**Практическая работа № 10.**

**Тема:** «Настройка групповой политики в Windows Server 2003».

**Цель работы:** освоить возможности обеспечения сетевой безопасности путем управления системой политик безопасности домена, изучить систему формирования политик безопасности домена, научиться создавать подразделения домена c пользователями, сформировать групповую политику для подразделения домена.

**Выполнение практической работы**

**Формирование политики безопасности домена**

1. Загрузить виртуальные машины с операционной системой Windows 2003 Server и клиентскую машину с ОС Windows XP.
2. В одноранговой сети параметры безопасности назначаются локально на каждом компьютере сети при помощи оснастки **Локальная политика безопасности**. На рабочих станциях домена политика безопасности формируется путем наложения на **Локальную политику безопасности** конкретного компьютера **Политики безопасности домена**, которая формируется централизованно на контроллере домена при помощи соответствующей оснастки **в меню Администрирование** (рис. 1 - 2).

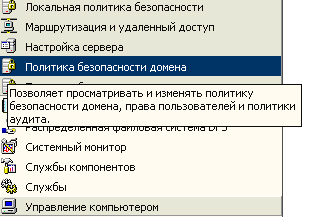


Рис. 1. Меню **Администрирование** на контроллере домена

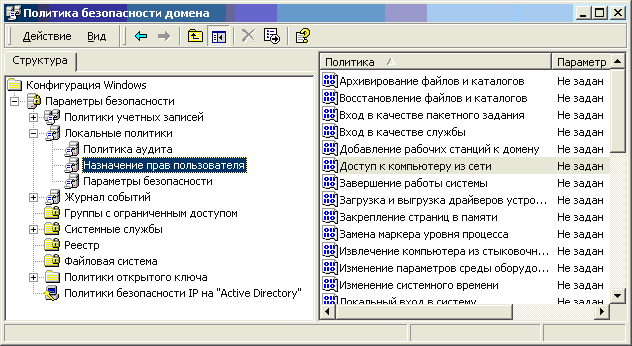


Рис. 2. Интерфейс оснастки **Политика безопасности домена**

При наличии в локальной политике безопасности и в политике безопасности домена одноименных параметров происходит их перекрытие, причем сначала в реестр загружаемой операционной системы компьютера записывается локальный параметр, а затем он замещается параметром домена.

Если в политике безопасности домена параметр локальной политики не задан, то действует локальный параметр.

Кроме этого, в домене для различных пользователей и компьютеров могут создаваться организационные единицы – **подразделения**, на которые могут назначаться **Групповые политики безопасности**, перекрывающие не только локальные политики безопасности, но и политики безопасности домена.

Групповая политика для пользователя определяет его возможности при работе на любой рабочей станции домена.

Групповая политика для компьютера определяет возможности любых пользователей домена при работе на этом компьютере.

Групповая политика может назначаться только подразделению. В меню оснастки **Active Directory – Пользователи и компьютеры** подразделение отображается как папка с пиктограммой в виде приоткрытой книги.

По умолчанию в домене создается только одно подразделение – **Domain Controllers** (рис. 3), членами которого являются компьютеры – контроллеры домена. Для них автоматически формируется специальная групповая политика, определяющая возможности допуска и работы на этих компьютерах различных пользователей домена. По умолчанию доступ к контроллерам домена обычным пользователям домена не разрешен.

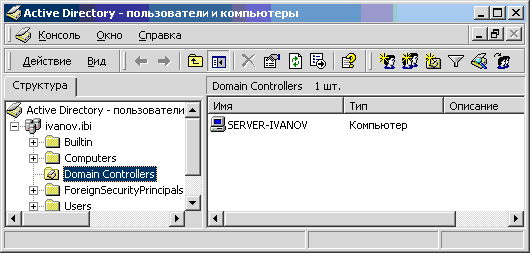


Рис. 3. Подразделение **Domain Controllers**

В свойствах подразделения (открываемых через контекстное меню) имеется закладка **Групповая политика** (рис. 4), в которой можно создать необходимую групповую политику для членов этого подразделения или выбрать уже имеющуюся групповую политику (щелчком мыши) и открыть ее (двойным щелчком мыши или кнопкой **Изменить**).

Следует заметить, что одна из основных частей групповой политики подразделения **Domain Controllers** (рис. 5), а именно **Параметры безопасности**, доступна также из меню **Администрирование** как **Политика безопасности контроллера домена** (рис. 6).

Внутри любого подразделения могут создаваться другие подразделения со своими групповыми политиками, которые также участвуют в процессе перекрытия параметров безопасности. По умолчанию групповые политики вложенных (дочерних) подразделений перекрывают родительские.

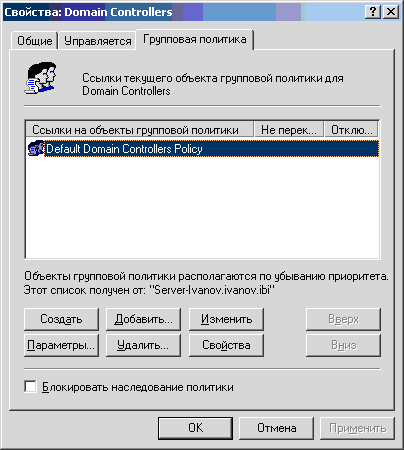


Рис. 4. Вкладка **Групповая политика** в свойствах подразделения **Domain Controllers**

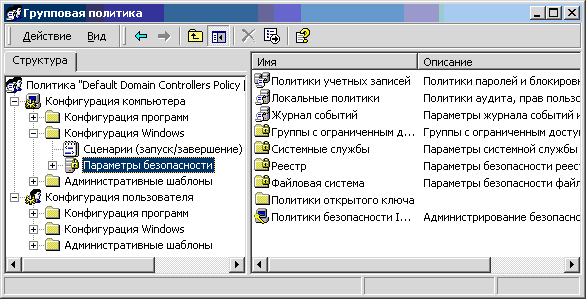


Рис. 5. Состав групповой политики подразделения **Domain Controllers**

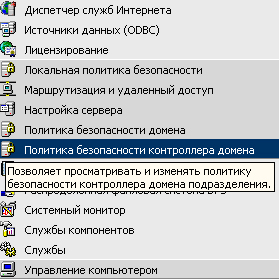


Рис. 6. Пункт **Политика безопасности контроллера домена** в меню **Администрирование**

Таким образом, политика безопасности домена в отношении конкретного пользователя формируется в результате перекрытия нескольких различных политик. Чтобы не возникло путаницы, рекомендуется пользоваться только групповыми политиками. Параметры локальной политики безопасности и политики безопасности домена следует изменять лишь в том случае, когда требуемые параметры безопасности нельзя реализовать при помощи групповых политик.

Для реализации этого правила все пользователи и компьютеры распределяются по подразделениям, на которые назначены необходимые групповые политики.

Если какие-то параметры безопасности нужно применить ряду подразделениям, то эти подразделения включаются в одно общее подразделение с общей групповой политикой.

Если многим пользователям требуется применить одинаковую политику безопасности, но эти пользователи находятся в разных подразделениях, то можно назначить одну групповую политику нескольким подразделениям.

***Создание подразделения домена***

1. На контроллере домена открыть оснастку **Active Directory – Пользователь и компьютеры**.
2. В контекстном меню домена с помощью пункта **Создать – Подразделение** (рис. 7) сформировать подразделение домена с именем **студенты** (рис. 8).

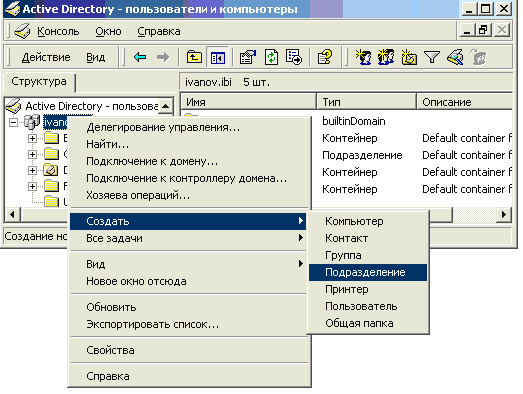


Рис. 7. Создание подразделения

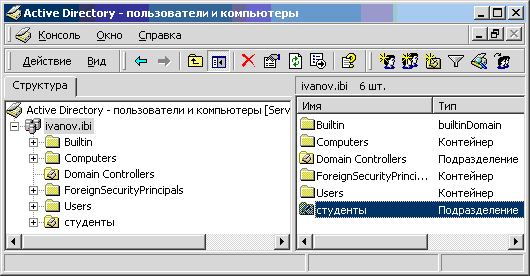


Рис. 8. Пример подразделения с именем **студенты**

1. Путем копирования имеющейся учетной записи **студент** создать новые учетные записи пользователей **Петров**, **Сидоров** и **Пиров** с именами входа соответственно **petrov**, **sidorov**, **pirov** и паролем **123**.
2. Создать группу пользователей **студенты** как глобальную группу и включить в нее созданных пользователей (рис. 9, 10).

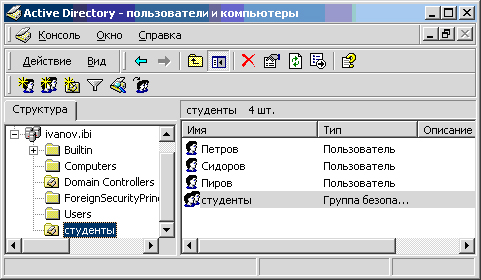


Рис. 9. Состав подразделения **студенты**

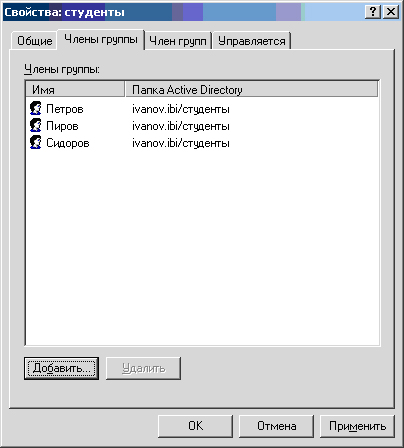


Рис. 10. Состав группы пользователей **студенты**

***Создание групповой политики безопасности домена***

К членам подразделения могут применяться **групповые политики** безопасности. Членами подразделения могут быть как пользователи, так и компьютеры. Следует отметить, что включение в подразделение **группы пользователей** домена не ведет к автоматическому включению в это подразделение членов указанной группы пользователей.

Для создания групповой политики подразделению **студенты** выполнить следующие действия:

1. При помощи контекстного меню подразделения **студенты** открыть свойства и выбрать закладку **Групповая политика** (рис. 11).
2. При помощи кнопки **Создать** назначить новый объект групповой политики с именем **групповая политика студенты** (рис. 12).

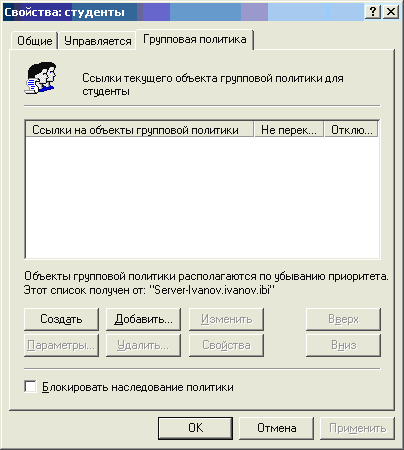


Рис. 11. Вкладка **Групповая политика** в свойствах подразделения **студенты**

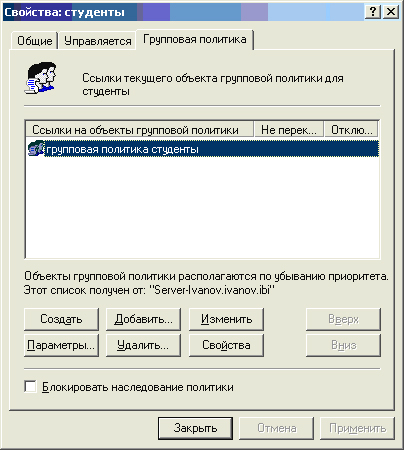


Рис. 12. Назначение объекта групповой политики **групповая политика студенты**

1. Двойным щелчком мыши по выбранному объекту групповой политики или при помощи кнопки **Изменить** открыть окно управления параметрами созданной групповой политики (рис. 13).

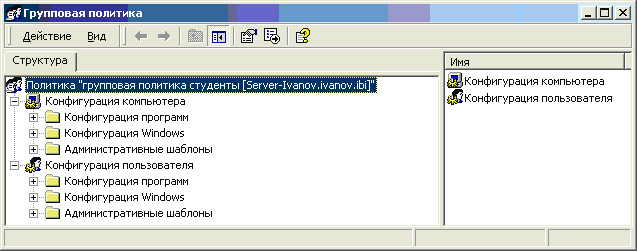


Рис. 13. Состав объекта групповой политики

Каждая групповая политика (см. рис. 13) имеет следующую структуру:

* **Конфигурация компьютера,** определяющая параметры компьютера при работе пользователя. Изменения этих политик применяются к рабочей станции при ее перезагрузке или через заданный интервал времени в результате фонового обновления. На практике рекомендуется не включать фоновое обновление групповых политик.
* **Конфигурация пользователя**, определяющая настройки профиля пользователя на клиентской рабочей станции. Изменения этих политик применяются к рабочей станции при смене сеанса работы пользователя или через заданный интервал времени в результате фонового обновления.

В обеих частях имеются следующие узлы групповой политики (рис. 14):

* **Конфигурация программ**, позволяющая задавать различные режимы установки новых программ на компьютере пользователя.
* **Конфигурация Windows**, служащая для настройки параметров системы безопасности компьютеров, на которые действует данная групповая политика.
* **Административные шаблоны**, задающие параметры реестра, рабочего стола, компонент операционной системы и приложений.

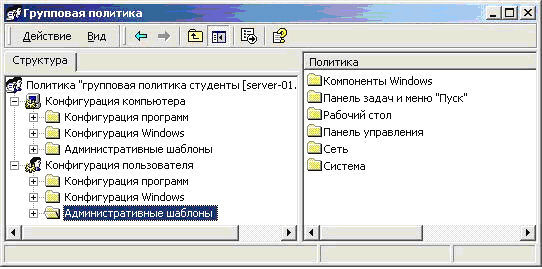


Рис. 14. Состав компонента **Административные шаблоны** групповой политики

Наиболее часто в компьютерной сети фирмы (организации) необходимо конфигурировать параметры профиля пользователей, большая часть которых находится в компоненте **Административные шаблоны Конфигурации пользователя** (см. рис. 14).

Настроить профиль пользователей, входящих в подразделение студенты, так, чтобы в программе **Проводник** в разделе меню **Сервис** отсутствовала команда **Свойства папки**, позволяющая открыть просмотр системных и скрытых файлов. Для этого необходимо выполнить следующие действия:

1. Открыть папку **Конфигурация пользователя – Административные шаблоны – Компоненты Windows** – **Проводник** и выбрать политику **Удалить команду «свойства папки» из меню «Сервис»** (рис. 15).
2. Двойным щелчком мыши открыть свойства выбранной политики и включить выбранную политику (рис. 16).
3. Открыть закладку **Объяснение** и изучить действие выбранной политики (рис.17). При помощи кнопок **Предыдущая политика** и **Следующая политика** можно изучать другие политики и управлять их назначением.

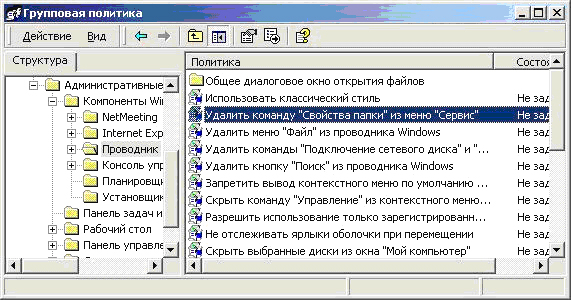


Рис. 15. Состав возможных политик компонента **Проводник**

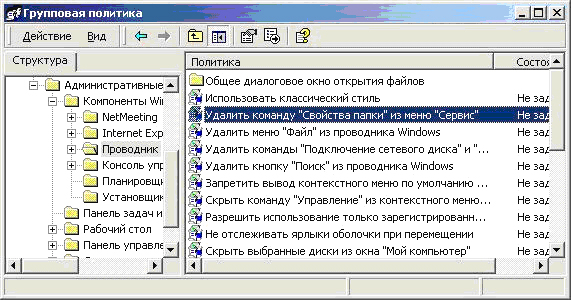


Рис. 16. Пример свойств выбранной политики

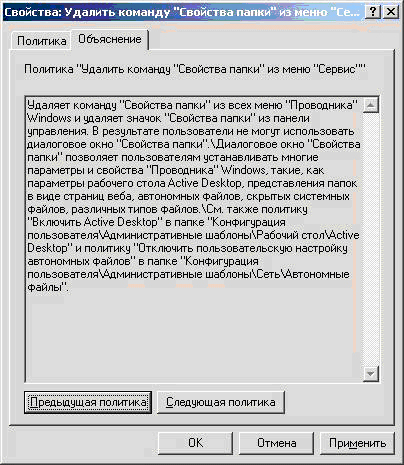


Рис. 17. Пример объяснения действия выбранной политики

1. Проверить действие выбранной политики на рабочей станции домена. Для этого войти в систему на виртуальной машине одним из пользователей подразделения **студенты**. Следует напомнить, что политики узла **Конфигурация пользователя** применяются на любом компьютере при входе пользователя в домен.
2. В групповой политике подразделения **студенты** включить политику **Удалить команду «Выполнить» из меню «Пуск»** (рис.18), изучить объяснение выбранной политики и проверить ее действие.

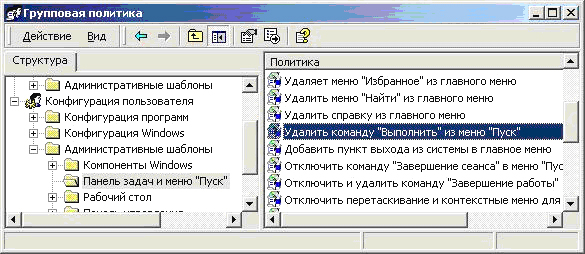


Рис. 18. Политика **Удалить команду «Выполнить» из меню «Пуск»**

1. Изучить другие возможные политики узла **Конфигурации пользователя – Административные шаблоны**.

***Перенаправление папки Мои документы на домашнюю папку пользователя***

Среди политик узла **Конфигурация пользователя – Конфигурация Windows** полезно использовать политику **Перенаправление папки**, позволяющую в профиле пользователя перенаправить папку **Мои документы** на домашнюю папку пользователя.

Отметим преимущества перенаправления папки **Мои документы**.

Некоторые из следующих преимуществ относятся к перенаправлению любой папки, но перенаправление папки **Мои документы** может быть особенно выгодным, поскольку эта папка со временем увеличивается.

* Даже если пользователь входит в сеть с различных компьютеров, все документы всегда доступны.
* При использовании перемещаемого профиля пользователя только сетевой путь к папке **Мои документы** является его частью, а не сама папка. Поэтому ее содержимое не нужно копировать и перемещать между клиентом и сервером каждый раз при входе пользователя в систему или его выходе, что ускоряет процессы входа и выхода.
* Сетевой администратор может архивировать данные, хранящиеся на сервере. Это является более безопасным, поскольку не требуется вмешательство пользователя.
* Системный администратор может устанавливать дисковые квоты с помощью групповой политики, ограничивая дисковое пространство, выделенное пользователю для домашних папок.
* Данные пользователя могут быть перенаправлены на жесткий диск локального компьютера с другого жесткого диска, на котором хранятся системные файлы. Это обезопасит пользовательские файлы, если необходимо будет переустановить операционную систему.

1. В групповой политике подразделения **студенты** выбрать политику **Конфигурация пользователя –** **Конфигурация Windows** – **Перенаправление папки – Мои документы** (рис.19) и открыть ее свойства (рис. 20).
2. В свойствах выбрать политику **Перенаправлять папки всех пользователей в одно место** и указать сетевой путь к конечной папке (рис. .21). При этом можно воспользоваться кнопкой **Обзор**, позволяющей указать размещение в сети каталога **Homedir** (рис. 22), в котором расположены домашние папки пользователей созданного домена. Чтобы пользователи получали доступ к своим домашним папкам, имя папки следует указать при помощи переменной **%Username%** (рис. 21).

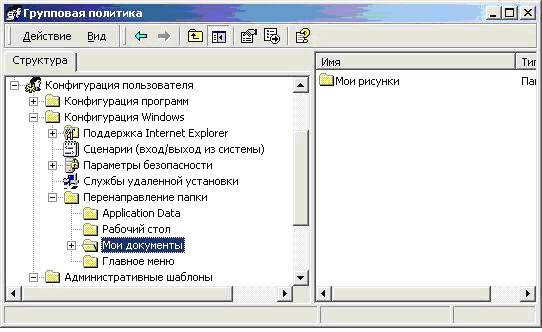


Рис. 19. Политика **Перенаправление папки Мои документы**

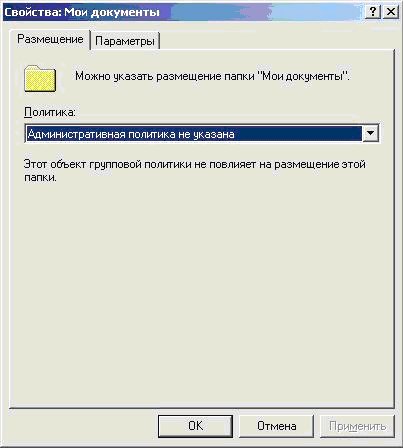


Рис. 20. Окно свойств политики **Перенаправление папки Мои документы**

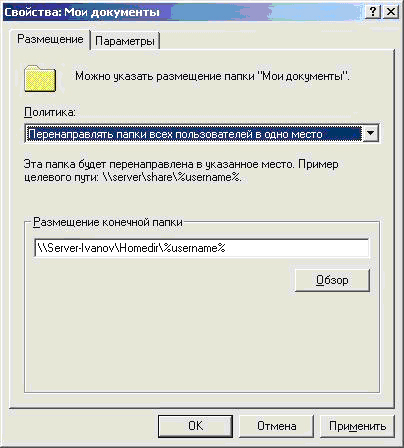


Рис. 21. Формирование политики перенаправления папки **Мои документы** на домашнюю папку пользователя

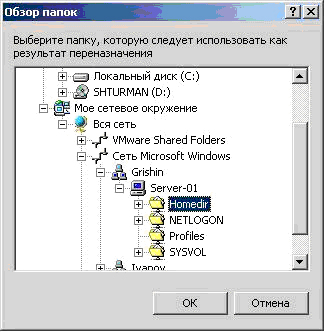


Рис. 22. Указание сетевого пути   
к каталогу размещения домашних папок пользователей

1. Проверить действие политики перенаправления папки **Мои документы**. Для этого войти на рабочую станцию домена пользователем подразделения **студенты**, сохранить произвольный документ в папке **Мои документы** и убедиться, что этот документ появился на сетевом диске **Z**.

**Задание на самостоятельную работу**

В групповой политике подразделения **студенты** найти и включить набор политик, не позволяющих пользователю этого подразделения просматривать сеть и сетевые ресурсы, кроме сетевой домашнее папки (диска  **Z**).