u` – установка ACL для пользователя, имя которого указывается в следующем поле. Если имя опущено, то права устанавливаются для владельца;
- `g` – установка ACL для группы, имя которой указывается в следующем поле. Если имя опущено, то права устанавливаются для группы-владельца;
- `m` – установка маски ACL. Маска является фильтром, определяющим максимально возможные права доступа;
- `o` – установка ACL для всех остальных пользователей;
- `права` – права доступа в символьном виде (`rwx`).

Если при написании ACL права доступа начинаются с символа `+`, то эти права добавляются к уже существующим. Если в начале описания прав стоит символ `^`, то их значение отнимается от существующих прав доступа.



## 1. Подключение к системе через SSH

Подключаемся к серверу, используя указанные учетные данные:

```
bash
```

Копировать Редактировать

```
ssh user@frail.ibst.psu  
# Введите пароль: user123
```

---

## 2. Создание пользователей

Создаем указанных пользователей (замените <username> на имена из задания):

```
bash
```

Копировать Редактировать

```
sudo useradd <username>  
sudo passwd <username>  
# Установите пароль для пользователя
```

### 3. Создание групп

Создаем указанные группы (замените <groupname> на названия из задания):

```
bash
```

Копировать Редактировать

```
sudo groupadd <groupname>
```

Добавляем пользователей в группы:

```
bash
```

Копировать Редактировать

```
sudo usermod -aG <groupname> <username>
```

---

### 4. Настройка прав на файлы и каталоги

Проверяем существующие каталоги и файлы:

```
bash
```

Копировать Редактировать

```
ls -l /path/to/directory
```

Меняем права доступа:

- Установка владельца и группы:

```
bash
```

Копировать Редактировать

```
sudo chown <owner>:<group> /path/to/file_or_directory
```

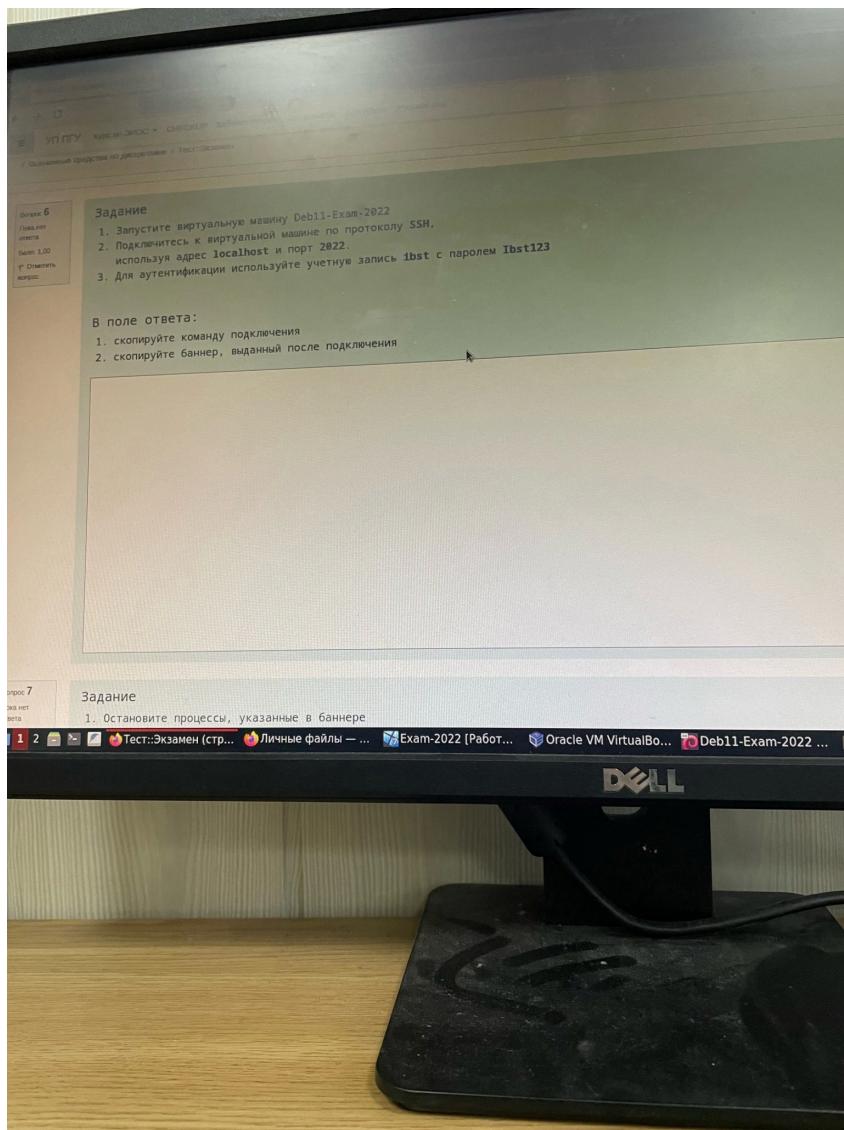
- Настройка прав (например, доступ только для владельца, группы или всех):

```
bash
```

Копировать Редактировать

```
sudo chmod 700 /path/to/file_or_directory # Только владелец и группа  
sudo chmod 777 /path/to/file_or_directory # Полный доступ для всех
```





## 1. Команда подключения по SSH

Подключитесь к виртуальной машине на порту 2022, используя учетные данные из задания:

```
bash
```

Копировать  Редактировать

```
ssh -p 2022 ibst@localhost
```

При запросе пароля введите: `Ibst123`.

---

## 2. Базовый вывод (баннер)

После успешного подключения система может отобразить приветственное сообщение (баннер). Оно появится автоматически. Например:

```
plaintext
```

Копировать  Редактировать

```
Welcome to Debian 11!  
Authorized access only.
```

Скопируйте это сообщение и вставьте в поле ответа.

### Примечание

- Если потребуется остановить процессы, указанные в баннере, выполните команду `ps` для просмотра запущенных процессов:

```
bash
```

Копировать  Редактировать

```
ps aux | grep <имя_процесса>  
sudo kill <PID>
```

Замените `<имя_процесса>` и `<PID>` на соответствующие значения.

Если потребуется дополнительная помощь, уточните детали задания!

### 3) Еще линукс

#### A) управление процессами

##### *Получение информации о процессах*

Для управления процессом необходимо знать его идентификатор. Эта задача решается с помощью команды *ps*. Эта команда делает мгновенный снимок состояния процессов и выводит его на устройство стандартного вывода. Какие данные и для какого подмножества процессов будут выведены зависит от параметров команды.

Вывод информации по всем процессам:

```
ps -e
```

Выводит идентификатор процесса; терминал, с которым связан процесс; процессорное время, затраченное процессом с момента старта; команда, породившая процесс.

Вывод информации по всем процессам, связанным с терминалами:

```
ps -a
```

Вывод информации по всем процессам, связанным с терминалами, указанными в списке:

```
ps -t terminal_list
```

В списке терминалы перечисляются через запятую без пробелов.

Вывод информации по всем процессам, принадлежащим пользователями, указанными в списке:

```
ps -u user_list
```

В списке могут быть указаны как имена пользователей, так и идентификаторы.

Вывод информации по всем процессам, запущенным пользователями, указанными в списке:

```
ps -U user_list
```

Команды вывода процессов по списку групп:

```
ps -g group_list  
ps -G group_list
```

Они аналогичны командам вывода процессов по списку пользователей. Параметр *-G* влияет на вывод информации о процессах с *sgid*-битом.

Команды вывода информации о процессах по списку идентификаторов процессов:

```
ps -p process_list
```

---

Команды вывода информации о процессах по списку идентификаторов сессий:

```
ps -s session_list
```

Команда *ps* без параметров выводит информацию о процессах текущей сессии, т. е. сессии, в которой запущена.

Далее рассмотрим параметры, позволяющие менять состав информации о процессах. Эти параметры могут комбинироваться с рассмотренными ранее, а также некоторые могут комбинироваться между собой. Если эти параметры не использовать, то выводятся только четыре основных поля: *PID*, *TTY*, *TIME* и *CMD*. Что находится в этих полях показано в таблице 1.

## *Управление процессами*

При управлении процессами можно посыпать им сигналы, менять им статический приоритет и класс шедулера, менять им динамический приоритет (*nice*).

Для смены шедулера и статического приоритета используется команда *chrt*. Ошибка в настройках этих параметров может привести к некорректному функционированию операционной системы.

Для получения информации о приоритете и шедулере процесса необходимо использовать команду с следующим формате:

```
chrt -p PID
```

где *PID* — идентификатор процесса.

Установка шедулера и приоритета выполняется так:

```
chrt scheduler_option -p prioritet PID
```

где *scheduler\_option* — один из параметров:

-o, --other — шедулер SCHED\_OTHER с разделением времени, основной в Linux;

-f, --fifo — шедулер реального времени SCHED\_FIFO с дисциплиной «первый пришел-первый вышел»;

-r, --rr — шедулер реального времени SCHED\_RR с дисциплиной кругового цикла;

-b, --batch — шедулер SCHED\_BATCH пакетных заданий

-i, --idle — шедулер SCHED\_IDLE для выполнения в свободное низкоприоритетных задач.

*prioritet* — статически приоритет процесса в диапазоне от 0 до 99.

Для шедулеров реального времени приоритет назначается в диапазоне от 1 до 99. Чем выше приоритет, тем больше процессорного времени получает процесс. Для остальных шедулеров приоритет всегда должен быть нулевым.

Шедулеры реального времени назначаются ядром ОС на свои компоненты и менять их не следует, как не следует и изменять приоритеты этих процессов. Практический интерес может представлять только установка шедулера SCHED\_IDLE на вычислительные задачи, сильно нагружающие процессор, но не требующие быстрого выполнения. Таким задачам можно сменить шедулер с SCHED\_OTHER на SCHED\_IDLE.

Для смены динамического приоритета используется команда *renice*:

```
renice -n prioritet -p PID
```

Устанавливает приоритет процессу с идентификатором *PID*. Приоритет должен быть в диапазоне от -20 (наивысший) до 19 (наименее высокий).

```
renice -n prioritet -u UID
```

Устанавливает приоритет всем процессам пользователя с идентификатором *UID*.

Для того, чтобы послать процессу сигнал используется команда *kill*. Большинство сигналов предназначены для завершения процессов по тем или иным причинам. Однако, процессы могут обрабатывать некоторые сигналы нестандартным образом. Среди сигналов есть только два, для которых процессы не могут изменить обработчик, это сигнал остановки процесса *SIGSTOP* и сигнал уничтожения процесса *SIGKILL*.

Формат команды следующий:

```
kill [-s SIGxxx] PID [PID [PID [...]]]
```

где *SIGxxx* — сигнал, *PID* — идентификатор процесса. Можно посылать сигнал сразу нескольким процессам. Рассмотрим некоторые сигналы:

*SIGTERM* — завершение процесса. Этот сигнал посылает команда *kill* если сигнал в командной строке не указан. Используется для нормального завершения процесса.

*SIGINT* — сигнал прерывания с клавиатуры. Этот сигнал посылает командный интерпретатор при нажатии комбинации *Ctrl-C*.

*SIGQUIT* — сигнал завершения с дампом памяти с клавиатуры. Этот сигнал посылает командный интерпретатор при нажатии комбинации *Ctrl-\*.

*SIGABRT* — сигнал аварийного завершения процесса. Посыпается своему процессу функцией *abort*.

*SIGKILL* — сигнал завершения в случае если другие сигналы не помогают завершить процесс.

*SIGSTOP* — сигнал остановки процесса.

*SIGTSTP* — сигнал остановки процесса с клавиатуры. Этот сигнал посылает командный интерпретатор при нажатии комбинации *Ctrl-Z*.

*SIGCONT* — сигнал возобновления работы после остановки. Этот же сигнал посыпают команды *bg* и *fg*.

*SIGUSR1*, *SIGUSR2* — сигналы, определяемые пользователем. Если не преопределены, то вызывают завершение программы.

## Б) сервисы

Приведем пример использования команд управления на системном сервисе *apache2.service*:

<code>sudo systemctl stop apache2.service</code>	– остановить сервис
<code>sudo systemctl start apache2.service</code>	– запустить сервис
<code>sudo systemctl restart apache2.service</code>	– перезапустить сервис
<code>sudo systemctl disable apache2.service</code>	– отключить сервис (нет автозапуска)
<code>sudo systemctl enable apache2.service</code>	– включить сервис (есть автозапуск)
<code>sudo systemctl mask apache2.service</code>	– запретить сервис (невозможно запустить)
<code>sudo systemctl unmask apache2.service</code>	– разрешить сервис (можно запустить)

При отключении сервиса отключается только автозапуск. Возможность ручного запуска сохраняется. При запрете сервиса любые операции с сервисом запрещаются, не только запуск, но и просмотр и редактирование его конфигурации.

## В) работа с журналами, информация о работе пользователей есть и в *systemd(systemctl)* и *authlog*

Команда *w* позволяет просмотреть журнал */var/run/utmp* и вывести информацию обо всех аутентифицированных пользователях в системе, а также время работы системы и среднюю загрузку

```
w /var/run/utmp
```

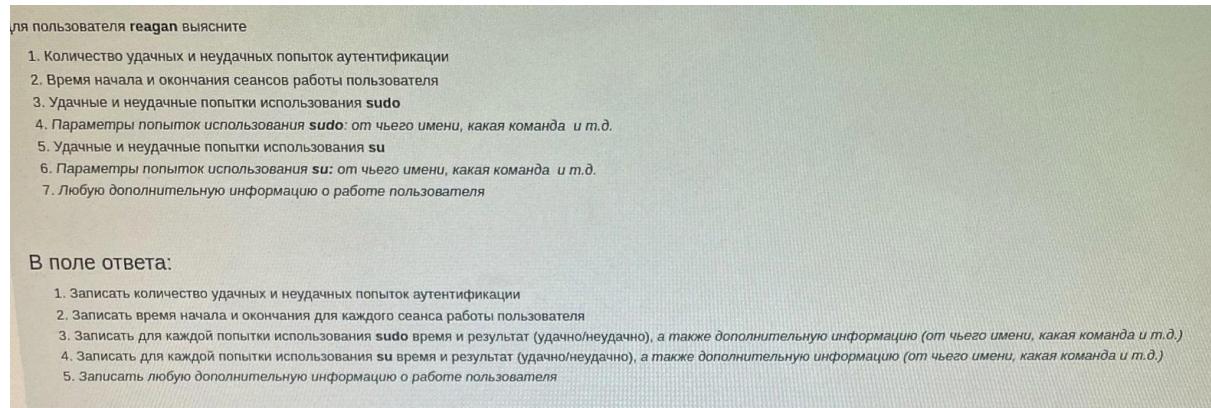
Команда *who* по умолчанию просматривает журнал */var/run/utmp*, но ей может быть указан и другой журнал. У данной команды много параметров, о которых можно узнать выполнив тап *who*. В зависимости от набора параметров команда отображает разную информацию.

Приведем пример, как использовать данную команду для просмотра журнала */var/log/wtmp*:

```
who /var/log/wtmp
```

Команда `last` предназначена для просмотра журнала `/var/log/wtmp`. Кроме времени входа и выхода пользователей она по умолчанию показывает еще и все моменты загрузки ОС.

## `last`



Задание выполняется командами:

`sudo cat journalctl | grep "имя_пользователя/команда"`

`sudo cat /var/log/auth.log | grep "имя_пользователя/команда"`



## 1. Управление пользователями, группами и журналами безопасности в Windows

### Теория:

#### 1. Управление пользователями:

- Добавление, удаление и редактирование учетных записей пользователей осуществляется через встроенные инструменты, такие как:
  - "Панель управления -> Управление учетными записями пользователей".
  - Консоль "Локальные пользователи и группы" (lusrmgr.msc) – используется для создания, редактирования и удаления пользователей на локальном компьютере (доступно только в редакциях Pro и выше).
  - Командная строка (cmd) или PowerShell:

```
cmd
```

Копировать Редактировать

```
net user <имя_пользователя> <пароль> /add
```

```
powershell
```

Копировать Редактировать

```
New-LocalUser -Name "<имя>" -Password (ConvertTo-SecureString "<пароль>" -AsPl
```

## 2. Управление группами:

- Группы позволяют упрощать управление доступом и правами пользователей.
- Для добавления пользователей в группу используется:
  - В консоли lusrmgr.msc.
  - В командной строке:

```
cmd                                     ⌂ Копировать ⌂ Редактировать

net localgroup <группа> <имя_пользователя> /add
```

- В PowerShell:

```
powershell                               ⌂ Копировать ⌂ Редактировать

Add-LocalGroupMember -Group "<группа>" -Member "<имя>"
```

## 3. Журналы безопасности:

- Журналы безопасности (Security Logs) содержат записи о событиях, связанных с безопасностью (например, успешные и неудачные попытки входа, изменения прав доступа).
- Для просмотра журналов используется "Просмотр событий" (eventvwr.msc):
  - В разделе "Журналы Windows -> Безопасность" отслеживаются события с идентификаторами, например:
    - 4624 – Успешный вход пользователя.
    - 4625 – Неудачная попытка входа.
    - 4720 – Создание нового пользователя.

- В PowerShell для анализа:

```
powershell                               ⌂ Копировать ⌂ Редактировать

Get-EventLog -LogName Security | Select-Object -First 10
```

Или:

```
powershell                               ⌂ Копировать ⌂ Редактировать

Get-WinEvent -LogName Security | Where-Object { $_.Id -eq 4624 }
```

## 2. Линукс: Настройка прав доступа и работа с SSH

---

### Теория:

#### Настройка прав доступа

В Linux права доступа определяют, кто может читать, изменять или выполнять файлы и каталоги.

##### 1. Структура прав доступа:

- Каждому файлу или каталогу назначены:
  - Владелец (Owner): Тот, кто создал файл.
  - Группа (Group): Группа пользователей, имеющая доступ.
  - Другие (Others): Все остальные пользователи системы.
- Права определяются тремя основными действиями:
  - Чтение (r): Просмотр содержимого файла или списка файлов в каталоге.
  - Запись (w): Изменение файла или добавление/удаление файлов в каталоге.
  - Исполнение (x): Выполнение файла как программы или доступ в каталог.

##### 2. Просмотр прав: Используйте команду `ls -l` для просмотра прав:

```
bash
```

Копировать Редактировать

```
ls -l /path/to/file_or_directory
```

Пример вывода:

```
plaintext
```

Копировать Редактировать

```
-rw-r--r-- 1 user group 1234 Jan 1 12:00 example.txt
```

##### • Первые 10 символов:

- `-`: Обычный файл (для каталога — `d`).
- `rw-`: Права владельца (чтение, запись, нет исполнения).
- `r--`: Права группы (чтение, нет записи и исполнения).
- `r--`: Права для других.

### 3. Изменение прав доступа:

- Используйте команду `chmod` для изменения прав:

```
bash
```

Копировать Редактировать

```
chmod 750 /path/to/file_or_directory
```

В данном примере:

- Владелец: чтение, запись, исполнение.
- Группа: чтение, исполнение.
- Другие: нет доступа.

### 4. Изменение владельца и группы:

- Для изменения владельца файла используйте команду `chown`:

```
bash
```

Копировать Редактировать

```
sudo chown <owner>:<group> /path/to/file_or_directory
```

## Подключение по SSH

SSH (Secure Shell) — это протокол для удаленного подключения к системам.

1. Подключение к серверу: Используйте команду:

```
bash
```

Копировать Редактировать

```
ssh username@host
```

Пример:

```
bash
```

Копировать Редактировать

```
ssh user@192.168.1.1
```

2. Настройка SSH-сервера (sshd): Файл конфигурации сервера находится по пути `/etc/ssh/sshd_config`. Пример изменений:

- Изменить порт:

```
plaintext
```

Копировать Редактировать

```
Port 2222
```

- Запретить доступ root-пользователю:

```
plaintext
```

Копировать Редактировать

```
PermitRootLogin no
```

3. Ключевая аутентификация:

- Создайте пару ключей:

```
bash
```

Копировать Редактировать

```
ssh-keygen
```

- Скопируйте открытый ключ на сервер:

```
bash
```

Копировать Редактировать

```
ssh-copy-id username@host
```

#### 4. Полезные команды:

- Отключение от SSH:

```
bash
```

Копировать Редактировать

```
exit
```

- Проверка статуса SSH-сервера:

```
bash
```

Копировать Редактировать

```
sudo systemctl status sshd
```

### 3. Линукс на виртуалке: Управление процессами, сервисами и журналами

---

#### Теория:

##### A) Управление процессами

###### 1. Просмотр процессов:

- Основная команда для просмотра процессов:

```
bash                                     ⌂ Копировать ⌂ Редактировать  
ps aux
```

- a: отображает процессы всех пользователей.
  - u: выводит информацию в удобном формате (с владельцем, CPU и RAM).
  - x: показывает все процессы, включая фоновые.
- Для динамического отслеживания процессов используйте:

```
bash                                     ⌂ Копировать ⌂ Редактировать  
top
```

или более наглядный вариант:

```
bash                                     ⌂ Копировать ⌂ Редактировать  
htop
```

###### 2. Управление процессами:

- Завершить процесс:

```
bash                                     ⌂ Копировать ⌂ Редактировать  
kill <PID>
```

Замените <PID> на идентификатор процесса (можно найти через ps ).

- Завершить процесс принудительно:

```
bash                                     ⌂ Копировать ⌂ Редактировать  
kill -9 <PID>
```

### 3. Поиск процесса:

- Найти процесс по имени:

```
bash
```

Копировать Редактировать

```
ps aux | grep <process_name>
```

---

## В) Работа с сервисами

### 1. Проверка статуса сервиса: Используйте команду `systemctl` для управления службами:

```
bash
```

Копировать Редактировать

```
systemctl status <service_name>
```

Пример для проверки SSH:

```
bash
```

Копировать Редактировать

```
systemctl status sshd
```

### 2. Запуск, остановка и перезапуск сервиса:

- Запустить:

```
bash
```

Копировать Редактировать

```
sudo systemctl start <service_name>
```

- Остановить:

```
bash
```

Копировать Редактировать

```
sudo systemctl stop <service_name>
```

- Перезапустить:

```
bash
```

Копировать Редактировать

```
sudo systemctl restart <service_name>
```

### 3. Автозапуск сервиса:

- Включить автозапуск:

```
bash
```

Копировать Редактировать

```
sudo systemctl enable <service_name>
```

- Отключить автозапуск:

```
bash
```

Копировать Редактировать

```
sudo systemctl disable <service_name>
```

### C) Работа с журналами

#### 1. Просмотр журналов с помощью `journalctl`:

- Общая команда для просмотра всех событий:

```
bash
```

Копировать Редактировать

```
journalctl
```

- Для просмотра событий определенного сервиса:

```
bash
```

Копировать Редактировать

```
journalctl -u <service_name>
```

Пример для SSH:

```
bash
```

Копировать Редактировать

```
journalctl -u sshd
```

- Фильтрация по времени:

```
bash
```

Копировать Редактировать

```
journalctl --since "2025-01-24 12:00" --until "2025-01-24 14:00"
```

#### 2. Логи работы пользователей:

- Команда `last` показывает список последних входов пользователей:

```
bash
```

Копировать Редактировать

```
last
```

- Для проверки текущих сессий:

```
bash
```

Копировать Редактировать

```
who
```

#### 3. Работа с `auth.log`:

- Файл `/var/log/auth.log` содержит информацию о входах и действиях пользователей.

```
bash
```

Копировать Редактировать

```
sudo cat /var/log/auth.log
```

<https://serverspace.by/support/help/zhurnaly-windows/>

<https://www.securityvision.ru/blog/praktika-ib-rabota-s-podsistemoy-zhurnalirovaniya-windows/>

