Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра вычислительной техники и защиты информации

Р.Р. Галимов, Е.И. Ряполова

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Рекомендовано к изданию Редакционно-издательским советом
федерального государственного бюджетного образовательного учреждения
высшего образования
«Оренбургский государственный университет»
в качестве методических указаний для студентов, обучающихся по программам
высшего образования по направлению подготовки
10.03.01 Информационная безопасность

Оренбург
2016

УДК 004.3(076)
ББК 32.973.26-04я7
Г 15

Рецензент - кандидат технических наук, доцент Д.В. Горбачев

Галимов, Р.Р.
Г 15 Управление информационной безопасностью: методические указания / Р.Р. Галимов, Е.И. Ряполова; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2016. – 88 с.

Методические указания содержат 13 лабораторных работ. Каждая работа включает теоретическое изложение материала, постановку задачи, порядок выполнения.

Методические указания рекомендованы преподавателям как вспомогательный материал в организации и проведении занятий, а также студентам по профилю подготовки – «Комплексная защита объектов информатизации» – для аудиторного и самостоятельного освоения лабораторного курса дисциплины «Управление информационной безопасностью».

Содержание

Введение

Настоящие методические указания предназначены для получения практических навыков студентами по профилю подготовки - «Комплексная защита объектов информатизации» при изучении дисциплины «Управление информационной безопасностью».

Методические указания содержат 13 работ. Предлагаемые задания охватывают основные разделы рабочей программы, связанные вопросами применения политик информационной безопасности в компьютерных вычислительных системах и её администрирования.

Общие методические рекомендации по использованию лабораторных работ и методических указаний:

- к выполнению лабораторной работы следует приступать после ознакомления с теоретической частью соответствующего раздела и рекомендациями, приведенными в конкретной работе;

- лабораторные работы рекомендуется выполнять в порядке их нумерации;

- рекомендуется для экономии времени отчеты о лабораторных работах оформлять в виде протоколов работы с обязательным указанием номера, темы, цели работы и выводов с краткой характеристикой результата;

- дополнительные сведения по лабораторным работам содержатся в прилагаемом списке литературы.

Лабораторный курс может быть освоен на индивидуальном компьютере с средствами виртуализации, например, VirtualBox, оценки защищенности MSAT, поиска уязвимостей Microsoft Baseline Security analyzer, дистрибутивом операционной системы Windows Server 2008,.

Методические указания рекомендовано преподавателям как вспомогательный материал в организации и проведении занятий, а также студентам - для аудиторного и самостоятельного освоения лабораторной части дисциплины «Управление информационной безопасностью».

1 Лабораторная работа №1. Оценка информационных рисков организаций с использованием Microsoft Security Assessment Tool

Цель работы: получить навыки по оценке рисков организаций

1.1 Теоретическая часть

В данной работе изучается метод оценки информационных рисков предприятия на основе метода Microsoft, реализованного в бесплатной программе Microsoft Security Assessment Tool (MSAT) .

Приложение предназначается для организаций с числом сотрудников менее 1000 человек, чтобы содействовать лучшему пониманию потенциальных проблем в сфере безопасности .

В ходе работы, пользователь, выполняющий роль аналитика, ответственного за вопросы безопасности, отвечает на две группы вопросов .

Первая из них посвящена бизнес-модели компании, и призвана оценить риск для бизнеса, с которым компания сталкивается в данной отрасли и в условиях выбранной бизнес-модели. Создается так называемый профиль риска для бизнеса (ПРБ) .

Вопросы этого этапа разбиты на 6 групп. Первая группа касается общих сведений о компании - название, число компьютеров, серверов и т.д.(рисунок 1.1). Вторая группа вопросов озаглавлена «Безопасность инфраструктуры». Примеры вопросов – «использует ли компания подключение к Интернет», «размещаются ли службы, используемые как внешними, так и внутренними клиентами, в одном и том же сегменте» и т.д. Остальные группы – «Безопасность приложений», «Безопасность операций», «Безопасность персонала», «Среда» .

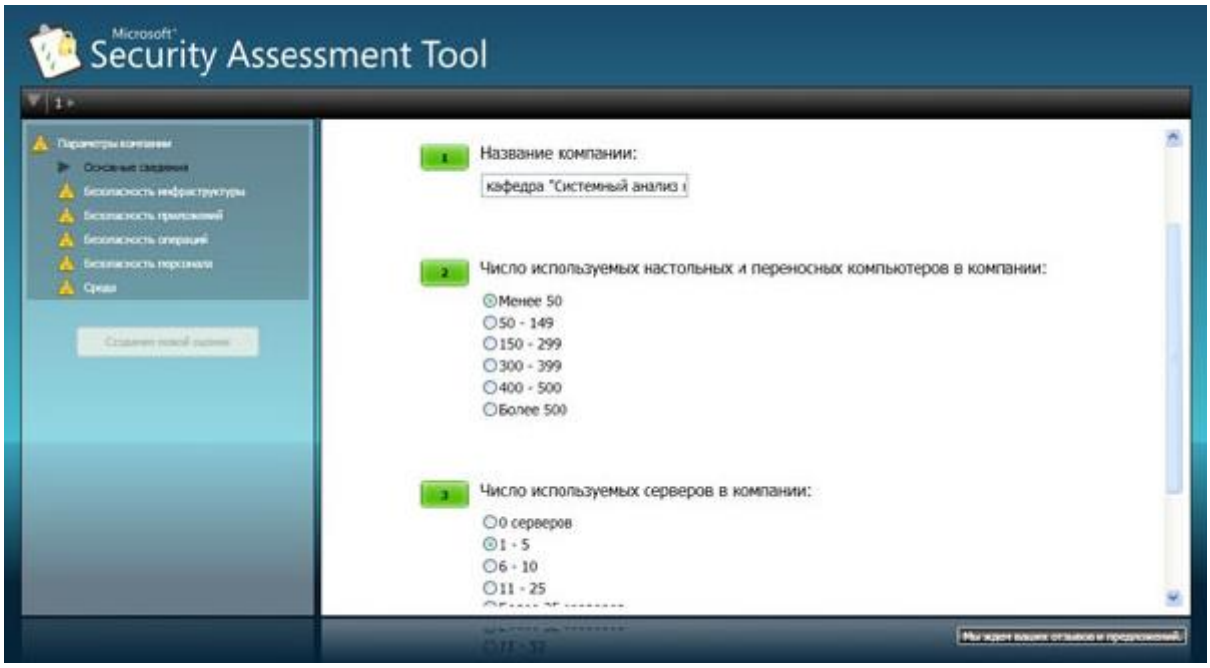


Рисунок 1.1 - Информация о компании

Когда проведен первый этап оценки, полученная информация обрабатывается (для этого требуется подключение к Интернет), после чего начинается второй этап анализа. Для технических специалистов он будет более интересен, так как касается используемых в компании политик, средств и механизмов защиты (рисунок 1.2).

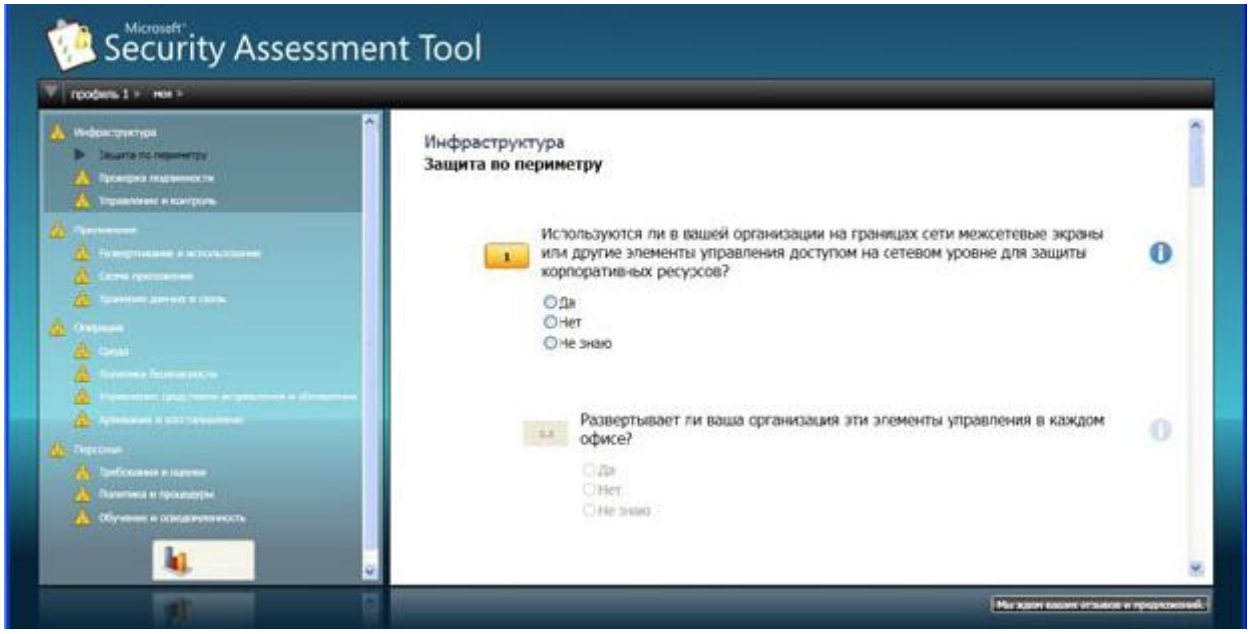


Рисунок 1.2 - Анализ используемых механизмов защиты

Вопросы организованы в соответствии с концепцией многоуровневой (эшелонированной) защиты. Сначала рассматривается защита инфраструктуры (защита периметра, аутентификация), затем вопросы защиты на уровне приложений, далее проводится анализ безопасности операций (определена ли политика безопасности, политика резервного копирования и т.д.), последняя группа вопросов касается работы с персоналом (обучение, проверка при приеме на работу и т.д.) .

Во многом тематика вопросов соответствует разделам стандартов ISO 17799 и 27001, рассмотренных в теоретической части курса .

После ответа на все вопросы программа вновь обращается к удаленному серверу и генерирует отчеты. Наибольший интерес для технических специалистов представляет «Полный отчет» . В частности, он содержит предлагаемый список приоритетных действий. Фрагмент списка представлен в таблице 1.1.

Таблица 1.1 - Список предлагаемых действий

Список приоритетных действий	
Предмет анализа	Рекомендация
Высокий приоритет	
Операции > Управление средствами исправления и обновления > Управление средствами исправления	Наличие политики исправлений и обновлений для операционных систем является полезным начальным шагом, однако необходимо разработать такую же политику и для приложений. Разработайте такую политику, пользуясь сведениями, доступными в разделе, посвященном передовым методикам. Сначала установите исправления для внешних приложений и приложений Интернета, затем для важных внутренних приложений и, наконец, для не особо важных приложений.

Таким образом, представленная программа позволяет оценить информационные риски предприятия и предлагает рекомендации для повышения уровня информационной безопасности.

1.2 Постановка задачи

Подробно опишите реально существующее или вымышленное малое предприятие: сферу деятельности, состав и структуру информационной системы, особенности организации процесса защиты информации, применяемые методы и средства.

С помощью программы MSAT проведите оценку рисков для организаций.

Таблица 1.2 –Варианты заданий

№	Типы предприятий
1	Факультет
2	Сеть магазинов розничной торговли
3	Банк
4	Отделение почты России
5	Отдел IT технологий
6	Производственный цех мебели
7	Интернет магазин
8	Складские помещения
9	Теплогенерирующая компания
10	Автомастерская

1.3 Контрольные вопросы

1 Дайте определение понятия риска, связанного с безопасностью?

2 Опишите метод оценки риска, реализованного в программе MSAT.

3 Чему посвящены вопросы из раздела «Инфраструктура»?

4 Перечислите 4 основных компонента информационной системы предприятия, которые анализируются в программе для оценки рисков.

5 Дайте определение понятия «Профиль риска для бизнеса».

6 Дайте определение понятия «Индекс эшелонированной защиты».

2 Лабораторная работа №2. Анализ уязвимостей компьютерной системы с использованием программных средств

Цель работы: получить навыки по анализу рисков информационной системы

2.1 Теоретическая часть

Microsoft Baseline Security analyzer - программа, позволяющая проверить уровень безопасности установленной конфигурации операционной системы (ОС) Windows 2000, XP, Server 2003, Vista, Server 2008. Также проверяется и ряд других приложений разработки Microsoft (http://technet.microsoft.com/ru-ru/security/cc184924(en-us).aspx) (рисунок 2.1).

Рисунок 2.1 – Выбор объекта сканирования

В процессе работы BSA проверяет наличие обновлений безопасности операционной системы, офисного пакета Microsoft Office(для версий XP и более поздних), серверных приложений, таких как MS SQL Server, MS Exchange Server, Internet Information Server и т.д. Кроме того, проверяется ряд настроек, касающихся безопасности, например, действующая политика паролей. При запуске открывается окно, позволяющее выбрать объект проверки – один компьютер (выбирается по имени или ip-адресу), несколько (задаваемых диапазоном ip-адресов или доменным именем) или просмотреть ранее сделанные отчеты сканирования системы. При выборе сканирования отдельного компьютера по умолчанию подставляется имя локальной станции, но можно указать имя или ip-адрес другого компьютера .

Можно задать перечень проверяемых параметров (рисунок 2.2):

- проверка на наличие уязвимостей Windows, вызванных некорректным администрированием;
- проверка на «слабые» пароли (пустые пароли, отсутствие ограничений на срок действия паролей и т.д.);
- проверка на наличие уязвимостей web-сервера IIS, вызванных некорректным администрированием;
- аналогичная проверка в отношении СУБД MS SQL Server;
- проверка на наличие обновлений безопасности.

Перед началом работы программа обращается на сервер Microsoft для получения перечня обновлений для ОС и известных уязвимостей. Если на момент проведения проверки компьютер не подключен к Интернет, база уязвимостей не будет обновлена, программа об этом сообщит и дальнейшие проверки выполняться не будут . В подобных случаях нужно отключать проверку обновлении безопасности (сбросив соответствующую галочку на экране рисунок 2.2).

Для успешной проверки локальной системы необходимо, чтобы программа выполнялась от имени учетной записи с правами локального администратора .

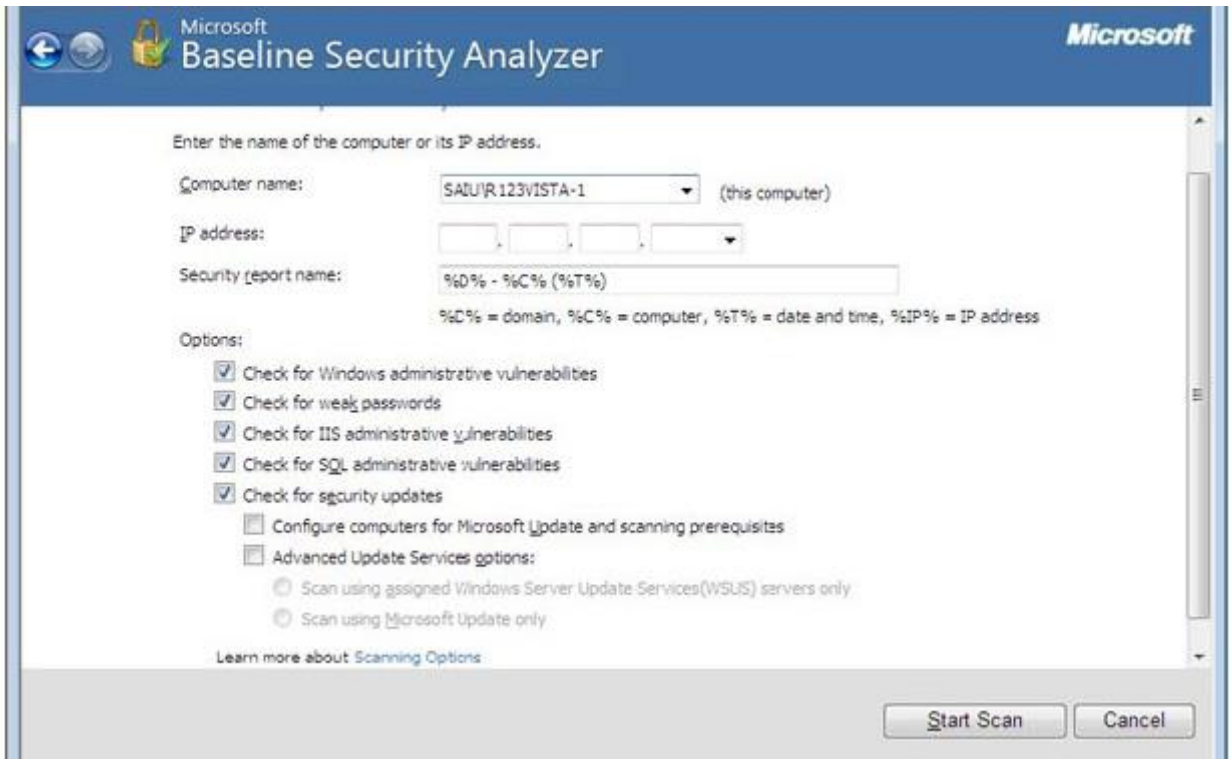


Рисунок 2.2 – Настройка параметров сканирования

По результатам сканирования формируется отчет, в начале которого дается общая оценка уровня безопасности конфигурации проверяемого компьютера. В приведенном примере на рисунке 2.3 уровень риска оценивается как «серьезный» (Severe risk).

Рисунок 2.3 - Оценка уровня риска

Далее приводится перечень обнаруженных уязвимостей, разбитый на группы: результаты проверки установки обновлений, результаты проверки Windows .

Кроме версии программы с графическим интерфейсом, существует также утилита с интерфейсом командной строки, называется она mbsacli.exe и находится в том же каталоге, куда устанавливался Baseline security analyzer, например, «C:\Program Files\Microsoft Baseline Security Analyzer 2». У утилиты есть достаточно много ключей, получить информацию о которых можно запустив ее с ключом «/?».

Запуск без ключей приведет к сканированию локального компьютера с выводом результатов на консоль. Чтобы сохранить результаты сканирования, можно перенаправить вывод в какой-либо файл. Например: mbsacli > mylog.txt. Хотелось бы еще раз обратить внимание на то, что при настройках по умолчанию сначала утилита обращается на сайт Майкрософт за информацией об обновлениях. Если соединение с Интернет отсутствует, то утилиту надо запускать или с ключом /nd (указание «не надо скачивать файлы с сайта Майкрософт») или с ключом /n Updates (указание «не надо проводить проверку обновлений»).

2.2 Постановка задачи

1 Выполните проверку вашего компьютера с помощью Microsoft Baseline security analyzer. В отчете о выполнении лабораторной укажите:

- как оценен уровень уязвимости вашего компьютера;
- какие проверки проводились, в какой области обнаружено наибольшее количество уязвимостей;
- опишите наиболее серьезные уязвимости каждого типа, выявленные на вашем компьютере.

Проведите анализ результатов - какие уязвимости можно устранить, какие - нельзя из-за особенностей конфигурации ПО или использования компьютера.

2 Выполните удаленную проверку соседнего компьютера из сети лаборатории. Опишите наиболее серьезные уязвимости.

3 Теперь выполните проверку нескольких компьютеров с помощью утилиты mbsacli. Для этого, предварительно создайте текстовый файл с перечнем имен компьютеров или ip-адресов и запускайте mbsacli с ключом /listfile, после которого указывается имя файла с перечнем компьютеров. В результате получите сообщение примерно следующего содержания:

Computer Name, IP Address, Assessment, Report Name

HOME\MYNBOOK, 127.0.0.1, Severe Risk, HOME - MYNBOOK (06.12.2008 13-51)

Для того, чтобы увидеть подробные результаты проверки, надо повторно запустить mbsacli с ключом /ld, после которого указывается имя отчета. Вывод можно перенаправить в текстовый файл для дальнейшей обработки. Например:

mbsacli /ld "HOME - MYNBOOK (06.12.2008 13-51)" > c:\test\report1.txt

После выполнения задания проанализируйте результаты, кратко опишите их в отчете по лабораторной работе.

3 Лабораторная работа №3. Создание контроллера домена на базе Windows Server 2008

Цель работы: закрепить теоретические знания о службе Active Directory

3.1 Постановка задачи

На виртуальной машине установить Windows Server 2008 и создать контроллер домена для определенной организации.

3.2 Порядок выполнения работы

1 Вставьте в DVD-привод установочный диск системы Windows Server 2008. При использовании виртуальной машины (VM) можно смонтировать ISO-образ установочного DVD. Справочная информация об этом есть в документации виртуальной машины .

2 Запустите установку системы. Если жесткий системный диск пустой, то следует загрузить систему с DVD. Когда же на диске есть данные, вам может быть предложено нажать клавишу для загрузки с DVD. Если система не загружается с DVD, то откройте параметры BIOS компьютера и сконфигурируйте порядок загрузки с DVD. Запустится Мастер установки Windows (Install Windows Wizard) .

3 Выберите язык, региональные параметры и раскладку клавиатуры для системы, после чего щелкните кнопку Далее (Next).

4 Щелкните кнопку Установить (Install Now).

5 Выберите вариант установки системы Windows Server 2008, пункт Полная установка (Full Installation), и щелкните кнопку Далее (Next).

6 Установите флажок Я принимаю условия лицензии (I Accept the License Terms') и щелкните кнопку Далее (Next).

7 Щелкните кнопку Полная установка (дополнительные параметры) (Custom (Advanced)).

8 На странице Выберите раздел для установки Windows (Where Do You Want to Install Windows) выберите диск, на который хотите установить систему. Чтобы создать, расширить или форматировать разделы либо загрузить настраиваемый драйвер массового храпения для получения доступа к подсистеме диска, щелкните кнопку Загрузка драйвера (Driver Options (Advanced)).

9 Щелкните кнопку Далее (Next). Откроется диалоговое окно Установка Windows (Installing Windows). В нем отображается ход выполнения установки. После ее завершения будет указано, что перед первым входом в систему надо изменить пароль пользователя.

10 Щелкните ОК. В поля Новый пароль (New Password) и Подтверждение (Confirm Password) введите пароль для учетной записи Администратор (Administrator) и нажмите клавишу Enter. Щелкните ОК. Откроется рабочий стол учетной записи Администратор (Administrator).

11 Дождитесь появления рабочего стола учетной записи Администратор (Administrator) . Откроется окно Задачи начальной настройки (Initial Configuration Tasks).

12 В окне задач начальной настройки сконфигурируйте следующие параметры:

– часовой пояс (Time Zone): в соответствии с вашей средой;
– имя компьютера (Computer Name)(например, SERVER01) .

13 В окне задач начальной настройки щелкните ссылку Настроить сеть (Configure Networking) и проверьте соответствие конфигурации IP с вашей средой.

14 Если сервер подключен к Интернету, то строго рекомендуется щелкнуть ссылку Загрузить и установить обновления (Download and Install Updates), чтобы установить на сервере последние обновления Microsoft.

15 После установки обновлений перезагрузите сервер. В дальнейшем будет создан домен с IP-адресами в диапазоне 10.0.0.11-10.0.0.20 и маской подсети 255.255.255.0. Если эти адреса используются в вашей производственной среде и сервер подключен к корпоративной сети, то надо соответствующим образом изме-

нить IP-адреса, чтобы создаваемый домен (например, contoso.com) не конфликтовал с вашей корпоративной сетью.

16 В окне Задачи начальной настройки (Initial Configuration Tasks) щелкните ссылку Настроить сеть (Configure Networking). Откроется диалоговое окно Сетевые подключения (Network Connections).

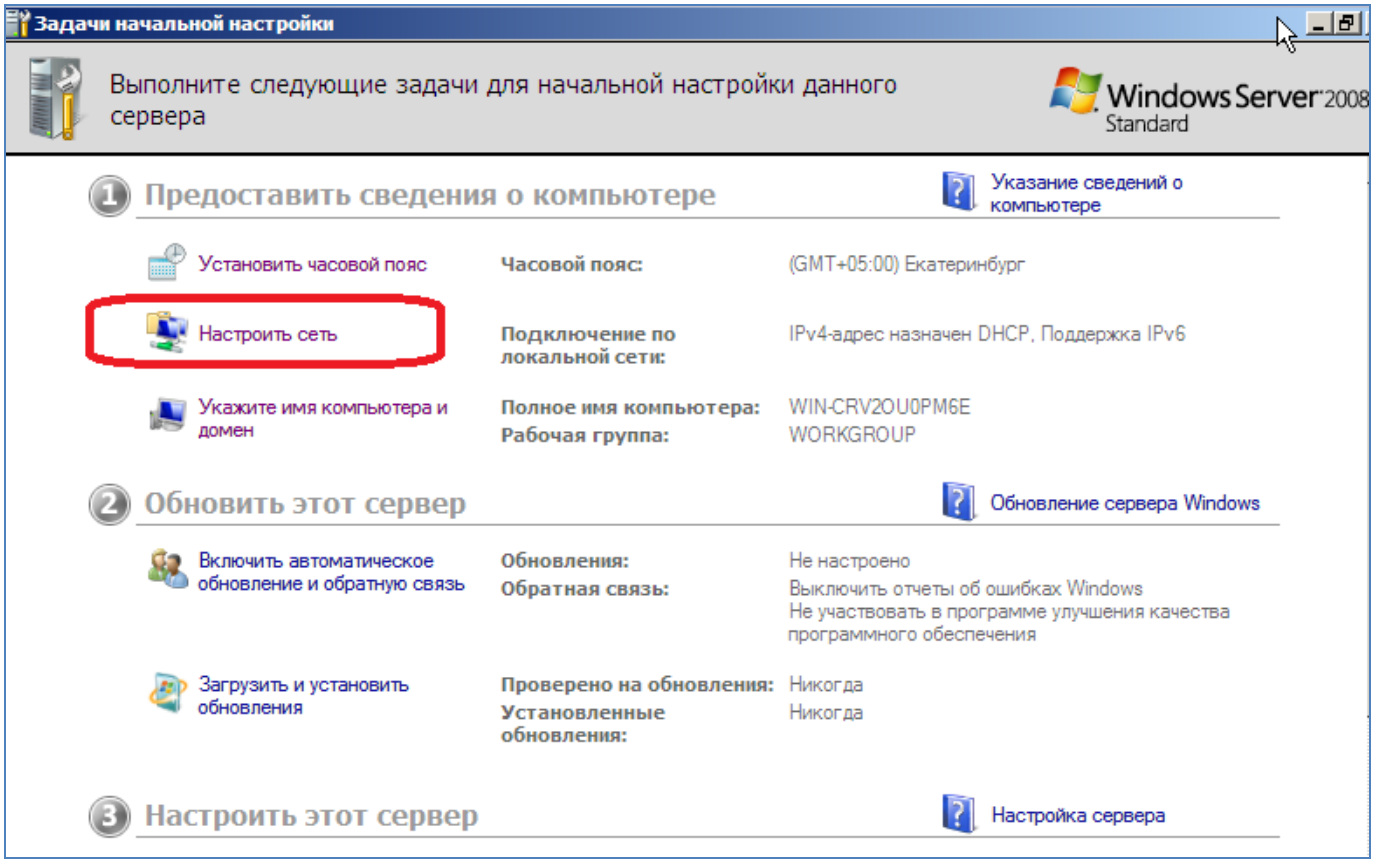


Рисунок 3.1 – Выбор настройки сети

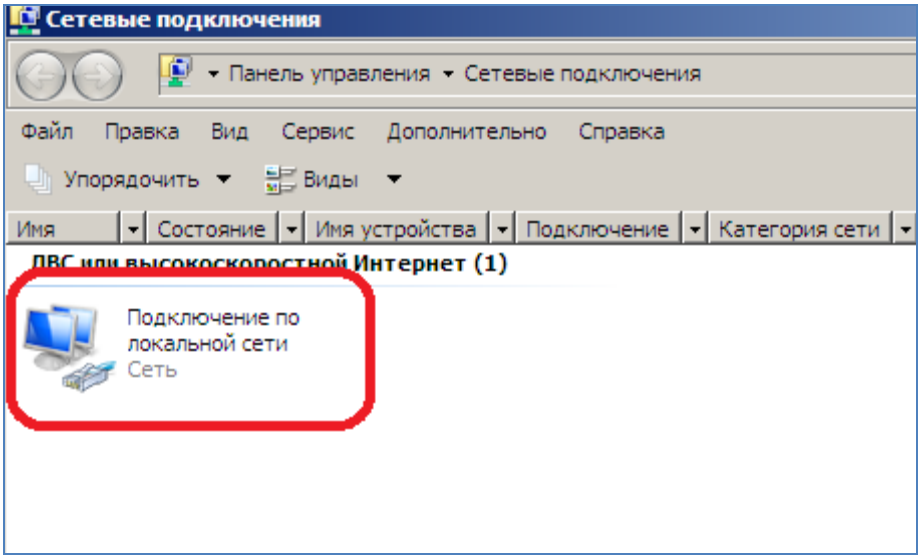


Рисунок 3.2 –Настройка локальной сети

17 Выберите Подключение по локальной сети (Local Area Connection).

18 На панели инструментов щелкните команду Настройка параметров подключения (Change Settings of This Connection).

19 Выберите пункт Протокол Интернета версии 4 (TCP / IP v 4) (Internet Protocol Version 4 (TCP/IPv4)) н щелкните кнопку Свойства (Properties) . В системе Windows Server 2008 реализована также встроенная поддержка протокола Интернета версии 6 (TCP/lPv6).

20 Щелкните пункт Использовать следующий IP-адрес (Use the Following IP Address). Введите такие параметры конфигурации:

– IP-адрес (IP Address): 10.0.0.11;
– маска подсети (Subnet Mask): 255.255.255.0;
– основной шлюз (Default Gateway): 10.0.0.11;
– предпочитаемый DNS-сервер (Preferred DNS Server): 10.0.0.11.

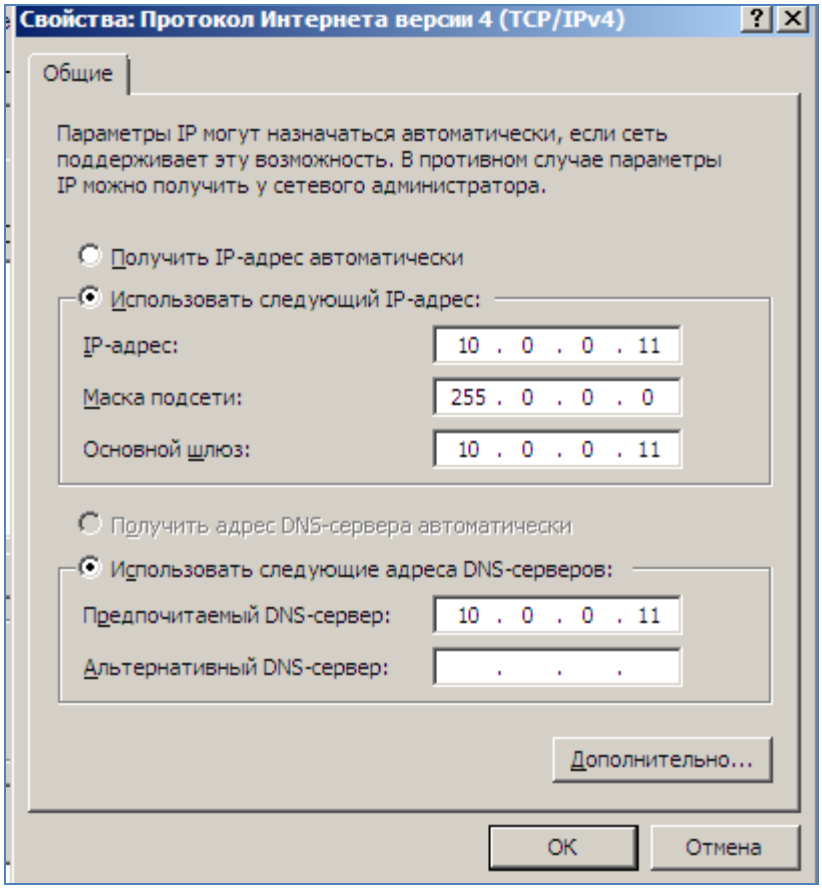


Рисунок 3.3 –Настройка локальной сети

Щелкните OK, а затем — кнопку Закрыть (Close).

21 Установите флажок Не показывать это окно при входе в систему (Do Not Show This Window at Logon), чтобы это окно больше не появлялось при загрузке. Чтобы в будущем открыть окно задач начальной настройки, используйте команду Oobe.exe.

22 Щелкните кнопку Закрыть (Close) в нижней части окна задач начальной настройки. Откроется Диспетчер сервера (Server Manager). Если данное окно не отображается, то в группе программ «Администрирование (Administrative Tools)» откройте «Диспетчер сервера (Server Manager)».

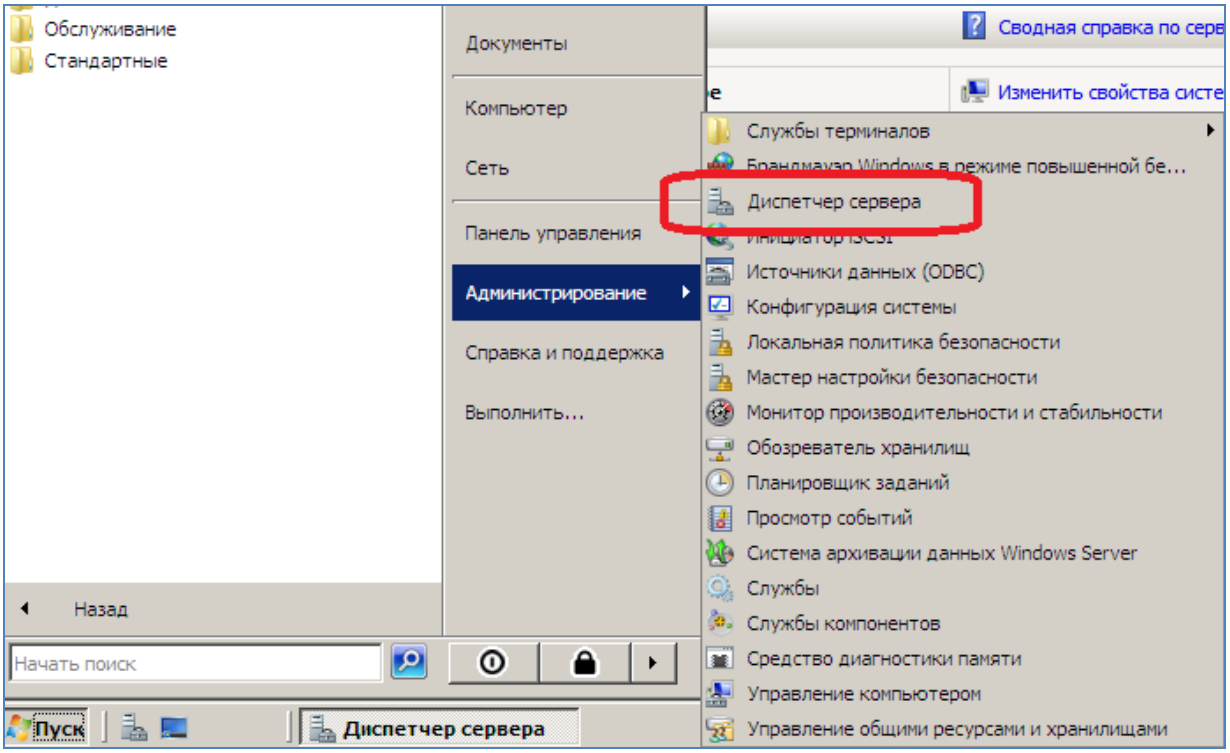


Рисунок 3.4 –Выбор пункта меню «Диспетчер сервера»

23 В разделе Состояние роли (Roles Summary) домашней страницы щелкните кнопку Добавить роли (Add Roles). Будет запущен Мастер добавления ролей (Add Roles Wizard). Щелкните кнопку Далее (Next).

24 На странице Выбор ролей сервера (Select Server Roles) установите флажок Доменные службы Active Directory (Active Directory Domain Services). Щелкните кнопку Далее (Next).

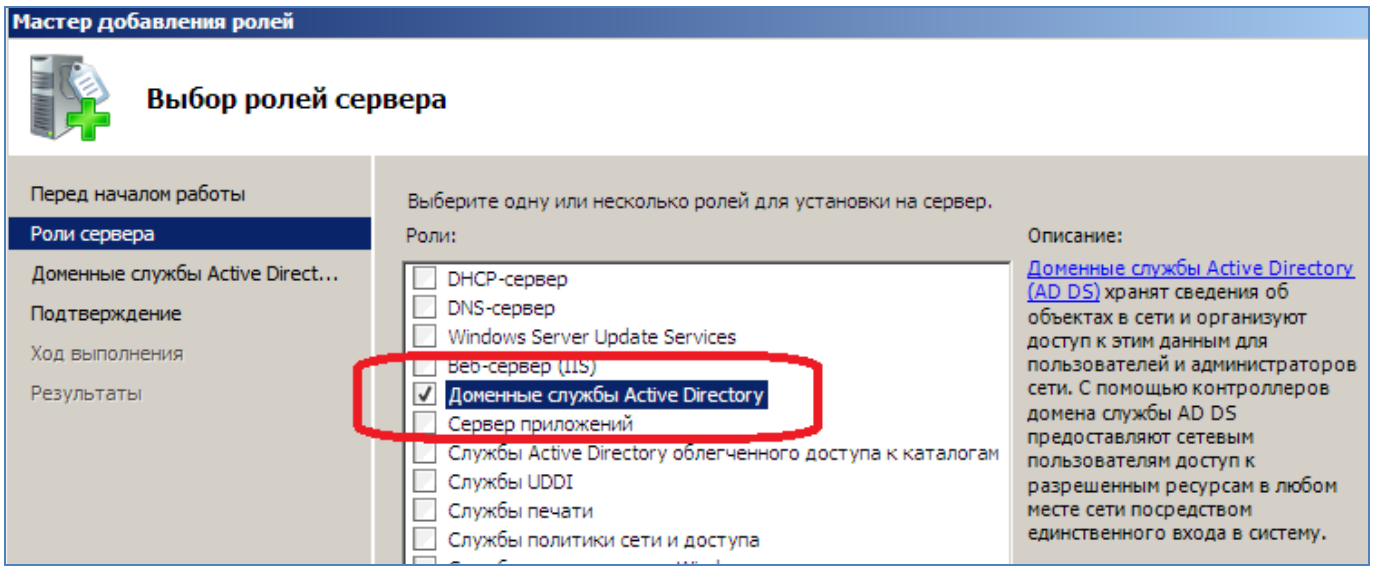


Рисунок 3.5 –Выбор роли сервера «Доменные службы Active Directory»

25 На странице Доменные службы Active Directory (Active Directory Domain Services) щелкните кнопку Далее (Next).

26 На странице Подтвердите выбранные элементы (Confirm Installation Selections) щелкните кнопку Установить (Install). Процесс выполнения задач установки отображается на странице Ход выполнения установки (Installation Progress).

27 На странице Результаты установки (Installation Results) просмотрите результаты установки и щелкните кнопку Закрыть (Close). В разделе Состояние роли (Roles Summary) домашней страницы Диспетчера сервера (Server Manager) вы увидите сообщение об ошибке, помеченное красным кружком с белым крестиком. В разделе Доменные службы Active Directory (Active Directory Domain Services) также появится сообщение. Обе ссылки открывают показанную на рисунке страницу роли доменных служб Active Directory в диспетчере сервера. Сообщение напоминает о том, что надо запустить команду Dcpromo.exe.

28 Щелкните кнопки Пуск (Start) и Выполнить (Run), введите команду Dcpromo.exe и нажмите клавишу Enter.

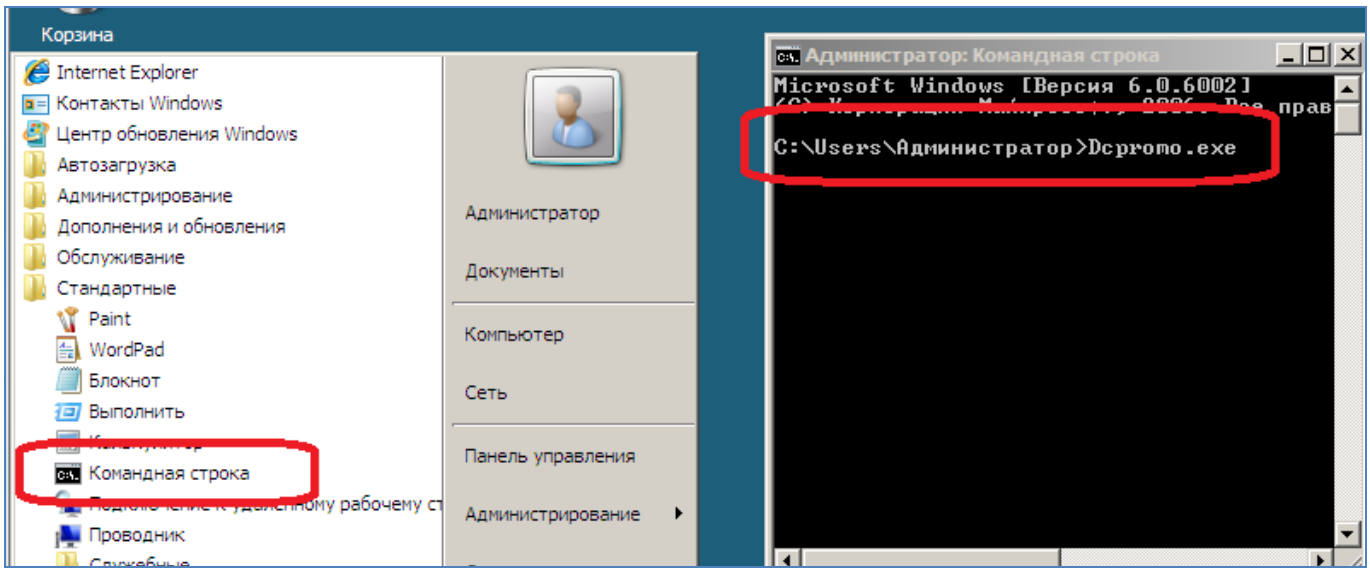


Рисунок 3.6 –Запуск программы командной строки Dcpromo.exe

29 Щелкните кнопку Далее (Next).

30 На странице Совместимость операционных систем (Operating System Compatibility) ознакомьтесь с предупреждением о заданных по умолчанию параметрах безопасности для контроллеров доменов системы Windows Server 2008, а затем щелкните кнопку Далее (Next).

31 На странице Выберите конфигурацию развертывания (Choose a Deployment Configuration) остановите свой выбор на конфигурации Создать новый домен в новом лесу (Create a New Domain in a New Forest) и щелкните кнопку Далее Next).

32 На странице Укажите имя корневого домена леса (Name the Forest Root Domain) введите в поле имя contoso.com и щелкните кнопку Далее (Next). Система проверит уникальность имен DNS и NetBIOS в сети.

33 На странице Задание режима работы леса (Set Forest Functional Level) выберите функциональный уровень Windows Server 2008 и щелкните кнопку Далее (Next).

34 Все функциональные уровни описаны в окне Подробности (Details) страницы. При выборе функционального уровня леса Windows Server 2008 все домены в лесу будут работать на уровне Windows Server 2008, обеспечивающем несколько новых возможностей системы Windows Server 2008.

35 Откроется страница Параметры дополнительного контроллера домена (Additional Domain Controller Options). По умолчанию будет выбран DNS-сервер. Мастер установки доменных служб Active Directory создаст инфраструктуру DNS в процессе установки AD DS. Первый контроллер домена в лесу должен быть сервером глобального каталога GC (Global Catalog) и не может быть контроллером домена только для чтения RODC (Read-Only Domain Controller).

36 Щелкните кнопку Далее (Next). Появится предупреждение о назначении статического IP-адреса. Поскольку конфигурация IPv6 не описана в данном руководстве, в упражнении 2 для сервера не был назначен статический IPv6-адрес. В упражнении 2 вы назначили статический IPv4-адрес, который будет использоваться в последующих упражнениях. В контексте текущего упражнения данное предупреждение можно проигнорировать.

37 Щелкните кнопку Да, компьютер будет использовать динамически назначаемый IP-адрес (не рекомендуется) (Yes, the Computer Will Use a Dynamically Assigned IP Address (Not Recommended)). Появится предупреждение о том, что для этого DNS-сервера не будет делегирования. В контексте данного упражнения вы можете проигнорировать эту ошибку. Делегирование доменов DNS будет рассмотрено в других работах.

38 Щелкните кнопку Да (Yes), чтобы закрыть окно предупреждения мастера установки доменных служб Active Directory.

39 На странице Расположение для базы данных, файлов журнала и SYSVOL (Location for Database, Log Files and SYSVOL) примите заданное по умолчанию размещение, для файла базы данных, файлов журнала службы каталогов и SYSVOL, а затем щелкните кнопку Далее (Next). В производственной среде эти файлы лучше всего хранить в трех отдельных томах, где нет приложений и других файлов, которые не имеют отношения к AD DS. Благодаря этому повысится производительность, а также эффективность архивации и восстановления.

40 На странице Пароль администратора для режима восстановления служб каталогов (Directory Services Restore Mode Administrator Password) введите строгий

пароль в поля Пароль (Password) и Подтверждение (Confirmed Password). Щелкните кнопку Далее (Next).

41 На странице Сводка (Summary) просмотрите выбранные параметры. Если какие-либо из них некорректны, то щелкните кнопку Назад (Back), чтобы внести модификации.

42 Дважды щелкните кнопку Далее (Next). Начнется процесс настройки AD DS. После его завершения потребуется перезагрузить сервер. При желании вы можете установить флажок Перезагрузка по завершении (Reboot on Completion).

4 Лабораторная работа №4. Оснастки Active Directory

Цель работы: получить навыки работы с оснасткой Active Directory

4.1 Постановка задачи

Создать настраиваемую консоль MMC с оснастками Active Directory — пользователи и компьютеры (Active Directory Users and Computers), Схема Active Directory (Active Directory Schema) и Управление компьютером (Computer Management).

4.1 Порядок выполнения работы

1 Войдите на машину SERVER01 как Администратор (Administrator).

2 Щелкните кнопку Пуск (Start) , в поле Начать поиск (Start Search) введите команду mmc. exe и нажмите клавишу Enter. Откроется пустая консоль MMC. По умолчанию новое окно консоли не развернуто внутри MMC. Разверните его, чтобы использовать преимущества полного размера окна приложения.

3 В меню Консоль (File) выберите команду Добавить или удалить оснастку (Add/Remove Snap-in). Откроется диалоговое окно Добавление и удаление оснастки Add or Remove Snap-ins), показанное на рисунке 4.1. Если оснастки не отображаются в списке справа, проверьте, установлен ли на машине набор средств RSAT.

4 В диалоговом окне Добавление и удаление оснастки (Add or Remove Snapins) в списке Доступные оснастки (Available Snap-ins) выберите Active Directory — пользователи и компьютеры (Active Directory Users and Computers).

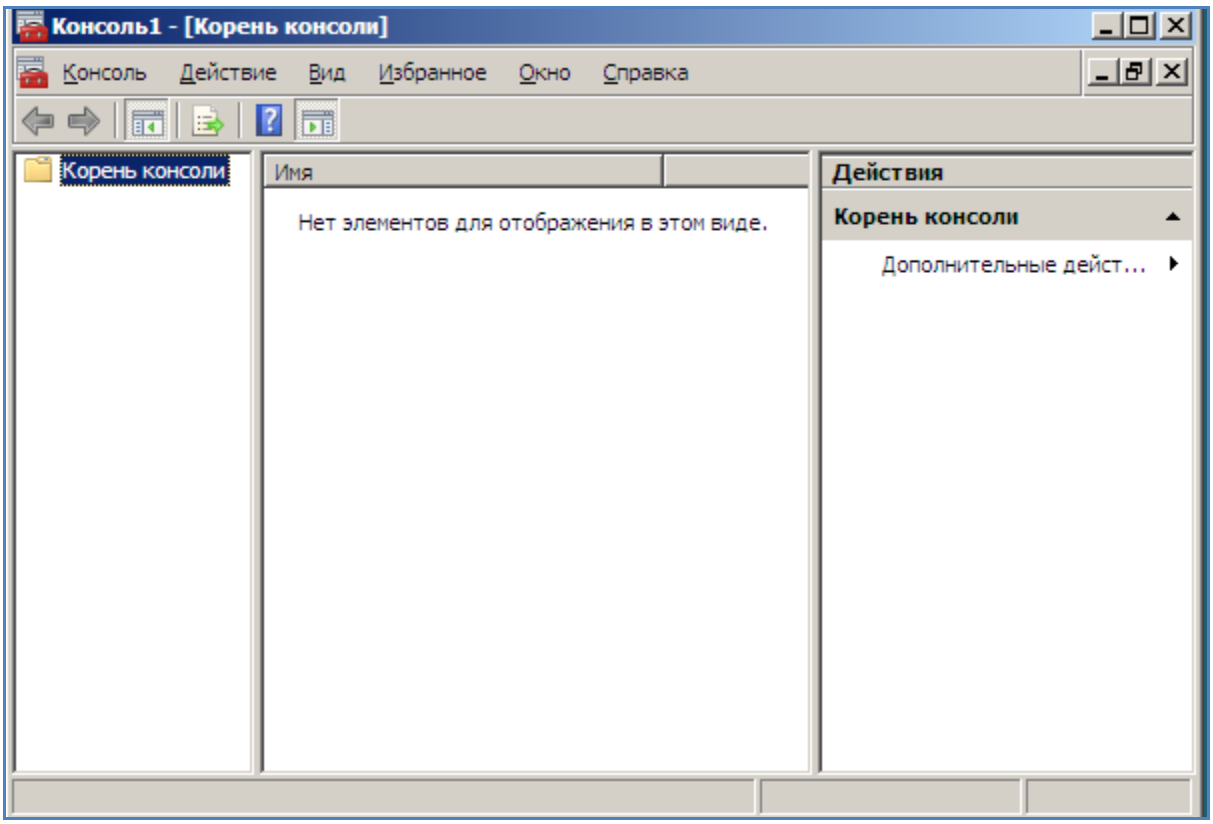


Рисунок 4.1 –Окно консоли

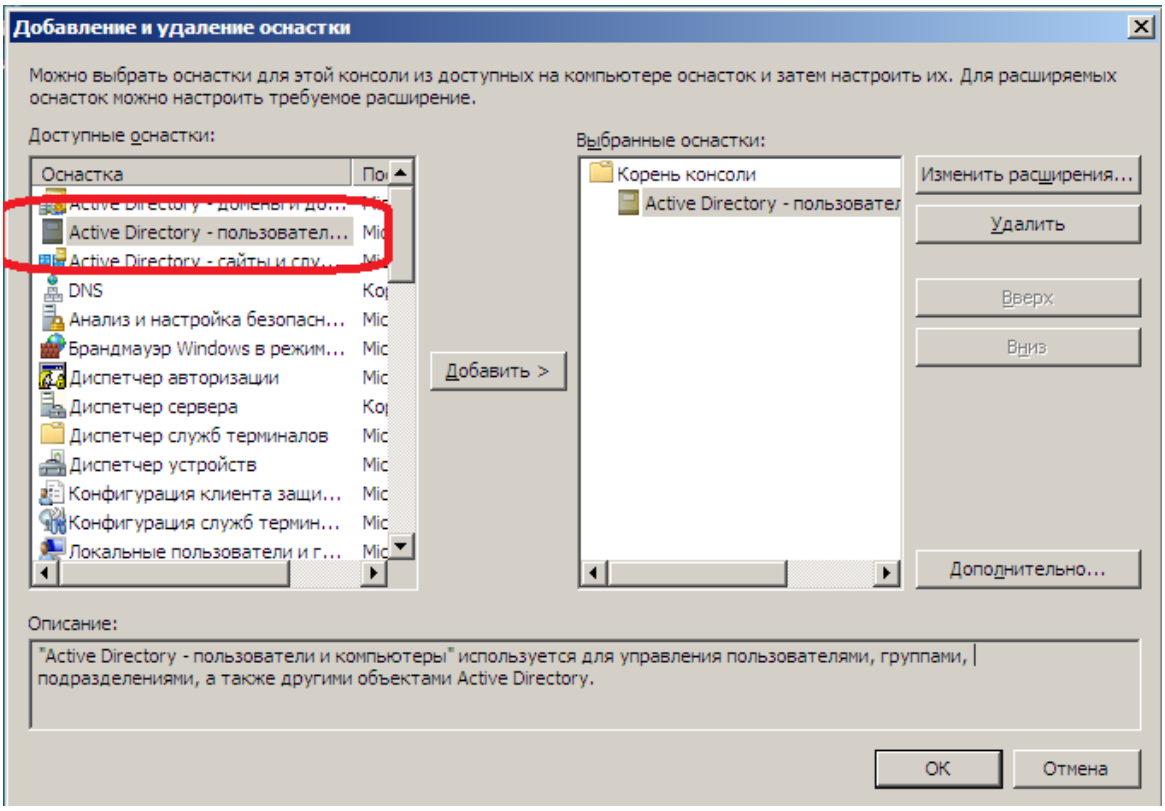


Рисунок 4.2 –Добавление оснастки «Active Directory - пользователи и компьютеры»

5 Щелкните кнопку Добавить (Add), чтобы добавить оснастку в список Выбранные оснастки (Selected Snap-ins). Обратите внимание, что оснастка Схема Active Directory (Active Directory Schema) недоступна. Она устанавливается вместе с ролью Доменные службы Active Directory (Active Directory Domain Services) с набором средств RSAT, но не регистрируется и не отображается.

6 Щелкните ОК, чтобы закрыть диалоговое окно добавления и удаления оснасток.

7 Щелкните кнопку Пуск (Start). В поле Начать поиск (Start Search) введите команду cmd.exe.

8 В окно командной строки введите команду regsvr32.exe schmmgmt.dll. Эта команда регистрирует динамически подключаемую библиотеку DLL (Dynamic Link Library) оснастки Схема Active Directory (Active Directory Schema). Данную операцию следует выполнить в системе один раз перед добавлением этой оснастки в консоль.

9 Появится строка с информацией об успешной регистрации. Щелкните ОК.

10 Вернитесь к настраиваемой консоли MMC и повторите шаги 2 - 6 , чтобы добавить оснастку Схема Active Directory (Active Directory Schema).

11 В меню Консоль (File) выберите команду Добавить или удалить оснастку (Add/Remove Snap-in).

12 В диалоговом окне Добавление и удаление оснастки (Add or Remove Snapins) выберите в списке доступных оснасток Управление компьютером (Computer Management).

13 Щелкните кнопку Добавить (Add), чтобы добавить оснастку в список Выбранные оснастки (Selected Snap-ins). Если оснастка поддерживает удаленное администрирование, вам будет предложено выбрать компьютер, которым вы хотите управлять (рисунок 4.3).

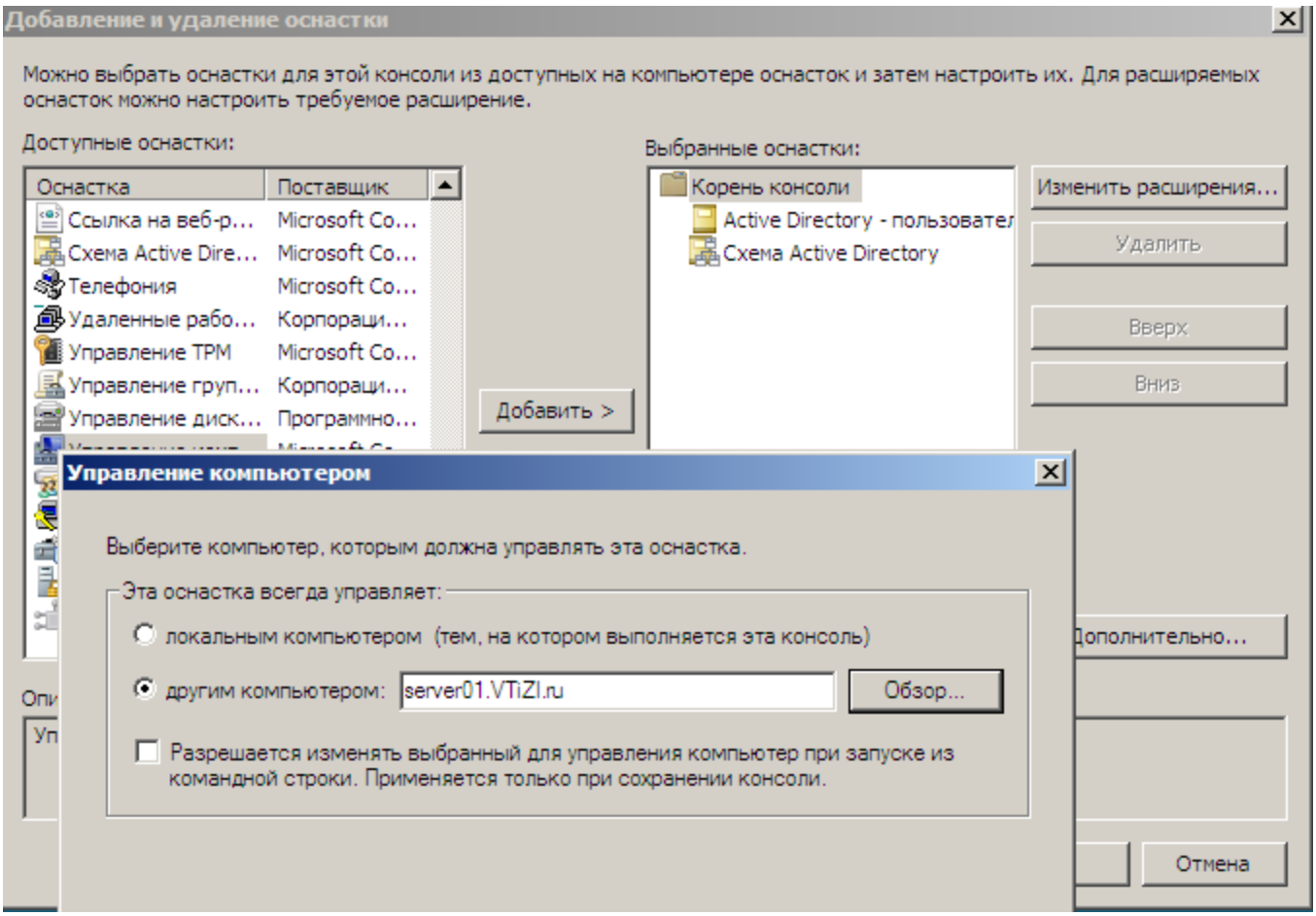


Рисунок 4.3 –Добавление оснастки «Управление компьютером»

14 Выберите опцию управления другим компьютером и введите имя компьютера - SERVER01м.

15 Щелкните кнопку Готово (Finish).

16 Щелкните ОК, чтобы закрыть диалоговое окно добавления и удаления оснасток.

17 В меню Консоль (File) выберите команду Сохранить (Save) и сохраните консоль под именем MyConsole.msc на рабочем столе. Закройте консоль.

18 Откройте консоль MyConsole.msc.

19 В меню Консоль (File) выберите команду Добавить или удалить оснастку (Add/Remove Snap-in).

20 В диалоговом окне Добавление и удаление оснастки (Add or Remove Snapins) выберите оснастку Просмотр событий (Event Viewer).

21 Щелкните кнопку Добавить (Add), чтобы добавить оснастку в список выбранных оснасток. Вам будет предложено выбрать компьютер для управления.

22 Выберите опцию Другим компьютером (Another Computer) и введите имя компьютера - SERVER01.

23 Щелкните ОК.

24 В меню Консоль (File) выберите команду Параметры (Options). В раскрывающемся списке Режим консоли (Console Mode) выберите режим «Пользовательский — полный доступ (User Mode — Full Access)»(рисунок 4.4).

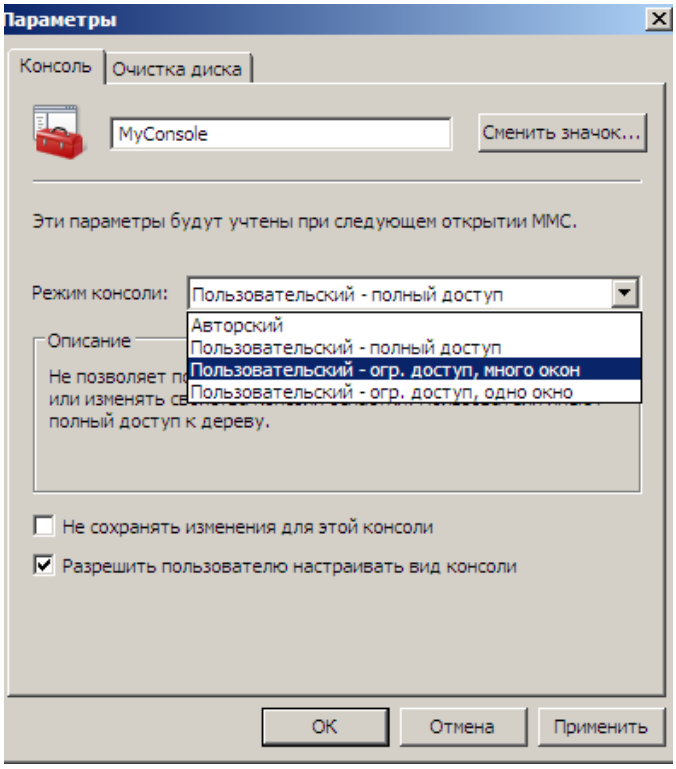


Рисунок 4.4 –Выбор режима консоли

25 Щелкните ОК. Сохраните и закройте консоль.

26 Откройте консоль, дважды щелкнув ее значок. Щелкните меню Консоль (File). Как видите, в меню нет команды «Добавить или удалить оснастку (Add/Remove Snap-in)». Закройте консоль.

27 Щелкните правой кнопкой мыши значок консоли и примените команду Автор (Author)(рисунок 4.4).

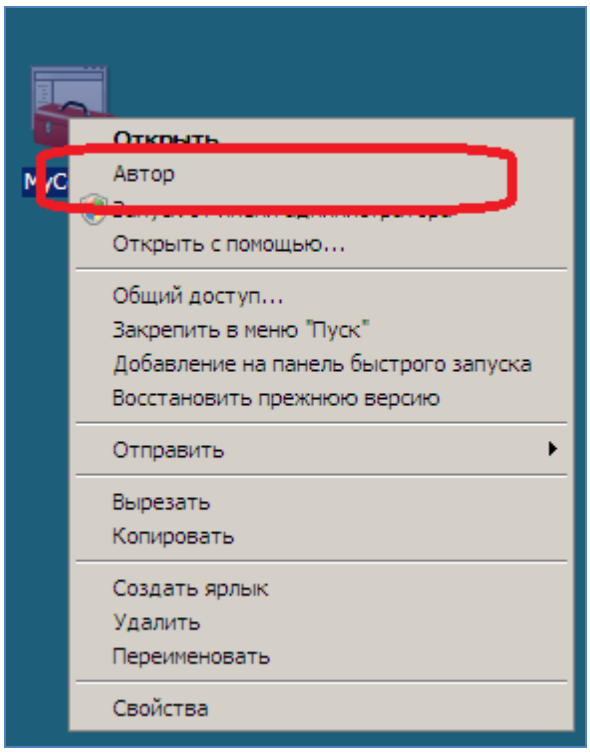


Рисунок 4.4 –Выбор команды «Автор»

28 Щелкните меню Консоль (File). В авторском режиме отображается команда «Добавить или удалить оснастку (Add/Remove Snap-in)». Закройте консоль.

5 Лабораторная работа №5. Создание объектов Active Directory

Цель работы: получить навыки по добавлению в Active Directory информации о ресурсах организации

5.1 Постановка задачи

Добавить информацию о ресурсах организации в Active Directory:

- новые подразделения организации;
- новых пользователей организации;
- компьютеры организации;
- группы безопасности.

5.2 Порядок выполнения работы

1 Войдите на машину SERVER01 как администратор. Откройте оснастку Active Directory — пользователи и компьютеры (Active Directory Users And Computers). Разверните узел домена.

2 Щелкните правой кнопкой мыши узел домена, выберите опцию «Создать (New)» и примените команду Подразделение (Organizational Unit).

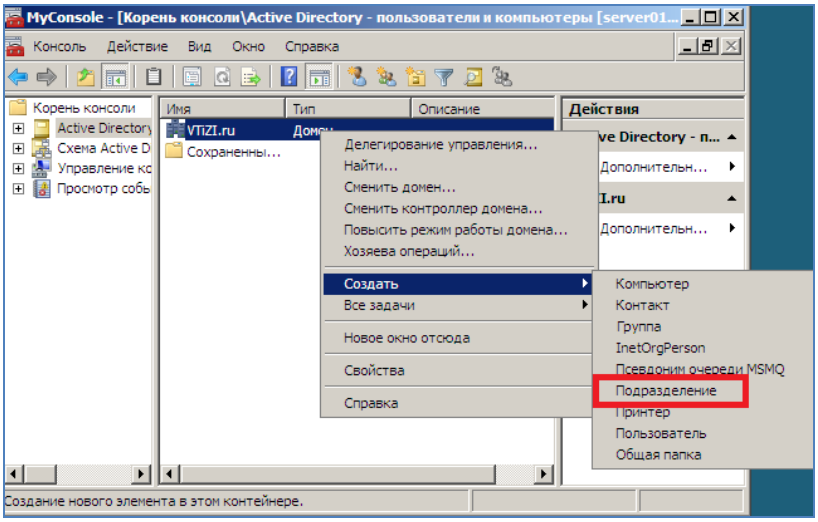


Рисунок 5.1 – Выбор команды создания нового подразделения

3 Введите для подразделения имя «Кадры».

4 Установите флажок Защитить контейнер от случайного удаления (Protect Container From Accidental Deletion). Щелкните ОК.

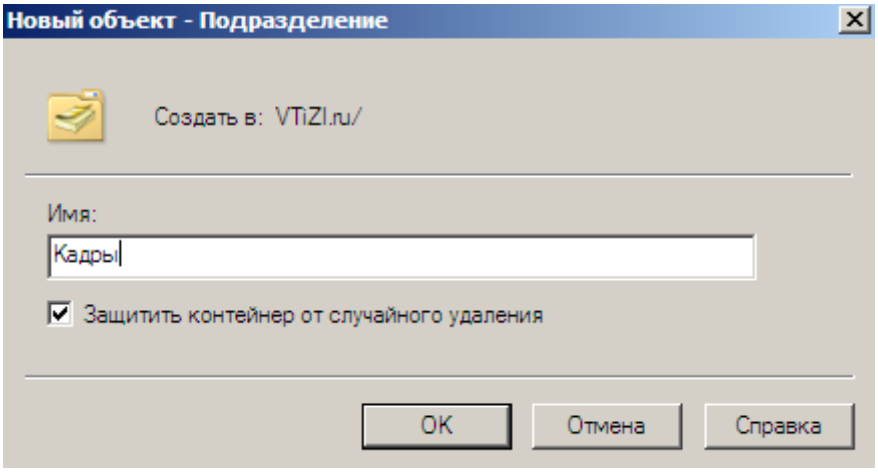


Рисунок 5.2 – Ввод имени нового подразделения

5 Щелкните подразделение правой кнопкой мыши и примените команду Свойства (Properties). В поле Описание (Description) введите «Неадминистративные пользовательские объекты идентификации». Щелкните ОК.

6 Повторите шаги 2 - 5 , чтобы создать подразделения, представленные в таблице 5.1

Таблица 5.1 – Подразделения организации

Имя	Описание
Клиенты	Клиентские компьютеры
Группы	Неадминистративные группы
Администраторы	Административные объекты идентификации и группы
Серверы	Серверы

7 Создайте в подразделении «Кадры» указанных ниже пользователей. Для каждого пользователя предусмотрите сложный безопасный пароль. Запомните

назначенные пароли, поскольку вы будете входить в систему с помощью этих учетных записей на последующих работах.

8 В дереве консоли разверните узел домена contoso.com и выберите подразделение «Кадры». Щелкните правой кнопкой мыши подразделение «Кадры», выберите опцию «Создать (New)» и примените команду «Пользователь (User)». Откроется диалоговое окно «Новый объект — пользователь (New Object -User)».

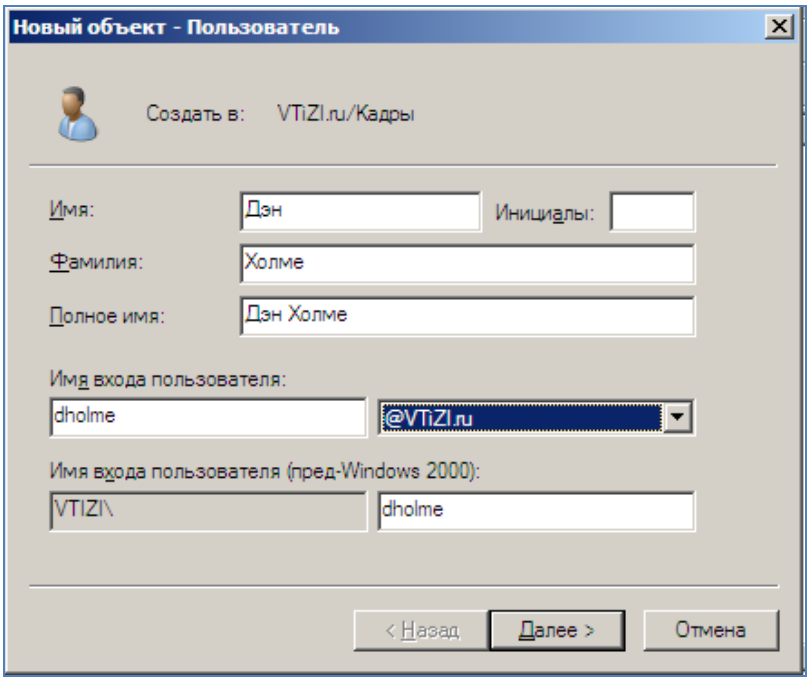


Рисунок 5.3 – Диалоговое окно добавления нового пользователя

9 В поле «Имя (First Name)» введите для пользователя имя Дэн. В поле «Фамилия (Last Name)» введите фамилию Холме. В поле «Имя входа пользователя (User Logon Name)» введите имя dholme. Щелкните кнопку Далее (Next).

10 Введите начальный пароль пользователя в поля «Пароль (Password)» и «Подтверждение (Confirm Password)». Запомните пароль, назначенный пользователю, поскольку эта учетная запись понадобится вам на практических занятиях далее.

11 Установите флажок «Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon)». Щелкните кнопку «Далее (Next)». Просмотрите введенные параметры и щелкните кнопку «Готово (Finish)».

12 Повторите шаги 8-11 и создайте следующих пользователей в подразделении «Кадры» , данные которых представлены в таблице 5.2

Таблица 5.2 – Пользователи подразделения «Кадры»

№	Имя	Фамилия	Имя входа пользователя
1	Джеймс	Файн	jfine
2	Барбара	Майер	bmayer
3	Барбара	Морленд	bmorelend

13 Еще раз повторите шаги 8 - 11 и создайте в подразделении «Кадры» учетную запись для себя. Создайте сложный безопасный пароль и запомните его, поскольку эта учетная запись будет использоваться в других работах.

14 Снова повторите шаги 8 - 11 и создайте для себя административную учетную запись в подразделении «Администраторы». Этой учетной записи будут предоставлены административные привилегии. В качестве имени входа пользователя для административной учетной записи возьмите имя и фамилию с суффиксом _admin, например dholme_admin.

15 В дереве консоли разверните узел домена и выберите подразделение «Серверы». Щелкните правой кнопкой мыши и выберите опцию «Создать (New)» и примените команду «Компьютер (Computer)». Откроется диалоговое окно «Новый объект – «Компьютер (New Object - Computer)» .

16 В поле «Имя компьютера (Computer Name)» введите для компьютера имя «FILESERVER01». Данные автоматически будут введены в поле «Имя компьютера (пред-Windows 2000) (Computer Name (Pre-Windows 2000))». Не устанавливайте флажок «Назначить учетной записи статус пред-Windows 2000 (Assign This Computer Account As A Pre-Windows 2000 Computer)».Щелкните «ОК» .

17 Щелкните правой кнопкой мыши компьютер и примените команду «Свойства (Properties)». Щелкните «ОК» .

18 Повторите шаги 15-17 и создайте два объекта компьютеров:

- SHAREPOINT02;

- EXCHANGE03.

19 Повторите шаги 15 - 17 и создайте еще три объекта компьютеров в подразделении «Клиенты»:

- DESKTOP101;

- DESKTOP102;

- LAPTOP103.

20 В дереве консоли разверните узел домена и выберите подразделение «Группы». Щелкните правой кнопкой мыши и выберите опцию «Создать (New)» и примените команду «Группа (Group)». Откроется диалоговое окно «Новый объект — Группа (New Object — Group)».

21 В текстовое поле «Имя группы (Group Name)» введите для группы имя «Финансы». Выберите для группы тип «Группа безопасности (Security)». Выберите область действия «Глобальная (Global)». Щелкните «ОК».

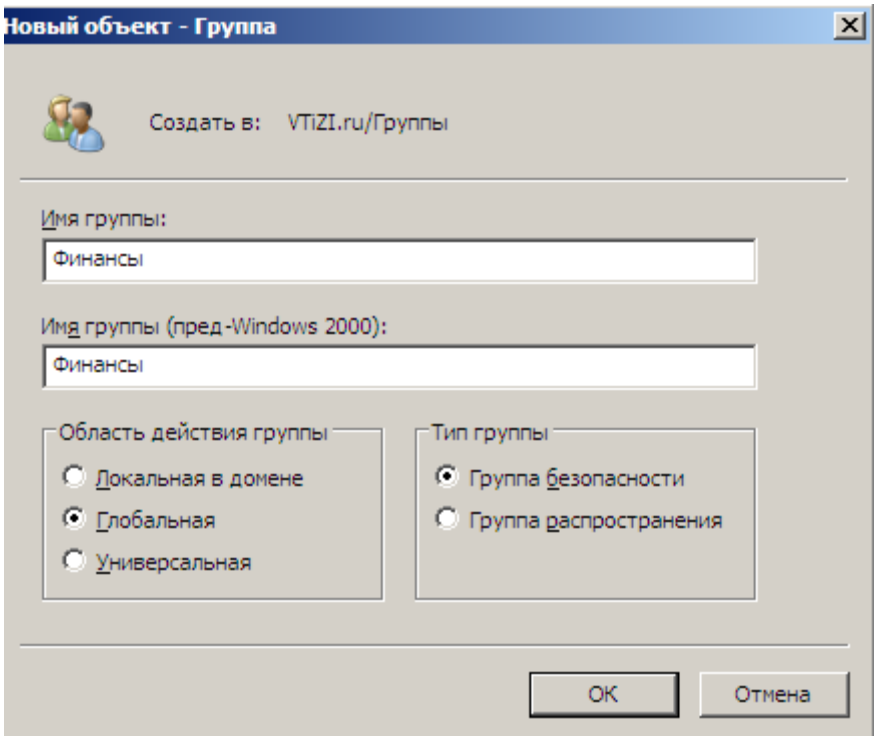


Рисунок 5.4 – Диалоговое окно добавления новой группы

22 Повторите шаги 20 - 21 для создания следующих глобальных групп безопасности в подразделении «Группы»:

- «Финансовые менеджеры»;

- «Продажи»;

- «APP_Office 2007».

23 Повторите шаги 20 - 21 и создайте две глобальные группы безопасности в подразделении «Администраторы»:

- «Справка»;

- «Администраторы Windows» .

24 Откройте свойства своей административной учетной записи в подразделении «Администраторы». Перейдите на вкладку «Член групп (Member Of)» и щелкните кнопку «Добавить (Add)». В диалоговое окно «Выбор»: "Группы" (Select Groups) введите имя «Администраторы домена (Domain Admins)». Щелкните «ОК» .

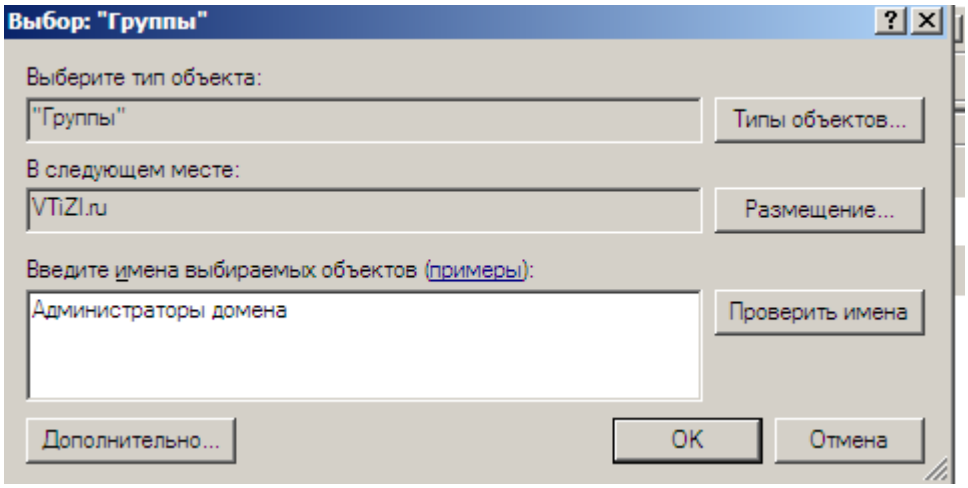


Рисунок 5.5 – Выбор группы

25 Вновь щелкните «ОК», чтобы закрыть окно свойств учетной записи.

26 Откройте свойства группы «Справка» в подразделении «Администраторы». Перейдите на вкладку «Члены группы (Members)» и щелкните кнопку «Добавить (Add)» .

27 В диалоговое окно Выбор (Select) введите имя «Барб». Щелкните кнопку «Проверить имена (Check Names)». Откроется диалоговое окно «Найдено несколько имен (Multiple Names Found)». Выберите имя Барбара Майер и щелкните «ОК». Щелкните «ОК», чтобы закрыть диалоговое окно «Выбор (Select)». Вновь щелкните «ОК», чтобы закрыть окно свойств группы.

28 Откройте свойства группы «APP_Office 2007» в подразделении «Группы». Перейдите на вкладку «Члены группы (Members)» и щелкните кнопку «Добавить (Add)» .

29 В окне «Выбор (Select)» щелкните кнопку «Типы объектов (Object Types)». Выберите тип объектов «Компьютеры (Computers)». В диалоговое окно «Выбор (Select)» введите имя «DESKTOP101» и щелкните «ОК» .

30 Щелкните кнопку «Проверить имена (Check Names)» и выберите компьютер «DESKTOP101» .

6 Лабораторная работа №6. Делегирование и безопасность объектов Active Directory

Цель работы: получить навыки по делегированию управления Delegation of Control Wizard в Active Directory

6.1 Постановка задачи

В данной работе необходимо, разрешить пользователям группы «Справка» сбрасывать пароли пользователей и снимать блокировку учетных записей в подразделении «Кадры».

6.2 Порядок выполнения работы

1 Войдите на машину SERVER01 как администратор и откройте оснастку Active Directory — пользователи и компьютеры (Active Directory Users and Computers) .

2 Разверните узел домена contoso.com, щелкните правой кнопкой мыши подразделение «Кадры» и примените команду «Делегирование управления (Delegate Control)», запуская «Мастер делегирования управления (Delegation of Control Wizard)». Щелкните кнопку «Далее (Next)» .

3 На странице Пользователи или группы (Users or Groups) щелкните кнопку «Добавить (Add)». В диалоговом окне Выбор (Select) введите имя «Справка» и щелкните ОК. Щелкните кнопку Далее (Next) .

4 На странице «Делегируемые задачи (Tasks to Delegate)» выберите задачу «Переустановить пароли пользователей и установить изменение пароля при следующей перезагрузке (Reset User Passwords and Force Password Change at Next Logon)». Щелкните кнопку «Далее» .

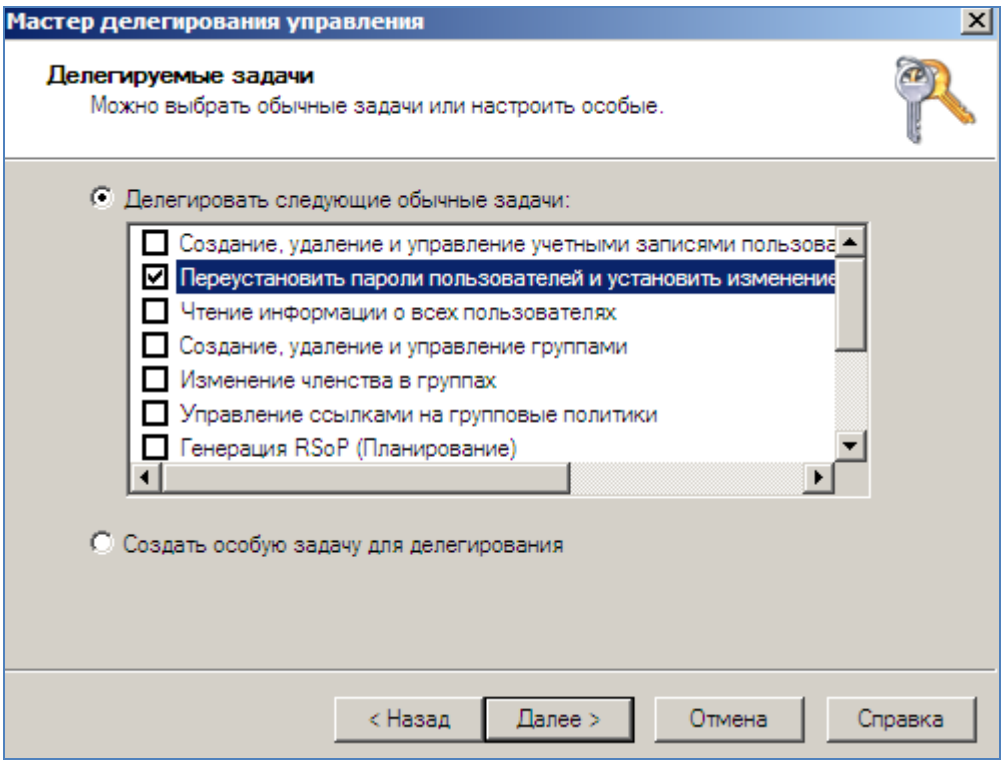


Рисунок 6.1 – Выбор задачи

5 Просмотрите выбранные действия и щелкните кнопку «Готово».

6 Сделайте группу «Пользователи домена» членом группы «Операторы печати», которая находится в контейнере «Builtin», с тем чтобы все пользователи в учебном домене могли входить на контроллер домена SERVER01.

7 Войдите на машину SERVER01 как пользователь Барбара Майер (она входит в группу «Справка»). Убедитесь, что Барбара может сбрасывать пароли других пользователей и собственный пароль в подразделении «Кадры».

8 Затем попытайтесь изменить пароль учетной записи в подразделении «Администраторы». Проанализируйте результат.

9 Войдите на машину SERVER01 как «Администратор». В подразделении «Кадры» создайте новое подразделение «Филиал». При создании подразделения «Филиал» проверьте, установлен ли флажок «Защитить контейнер от случайного удаления».

10 Создайте в этом подразделении учетную запись пользователя. Откройте список DACL объекта пользователя в диалоговом окне «Дополнительные параметры» безопасности. Просмотрите разрешения, назначенные подразделению

«Справка»: они явные или унаследованные? Если эти разрешения унаследованы, то откуда?

11 В диалоговом окне «Дополнительные параметры безопасности» откройте список DACL подразделения «Филиал». Сбросьте флажок «Добавить разрешения, наследуемые от родительских объектов». В окне предупреждения «Безопасность Windows» выберите пункт «Удалить».

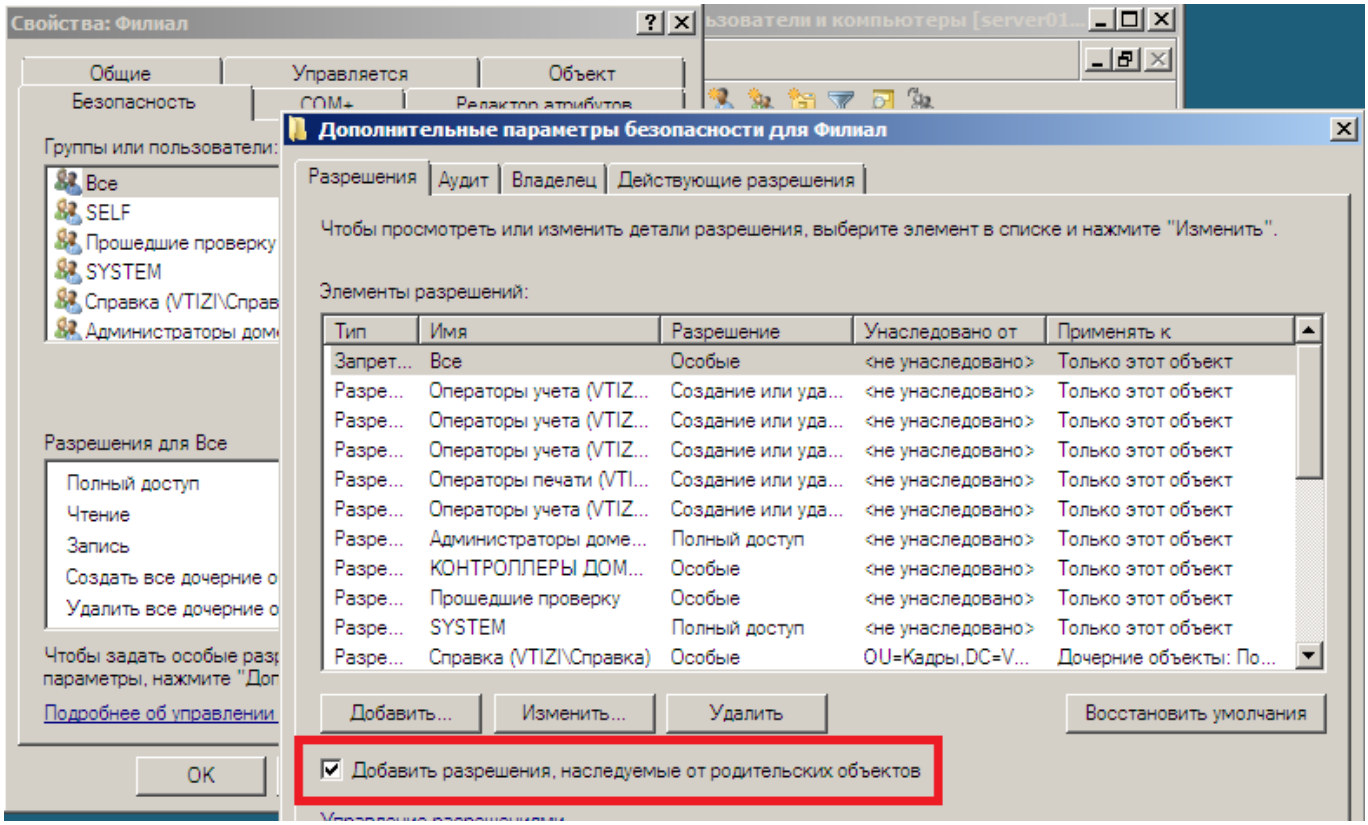


Рисунок 6.2 – Сброс наследуемых разрешений

12 Выйдите из системы и вновь войдите как пользователь Барбара Майер. Убедитесь, что Барбара может сбросить пароль пользователя в подразделении «Кадры». После этого попытайтесь сбросить этот пароль в подразделении «Филиал». В доступе будет отказано.

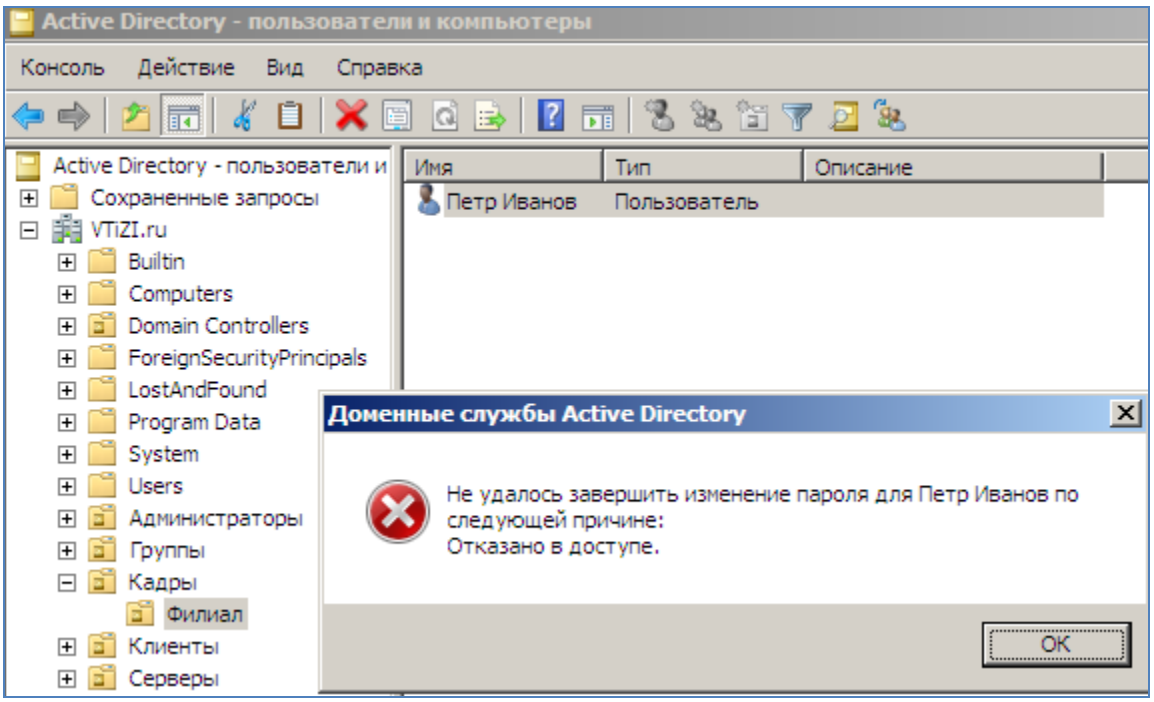


Рисунок 6.3 – Результат выполнения операции «Смена пароля»

13 Выйдите из системы и вновь войдите как администратор. Устраните ошибку доступа Барбары, восстановив наследование для подразделения «Филиал». Выйдите из системы и вновь войдите как пользователь Барбара, чтобы проверить результат. Может ли она сбросить пароль пользователя в подразделении «Филиал»?

14 Войдите на машину SERVER01 как пользователь Барбара Майер. Попытайтесь удалить подразделение «Филиал». В доступе будет отказано. Выйдите из системы и вновь войдите как администратор. Попытайтесь удалить подразделение «Филиал». В доступе будет отказано. Откройте свойства подразделения «Филиал». Перейдите на вкладку «Объект». Если эта вкладка не отображается, включите представление «Дополнительные компоненты» в оснастке «Active Directory — пользователи и компьютеры». На вкладке «Объект снимите защиту подразделения» «Филиал». И, наконец, удалите подразделение «Филиал» вместе с содержащейся в нем учетной записью пользователя.

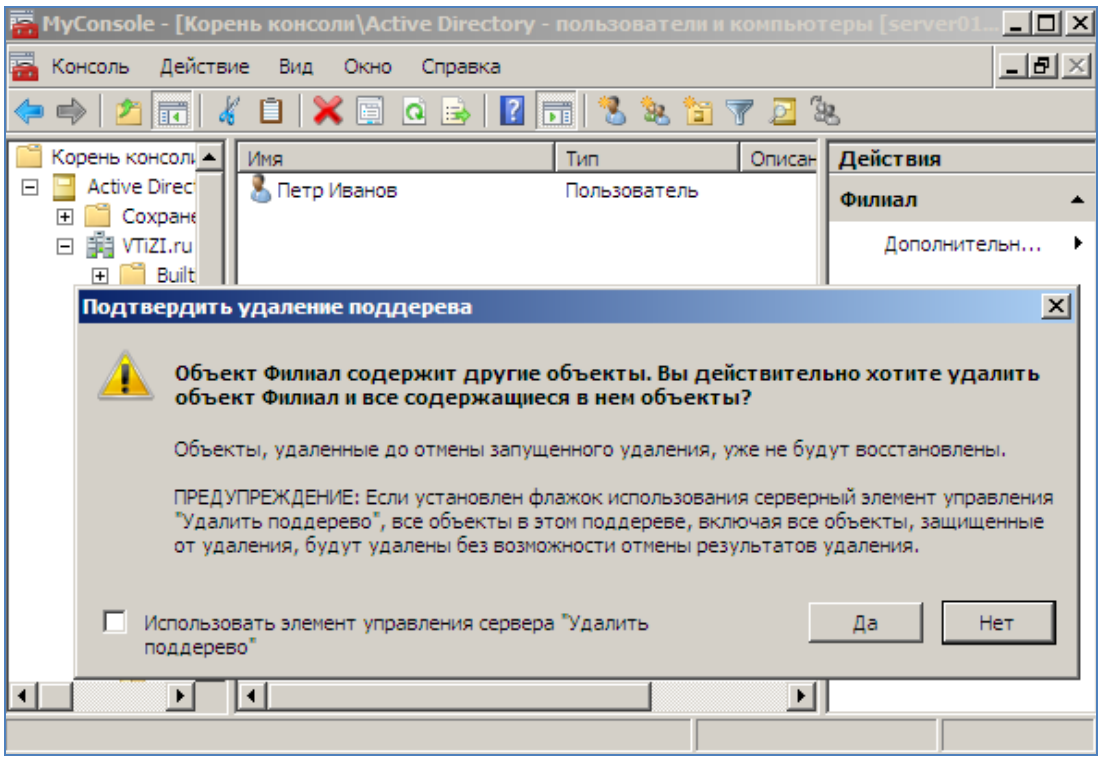


Рисунок 6.4 – Окно предупреждения удаления филиала

7 Лабораторная работа №7. Автоматизация создания учетных записей пользователей

Цель работы: получить навыки по автоматизации и созданию учетных записей пользователей в Active Directory

7.1 Постановка задачи

В данной работе необходимо

- создать шаблон учетной записи пользователя, настроить атрибуты и обеспечивать их безопасность в Active Directory;
- создать при помощи шаблона нескольких пользователей.

7.2 Порядок выполнения работы

1 Войдите на машину SERVER01 как администратор. Откройте оснастку «Active Directory — пользователи и компьютеры» и разверните узел домена.

2 Щелкните правой кнопкой мыши подразделение «Кадры», выберите опцию «Создать» и примените команду «Пользователь». В поле «Имя» введите имя «Продажи» с символом подчеркивания.

3 В поле «Фамилия» введите имя «Шаблон». В поле «Имя входа пользователя» введите имя «_шаблон_продаж» с символами подчеркивания. Щелкните кнопку «Далее».

4 В поля «Пароль» и «Подтверждение» введите сложный пароль.

5 Установите флажок «Отключить учетную запись». Щелкните кнопку «Далее», а затем кнопку «Готово».

6 Дважды щелкните шаблонную учетную запись, чтобы открыть ее диалоговое окно «Свойства». Перейдите на вкладку «Организация». В поле «Отдел» введите имя «Продажи». В поле «Организация» введите имя «Contoso, Ltd».

7 Перейдите на вкладку «Член групп». Щелкните кнопку «Добавить». 15. Введите имя «Продажи» и щелкните ОК.

8 Перейдите на вкладку «Профиль». В поле «Путь к профилю» введите «\\server01\profiles\%username%». Щелкните ОК. Вы создали шаблонную учетную запись, которую можно копировать с целью генерирования учетных записей для новых менеджеров по продажам.

9 Щелкните правой кнопкой мыши учетную запись Продажи Шаблон и примените команду «Копировать». Откроется диалоговое окно «Копировать объект — Пользователь». В поле «Имя» введите «Джефф». В поле «Фамилия» введите «Форд». В поле «Имя входа пользователя» введите «jford». Щелкните кнопку «Далее».

10 В поля «Пароль» и «Подтверждение» введите сложный пароль. Сбросьте флажок «Отключить учетную запись». Щелкните кнопку «Далее», а затем кнопку «Готово».

11 Откройте свойства учетной записи пользователя Джефф Форд и убедитесь, что отконфигурированные в шаблоне атрибуты скопированы в новую учетную запись.

8 Лабораторная работа №8. Создание групп и управление ими

Цель работы: получить навыки по созданию и управлению группами в Active Directory

8.1 Постановка задачи

В данной работе необходимо создать групп с различными областями действия и типами.

8.2 Порядок выполнения работы

1 Войдите на машину SERVER01 как администратор и откройте оснастку Active Directory — пользователи и компьютеры . В дереве консоли выберите подразделение Группы .

2 Щелкните правой кнопкой мыши подразделение Группы, выберите опцию. Создать (New) и примените команду Группа (Group) .

3 В поле Имя группы (Group Name) введите имя Продажи.

4 Выберите для группы область действия Глобальная (Global) и тип Безопасность (Security) . Щелкните ОК.

5 Щелкните правой кнопкой мыши группу Продажи и примените команду Свойства (Properties) .

6 Перейдите на вкладку Члены группы (Members). Щелкните кнопку Добавить (Add). Введите имена Джефф;Тони и щелкните ОК. Щелкните ОК, чтобы закрыть диалоговое окно Свойства (Properties) .

7 Повторите шаги 2 - 4 , чтобы создать две глобальные группы безопасности — Маркетинг и Консультанты.

8 Повторите шаги 2 - 4 , чтобы создать локальную группу безопасности домена ACL_Sales Folder_Read .

9 Откройте свойства группы ACL_Sales_Folder_Read. Перейдите на вкладку Члены групп (Member Of). Щелкните кнопку Добавить (Add). Введите имена Продажи; Маркетинг; Консультанты и щелкните ОК. Щелкните кнопку Добавить (Add). Введите имя Линда и щелкните ОК. Щелкните О К, чтобы закрыть диалоговое окно Свойства (Properties).

10 Откройте диалоговое окно Свойства (Properties) группы Маркетинг. Перейдите на вкладку Член групп (Member Of) и щелкните кнопку Добавить (Add). Введите имя ACL_Sales Folder_Read и щелкните ОК. Вы не можете добавить локальную группу домена в глобальную группу. Отмените операции и закройте все диалоговые окна.

11 На диске С: создайте папку с именем Продажи. Щелкните правой кнопкой мыши папку Продажи, примените команду. Свойства (Properties) и перейдите на вкладку Безопасность (Security). Щелкните кнопку Изменить (Edit), а затем щелкните кнопку Добавить (Add). Щелкните кнопку Дополнительно (Advanced), а затем кнопку Поиск (Find Now). С помощью префикса имен групп, например префикса ACL_ для групп управления доступом к ресурсам, можно быстро найти и сгруппировать эти группы в начале списка. Отмените операции во всех открытых диалоговых окнах. Щелкните правой кнопкой мыши подразделение Группы, выберите опцию Создать (New) и примените команду Группа (Group). В поле Имя группы (Group Name) введите имя Служащие. Выберите для группы область действия Локальная в домене (Domain Local) и тип Безопасность (Security). Щелкните ОК.

9 Лабораторная работа №9. Реализация групповой политики

Цель работы: получить навыки реализации групповой политики в Active Directory

9.1 Постановка задачи

В данной работе выполнить следующие задачи:

- создать объект групповой политики, который реализует параметр обязательной политики безопасности домена с областью действия для всех пользователей и компьютеров в домене;

- проверить результат применения параметра групповой политики, а также получить навыки в обновлении политики вручную с помощью инструмента Gpupdate.exe;

- просмотреть результат применения GPO и сам объект GPO;

- провести анализ административного шаблона;

- создать центральное хранилище административных шаблонов, для централизации управления шаблонами.

9.2 Порядок выполнения работы

1 Войдите на машину SERVER01 как администратор. В группе «Администрирование» откройте консоль «Управление групповой политикой».

2 Разверните лес и домен contoso.com и откройте контейнер «Объекты групповой политики». В дереве консоли щелкните правой кнопкой мыши контейнер «Объекты групповой политики» и выполните команду «Создать» (рисунок 9.1) .

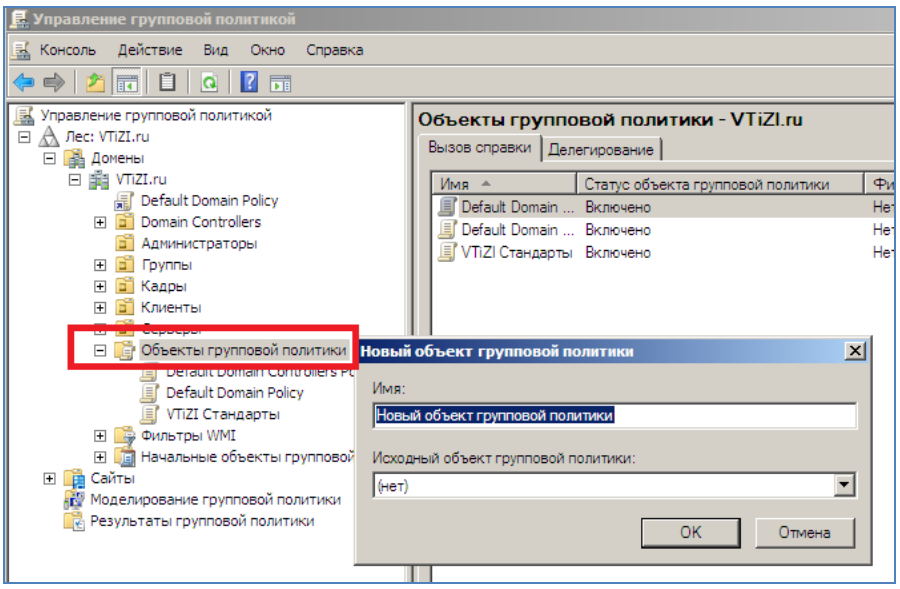


Рисунок 9.1 – Окно выбора имени нового объекта групповой политики

3 В поле «Имя» введите имя «CONTOSO Стандарты». Щелкните «ОК».

4 Щелкните правой кнопкой мыши объект «CONTOSO Стандарты» и выполните команду «Изменить». Откроется «Редактор управления групповыми политиками» (Group Policy Management Editor) .

5 В консоли щелкните правой кнопкой мыши корневой узел «CONTOSO Стандарты» и выполните команду «Свойства». Перейдите на вкладку «Комментарий» и введите комментарий «Стандарты корпоративных политик Contoso. Параметры влияют на всех пользователей и компьютеры в домене. Ответственное лицо за объект GPO: ваше имя». Щелкните ОК (рисунок 9.2).

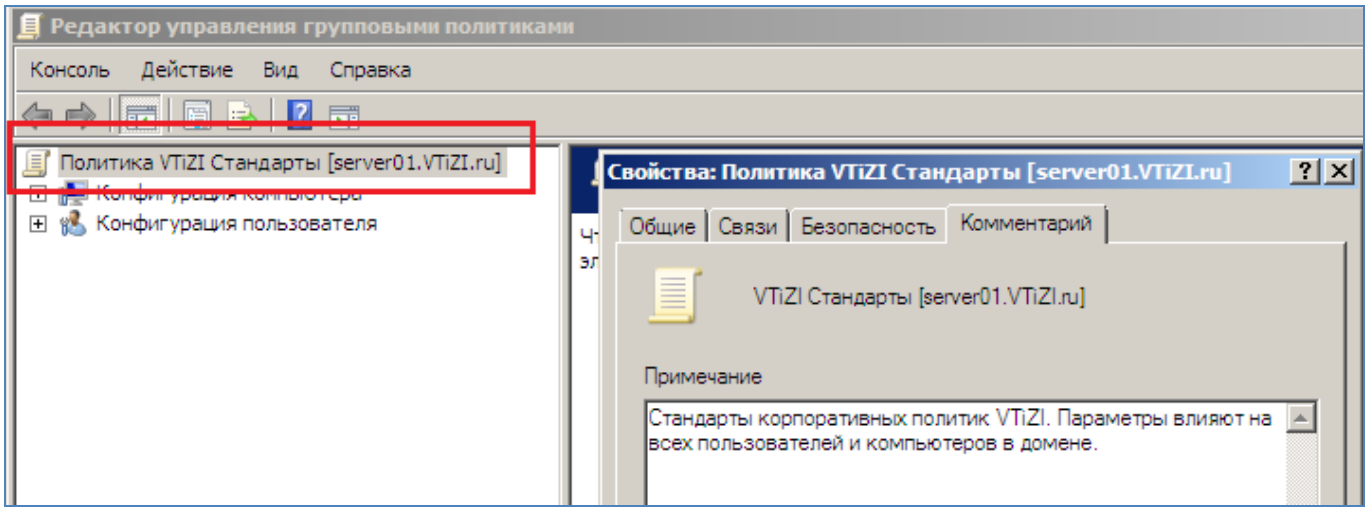


Рисунок 9.2 – Добавления комментария в объект групповой политики

6 В этом сценарии корпоративная политика безопасности Contoso указывает, что компьютеры нельзя оставлять без присмотра и входить на них после 10 мин. простоя. Для того чтобы выполнить это требование, конфигурируется время ожидания экранной заставки и параметры политики пароля защиты экранной заставки. Для локализации этих параметров политики применяются новые поисковые возможности Windows Server 2008.

7 Разверните узел «Конфигурация пользователя \ Политики \ Административные шаблоны». Просмотрите параметры в этом узле. Прочитайте описание интересующих вас параметров политики. Не вносите изменения в конфигурацию (рисунок 9.3).

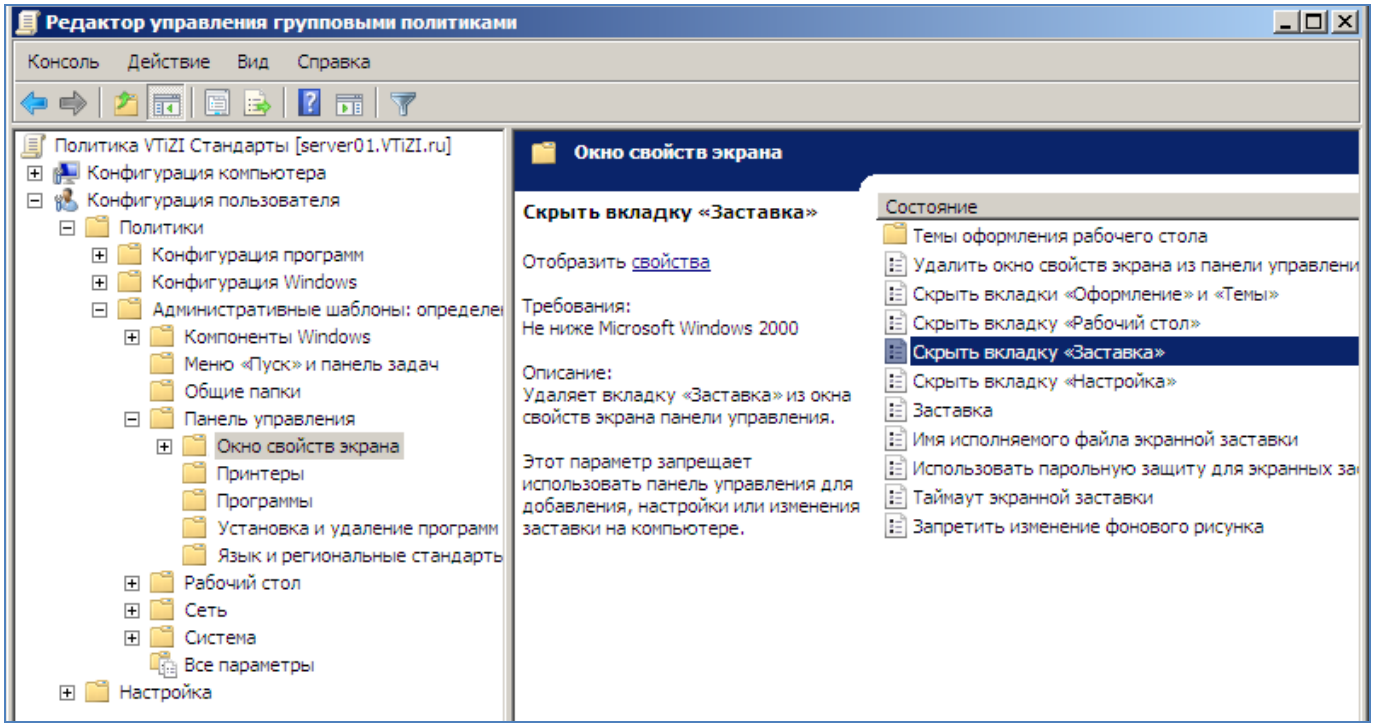


Рисунок 9.3 – Просмотр политик

8 В узле «Конфигурация пользователя» щелкните правой кнопкой мыши узел «Административные шаблоны» и выполните команду «Параметры фильтра».

9 Установите флажок «Включить фильтры по ключевым словам». В текстовом поле «Фильтры по словам» введите слова «экранная заставка». В раскрывающемся списке возле текстового поля выберите опцию «Точное» (рисунок 9.4). Щелкните ОК.

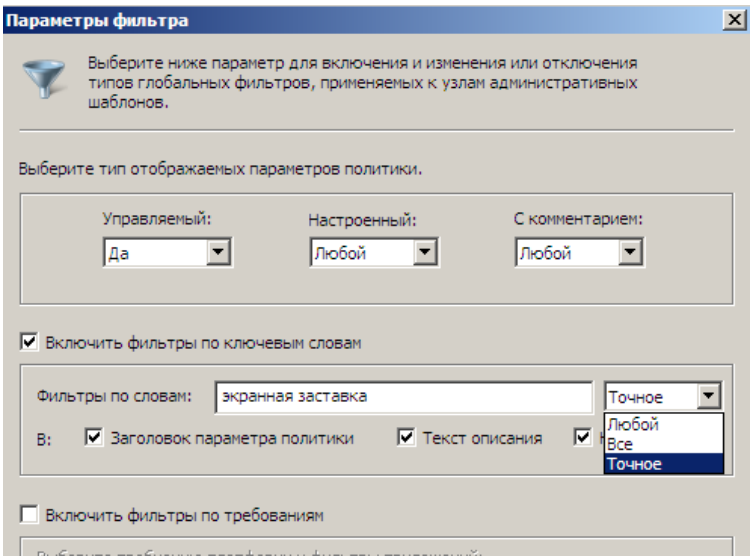


Рисунок 9.4 – Настройка параметров фильтра

10 Параметры политики административных шаблонов будут отфильтрованы для отображения параметров со словами экранная заставка. Просмотрите найденные политики экранной заставки.

11 В узле «Панель управления \ Окно свойств экрана» щелкните параметр политики «Таймаут экранной заставки». В левой части панели сведений консоли отобразится описание параметра. Дважды щелкните параметр политики «Таймаут экранной заставки».

12 Перейдите на вкладку «Параметр» и выберите опцию «Включен» В поле «Секунды» введите значение 600 (рисунок 9.5).

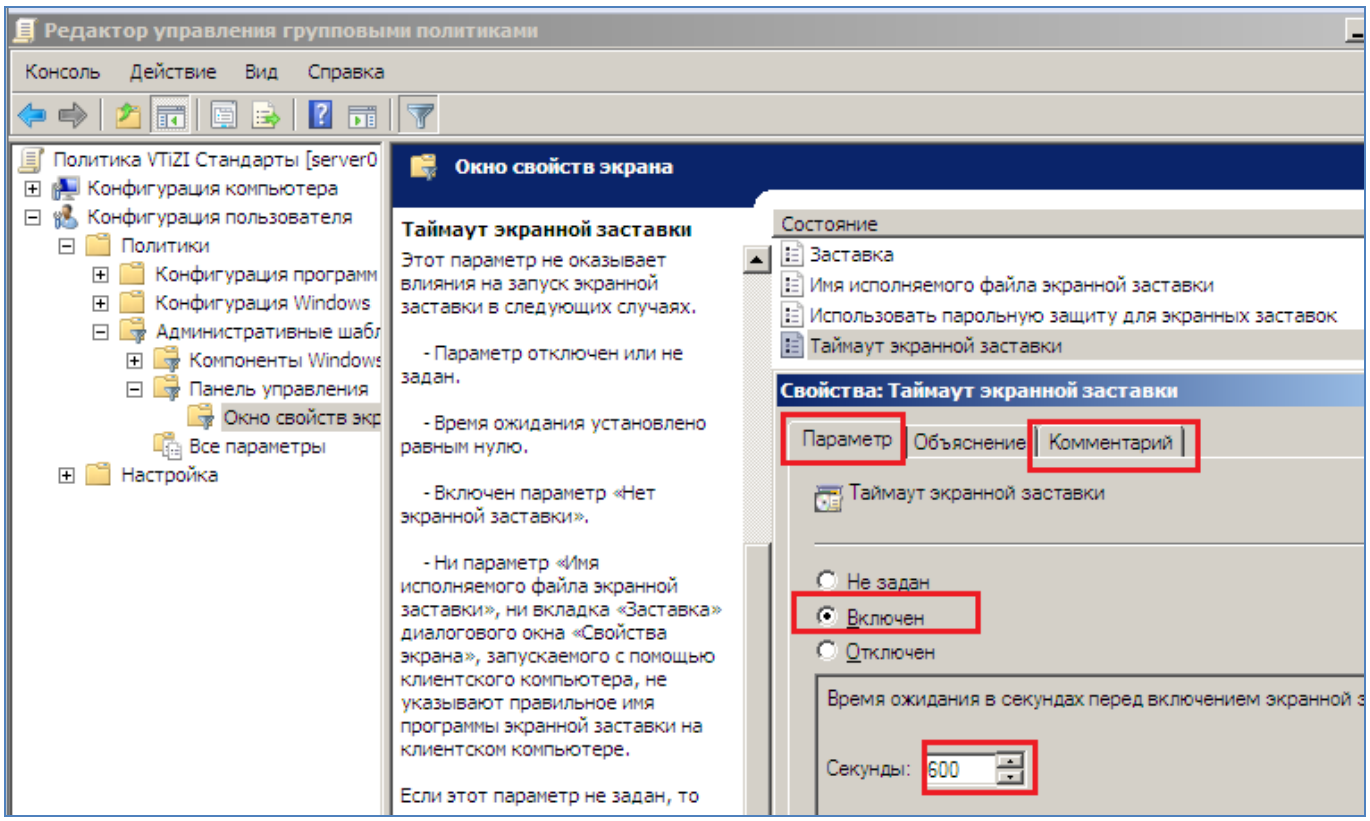


Рисунок 9.5 – Настройка параметра «Таймаут экранной заставки»

13 На вкладке «Комментарий» введите «Корпоративная политика безопасности реализована с помощью этой политики в комбинации с парольной защитой экранной заставки». Щелкните ОК.

14 Дважды щелкните параметр политики «Использовать парольную защиту для экранных заставок». Выберите опцию «Включить». На вкладке «Комментарий» введите «Корпоративная политика безопасности реализована с помощью этой политики в комбинации с политикой таймаута экранной заставки» (рисунок 9.6). Щелкните ОК.

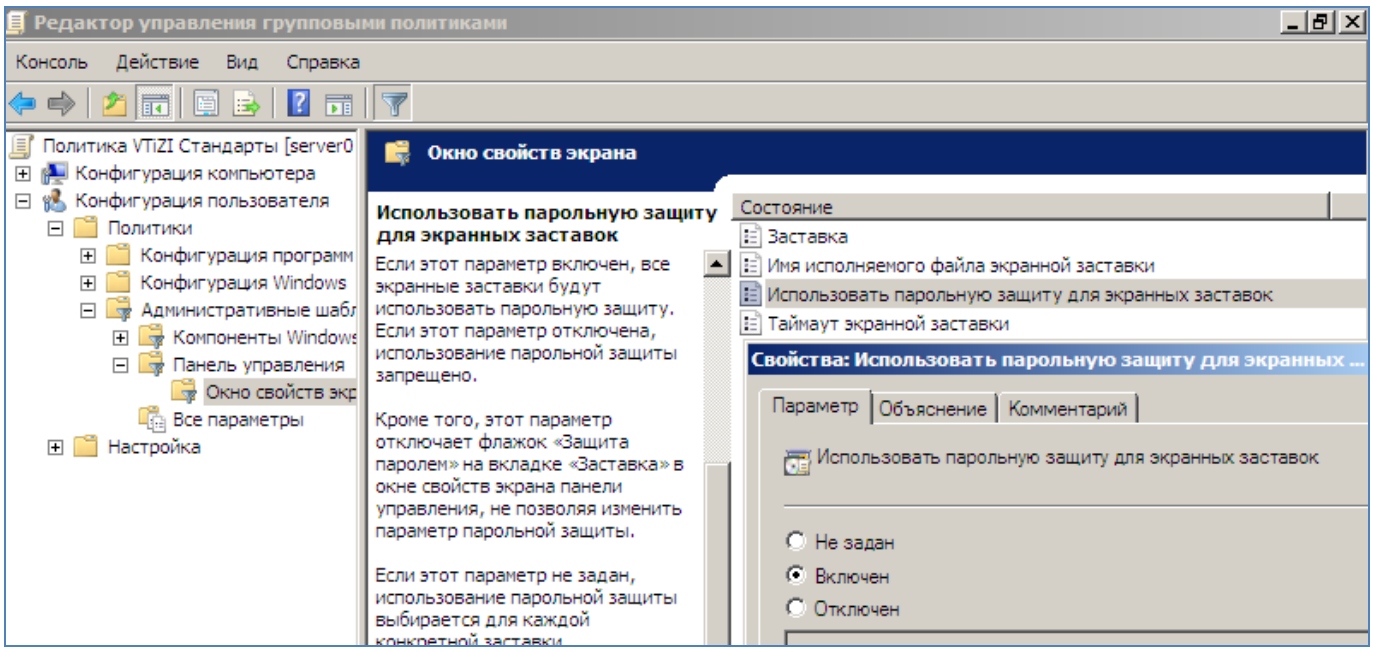


Рисунок 9.6 – Настройка параметра «Использовать парольную защиту для экранных заставок»

15 Закройте редактор GPME. Изменения, внесенные в GPME, сохраняются в реальном времени. Такая команда, как «Сохранить», отсутствует.

16 В консоли «Управление групповой политикой» щелкните правой кнопкой мыши домен contoso.com и выполните команду «Связать существующий объект GPO».

17 Выберите объект групповой политики «CONTOSO Стандарты» и щелкните ОК.

18 На машине SERVER01 щелкните правой кнопкой мыши рабочий стол и выполните команду «Персонализация». Щелкните ссылку «Экранная заставка».

19 Вы можете изменить время ожидания экранной заставки и ее отображение, начиная с экрана входа в систему. Закройте диалоговое окно «Параметры экранной заставки».

20 Откройте окно командной строки и введите команду gpupdate.exe /force / boot/logoff. Эти опции команды Gpudate.exe указывают на полное обновление групповой политики. Подождите, пока закончится обновление политик компьютера и пользователя.

21 Вновь откройте диалоговое окно «Параметры экранной заставки». Теперь вы не сможете изменить время ожидания и отображение экранной заставки (рисунок 9.7).

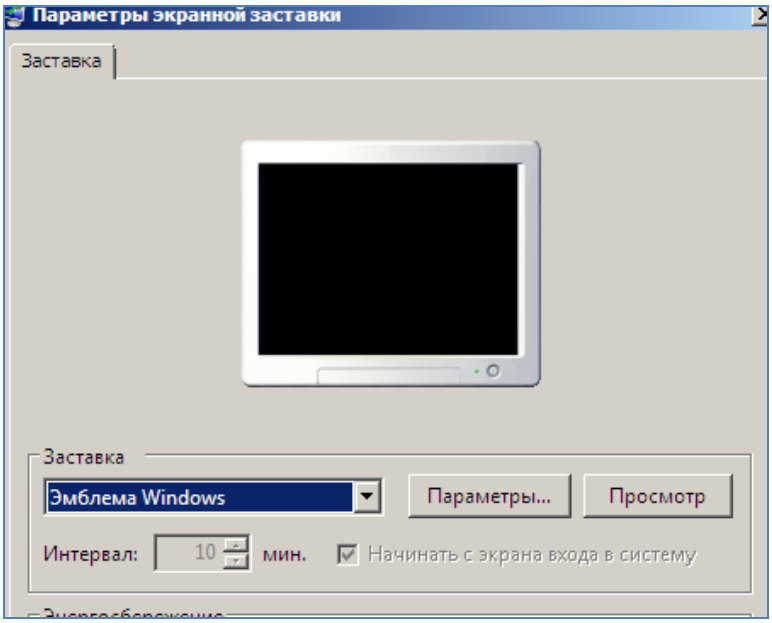


Рисунок 9.7 – Параметры экранной заставки

22 В контейнере «Объекты групповой политики» консоли «Управление групповой политикой» выберите объект «CONTOSO Стандарты» .

23 В секции «Связи» вкладки «Область» показаны связи GPO. Перейдите на вкладку «Параметры», чтобы просмотреть отчет о параметрах в объекте GPO. Если включена конфигурация повышенной безопасности Internet Explorer, подтвердите добавление содержимого веб-узла «about:security_mmc.exe» в зону надежных узлов (Trusted Sites) .

24 Щелкните ссылку «Показать все» в верхней части отчета, чтобы развернуть все секции отчета. Как видите, в отчет добавлены комментарии к параметрам политики (рисунок 9.8).

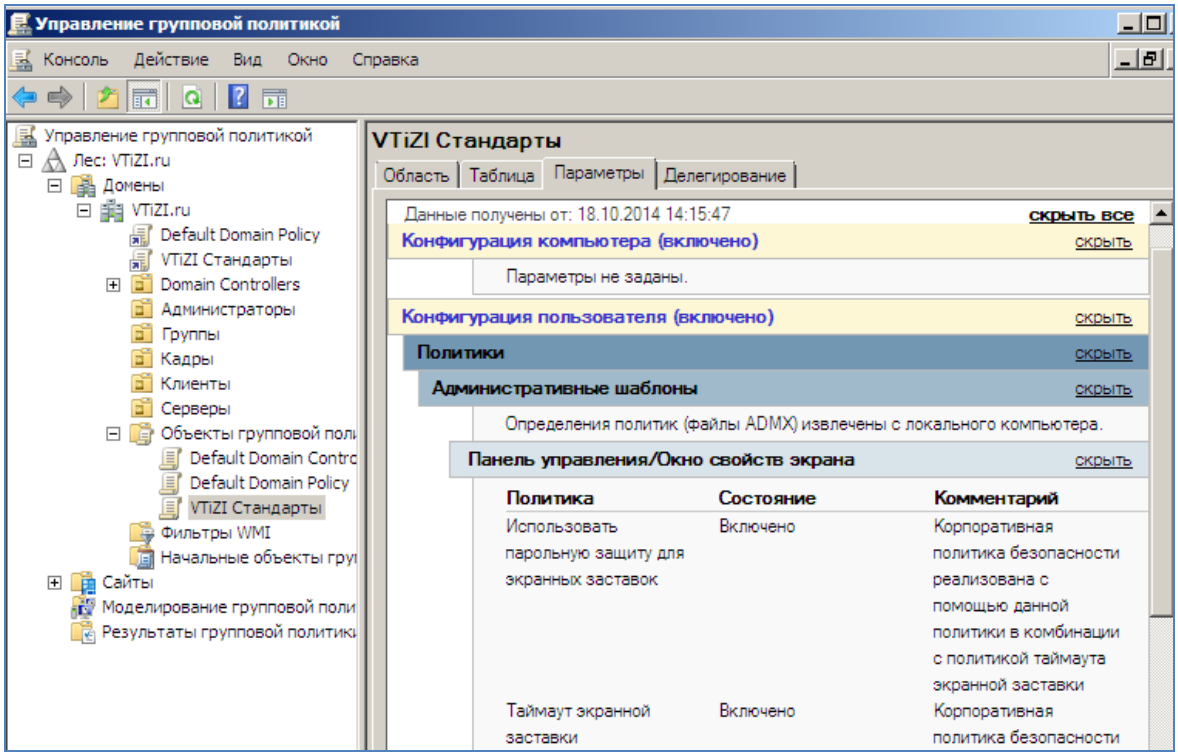


Рисунок 9.8 – Окно отчета объекта групповой политики

25 Наведите указатель мыши на имя политики «Таймаут экранной заставки». Как видите, оно представляет собой гиперссылку. Щелкните ее, чтобы просмотреть объяснение данного параметра политики.

26 Перейдите на вкладку «Таблица», где отображаются ваши комментарии к объекту GPO вместе с информацией о номерах версии GPO (рисунок 9.9).

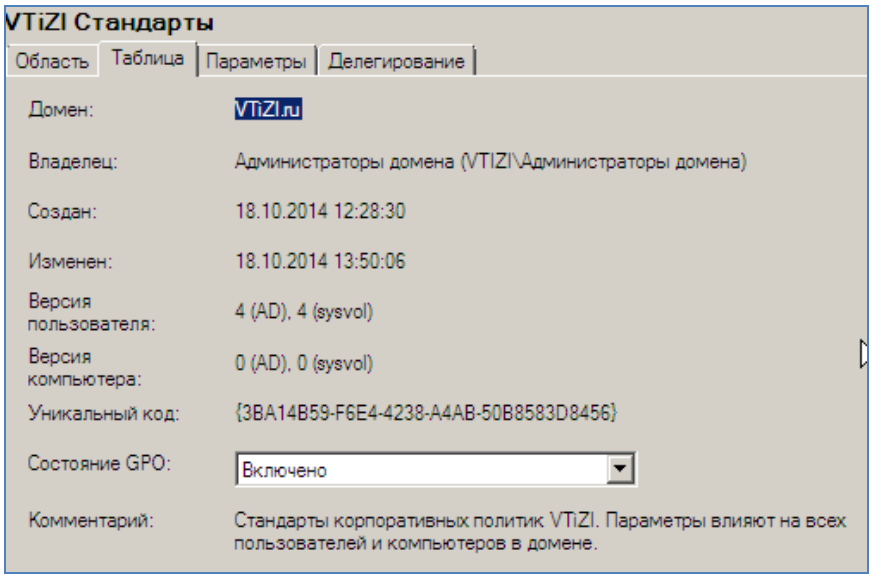


Рисунок 9.9 – Окно с данными о версии объекта групповой политики

27 Запишите уникальный код, отображаемый на вкладке «Таблица».

28 Откройте папку \\contoso.com\SYSVOL\contoso.com\Policies. Дважды щелкните папку с именем, которое соответствует уникальному коду объекта GPO. Эта папка представляет шаблон GPT объекта GPO (рисунок 9.10).

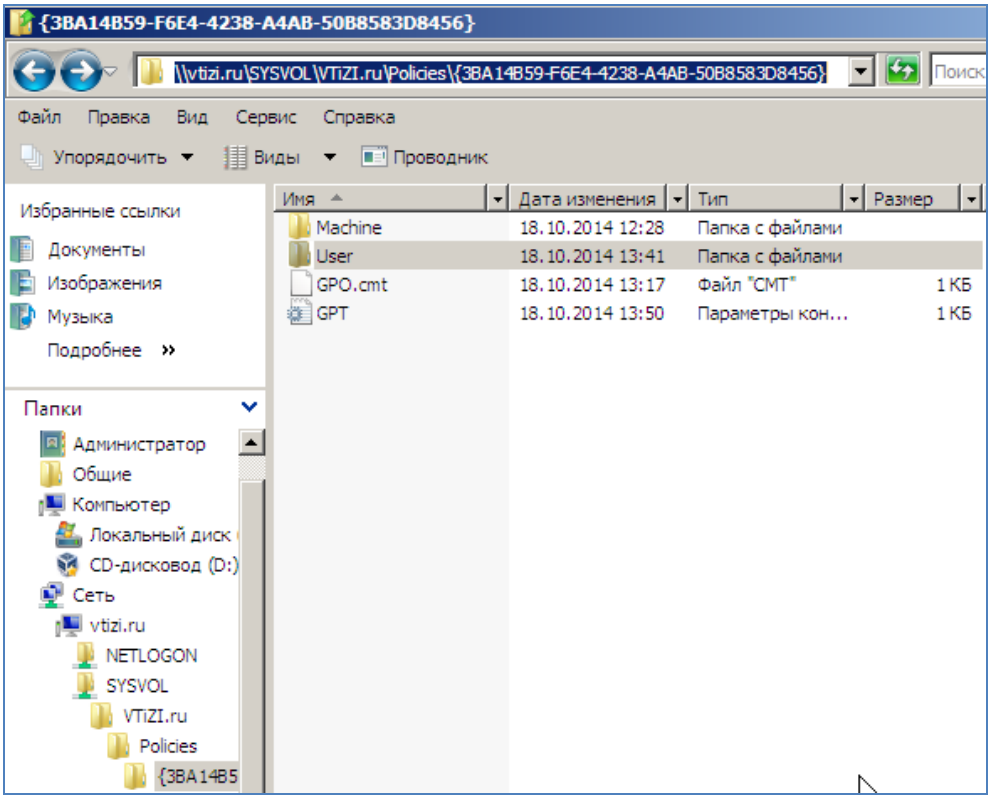


Рисунок 9.10 – Скриншот окна шаблон GPT объекта GPO

29 Откройте папку %SystemRoot%\PolicyDefinitions. Откройте в ней папку ru-RU для русского региона и языка. Дважды щелкните файл ControlPanelDisplay.adml.

30 Щелкните опцию «Выбор программы из списка установленных программ», а затем ОК. Откройте файл с помощью программы «Блокнот» и щелкните ОК. В меню «Формат» выберите параметр «Перенос по словам».

31 Выполните поиск текста «ScreenSaverIsSecure». Просмотрите метку параметров и текст объяснения в следующей строке (рисунок 9.11).

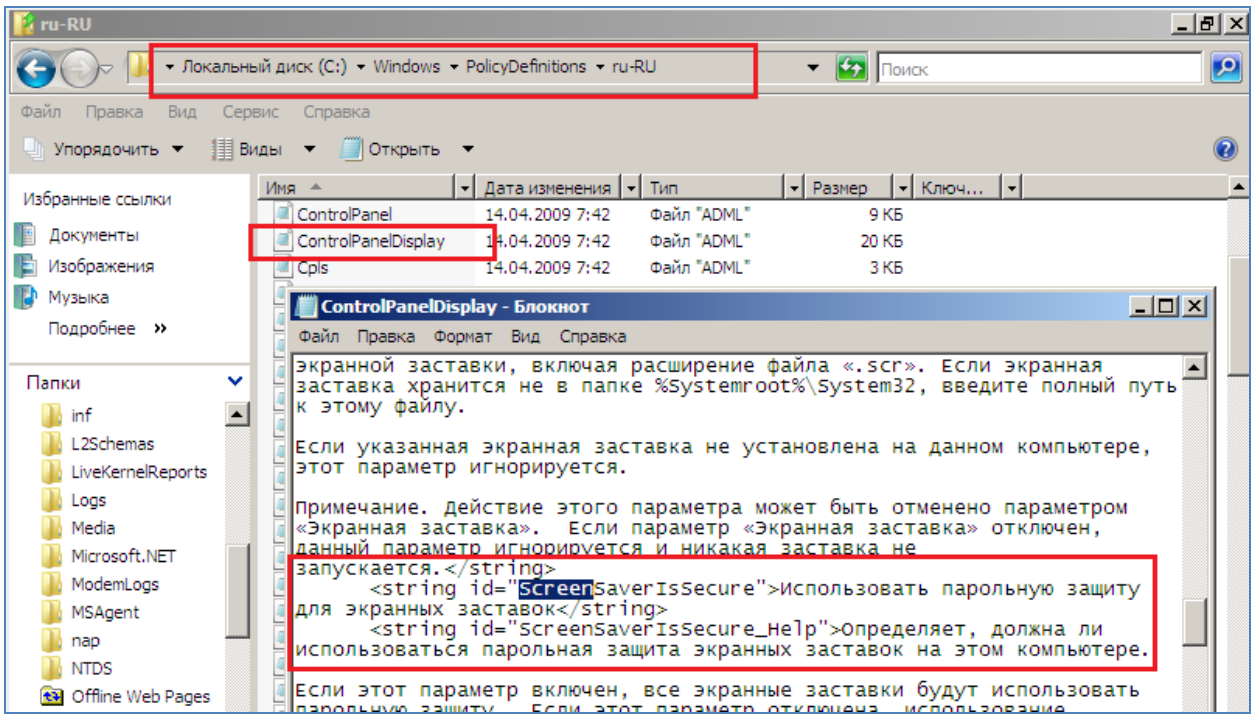


Рисунок 9.11 – Просмотр шаблона групповой политики

32 Закройте файл и перейдите к папке PolicyDefinitions.

33 Дважды щелкните файл ControlPanelDisplay.admx. Щелкните опцию «Выбор программы из списка установленных программ» и ОК. Откройте файл с помощью программы «Блокнот» и щелкните ОК.

34 Найдите в файле приведенный ниже текст:

<policy name="ScreenSaverIsSecure" class="User"

dlsplayName="$(string. ScreenSaverIsSecure)"

explainText="$(string.ScreenSaverIsSecu re_Help)"

key="Software\Policies\Microsoft\Windows\Control Panel\Desktop"

' valueName="ScreenSaverIsSecure">

<parentCategory ref="Display" />

<supportedOn ref="windows:SUPP0RTED_Win2kSP1" />

<enabledValue>

<string>1</string>

</enabledValue>

<disabledValue>

<string>0</string>

</disabledValue>

</policy> 1

35 Идентифицируйте следующие элементы в шаблоне (рисунок 9.12):

– имя параметра политики, которое отображается в редакторе GPME;

– текст объяснения параметра политики;

– ключ реестра и значение, измененное параметром политики;

– данные, помещаемые в реестр в случае включения политики;

– данные, помещаемые в реестр в случае отключения политики.

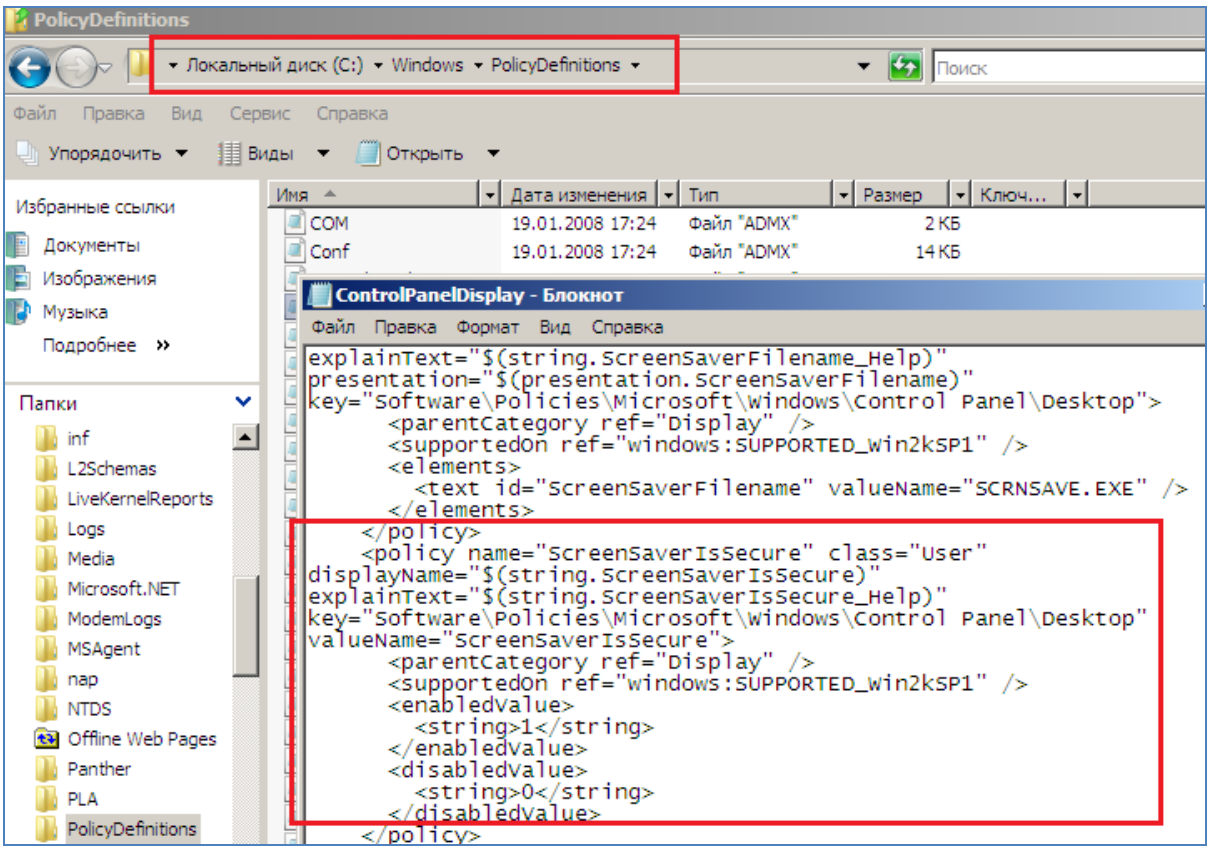


Рисунок 9.12 – Просмотр шаблона групповой политики

36 В консоли «Управление групповой политикой» щелкните правой кнопкой мыши объект групповой политики «CONTOSO Стандарты» и выполните команду «Изменить».

37 Разверните узел «Конфигурация пользователя \ Политики \Административные шаблоны». Отметьте: в имени узла указано, что Определения

политик (ADMX-файлы) получены с локального компьютера. Закройте «Редактор GPME» (рисунок 9.13).

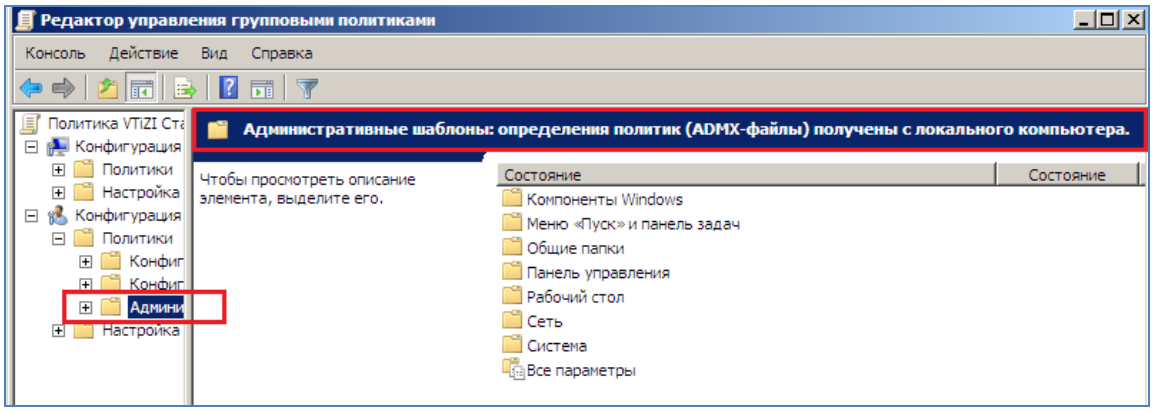


Рисунок 9.13 – Окно редактора групповой политики

38 Откройте папку \\contoso.com\SYSVOL\contoso.com\Policies. Создайте папку с именем PolicyDefinitions. Скопируйте в созданную папку содержимое папки %SystemRoot%\ PolicyDefinitions.

39 В консоли «Управление групповой политикой» щелкните правой кнопкой мыши объект «CONTOSO Стандарты» и выполните команду «Изменить». Разверните узел «Конфигурация пользователя \Политики \Административные шаблоны».

40 Отметьте: в имени узла указано, что Определения политик (ADMX-файлы) получены с центрального хранилища (рисунок 9.14).

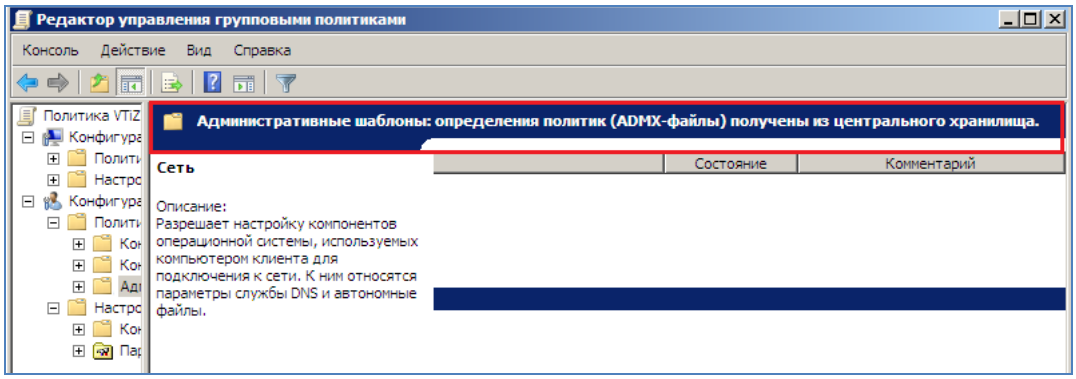


Рисунок 9.14 – Окно редактора групповой политики

10 Лабораторная работа №10. Настройка области действия групповой политики

Цель работы: получить навыки по настройке области действия групповой политики в Active Directory

10.1 Постановка задачи

1 Вы являетесь администратором домена contoso.com. Объект групповой политики «CONTOSO Стандарты», связанный с доменом, конфигурирует параметр политики, которому требуется десятиминутный таймаут экранной заставки. Некое критически важное приложение, выполняющее длинный процесс вычислений, вылетает при запуске экранной заставки, поэтому инженер попросил отключить экранную заставку для тех, кто ежедневно использует это приложение.

2 Необходимо максимально ускорить процесс получения изменений групповой политики всеми системами, и вы принимаете решение отконфигурировать параметр «Всегда ждать сеть при запуске и входе в систему». Администраторы не должны изменять эту политику; политика должна принудительно применяться ко всем системам.

3 Вы обнаруживаете, что небольшое число пользователей нужно освободить от политики таймаута экранной заставки, конфигурируемой объектом «CONTOSO Стандарты». Замена параметров непрактична, и вы используете фильтры безопасности для управления областью действия GPO.

4 Обработка замыкания политики. Недавно один из менеджеров по продажам Contoso, Ltd показал презентацию важному клиенту на своем компьютере, на рабочем столе которого была непристойная картинка. Руководство Contoso, Ltd попросило вас сделать так, чтобы рабочие столы ноутбуков менеджеров по продажам не содержали фоновых рисунков. Это необязательно делать для рабочих столов менеджеров, когда они входят на настольные компьютеры в офисе. Поскольку параметры политики, управляющие фоновым рисунком рабочего стола, относятся к

конфигурации пользователя, а вам нужно применить параметры к ноутбукам менеджеров по продажам, требуется использовать обработку политики замыкания. Кроме того, объекты ноутбуков менеджеров по продажам распределены по нескольким подразделениям, и вы используете фильтры безопасности, которые объект GPO применит к группе, а не к подразделению ноутбуков менеджеров по продажам.

10.2 Порядок выполнения работы

1 Войдите на машину SERVER01 как администратор и откройте оснастку «Active Directory — пользователи и компьютеры» и создайте в подразделении первого уровня «Кадры» подразделение «Инженеры».

2 Откройте консоль «Управление групповой политикой». Щелкните правой кнопкой мыши подразделение «Инженеры» и выполните команду «Создать объект GPO этом домене и связать его» (рисунок 10.1).

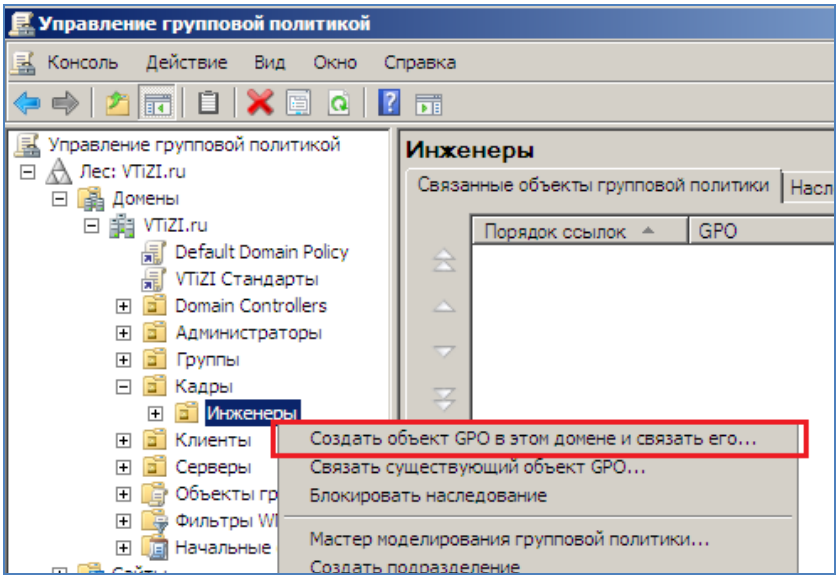


Рисунок 10.1 – Оснастка управление групповой политикой

3 Введите имя «Параметры политики инженеров» и щелкните ОК.

4 Разверните подразделение «Инженеры», щелкните правой кнопкой мыши объект GPO и выполните команду «Изменить» (рисунок 10.2).

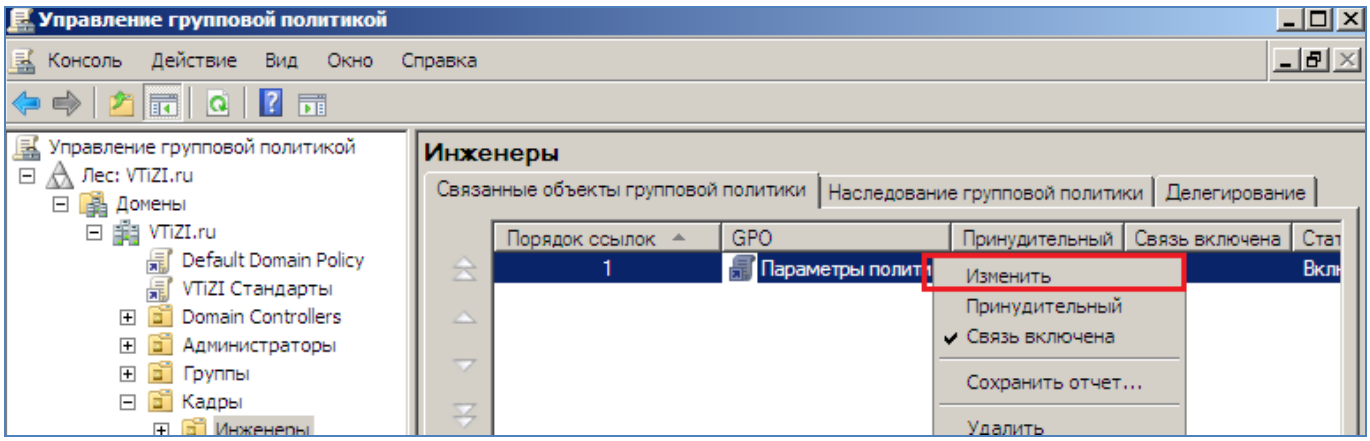


Рисунок 10.2 – Оснастка управление групповой политикой

5 Разверните папку «Конфигурация пользователя \ Политики \Административные шаблоны \ Панель управления \ Окно свойств экрана». Дважды щелкните параметр политики «Таймаут экранной заставки». Щелкните опцию «Отключен», а затем ОК. Закройте редактор GPME.

6 В консоли управления групповой политикой GPMC выберите подразделение «Инженеры» и перейдите на вкладку «Наследование групповой политики». Объект GPO «Параметры политики инженеров» должен превалировать над объектом групповой политики «CONTOSO Стандарты». Отконфигурированный параметр, явно отключающий экранную заставку, заменит параметр в объекте групповой политики «CONTOSO Стандарты» (рисунок 10.3).

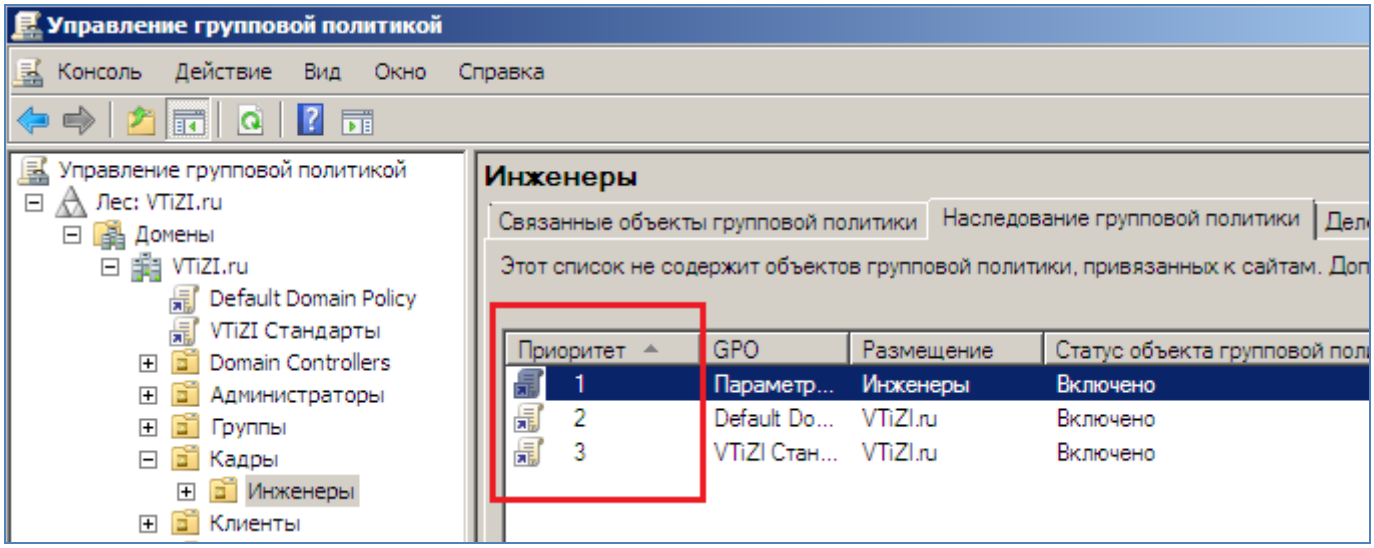


Рисунок 10.3 – Оснастка управление групповой политикой

7 В консоли управления групповой политикой GPMC щелкните правой кнопкой мыши домен contoso.com и выполните команду «Создать объект GPO в этом домене и связать его». Введите имя «Принудительные политики домена» и щелкните ОК.

8 Щелкните правой кнопкой мыши объект GPO и выполните команду «Изменить».

9 Разверните папку «Конфигурация компьютера \ Политики \Административные шаблоны \ Система \ Вход в систему». Дважды щелкните параметр политики «Всегда ждать сеть при запуске и входе в систему». Выберите опцию «Включен» и щелкните ОК (рисунок 10.4).

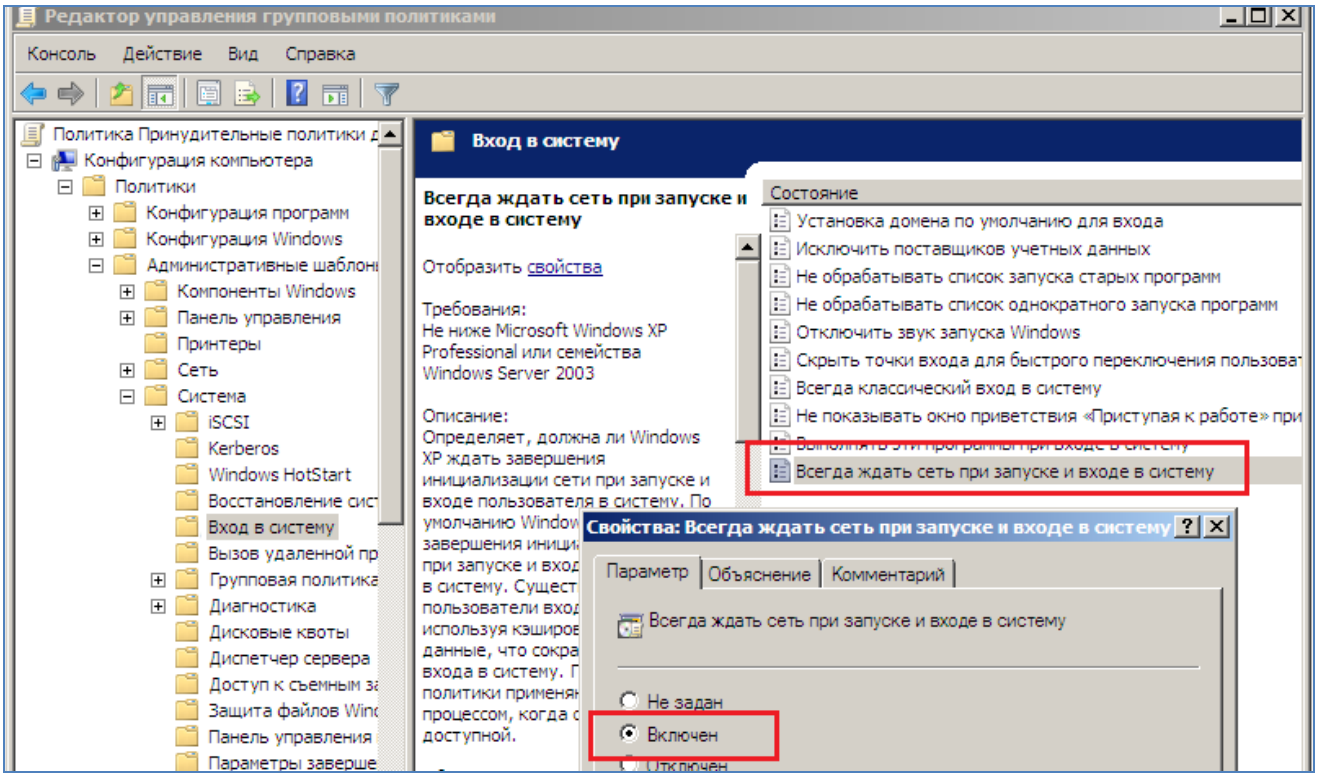


Рисунок 10.4 – Изменение политики «Всегда ждать сеть при запуске и входе в систему»

10 Закройте редактор GPME. Щелкните правой кнопкой мыши объект GPO «Принудительные политики домена» и установите флажок «Принудительный» (рисунок 10.5).

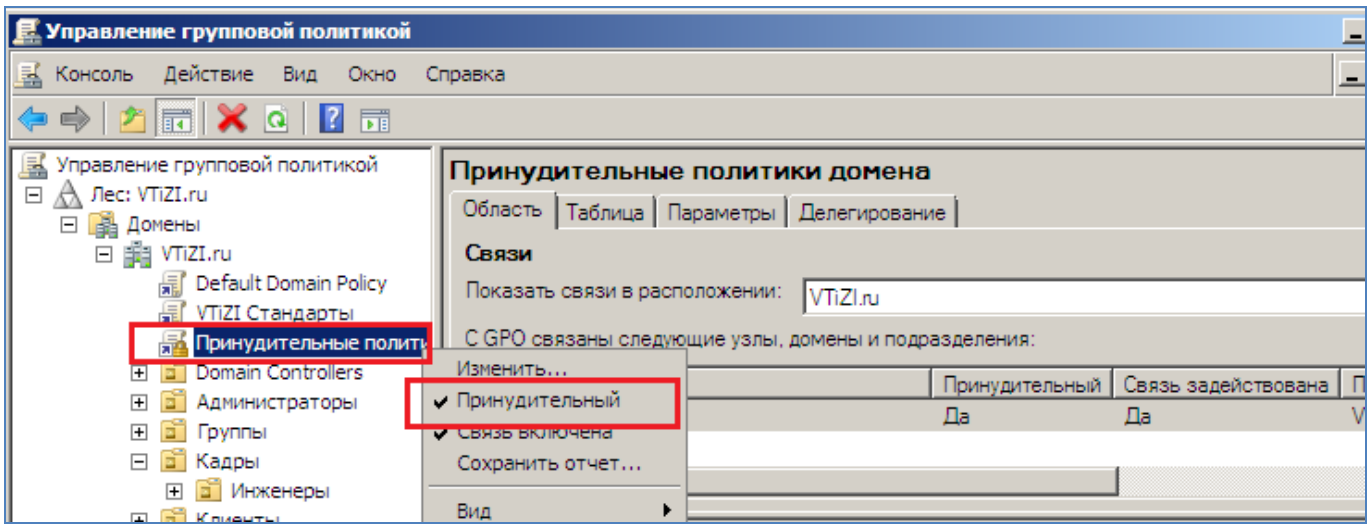


Рисунок 10.5 – Изменение приоритета политики

11 Выберите подразделение «Инженеры» и перейдите на вкладку «Наследование групповой политики». Принудительно связанный объект GPO будет превалировать даже над объектами GPO, непосредственно связанными с подразделением «Инженеры» (рисунок 10.6) .

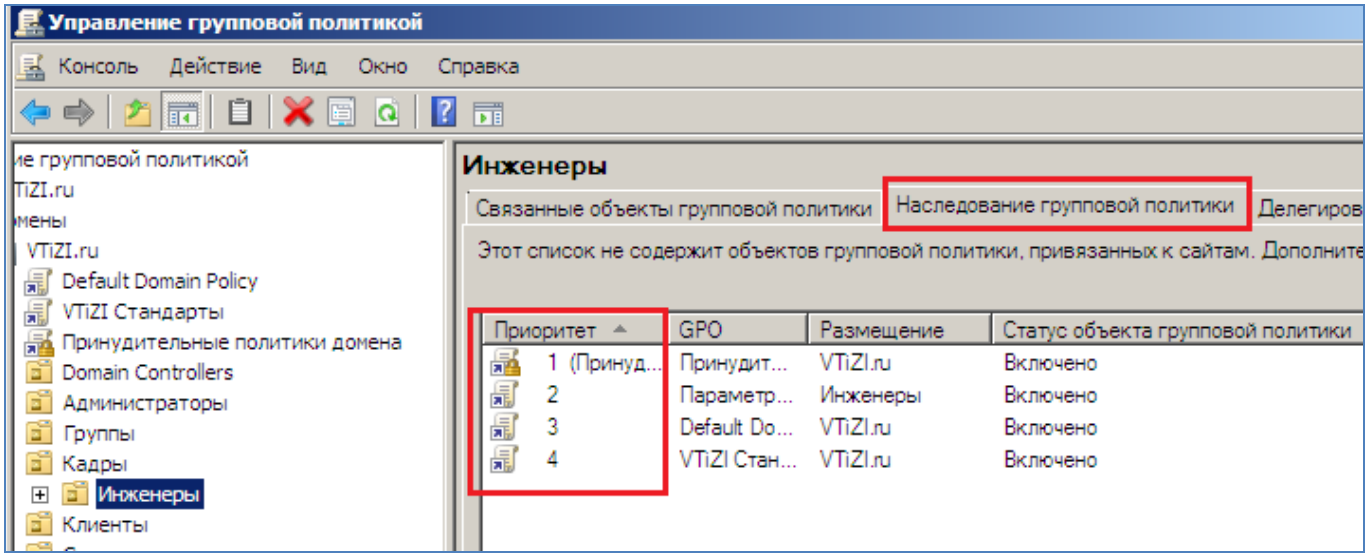


Рисунок 10.6 – Просмотр приоритета групповых политик для подразделения «Инженеры»

12 Откройте оснастку «Active Directory — пользователи и компьютеры», создайте подразделение «Группы», а в этом подразделении — глобальную группу безопасности с именем «Исключения GPO_CONTOSO_Стандарты» (рисунок 10.7) .

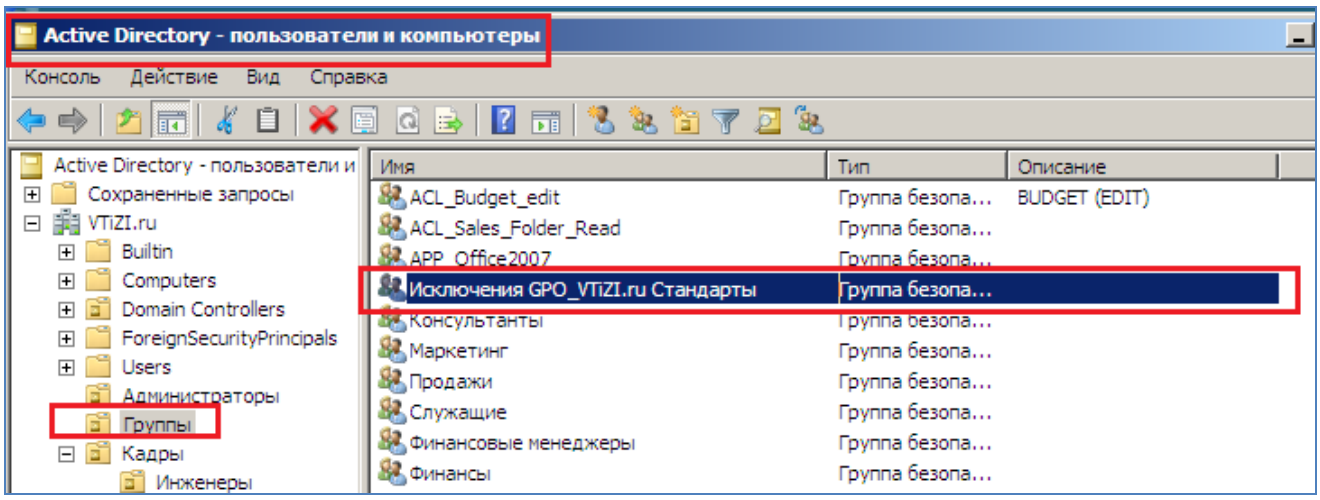


Рисунок 10.7 – Результат создания глобальной группы безопасности

13 В консоли управления групповой политикой GPMC выберите контейнер «Объекты групповой политики». Щелкните правой кнопкой мыши объект GPO «Параметры политики инженеров» и выполните команду «Удалить». Подтвердить удаление, щелкнув «Да» .

14 В домене выберите объект «CONTOSO Стандарты». Перейдите на вкладку «Делегирование». Щелкните кнопку «Дополнительно». В диалоговом окне «Параметры безопасности» щелкните «Добавить». Введите имя группы «Исключения GPO_CONTOSO_Стандарты» и щелкните ОК.

15 В списке разрешений найдите разрешение «Применить групповую политику» и установите флажок «Запретить». Затем щелкните ОК. Для того чтобы подтвердить изменение, щелкните кнопку Да (рисунок 10.8).

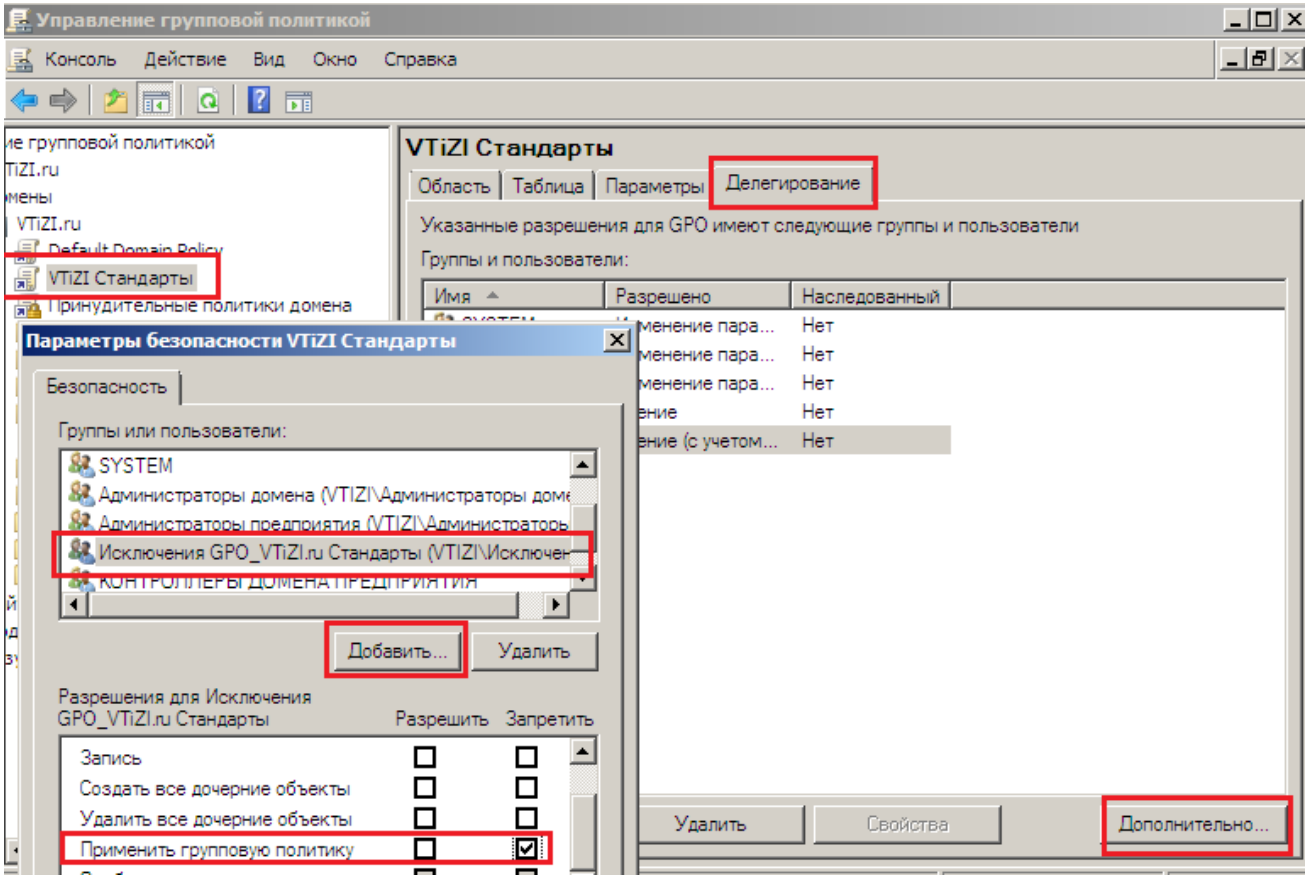


Рисунок 10.8 – Изменение параметр безопасности «Применить групповую политику»

16 Просмотрите запись на вкладке «Делегирование» в столбце «Разрешено» группы «Исключения GPO_CONTOSO_Стандарты».

17 Перейдите на вкладку «Область» и проанализируйте секцию «Фильтры безопасности». По умолчанию в фильтрах безопасности нового GPO группа «Прошедшие проверку обладает разрешением «Применить групповую политику», чтобы все пользователи и компьютеры в области действия GPO могли применять параметры этого GPO. Вы отконфигурировали группу с запретом чтения групповой политики, который заменяет разрешение. Чтобы освободить пользователя от политики объекта «CONTOSO Стандарты», можно просто добавить его в группу.

11 Лабораторная работа №11. Делегирование членства с помощью групповой политики

Цель работы: получить навыки делегирования членства с помощью групповой политики в Active Directory

11.1 Постановка задачи

Создайте GPO с параметром политики групп с ограниченным доступом, который добавляет группу Справка в локальную группу Администраторы (Administrators) на всех клиентских компьютерах.

11.2 Порядок выполнения работы

1 В консоли Управление групповой политикой (Group Policy Management) разверните узел Лес\Домены \contoso.com (Forest\Domains\contoso.com). Выберите контейнер Объекты групповой политики (Group Policy Objects) .

2 Щелкните правой кнопкой мыши контейнер Объекты групповой политики и выполните команду Создать (New). В поле Имя (Name) введите имя «Корпоративная справка» и щелкните ОК.

3 Щелкните правой кнопкой мыши созданный объект GPO и выполните команду Изменить (Edit). В редакторе управления групповыми политиками (Group Policy Management Editor) откройте узел Конфигурация компьютера \Политики\ Конфигурация Windows \ Параметры безопасности \Группы с ограниченным доступом. Щелкните правой кнопкой мыши узел «Группы с ограниченным доступом» и выполните команду «Добавить группу» .

4 Щелкните кнопку «Обзор (Browse)», в диалоговом окне «Выбор: "Группы"(Select Groups)» введите имя группы «CONTOSO\Справка» и щелкните ОК (рисунок 11.1).

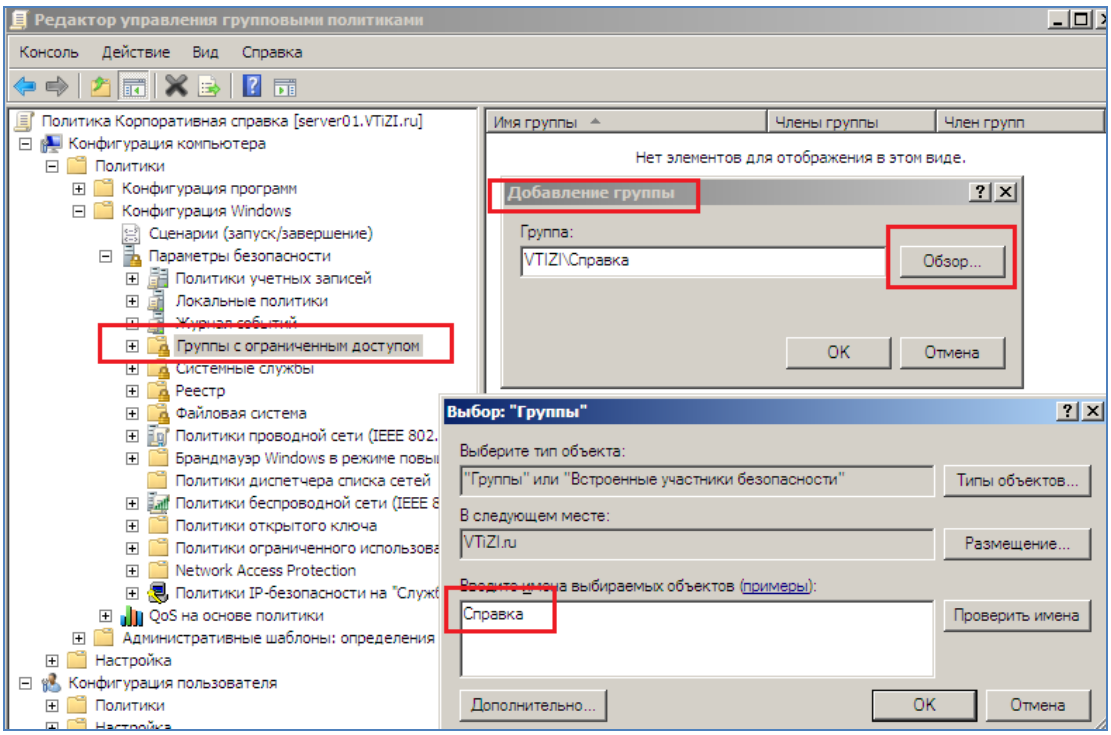


Рисунок 11.1 – Добавление группы

5 Закроите диалоговое окно «Добавление группы», щелкнув «ОК».

6 Напротив секции «Эта группа является членом в» щелкните кнопку «Добавить». Введите имя группы «Администраторы» и щелкните «ОК» (рисунок 11.2) .

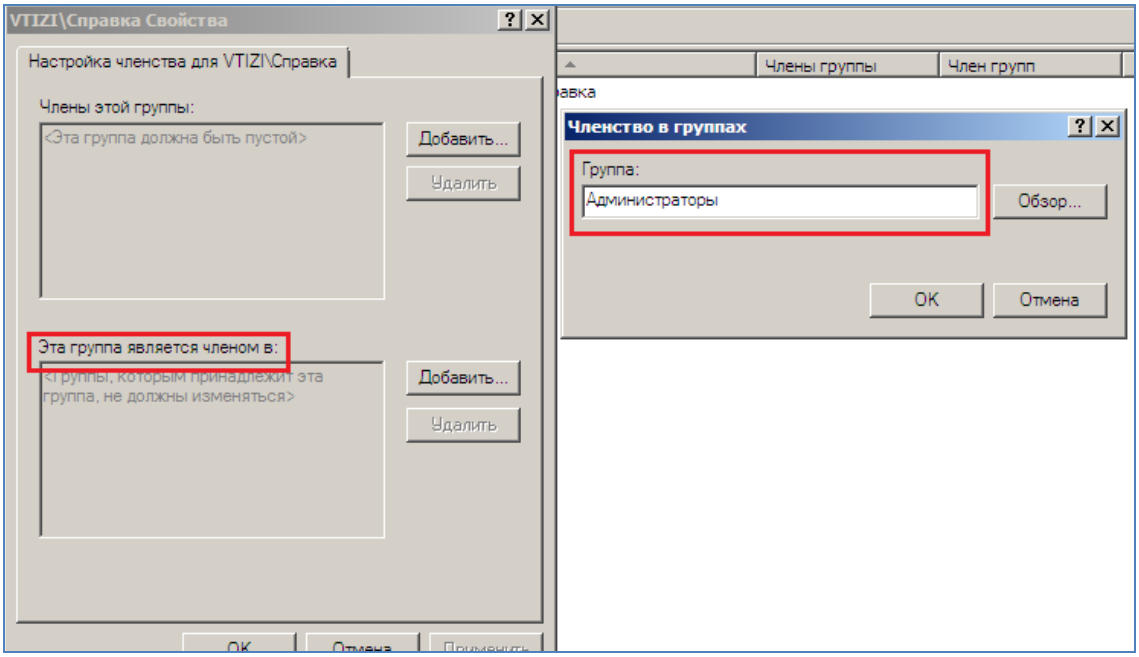


Рисунок 11.2 – Окно справка свойств

7 Вновь щелкните «ОК», чтобы закрыть диалоговое окно «Свойства». Закройте редактор управления групповыми политиками.

8 В консоли «Управление групповой политикой» щелкните правой кнопкой мыши подразделение «Клиенты» и выполните команду «Связать существующий объект GPO» (рисунок 11.3).

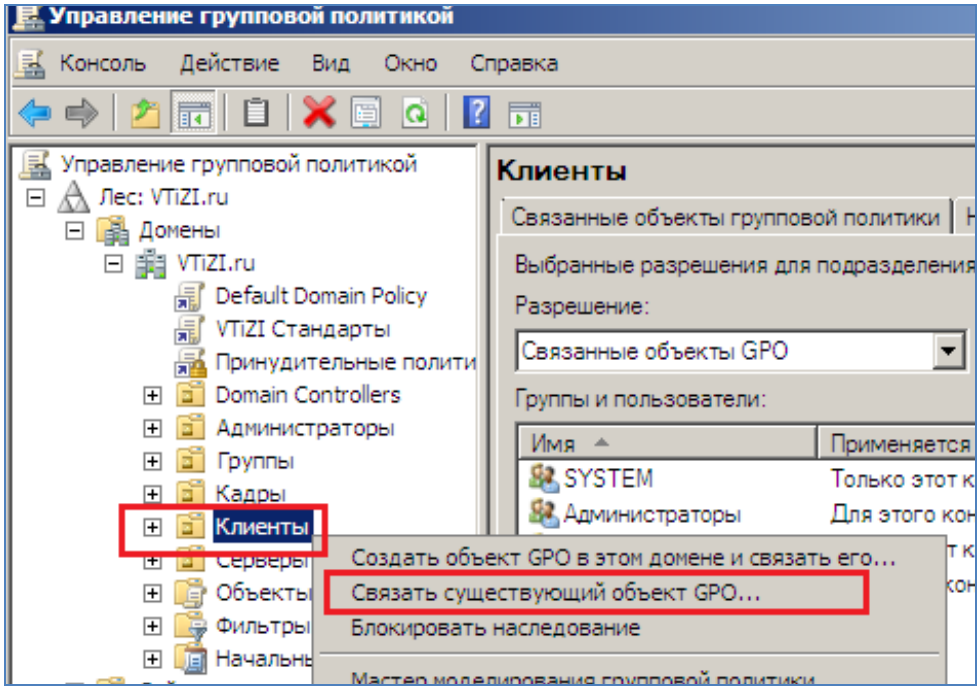


Рисунок 11.3 – Управление групповой политикой

9 Выберите объект групповой политики «Корпоративная справка», щелкните «ОК».

12 Лабораторная работа №12. Управление параметрами безопасности

Цель работы: получить навыки управления параметрами безопасности в Active Directory

12.1 Постановка задачи

1 В этом упражнении используется локальная политика безопасности, чтобы разрешить группе входить на контроллер домена SERV ER01 с помощью «Удаленного рабочего стола». Локальная политика безопасности контроллера домена влияет только на отдельный контроллер домена и не реплицируется на другие контроллеры в домене.

2 Создайте шаблон безопасности, предоставляющий группе «Удаленный рабочий стол SYS_DC» право входа, с помощью удаленного рабочего стола.

3 Проанализируйте конфигурацию машины SERVER01 с помощью шаблона безопасности «Удаленный рабочий стол DC», определите отличия между текущей конфигурацией сервера и конфигурацией, определенной в шаблоне, и создайте новый шаблон безопасности.

4 Создайте политику безопасности контроллеров в домене contoso.com на основе конфигурации машины SERVER01 с помощью мастера настройки безопасности.

5 Преобразуйте политику безопасности, созданную в упражнении 4, в объект групповой политики GPO, который затем можно развернуть на компьютерах с помощью групповой политики.

12.2 Порядок выполнения работы

1 Войдите на машину SERVER01 как администратор. В группе «Администрирование» откройте консоль «Локальная политика безопасности». Развер-

ните узел «Параметры безопасности \Локальные политики \Назначение прав пользователя» (рисунок 12.1).

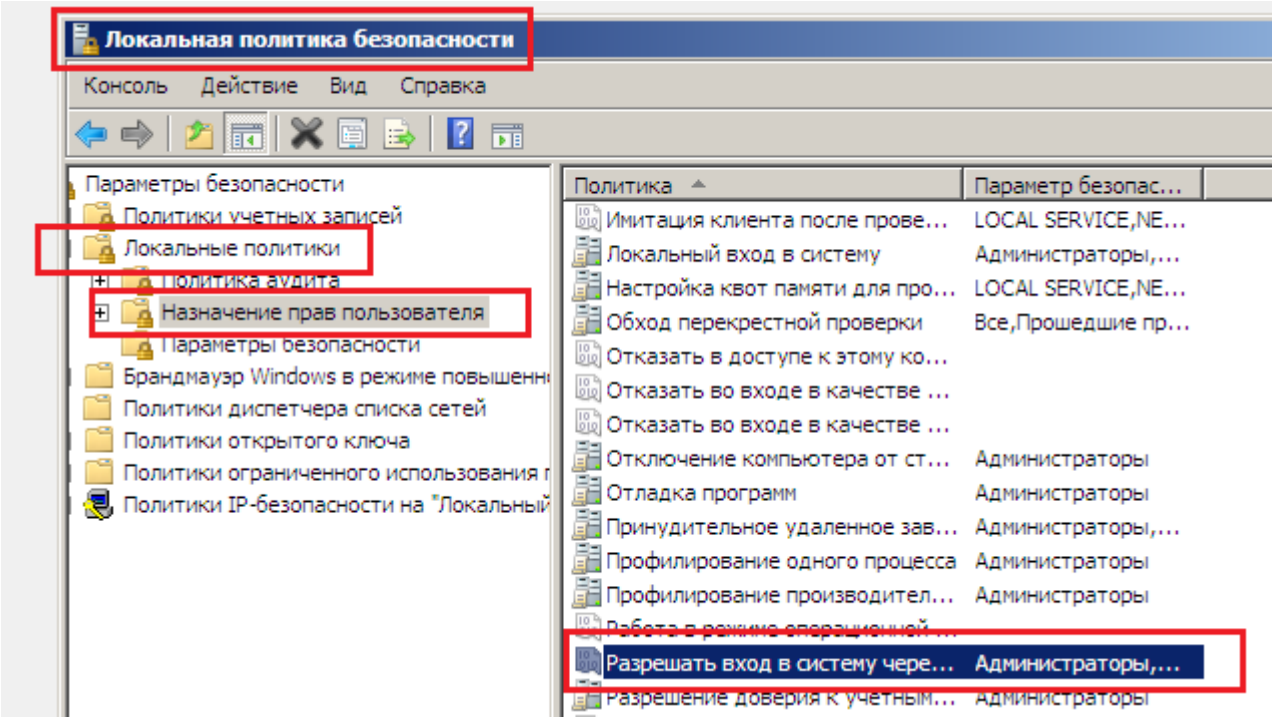


Рисунок 12.1 - Окно Локальной политики безопасности

2 На панели сведений дважды щелкните параметр «Разрешать вход в систему через службу терминалов». Щелкните кнопку «Добавить пользователя или группу». Введите имя группы «Удаленный рабочий стол SYS_DC» и щелкните ОК.

1 Если вы хотите протестировать результат упражнения путем входа на контроллер домена как член группы «Удаленный рабочий стол SYS_DC» с помощью подключения удаленного рабочего стола, создайте учетную запись пользователя и добавьте ее в группу. Убедитесь, что группа является членом группы «Пользователи удаленного рабочего стола», или хотя бы имеют разрешение на подключение RDP-Tcp.

2 Теперь удалите этот параметр, поскольку в последующих упражнениях вы будете управлять им с помощью других инструментов.

3 Дважды щелкните параметр «Разрешать вход в систему через службу терминалов». Выберите группу «Удаленный рабочий стол SYS_DC». Щелкните «Удалить» и ОК (рисунок 12.2).

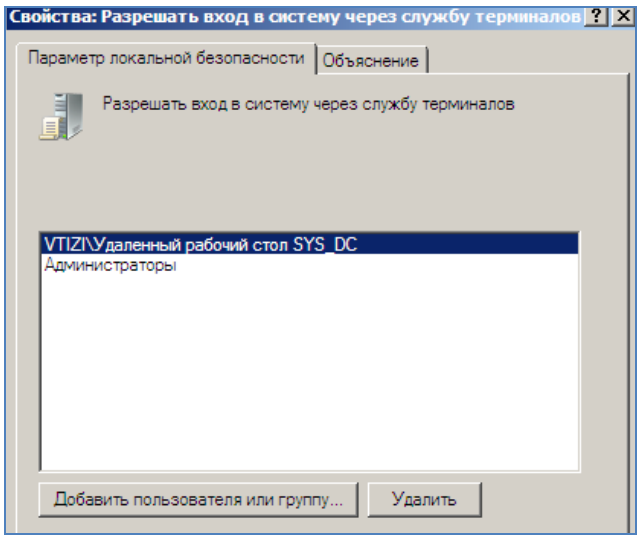


Рисунок 12.2 – Настройки удаленного стола

4 Войдите на машину SERVER01 как администратор. В меню «Пуск» щелкните команду «Выполнить». Введите имя mmc и нажмите клавишу «Enter» .

5 В меню «Консоль» выберите команду «Добавить или удалить оснастку».

6 В списке «Доступные оснастки» выберите оснастку «Шаблоны безопасности» и щелкните «Добавить» и ОК (рисунок 12.3) .

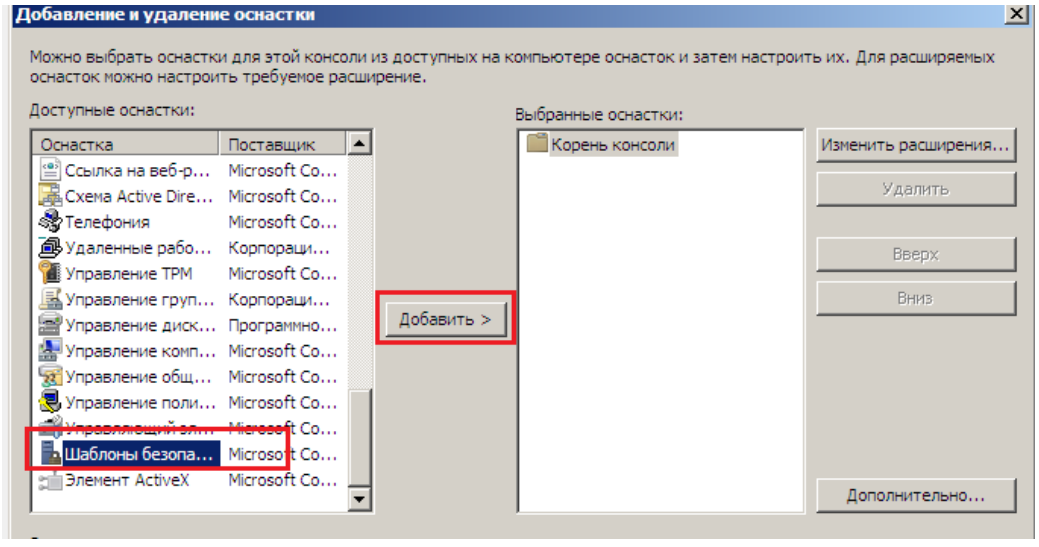


Рисунок 12.3 – Выбор оснастки

7 В меню «Консоль» выберите команду «Сохранить» и сохраните консоль на рабочем столе под именем «Управление безопасностью» .

8 Щелкните правой кнопкой мыши узел C:\Users\Administrator \Documents\ Security\Templates и выполните команду «Создать шаблон» (рисунок 12.4) .

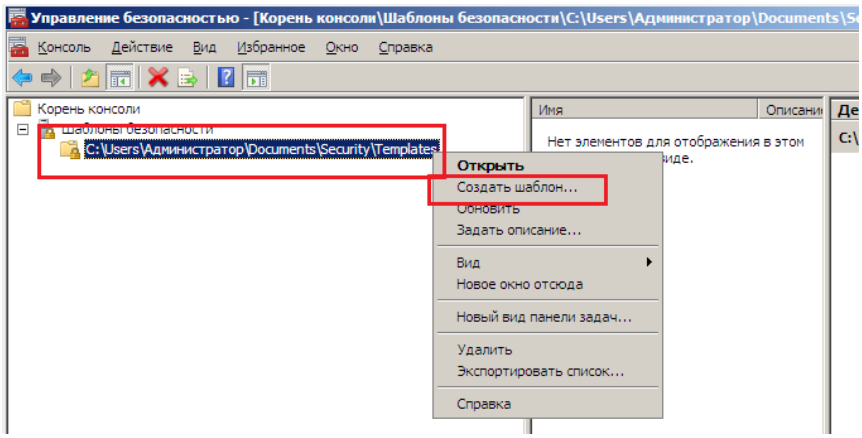


Рисунок 12.4 – Создание шаблона

9 Введите имя «Удаленный рабочий стол DC» и щелкните ОК.

10 В узле «Удаленный рабочий стол DC» разверните узел «Локальные политики \Назначение прав пользователя» (рисунок 12.5) .

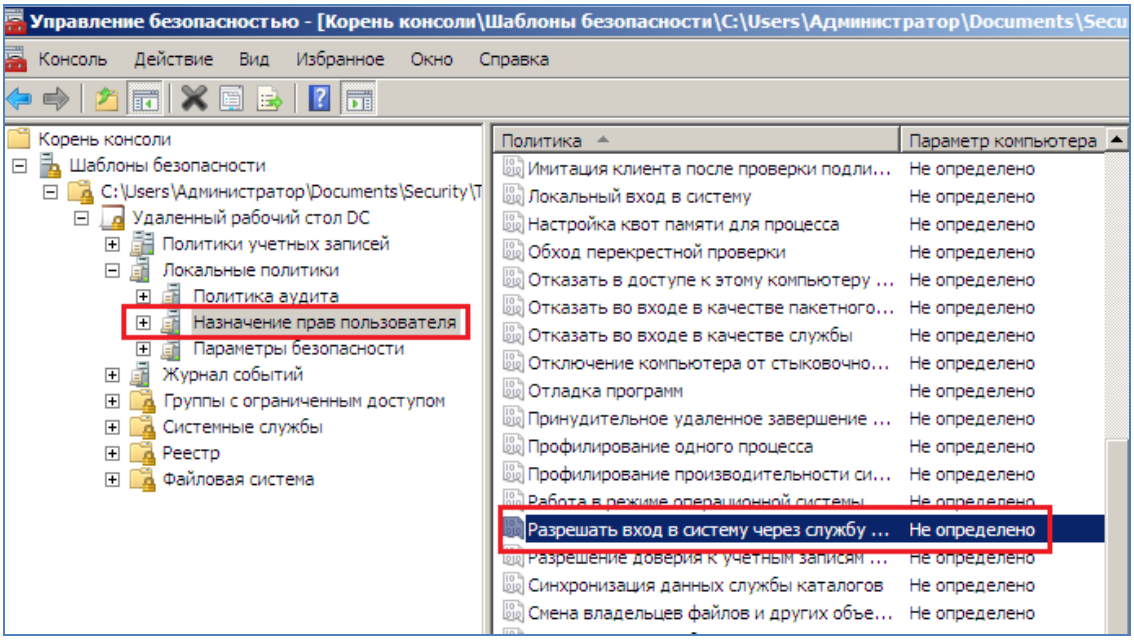


Рисунок 12.5 - Назначение прав пользователей

11 На панели сведений дважды щелкните параметр «Разрешать вход в систему через службу терминалов». Установите флажок «Определить следующие параметры политики в шаблоне» .

12 Щелкните кнопку «Добавить пользователя или группу». Введите имя группы «CONTOSO\ Удаленный рабочий стол SYS_DC» и щелкните ОК (рисунок 12.6). .

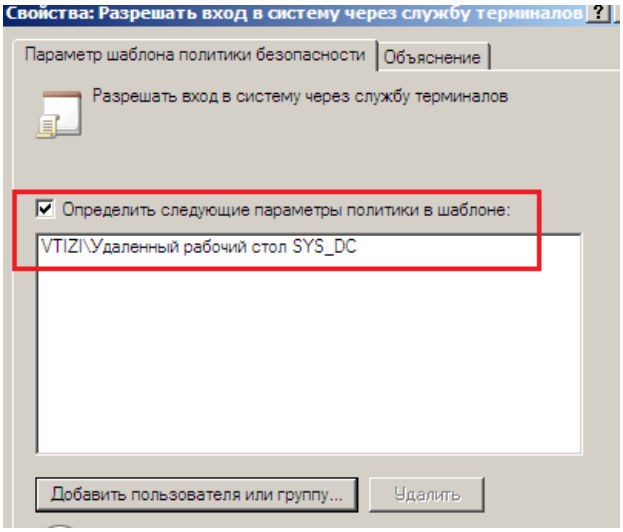


Рисунок 12.6 – Определение политики безопасности для удаленного рабочего стола

13 Щелкните правой кнопкой мыши шаблон «Удаленный рабочий стол DC» и выполните команду «Сохранить» .

14 Войдите на машину SERVER01 как администратор. Откройте консоль «Управление безопасностью», созданную и сохраненную .

15 В меню «Консоль» выберите команду «Добавить или удалить оснастку».

16 Затем в списке «Доступные оснастки» выберите оснастку «Анализ и настройка безопасности» и щелкните кнопку «Добавить» . Щелкните ОК (рисунок 12.7) .

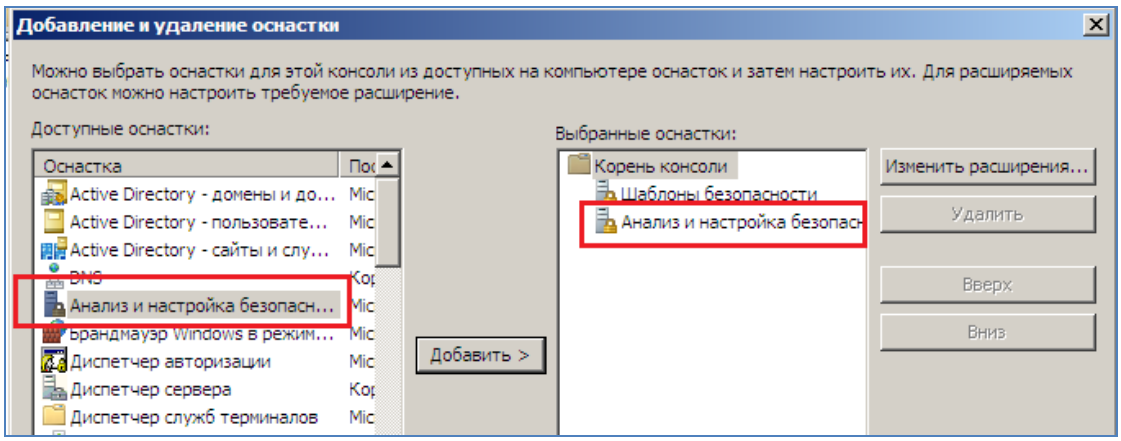
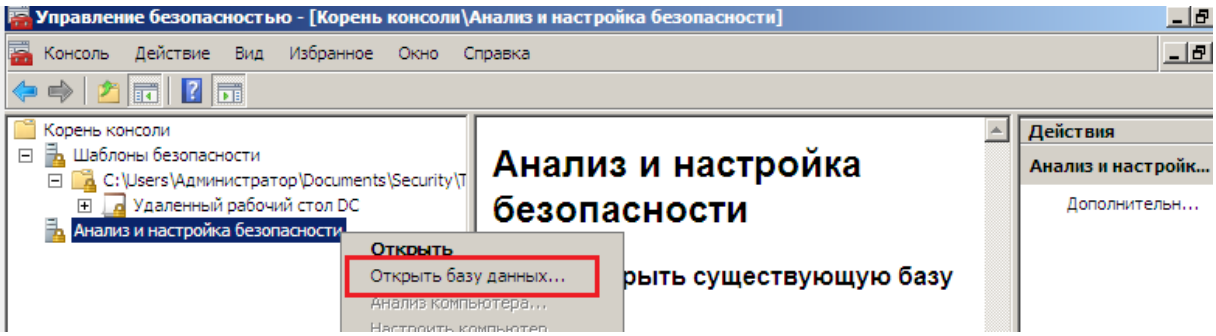


Рисунок 12.7 – Анализ настроеек безопасности

17 Выберите в меню «Консоль» команду «Сохранить», чтобы сохранить модифицированную консоль.

18 В дереве консоли выберите узел «Анализ и настройка безопасности».

19 Щелкните правой кнопкой мыши этот узел и выполните команду «Открыть базу данных», с помощью которой будет создана новая база данных безопасности (рисунок 12.8).



Риунок 12.8 – Открытие базы данных для создания базы данныз безопасности

20 Введите имя «SERVER01Test» и щелкните кнопку «Открыть». Откроется диалоговое окно «Импорт шаблона». Выберите шаблон «Удаленный рабочий стол DC», созданный в упражнении 2, и щелкните кнопку «Открыть».

21 Щелкните правой кнопкой мыши узел «Анализ и настройка безопасности» и выполните команду «Анализ компьютера». Щелкните ОК, чтобы подтвердить путь к журналу ошибок по умолчанию.

22 Разверните узел «Локальные политики» и выберите папку «Назначение прав пользователя».

23 Политика «Разрешать вход в систему через службу терминалов» будет помечена флажком в виде крестика в красном кружке. Этот флажок указывает на наличие отличия между параметром базы данных и параметром компьютера. Дважды щелкните параметр «Разрешать вход в систему через службу терминалов» (рисунок 12.9).

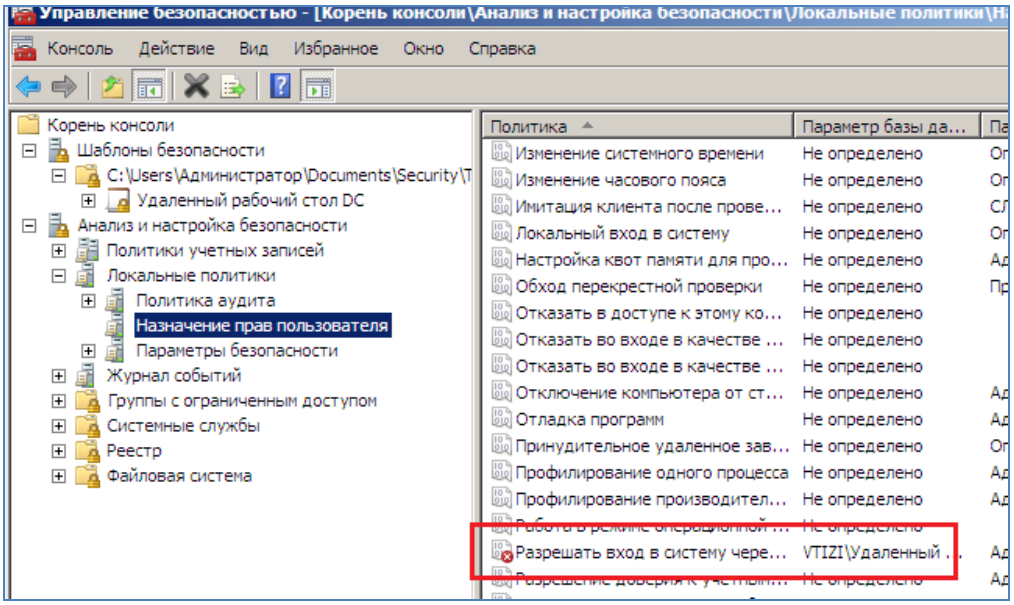


Рисунок 12.9 – Управление локальной политикой безопасности

24 Просмотрите отличия. На компьютере для группы «Удаленный рабочий стол SYS_DC» не отконфигурировано разрешение на подключение с помощью удаленного рабочего стола.

25 Обратите также внимание на то, что флажок «На компьютере» разрешает администраторам входить через службы терминалов. Этот важный параметр следует внедрить в базу данных.

26 Установите флажок «В базе данных» для администраторов и щелкните ОК. Таким образом, в базу данных будет добавлено право входа через службы терминалов для администраторов. Шаблон при этом не будет изменен, как и текущая конфигурация компьютера (рисунок 12.10).

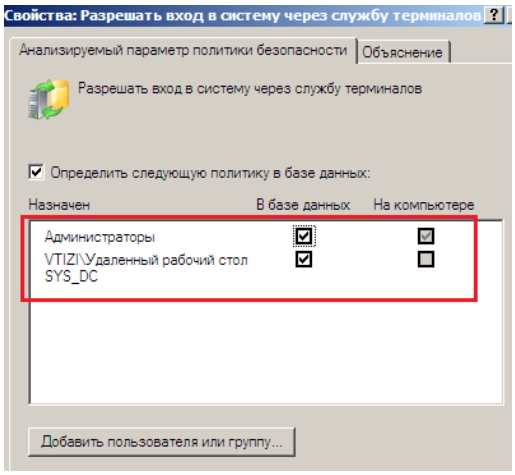


Рисунок 12.10 – Добавление права входа через службу терминалов

27 Щелкните правой кнопкой мыши узел «Анализ и настройка безопасности» и выполните команду «Сохранить». База данных безопасности будет сохранена вместе с параметрами, импортированными из шаблона, и внесенным изменением, разрешающим вход администраторов через службы терминалов. На панели состояния при выборе команды «Сохранить» отображается подсказка, где указано, что вы сохраняете шаблон. Это некорректная подсказка. На самом деле вы сохраняете базу данных.

28 Щелкните правой кнопкой мыши узел «Анализ и настройка безопасности» и выполните команду «Экспорт шаблона». Выберите шаблон «Удаленный рабочий стол DC» и щелкните кнопку «Сохранить». Таким образом, вы заменяете в шаблоне, созданном, параметры, определенные в базе данных оснастки «Анализ и настройка безопасности».

29 Закройте и вновь откройте консоль «Управление безопасностью», чтобы полностью обновить параметры в оснастке «Шаблоны безопасности». Разверните шаблон C:\Users\Администратор\Documents\Security\Templates\ Удаленный рабочий стол DC и откройте папку Локальные политики \ Назначение прав пользователя.

30 На панели сведений дважды щелкните параметр «Разрешать вход в систему через службу терминалов». Обратите внимание на то, что в шаблоне безопас-

ности обеим группам – «Администраторы» и «Удаленный рабочий стол SYS_DC» - разрешено входить через службы терминалов.

31 Щелкните правой кнопкой мыши узел «Анализ и настройка безопасности» и выполните команду «Настроить компьютер». Щелкните ОК, чтобы подтвердить путь к журналу ошибок. Параметры базы данных будут применены к серверу. Далее проверьте, изменены ли права пользователя.

32 В группе «Администрирование» откройте консоль «Локальная политика безопасности». Если во время выполнения этого упражнения консоль была открыта, щелкните правой кнопкой мыши узел «Параметры безопасности» и выполните команду «Перезагрузить».

33 Разверните узел «Параметры безопасности\Локальные политики\ Назначение прав пользователя». Дважды щелкните параметр «Разрешать вход в систему через службу терминалов». Убедитесь, что в списке перечислены обе группы – Администраторы» и «Удаленный рабочий стол SYS_DC». Консоль Локальная политика безопасности отображает реальные текущие параметры сервера.

34 Войдите на машину SERVER01 как администратор. В группе Администрирование откройте «Мастер настройки безопасности» (рисунок 12.11).

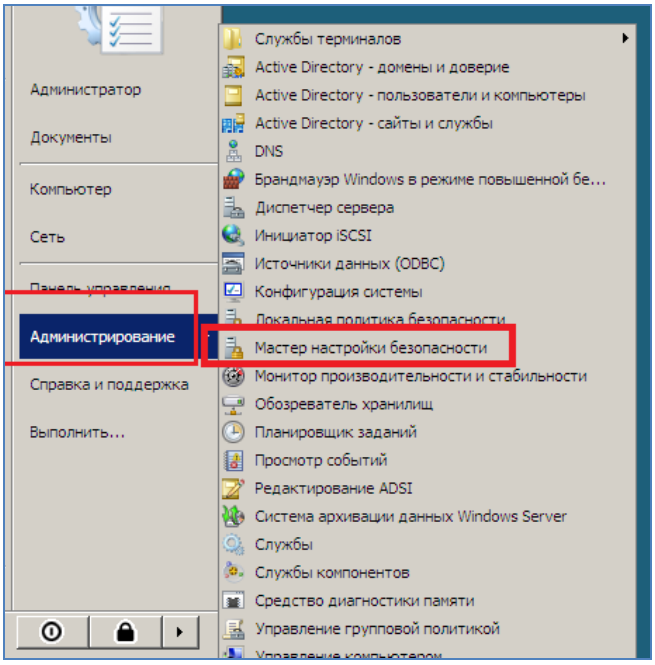


Рисунок 12.11 – Мастер настройки безопасности

35 Щелкните «Далее». Выберите действие «Создать новую политику безопасности». Примите имя сервера SERVER01 по умолчанию и щелкните «Далее» .

36 На странице «Обработка данных настройки безопасности» вы можете щелкнуть кнопку «Просмотр базы данных» и просмотреть конфигурацию на машине SERVER01 (рисунок 12.12).

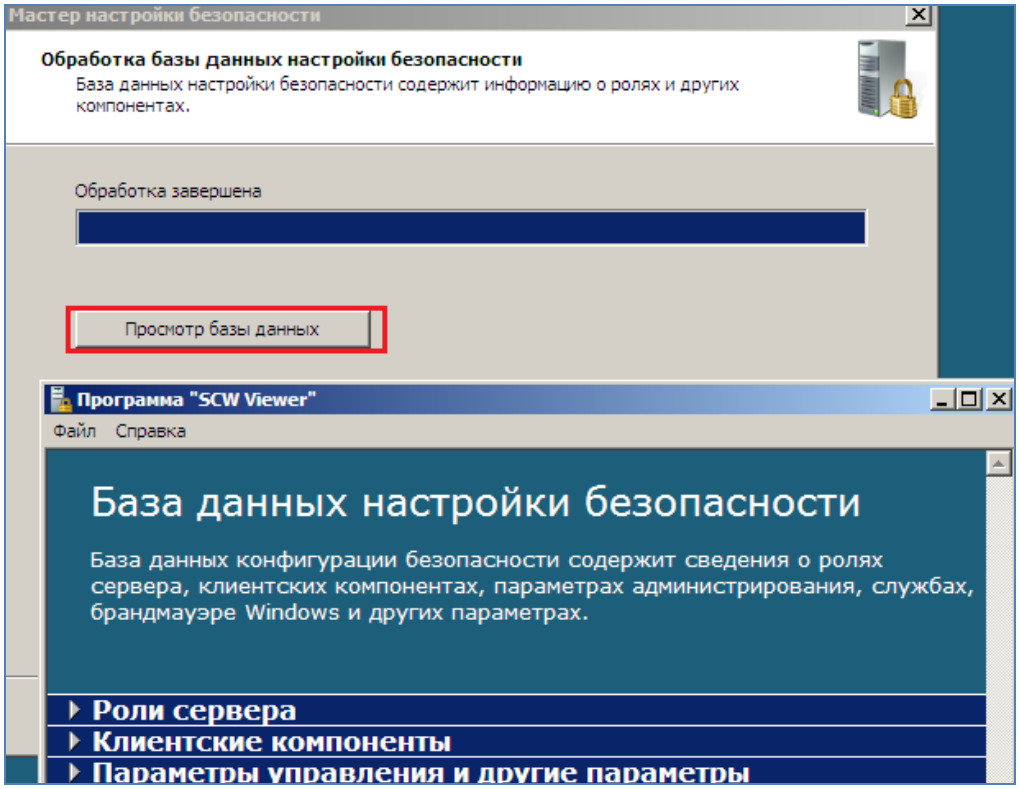


Рисунок 12.12 – Обработка данных настройки безопасности

37 Щелкните «Далее» и на вводной странице секции «Настройка служб на основе ролей» щелкните «Далее».

38 На страницах «Выбор ролей сервера», «Выбор клиентских возможностей», «Выбор управления» и других параметров, Выбор дополнительных служб и «Обработка неопределенных ролей» просмотрите при желании параметры, обнаруженные на машине SERVER01, однако не изменяйте их. На каждой странице щелкайте «Далее» .

39 На странице «Подтверждение изменений для служб» щелкните раскрывающийся список «Просмотреть» и выберите «Все службы». Проанализируйте параметры в столбце «Текущий режим запуска», отображающем режимы запуска на

машине SERVER01, и сравните их с параметрами в столбце «Режим запуска политики». Щелкните раскрывающийся список «Просмотреть» и выберите «Измененные службы». Щелкните «Далее» (рисунок 12.13).

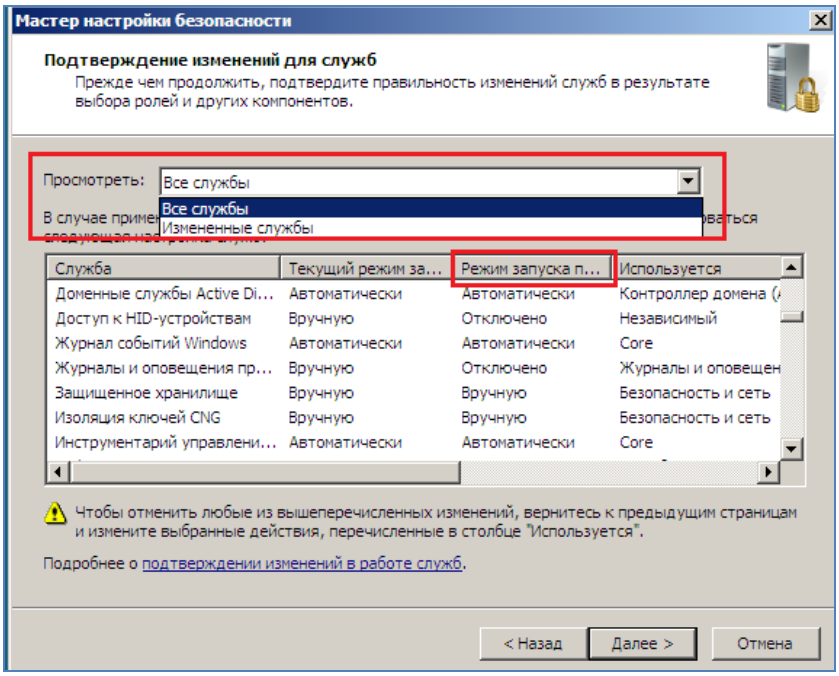


Рисунок 12.13 – Подтверждение изменении для служб

40 На вводной странице секции «Сетевая безопасность» щелкните «Далее».

41 На странице «Правила сетевой безопасности» вы можете при желании проанализировать правила брандмауэра, выведенные из конфигурации SERVER01. Не изменяйте их. Щелкните «Далее» .

42 На вводной странице секции «Параметры реестра» щелкните «Далее».

43 Щелкайте «Далее» на каждой странице секции «Параметры реестра». Проанализируйте, но не изменяйте параметры. На странице «Сводка параметров реестра» просмотрите заданные параметры и щелкните «Далее» (рисунок 12.14).

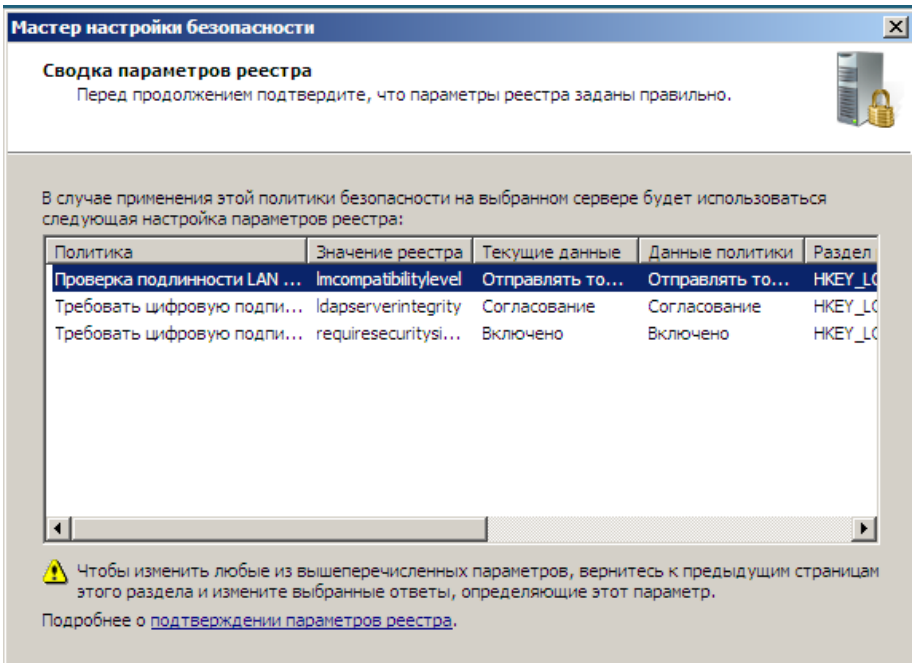


Рисунок 12.15 – Параметры реестра

44 На вводной странице секции «Политика аудита» щелкните «Далее». На странице «Политика аудита системы» просмотрите, но не изменяйте параметры. Щелкните «Далее» .

45 На странице «Сводка политики аудита» проанализируйте параметры в столбцах «Текущее значение» и «Параметр политики». Щелкните «Далее» (рисунок 12.16) .

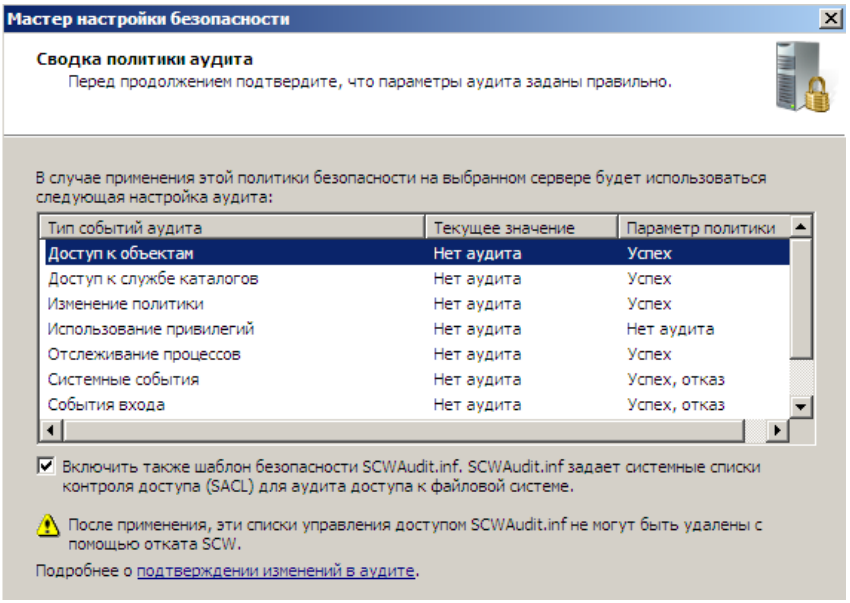


Рисунок 12.16 – Сводка политики аудита

46 На вводной странице секции «Сохранение политики безопасности» щелкните «Далее». В текстовое поле «Имя файла политики безопасности» введите имя «Политика безопасности DC» (рисунок 12.17).

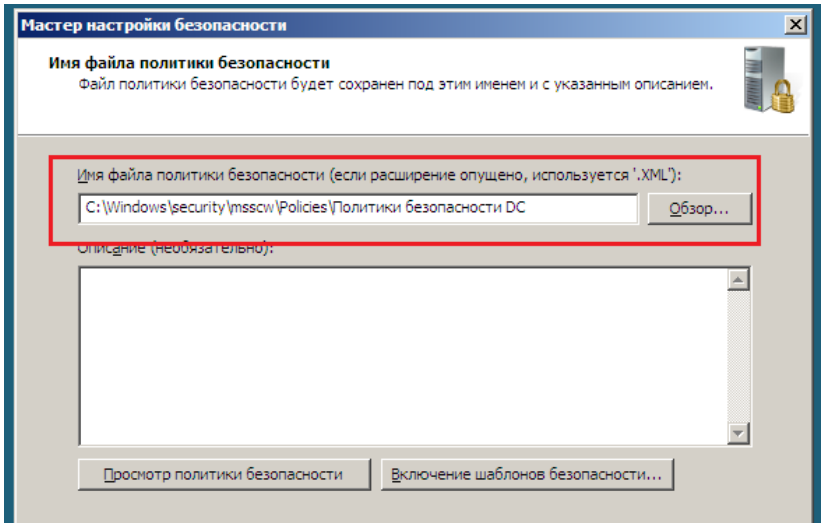


Рисунок 12.17 – Политика безопасности DC

47 Щелкните кнопку «Включение шаблонов безопасности». Щелкните «Добавить». Локализуйте шаблон «Удаленный рабочий стол DC», созданный в упражнении 2, который находится в папке «Documents\Security\Templates» . Выбрав шаблон, щелкните «Открыть» (рисунок 12.18).

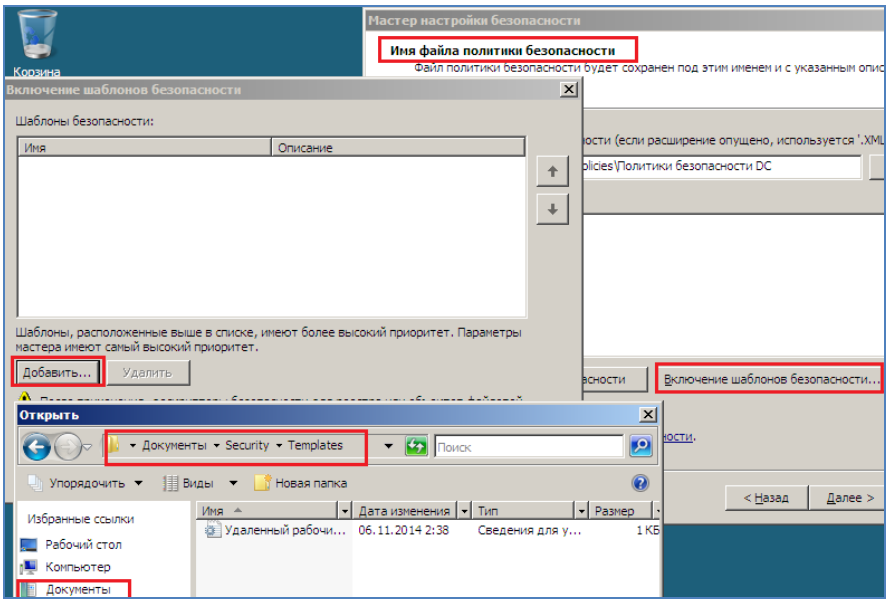


Рисунок 12.18 – Включение шаблонов безопасности

48 Щелкните «ОК», чтобы закрыть диалоговое окно «Включение шаблонов безопасности». Щелкните кнопку «Просмотр политики безопасности», чтобы просмотреть параметры в политике безопасности. Вам будет предложено подтвердить использование элемента управления ActiveX. Щелкните «Да». Просмотрев параметры политики, закройте окно, а затем щелкните «Далее» .

49 Выберите опцию «Применить позже» и щелкните «Далее». Щелкните «Готово».

50 Войдите на машину SERVER01 как администратор. Откройте окно командной строки. Введите команду «cd c:\windows\security\msscw\policies» и нажмите клавишу «Enter» .

51 Введите команду «scwcmd transform/?» и нажмите клавишу Enter.

52 Введите команду «scwcmd transform /p: "Политика безопасности DC.xml"/g: "Политика безопасности DC" и нажмите клавишу Enter (рисунок 12.19).

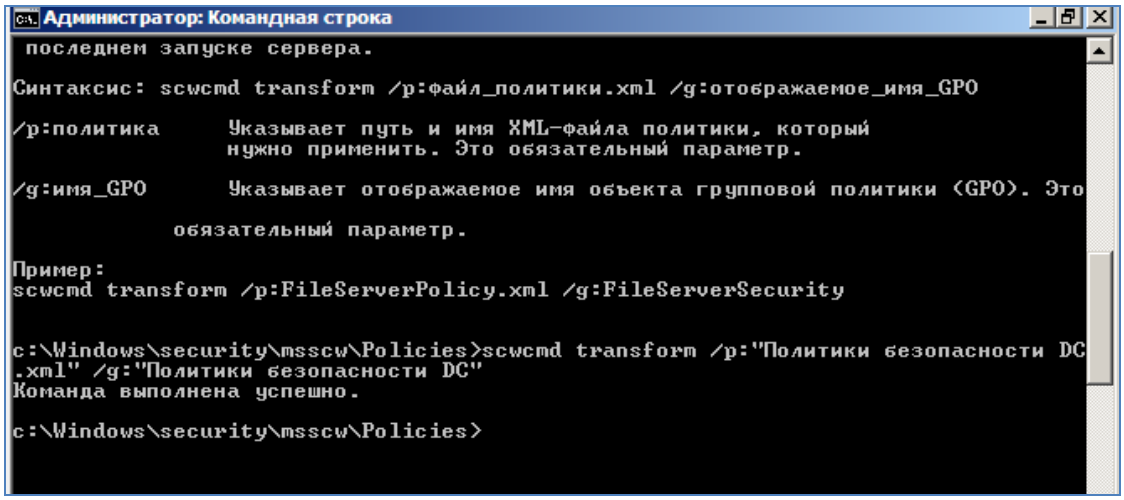


Рисунок 12.19 – Политики безопасности DC

53 В группе «Администрирование» откройте консоль «Управление групповой политикой». В дереве консоли разверните узлы «Лес», «Домены», домен contoso.com и откройте папку «Объекты групповой политики» .

54 Выберите объект групповой политики «Политика безопасности DC», созданный командой Scwcmd.exe. Перейдите на вкладку «Параметры», чтобы про-

смотреть параметры GPO. В секции «Параметры безопасности» щелкните ссылку «Показать» (рисунок 12.20).

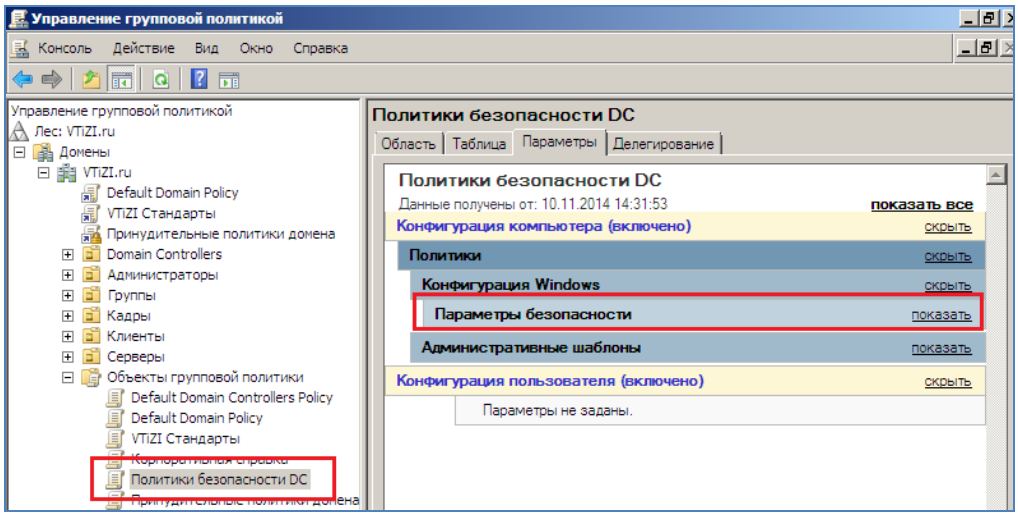


Рисунок 12.20 – Параметры безопасности

55 В секции «Локальные политики/Предоставление прав пользователям» щелкните ссылку «Показать». Убедитесь, что группам «Администраторы» в папке BUILTIN и «contoso\Удаленный рабочий стол SYS_DC» предоставлено разрешение «Разрешать вход в систему через службу терминалов».

56 Этот объект GPO не будет применен к контроллеру домена, поскольку он несвязан с подразделением Domain Controllers. Выполняя упражнение, не связывайте GPO с доменом, сайтом или подразделением. В производственной среде нужно потратить много времени на анализ, настройку и тестирование параметров безопасности в политике безопасности, прежде чем развернуть ее в качестве объекта GPO на производственных контроллерах домена.

13 Лабораторная работа №13. Конфигурация параметров аудита

Цель работы: получить навыки по конфигурированию параметров аудита, фильтрованию конкретных событий в журнале «Безопасность»

13.1 Постановка задачи

В данной работе предлагается отконфигурировать параметры аудита, включить политики аудита доступа к объектам и отфильтровать конкретные события в журнале «Безопасность». Бизнес-цель состоит в мониторинге папки с конфиденциальными данными, к которой не должны получать доступ пользователи из группы «Консультанты». Кроме того, необходимо отконфигурировать аудит для отслеживания изменений членства группы «Администраторы домена» .

Прежде всего нужно выполнить в среде следующие подготовительные шаги:

– на диске «С» создать папку «Конфиденциальные данные»;

– создать глобальную группу безопасности «Консультанты»;

– добавить группу «Консультанты» в группу «Операторы печати» — благодаря этому пользователь в группе «Консультанты» сможет локально входить на машину SERVER01, которая в данном упражнении является контроллером домена;

– создать пользователя «Джеймс Файн» и добавить его в группу «Консультанты» .

Настройка разрешений и параметров аудита. Необходимо отконфигурировать разрешения папки «Конфиденциальные данные для запрета доступа пользователям из группы «Консультанты», затем включить для них аудит попыток получить, доступ к этой папке .

Поскольку машина SERVER01 является контроллером домена, для включения аудита используется ранее созданный объект групповой политики «Политика безопасности DC». На автономном сервере применяется оснастка Локальная поли-

тика безопасности (Local Security Policy) или объект GPO, под область действия которого подпадает сервер .

Генерирование событий аудита. Теперь следует попытаться получить доступ к папке «Конфиденциальные данные» как член группы «Консультанты» .

13.2 Порядок выполнения работы

1 Войдите на машину SERVER01 как администратор. Откройте окно свойств папки «C:\Конфиденциальные данные» и перейдите на вкладку «Безопасность» .

2 Щелкните кнопку «Изменить, а затем «Добавить». Введите имя группы «Консультанты» и щелкните «ОК».

3 Установите флажок «Запретить» напротив разрешения «Полный доступ». Последовательно щелкните кнопки «Применить» и «Да», чтобы подтвердить запрет разрешения (рисунок 13.1).

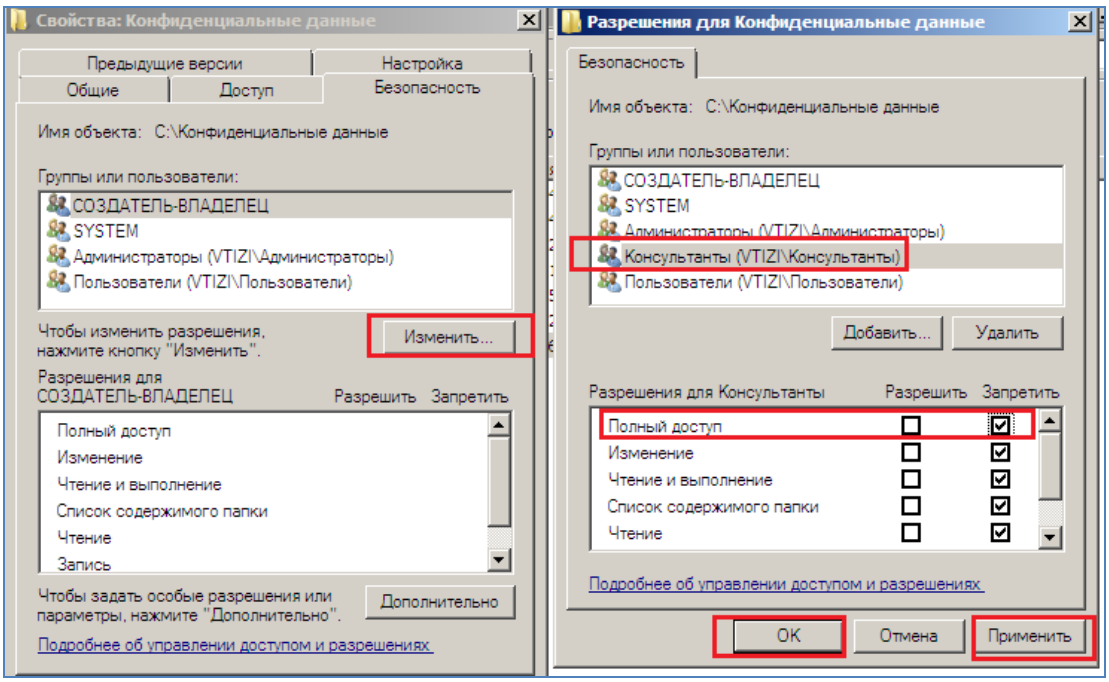


Рисунок 13.1 – Установка полного доступа

4 Для того чтобы закрыть диалоговое окно «Разрешения», щелкните «ОК».

5 Щелкните «Дополнительно». Перейдите на вкладку «Аудит». Щелкните «Изменить», а затем «Добавить». Введите имя «Консультанты» и щелкните «ОК» .

6 В диалоговом окне «Элементы аудита» установите флажок «Отказ» напротив разрешения «Полный доступ». Закройте все диалоговые окна (рисунок 13.2) .

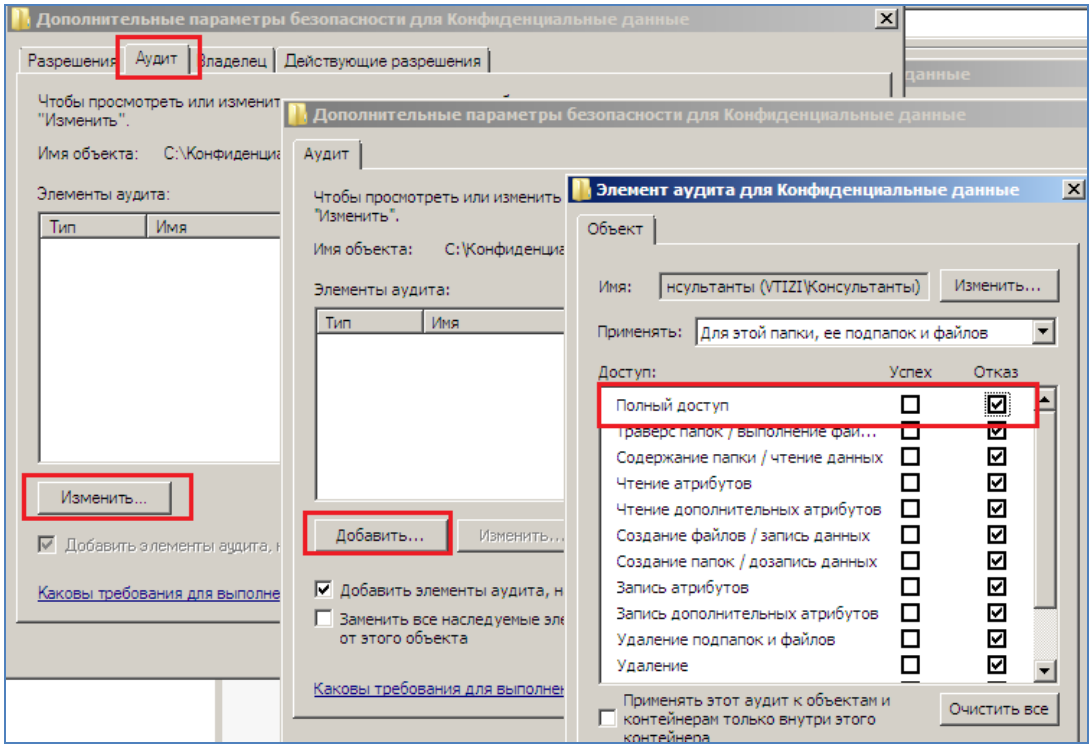


Рисунок 13.2 – Окно элементов аудита для конфиденциальных данных

7 Откройте консоль «Управление групповой политикой» и выберите контейнер «Объекты групповой политики». Щелкните правой кнопкой мыши объект «Политики безопасности DC» и выполните команду «Изменить» .

8 Разверните узел «Конфигурация компьютера\Политики \ Конфигурация Windows \Параметры безопасности\Локальные политики\Политика аудита .

9 Дважды щелкните параметр политики «Аудит доступа к объектам». Установите флажок «Определить следующие параметры политики» .

10 Установите флажок «Отказ». Щелкните «ОК», а затем закройте консоль (рисунок 13.3).

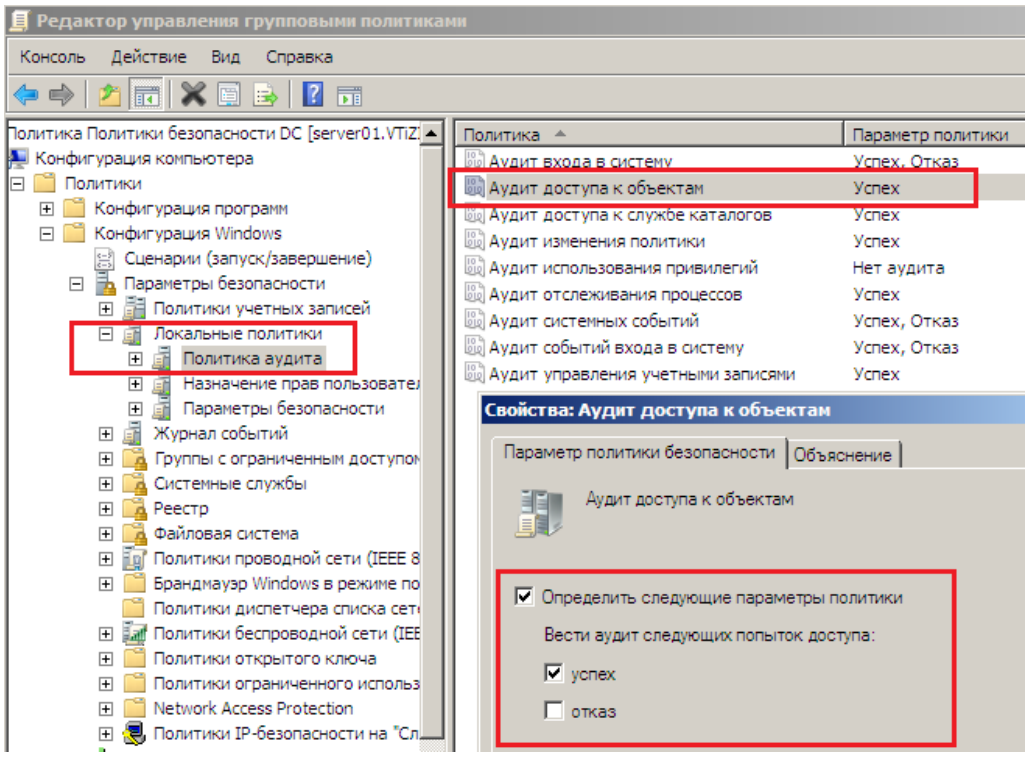


Рисунок 13.3 – Аудит доступа к объектам

11 Для обновления политики и применения всех параметров откройте окно командной строки и введите команду «gpupdate» .

12 Войдите на машину SERVER01 как пользователь Джеймс Файн. Откройте окно «Мой компьютер» и попытайтесь открыть папку «C:\Конфиденциальные данные» .

13 Создайте текстовый файл на рабочем столе и попытайтесь вырезать и вставить его в папку «Конфиденциальные данные» .

14 Войдите на машину SERVER01 как администратор. В группе «Администрирование» откройте оснастку «Просмотр событий» .

15 Разверните узел «Журналы Windows»\Безопасность. Для фильтрации журнала и ограничения области поиска на панели «Действия» щелкните ссылку «Фильтр текущего журнала» .

16 Отконфигурируйте фильтр для ограничения поиска. Чтобы указать событие для локализации, используйте следующие параметры: события за последний час с источником событий Microsoft Windows security auditing и категорией задачи «Файловая система» (рисунок 13.4).

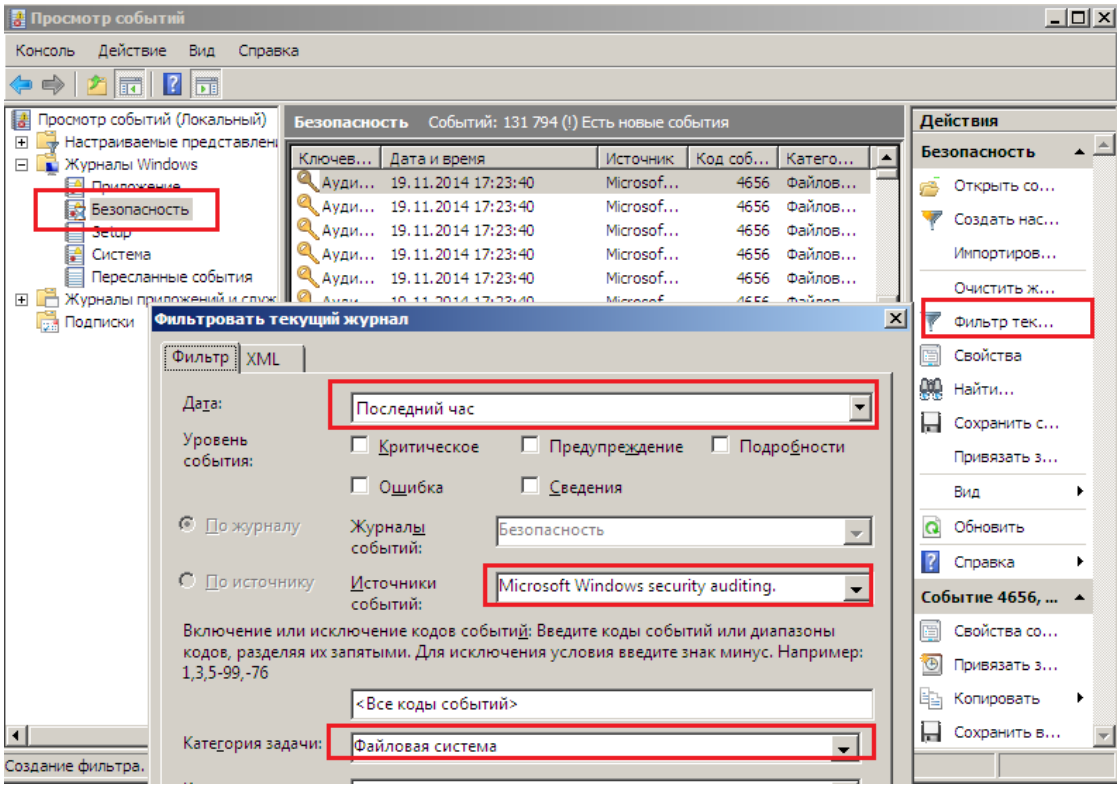


Рисунок 13.4 – Фильтрация текущего журнала

17 Отконфигурируйте фильтр. Щелкните ОК. На панели Действия (Actions) щелкните ссылку Сохранить файл отфильтрованного журнала (Save Filter Log As) .

18 На панели Избранные ссылки (Favorite Links) диалогового окна Сохранить как (Save As) щелкните ссылку Рабочий стол (Desktop) .

19 Щелкните раскрывающийся список Тип файла (Save As Type) и выберите тип Текст (Text).В текстовое поле Имя файла (File Name) введите имя Экспорт журнала аудита .

20 Щелкните кнопку Сохранить (Save). В программе Блокнот (Notepad) откройте полученный текстовый файл и выполните поиск по ключевым словам C:\Конфиденциальные данные .

Список использованных источников

1 Нестеров С. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft/ С. Нестеров, В. Ефименко// http://www.intuit.ru/studies/courses/531/387/info.

2 Microsoft *Security Assessment* Tool. Страница загрузки программы. http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=cd057d9d-86b9-4e35-9733-7acb0b2a3ca1.

3 Кенин А. М. Самоучитель системного администратора/А.М. Кенин// — 3-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2012.

4 Холмс Д. Настройка Active Directory. Windows Server 2008. Учебный курс Microsoft / Д. Холмс, Н. Реет, Д. Реет// Пер. с англ. — М.: Издательство «Русская редакция», 2011.