

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)

Кафедра информационных систем
и программной инженерии

Х.М. Салех

АДМИНИСТРИРОВАНИЕ И БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

Методические указания к лабораторным работам

Владимир 2014

Содержание

Лабораторная работа №1
Лабораторная работа №2
Лабораторная работа №3
Лабораторная работа №4
Лабораторная работа №5
Лабораторная работа №6
Лабораторная работа №7
Лабораторная работа №8

ЛАБОРАТОРНАЯ РАБОТА №1 АДМИНИСТРИРОВАНИЕ WINDOWS SERVER 2012 R2. ЧАСТЬ 1

1. Цель работы

- 1) Установить в виртуальную среду (VirtualBox) Windows server 2012 R2
- 2) Установить Доменные службы Active Directory
- 3) Сделать сервер контроллером домена
- 4) Установить и настроить роль файлового сервера
- 5) Создать несколько подразделений AD (2-3)
 - Company user (основная группа пользователей)
 - Simple users (простые пользователи)
 - Manager (менеджеры)
 - Accounting (бухгалтерия)
 - Administration (администрация)
- 6) Создать пользователей домена в соответствующих подразделениях (3-5)
 - ivanov (Иванов Иван Сергеевич) \ Обычный пользователь
 - petrov (Петров Евгений Сидорович) \ Менеджер
 - pilula (Пиллюля Федор Бедросович) \ Менеджер
 - jigurga (Никита Жигурда) \ Бухгалтер
 - alisa (Федюшкина Алиса Викторовна) \ Бухгалтер
 - boss (Путин Владимир Геннадьевич) \ Администрация
 - medved (Медведев Дмитрий Геннадьевич) \ Администрация
- 7) Создать несколько групп безопасности пользователей
 - Buhi (Бухгалтерия)
 - Adm (Администрация)
 - Man (менеджеры)
- 8) Распределим пользователей по группам безопасности

2. Общие сведения

Для выполнения лабораторной работы потребуется:

- Программа виртуализации VirtualBox
- Образ операционной системы Windows Server 2012 R2 (например, редакции Standart). Пробную версию можно [скачать с сайта technet.microsoft.com](#)
- Образ операционной системы Windows 7 или Windows 8. Эти операционные системы можно так же скачать с сайта [technet.microsoft.com](#).

2.1 Устанавливаем приложение для установки и запуска виртуальных машин.

Для этого с сайта www.virtualbox.org скачиваем программу VirtualBox* для вашей операционной системы. Внимание во время установки VirtualBox сетевые интерфейсы будут перезапущены (на время отключены).

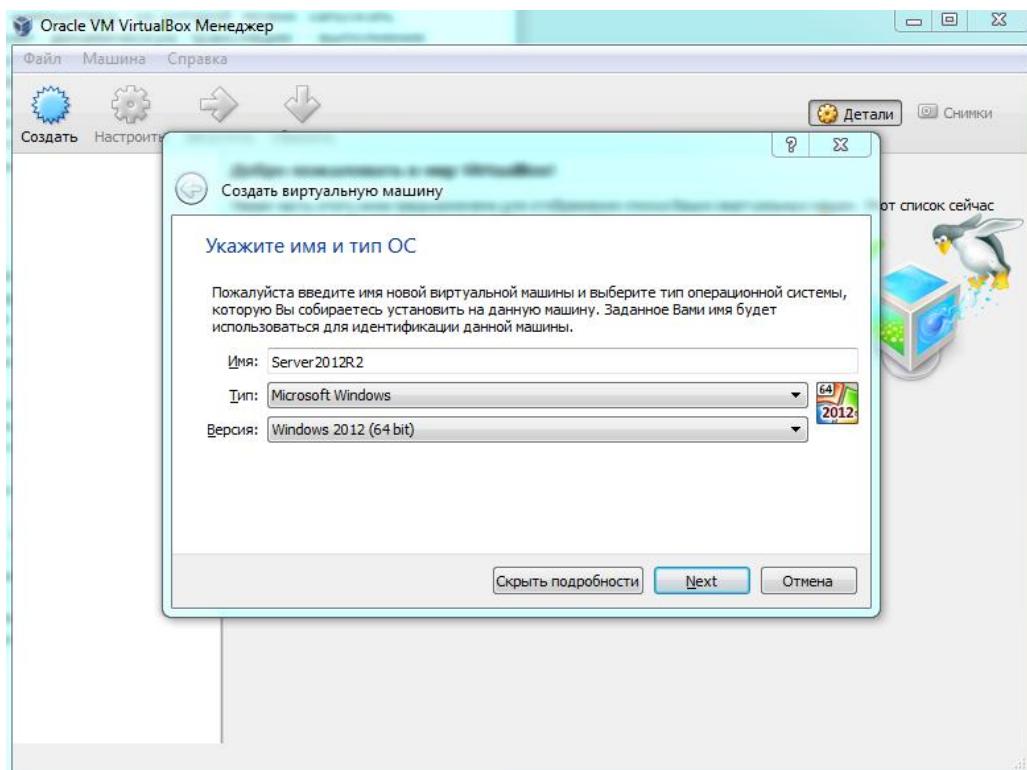
*VirtualBox - система виртуализации, предназначенная для создания виртуальной машины с параметрами железа реального компьютера, на которой можно запускать любую операционную систему. Поддерживает динамическую трансляцию - выполнение большей части инструкций гостевой ОС производится на реальном оборудовании. В роли гостевой системы могут выступать Windows, GNU/Linux, BSD, Solaris и другие операционные системы. Отличается высокой производительностью и стабильностью. Имеет ярко

выраженную модульную архитектуру с хорошо описанными компонентами и предоставляет удобные интерфейсы доступа к виртуальным машинам, которые позволяют контролировать гостевые системы как через GUI, так и через командную строку и удаленно.

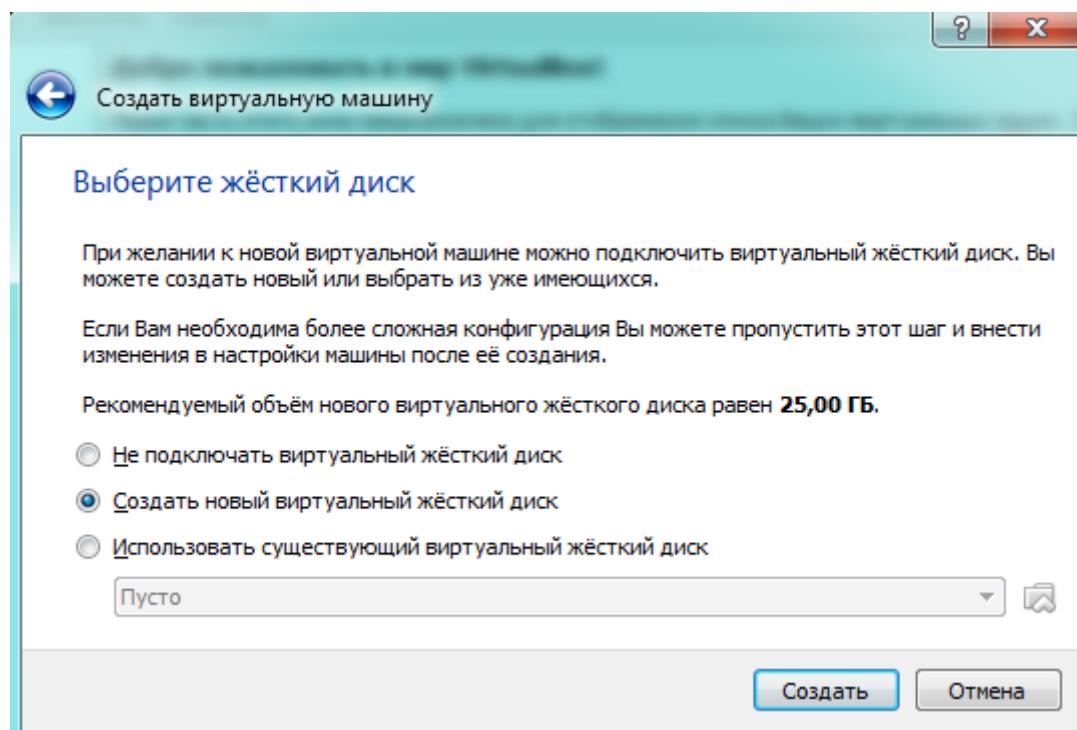
2.2 Создаём виртуальную машину «Server2012R2»

Сервер - программное обеспечение, принимающее запросы от клиентов или компьютер (или специальное компьютерное оборудование), выделенный и/или специализированный для выполнения определенных сервисных функций.

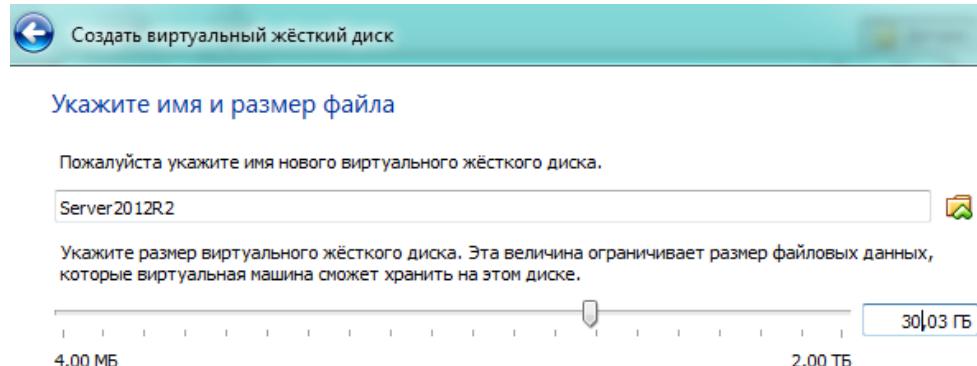
Windows Server 2012 R2 - версия серверной операционной системы от Microsoft. Принаследует семейству ОС Microsoft Windows. Привносит в вашу инфраструктуру опыт Microsoft в области создания и предоставления глобальных облачных сервисов и содержащие новые возможности и улучшения для виртуализации, управления, хранения, работы с сетями, инфраструктуры виртуальных рабочих столов, защиты доступа и информации, веб-платформы и платформы приложений, а также многих других компонентов.



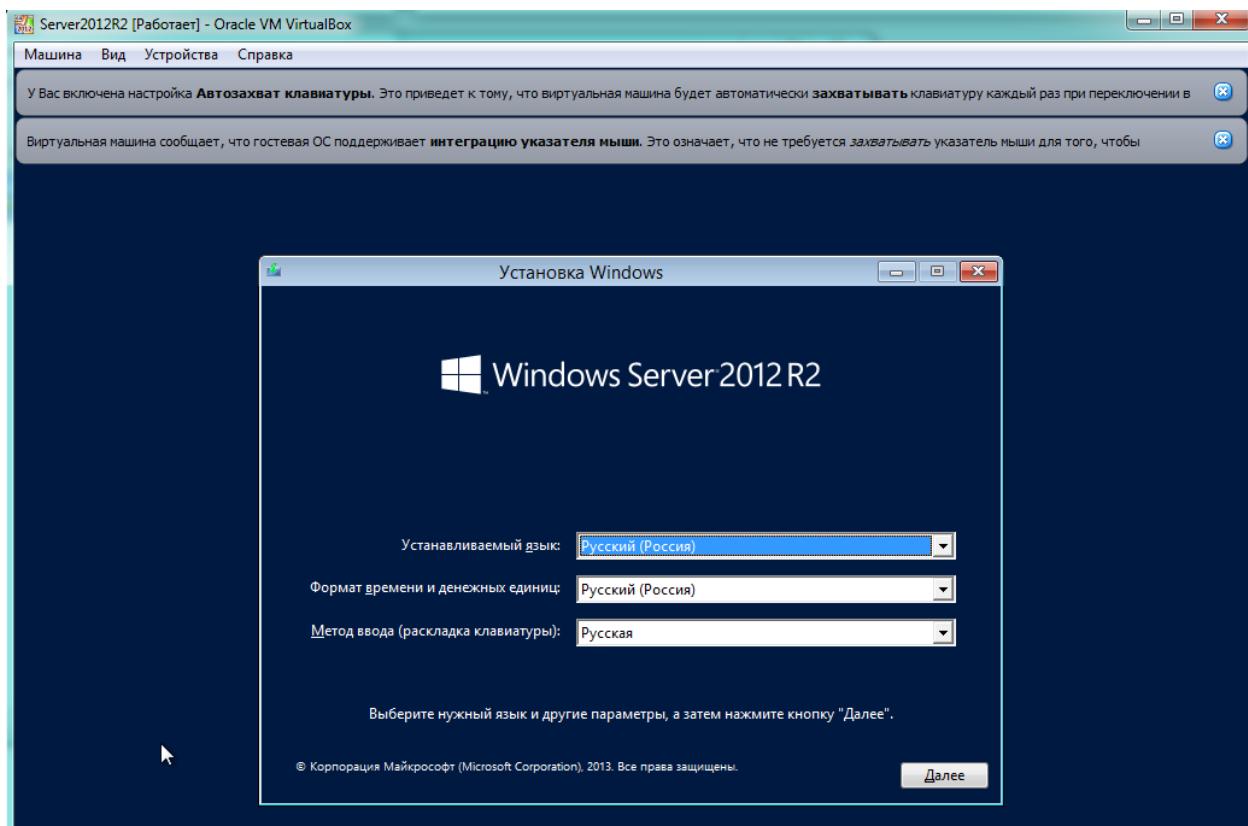
Исходя из конфигурации и объема оперативной памяти вашего компьютера, выделяем для виртуальной машины достаточное количество ОЗУ. Рекомендуется не менее 2 ГБ. Далее создаём новый динамический виртуальный диск (VDI).



Для Windows Server 2012 R2 рекомендуется выделить не менее 30 ГБ под виртуальный жёсткий диск.



В процессе запуска виртуальной машины выбрать образ операционной системы Windows Server 2012 R2 и установить её.



В случае появления окна выбора редакции, необходимо выбрать «Windows Server 2012 R2 Standart (сервер с графическим интерфейсом)

[Выберите операционную систему, которую вы хотите установить](#)

Операционная система	Архитектура	Дата из
Windows Server 2012 R2 Standard (установка основных серверных ...	x64	14.11.20
Windows Server 2012 R2 Standard (сервер с графическим интерф...)	x64	14.11.20
Windows Server 2012 R2 Datacenter (установка основных серверны...	x64	14.11.20
Windows Server 2012 R2 Datacenter (сервер с графическим интерф...	x64	14.11.20

Описание:

Этот вариант полезен, когда требуется графический интерфейс пользователя. Например, чтобы обеспечить обратную совместимость приложения, которое невозможно выполнить в среде установки основных серверных компонентов. При этом поддерживаются все роли и компоненты сервера. Позднее вы можете перейти на другой вариант установки. См. раздел «Варианты установки Windows Server».

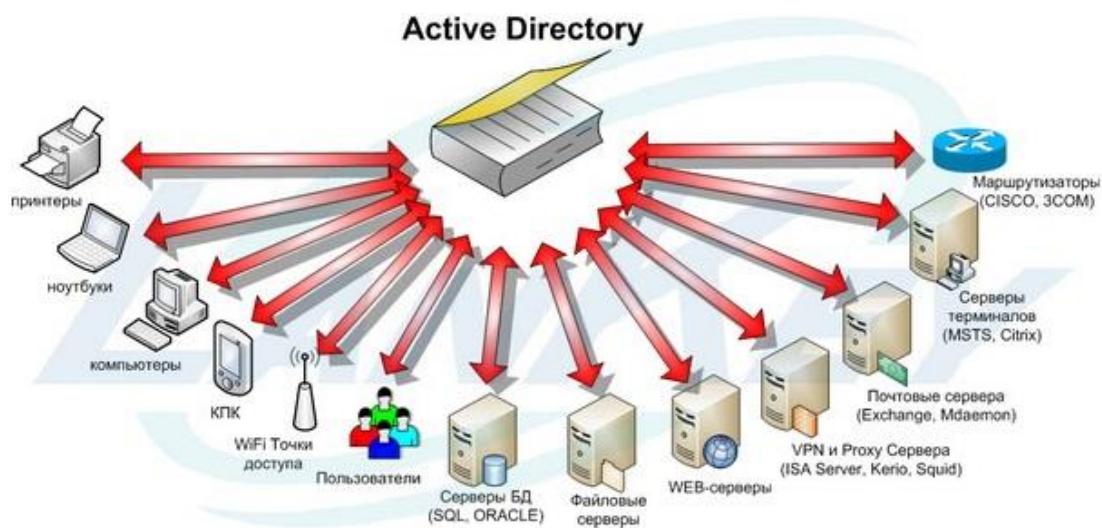
После успешной установки операционной системы, на этапе запуска необходимо будет ввести пароль который должен отвечать требованием сложности, заданным по умолчанию:

- ✓ Иметь длину не менее 6 знаков
- ✓ Содержать знаки из четырёх категорий (латинские строчные буквы, латинские заглавные буквы, цифры).

В качестве пароля можно ввести, например, «Password11111».

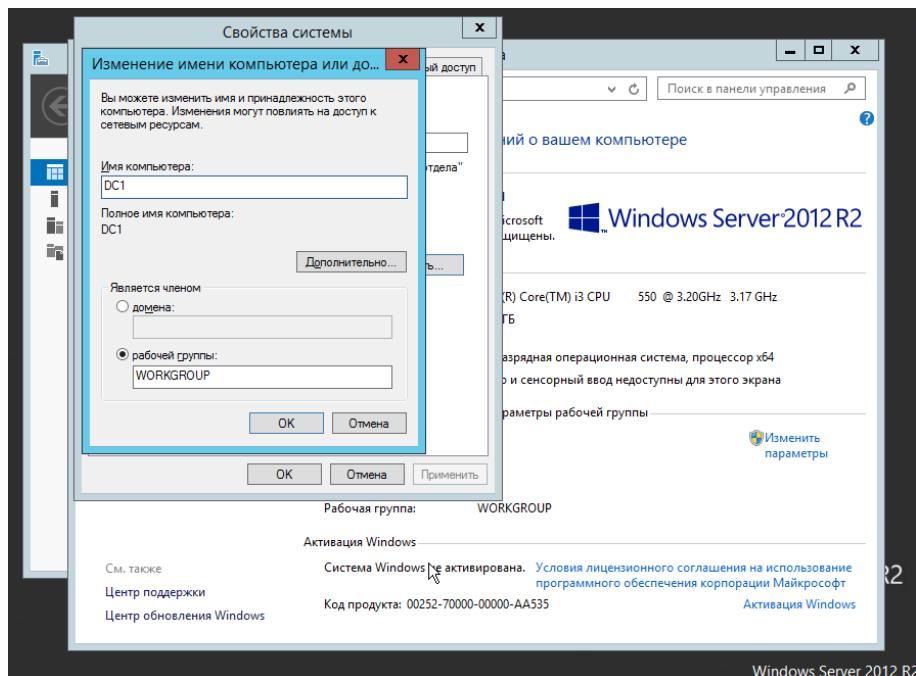
2.3 Подготовка

Active Directory — это иерархически организованное хранилище данных об объектах сети, обеспечивающее удобные средства для поиска и использования этих данных. Компьютер, на котором работает Active Directory, называется контроллером домена. С Active Directory связаны практически все административные задачи. Имеет иерархическую структуру, она способна поддерживать несколько ведущих узлов и вмещать миллионы объектов. Поддержка нескольких ведущих узлов позволяет изменять базу данных с любого контроллера домена в пределах предприятия вне зависимости от состояния его подключения к сети.



Прежде, чем настраивать роль Active Directory необходимо произвести настройку Windows Server 2012 R2 — задать статический IP адрес и переименовать компьютер.

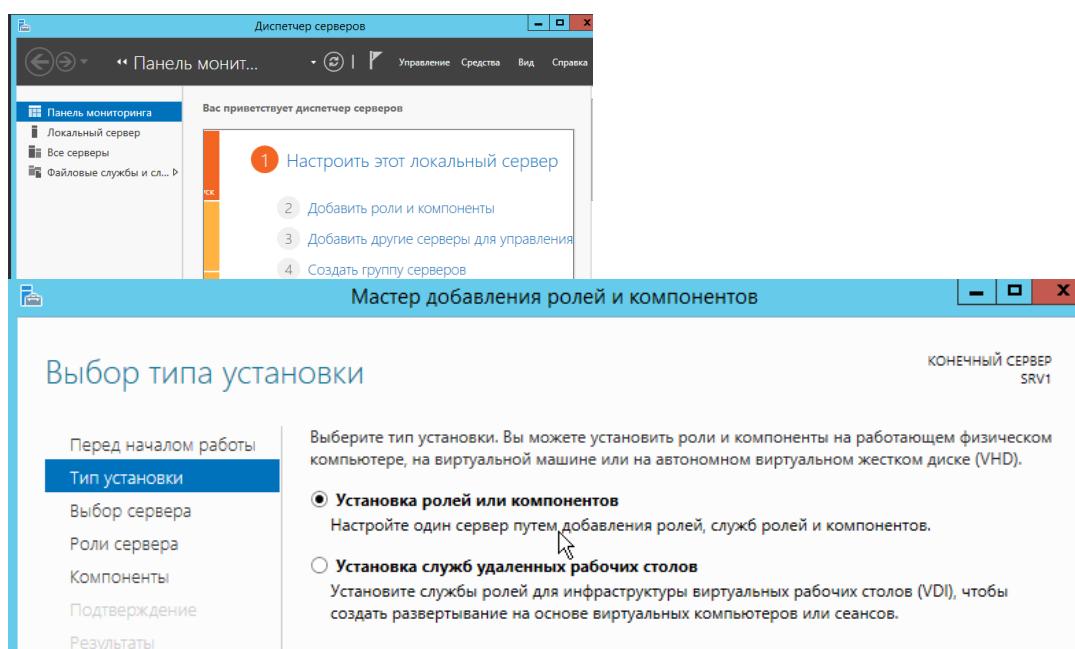
Зададим имя нашему серверу – «DC1», для этого зайдём в настройки системы и изменим имя компьютера по умолчанию на нужное нам.

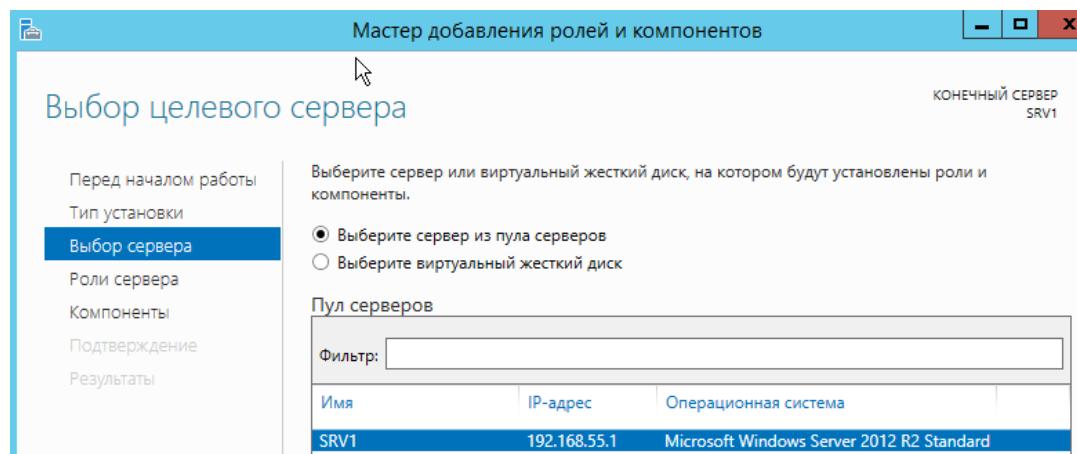


3) Сделать сервер контроллером домена

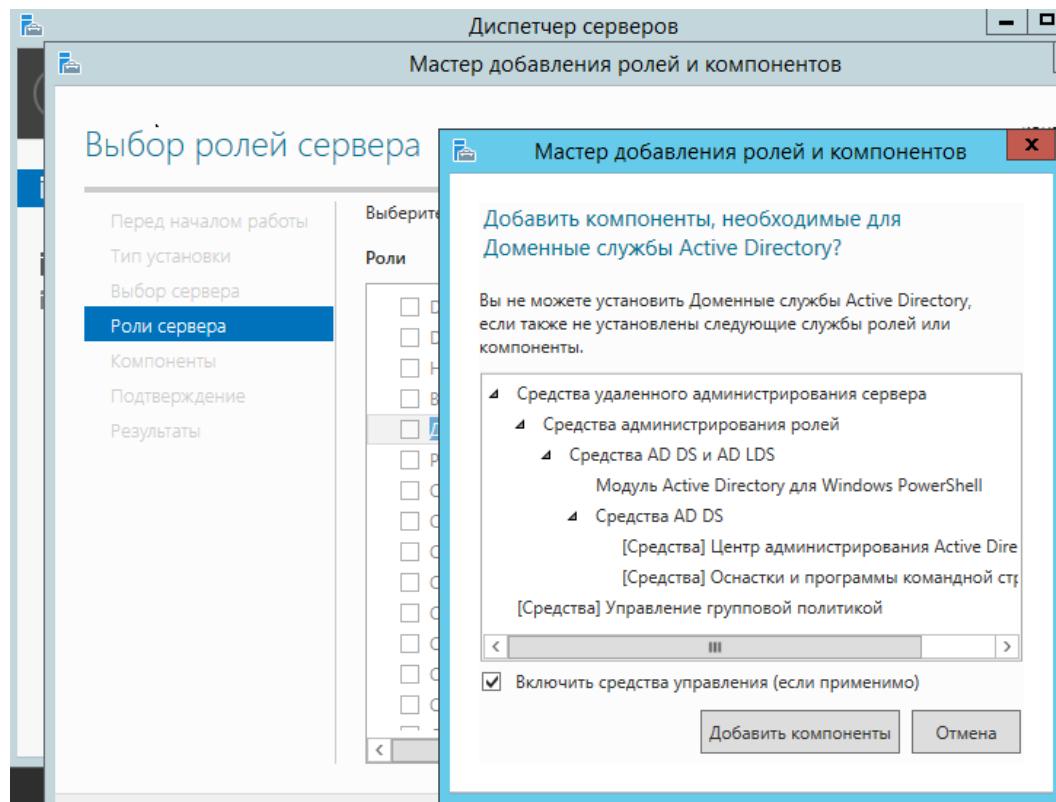
Контроллер домена в компьютерных сетях - сервер, контролирующий область компьютерной сети (домен). Запускает службы Active Directory. Контроллеры домена, работающие под управлением Windows Server, хранят данные каталога и управляют взаимодействиями пользователя и домена, включая процессы входа пользователя в систему, проверку подлинности и поиски в каталоге.

Далее нам необходимо сделать наш сервер контроллером домена. Для этого зайдём в диспетчер серверов и добавим необходимые роли и компоненты.



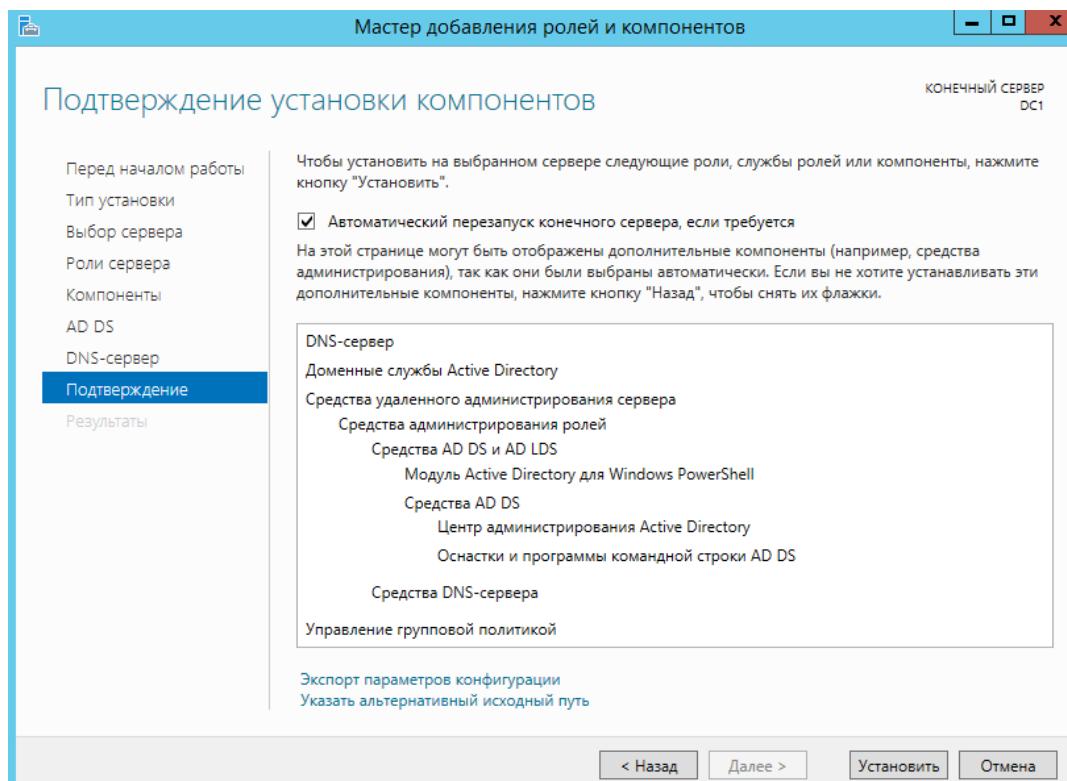


Выбираем роль «Доменные службы Active Directory», после чего появляется окно с предложением добавить роли и компоненты, необходимые для установки роли AD. Нажимаем кнопку «Добавить компоненты».



Так же для контроллера домена необходимо установить роль DNS-сервер. DNS — это протокол разрешения имен для сетей TCP/IP. Клиентские компьютеры запрашивают DNS-сервер, чтобы разрешить запоминающиеся, состоящие из буквенно-цифровых символов имена DNS IP-адресов, которые используются компьютерами для соединения друг с другом.

После выбора необходимых ролей и компонентов жмём каждый раз кнопку «Далее» и устанавливаем.



2.4 Настройка доменных служб Active Directory

Службы Active Directory включают службы сертификатов Active Directory (AD CS), доменные службы Active Directory (AD DS), службы федерации Active Directory (AD FS), службы облегченного доступа к каталогам Active Directory (AD LDS) и службы управления правами Active Directory (AD RMS).

Дополнительные сведения

Active Directory Certificate Services. Службы сертификатов Active Directory позволяют создавать, распространять настраиваемые сертификаты открытых ключей и управлять ими.

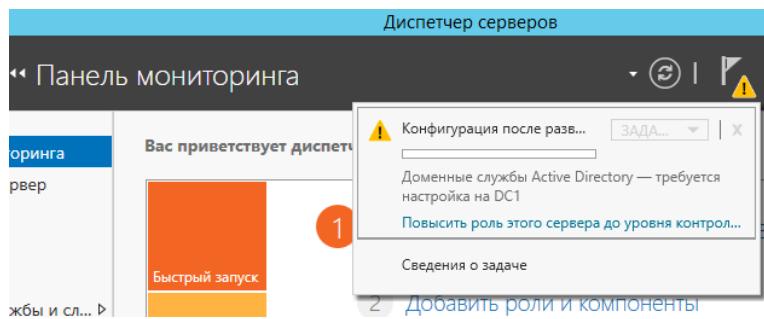
Active Directory Domain Services. Доменные службы Active Directory хранят данные каталогов и управляют связью между пользователями и доменами, в том числе процессами входа пользователей в систему, проверки подлинности и поиска в каталогах.

Active Directory Federation Services. Службы федерации Active Directory обеспечивают технологию единого входа для проверки подлинности пользователя в нескольких веб-приложениях в течение существования одного интерактивного сеанса.

Active Directory Lightweight Directory Services. Службы Active Directory облегченного доступа к каталогам — это служба каталогов протокола LDAP, которая обеспечивает гибкую поддержку приложений, работающих с каталогами, и не имеет ограничений, свойственных доменным службам Active Directory.

Active Directory Rights Management Services. Службы управления правами Active Directory — это средство обеспечения безопасности данных, которое облегчает защиту цифровых данных от несанкционированного использования в приложениях, поддерживающих эту службу.

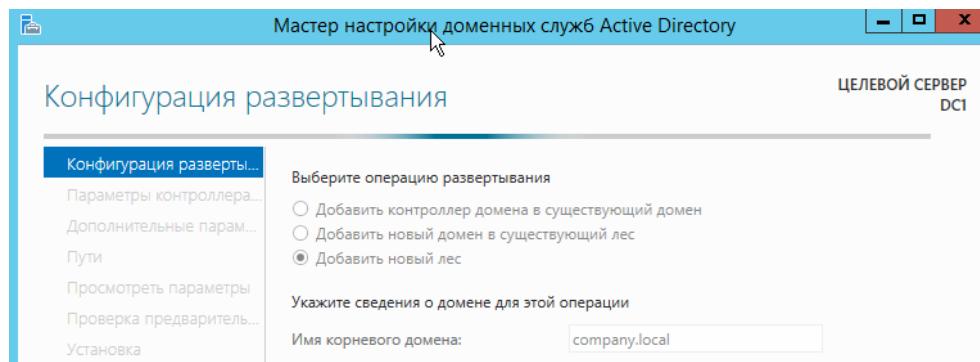
После установки роли, закрыть окно. Теперь необходимо перейти к настройке роли AD. В окне «Диспетчер серверов» нажать пиктограмму флага с уведомлением и нажать «Повысить роль этого сервера до уровня контроллера домена».



Выбрать «Добавить новый лес», ввести название домена (например company.local) и нажать Далее.

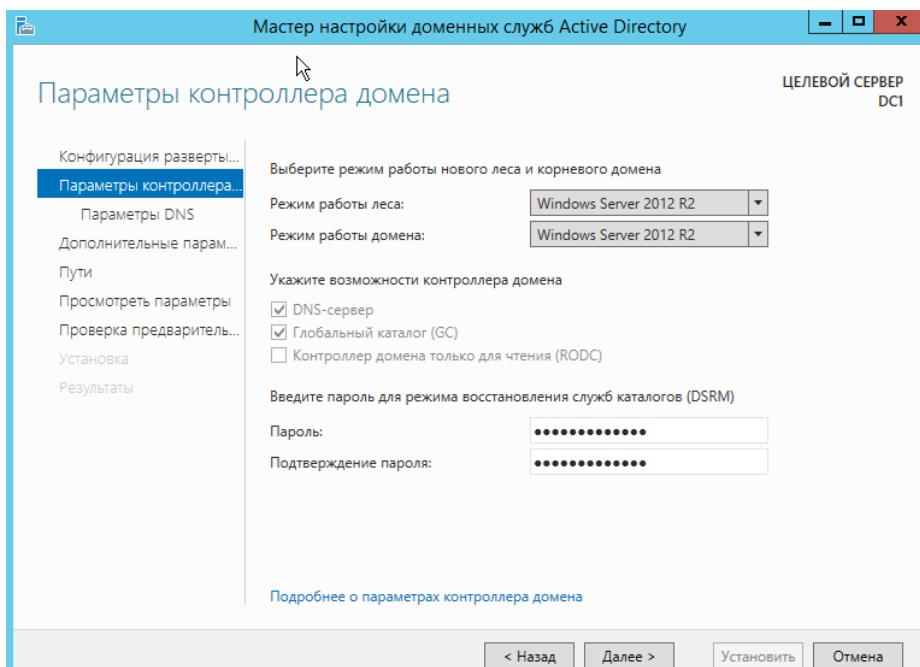
Внимание, если Вы планируете в работе использовать домен в интрасети рекомендуется использовать домен «local» а не «ги», «сом» и так далее, это позволит избежать ряд проблем в процессе эксплуатации и дальнейшей настройки сервера.

Нажимаем далее.



Далее необходимо установить нужный режим работы леса и ввести пароль для DSRM Режим восстановления службы каталогов (DSRM) и нажимаем Далее.

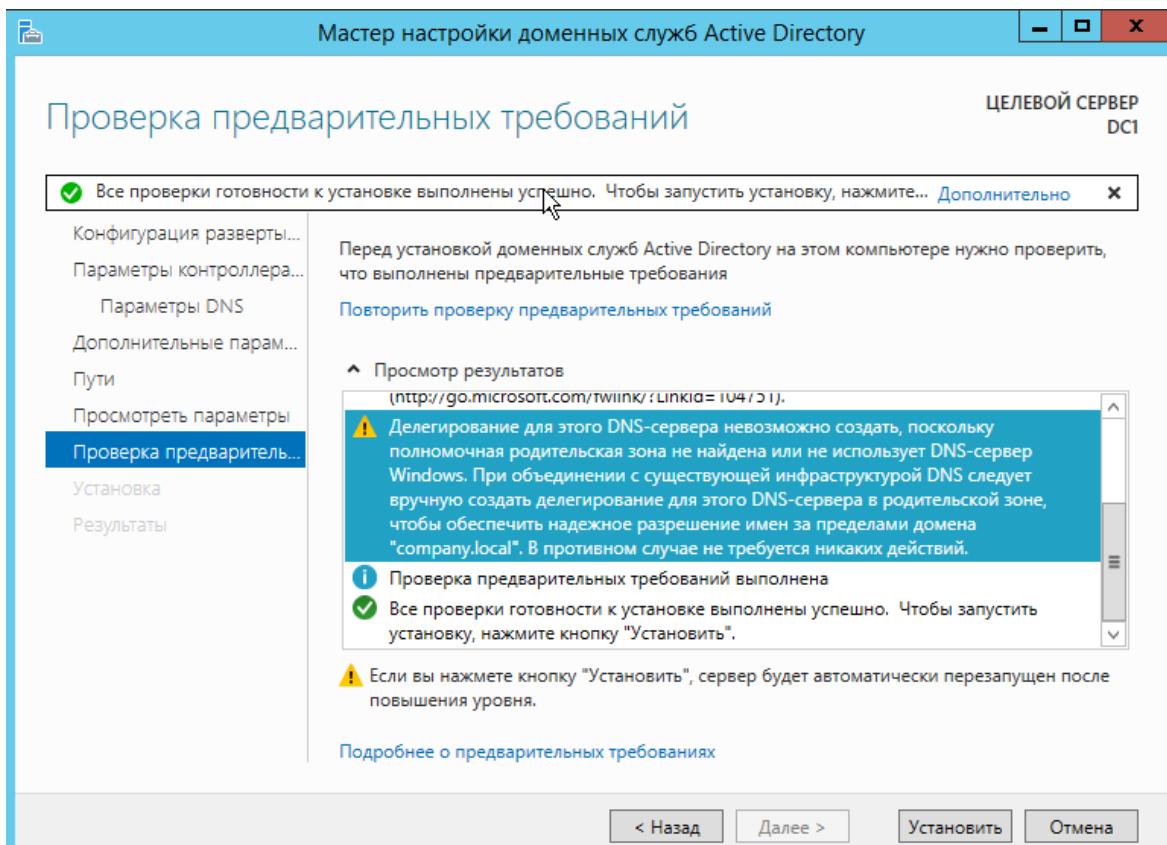
Режим восстановления службы каталогов - помогает восстановить службу каталогов Active Directory. Сбросить или восстановить пароль администратора, восстановить удаленный объект Active Directory а также другие операции по восстановлению.



На следующем шаге мастер предупреждает о том, что делегирование для этого DNS-сервера создано не было, нажимаем «Далее».

Остальные параметры оставляем без изменения, как есть.

На шаге «Проверка предварительных требований» внимательно знакомимся с результатом. Вывод из всех проверок и предупреждений должен быть – «Все проверки готовности к установке выполнены успешно». Если всё хорошо, нажимаем «Установить».



После завершения всех настроек, сервер перезагрузится, и вы совершиете первый ввод компьютера в ваш домен COMPANY. Для этого необходимо ввести логин и пароль администратора домена.



Информация в системе сервера так же изменится. Обратите внимание, на то, что появился домен «company.local», а имя сервера изменилось на DC1.company.local
На этом настройка контроллера домен завершена.

2.5 Установить и настроить роль файлового сервера



Роль "Файловые службы и службы хранения" включает технологии, предназначенные для настройки одного или нескольких файловых серверов (и управления ими), занимающих центральное расположение в сети, где можно хранить файлы и использовать их совместно с другими пользователями. Если пользователям требуется доступ к одним и тем же файлам и приложениям или если в организации необходимо централизованное управление файлами и архивированием, то один или несколько серверов следует настроить как файловый сервер, установив роль "Файловые службы и службы хранения" и соответствующие службы роли.

Службы ролей "Файловые службы и службы хранения" и "Службы хранения" установлены в системе по умолчанию, но без дополнительных служб ролей. Эти базовые возможности позволяют использовать диспетчер сервера или Windows PowerShell для управления функциями хранения данных на серверах. Однако для настройки файлового сервера и управления им необходимо использовать мастер добавления ролей и компонентов в диспетчере серверов или командлет Install-WindowsFeatureWindows PowerShell для установки дополнительных служб роли "Файловые службы и службы хранения", описанных в этом разделе.

Практические применения

Администраторы могут использовать роль "Файловые службы и службы хранения" для настройки нескольких файловых серверов и их хранилищ, а также для управления этими серверами, с помощью диспетчера серверов или Windows PowerShell. Некоторые конкретные приложения включают следующие функции.

- Функция "Дедупликация данных" для снижения требований к месту на диске для хранения файлов, экономии средств на хранилище.
- Конечный iSCSI-сервер для создания централизованных, программных и аппаратно-независимых дисковых подсистем iSCSI в сетях хранения данных (SAN).
- Дисковые пространства для развертывания хранилища с высоким уровнем доступности, отказоустойчивого и масштабируемого за счет применения экономичных стандартизованных в отрасли дисков.
- Диспетчер серверов для удаленного управления несколькими файловыми серверами из одного окна.
- Windows PowerShell для автоматизации управления большинством задач администрирования файловых серверов.

Требования к выполнению файловых служб и служб хранения

- Специальные требования к оборудованию или программному обеспечению для файловых служб и служб хранения отсутствуют. Тем не менее диспетчер ресурсов файлового сервера и репликация DFS поддерживают тома, форматированные только в файловой системе NTFS. Системы ReFS и FAT не поддерживаются.
- В последующих разделах рассматриваются общие вопросы, связанные с требованиями файловых служб и служб хранения.

Развертывание и конфигурация роли в многосерверной среде

- Вы можете разделить набор функций файловых служб и служб хранения на нескольких серверах, установив роли и соответствующие службы ролей на каждом сервере. Затем вы можете добавить все серверы в диспетчера серверов для централизованного управления или использовать сценарии Windows PowerShell для одновременного управления несколькими серверами.

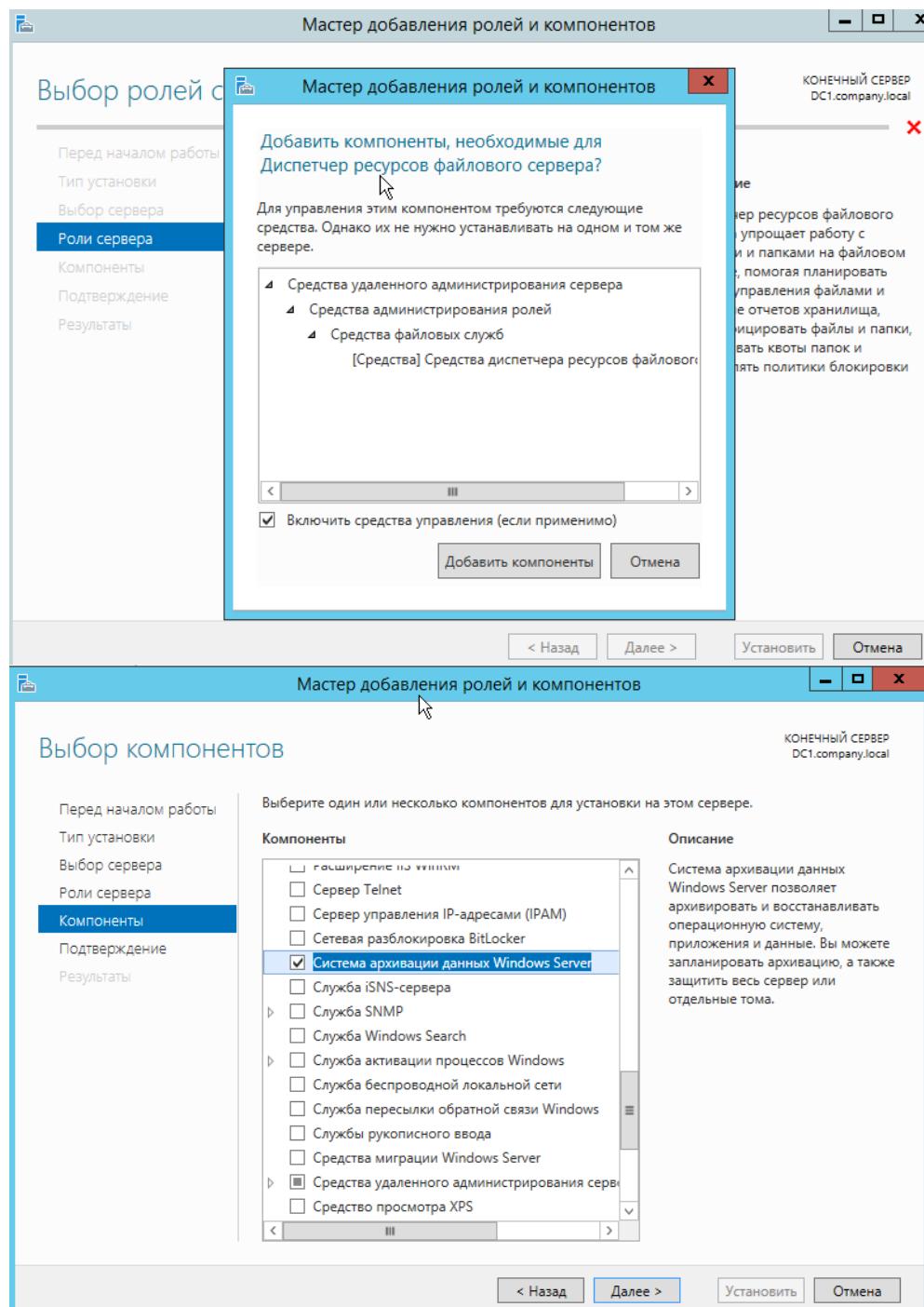
Установка роли файлового сервера (дополнительных компонентов).

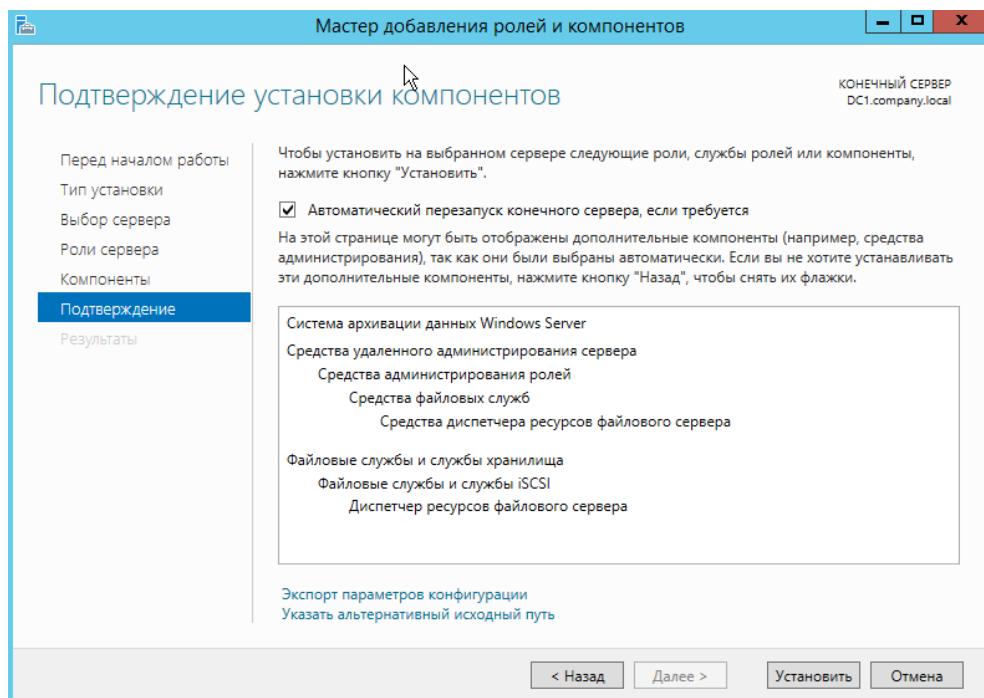
Так как мы используем в качестве файлового сервера тот же сервер - роль «Файловые службы и службы хранения» на нём уже установилась вместе с ролью Active Directory.

Но для управления и настройки общих ресурсов нам понадобится «Средство диспетчера ресурсов файлового сервера», а также для резервного копирования данных компонент «Система архивации данных Windows Server».

Система архивации данных Windows Server - это инструмент Windows Server 2008, предоставляющий набор мастеров и других средств выполнения основных задач резервного копирования и восстановления для сервера, на котором он установлен.

Установка этих средств и компонентов производится из диспетчера серверов с помощью «Мастера добавления ролей и компонентов».





Нажимаем установить и дожидаемся окончания установки.

2.6 Создание организационных подразделений.

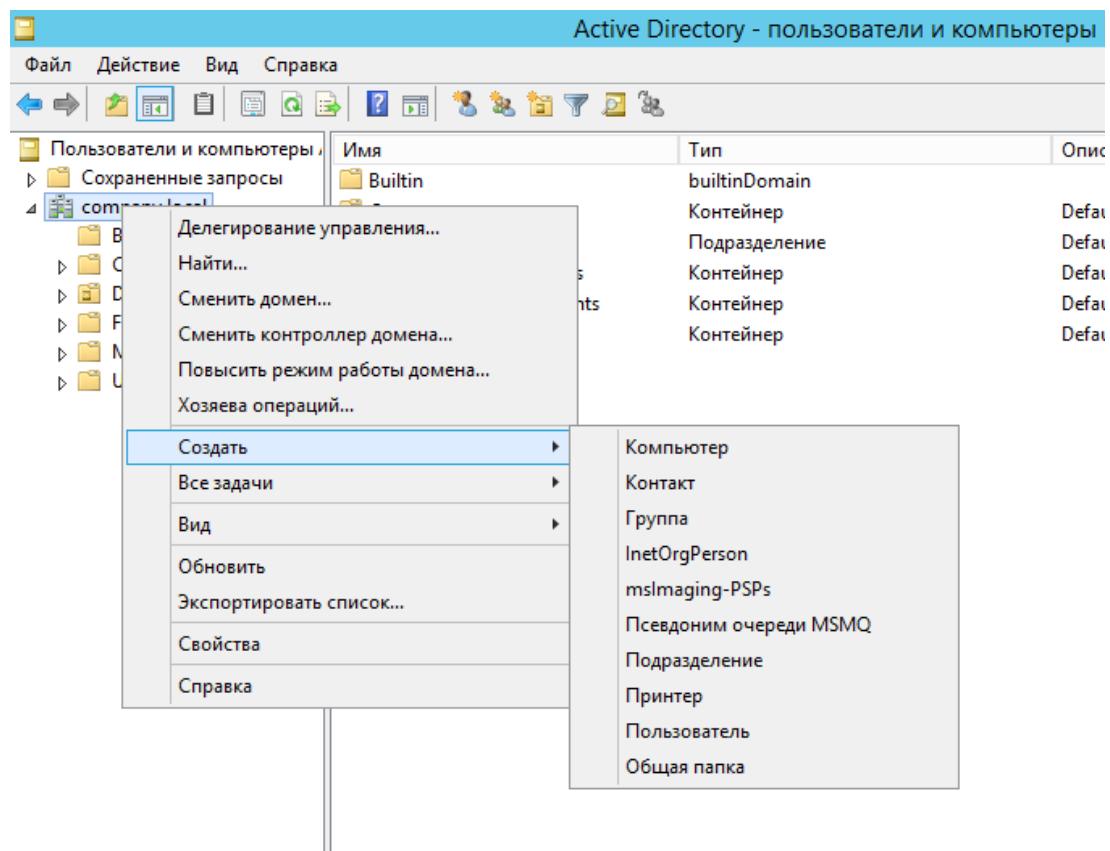
Организационные подразделения (ОП) — это подгруппы в доменах, которые часто отражают функциональную структуру организации. ОП представляют собой своего рода логические контейнеры, в которых размещаются учетные записи, общие ресурсы и другие ОП. Например, можно создать в домене microsoft.com подразделения Resources, IT, Marketing. Потом эту схему можно расширить, чтобы она содержала дочерние подразделения.

В ОП разрешается помещать объекты только из родительского домена. Например, ОП из домена Seattle.microsoft.com содержат объекты только этого домена. Добавлять туда объекты из tu.microsoft.com нельзя. ОП очень удобны при формировании функциональной или бизнес - структуры организации. Но это не единственная причина их применения.

ОП позволяют определять групповую политику для небольшого набора ресурсов в домене, не применяя ее ко всему домену. С помощью ОП создаются компактные и более управляемые представления объектов каталога в домене, что помогает эффективнее управлять ресурсами.

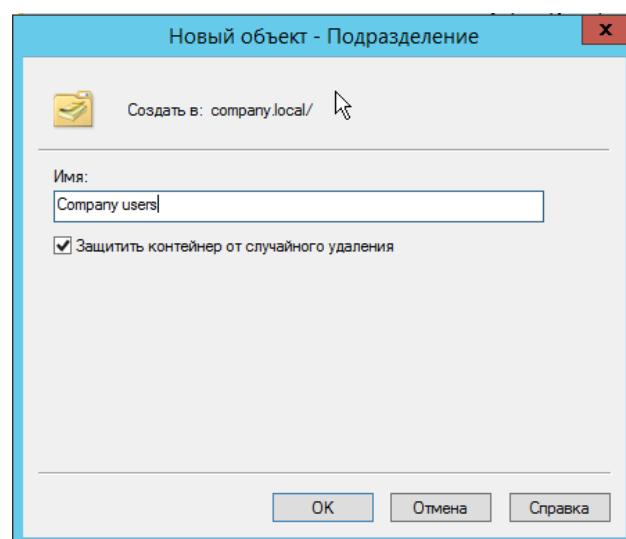
ОП позволяют делегировать полномочия и контролировать административный доступ к ресурсам домена, что помогает задавать пределы полномочий администраторов в домене. Можно передать пользователю А административные полномочия только для одного ОП и в то же время передать пользователю В административные полномочия для всех ОП в домене.

Для того, что бы создать подразделение необходимо зайти в оснастку «Active Directory Пользователи и компьютеры». Выбрать наш домен, далее через меню правой кнопки мыши выбрать «Создать» → «Подразделение»



Создадим подразделение «Company users».

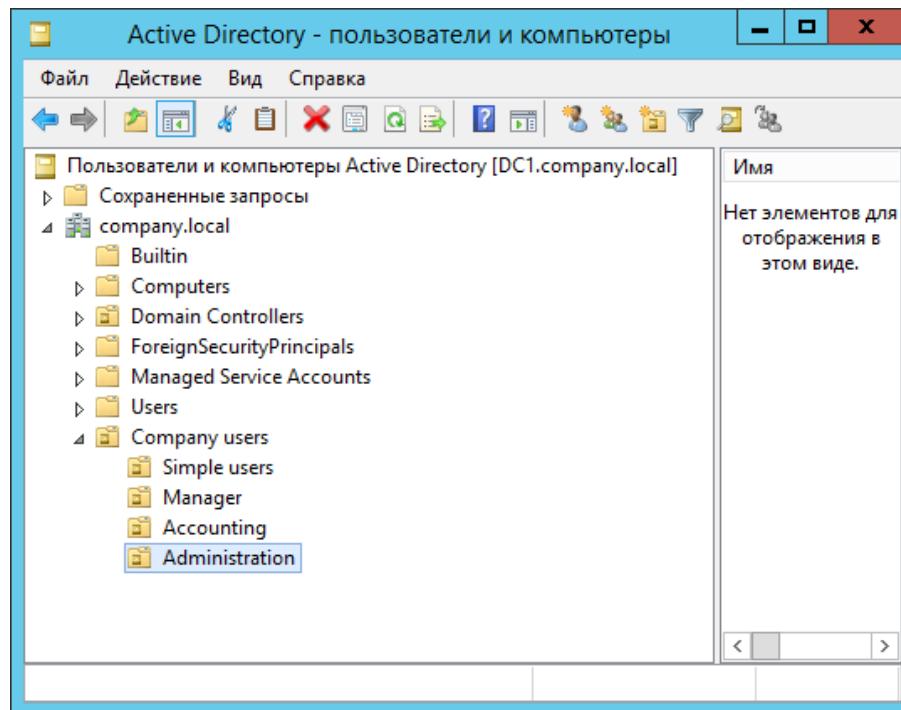
Примечание: Наименование подразделений можно делать и на кириллице, но всё-таки рекомендуется использовать латинские буквы в наименовании объектов Active Directory.



Внутри нашего основного организационного подразделения создадим другие подразделения

- Simple user (простые пользователи)
- Manager (менеджеры)
- Accounting (бухгалтерия)

- Administration (администрация)

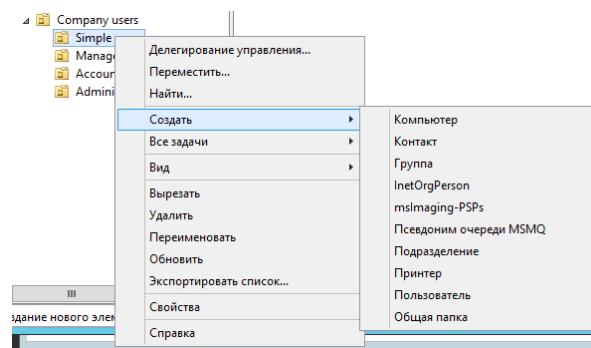


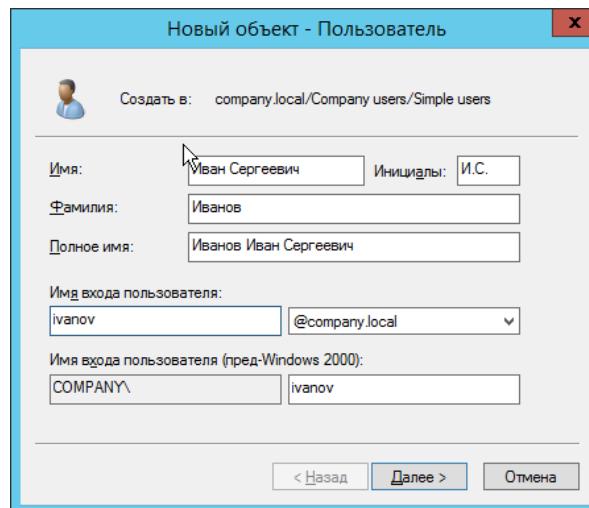
2.7 Создание пользователей домена в соответствующих подразделениях

Создать пользователей домена в соответствующих подразделениях (3-5)

- ivanov (Иван Сергеевич), обычный пользователь
- petrov (Петров Евлампий Сидорович), менеджер
- pilula (Пилюля Федр Бедросович), менеджер
- jigurga (Никита Жигурда), бухгалтер
- Alisa (Федюшкина Алиса Викторовна), бухгалтер
- boss (Путин Владимир Геннадьевич), администрация
- medved (Медведев Дмитрий Геннадьевич), администрации

Создание пользователей можно создать из той же оснастки «Active Directory Пользователи и компьютеры» через меню правой кнопки мыши



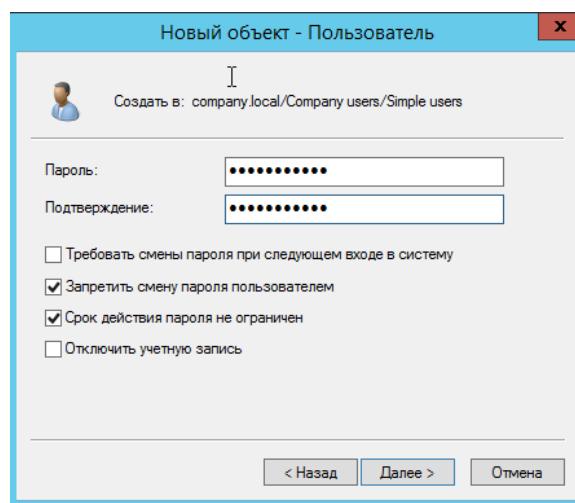


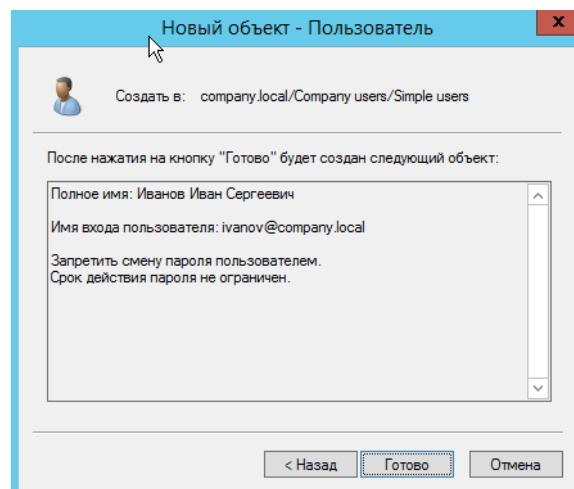
Назначим пользователю Ivanov пароль, например «asQW!@12». Тут же запретим смену пароля и выставим срок службы пароля без ограничений.

Примечание:

Пароль не может содержать имя учетной записи пользователя или какую-либо его часть. Пароль должен состоять не менее чем из шести символов. В пароле должны присутствовать символы трех категорий из числа следующих четырех:

- *прописные буквы английского алфавита от A до Z;*
- *строчные буквы английского алфавита от a до z;*
- *десятичные цифры (от 0 до 9);*
- *неалфавитные символы (например, !, \$, #, %)*





В операционных системах нового поколения, начиная с windows server 2012 появилась новая оснастка работы и навигации по задачам и объектам Active Directory – «Центр администрирования Active Directory».

Оснастка "Центр администрирования Active Directory" основывается на технологии командной строки Windows PowerShell™. Она обеспечивает улучшенное управление данными Active Directory и богатые возможности графического пользовательского интерфейса.

Оснастку "Центр администрирования Active Directory" можно использовать для выполнения типовых задач управления объектами Active Directory как с помощью переходов на основе данных, так и с помощью переходов, ориентированных на задачи.

- Управление пользователями
- Управление группами
- Управление компьютерами
- Управление доменами и контроллерами домена
- Управление подразделениями
- Нахождение объектов Active Directory в оснастке "Центр администрирования Active Directory"
- Пользовательский интерфейс: центр администрирования Active Directory

Создадим ещё одного пользователя (Федюшкина Алина Викторовна) используя данную оснастку.

The screenshot shows the 'Centre d'administration Active Directory' window. In the center, there is a table titled 'Company users (4)' with columns 'Полное имя' (Full name), 'Тип' (Type), and 'Описание' (Description). A context menu is open over the first row, which includes options like 'Создать' (Create), 'Удалить' (Delete), 'Переместить...' (Move), 'Искать в этом узле' (Search in this node), and 'Свойства' (Properties). On the left, a navigation pane shows 'company (локальный)' and various sub-options like 'Company users', 'System', and 'Dynamic Site...'. Below the table, a search bar says 'Создать Пользователь: Федюшкина Алиса Викторовна'.

Создать Пользователь: Федюшкина Алиса Викторовна

Учетная запись

Имя: Алиса Викторовна
Отчество: А.В.
Фамилия: Федюшкина
Полное имя: * Федюшкина Алиса Викторовна
Вход пользователя (UPN): alisa @ company.local
Вход пользователя (Sam... company * alisa
Пароль: *****
Подтверждение пароля: *****
Создать в: OU=Accounting,OU=Company users,DC=company,DC=local
Изменить...
Задача от случайного удаления
Время входа в систему... Вход в...

Срок действия учетной з Никогда Конец

Параметры пароля:
 Требовать смены пароля при следующем входе в систему
 Другие параметры пароля
 Для интерактивного входа в сеть нужна смарт-карта
 Срок действия пароля не ограничен
 Запретить смену пароля пользователем

Параметры шифрования:
Другие параметры:

Организация

Отображаемое имя: Федюшкина Алиса Викторовна
Комната: Бухгалтерия
Эл. почта: alisa@company.mail
Веб-страница: Другие веб-страницы...
Должность: Бухгалтер
Отдел: Бухгалтерия
Организация:
Менеджер: Изменить... Очистить
Подчиненные:

Создадим остальных пользователей любым из приведённых ранее методов.

2.8 Создание групп безопасности пользователей.

В Active Directory существуют два типа групп: группы распространения и группы безопасности. Группы распространения могут быть использованы для создания списков рассылки электронной почты, а группы безопасности — для задания разрешений на использование общих ресурсов.

Группы распространения

Группы распространения используются только приложениями электронной почты (например, Exchange) для отправки сообщений электронной почты группам пользователей. Группы распространения не используют систему безопасности, иначе говоря, они не могут быть включены в избирательные таблицы управления доступом (DACL). Если группа создается для контроля доступа к общим ресурсам, эта группа должна быть группой безопасности.

Группы безопасности

При осторожном использовании группы безопасности обеспечивают эффективное управление доступом к ресурсам сети. Использование групп безопасности позволяет выполнять следующие действия.

- **Назначать права пользователя группе безопасности в Active Directory.**

Права пользователя, заданные для групп безопасности, определяют, что может делать член данной группы в области действий домена (или леса). Права пользователя автоматически задаются для групп безопасности во время установки Active Directory для помощи администраторам в определении роли административных пользователей в домене. Например, пользователь, добавленный в группу «Операторы архива» в Active Directory, получает возможность создавать архивы и восстанавливать файлы и каталоги на любом контроллере домена в домене.

Это происходит потому, что по умолчанию права пользователя [Архивирование файлов и каталогов](#) и [Восстановление файлов и каталогов](#) автоматически задаются для группы «Операторы архива». Члены этой группы наследуют права пользователя, заданные для всей группы. Дополнительные сведения о правах пользователей см. в разделе [Права пользователей](#). Дополнительные сведения о правах пользователей, заданных для групп безопасности, см. в разделе [Группы по умолчанию](#).

Можно задать права пользователей группе безопасности, используя групповую политику, для делегирования конкретных задач. При задании делегированных задач необходимо соблюдать осторожность. Неопытный пользователь, наделенный слишком большими правами в группе безопасности, потенциально может нанести серьезный урон сети. Дополнительные сведения см. в разделе [Делегирование администрации](#). Дополнительные сведения о задании прав пользователей в группах см. в разделе [Назначение прав пользователя группе в службе каталогов Active Directory](#).

- **Назначать разрешения на использование ресурсов для групп безопасности.**

Не следует путать разрешения с правами пользователей. Разрешения задаются для групп безопасности, использующих общие ресурсы. Разрешения определяют, кто может получить доступ к данному ресурсу и уровень доступа, например полный доступ. Некоторые разрешения, установленные для объектов домена, автоматически задаются для различных уровней доступа группам по умолчанию, таким как «Операторы учета» или «Операторы домена». Дополнительные сведения о разрешениях см. в разделе [Управление доступом в Active Directory](#).

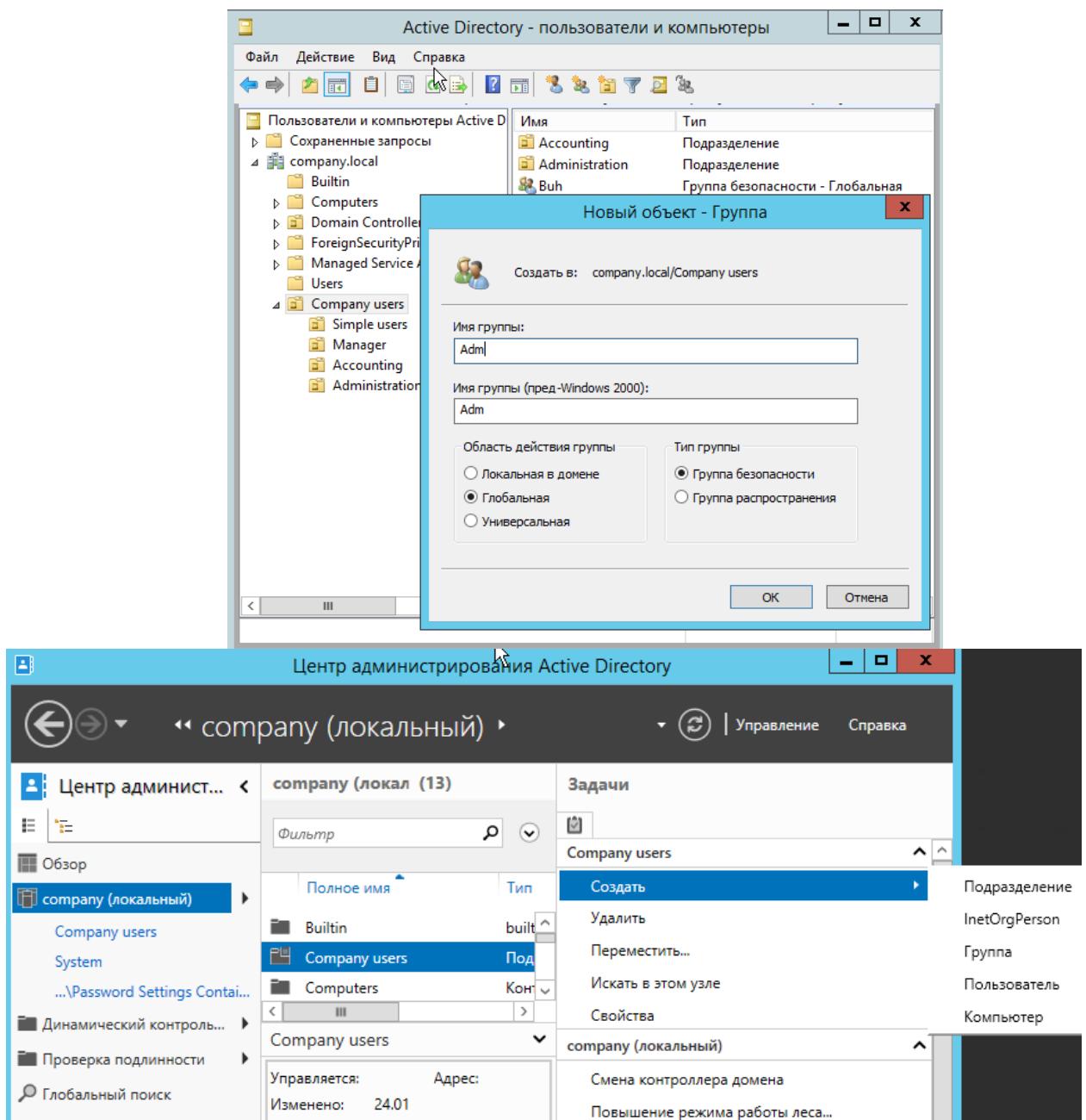
Группы безопасности перечислены в избирательных таблицах управления доступом, которые определяют разрешения на ресурсы и объекты. Администраторам следует назначать разрешения для ресурсов (общих файлов, принтеров, и т. д.) группам безопасности, а не отдельным пользователям. Разрешения назначаются группе один раз, вместо назначения прав каждому отдельному пользователю. Каждая учетная запись при добавлении к группе получает права, заданные данной группе в Active Directory, и разрешения, определенные для данной группы на ресурсе.

Группы безопасности могут использоваться в качестве адресатов электронной почты, как и группы распространения. Сообщение электронной почты, отправленное группе, отправляется всем членам группы.

Так как мы в дальнейшем будем использовать созданные нами группы для разграничения доступа к общим ресурсам, то нам необходимо использовать глобальную группу безопасности.

Создадим несколько необходимые группы в подразделении «Company users» через оснастку "Центр администрирования Active Directory" или «Active Directory Пользователи и компьютеры»

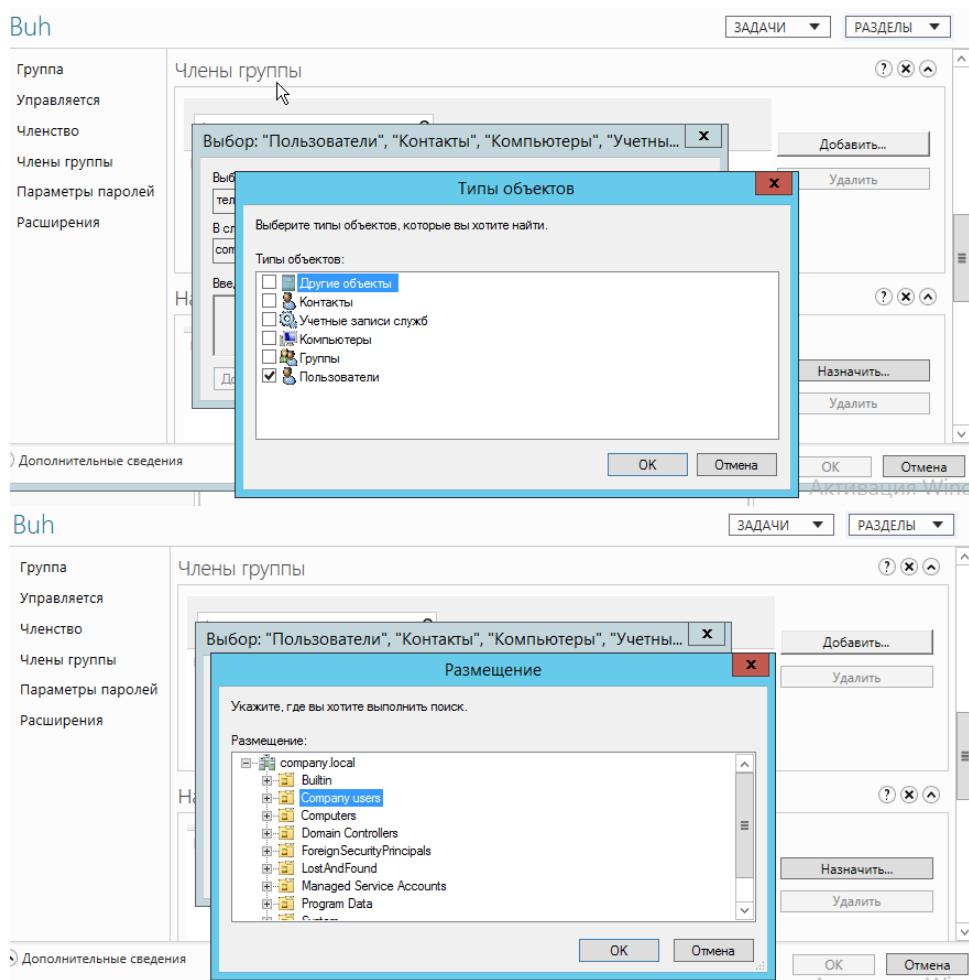
- Buhi (Бухгалтерия)
- Adm (Администрация)
- Man (менеджеры)

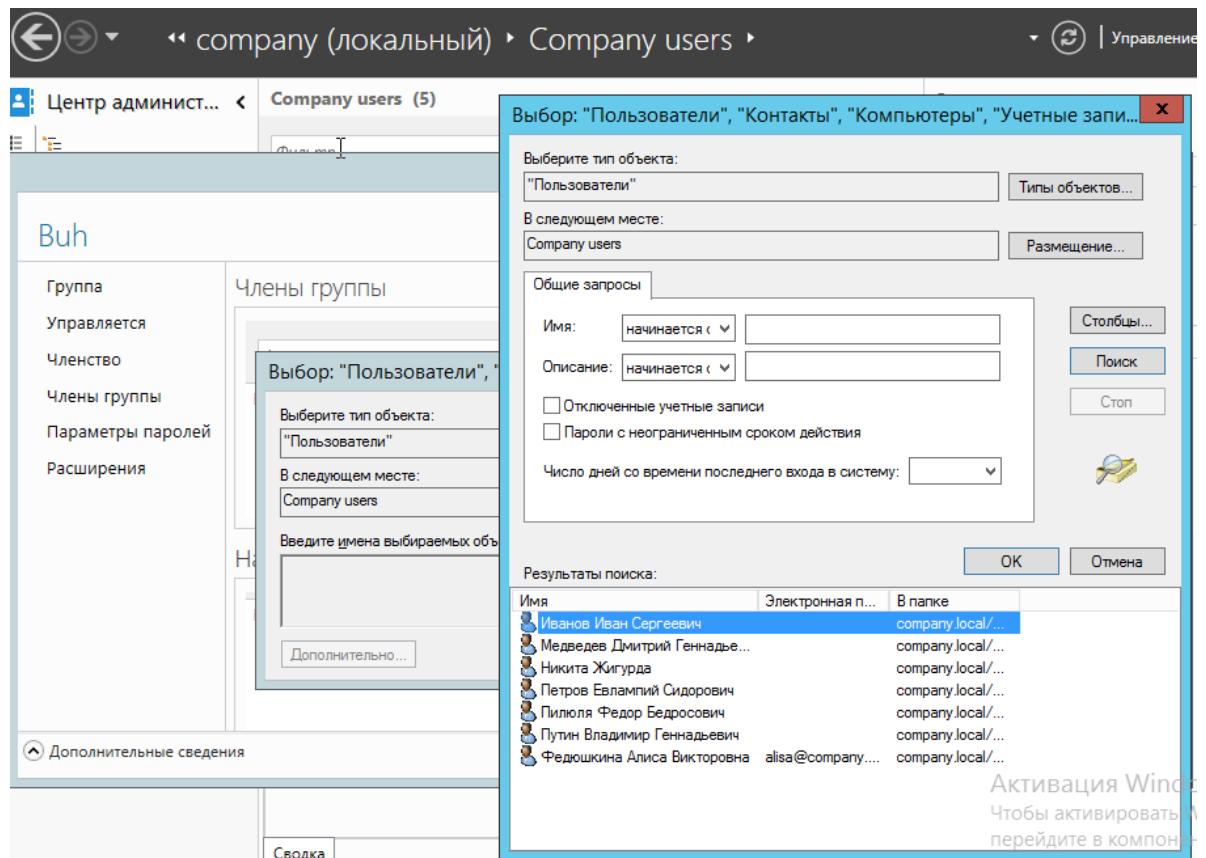


2.9 Распределим пользователей по группам безопасности

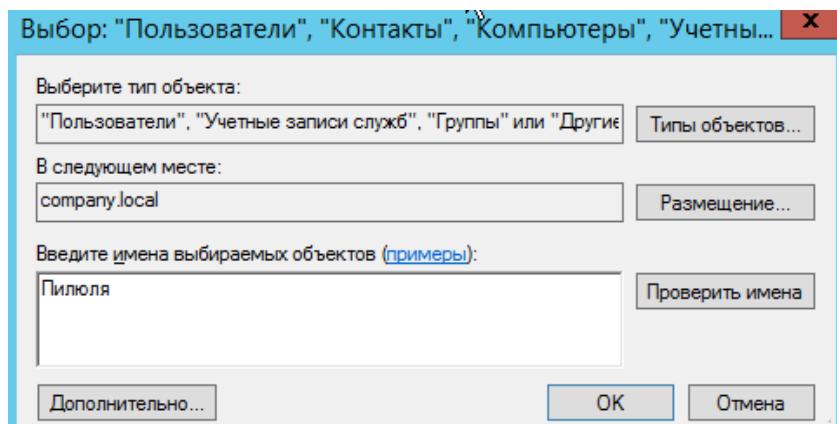
В соответствии с должностями и наименованием подразделение распределим пользователей по группам в любой. Это действие так же можно сделать из знакомых нам оснасток.

Для быстрого поиска нужных пользователей необходимо настроить фильтр поиска. Для этого в «Типы объектов» необходимо выбрать «Пользователи», а в «Размещение» указать ваше подразделение «Company users». После чего нажав на кнопку «Дополнительно» → «Поиск», отобразятся все Ваши пользователи из которых можно выбрать необходимых и добавить в группу.





Для более быстрого добавления пользователей в группу достаточно просто ввести первые буквы фамилии пользователя или фамилию целиком.



ЛАБОРАТОРНАЯ РАБОТА №2 АДМИНИСТРИРОВАНИЕ WINDOWS SERVER 2012 R2. ЧАСТЬ 2

1. Цель работы

- 1) Создать и открыть для общего доступа несколько папок пользователей
 - Doc - Документы (содержит папки с документами всех пользователей домена)
 - Unit - Подразделения (содержит папки каждого из подразделений)

Folder_unit(buh) – общая папка бухгалтерии компании

Folder_unit(Managers) – общая папка менеджеров компании

Folder_unit(Adm) – общая папка администрации

- Exchange Обмен (папка с полным доступом для всех)

На уровне прав NTFS разграничить доступ к папкам пользователей используя группы безопасности.

- 2) Назначить права доступа созданным ранее пользователям домена к подпапкам (Администрация, Бухгалтерия, Менеджеры) директории «Unit» согласно их должности. Пользователю Путин Владимир Геннадьевич дать полные права к папке «Unet», а также всем её подпапкам.

- 3) Установить и настроить DFS с помощью среды PowerShell

- Подключить через DFS папки общего доступа

- 4) С помощью групповых политик (GPO) реализовать:

- Перемещаемые профили (Перенаправление папки «Мои документы» и «Рабочий стол»)
- Подключить всем пользователям домена сетевой диск «P» (Public, он же «Общий ресурс компании») ссылающийся на пространство имён DFS созданный ранее.

- 5) Установить в виртуальную среду (VirtualBox) Windows 7.

- Ввести компьютер в домен

- Проверить работу политик

- Проверить работу папок общего доступа

2. Общие сведения

2.1 Создание и открытие для общего доступа папок пользователей. Разграничение на уровне прав NTFS доступа к папкам пользователей по критериям

Создать и открыть для общего доступа несколько папок пользователей. На уровне прав NTFS разграничить доступ к папкам пользователей по некоторым критериям: чтение и запись, только чтение, только просмотр, доступ запрещён.

- Doc - Документы (перенаправленная папка Мои документы)
- Unit - Подразделения (содержит папки каждого из подразделений)
- Exchange Обмен (папка с полным доступом для всех)

Права доступа в NTFS

NTFS рассматривает каталоги (папки) и файлы как разнотипные объекты и ведет отдельные (хотя и перекрывающиеся) списки прав доступа для каждого типа. Ниже перечислены права NTFS, назначаемые папкам (соответствующие права для файлов приведены ниже):

- *Нет доступа (No Access) (None)(НеT).*
- *Полный доступ (Full Control) (All)(A11) (Все)(Все).*
- *Право чтения (Read) (RX)(RX) (чтение)(чтение).*
- *Право добавления (Add) (WX)(Not Specified) (запись/выполнение^ Не указано).*
- *Право добавления и чтения (Add & Read) (RWX)(RX) (чтение/запись/выполнение)(чтение/выполнение).*
- *Право просмотра (List) (RX)(Not Specified) (чтение/выполнение- ние)(Не указано).*
- *Право изменения (Change) (RWXD)(RWXD) (чтение/запись/ выполнение/удаление) (чтение/запись/выполнение/удаление).*

Обратите внимание на два выражения в скобках, указанные после имени права доступа. Первое выражение относится к самой папке, а второе — ко всем файлам, которые могут быть созданы внутри нее. Например, при полном доступе для папки разрешаются любые действия, однако пользователь с полным доступом к папке также будет обладать полным правом доступа ко всем созданным в ней файлам (если только права доступа к файлу не были изменены его владельцем или администратором). Другими словами, в NTFS файлы и папки по умолчанию наследуют права доступа, установленные для их родительской папки, однако эти права могут быть изменены любым пользователем, которому разрешено изменять права доступа для соответствующих объектов NTFS.

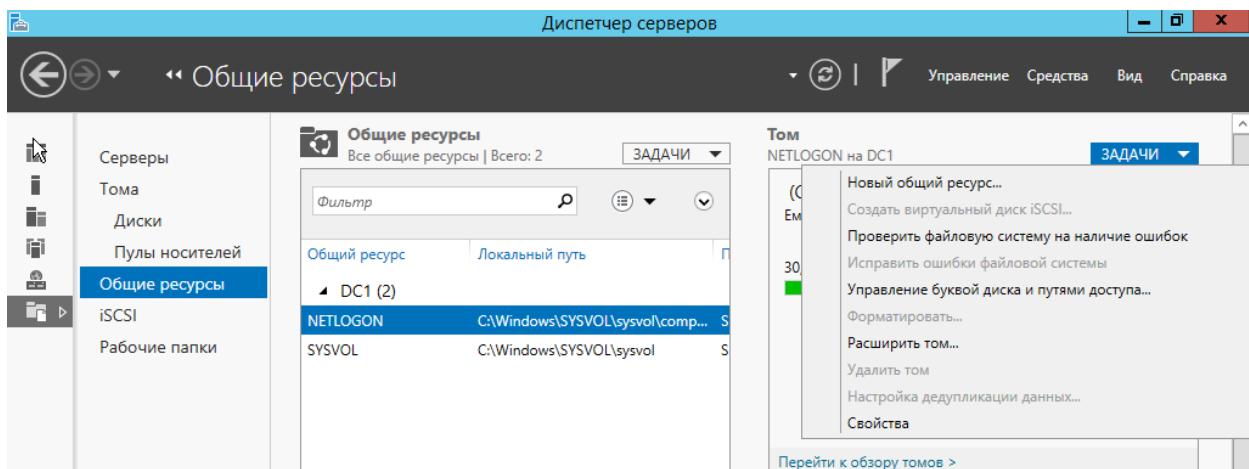
Файлы в NTFS могут обладать следующими правами:

- *Полный доступ (Full Control) (All) (Все).*
- *Нет доступа (No Access) (None) (Нет).*
- *Право изменения (Change) (RWXD) (чтение/запись/выполнение/удаление).*
- *Право чтения (Read) (RX) (чтение/выполнение).*

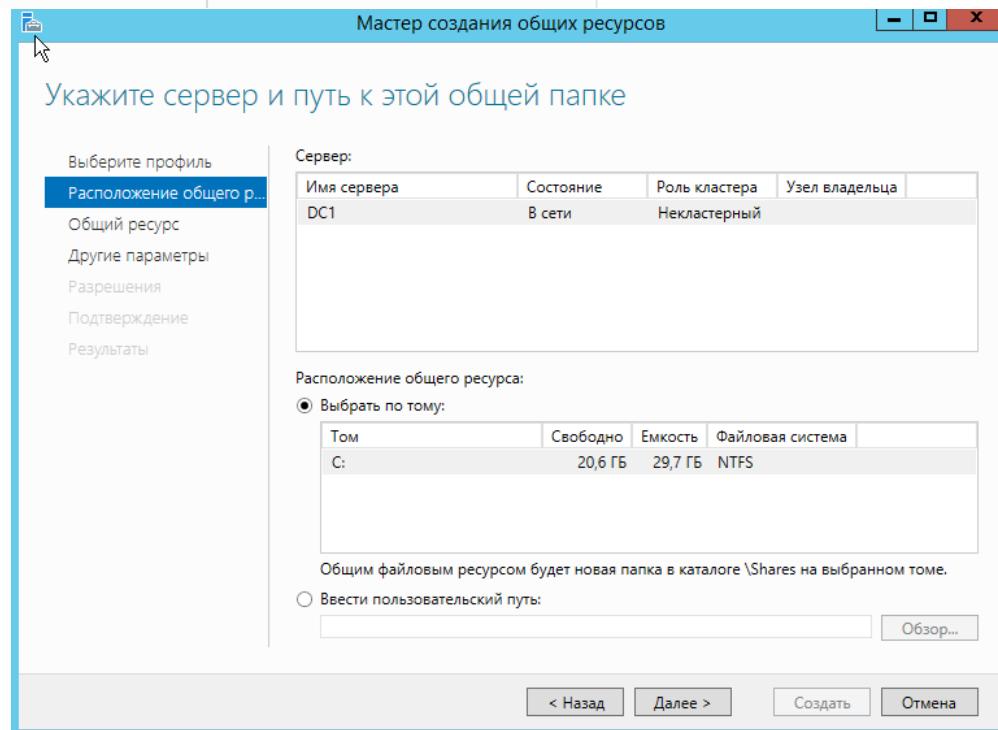
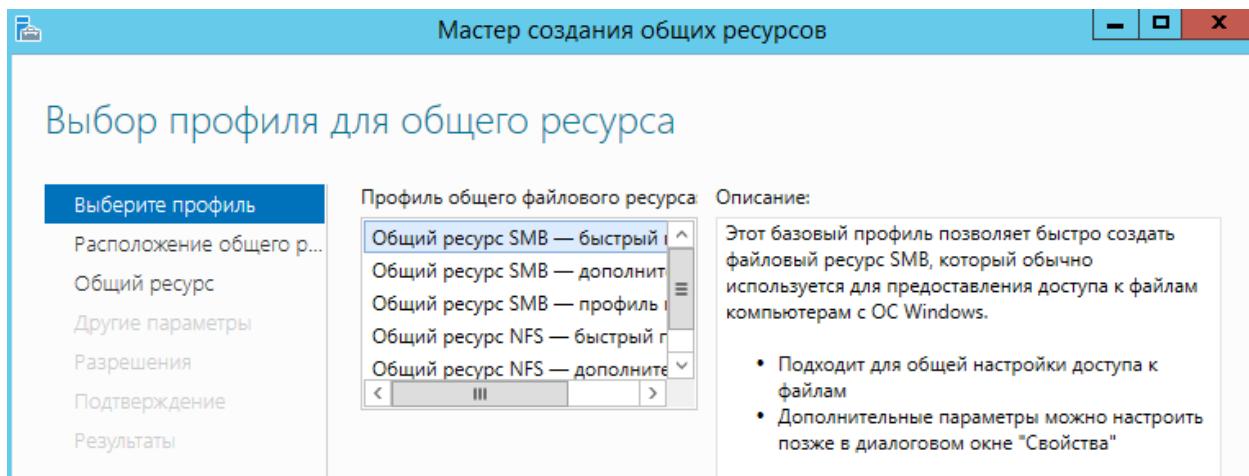
Для прав доступа NTFS, как и для прав общих каталогов, действует принцип поглощения. Исключение составляет отсутствие доступа, отменяющее действие всех остальных прав. При сетевом подключении пользователей права NTFS могут вступить в конфликт с правами общих каталогов. В такой ситуации применяется право доступа с наиболее жесткими ограничениями.

Создавать папки общего доступа мы будем через оснастку диспетчер серверов, с помощью мастера «Мастер создания общих ресурсов»

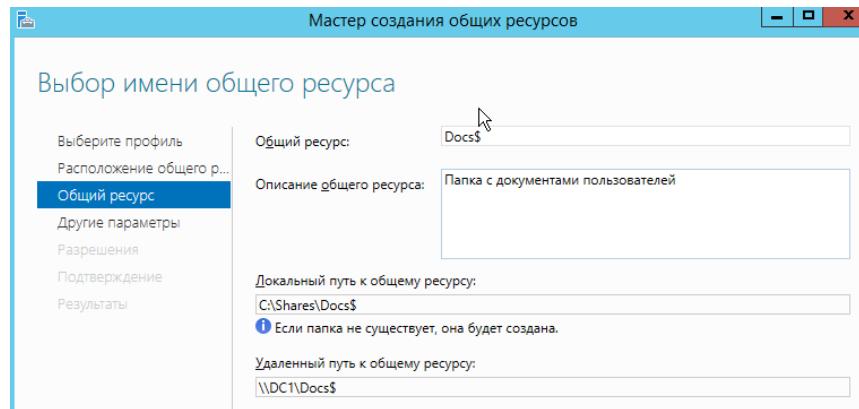
Создадим папку «Doc\$»



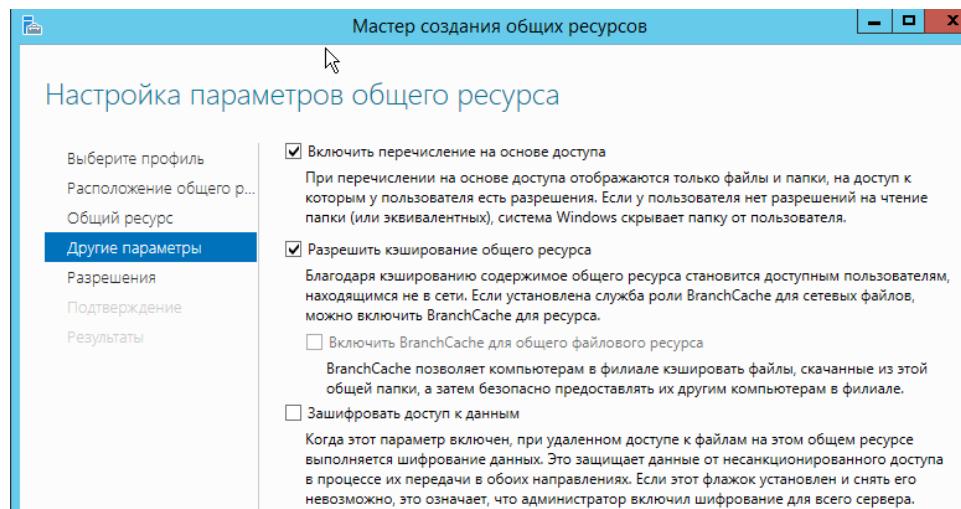
Выберем тип профиля – «Быстрый профиль»



Далее введём название и описание общего ресурса. Значок \$ в конце названия папки, позволит сделать невидимым этот ресурс в сети, но к ней всё равно можно будет обратиться по полному имени - «\\DC1.company.local\Doc\$»

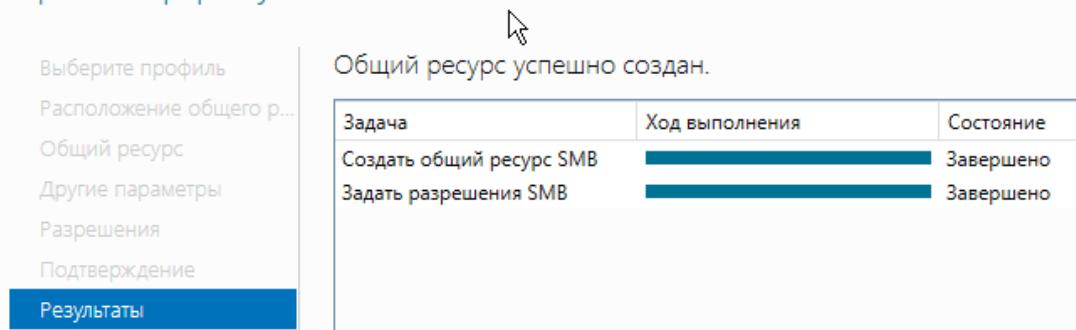


В других параметрах поставим галочку «Включить перечисление на основе доступа». Это позволит разграничить видимость вложенных папок на основе прав NTFS.



Параметры безопасности оставляем без изменения и переходим к созданию папки.

Просмотр результатов



После того как ресурс успешно создан можно закрыть мастер создания общих ресурсов.

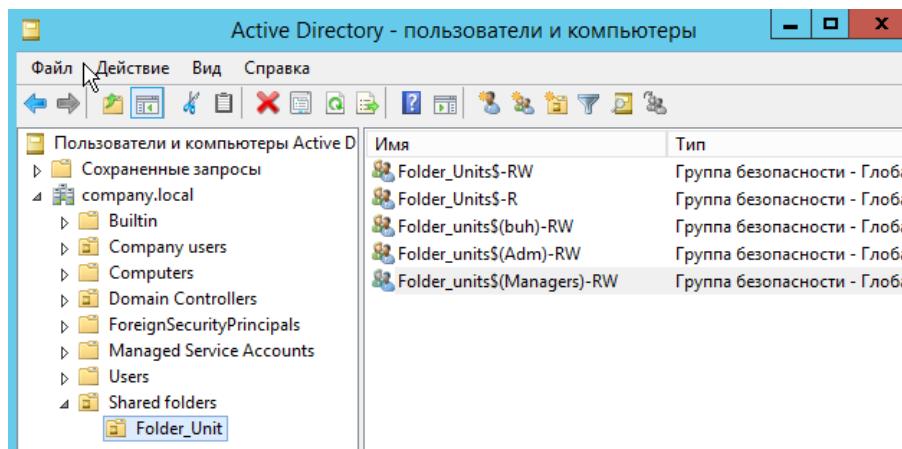
Созданная папка находится по следующему адресу - «\DC1.company.local\Doc\$».

Создание папки «Unit»

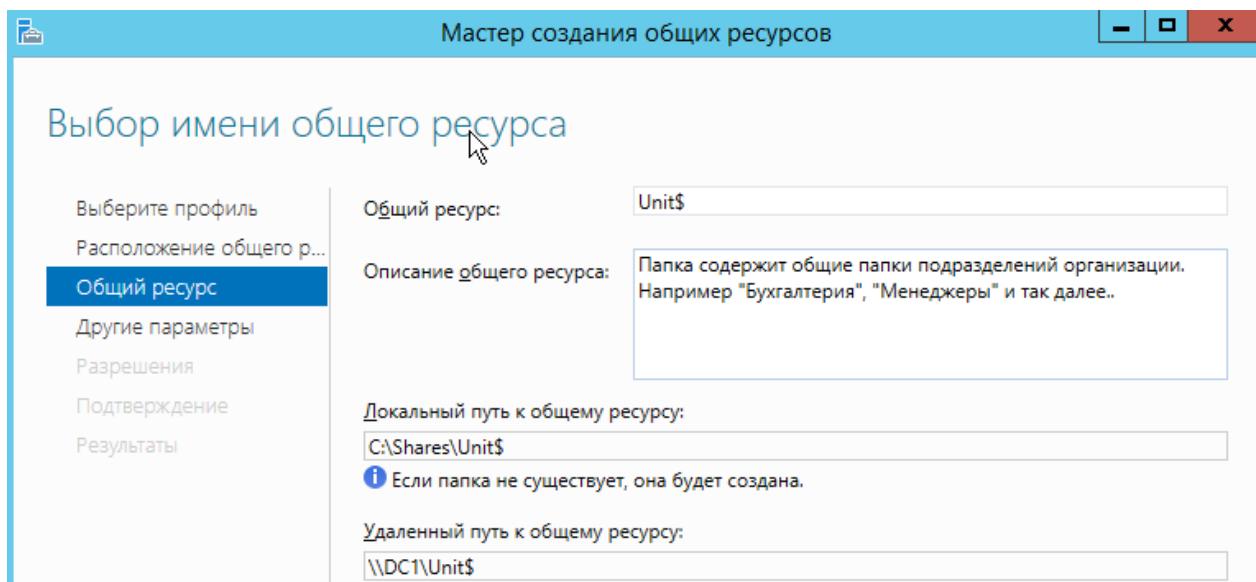
Прежде чем создать общую папку «unit» создадим новое подразделение в AD - «Shared Folders». В данном подразделении будут располагаться группы безопасности, которые мы будем использовать для распределения прав NTFS. Такая организация распределения доступа к общим ресурсам в будущем даст наглядную картинку безопасности и доступа к общим папкам компании, а также позволил быстро давать нужные права доступа пользователям к папкам.

После создания подразделений создадим следующие группы безопасности:

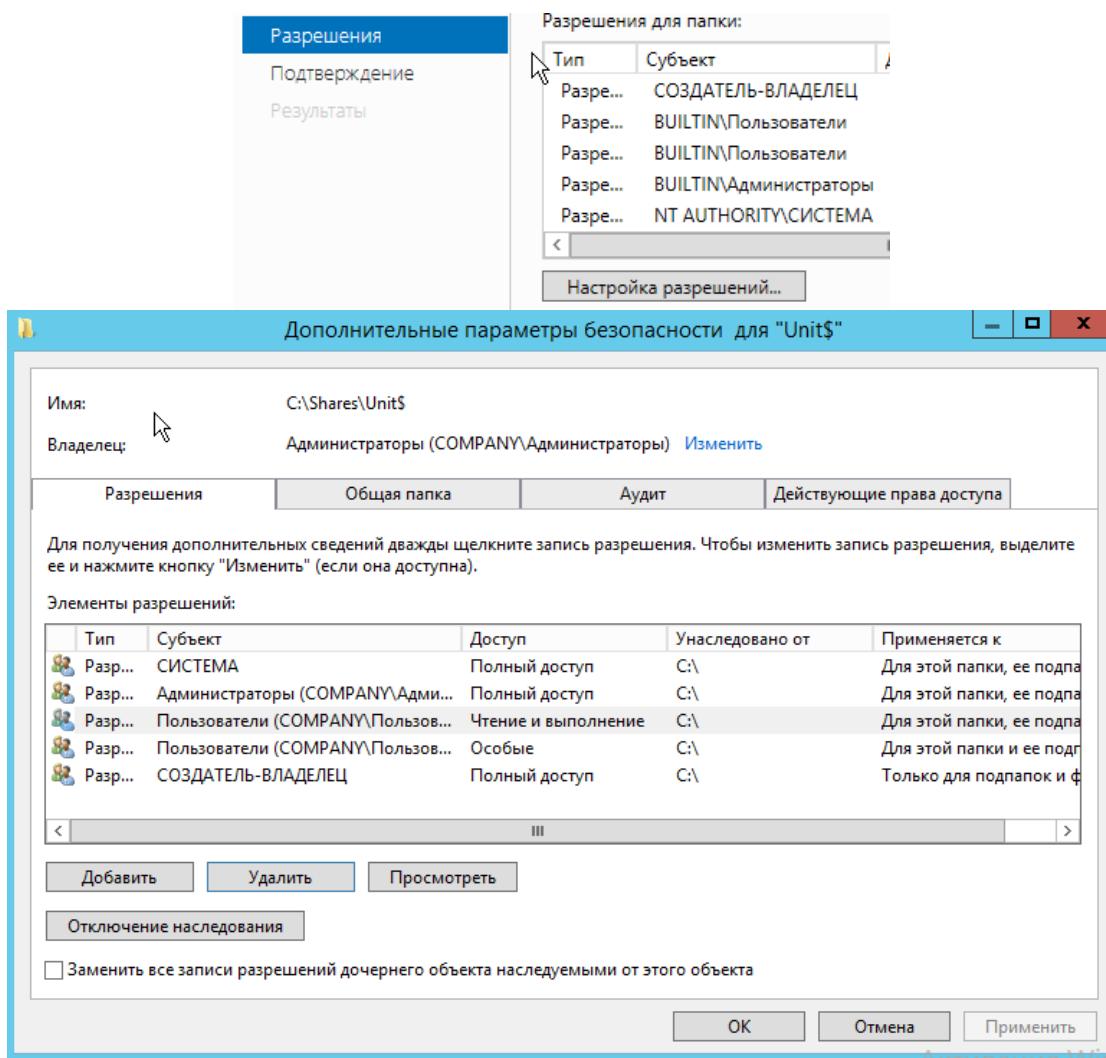
- Folder_unit-RW – группа безопасности, которая будет обладать доступом на чтение (R) и запись (W) файлов и папок в папке «Unit\$».
- Folder_unit-R – группа безопасности, которая будет обладать доступом только на чтение файлов и папок в папке «Unit\$».
- Folder_unit(Buh)-RW – группа безопасности, которая будет обладать доступом на чтение и запись файлов и папок в папке подразделения «Бухгалтерия», которая в свою очередь будет располагаться в папке «Unit\$»
- Folder_unit(Man)-RW – группа безопасности, которая будет обладать доступом на чтение и запись файлов и папок в папке подразделения «Менеджеры», которая в свою очередь будет располагаться в папке «Unit\$»
- Folder_unit(Adm)-RW – группа безопасности, которая будет обладать доступом на чтение и запись файлов и папок в папке подразделения «Менеджеры», которая в свою очередь будет располагаться в папке «Unit\$»



После создания нужных групп безопасности можно перейти к созданию папки «Unit\$», для этого используем уже известный нам «Мастер создания общих ресурсов».

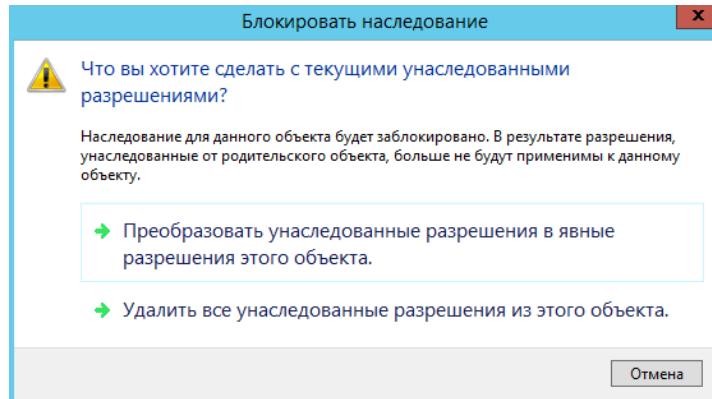


На этапе «Разрешения» перейдём к «Настройкам расширений»

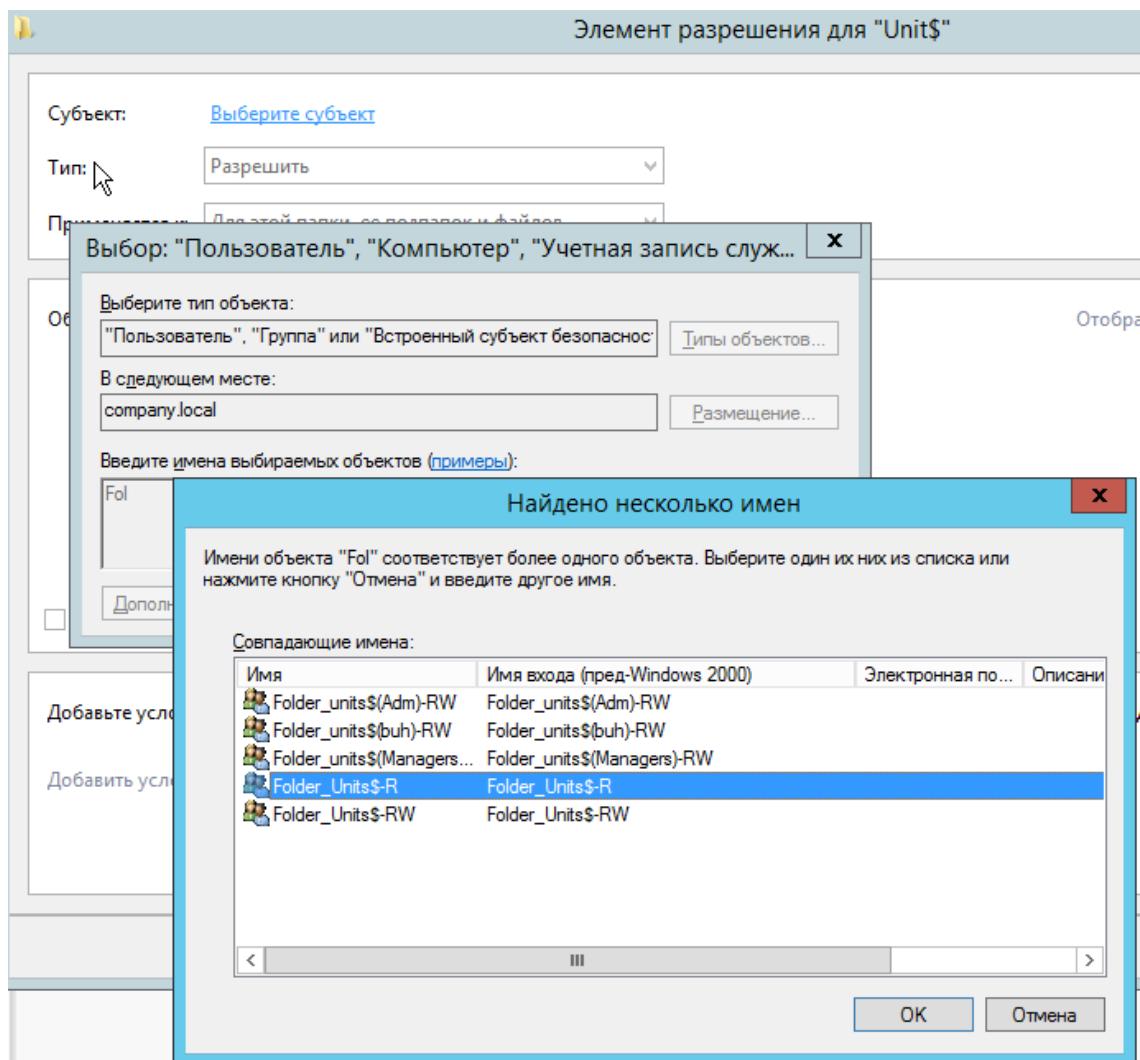


В окне «Дополнительные параметры безопасности для Unit\$» нажмём на «Отключить наследование». *Отключение этого параметра позволит нам назначить свои права доступа на данную папку.*

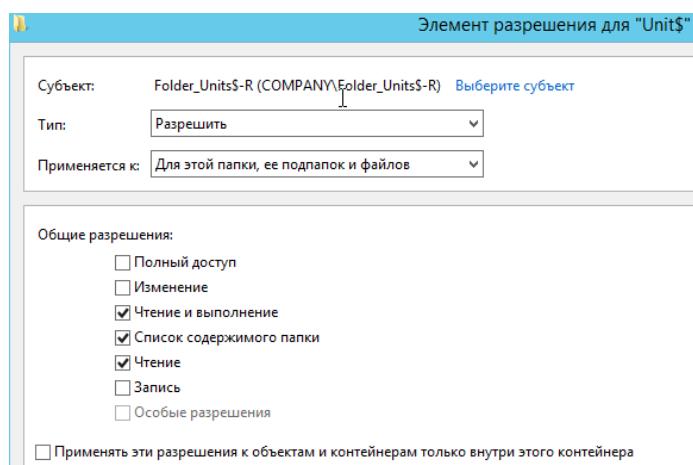
В окне «Блокировать наследование» выберем «Преобразовать унаследованные разрешения в явные разрешения этого объекта», что позволит нам сохранить включенные ранее в этот объект группы и пользователей.

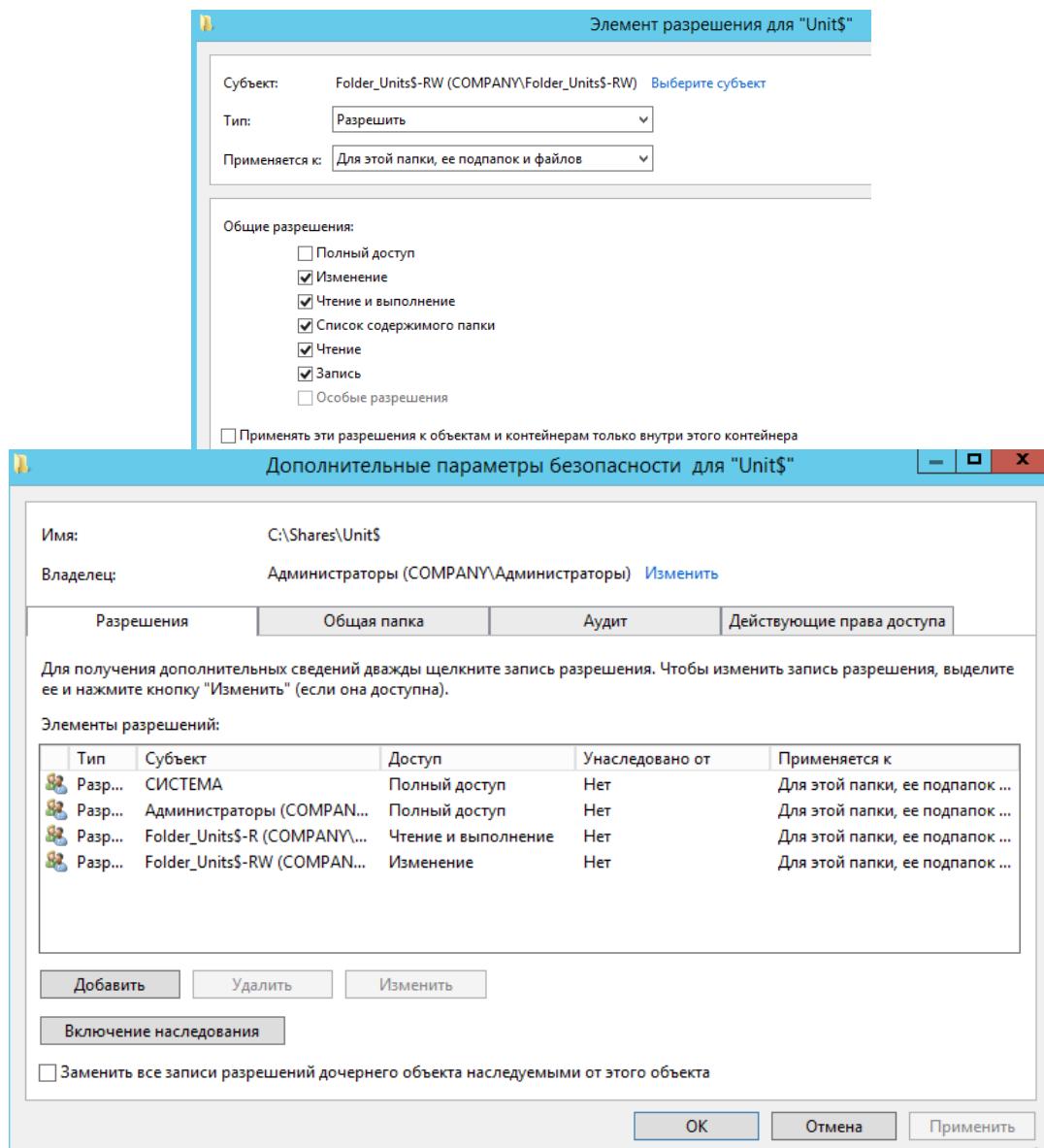


Далее на вкладке разрешения удалим все объекты за исключением СИСТЕМА и Администраторы. Добавим (Выберите субъект) созданную ранее группы: «Folder_units\$-R» и «Folder_units\$-RW». Найти их можно поиском по слову «Folder» или просто «Fol».



Назначим каждой из этих групп соответствующие права: Folder_units\$-R – чтение, Folder_units\$-RW – чтение и запись.



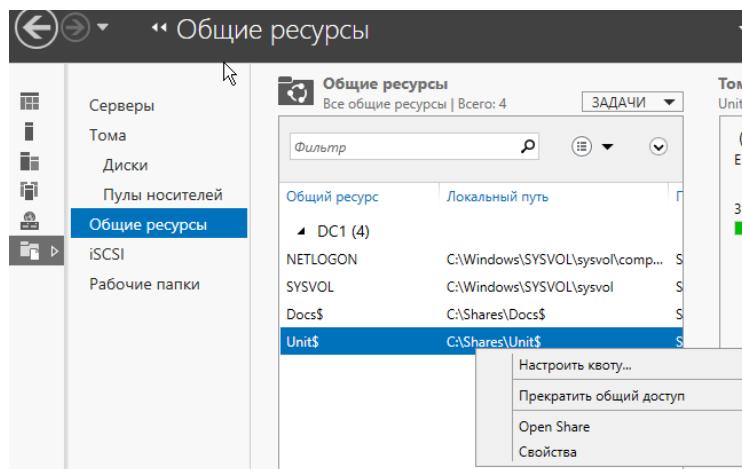


После того как разрешения выставленные и все группы добавлены нажимаем «OK». Далее заканчиваем работу мастера и создаём нужную нам папку.

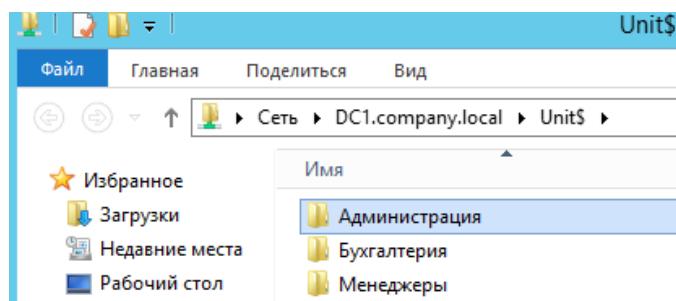
После того как основная папка создана перейдём к созданию и распределению прав вложенных папок:

- Бухгалтерия
- Администрация
- Менеджеры

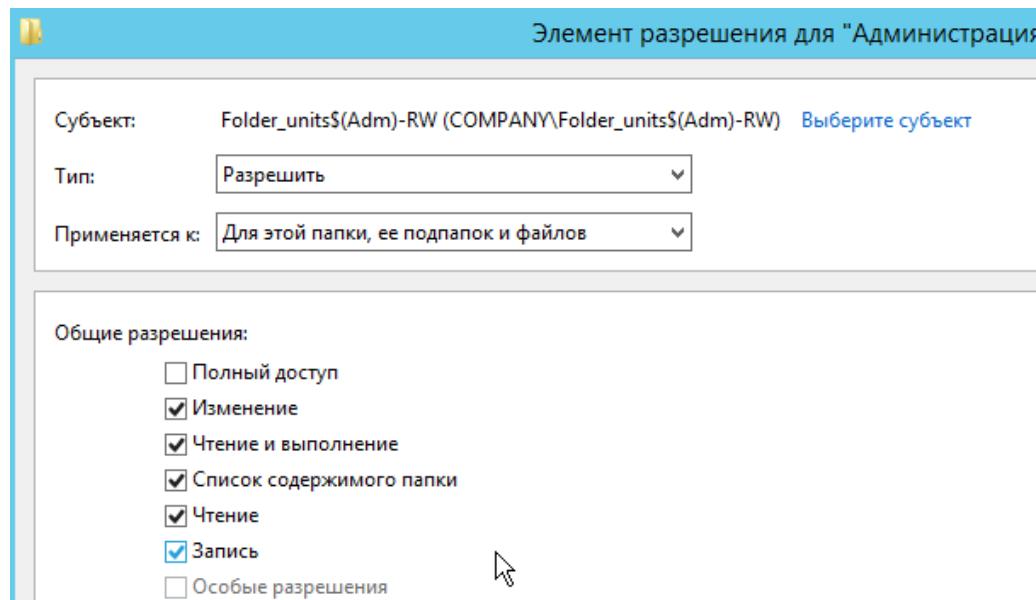
Для этого перейдем в созданную нами папку через меню правой кнопки мыши – «Open Share»

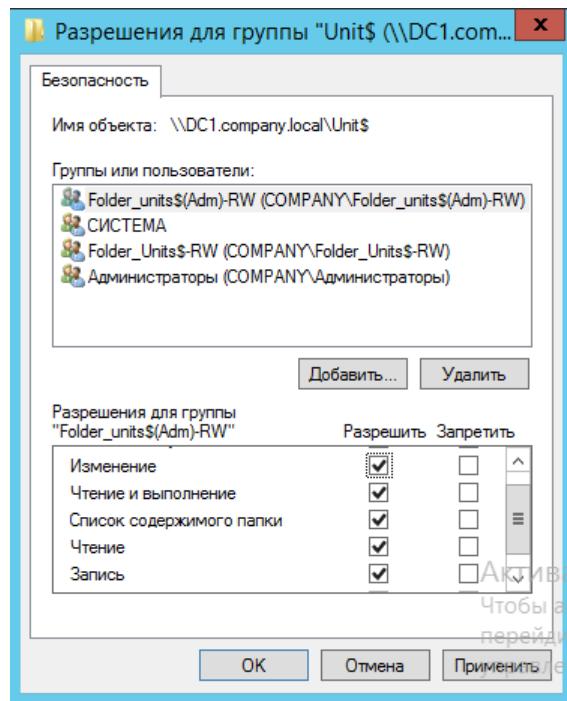


создадим внутри её необходимые папки

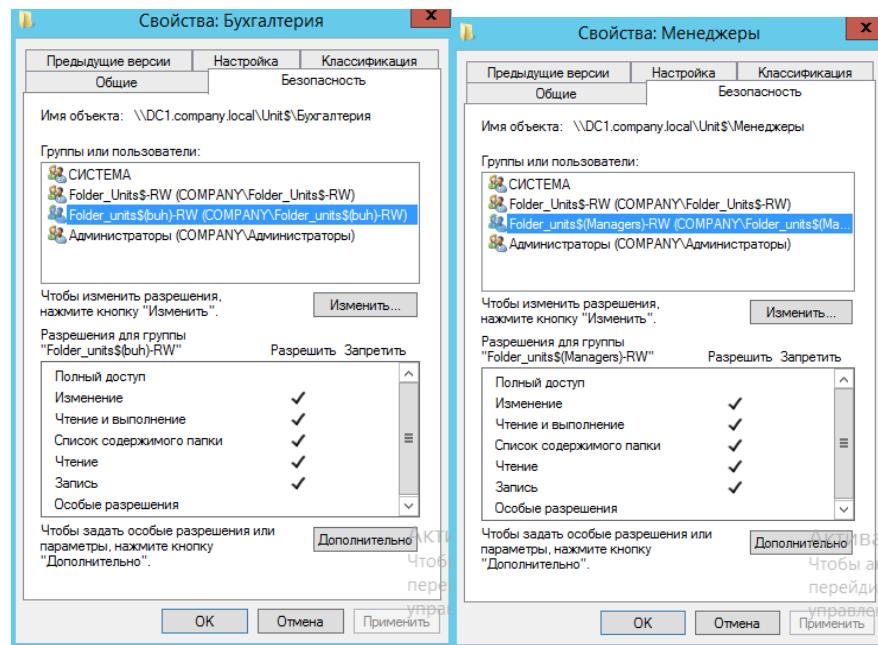


Выставим права доступа NTFS на папку «Администрация». Для этого зайдём в свойства папки и на вкладке безопасность удалим группу «Folder_units\$-R» и добавим созданную ранее группу «Folder_units\$(Adm)-RW», которой назначим права на «изменение» и «чтение».



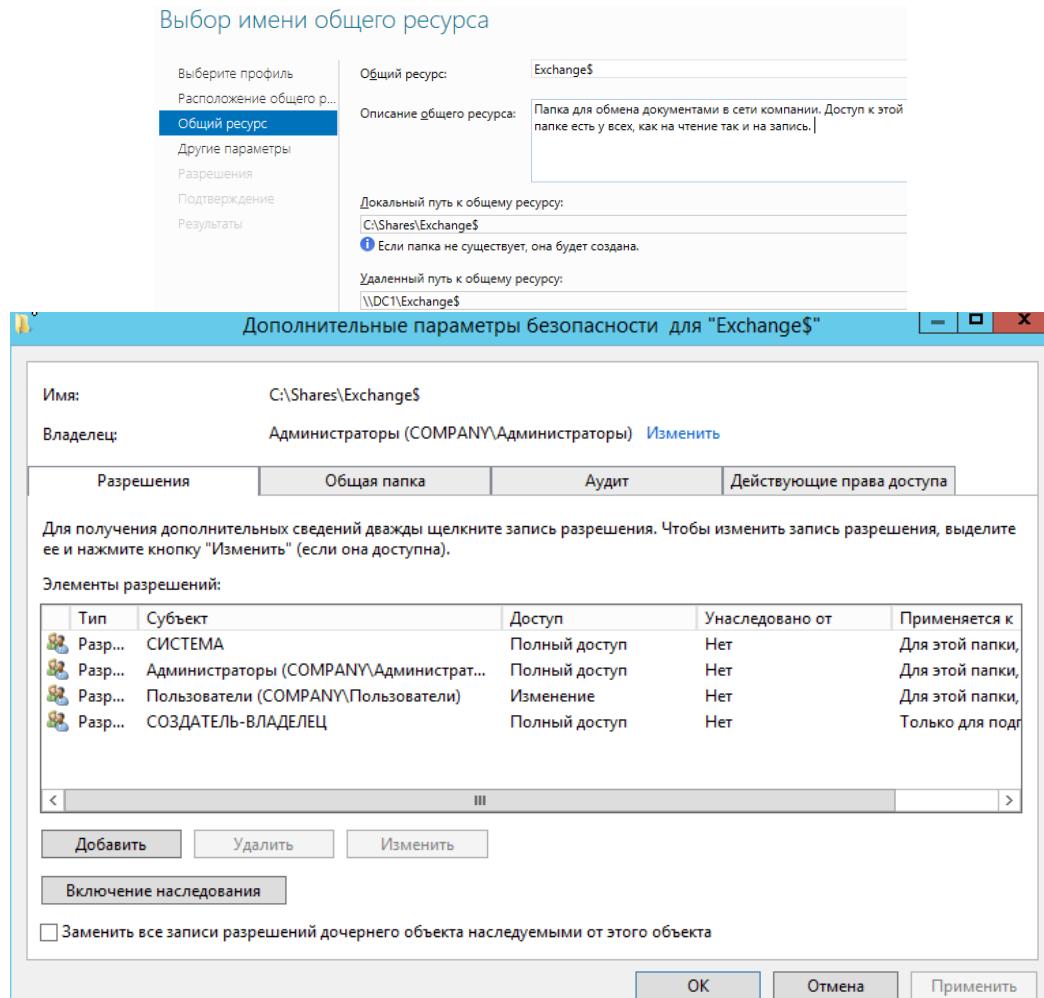


Аналогичным образом раздадим права на папку «Бухгалтерия» и «Менеджеры».



Создание папки «Exchange».

Это папка отличается от папки документы лишь тем, что доступ на чтение и запись должен быть у всех пользователей компании, т.е. домена company.local.

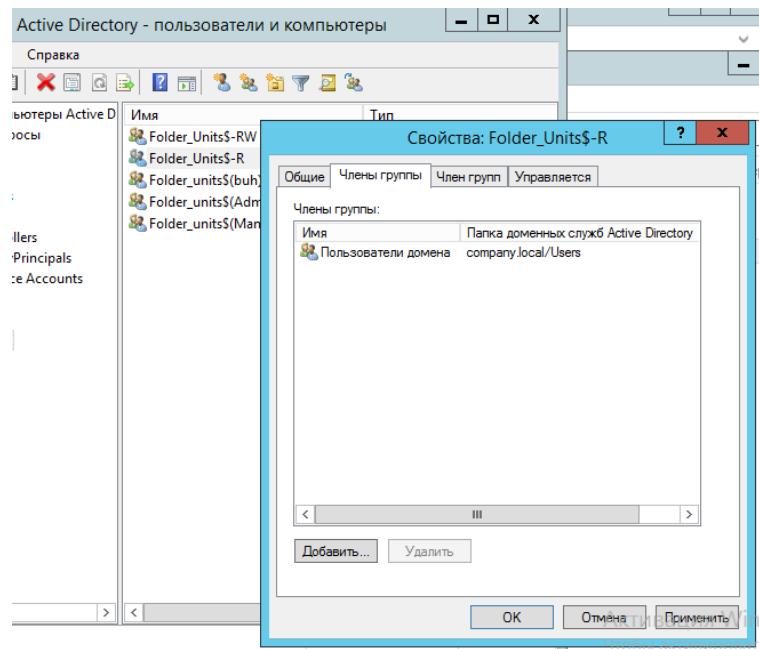


2.2 Назначение прав доступа созданным ранее пользователям домена к подпапкам (Администрация, Бухгалтерия, Менеджеры) директории «Unit» согласно их должности.

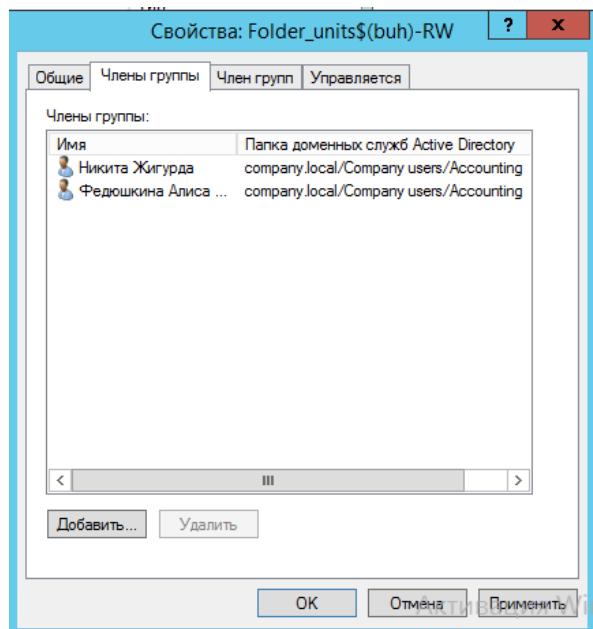
Назначить права доступа созданным ранее пользователям домена к подпапкам (Администрация, Бухгалтерия, Менеджеры) директории «Unit» согласно их должности. Пользователю Путин Владимир Геннадьевич дать полные права к папке «Unit», а также всем её подпапкам.

Ранее в Active Directory были созданы специальные группы, отвечающие за распределение прав на папку «Unit», а также её подпапок. Теперь всё, что нам необходимо сделать что бы раздать необходимые права - это добавить пользователей (или даже группы) в одну из созданных групп.

- Folder_unit-R – в эту группу включим всех пользователей домена, таким образом они получат доступ на чтение и просмотр папок внутри папки «Unit».

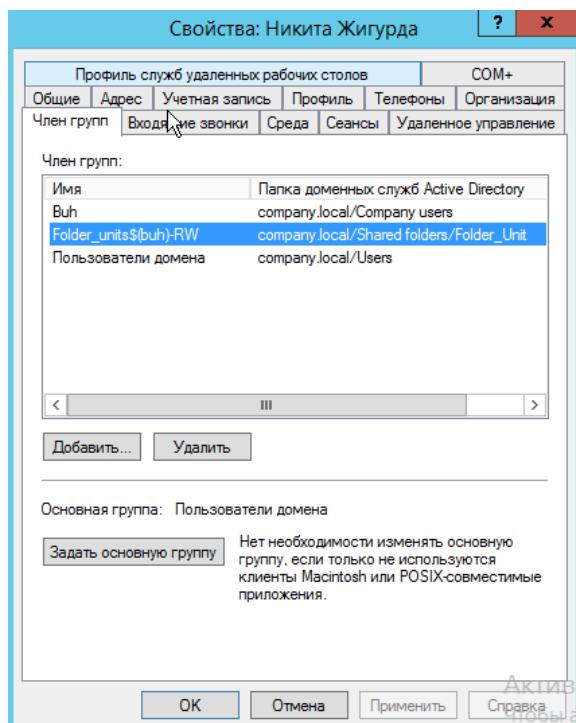


- В группу «Folder_unit-RW» добавим пользователя «Путин Владимир Геннадьевич», так как это *группа безопасности обладать доступом на чтение и запись файлов и папок в папке «Unit\$»*.
- Folder_unit(Buh)-RW – в эту группу добавим пользователей бухгалтерии: Никита Джигурда и Федюшкина Алиса Викторовна



- Folder_unit(Man)-RW – в эту группу добавим менеджеров: Петров и Пелюля.
- Folder_unit(Adm)-RW - в данную группу добавим оставшегося сотрудника администрации Медведева Дмитрия Генадьевича

Теперь, что бы посмотреть к каким папкам тот или иной пользователь имеет доступ достаточно посмотреть в свойства этого пользователя принадлежность к группе начинаящейся на признак папки - «Folder....»



2.3 Установить и настроить DFS. Подключить через DFS созданные ранее папки общего доступа.



Сервер

Distributed File System (DFS) — компонент *Microsoft Windows*, использующийся для упрощения доступа и управления файлами, физически распределёнными по сети. При её использовании файлы, распределённые по серверам, представляются находящимися в одном месте.

DFS может быть реализована двумя способами:

- Распределенная файловая система с изолированным корнем;
- Доменная распределенная файловая система.

Основные понятия

Узловой сервер — сервер домена, на котором располагается корень DFS. Можно реплицировать корень DFS, создав корневые целевые папки на других серверах домена. Это обеспечит доступ к файлам при отключении узлового сервера.

Пространство имен (или корень DFS) — особое имя, используемое пользователями для доступа к файловым ресурсам.

Целевая папка — общедоступная папка на файловом сервере, к которой происходит доступ.

Папка — ссылка в пространстве имён, указывающая на целевую папку.

Преимущества

Простой доступ к файлам

Распределенная файловая система упрощает доступ к файлам. Пользователи используют единый сетевой ресурс для доступа к файлам, даже если эти файлы физически находятся на разных серверах. Даже если изменится физическое расположение целевой папки, это не повлияет на доступ пользователей к ней. Они смогут обращаться к папке как раньше, поскольку её видимое расположение не изменится. Пользователям не требуется подключать несколько дисков для доступа к своим файлам. Кроме того, задачи по обслуживанию сервера, обновлению программ и другие, которые обычно требуют отключения сервера, могут выполняться без отключения пользователей от ресурсов. Это особенно полезно для веб-серверов. Выбрав корневой каталог веб-узла в качестве корня DFS, можно перемещать ресурсы в рамках распределенной файловой системы, не нарушая ссылки HTML.

Доступность

Доменные DFS обеспечивают пользователям доступ к файлам двумя способами.

Во-первых, операционная система Windows Server автоматически публикует топологию DFS в Active Directory. Благодаря этому, пространство имен DFS всегда видимо для пользователей всех серверов в домене.

Во-вторых, администратор может реплицировать корень DFS и целевые папки. Репликация означает дублирование корней и целевых папок DFS на нескольких серверах домена. При этом пользователи всегда могут получить доступ к своим файлам, даже если один из физических серверов, на котором эти файлы находятся, становится недоступным.

Эффективная загрузка сервера

Корень DFS может поддерживать несколько целевых папок DFS, которые физически распределены по сети. Например, это полезно, если есть файл, который активно используется пользователями. Пользователи будут обращаться к этому файлу не на одном сервере, сильно загружая его, а к файлу, распределенному системой DFS по разным серверам. Однако для пользователей этот файл будет виден в едином месте в сети.

Безопасность файлов и папок

Поскольку общие ресурсы, управляемые DFS, используют стандартные разрешения NTFS и разрешения общего доступа к файлам, можно использовать существующие группы безопасности и учетные записи пользователей, чтобы гарантировать, что только авторизованные пользователи имеют доступ к важным данным.

DFS - это технология, обеспечивающая возможности упрощения доступа к общим файловым ресурсам и глобальной репликации данных. Благодаря DFS распределённые по различным серверам общие ресурсы (каталоги и файлы) можно объединить в единую логическую UNC структуру, которая для пользователя выглядит, как единый сетевой ресурс. Даже при изменении физического местоположения целевой папки, это не влияет на доступ пользователя к ней.

Реализация служб DFS в Windows Server 2012 отличается от предыдущих версиях Windows. В первую очередь отметим, что технологии DFS в Windows Server 2012 реализованы в виде двух отдельных, независимых друг от друга служб – DFS

Namespaces и DFS Replication, включенных в роль файлового сервера (File and Storage Services).

- *DFS Namespaces (DFSN или DFS-N) – пространство имен DFS. Позволяет объединять в единую логическую структуру общие папки, расположенные на различных серверах организации. Каждое пространство имен для пользователя выглядит как единая сетевая папка с подкаталогами. Реальная структура данного пространства имен DFS является скрытой от пользователя, и может включать в себя различные сетевые папки, расположенные на различных серверах и сайтах.*
- *DFS Replication (DFSR или DFS-R) – служба DFS репликации. Позволяет организовать эффективную службу репликации каталогов (в том числе включенных в пространство имен DFS) между различными серверами и сайтами AD. Данная служба для репликации использует специальный алгоритм удаленного разностного сжатия – RDC- remote differential compression. Благодаря RDC, которая отслеживает изменения в файлах, при репликации копируются не файлы целиком (как в случае с FRS репликацией), а только их блочные изменения*

Установка служб DFS в Windows Server 2012

Установить службы DFS можно с помощью уже знакомой нам консоли «Диспетчер серверов» или же при помощи Windows PowerShell.



Среда Windows PowerShell™ — это новые, ориентированные на задачи оболочка командной строки и язык сценариев, разработанные для системного администрирования. Основанная на .NET Framework, среда Windows PowerShell™ помогает ИТ-специалистам и опытным пользователям в управлении и автоматизации администрирования операционной системы Windows, а также ее приложений.

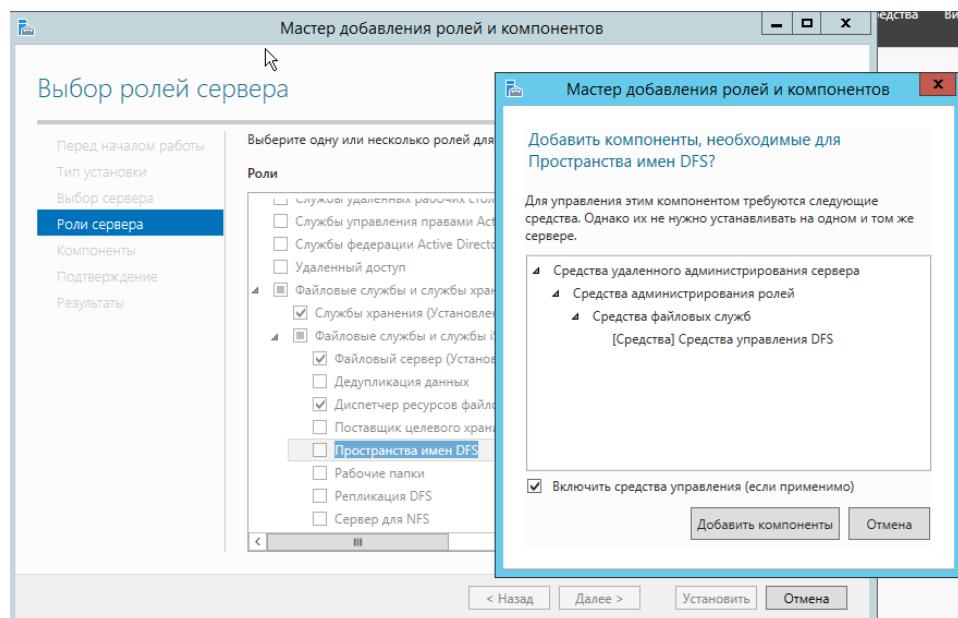
Встроенные команды Windows PowerShell, называемые cmdlets, позволяют управлять компьютерами предприятия из командной строки. При использовании providers среды Windows PowerShell™ доступ к хранилищам данных, таким как реестр и хранилище сертификатов, становится таким же простым, как и доступ к файловой системе. Кроме того, среда Windows PowerShell™ содержит полноценное средство синтаксического анализа выражений и полностью разработанный язык сценариев.

Windows PowerShell™ включает следующие компоненты.

- *Cmdlets для выполнения общих задач системного администрирования, таких как управление реестром, службами, процессами и журналами событий, а также использования инструментария управления Windows.*
- *Язык сценариев, ориентированный на задачи, и поддержка существующих сценариев и средств командной строки.*
- *Постоянство. Так как в cmdlets и хранилищах системных данных используются одинаковый синтаксис и система именования, данные могут использоваться различными cmdlets, а выходные данные одного cmdlet могут быть использованы как входные данные другого без необходимости дополнительных форматирования и обработки.*

- Упрощенный механизм обращения к операционной системе, основанный на командной строке, который позволяет пользователю просматривать реестр и другие хранилища данных с помощью тех же приемов, которые используются для просмотра файловой системы.
- Мощные возможности обработки объектов. Объекты могут быть обработаны напрямую или переданы в другие средства или базы данных.
- Расширяемый интерфейс. Независимые производители программного обеспечения и разработчики предприятия могут создавать настраиваемые средства и инструменты для администрирования соответствующего программного обеспечения.

Как мы уже, службы DFS являются элементами роли файлового сервера, а именно «Файловые службы и службы хранилища». С помощью мастера добавления ролей и компонентов добавим роль «Пространство имён DFS»



Но проще и быстрее установить все DFS службы и консоль управления DFS с помощью PowerShell

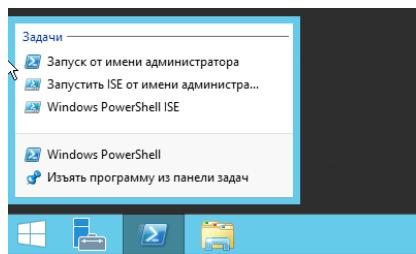
Например:
Install-WindowsFeature FS-DFS-Namespace, FS-DFS-Replication, RSAT-DFS-Mgmt-Con

Где **FS-DFS-Namespace** – служба DFS Namespaces
FS-DFS-Replication – служба репликации DFS Replication
RSAT-DFS-Mgmt-Con – mmc консоль управления службами DFS – DFS Management Tools

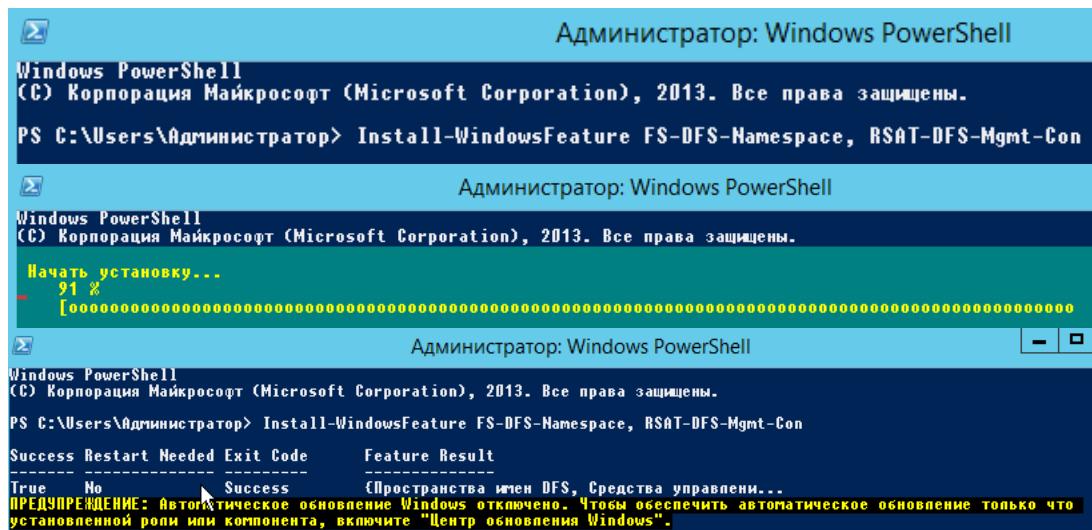
Соответственно, службы и консоль управления DFS можно установить и по отдельности.

Так как службы репликации мы использовать не будем, установим только службу DFS и консоль управления службами.

Откроем командную строку PowerShell от имени администратора.

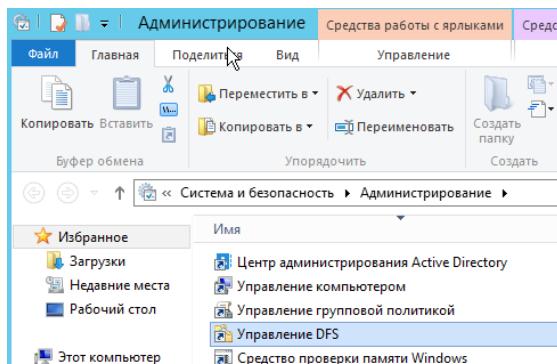


Введём команду
Install-WindowsFeature FS-DFS-Namespace, RSAT-DFS-Mgmt-Con



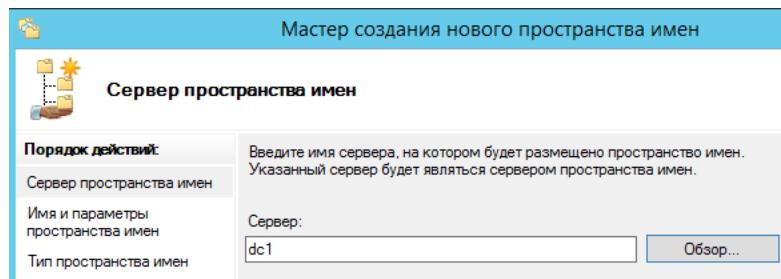
Не смотря на предупреждение все необходимы компоненты и службы устанавливаются (Feature Result – Пространство имен DFS, Средство управления...). Как видите зная язык PowerShell можно гораздо быстрее устанавливать и управлять ролями службами и компонентами Windows Server.

Закрываем PowerShell и переходим к настройке пространства имен DFS. Для этого открываем оснастку «Управление DFS».



Запустим мастер создания нового пространства имён, для этого в панели «Действия» Управление DFS выберем новое пространство имён.

На первом этапе мастера предложит выбрать сервер на котором будет размещено пространство имён, так как у нас только один сервер то его и выбираем, т.е. – DC1.

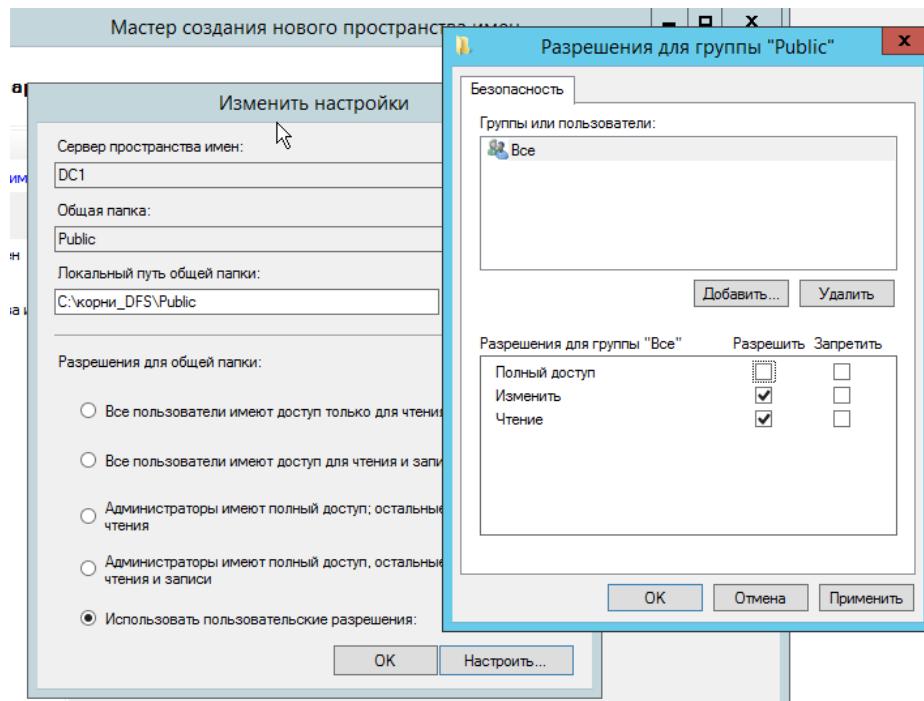


Далее вводим имя пространства имён – Public (Общий).



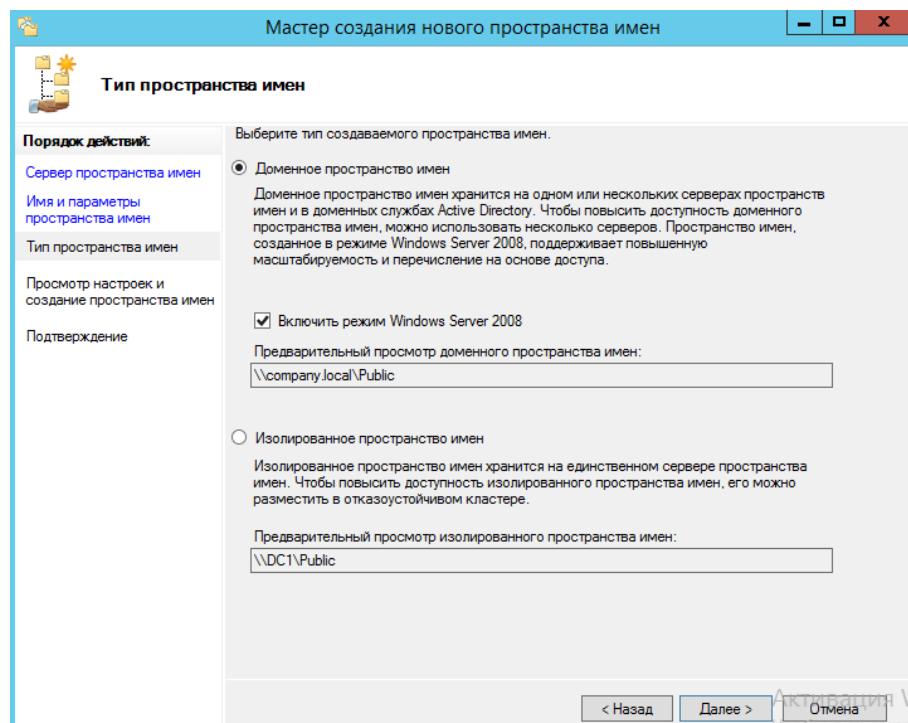
Прежде чем продолжить зайдём в «Изменить настройки».

Для того, чтобы права доступа проверяются на уровне файловой системы NTFS нам необходимо установить галочку «Использовать пользовательские разрешения», после чего зайти в меню «Настроить» и установить галочку на поле «Изменить» и «Чтение».

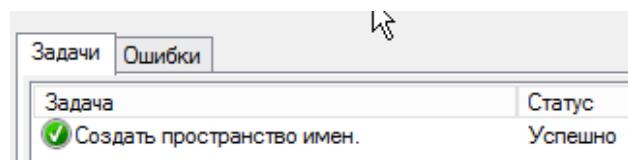


Сохраняем настройки (OK) и продолжаем работу мастера – «Далее».

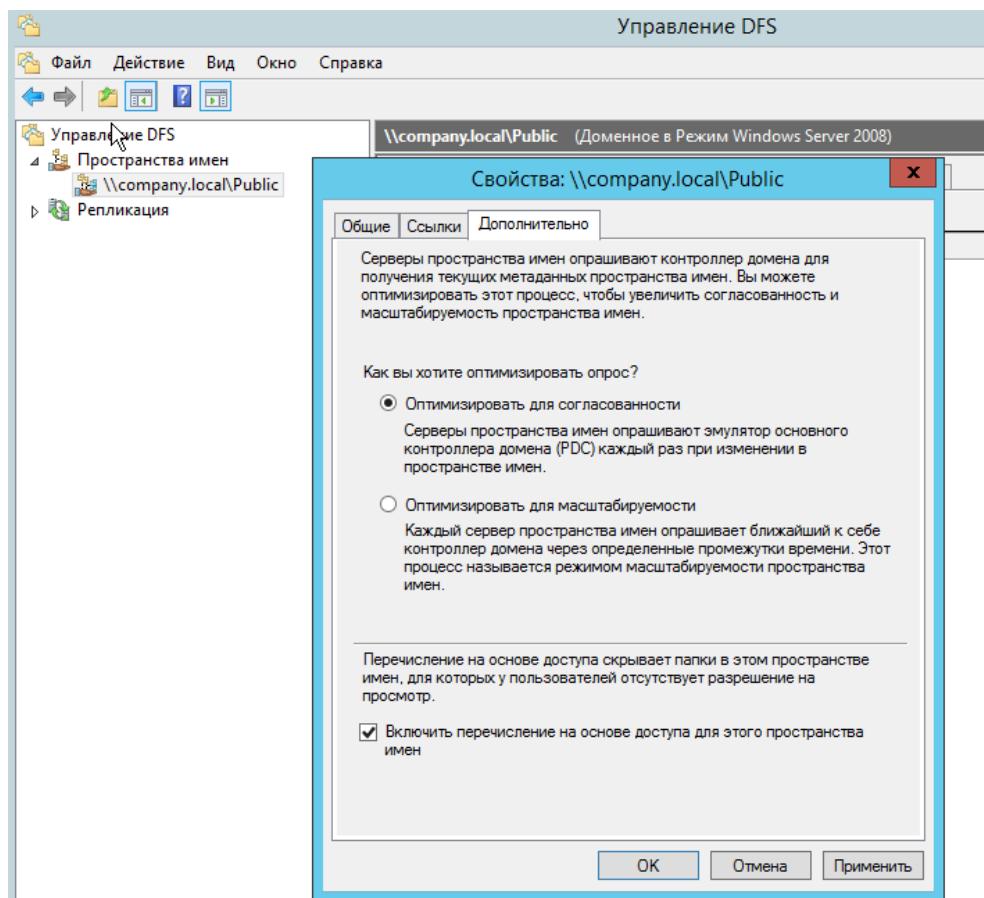
Далее мастер предложит указать тип создаваемого пространства имен. Это может быть «Доменное пространство имен» (Domain-based namespace) или «Изолированное пространство имен» (Stand-alone namespace). Так как у нас домен мы будем использовать «Доменное пространство имён», к оно обладает рядом преимуществ.



Нажимаем «Далее», а затем «Создать». Пространство имён успешно создано



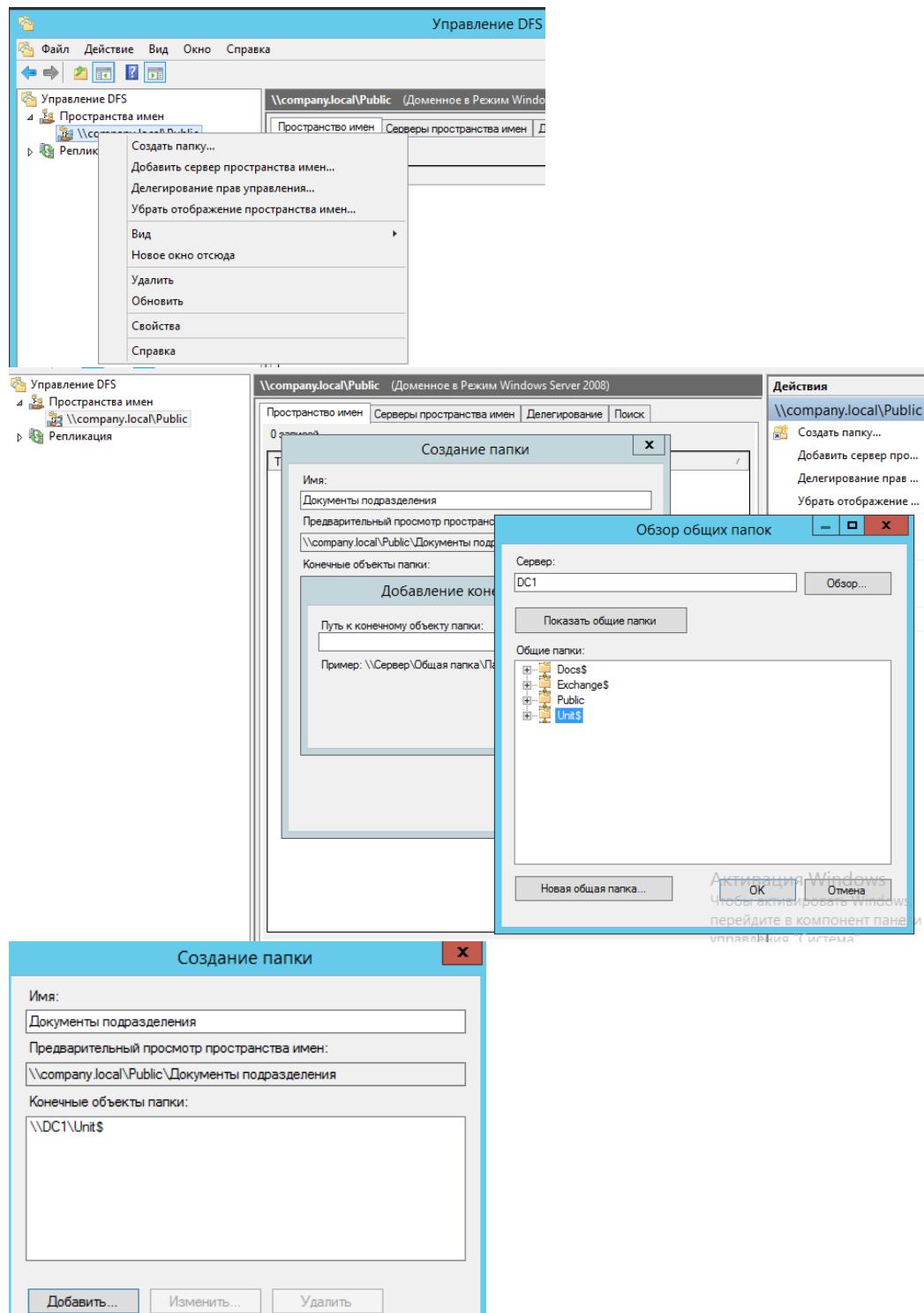
После окончания работы мастера в ветке «Пространства имен» консоли управления DFS появится созданное нами новое пространство имен DFS «\\company.local\Public». Чтобы пользователи при доступе к DFS каталогам видели только те каталоги, к которым у них имеется доступ, включим для данного пространства «Перечисление на основе доступа» (DFS Access-Based Enumeration). Для этого откройте окно свойств созданного пространства и на вкладке «Дополнительно» установите соответствующую галочку.



Технология *Access-based Enumeration* (*доступ на основе разрешений*) позволяет на общих сетевых ресурсах (шарах) скрыть от пользователей файлы и папки, к которым у них отсутствует NTFS-доступ. Тем самым можно обеспечить дополнительную конфиденциальность информации, хранящейся в сетевом каталоге (за счет скрытия структуры и имен каталогов и файлов), улучшить юзабилити для пользователя, которому в процессе работы с сетевым каталогом не будет отображаться лишняя информация (тем более доступ к которой у него все равно отсутствует) и, самое главное, оградим системного администратора от постоянных вопросов пользователей «почему меня не пускает в эту папку!!». Попробуем детальнее разобраться в этой технологии и особенностях ее настройки и использования в различных версиях Windows.

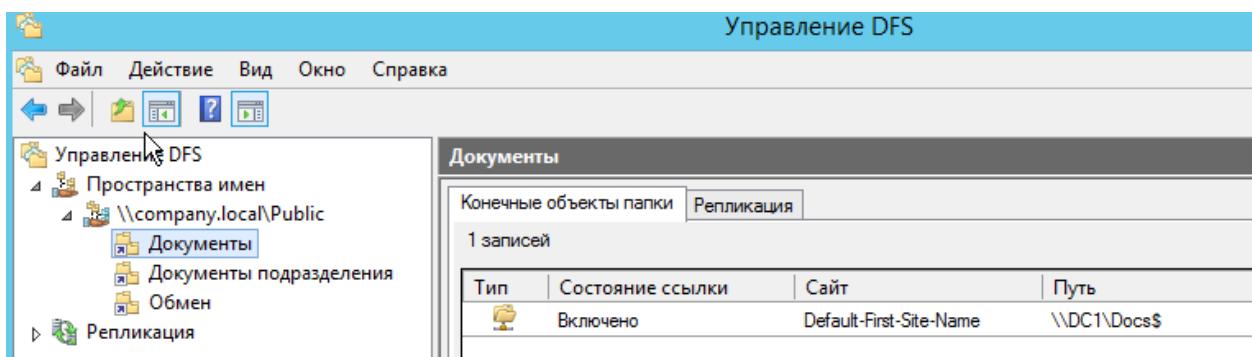
Теперь, когда пространство имён создано и настроено можно добавить в него наши сетевые ресурсы: папку «Unit\$», «Doc\$» и «Exchange».

Создадим папку «Документы подразделения» со ссылкой на папку «Unit\$».

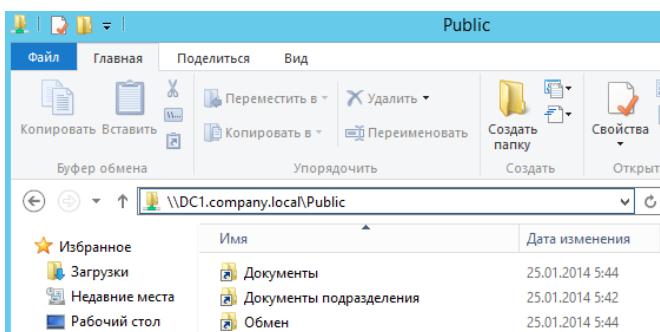


Аналогичным способом создадим папку «Документы» со ссылкой на папку «Doc\$» и папку «Обмен» со ссылкой на папку «Exchange».

После чего настройку DFS можно считать завершённой.



Перейдя по ссылке «\\company.local\Public» мы увидим созданные нами папки с сетевыми ресурсами.



Используя DFS мы можем поменять конечный путь папки, например, если необходимо перекинуть документы пользователей на другой сервер. Пользователи в свою очередь будут видеть всё теже пути DFS, т.е. фактически даже не пойму, что документы переехали на другой сервер. Благодаря этому можно грамотно распределить нагрузку между файловыми серверами компании при этом не усложняя жизнь рядовых пользователей.

2.4 Групповые политики (GPO)

С помощью групповых политик (GPO) реализовать:

- Перенаправление папки «Мои документы»
- Подключить всем пользователям домена сетевой диск «P» (Public, он же «Общий ресурс компании») ссылающийся на пространство имён DFS (созданный ранее).
- Выполнить настройку браузер у пользователей IE с помощью GPO

Групповые политики – это набор правил, обеспечивающих инфраструктуру, в которой администраторы локальных компьютеров и доменных служб Active Directory могут централизовано развертывать и управлять настройками пользователей и компьютеров в организации. Все настройки учетных записей, операционной системы, аудита, системного реестра, параметров безопасности, установки программного обеспечения и прочие параметры развертываются и обновляются в рамках домена при помощи параметров объектов групповой политики GPO (Group Policy Object). Групповые политики являются компонентом операционной системы Windows и основываются на тысячах отдельных параметров политик, иначе говоря, политик, определяющих определённую конфигурацию для своего применения.



Все параметры политик располагаются в объекте групповых политик GPO (Group Policy Object). Объекты групповых политик делятся на две категории:

- Доменные объекты групповых политик, которые используются для централизованного управления конфигурацией компьютеров и пользователей, входящих в состав домена Active Directory. Эти объекты хранятся только на контроллере домена;
- Локальные объекты групповых политик, которые позволяют настраивать конфигурацию локального компьютера, а также всех пользователей, созданных на этом компьютере. Эти объекты хранятся только в локальной системе. Локальные объекты групповых политик могут применяться, даже если компьютер входит в состав домена.

Работая с групповыми политиками, следует учитывать, что:

- ✓ *объекты GPO применяются в отношении контейнеров, а не замыкающих объектов;*
- ✓ *один контейнер может быть связан с несколькими объектами GPO;*
- ✓ *объекты GPO, связанные с одним и тем же контейнером, применяются в отношении этого контейнера в том порядке, в котором они были назначены;*
- ✓ *объект GPO включает в себя две составляющие: параметры, относящиеся к компьютеру, и параметры, относящиеся к пользователю;*
- ✓ *обработку любой из этих составляющих можно отключить;*
- ✓ *наследование объектов GPO можно блокировать;*
- ✓ *наследование объектов GPO можно форсировать;*
- ✓ *применение объектов GPO можно фильтровать при помощи списков ACL.*

Контейнером (container) называется объект верхнего уровня, содержащий другие объекты.

Применение групповых политик происходит в последовательности, соответствующей иерархии GPO: сначала объект групповой политики сайта, затем домена, затем GPO, связанные с подразделениями в соответствии с их вложенностью. Порядок выполнения групповых политик можно изменить с помощью настроек, блокирующих определенные групповые политики или заставляющих их выполняться принудительно. Кроме того, на порядок выполнения групповых политик влияет применение групп безопасности.

По умолчанию настройки групповой политики, применяемые к контейнеру определенного уровня, наследуются всеми контейнерами более низких уровней и находящимися внутри них пользователями и компьютерами. Если с дочерней организационной единицей

(контейнером) связан свой GPO, он может устанавливать для нее индивидуальные настройки групповых политик, отменяющие применение к ней наследуемых настроек. Если некоторые настройки групповых политик родительского контейнера не заданы (*not defined*), то они не наследуются и дочерними контейнерами. Если родительский контейнер обладает сконфигурированными настройками групповых политик, которые не заданы в GPO дочернего контейнера, то такие настройки наследуются.

Наследование настроек групповых политик родительского контейнера дочерним контейнером, с которым связан собственный объект групповой политики, может иметь место только в случае совместимости этих групповых политик. Например, если политика родительского контейнера задает определенную конфигурацию рабочего стола компьютера пользователя, а политика дочернего контейнера дополняет ее, пользователь увидит на своем рабочем столе все элементы, заданные обеими политиками. Если же групповая политика родительского контейнера противоречит групповой политике дочернего контейнера, выполняются только настройки GPO, связанного с дочерним контейнером.

Рекомендации по использованию

Для именования объектов групповых политик используйте информативные, содержательные имена. Это поможет вам быстро определить, зачем нужна та или иная политика. Если либо пользовательский, либо компьютерный раздел политики не содержит настраиваемых параметров, отключите обработку этого раздела. Этим вы сократите время обработки политики и снизите нагрузку на сервер. Используйте механизмы *Block Inheritance* (блокирование наследования) и *No Override* (не отменять) с большой осторожностью. В рабочих средах, в которых эти возможности используются слишком часто, становится сложно решать проблемы, связанные с применением политик. Если грамотно спроектировать архитектуру групповых политик вашей сети, можно вообще обойтись без использования этих возможностей.

Создадим политику подключения сетевого диска «P - Общий ресурс компании» со ссылкой на пространство имён DFS («\\company.local\Public») всем пользователям домена.

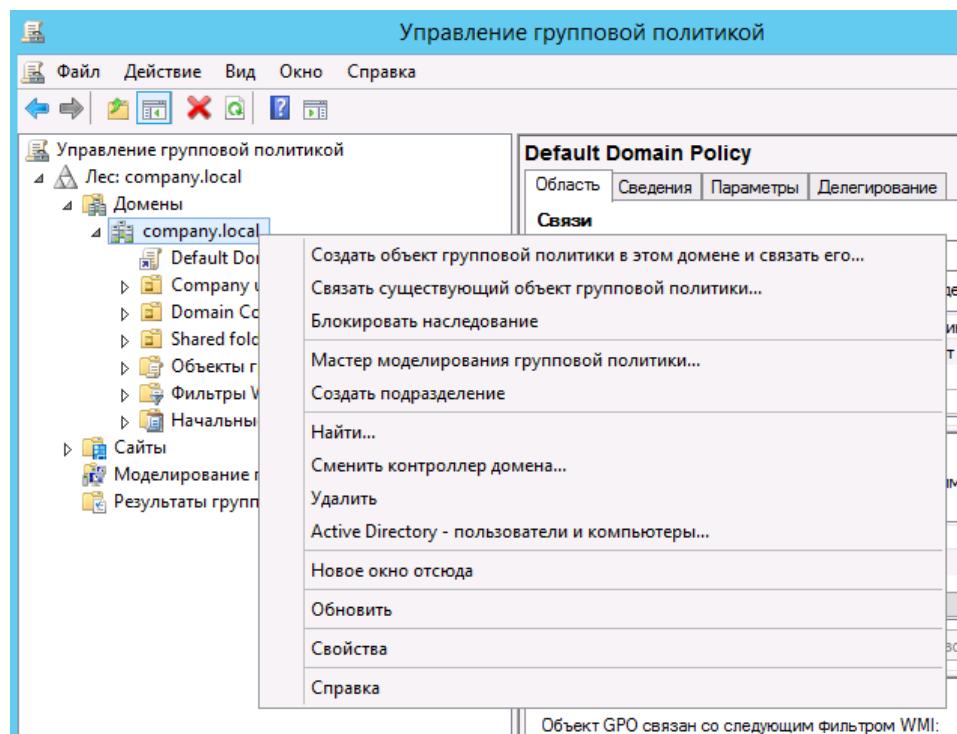
Потребность использования данной политики (GPO) возникает в связи с необходимостью подключения различных сетевых дисков большому количеству пользователей в сети. Так как процесс подключения сетевых дисков каждому пользователю отдельно достаточно трудоемкий, мы используем GPO.

Для начала создадим новую групповую политику.

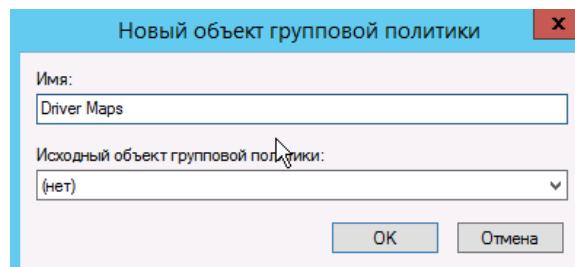
Заходим в панель управления групповыми политиками, она находится в следующем местоположении:

Панель управления\Администрирование\Управление групповой политикой

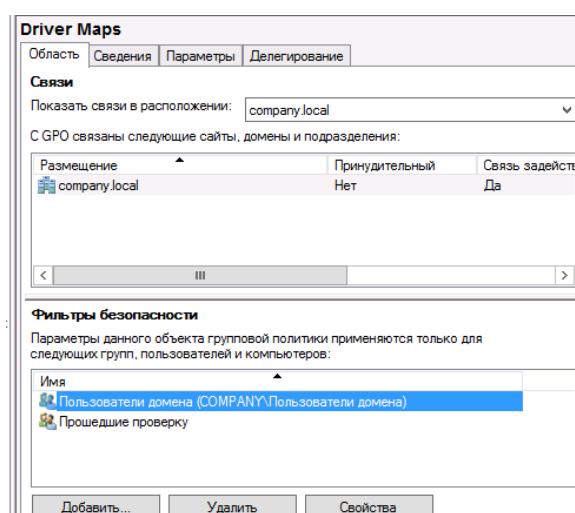
В появившемся окне нажимаем правой кнопкой мыши на домене (company.local), к которому будет применяться наша политика, и выбираем «**Создать объект групповой политики в этом домене и связать его...**»



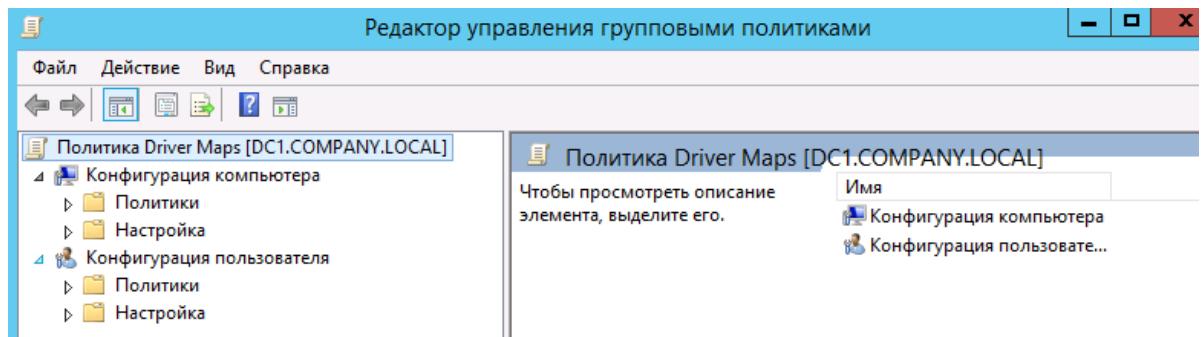
Присваиваем имя для объекта групповой политики – «Driver maps»



Настраиваем доступ (Для кого будет применяться данная политика).
В фильтрах безопасности нажимаем «Добавить». Появляется окно, в котором необходимо ввести: Пользователи домена. Таким образом, мы добавим всех пользователей нашего домена.

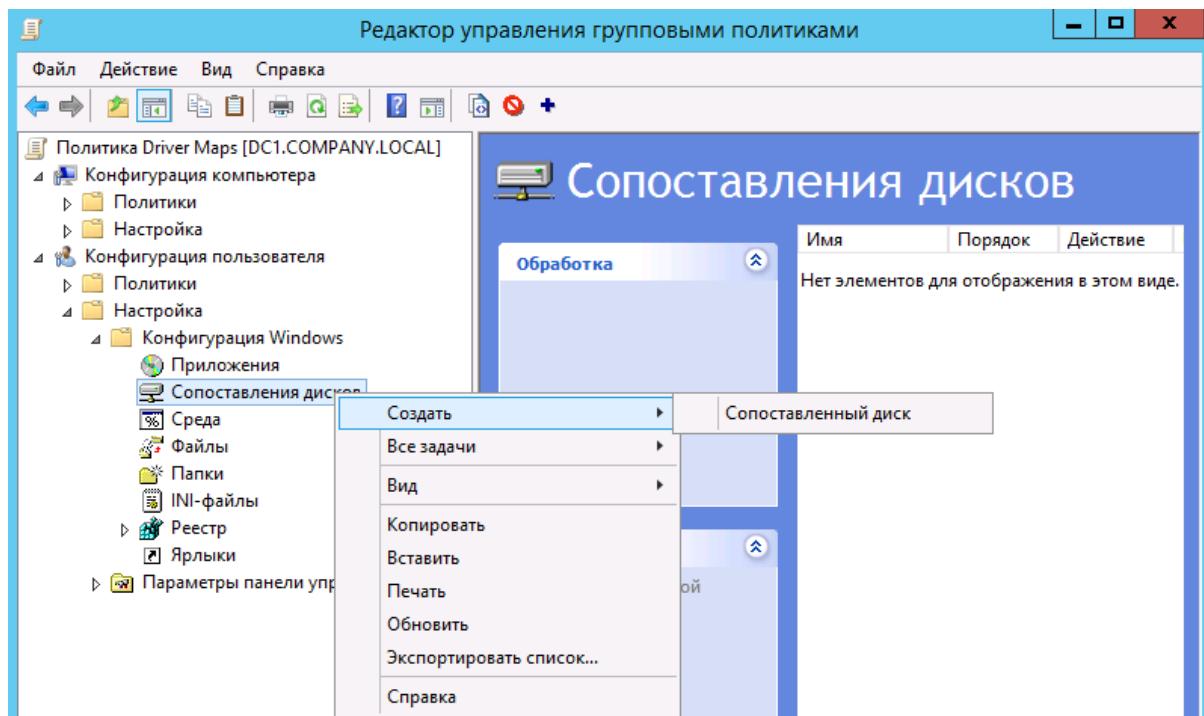


Далее для изменения нужных нам параметров самой политики, нажимаем правой кнопкой на созданном объекте групповой политики (Driver Maps) и выбираем «Изменить». Появится окно «Редактор управления групповыми политиками»



В появившемся окне переходим по следующему пути:
Конфигурация пользователя\Настройка\Конфигурация Windows\Сопоставления дисков

Правой кнопкой мыши нажимаем на «Сопоставления дисков» выбираем действие «Создать-Сопоставленный диск». Появляется окно, в котором вводим следующие данные: «Действие» — «Создать» - «Сопоставленный диск»



Заполняем необходимые поля:

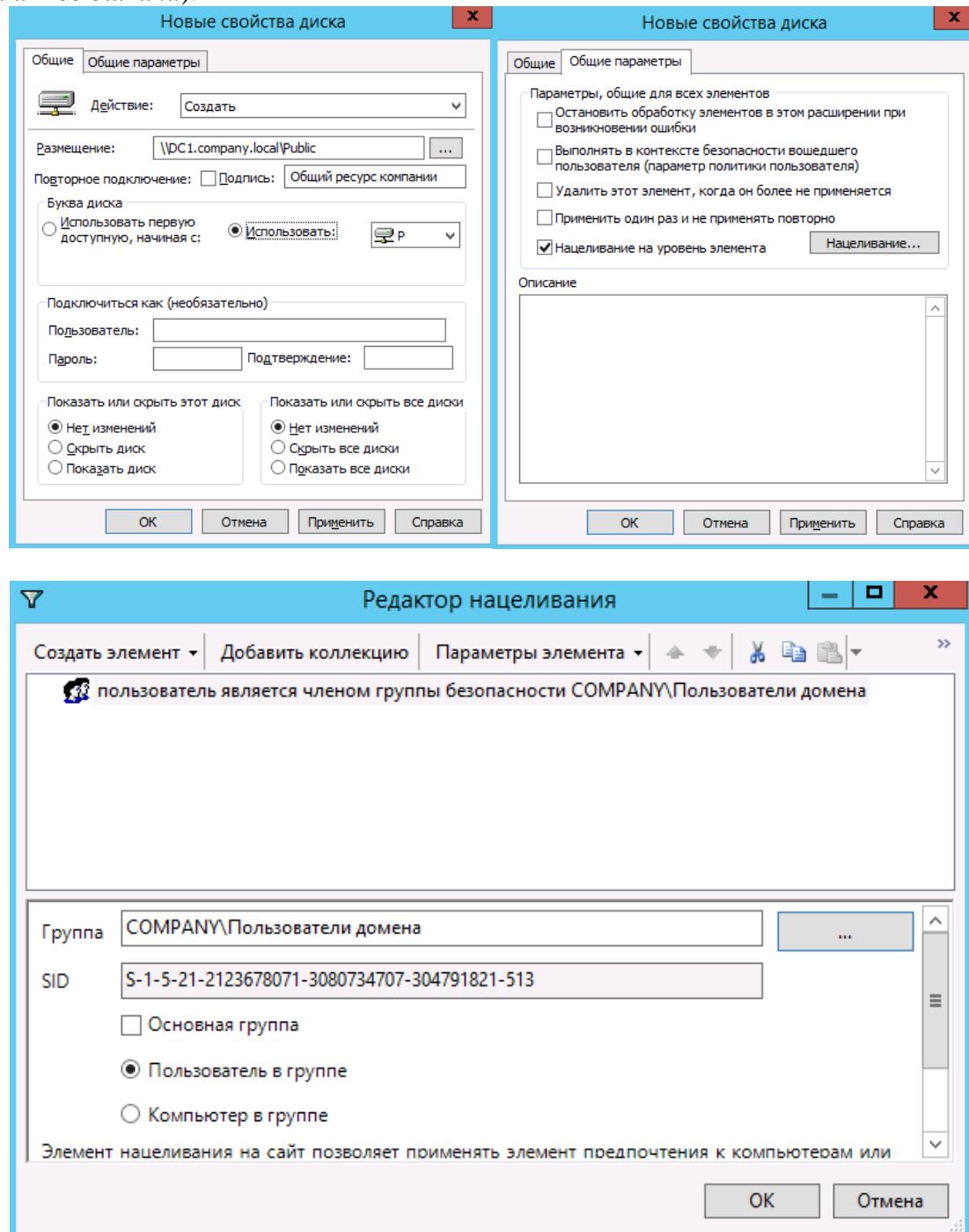
- «Размещение» - тут укажем созданный нами ранее путь к пространству имён DFS «\\company.local\\Public\\».
- Буква диска – используем букву «P» (Public)
- Подпись – Общий ресурс компании

Больше никаких параметров на вкладке общие трогать не будем.

Перейдём на вкладку «Общие параметры» и установим галочку в пункте «Нацеливание на уровень элемента». Далее перейдём к настройкам «Нацеливание..»

Нажимаем на кнопку: «создать элемент» - «пользователь является членом группы безопасности», в поле «Группа» выбираем – «Пользователи домена». Нажимаем ОК. Нажимаем применить.

Управляя настройками «Наследования» можно назначить объектов, к которым будет применяться эта политика. Таким образом выбрав там, например, группу «Вин» мы бы применили эту политику только к сотрудникам входящим в эту группу (бухгалтерами Жигурда и Федюшкина).



На этом настройка политики подключения сетевого диска закончена.

Теперь необходимо применить политику на компьютере или в домене. Это можно сделать несколькими способами:

- Через средства командной строки «GPUpdate» или «GPUpdate /force»

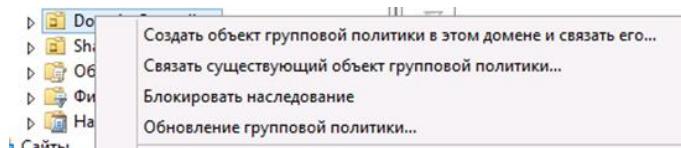
GPUpdate применяет все новые и измененные политики.

GPUpdate /force применяет все политики: новые и старые.

В 99% случаев стоит использовать GPUpdate. Если Вы только что отредактировали политику и хотите видеть результат, запустите GPUpdate.

На самом деле, использование /force на большом количестве компьютеров вредит вашей карьере. Потому что эти машины бомбят контроллер домена и запрашивают каждую политику, относящуюся к ним.

- Через интерфейс, нажав правой кнопкой на объекте и вызвать GPUpdate удаленно. Данная функция появилась с версии Server 2012.



Давайте применим политику через средства командной строки «GPUpdate»

A screenshot of a Windows Command Prompt window titled "Администратор: Командная строка". The window shows the command "C:\>GPUpdate" being run. The output indicates that the update is in progress: "Выполняется обновление политики...". After the update completes, the message "Обновление политики для компьютера успешно завершено." and "Обновление политики пользователя завершено успешно." is displayed.

2.5 Создание Перемещаемые профили (Перенаправление папки «Мои документы» и «Рабочий стол»)

Перемещаемый профиль пользователя — технология, используемая в семействе операционных систем Microsoft Windows, которая позволяет пользователям, подключенным к домену Windows Server, при входе в операционную систему с различных компьютеров локальной сети, получить доступ к своему профилю. Загружаемый профиль пользователя включает настройки программ, документы, ветви реестр и рабочее окружение, в том числе расположение иконок на рабочем столе и прочие настройки. При выходе из системы все измененные настройки профиля и документы синхронизируются с сервером.

Перемещаемый профиль загружается на компьютер, с которого пользователь входит в домен Active Directory. При выходе пользователя из системы изменения в профиле синхронизируются с копией, находящейся на сервере. Если вход в домен невозможен, используется сохранённый локально при предыдущем входе в систему (кэшированный) профиль, который может не содержать последних изменений, или создаётся временный профиль.

Преимущества использования перемещаемых профилей:

- *перемещаемый профиль позволяет пользователю автоматически получать доступ к своим данным с любого сетевого компьютера, входящего в домен;*

- *использование перемещаемых профилей упрощает резервное копирование данных пользователей;*
- *при замене компьютера нет необходимости сохранять документы и настройки пользователя, при входе в домен они автоматически загружаются на новый компьютер.*

Недостатком перемещаемых профилей является создаваемый при их использовании дополнительный сетевой трафик и увеличение времени входа в систему и выхода из системы, хотя сейчас в век скоростного интернета и гигабитной интрасети сетей это не является проблемой.

Приступим к созданию политики. Создадим новый объект групповой политики с именем «Roaming User Profile» в подразделении «Company Users».

Настраиваем доступ (Для кого будет применяться данная политика).

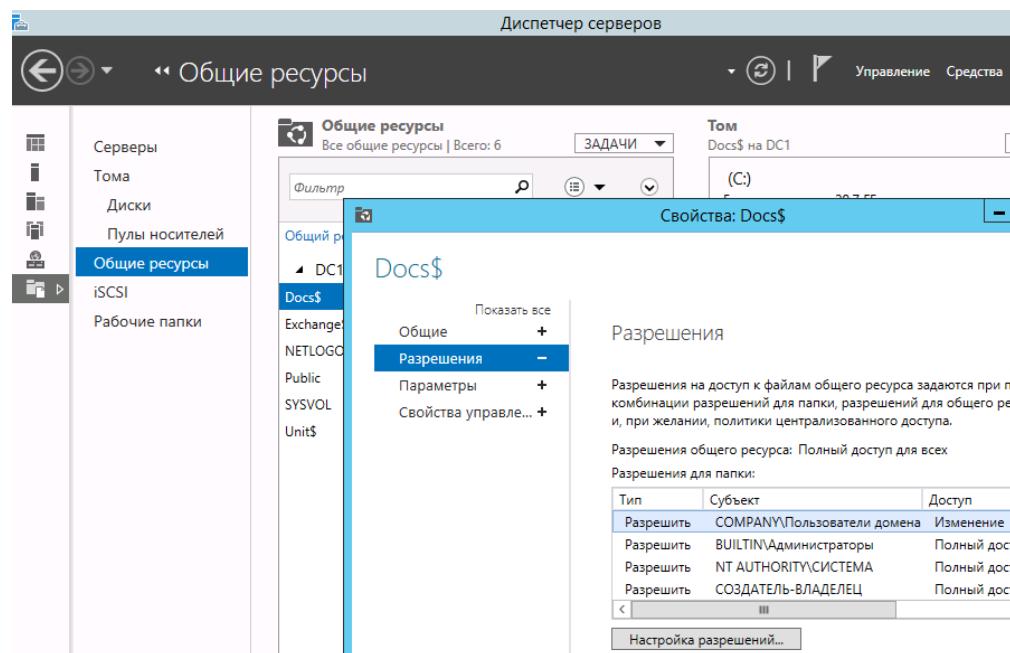
В фильтрах безопасности нажимаем «Добавить». Появляется окно, в котором необходимо ввести: Пользователи домена.

Далее для изменения нужных нам параметров самой политики, нажимаем правой кнопкой на созданном объекте групповой политики (Roaming User Profile) и выбираем «Изменить». Появится окно «Редактор управления групповыми политиками»

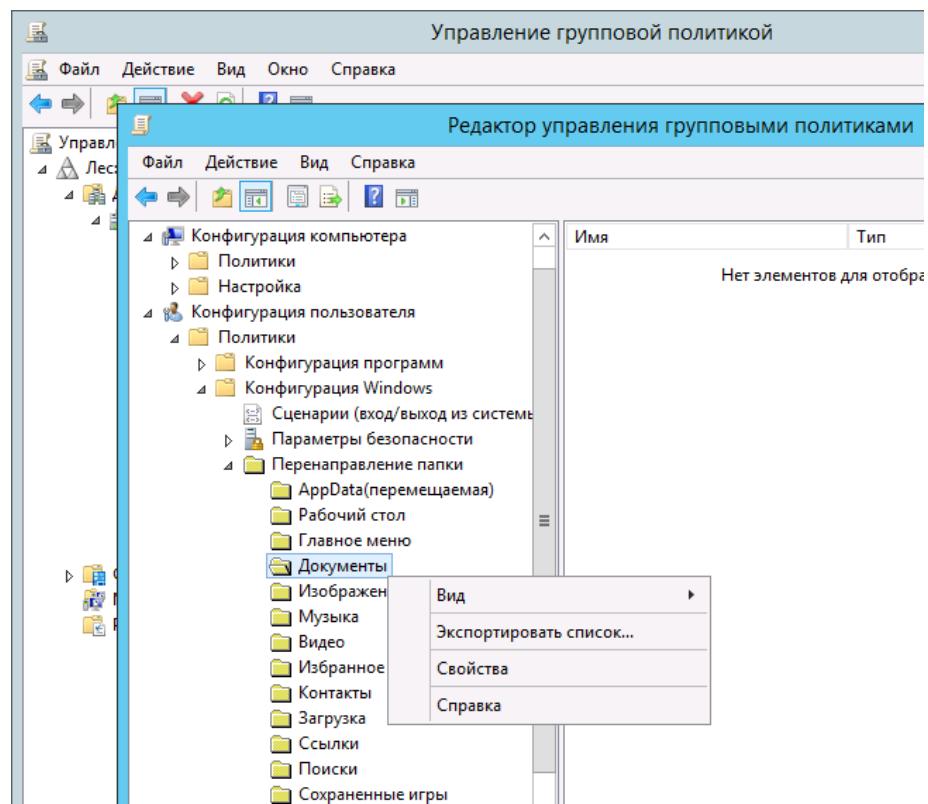
В появившемся окне переходим по следующему пути:

Конфигурация пользователя\Политики\Конфигурация Windows\Перенаправление папки

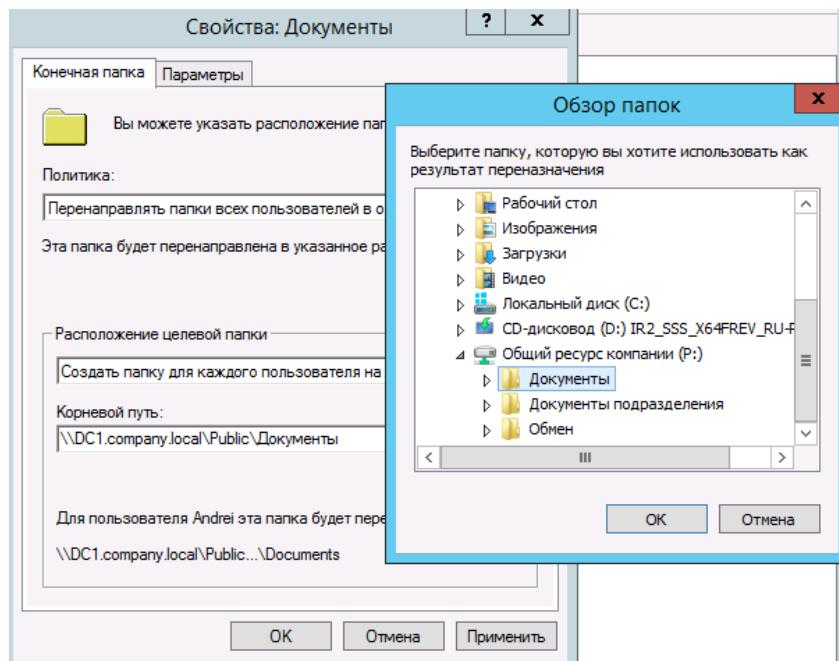
Так как папка для перемещения документов пользователей (Docs\$) была создана ранее, нам необходимо только проверить, что пользователи домена имеют к ней доступ на чтение и запись. Если это не так, то необходимо сделать это!



Выбираем папки, которые будут храниться на сервере, в нашем случае это папка «Мои Документы». Через меню правого клика выбираем «Свойства».

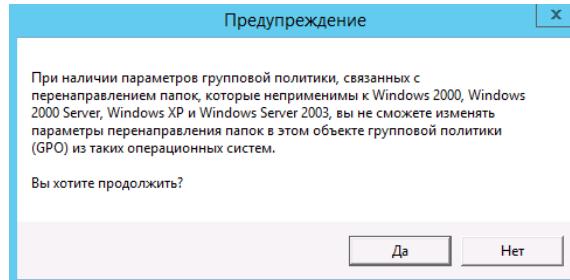


Настраиваем перенаправление:



Обратите внимание на то, что мы указали для перенаправления ссылку DFS. А не локальный путь к папке на сервере. Благодаря этому мы при необходимости сможем менять физическое расположение документов, не изменяя политики перенаправления папок. Это очень удобно.

Соглашаем с предубеждением о том, что данная политика может не корректно применится на компьютерах под управлением старых операционных систем, таких как Windows XP, Windows 2000 и так далее.



Теперь, когда политика создана необходимо выполнить её обновление (применения).

2.6 Создание Установить в виртуальную среду (VirtualBox) Windows 7.

Установить в виртуальную среду (VirtualBox) Windows 7.

- Ввести компьютер в домен
- Проверить работу политик
- Проверить работу папок общего доступа

ЛАБОРАТОРНАЯ РАБОТА №3 АДМИНИСТРИРОВАНИЕ WINDOWS SERVER 2012 R2. ЧАСТЬ 3

1. Цель работы

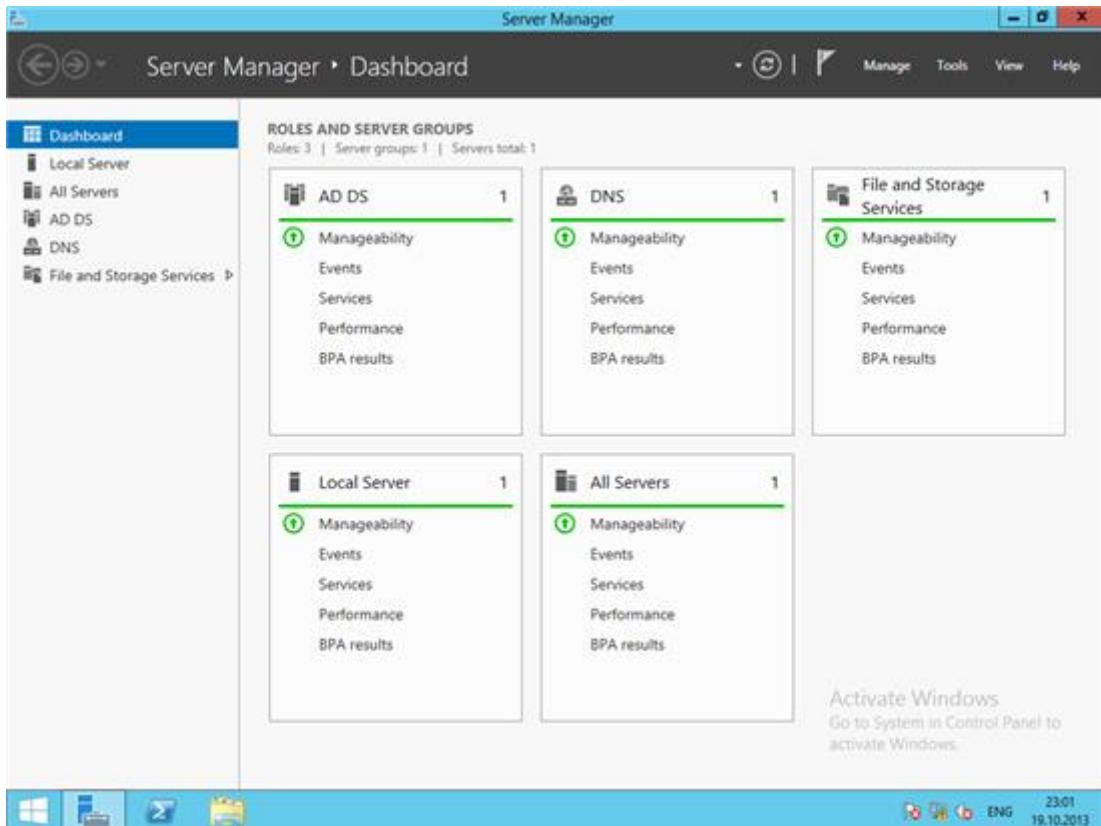
1. Изучить установку служб удаленных рабочих столов на контроллере домена в Windows Server 2012 R2.
2. Изучить установку служб IIS на Windows Server 2012 с помощью пользовательского интерфейса.

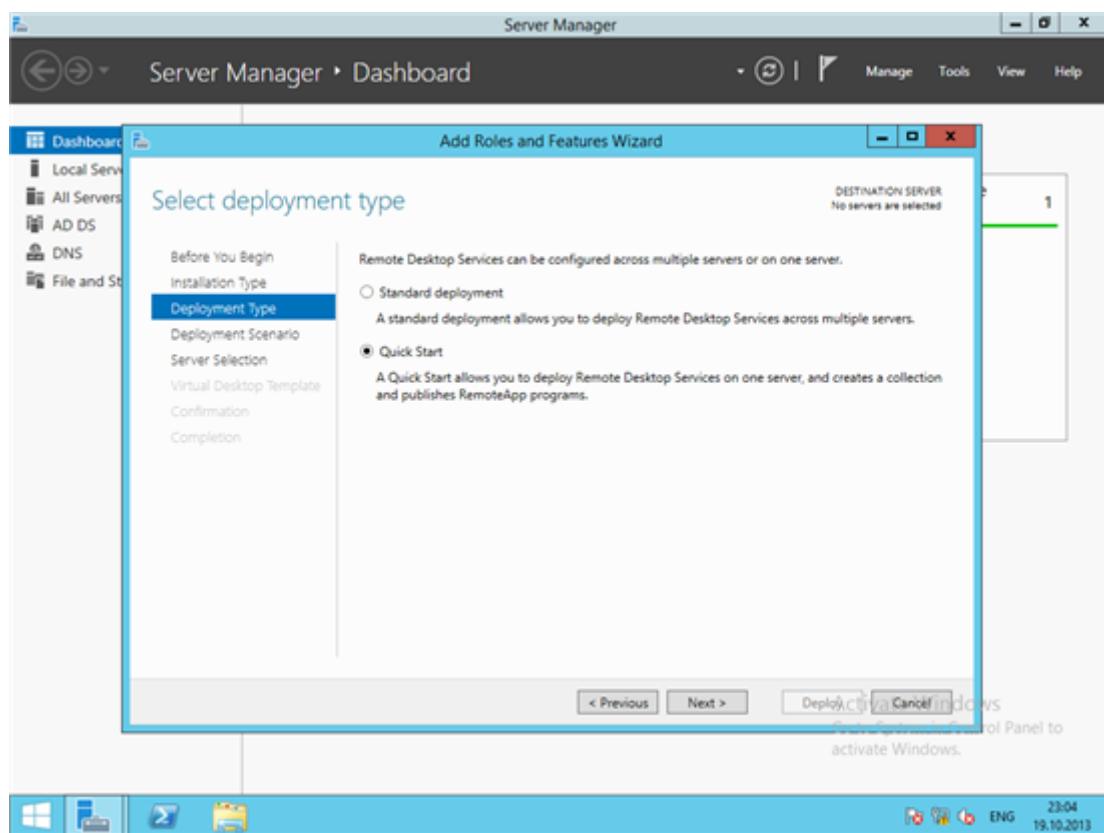
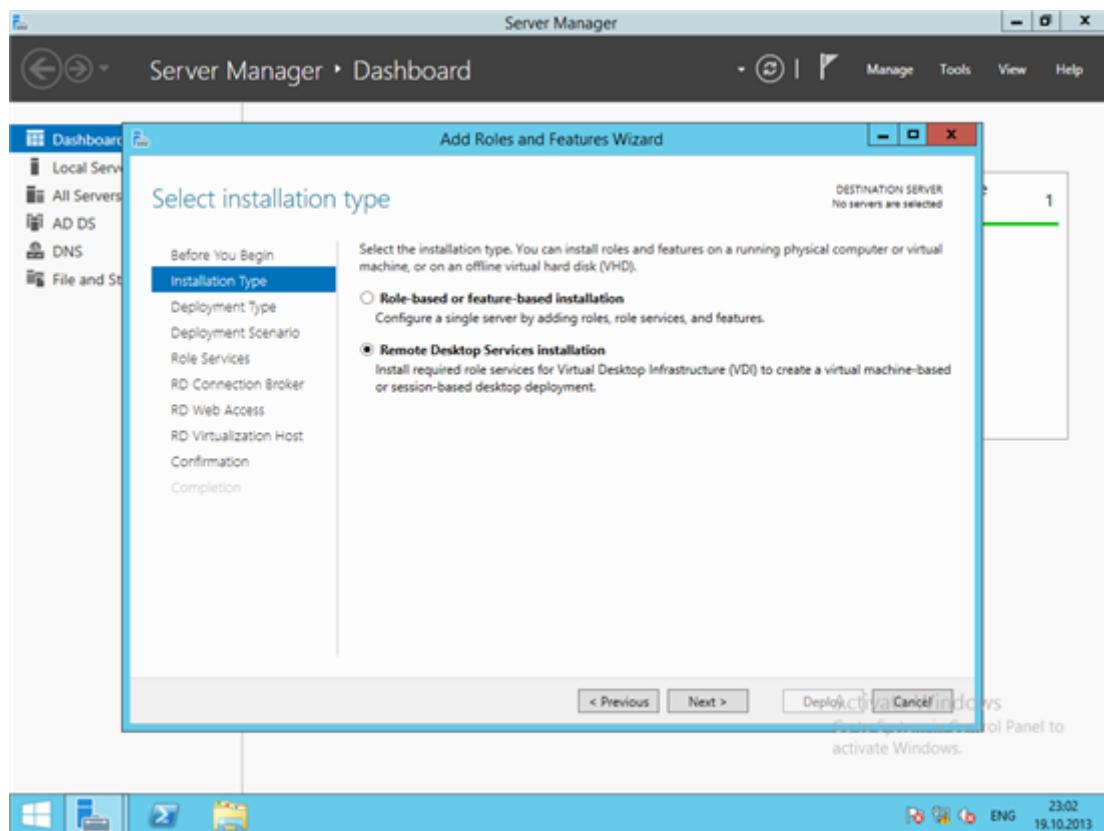
2. Общие сведения

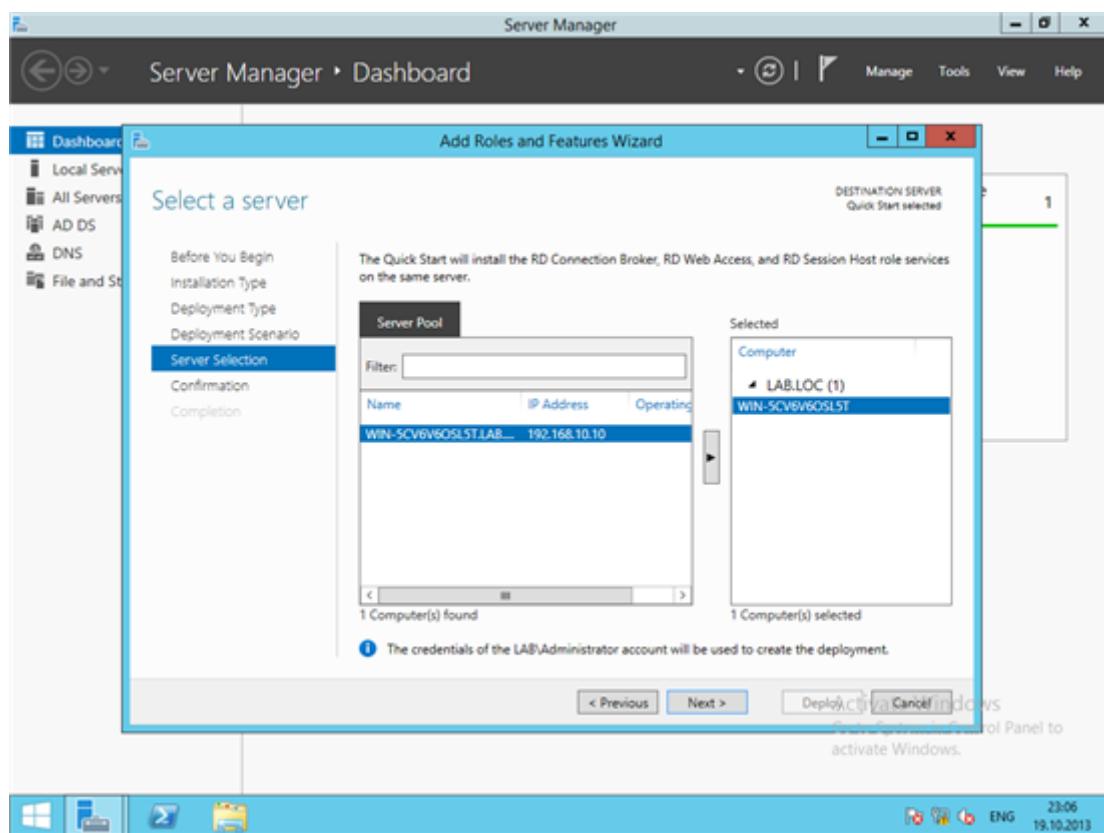
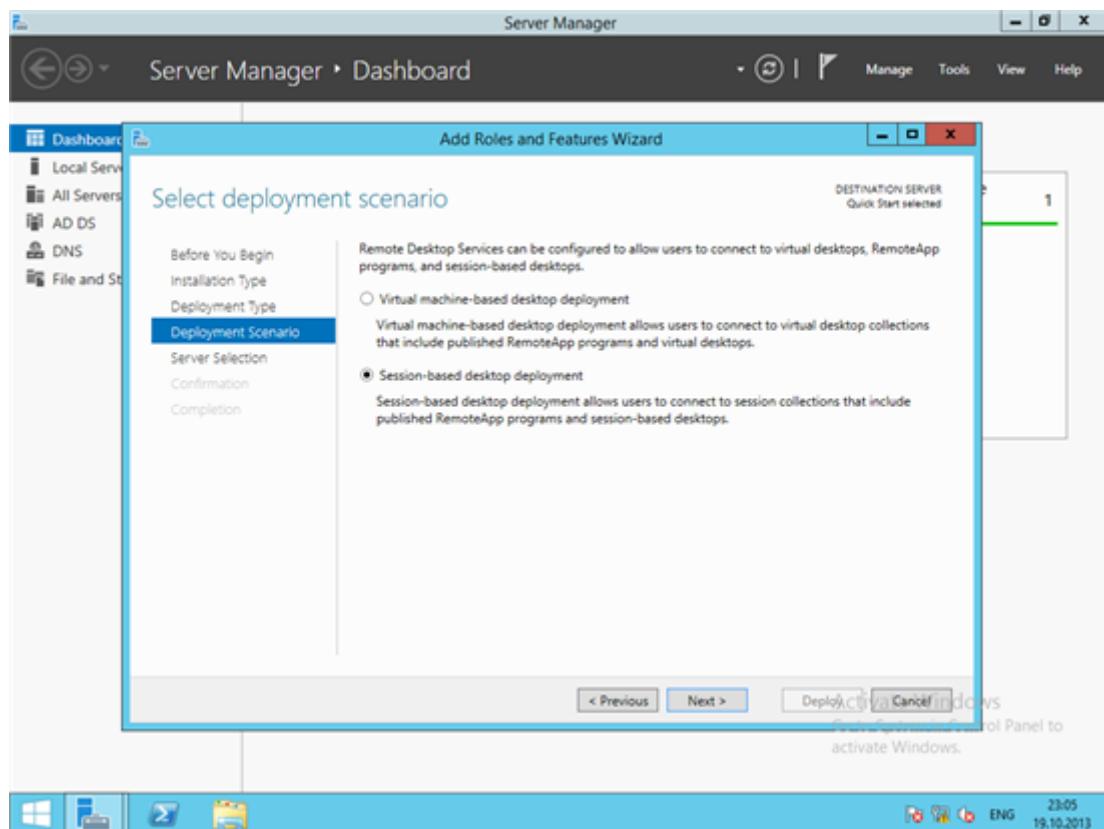
2.1 Windows Server 2012 R2: Установка служб удаленных рабочих столов на контроллере домена

В Windows Server 2012 R2 появилась новая возможность, теперь можно развернуть на действующем контроллере домена службы удаленных рабочих столов штатным способом. Очевидно, этот сценарий установки будет востребован предприятиями малого бизнеса, которые ограничены в количестве физических серверов.

Ниже, на скриншотах, показан процесс установки Служб удаленных рабочих столов с использованием мастера. Установка в Windows Server 2012 R2 на контроллере домена производится с использованием службы посредника подключений к удаленному рабочему столу (Remote Desktop Connection Broker).



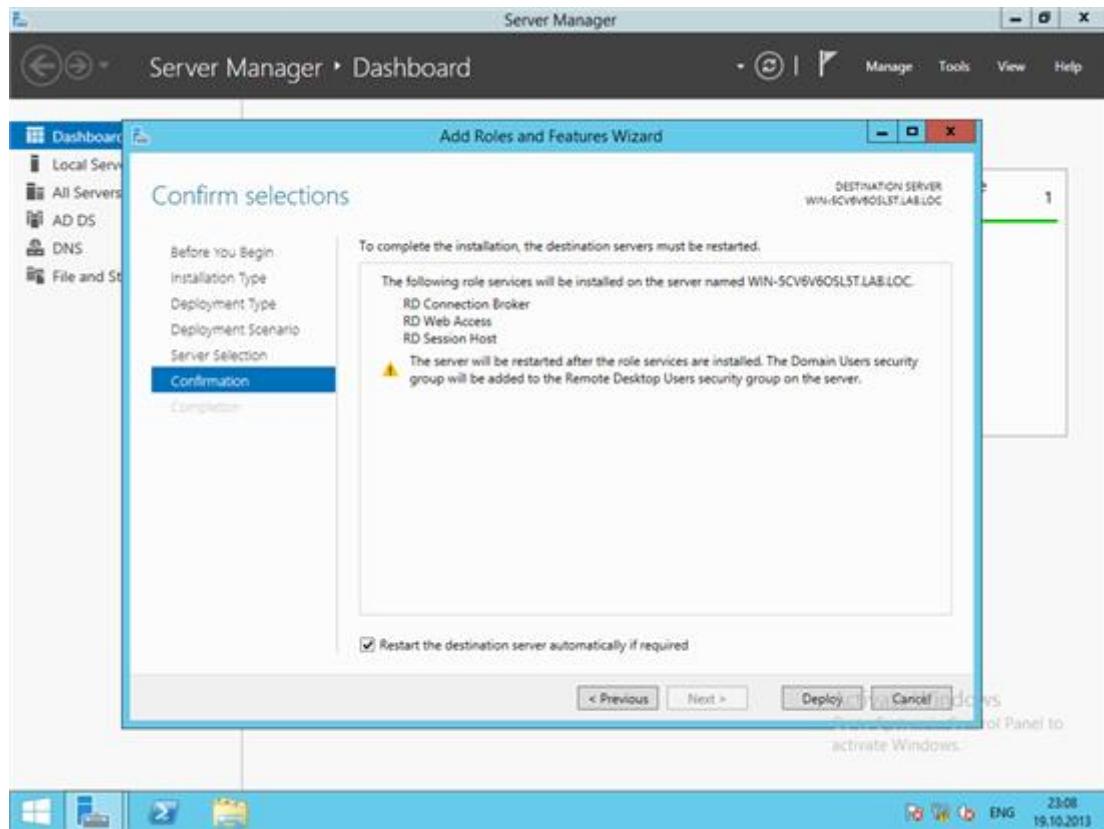




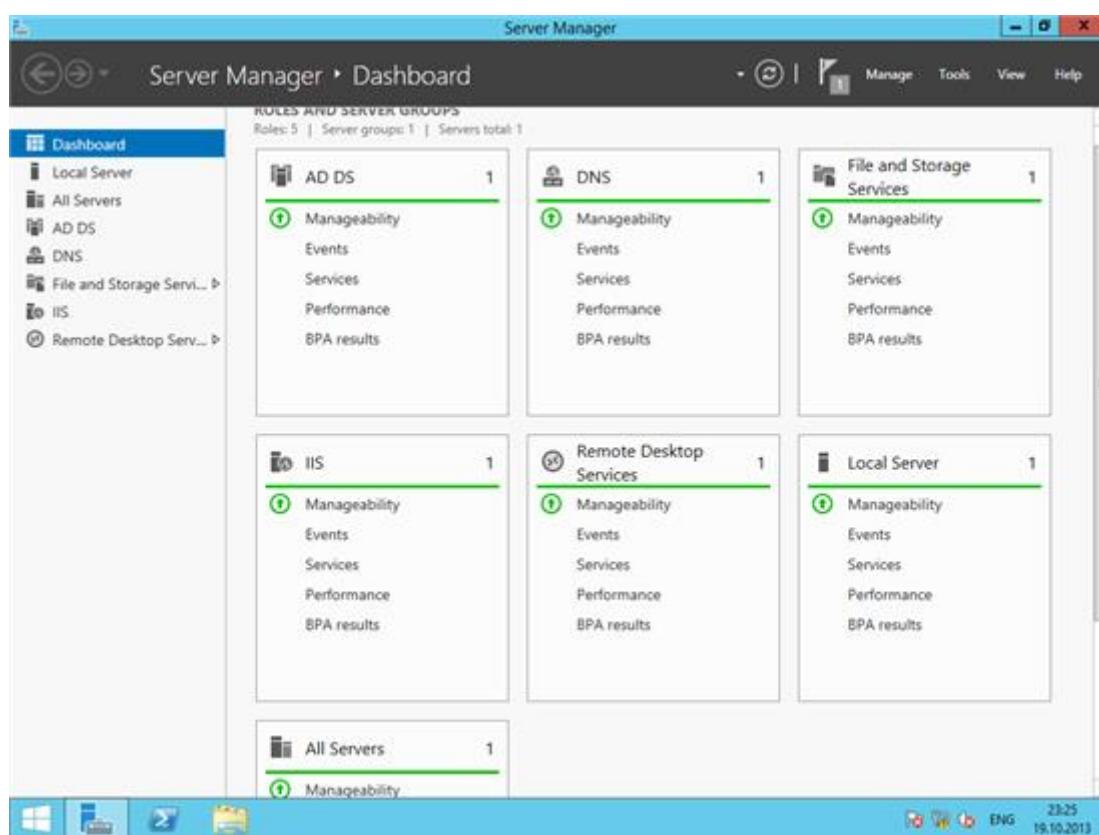
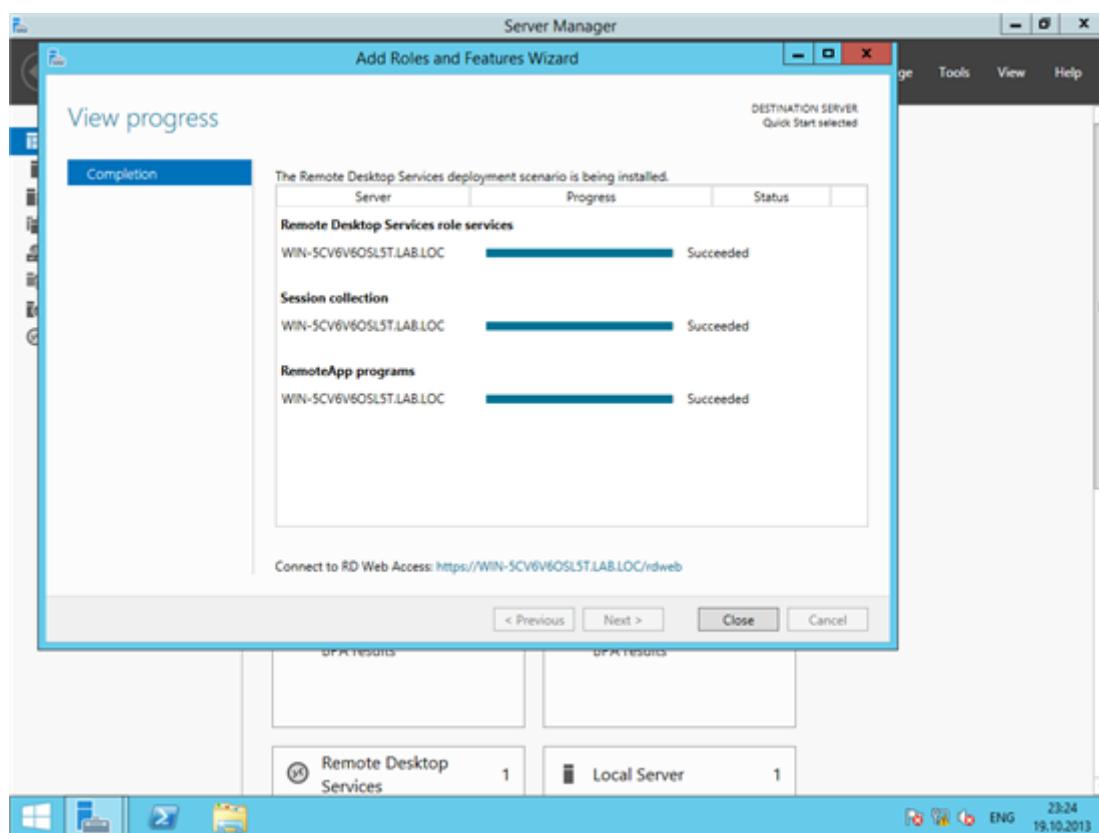
Видно, что процесс установки ничем не отличается от процесса установки, который использовался на рядовых серверах с Windows Server 2012, выделенных для обеспечения работы

терминальных

служб.

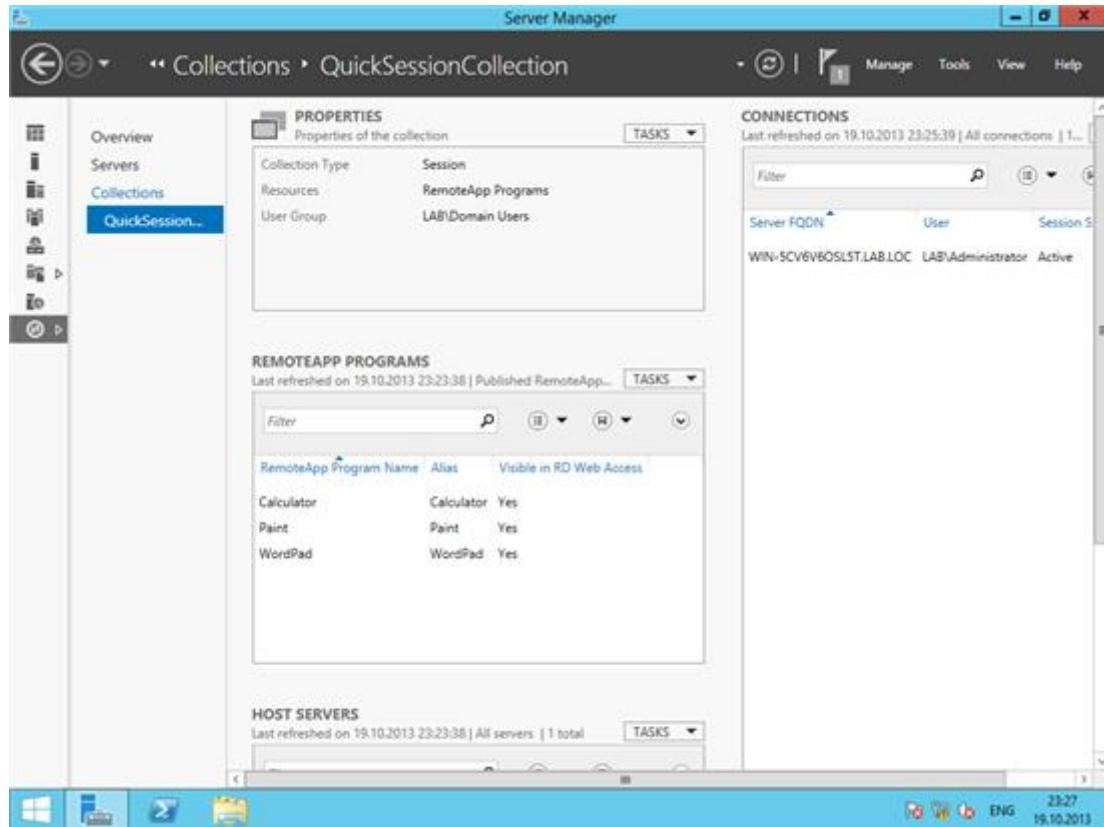


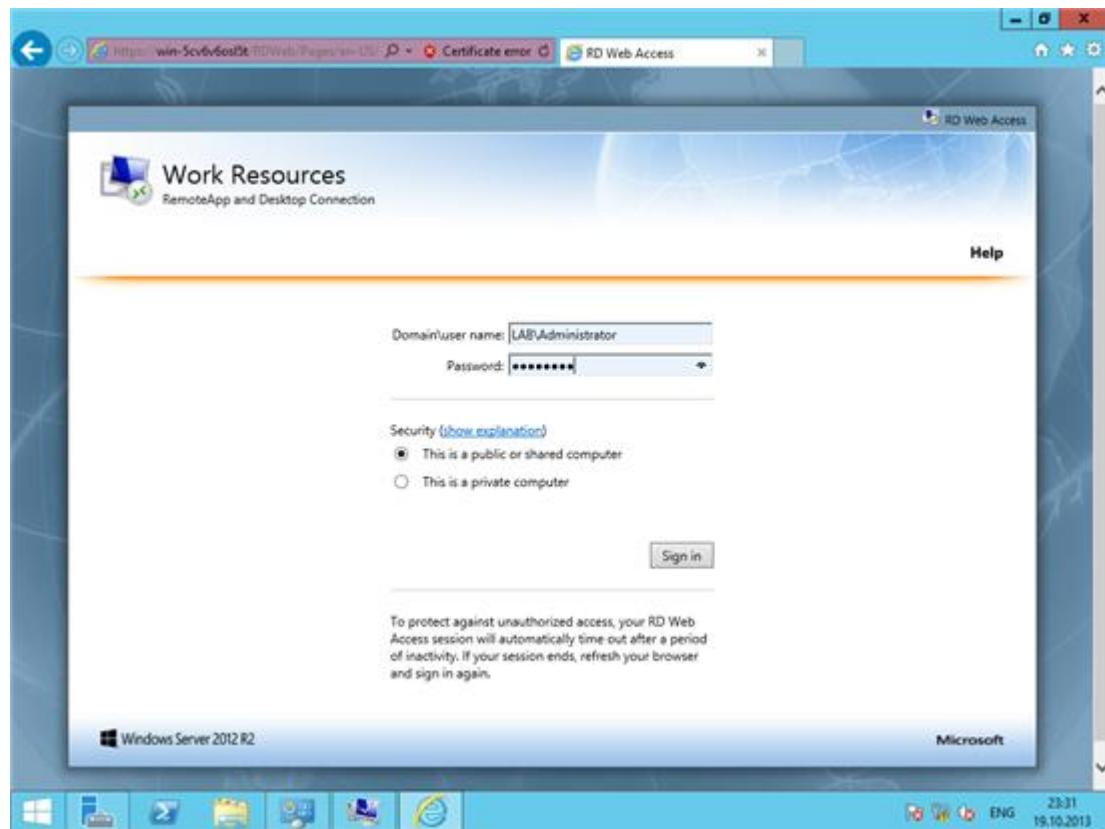
После перезагрузки сервера дождитесь окончания установки. Если установка закончилась успешно, проверить работу Служб удаленных рабочих столов можно перейдя по ссылке в мастере - <https://servername/rdweb>



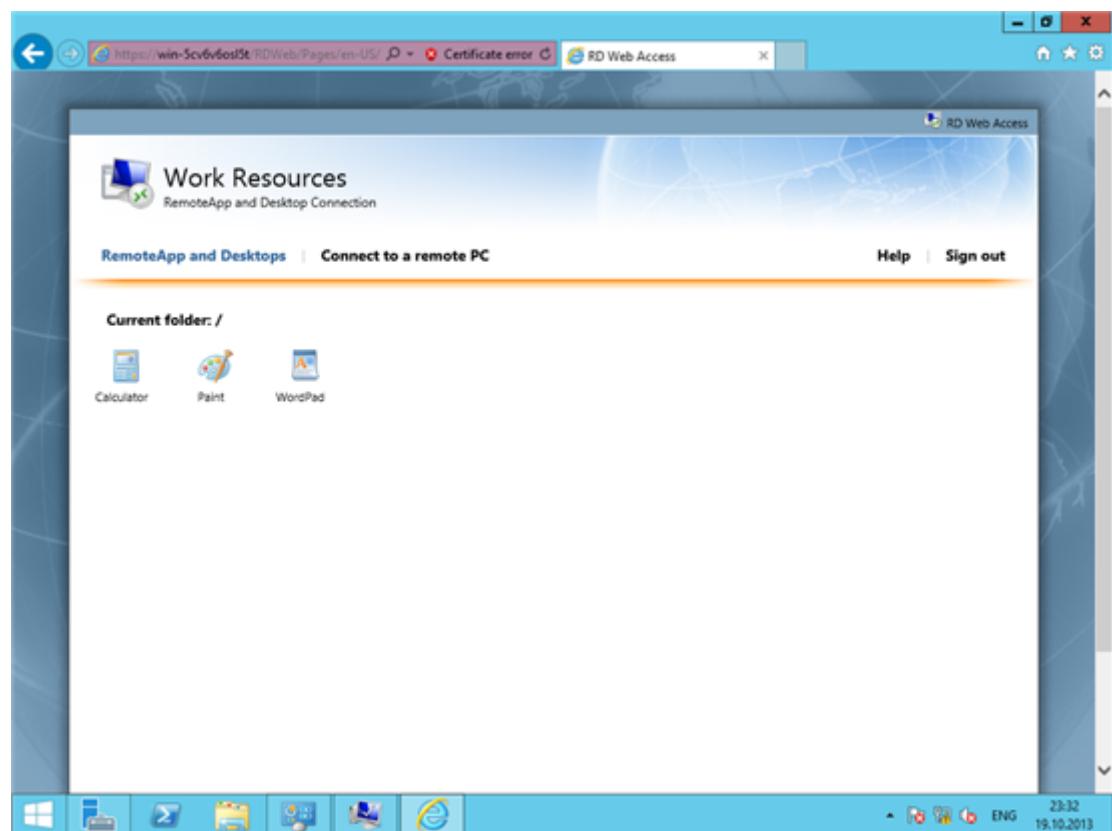
После успешной установки, в Диспетчере серверов появляются инструменты управления,

которые потребуются для дальнейшего администрирования роли терминального сервера.





Как видно на скриншоте, служба RD Web Access работает также безупречно.



2.2 Установка служб IIS на Windows Server 2012 с помощью пользовательского интерфейса

1. На **начальной** странице щелкните заголовок **Диспетчер сервера**, затем нажмите кнопку **OK**.
2. В поле **Диспетчер сервера** выберите **Панель мониторинга** и выберите **Добавить роли и компоненты**.
3. В **мастере добавления ролей и компонентов** на странице **Перед началом** нажмите кнопку **Далее**.
4. На странице **Выбор типа установки** выберите **Установка на основе ролей или компонентов** и нажмите кнопку **Далее**.
5. На странице **Выбор целевого сервера** выберите **Выбор сервера из пула серверов**, выберите имя своего компьютера и нажмите кнопку **Далее**.
6. На странице **Выбор ролей сервера** укажите **Веб-сервер (IIS)** и нажмите кнопку **Далее**.
7. На странице **Выбор компонентов** просмотрите выбранные по умолчанию компоненты, а затем нажмите кнопку **Далее**.
8. На странице **Роль веб-сервера (IIS)** нажмите кнопку **Далее**.
9. На странице **Выбор служб ролей** просмотрите выбранные службы и нажмите кнопку **Далее**.
10. На странице **Подтверждение выбранных элементов для установки** подтвердите свой выбор, а затем нажмите кнопку **Установить**.
11. На странице **Ход выполнения установки** убедитесь, что установка роли веб-сервера (IIS) и требуемых служб ролей успешно завершена, а затем нажмите кнопку **Закрыть**.
12. Чтобы убедиться, что службы IIS успешно установлены, введите в веб-браузер следующее:
http://localhost
Должна отобразиться страница приветствия службы IIS по умолчанию.

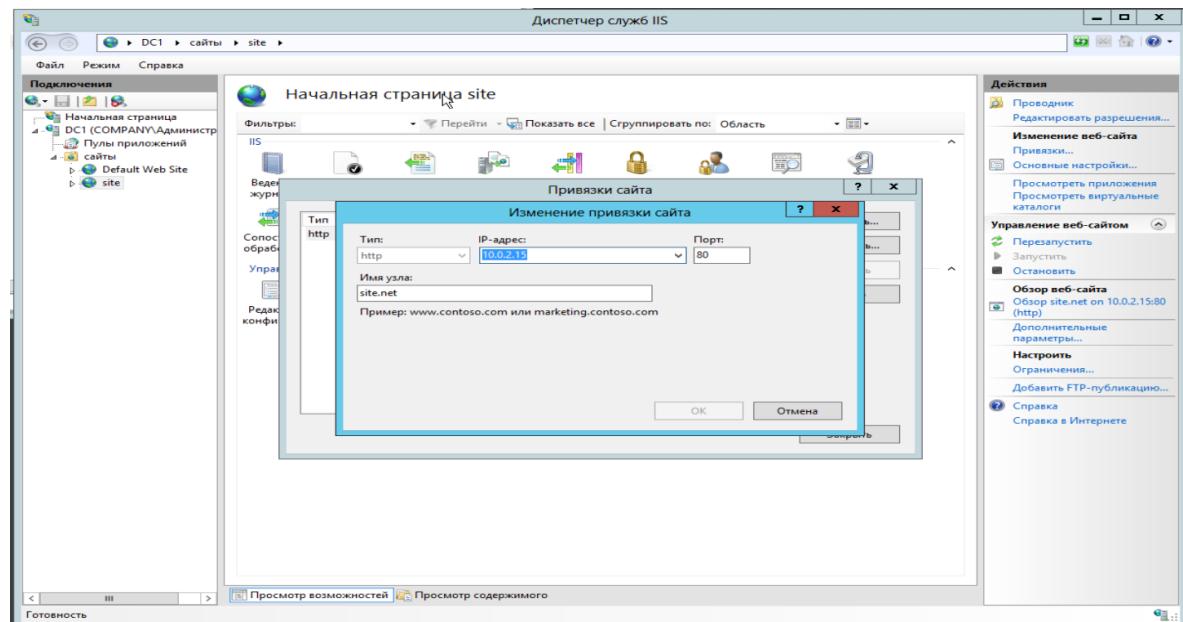
Шаг 2. Добавление веб-сайта

На этом шаге поясняется, как добавить веб-сайт для служб IIS с помощью пользовательского интерфейса диспетчера служб IIS или путем запуска команд Appcmd.exe в окне командной строки.

Добавление веб-сайта с помощью пользовательского интерфейса

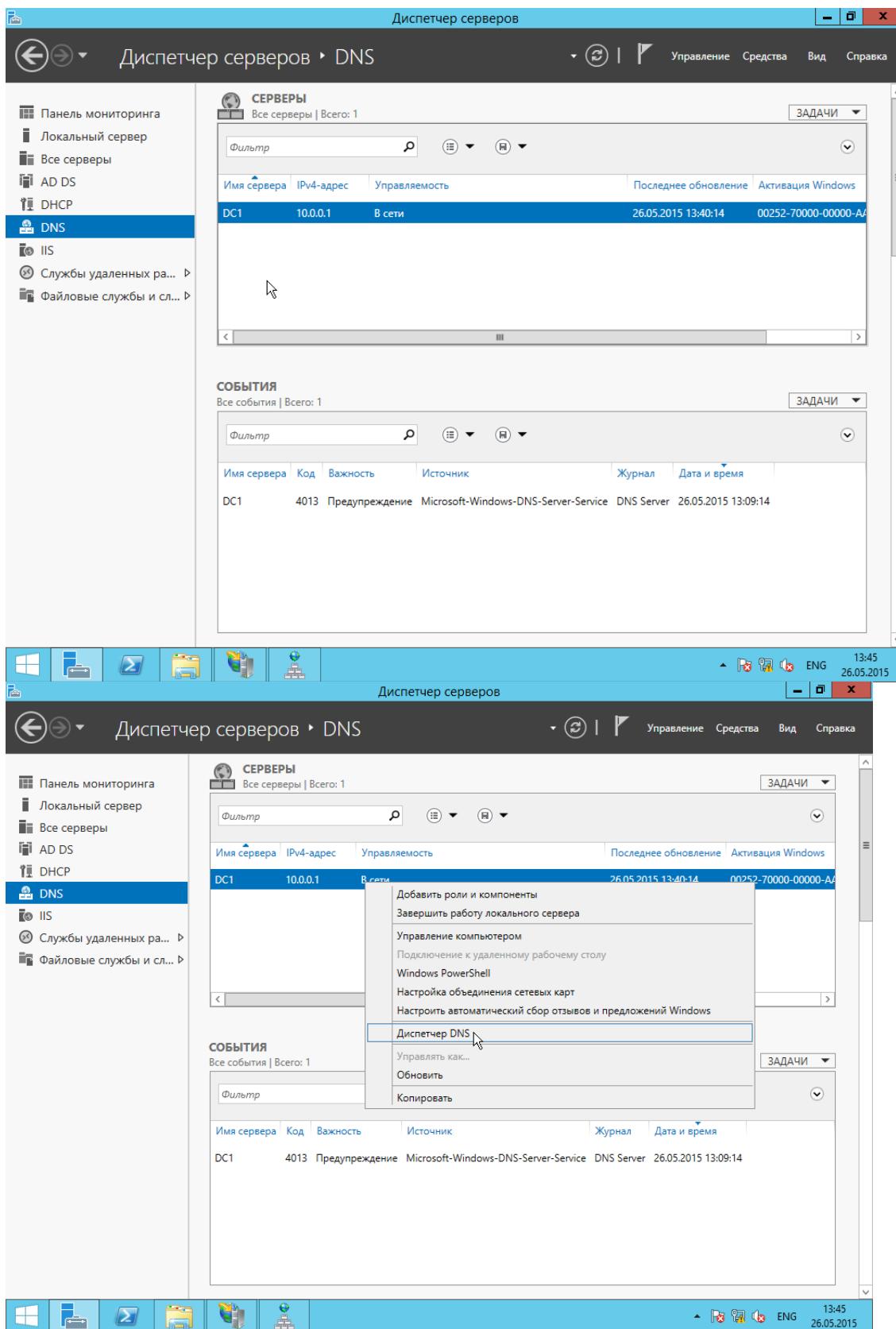
1. Откройте диспетчер служб IIS.
 - При работе в Windows Server 2012 на **начальной** странице щелкните заголовок **Диспетчер сервера**, затем нажмите кнопку **OK**. В **диспетчере сервера** выберите меню **Сервис**, а затем выберите **Диспетчер служб IIS**.
 - При работе в Windows 8 на **начальной** странице введите **Панель управления**, затем щелкните значок **Панель управления** в результатах поиска. На экране **Панель управления** выберите **Система и безопасность**, затем **Администрирование**, после чего выберите пункт **Диспетчер служб IIS**.
2. На панели **Соединения** щелкните правой кнопкой мыши узел **Сайты** в дереве, затем выберите команду **Добавить веб-сайт**.
3. В диалоговом окне **Добавление веб-сайта** в поле **Имя сайта** введите понятное имя веб-сайта.

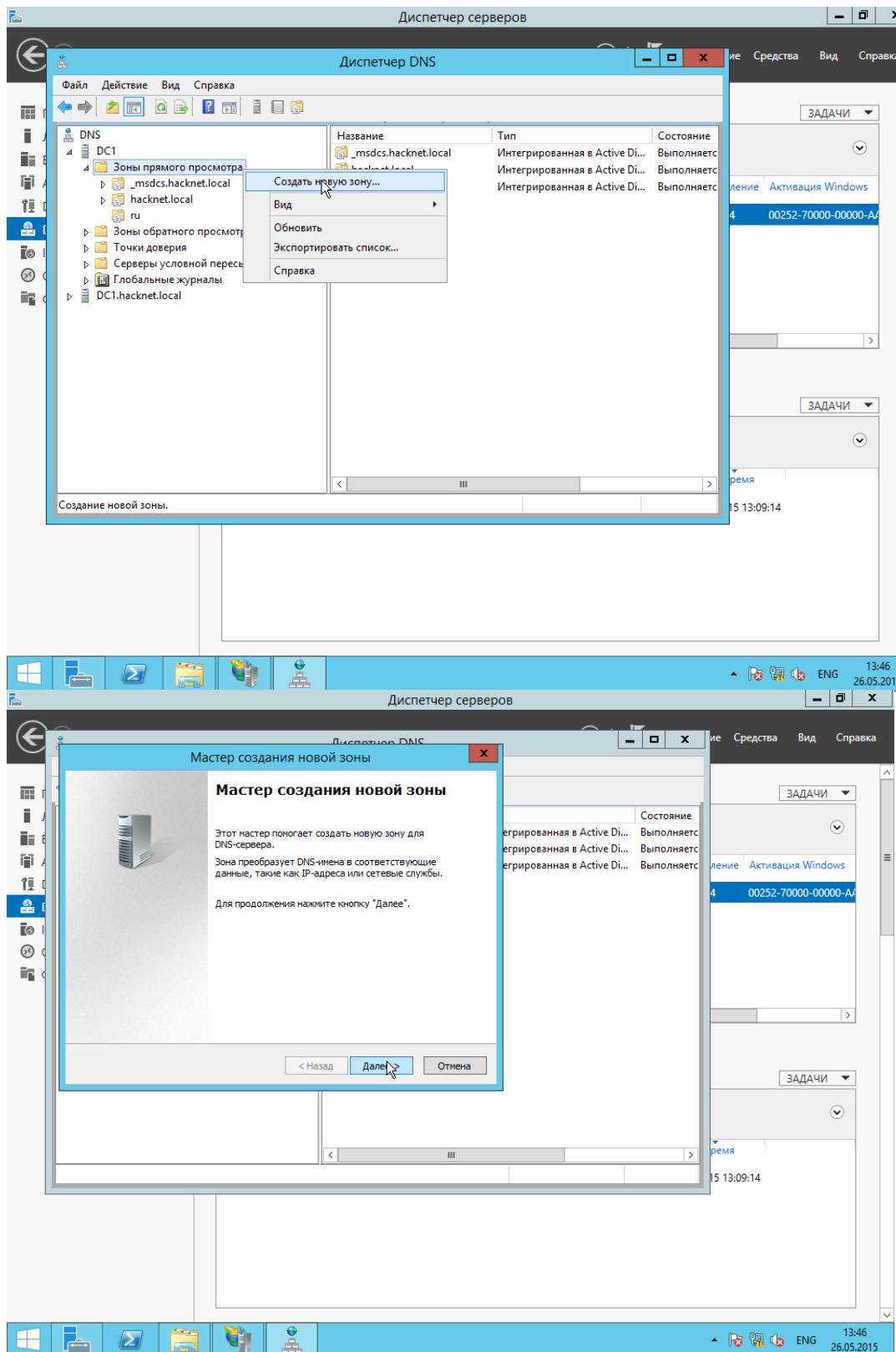
4. Если следует выбрать пул приложений, отличный от пула, указанного в поле **Пул приложений**, нажмите кнопку **Выбрать**. В диалоговом окне **Выбор пула приложений** выберите пул приложений в списке **Пул приложений**, а затем нажмите кнопку **OK**.
5. В поле **Физический путь** введите физический путь к папке веб-сайта или нажмите кнопку обзора (...), чтобы выбрать папку в файловой системе.
6. Если физический путь, указанный в предыдущем шаге, ведет к удаленной общей папке, нажмите **Подключиться как**, чтобы указать учетные данные, имеющие разрешение на доступ к ресурсу по этому пути. Если не используются определенные учетные данные, выберите параметр **Пользователь веб-приложения (сквозная проверка подлинности)** в диалоговом окне **Подключиться как**.
7. В списке **Тип** выберите протокол для веб-сайта.
8. Если необходимо указать статический IP-адрес для веб-сайта (по умолчанию для этого параметра задано **Все неназначенные**), введите IP-адрес в поле **IP-адрес**.
9. В текстовом поле **Порт** введите номер порта.
10. Дополнительно введите имя заголовка узла для веб-сайта в поле **Заголовок узла**.
11. Если не следует вносить изменения в параметры веб-сайта и следует сделать его незамедлительно доступным, установите флажок **Немедленный запуск веб-сайта**.
12. Нажмите кнопку **OK**.
13. Необходимо зайти в Привязки сайта и изменить привязки, как показано на картинке:
14. IP-адрес сервера, имя узла БЕЗ www
15. Зайти в Windows 7 и в браузере запустить сайт

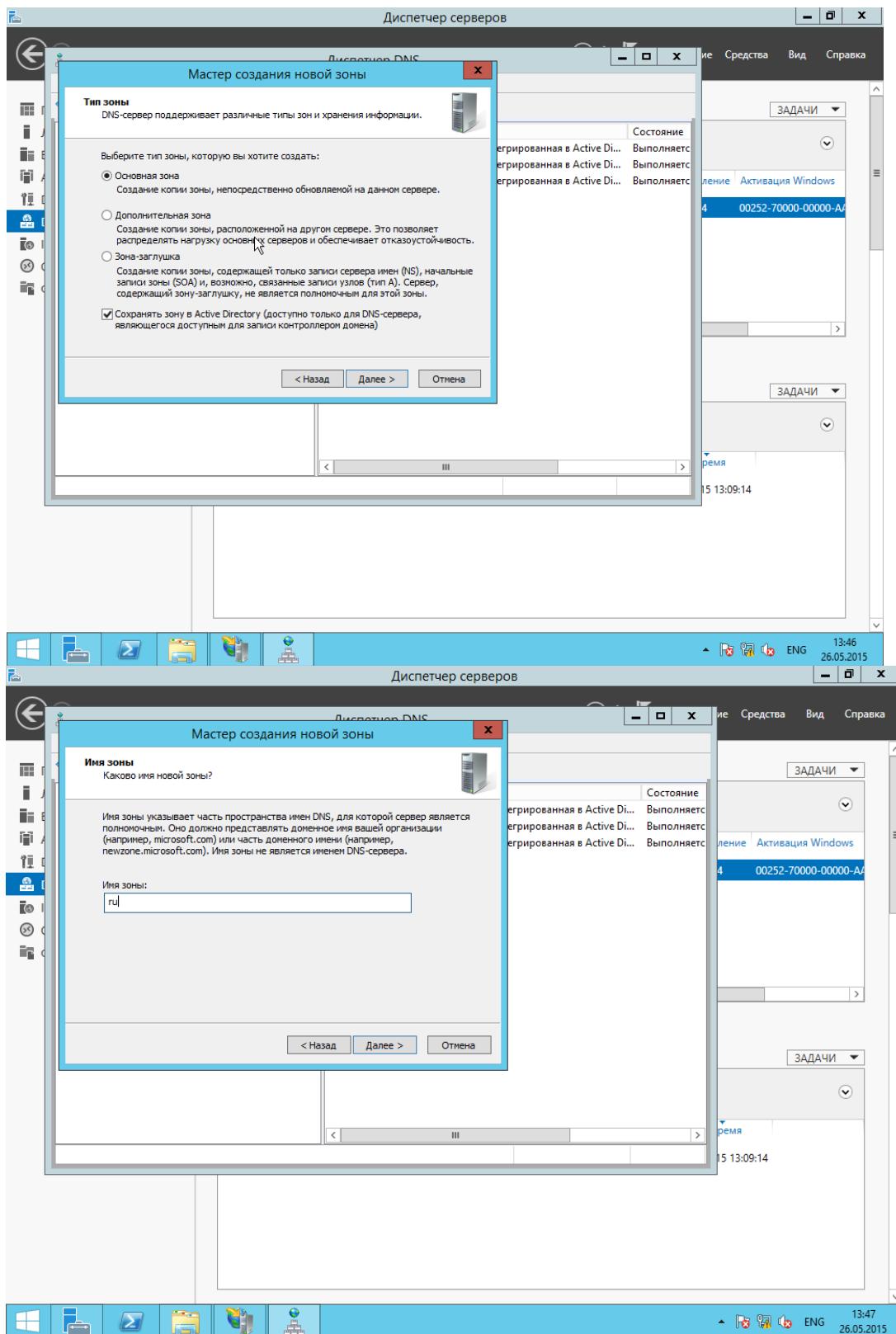


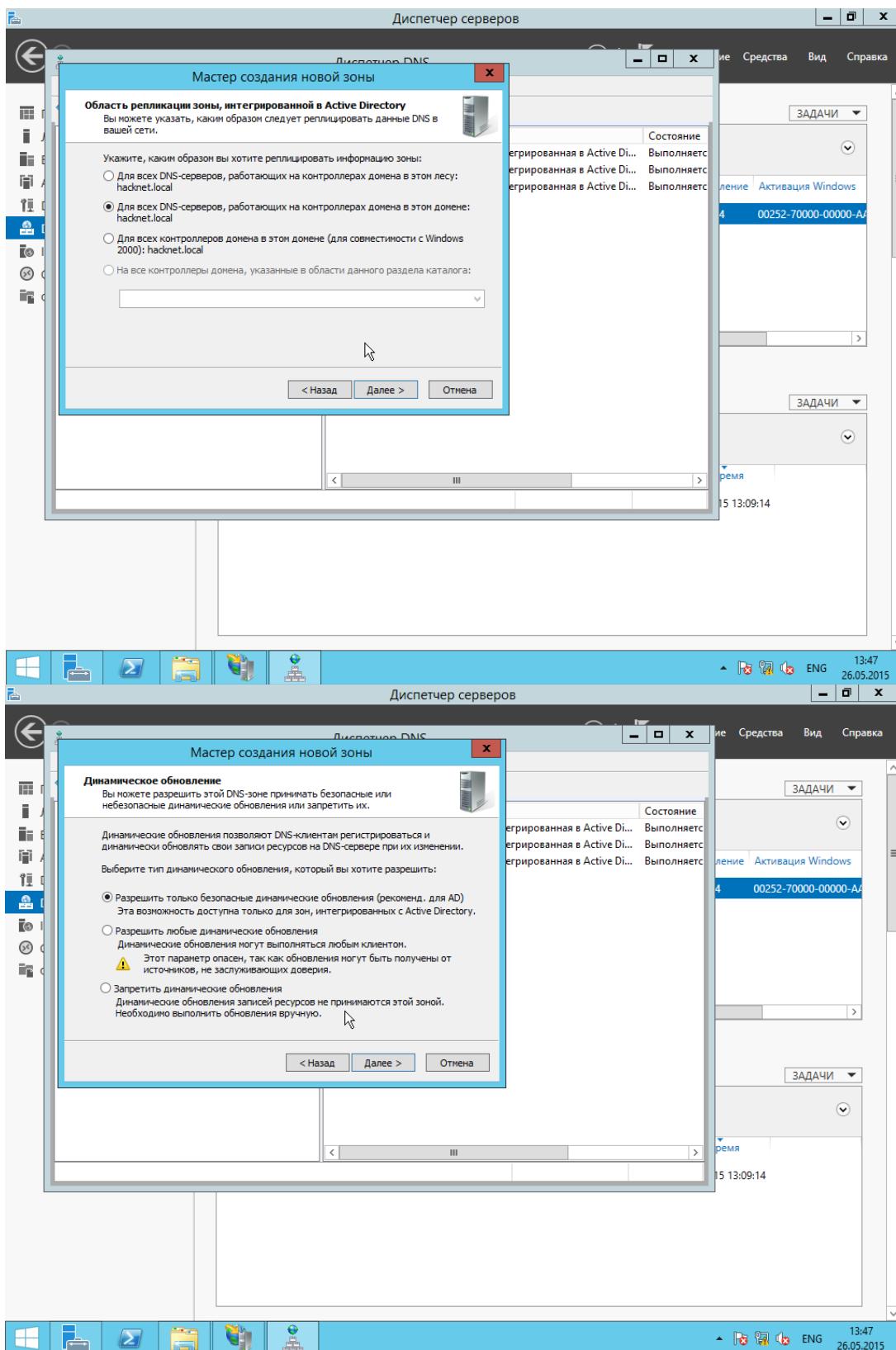
Шаг 3. Настройка веб-сайта

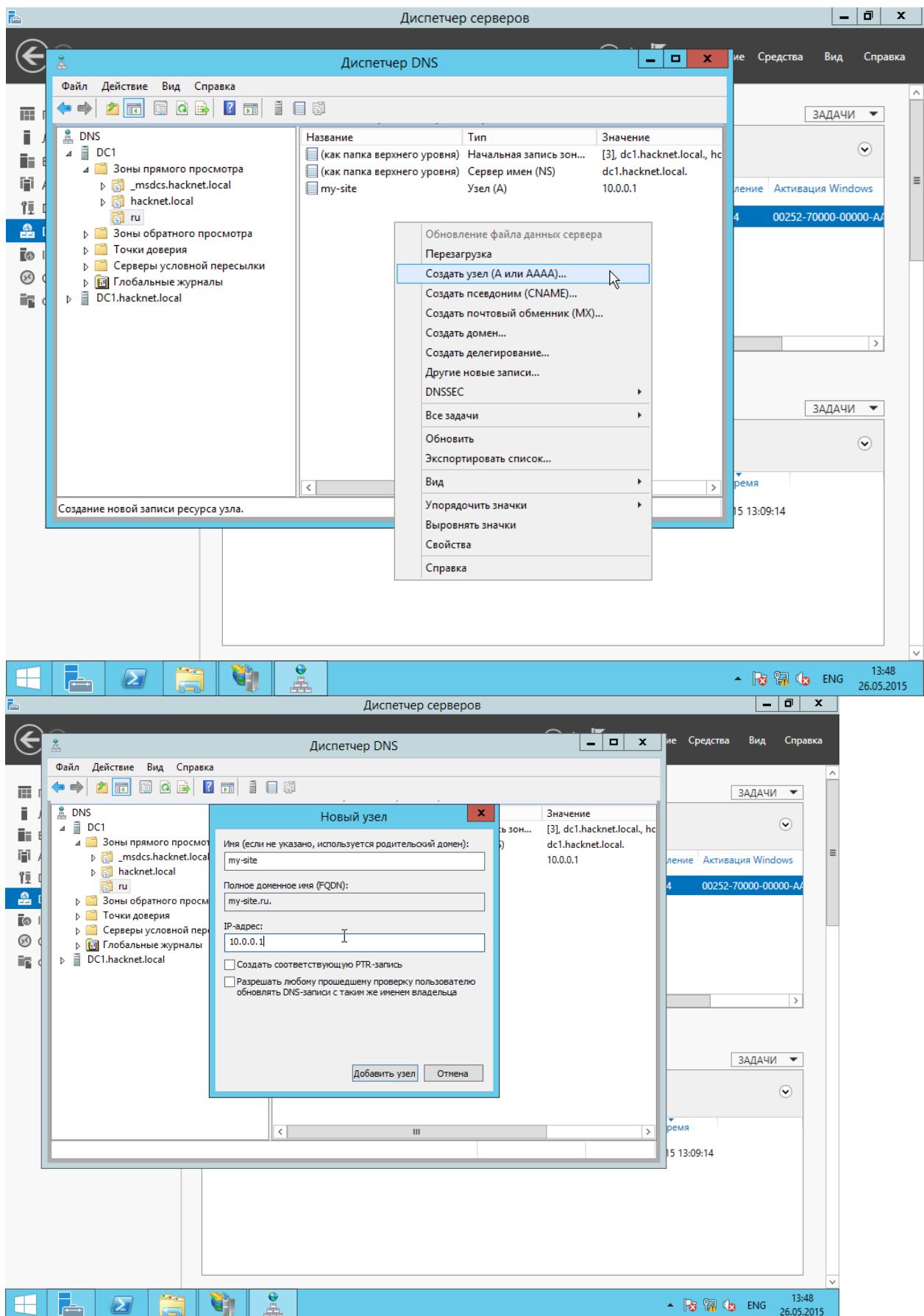
1. Необходимо настроить DNS, чтобы он перенаправлял запросы клиентских машин на IP-адрес сервера. Например, сайт называется my-site.ru.











Создание FTP-сайта на основе служб IIS

Шаг 1. Установка службы FTP на существующем веб-сервере IIS

В этом шаге показывается, как установить службу FTP на существующий веб-сервер IIS, работающий в Windows Server 2012 или Windows 8.

[Установка службы FTP на Windows Server 2012](#)

1. На **начальном** экране щелкните заголовок **Диспетчер сервера**, затем нажмите кнопку **Да**.
2. На **панели мониторинга диспетчера сервера** нажмите **Добавить роли и компоненты**.
3. Если откроется страница **Перед началом мастера добавления ролей и компонентов**, нажмите кнопку **Далее**.
4. На странице **Выбор типа установки** выберите **Установка на основе ролей или компонентов** и нажмите кнопку **Далее**.
5. На странице **Выбор целевого сервера** выберите **Выбор сервера из пулла серверов**, затем из списка **Пул серверов** выберите сервер и нажмите кнопку **Далее**.
6. На странице **Выбор ролей сервера** разверните узел **Веб-сервер (IIS)**, а затем разверните узел **FTP-сервер**.
7. Установите флажок **FTP-сервер** и флажок **Служба FTP**, затем нажмите кнопку **Далее**.
8. На странице **Выбор компонентов** нажмите кнопку **Далее**.
9. На странице **Подтверждение выбранных элементов для установки** нажмите **Установить**.

[Шаг 2. Добавление FTP-сайта](#)

После установки службы FTP на веб-сервере IIS можно добавить один или несколько FTP-сайтов. Если нужно разрешить клиентам передачу файлов с сайта и на сайт, используя протокол FTP, добавьте FTP-сайт.

Добавление FTP-сайта

1. Откройте диспетчер служб IIS.
2. На панели **Соединения** разверните узел сервера и щелкните узел **Сайты**.
3. На панели **Действия** выберите **Добавить FTP-сайт**, чтобы открыть мастер **Добавление FTP-сайта**.
4. На странице **Сведения о сайте** в поле **Имя FTP-сайта** введите уникальное понятное имя FTP-сайта.
5. В поле **Физический путь** введите физический путь или нажмите кнопку обзора (...), чтобы указать физический путь к каталогу содержимого.
6. Нажмите кнопку **Далее**, чтобы открыть страницу **Привязки и параметры SSL**.
7. В области **Привязка** в списке **IP-адрес** выберите или введите IP-адрес, если требуется изменить заданное в качестве IP-адреса значение **Все неназначенные**.
8. В поле **Порт** введите номер порта.
9. Либо в поле **Виртуальный узел** введите имя узла, если нужно, чтобы по одному IP-адресу размещалось несколько FTP-сайтов. Например, введите **contoso.com**.
10. Если нужно запускать сайт вручную, снимите флажок **Автоматически запускать FTP-сайт**.
11. В разделе **SSL** выберите сертификат из списка **SSL-сертификат**. Либо нажмите **Просмотр**, чтобы открыть диалоговое окно **Сертификаты** и проверить сведения о выбранном сертификате.
12. Задайте один из следующих параметров:

- **Разрешить SSL:** разрешает FTP-серверу поддерживать соединения с клиентом с использованием SSL и подключений без SSL.
 - **Требовать SSL:** требует SSL-шифрование связи между FTP-сервером и клиентом.
13. Нажмите кнопку **Далее**, чтобы открыть страницу **Сведения о проверке подлинности и авторизации**.
14. В разделе **Проверка подлинности** выберите метод проверки подлинности или методы, которые нужно использовать.
- **Анонимная:** разрешает доступ к содержимому любому пользователю, предоставившему только имя пользователя **anonymous** или **ftp**. (Большинство клиентов FTP, но не все вводят имя пользователя автоматически.)
 - **Обычная:** требует, чтобы для доступа к содержимому пользователи предоставляли допустимое имя и пароль. Поскольку обычная проверка подлинности передает незашифрованные пароли по сети, этот метод проверки подлинности можно использовать, если только известно, что соединение между клиентом и FTP-сервером безопасно, например с помощью протокола SSL.
15. В разделе **Авторизация** выберите в из списка **Разрешить доступ для** один из следующих параметров.
- **Все пользователи:** все пользователи имеют доступ к содержимому независимо от того, являются они анонимными или определенными.
 - **Анонимные пользователи:** доступ к содержимому могут иметь анонимные пользователи.
 - **Указанные роли или группы пользователей:** доступ к содержимому предоставляется только членам конкретных ролей или групп пользователей. В соответствующем поле введите роль или группу пользователей.
 - **Указанные пользователи:** доступ к содержимому предоставляется только указанным пользователям. Введите в соответствующее поле имя пользователя.
16. Если выбран параметр из списка **Разрешить доступ для**, выберите одно или оба следующих разрешения.
- **Чтение:** разрешает авторизованным пользователям читать содержимое из каталога.
 - **Запись:** разрешает авторизованным пользователям записывать в каталог.
17. Нажмите кнопку **Готово**.

[Шаг 3. Настройка параметров FTP-сайта по умолчанию](#)

Если требуется, чтобы новые FTP-сайты использовали другое значение по умолчанию, измените значение по умолчанию FTP-сайта.

Примечание

При изменении значения по умолчанию значения, заданные для существующих сайтов, не переопределяются. Вручную измените значение для существующих сайтов.

[Настройка параметров FTP-сайта по умолчанию](#)

1. Откройте диспетчер служб IIS.
2. На панели **Соединения** щелкните узел сервера и узел **Сайты**.
3. На панели **Действия** нажмите кнопку **Значения по умолчанию для FTP-сайтов**.
4. Измените параметры и нажмите кнопку **OK**.

В следующей таблице перечислены параметры, значения которых можно задать в диалоговом окне **Значения по умолчанию для FTP-сайтов**.

Категория параметра	Имя параметра	Описание
Общие	Разрешить UTF-8	Указывает, следует ли использовать кодировку UTF8. Значение по умолчанию — true.
Общие	Автоматический запуск	Если значение равно true, FTP-сайт запускается после создания или при запуске службы FTP. Значение по умолчанию — true.
Соединения	Время ожидания канала управления	Указывает время ожидания (в секундах) завершения соединения из-за неактивности.
Соединения	Время ожидания канала данных	Указывает время ожидания (в секундах) отключения канала данных из-за неактивности.
Соединения	Отключить группировку сокетов	Указывает, используется ли группировка сокетов для сайтов, различаемых по IP-адресу, а не по номеру порта или имени узла.
Соединения	Макс. число соединений	Максимально допустимое число одновременных соединений с сервером.
Соединения	Сброс при макс. числе соединений	Указывает, следует ли отключать сеанс FTP при отправке ответа о максимальном числе соединений.
Соединения	Журнал прослушивания сервера	Максимальное количество необработанных сокетов, которые можно поставить в очередь.

Соединения	Время ожидания без проверки подлинности	Время ожидания (в секундах) между созданием нового соединения и успешной проверкой подлинности.
Кэширование учетных данных	Включено	Указывает, включено ли кэширование учетных данных для службы FTP.
Кэширование учетных данных	Интервал записи на диск	Указывает время существования кэша (в секундах) для учетных данных, которые хранятся в кэше.
Обработка файлов	Разрешить чтение файлов при передаче	Указывает, разрешается ли чтение файлов в процессе их передачи на сервер.
Обработка файлов	Разрешить замену при переименовании	Указывает, разрешается ли перезапись файлов при их переименовании.
Обработка файлов	Сохранять частично переданные файлы	Указывает, следует ли сохранять файлы, которые были не полностью переданы на сервер.

Шаг 4. Настройка поддержки брандмауэра

Страница **Поддержка брандмаузеров FTP** служит для настройки следующих параметров, которые позволяют FTP-серверу принимать пассивные подключения к данным от брандмауэра.

- **Диапазон портов канала данных:** укажите диапазон портов для пассивного подключения к данным. Необходимо также открыть такой же диапазон портов на брандмауэре. Этот параметр можно настроить только на уровне сервера, а диапазон портов «0-0» означает необходимость использования диапазона кратковременных портов сервера. Временный порт является кратковременным транспортным портом, который протокол TCP/IP выделяет из стандартного диапазона.

- **Внешний IP-адрес брандмауэра:** укажите внешний IP-адрес вашего брандмауэра, чтобы клиенты знали, какой IP-адрес нужно использовать при обмене данными с FTP-сервером через брандмауэр.

Настройка поддержки брандмауэра

1. Откройте диспетчер служб IIS.
2. На панели **Соединения** выберите узел сервера.
3. В представлении **Просмотр возможностей** дважды щелкните пункт **Поддержка брандмаузеров FTP**.

4. В поле **Диапазон портов канала данных** введите диапазон номеров портов (разделенных дефисом). Например, введите **5000–6000**. Или введите **0-0**, чтобы использовать диапазон портов по умолчанию, заданный в параметрах Windows TCP/IP.

Примечание

Не используйте порты 0–1024, поскольку эти порты зарезервированы.

5. В поле **Внешний IP-адрес брандмауэра** введите IP-адрес вашего брандмауэра.
 6. На панели **Действия** нажмите кнопку **Применить**.

Шаг 5. Настройка изоляции пользователей

Функция изоляции пользователей позволяет настроить FTP-сервер для изоляции пользователей, которая запрещает пользователям доступ к каталогам других пользователей на одном FTP-сайте. Если вы не хотите изолировать пользователей, то они будут совместно использовать общую структуру каталогов.

Например, можно не изолировать пользователей на сайте, который предлагает только возможности загрузки общего содержимого, или для сайта, который не требует защиты данных между пользователями.

Если нужно изолировать пользователей на сайте, можно выбрать один из следующих параметров изоляции.

- Каталог пользователя:** изолирует сеансы пользователей, предоставляя им доступ только к физическим или виртуальным каталогам, имя которых соответствует именам учетных записей пользователей FTP. Пользователь видит только собственный корневой каталог FTP, поэтому он не может перемещаться выше по дереву физических или виртуальных каталогов. Игнорируются любые создаваемые глобальные виртуальные каталоги.
- Физический каталог пользователя:** изолирует сеансы пользователей, предоставляя им доступ только к физическим каталогам, имя которых соответствует именам учетных записей пользователей FTP. Пользователь видит только собственное коренное расположение FTP и, следовательно, не может переместиться выше по дереву физических каталогов. Любые создаваемые глобальные виртуальные каталоги применяются ко всем пользователям.
- Корневая папка каталога FTP, настроенного в Active Directory:** изолирует сеансы пользователей, предоставив им доступ только к домашнему каталогу, настроенному в параметрах учетной записи Active Directory для каждого пользователя FTP.

Настройка изоляции пользователей

- Откройте диспетчер служб IIS.
- В представлении **Просмотр возможностей** дважды щелкните **Изоляция пользователей FTP**.
- Если изолировать пользователей не требуется, в разделе **Не изолировать пользователей. Начинать сеансы пользователей** в выберите один из следующих параметров.
 - Корневой каталог FTP:** указывает, что все сеансы FTP начинаются в корневом каталоге FTP-сайта. Этот параметр отключает изоляцию всех пользователей и запускает логику папок.

- **Каталог пользователя:** указывает, что все сеансы FTP начинаются в физическом или виртуальном каталоге, имя которого соответствует имени вошедшего в систему пользователя, если каталог существует. Если этого каталога нет, сеансы FTP начинаются в корневом каталоге FTP-сайта.
4. Если нужно изолировать пользователей, в разделе **Изолировать пользователей. Ограничить пользователям доступ следующим каталогом** выберите один из приведенных далее параметров.
- **Каталог пользователя (отключить глобальные виртуальные каталоги):** изолирует сеансы пользователей, предоставляя им доступ только к физическим или виртуальным каталогам, имя которых соответствует именам учетных записей пользователей FTP.
 - **Физический каталог пользователя (включить глобальные виртуальные каталоги):** изолирует сеансы пользователей, предоставляя им доступ только к физическим каталогам, имя которых соответствует именам учетных записей пользователей FTP.
 - **Корневая папка каталога FTP, настроенного в Active Directory:** изолирует сеансы пользователей, предоставив им доступ только к домашнему каталогу, нальному в параметрах учетной записи Active Directory для каждого пользователя FTP.
 - **Настраиваемые:** этот параметр представляет дополнительную возможность, он позволяет разработчикам создавать настраиваемые поставщики, которые обеспечивают поиск в корневой папке каталога подстановок на основе уникальных бизнес-потребностей.
5. Если в предыдущем шаге выбран вариант **Корневая папка каталога FTP, настроенного в Active Directory**, нажмите кнопку **Установить**, а затем введите имя пользователя и пароль в поля **Имя пользователя** и **Пароль** диалогового окна **Установка учетных данных**, имеющего доступ к вашему серверу Active Directory. Вновь введите пароль в поле **Подтверждение пароля**, затем нажмите кнопку **OK**.
6. На панели **Действия** нажмите кнопку **Применить**.

Шаг 6. Настройка параметров просмотра каталогов

Возможность «Просмотр каталогов FTP» позволяет контролировать то, что отображается, когда пользователи просматривают каталоги FTP.

Настройка параметров просмотра каталогов

1. Откройте диспетчер служб IIS.
2. На панели **Соединения** выберите уровень сервера или уровень сайта.
3. В представлении **Просмотр возможностей** дважды щелкните пункт **Просмотр каталогов FTP**.
4. На странице **Просмотр каталогов FTP** в разделе **Стиль вывода каталогов** выберите один из следующих параметров.
 - **MS-DOS:** отображает содержимое каталога в соответствии со стилем MS-DOS.
 - **UNIX:** отображает содержимое каталога в соответствии со стилем UNIX.
5. В разделе **Параметры вывода каталогов** выберите сведения, которые будут отображаться при выводе данных каталогов. Можно выбрать любой из следующих параметров.
 - a. **Виртуальные каталоги:** отображение виртуальных каталогов.
 - b. **Доступно байтов:** отображение размера файла в байтах.
 - c. **Год из четырех знаков:** отображение года с использованием четырех цифр, а не двух.

6. На панели **Действия** нажмите кнопку **Применить**.

Шаг 7. Настройка ограничений на попытки входа в систему

Эта возможность позволяет настроить максимальное количество неудачных попыток входа, которые разрешаются в течение заданного времени, прежде чем доступ для IP-адреса будет запрещен.

Настройка ограничений на попытки входа в систему

1. Откройте диспетчер служб IIS.
2. На панели **Соединения** выберите уровень сервера.
3. В представлении **Просмотр возможностей** дважды щелкните пункт **Ограничение попыток входа на FTP**.
4. На странице **Ограничение попыток входа на FTP** установите флажок **Включить ограничение попыток входа на FTP**.
5. В поле **Максимальное количество неудачных попыток входа в систему** введите положительное целое число. Значение по умолчанию — 4.
6. В поле **Интервал времени (в секундах)** введите положительное целое число. Значение по умолчанию — 30.
7. Выберите **Запрещать доступ IP-адресам при достижении заданного количества неудачных попыток входа в систему** или **Только запись в журнал**. Если выбран вариант **Только запись в журнал**, службы IIS не будут запрещать доступ клиентам, даже если превышено максимальное число неудачных попыток.
8. На панели **Действия** нажмите кнопку **Применить**.

Шаг 8. Настройка фильтрации запросов

Страница **Фильтрация FTP-запросов** служит для настройки параметров фильтрации запросов к FTP-сайту. Фильтрация FTP-запросов — это средство безопасности, позволяющая поставщикам услуг Интернета и поставщикам служб приложений ограничивать поведение протокола и содержимого.

Настройка фильтрации запросов

1. Откройте диспетчер служб IIS.
2. На панели **Соединения** выберите уровень сервера или уровень сайта.
3. В представлении **Просмотр возможностей** дважды щелкните пункт **Фильтрация запросов FTP**.
4. Чтобы изменить общие параметры фильтрации запросов, нажмите **Изменить параметры** на панели **Действия**. Затем измените общие параметры.
5. Чтобы добавить фильтр, основанный на расширениях имен файлов, перейдите на вкладку **Расширение имени файла**. На панели **Действия** выберите вариант **Разрешить расширение имени файла** или **Запретить расширения имен файлов**. Затем введите расширение в поле **Расширение имени файла** и нажмите кнопку **OK**.
6. Чтобы добавить фильтр, основанный на сегменте URL-адреса (например, имя папки), перейдите на вкладку **Скрытые сегменты**. На панели **Действия** нажмите **Добавить скрытый сегмент**. Затем введите сегмент в поле **Скрытый сегмент** и нажмите кнопку **OK**.
7. Чтобы добавить фильтр, основанный на последовательности URL-адресов, перейдите на вкладку **Запрещенные последовательности URL-адресов**. На панели **Действия** нажмите кнопку **Добавить последовательность URL-адресов**. Затем введите последовательность в поле **Последовательность URL-адресов** и нажмите кнопку **OK**.

8. Чтобы добавить фильтр, основанный на команде, перейдите на вкладку **Команды**. На панели **Действия** выберите вариант **Разрешить команду** или **Запретить команду**. Затем введите команду в поле **Команда** и нажмите кнопку **OK**.

Шаг 9. Настройка ведения журнала FTP

Возможность **Ведение журнала FTP** можно использовать для настройки ведения журнала на уровне сервера или сайта, а также для настройки параметров ведения журнала.

Настройка ведения журнала FTP

1. Откройте диспетчер служб IIS.
2. На панели **Соединения** выберите уровень сервера или уровень сайта.
3. В представлении **Просмотр возможностей** дважды щелкните пункт **Ведение журнала FTP**.
4. В меню **Один файл журнала** на выберите пункт **Сайт либо Сервер**.
5. В разделе **Файл журнала** нажмите кнопку **Выбрать поля W3C**, затем выберите сведения, которые нужно занести в журнал.
6. В разделе **Каталог** введите путь к базовой папке, где должны храниться файлы журналов FTP, или нажмите кнопку **Обзор**, чтобы перейти к базовой папке.
7. В разделе **Кодировка** выберите либо **UTF8** (однобайтовые и многобайтовые знаки), либо **ANSI** (только однобайтовые знаки).
8. В разделе **Переключение на файл продолжения журнала** выберите способ создания службой FTP новых файлов журнала из следующего списка.
 - a. **Расписание:** выберите **Ежечасно, Ежедневно, Еженедельно** или **Ежемесечно** для создания новых файлов журнала с определенным интервалом времени.
 - b. **Максимальный размер файла (в байтах):** введите положительное целое число для создания новых файлов журнала, если размер файла превышает это число байтов.
 - c. **Не создавать новые файлы журналов**
9. Установите флажок **Использовать местное время в имени файла**, если нужно, чтобы имена файлов журнала и время переключения были основаны на местном часовом поясе, а не на времени в формате UTC.
10. На панели **Действия** нажмите кнопку **Применить**.

Шаг 10. Настройка сообщений FTP

Возможность **Сообщения FTP** используется для изменения параметров сообщений, отправляемых при подключении пользователя к FTP-сайту.

Настройка сообщений FTP

1. На панели **Соединения** выберите уровень сервера или уровень сайта.
2. В представлении **Просмотр возможностей** дважды щелкните пункт **Сообщения FTP**.
3. На странице **Сообщения FTP** в разделе **Поведение сообщений** выберите поведение ваших сообщений FTP. Можно выбрать любой из следующих параметров.
 - a. **Подавить баннер по умолчанию:** указывает, следует ли отображать идентификационный заголовок FTP-сервера по умолчанию.
 - b. **Поддерживать пользовательские переменные в сообщениях:** указывает, следует ли отображать определенный набор пользовательских переменных в сообщениях FTP. Поддерживаются следующие пользовательские переменные.
 - %BytesReceived% — число байтов, отправленных с сервера клиенту в текущем сеансе.

- %BytesSent% — количество байт, полученных сервером от клиента в текущем сеансе.
 - %SessionID% — уникальный идентификатор текущего сеанса.
 - %SiteName% — имя FTP-сайта, на котором выполняется текущий сеанс.
 - %UserName% — имя учетной записи пользователя, который в данный момент вошел на сервер.
- c. **Показывать подробные сообщения для локальных запросов:** указывает, следует ли отображать подробные сообщения об ошибках, если клиент FTP соединяется с FTP-сервером на самом сервере (локальный узел).
4. В области текста сообщения введите сообщения в следующих полях.
- a. **Баннер:** указывает сообщение, отображаемое FTP-сервером при первом подключении клиента.
 - b. **Приветствие:** указывает сообщение, отображаемое FTP-сервером при входе клиента на FTP-сервер.
 - c. **Выход:** указывает сообщение, отображаемое FTP-сервером при выходе (отключении) клиента.
 - d. **Максимальное число соединений:** указывает сообщение, отображаемое FTP-сервером, если клиенты пытаются подключиться к серверу, но не могут это сделать, поскольку достигнуто максимально допустимое для службы FTP число клиентских соединений.
5. На панели **Действия** нажмите кнопку **Применить**.

ЛАБОРАТОРНАЯ РАБОТА №4 АЛГОРИТМ ВИЖЕНЕРА

1. Цель работы

Целью работы является реализация криптографического алгоритма шифрования с использованием открытого текста в качестве ключа по таблице Виженера.

2. Общие сведения

Метод *Виженера*, относящийся к числу много алфавитных подстановок. Здесь берется небольшое целое число m и алфавит после каждой символьной подстановки сдвигается на m символов. Например, для $m=4$. Пусть ключом будет слово мышь (смотри левую вертикальную колонку символов), тогда получим:

абвгдёжзийклмнопрстуфхцчшщъэюя

- 1 мнопрстуфхцчшщъэюяабвгдёжзийкл
- 2 ыъэюяабвгдёжзийклмнопрстуфхцчшщъ
- 3 шщъэюяабвгдёжзийклмнопрстуфхцч
- 4 ьэюяабвгдёжзийклмнопрстуфхцчшщъы

И сходный текст разбивается на группы по m символов (в рассмотренном случае по 4). Для каждой группы первый символ заменяется соответствующей буквой первого алфавита, вторая – из второго и т.д. Например, фраза “от улыбки каждый день светлей” будет преобразована следующим образом:

отул ыбки кажд ыйде нысв етле й
ынлз зъге чыяя зеъб ъчию снđб ц

3. Задания для выполнения

1. Зашифруйте с помощью алгоритма Виженера следующую последовательность:
Ей рано нравились романы
Они ей заменяли все
Она влюблялася в обманы
И Ричардсона и Руссо

Для шифрования используйте ключ «идеал»

2. Расшифруйте помощью алгоритма Виженера следующую последовательность:

Фу эъцё сий дюсягм ьръгм
С аяцшффжмм схщм зпаэпдпйс
Ню т щхитрд хе сштзл сбула

Для дешифрования используйте ключ «проза»

3. Напишите алгоритм и программу для шифрования/дешифрования строк алгоритмом Виежера. Варианты (m=name-2, key= name)

Не мысля гордый свет забавить,
Вниманье дружбы возлюбя,
Хотел бы я тебе представить
Залог достойнее тебя,
Достойнее души прекрасной,
Святой исполненной мечты,
Поэзии живой и ясной,
Высоких дум и простоты;
Но так и быть - рукой пристрастной
Прими собранье пестрых глав,
Полусмешных, полупечальных,
Простонародных, идеальных,
Небрежный плод моих забав,
Бессонниц, легких вдохновений,
Незрелых и увядших лет,
Ума холодных наблюдений
И сердца горестных замет.

I

"Мой дядя самых честных правил,
Когда не в шутку занемог,
Он уважать себя заставил
И лучше выдумать не мог.
Его пример другим наука;
Но, боже мой, какая скуча
С больным сидеть и день и ночь,
Не отходя ни шагу прочь!
Какое низкое коварство
Полуживого забавлять,
Ему подушки поправлять,
Печально подносить лекарство,
Вздыхать и думать про себя:
Когда же черт возьмет тебя!"

Лабораторная работа №5

Шифрование методом перестановки

1. Цель работы

Выполнить шифрование заданного сообщения простейшим шифром перестановок и выполнить проверку правильности шифрования.

2. Теоретическая часть

Метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов.

Самая простая перестановка – написать исходный текст задом наперед и одновременно разбить шифrogramму на пятерки букв. Например:

пусть будет так, как мы хотели

получится такой шифротекст:

илемо хымка ккатт ебудь тсуп

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем зашифровать исходное выражение, следует его дополнить незначащей буквой, например, О, до числа, кратного пяти:

пусть будет такка кмыхо телио

Тогда шифrogramма, будет выглядеть:

оилем охымк аккат тебуд ьтсуп

Другой метод заключается в том, что исходный текст записывали в несколько строк. Например по пятнадцать букв в каждой (с заполнением последней строки незначащими буквами).

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
п	у	с	т	ь	б	у	д	е	т	т	а	к	к	а
к	м	ы	х	о	т	е	л	и	к	л	м	н	о	п

После этого вертикальные столбцы по порядку пишутся в строку с разбивкой на пятерки букв:

пкумс ытхъо бтуед леитк тlamk нкоап

Если строки укоротить, а количество строк увеличить, то получится **прямоугольник – решетка**, в которую записывается исходный текст. Например:

1	2	3	4	5	6
п	у	с	т	ь	б
у	д	е	т	т	а
к	к	а	к	м	ы
р	е	ш	и	л	и
а	б	в	г	д	е
м	л	к	и	з	ж

Если шифровать по диагоналям сверху вниз с левого верхнего угла, то получим:

п уу сдк текх ьтаоб бтктбм амевл ылгк иди ез ж

Третий вид данного шифра: перестановки с ключем. Необходимо знать ключ, например «радиатор». В соответствии с расположением букв в алфавите буква А получает номер 1, вторая буква А – 2, следующая по алфавиту буква Д – 3, потом И – 4, О – 5, первая буква Р – 6, вторая Р – 7 и буква Т – 8. Получим:

Р	А	Д	И	А	Т	О	Р
6	1	3	4	2	8	5	7
п	у	с	т	ь	б	у	д
е	т	т	а	к	к	а	к
м	ы	х	о	т	е	л	и
о							

Записывая столбики в соответствии с номерами букв ключа:
уты ъкт стх тао уал пемо дки бке

Задание

Зашифровать последним методом следующий текст:

Двадцать первое. Ночь. Понедельник. Очертанья столицы во мгле. Сочинил же какой-то бездельник, что бывает любовь на земле. И от лености или от скуки все поверили, так и живут: ждут свиданий, боятся разлуки и любовные песни поют.

При зашифровывании используете ключ

- 1 вариант - «головоломка»;
- 2 вариант - «ловушка»;
- 3 вариант - «положение»;
- 4 вариант – «свобода».

Лабораторная работа №6

Использование гаммирования при шифровании

1. Цель работы

Освоить на практике применение алгоритма шифрования методом гаммирования.

2. Теоретическая часть

Гаммирование - это процесс наложения по определенному закону гаммы шифра на открытые данные.

Гамма шифра - псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму для зашифровывания открытых данных и расшифровывания зашифрованных данных.

Суть метода заключается в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется гаммой.

Процедура наложения гаммы осуществляется следующими способами:

1. Символы исходного текста и гаммы заменяются цифрами эквивалентными, которые затем складываются по модулю k , где k – число символов в алфавите, т.е.:

$$R_i = (S_i + G_i) \bmod (k-1),$$

где R_i , S_i , G_i – символы зашифрованного, исходного текста и гаммы соответственно.

2. Символы исходного текста и гаммы представляются в виде двоичного кода, затем соответствующие разряды складываются по модулю 2. Вместо сложения по модулю 2 при гаммировании можно использовать другие логические функции.

Пример шифрования гаммированием представлен в таблице 1.

Таблица 1 - Пример

Шифруемый текст	Б	У	Д	Ь	...
	010010	100000	110010	100100	
Знаки гаммы	7	1	8	2	...
	000111	000001	001000	000010	
Шифрованный текст	010101	100001	111010	100110	

Задание

Зашифруйте следующее предложение методом гаммирования.

«Помехоустойчивое кодирование – это кодирование с возможностью восстановления потерянных или ошибочно принятых данных.»

Знаки гаммы: 2 3 10 4 1 5 6 7 8 11 15 14 12 13 9 0.

Шифрование происходит в цикле (знак гаммы повторяется циклически).

Представление букв в двоичной системе счисления представлено в таблице 2.

Таблица 2 – Представление букв

Буква	Шифр								
А	000001	Ж	001101	Н	010010	У	000101	Щ	011100
Б	001001	З	001110	О	000100	Ф	010111	Ы	011101
В	001010	И	000011	П	010011	Х	011000	Ь	011110
Г	001011	К	001111	Р	010100	Ц	011001	Э	000110
Д	001100	Л	010000	С	010101	Ч	011010	Ю	000111
Е	000010	М	010001	Т	010110	Ш	011011	Я	001000

Лабораторная работа №7

Шифрование с помощью аналитических преобразований

1. Цель работы

Освоить на практике применение алгоритма шифрования с помощью аналитических преобразований.

2. Теоретическая часть

Достаточно надежное закрытие информации может быть обеспечено при использовании для шифрования некоторых аналитических преобразований. Например умножение матрицы не вектор по правилу:

$$\bar{C} = A \times \bar{B}; \quad \sum_{j=1}^N a_{ij} b_j$$

Если матрицу $A=(a_{ij})$ использовать в качестве ключа, а вместо компонента вектора $B=(b_j)$ подставить символы текста, то компоненты вектора $C=(c_i)$ будут представлять собой символы зашифрованного текста.

Пример.

Возьмем в качестве ключа квадратную матрицу третьего порядка

$$A = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix}$$

Заменим буквы алфавита цифрами, соответствующими их порядковому номеру в алфавите: А-0, Б-1, В-2 и т.д. Тогда отрывку текста ВАТАЛА будет соответствовать 2, 0, 19, 0, 12, 0. По принятому алгоритму шифрования необходимо выполнить следующие действия:

$$\bar{C} = A \times \bar{B} = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 85 \\ 54 \\ 25 \end{pmatrix};$$

$$\bar{C} = A \times \bar{B} = \begin{pmatrix} 14 & 8 & 3 \\ 8 & 5 & 2 \\ 3 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 0 \\ 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 96 \\ 60 \\ 24 \end{pmatrix}.$$

При этом шифрованный текст будет иметь вид: 85, 54, 25, 96, 60, 24.

Дешифрование осуществляется с использованием того же правила умножения матрицы на вектор, только в качестве ключа берется матрица, обратная той, с помощью которой осуществляется зашифровывание, а в качестве вектора-сомножителя – соответствующие фрагменты символов закрытого текста; тогда значениями вектора – результата будут цифровые эквиваленты знаков открытого текста.

Матрицей, обратной данной A , называется матрица A^{-1} , получающаяся из присоединения матрицы делением всех ее элементов на определитель данной матрицы. Присоединенной называется матрица, составленная из алгебраических дополнений A_{ij} , к элементам данной матрицы, которые вычисляются по формуле:

$$A_{ij} = (-1)^{i+j} \Delta_{ij},$$

где Δ_{ij} - определитель матрицы, получаемой вычеркиванием i -й строки и j -го столбца исходной матрицы.

Определителем матрицы называется алгебраическая сумма $n!$ Членов (для определителя n -го порядка), составленная следующим образом: членами служат всевозможные произведения n элементов матрицы, взятых по одному в каждой строке и в каждом столбце; причем член суммы берется со знаком «+», если его индексы составляют четную подстановку, и со знаком «-» - в противоположном случае. Для матрицы третьего порядка определитель вычисляется следующим образом:

$$\Delta = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}.$$

Процесс раскрытия выглядит так:

$$A^{-1} \times \bar{C} = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix} \times \begin{pmatrix} 85 \\ 54 \\ 25 \end{pmatrix} = \begin{pmatrix} 1 \cdot 85 - 2 \cdot 54 + 1 \cdot 25 \\ -2 \cdot 85 + 5 \cdot 54 - 4 \cdot 25 \\ 1 \cdot 85 - 4 \cdot 54 + 6 \cdot 25 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix};$$

$$A^{-1} \times \bar{C} = \begin{pmatrix} 1 & -2 & 1 \\ -2 & 5 & -4 \\ 1 & -4 & 6 \end{pmatrix} \times \begin{pmatrix} 96 \\ 60 \\ 24 \end{pmatrix} = \begin{pmatrix} 1 \cdot 96 - 2 \cdot 60 + 1 \cdot 24 \\ -2 \cdot 96 + 5 \cdot 60 - 4 \cdot 24 \\ 1 \cdot 96 - 4 \cdot 60 + 6 \cdot 24 \end{pmatrix} = \begin{pmatrix} 0 \\ 12 \\ 0 \end{pmatrix}.$$

Таким образом, получена последовательность знаков раскрытоого текста 2, 0, 19, 0, 12, 0, что соответствует исходному тексту.

Задание

Зашифровать описанным методом следующее выражение:

«Помехоустойчивое кодирование – это кодирование с возможностью восстановления потерянных или ошибочно принятых данных». В качестве ключа использовать следующую матрицу:

$$1 \text{ вариант} - A = \begin{pmatrix} 11 & 7 & 14 \\ 13 & 4 & 13 \\ 6 & 15 & 4 \end{pmatrix}$$

$$2 \text{ вариант} - A = \begin{pmatrix} 1 & 7 & 12 \\ 8 & -5 & 0 \\ 7 & 8 & 2 \end{pmatrix}$$

$$3 \text{ вариант} - A = \begin{pmatrix} 1 & 2 & 5 & 4 \\ 3 & 13 & 9 & 7 \\ 2 & 3 & 5 & 11 \\ 5 & 6 & -5 & 29 \end{pmatrix}$$

$$4 \text{ вариант} - A = \begin{pmatrix} 5 & 12 & -4 & 8 \\ 3 & 0 & 7 & 21 \\ 5 & 2 & 1 & 1 \\ 5 & 3 & 2 & 9 \end{pmatrix}$$

ЛАБОРАТОРНАЯ РАБОТА №8 ОПЕРАЦИОННАЯ СИСТЕМА FREEBSD

1. Цель работы

1. Изучить процесс установки FreeBSD 9.
2. Установка и настройка приложений FreeBSD 9.

2. Общие сведения

2.1 Установка FreeBSD 9

1. Для начала вам необходимо приобрести установочный образ ОС FreeBSD. Вы можете скачать его на сайте разработчика или же с другого ресурса. Адрес сайта разработчика: freebsd.org. Если у вас есть образ диска с операционной системой, запишите его на DVD диск с помощью соответствующей программы (Nero, Alcohol 120%, др.). Или запишите этот образ на USB флэшку с помощью одной из специальных программ (например, WinSetupFromUSB). Затем вставьте диск в дисковод или флэшку в USB порт и перезагрузите компьютер. Во время загрузки компьютера нажмите на клавишу выбора загрузочного устройства (для разных моделей компьютера эта клавиша может быть разной).

2. Можно приступать к установке операционной системы. После загрузки необходимых файлов первое, что вы увидите – изображение на Рис. 1.



Рис. 1 Стартовый загрузчик FreeBSD

На данном этапе вам доступны следующие действия:

- При нажатии клавиши Пробел останавливается таймер в нижней части экрана.
- При нажатии клавиши Enter происходит дальнейшая загрузка файлов для установки операционной системы.
- При нажатии цифры 3 на клавиатуре происходит перезагрузка системы.
- При нажатии клавиши А происходит включение/отключение поддержки ACPI.

При нажатии клавиши M происходит включение/отключение режима загрузки операционной системы в безопасном режиме.

При нажатии клавиши S происходит включение/отключение загрузки операционной системы в однопользовательском режиме.

При нажатии клавиши V происходит включение/отключение режима пошагового вывода.

Для установки операционной системы нажмите клавишу Enter или дождитесь завершения отсчёта таймера.

3. Ядром FreeBSD будет произведён поиск распознанных устройств. Просмотреть весь список вы сможете с помощью нажатий клавиш Page UP и Page Down (прокрутка включается/выключается клавишей Scroll Lock). После процедуры идентификации имеющихся устройств появится окно, предоставляющее выбор одного из трёх режимов загрузки, изображённое на Рис. 2.

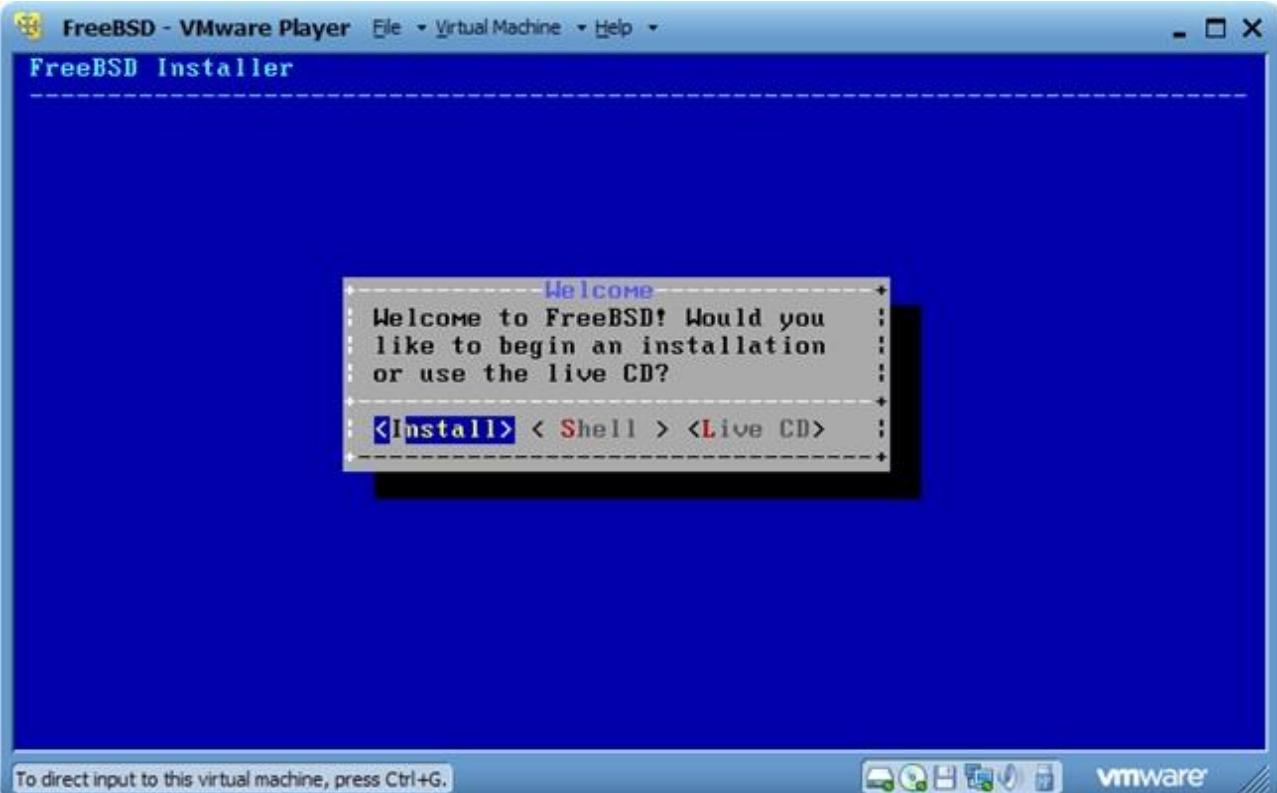


Рис. 2 Диалоговое окно выбора режима загрузки

Для выбора одного из действий при появлении подобных диалоговых окон перемещайте выделение клавишами со стрелками Вправо и Влево, а для подтверждения выбора нажмите Enter. На данном этапе вам доступны следующие действия:

При выборе Install продолжается установка FreeBSD.

При выборе Shell запускается интерфейс командной строки FreeBSD с текущего носителя (CD, DVD, USB Flash). В этом режиме вы можете просматривать содержимое каталогов носителя, а также содержимое файлов, например, с помощью текстового редактора.

При выборе Live CD запускается “портативный вариант” операционной системы FreeBSD для ознакомления с ней.

Нас интересует установка FreeBSD, поэтому выберите Install.

4. Далее на экране появляется окно, представленное на Рис. 3.



Рис. 3 Диалоговое окно выбора раскладки клавиатуры

На данном этапе система спрашивает, хотите ли вы установить раскладку клавиатуры отличную от стандартной раскладки.

Если вы выбрали No, см. пункт 5.

Если же вы выбрали да, то на экране появится диалоговое окно, представленное на Рис. 4.



Рис. 4 Диалоговое окно выбора раскладки клавиатуры

На данном этапе для выбора раскладки используются клавиши со стрелками Вверх и Вниз, а для выбора подтверждения или отклонения – Влево и Вправо. Как при подтверждении выбора, так и при его отклонении вы переходите на пункт 5.

5. На следующем этапе появляется диалоговое окно, представленное на Рис. 5.



Рис. 5 Диалоговое окно ввода имени машины (компьютера)

На данном этапе система просит вас ввести имя данной машины (компьютера). Также система сообщает: “Если ваша машина входит в корпоративную сеть, пожалуйста, узнайте у вашего администратора сети соответствующее имя”. Иными словами, так будет называться ваш компьютер в сети. После ввода имени нажмите Enter.

6. На следующем этапе появляется диалоговое окно, представленное на Рис. 6.

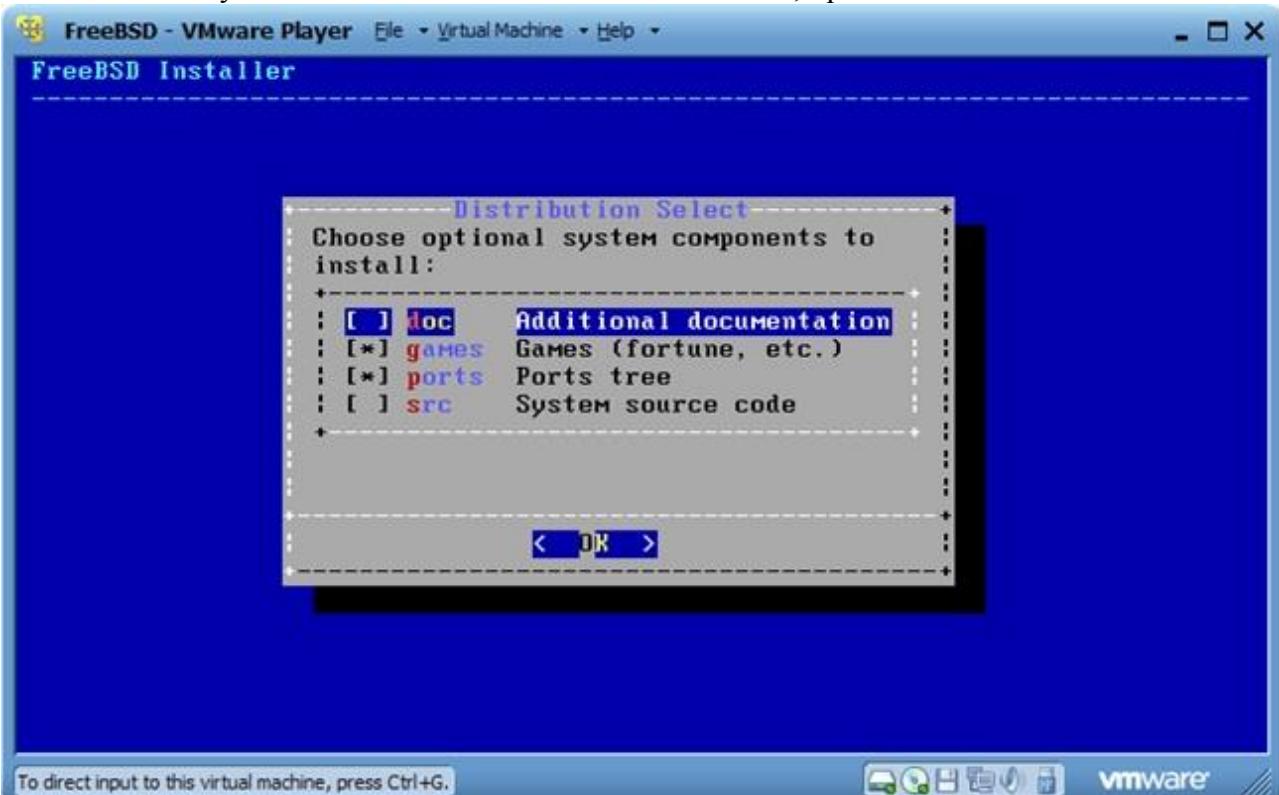


Рис. 6 Диалоговое окно выбора дистрибутивов

На данном этапе система предлагает вам выбрать необязательные, но доступные для установки компоненты системы. Сверху вниз: Дополнительная документация, Игры (удача, т.д.), Коллекция портов, Исходные коды системы. Здесь для того, чтобы поставить/снять отметку установки компонента (*), перемещайте выделение с помощью клавиш со стрелками Вверх и Вниз, нажмите пробел непосредственно для отметки/снятия компонента. Затем нажмите Enter.

7. На следующем этапе появляется диалоговое окно, представленное на Рис. 7.



Рис. 7 Диалоговое окно выбора режима разметки диска

На данном этапе система предлагает вам выбрать один из трёх режимов разбиения жёсткого диска на разделы и подразделы. Система сообщает: “Хотели бы вы использовать управляемый режим разметки диска (рекомендуется для начинающих) или же вручную разметить жёсткий диск (для экспертов)? Также вы можете запустить оболочку и полностью вручную разметить жёсткий диск”.

На данном этапе вам доступны следующие действия:

- При выборе Guided запускается управляемый режим разметки диска.
- При выборе Manual запускается ручной режим разметки диска.
- При выборе Shell запускается ручной режим разметки диска с помощью интерфейса командной строки FreeBSD.

Выберите Guided и нажмите Enter.

8. На следующем этапе появляется диалоговое окно, представленное на Рис. 8.



Рис. 8 Диалоговое окно выбора способа разметки диска

На данном этапе система сообщает: “Хотели бы вы использовать жёсткий диск (ada0) полностью для О.С. FreeBSD или же хотите создать дополнительный раздел на диске для его совместного использования и другими операционными системами? Использование всего диска полностью уничтожит все хранящиеся на нём данные”.

На данном этапе вам доступны следующие действия:

□ При выборе Entire Disk система удаляет ВСЕ разделы и данные, которые находились на момент выбора этой опции независимо от их типа, количества, размера и т.д. Вследствие этого весь жёсткий диск представляет собой неразмеченное пространство. Затем система формирует из этого пространства Таблицу разделов GUID (GPT), т.е. особым образом размечает это пространство. Затем в этом размеченном пространстве создаются три раздела, необходимых для установки и функционирования FreeBSD. Результат этого действия вы можете увидеть на Рис. 9.

□ Вариант Partition выбирается в том случае, если у вас на текущий момент жёсткий диск размечен определённым образом (например, если у вас имеющийся раздел жёсткого диска используется для хранения каких-то данных или же на каком-то разделе установлена операционная система и вы НЕ ХОТИТЕ ТЕРЯТЬ ЭТИ ДАННЫЕ). Т.е. в этом случае система размечает ТЕКУЩЕЕ НЕРАЗМЕЧЕННОЕ ПРОСТРАНСТВО жёсткого диска.

Если вы выбрали второй вариант, см. пункт 10.

9. При выборе EntireDisk результат операции будет соответствовать изображению на Рис. 9.

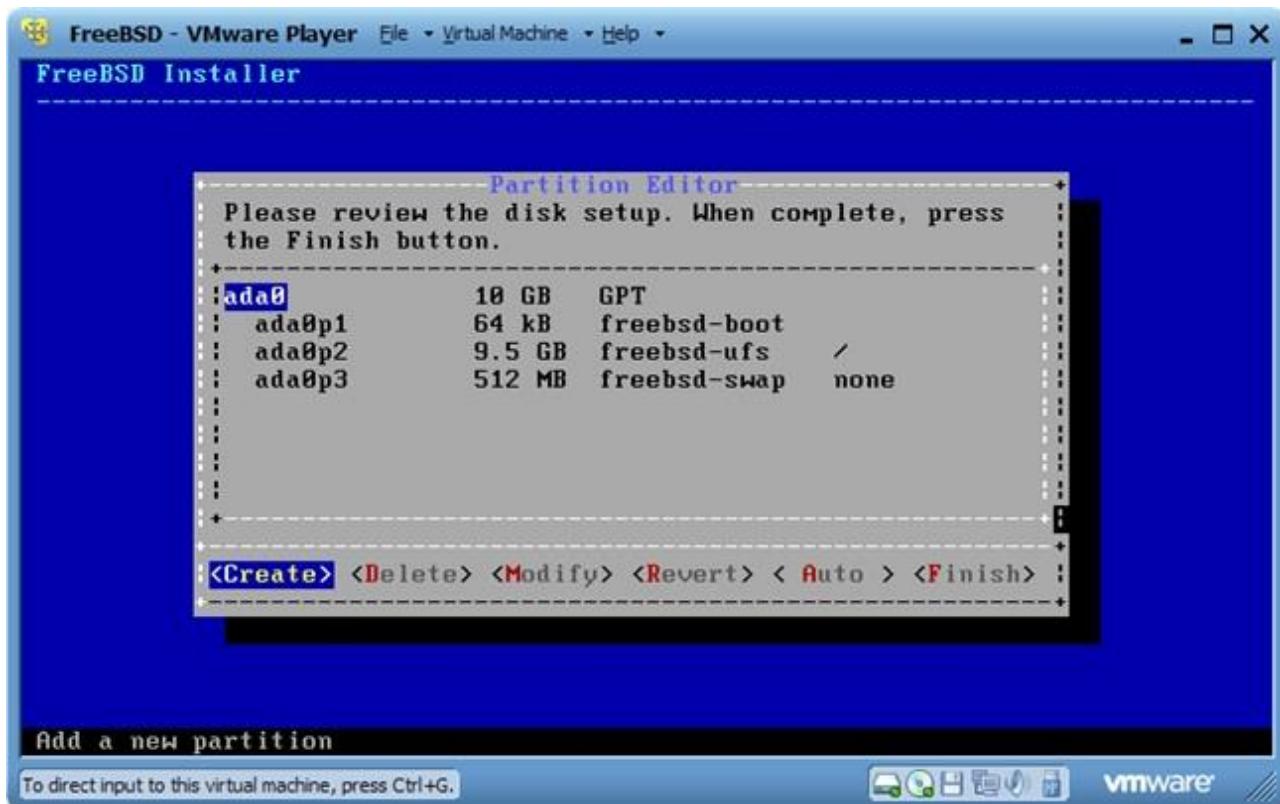


Рис. 9 Результат выбора EntireDisk

Перед вами диалоговое окно редактора разделов. Система сообщает: “Пожалуйста, проверьте правильность разметки диска. Когда закончите, нажмите кнопку Finish”. Как вы видите, система разделила всё дисковое пространство на три раздела: freebsd-boot – это раздел, необходимый для загрузки операционной системы; freebsd-ufs – это основной раздел, на котором будут храниться файлы О.С. и пользовательские файлы; freebsd-swap – это раздел “подкачки”, используемый для увеличения быстродействий системы. Далее выберите Finish и нажмите Enter. См. пункт 11.

10. При выборе Partition могут возникнуть две ситуации:

- Если на момент выбора Partition жёсткий диск совсем не размечен или имеет разметку GPT, то система автоматически формирует ИЗ НЕРАЗМЕЧЕННОГО пространства разделы, необходимые для установки и функционирования FreeBSD. На Рис. 10 изображён пример такого случая: перед выбором варианта Partition на диске находился раздел типа freebsd-ufs размером 3 Гб для хранения определённых данных.

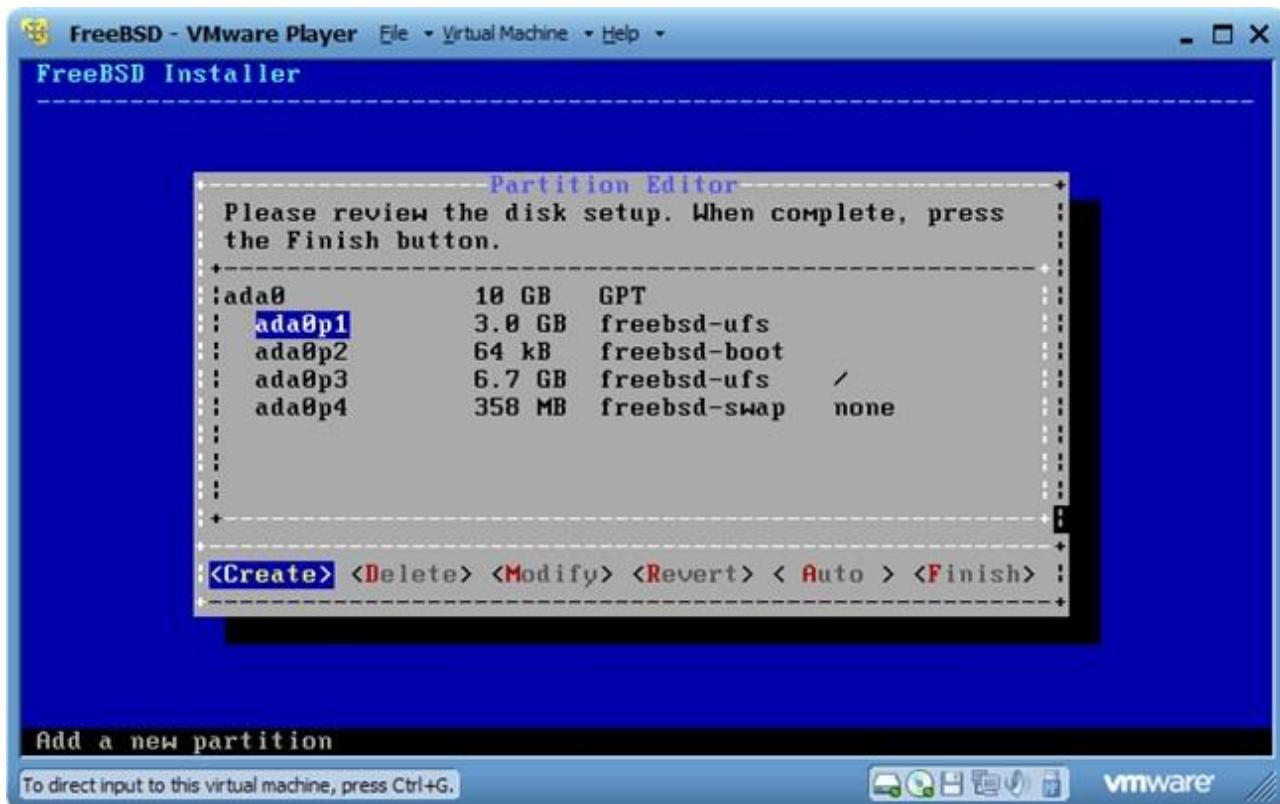


Рис. 10 Результат выбора варианта Partition при разметке GPT

Как вы видите, раздел типа freebsd-ufsразмером 3 Гб после действий системы остался нетронутым, а всё остальное неразмеченное пространство размером 7 Гб система распределила автоматически между тремя разделами: freebsd-boot – это раздел, необходимый для загрузки операционной системы;freebsd-ufs– это основной раздел, на котором будут храниться файлы О.С. и пользовательские файлы; freebsd-swap– это раздел “подкачки”, используемый для увеличения быстродействий системы. Далее выберите Finishи нажмите Enter. См. пункт 11.

В случае если на момент выбора Partition жёсткий диск имеет разметку типа отличного от GPT, система выдаст диалоговое окно, изображённое на Рис. 11.

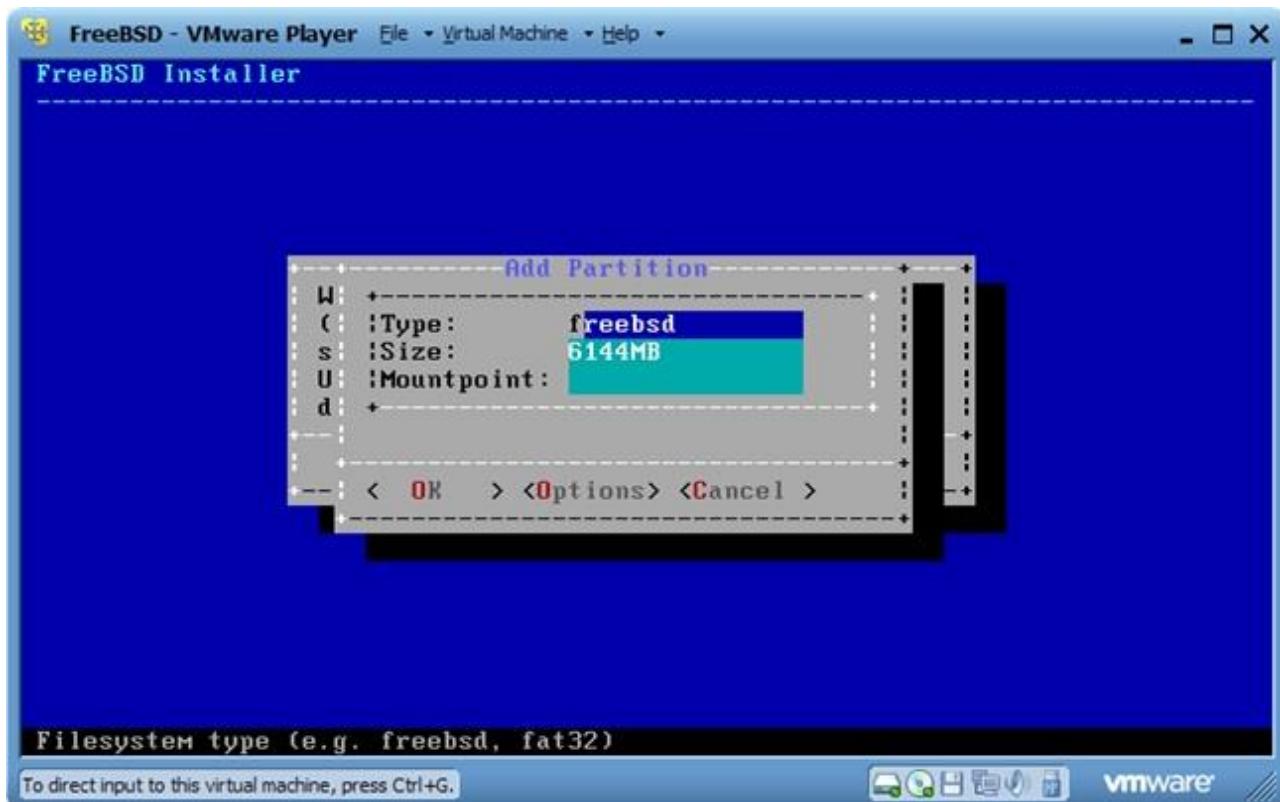


Рис. 11 Результат выбора варианта Partition при разметке отличной от GPT

В случае, изображённом на Рис. 11 на момент выбора Partition жёсткий диск имел разметку типа MBR, характерную для О.С. Dosi Windows, а также раздел с файловой системой NTFS размером 4 Гб. Поэтому система и предлагает нам создать раздел типа freebsd (что означает, что он будет использоваться для создания в нём подразделов необходимых для установки и функционирования FreeBSD) размером равным оставшемуся неразмеченному дисковому пространству (6 Гб).

Для изменения размера пространства, выделяющегося для раздела, выберите поле Size и введите необходимый размер. Для подтверждения действия нажмите Tab с помощью клавиш со стрелками выберите OK и нажмите Enter. На Рис. 12 изображён результат этих действий.

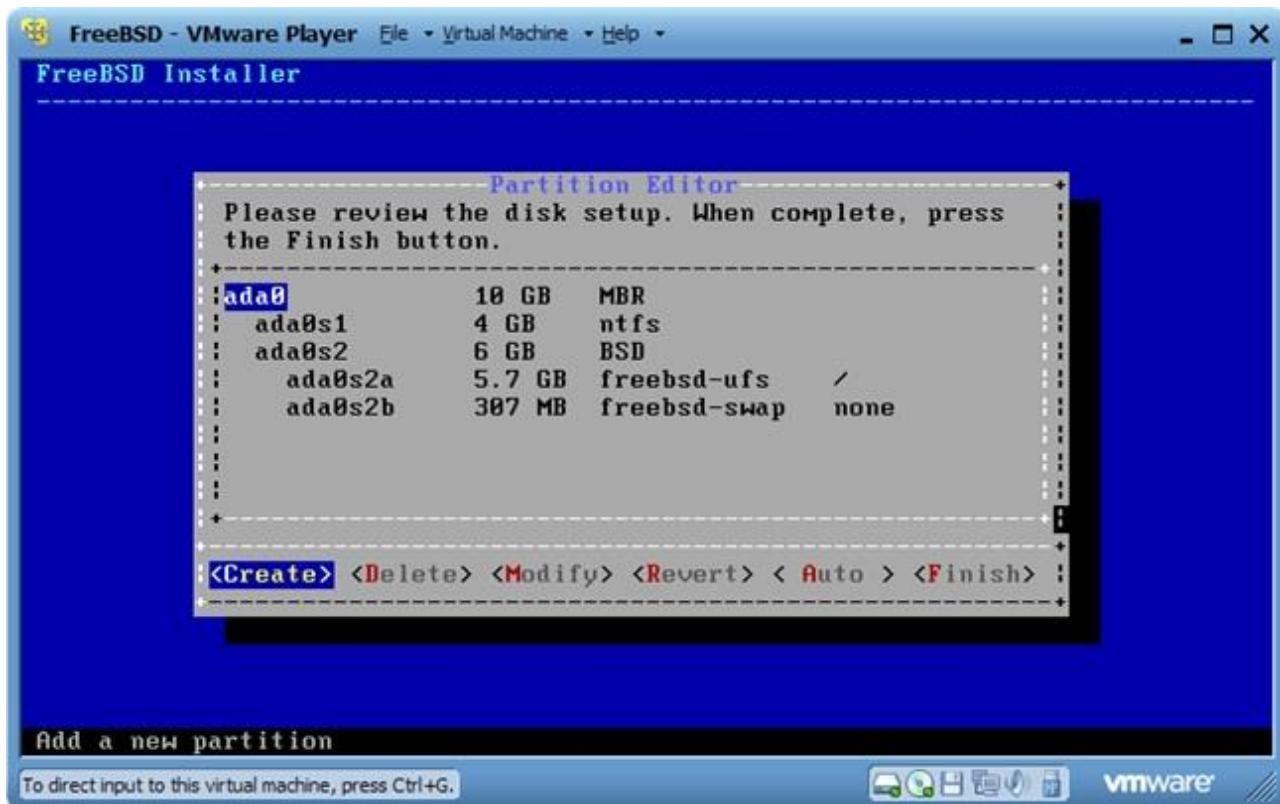


Рис. 12 Результат подтверждения создания раздела

Как вы видите, раздел типа NTFS размером 4 Гб после действий системы остался не-тронутым, а в неразмеченном ранее пространстве система сформировала новый раздел, размер которого мы указали равным оставшимся шести Гб. Пространство этого раздела система распределела автоматически между двумя разделами: freebsd-ufs – это основной раздел, на котором будут храниться файлы О.С. и пользовательские файлы; freebsd-swap – это раздел “подкачки”, используемый для увеличения быстродействий системы. Далее выберите Finish и нажмите Enter.

11. На следующем этапе появляется диалоговое окно, представленное на Рис. 13.



Рис. 13 Диалоговое окно подтверждения принятия изменений разметки

Система сообщает: “Сейчас будут сохранены все ваши изменения. Если вы выбрали перезапись имеющихся данных, они будут БЕЗВОЗВРАТНО СТЁРТЫ. Вы уверены, что хотите подтвердить все изменения?”.

На данном этапе вам доступны следующие действия:

- При выборе Commit система сохраняет все ваши действия по разметке диска и приступает к следующей стадии установки.
- При выборе Revert & Exit система отменяет ваши действия связанные с установкой FreeBSD и предлагает либо отменить, либо перезапустить установку с самого начала.
- При выборе Back система возвращается в редактор разделов.

Выберите Commit и нажмите Enter.

12. Далее система производит инициализацию файловой системы. Процесс инициализации изображён на Рис. 14.



Рис. 14 Инициализация файловой системы

После успешной инициализации файловой системы следует проверка контрольных сумм установочных архивов. Процесс проверки контрольных сумм изображён на Рис. 15.

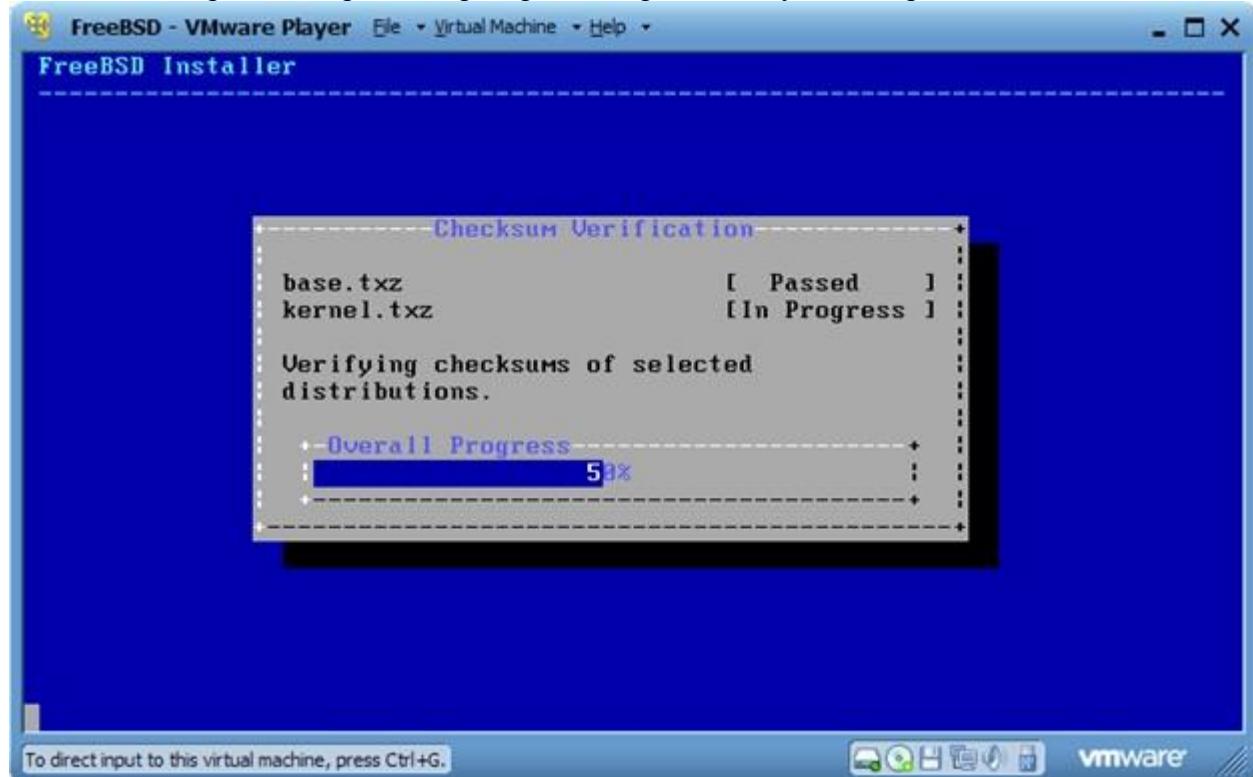


Рис. 15 Проверка контрольных сумм

После успешной проверки контрольных сумм установочных архивов следует извлечение из этих архивов данных. Процесс извлечения данных изображён на Рис. 16.

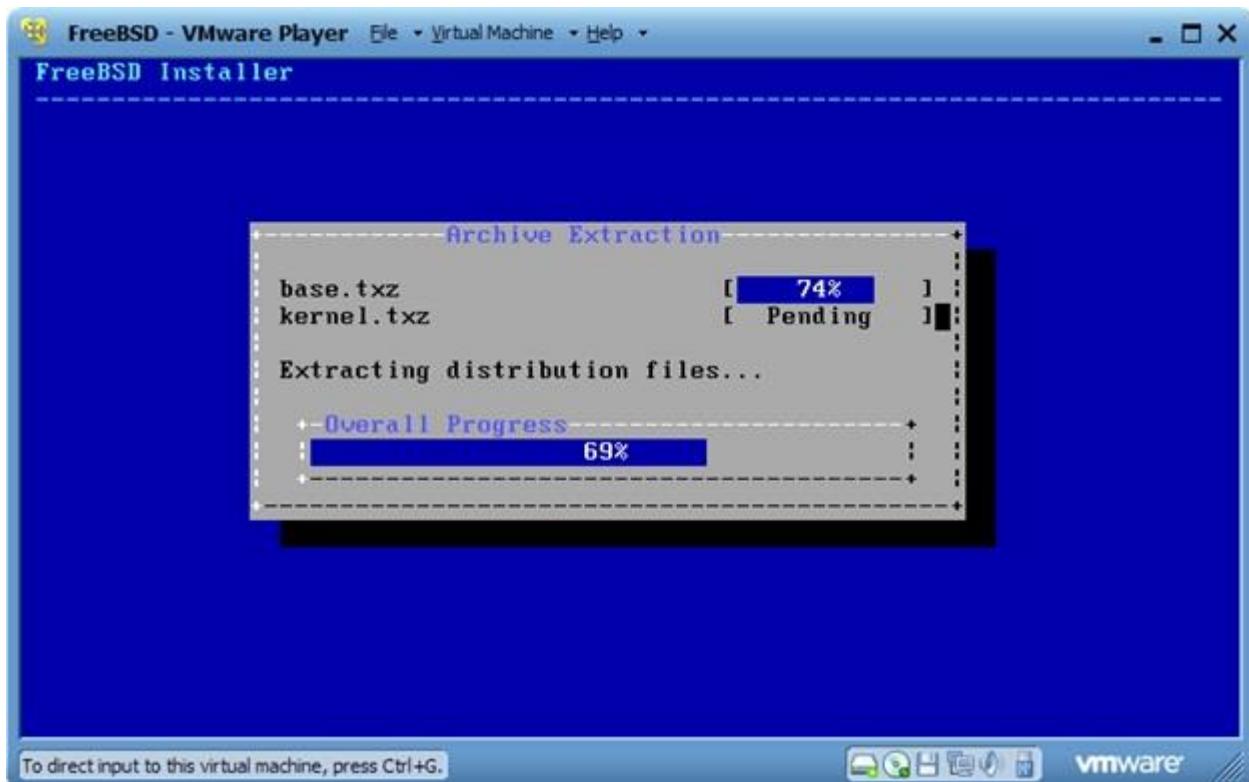


Рис. 16 Извлечение данных из архивов

13. После успешного выполнения всех трёх вышеперечисленных действий система выдаёт следующее сообщение, изображённое на Рис. 17.

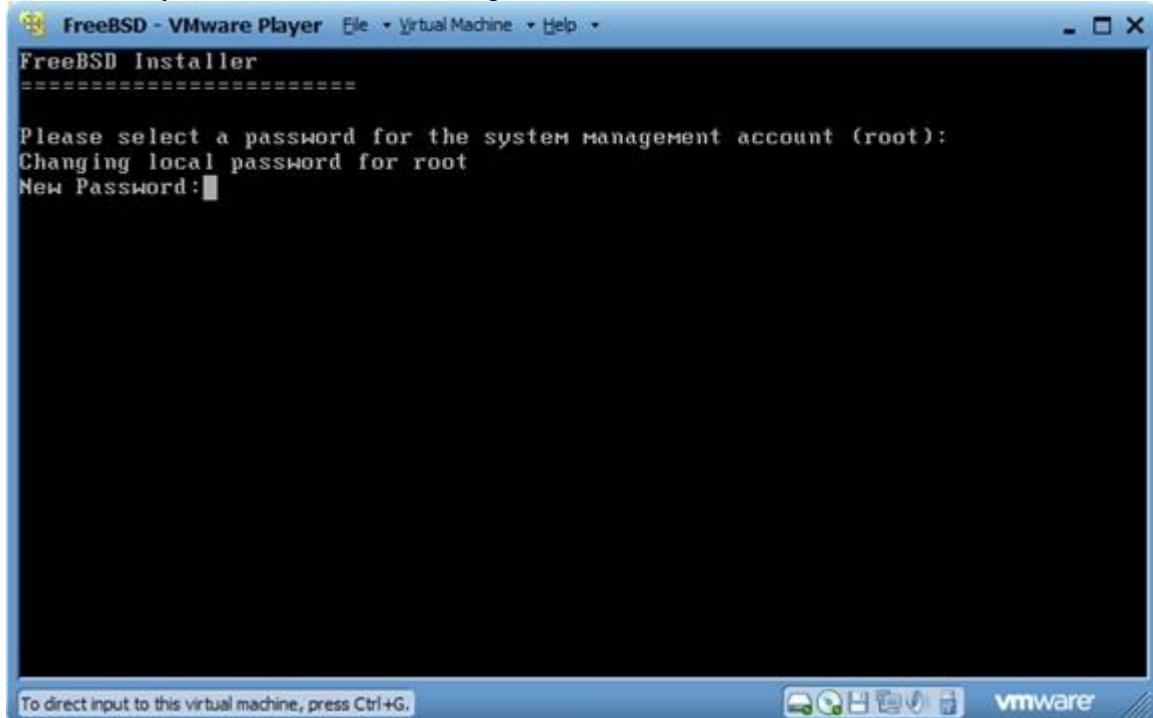


Рис. 17 Запрос ввода пароля для пользователя root

На данном этапе система сообщает: “Пожалуйста, выберите пароль для учётной записи управления системой (root): Изменение локального пароля для root”. ВНИМАНИЕ!!! В операционной системе FreeBSD имеется такая “особенность”, что при вводе пароля символы НЕ ОТОБРАЖАЮТСЯ, НО НА САМОМ ДЕЛЕ ВВОДЯТСЯ, поэтому будьте предельно внимательны при вводе пароля и его подтверждении. Введите необходимый вам пароль и нажмите Enter. Результат изображён на Рис 18.



Рис. 18 Запрос подтверждения введённого пароля для root

На данном этапе система просит подтвердить пароль. Введите этот же пароль ещё раз и нажмите Enter.

14. На следующем этапе появляется диалоговое окно, представленное на Рис. 19.



Рис. 19 Выбор сетевого интерфейса для настройки

На данном этапе вы можете настроить интерфейс (оборудование) для функционирования вашей рабочей станции в составе сети. Вы можете настроить любой из подключённых сетевых интерфейсов после установки операционной системы, обратившись к статье настройки сетевых интерфейсов в FreeBSD. На данном же этапе выберите Cancel и нажмите Enter.

15. На следующем этапе появляется диалоговое окно, представленное на Рис. 20.

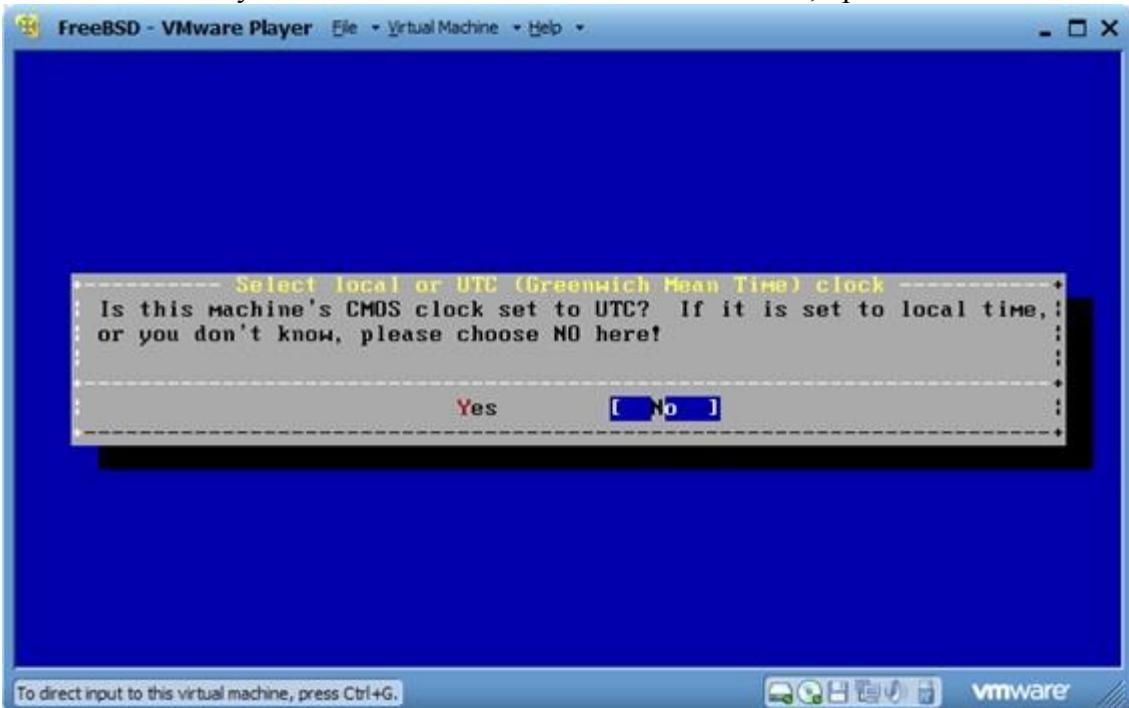


Рис. 20 Подтверждения установки среднего времени по Гринвичу

На данном этапе система сообщает: “Электронные схемы этой машины установлены на UTC? Если они установлены на местное время или вы просто не знаете, пожалуйста, выберите НЕТ”. Аббревиатура UTC означает единое мировое время. Выберите Нои нажмите Enter.

На следующем этапе появляется диалоговое окно, представленное на Рис. 21.



Рис. 21 Выбор временной зоны

На данном этапе вам необходимо выбрать временную зону, в которой вы находитесь, выбрать ОК и нажать Enter.

16. На следующем этапе появляется диалоговое окно, представленное на Рис. 22.



Рис. 22 Выбор страны или региона

На данном этапе вам необходимо выбрать страну или регион, в котором вы находитесь, выбрать OK и нажать Enter.

На следующем этапе появляется диалоговое окно, представленное на Рис. 23.



Рис. 23 Выбор местной временной зоны

На данном этапе вам необходимо выбрать местную для вашей страны или региона временную зону, выбрать OK и нажать Enter.

На следующем этапе появляется диалоговое окно, представленное на Рис. 24.



Рис. 24 Подтверждение аббревиатуры

На данном этапе система спрашивает: “Приемлема ли аббревиатура ‘SAKT’? ”. При задании временной зоны система формирует аббревиатуру, этой зоне соответствующую. Т.к. система не предоставляет возможности пользователю вручную изменить аббревиатуру, вам необходимо выбрать Yes и нажать Enter.

17. На следующем этапе появляется диалоговое окно, представленное на Рис. 25.

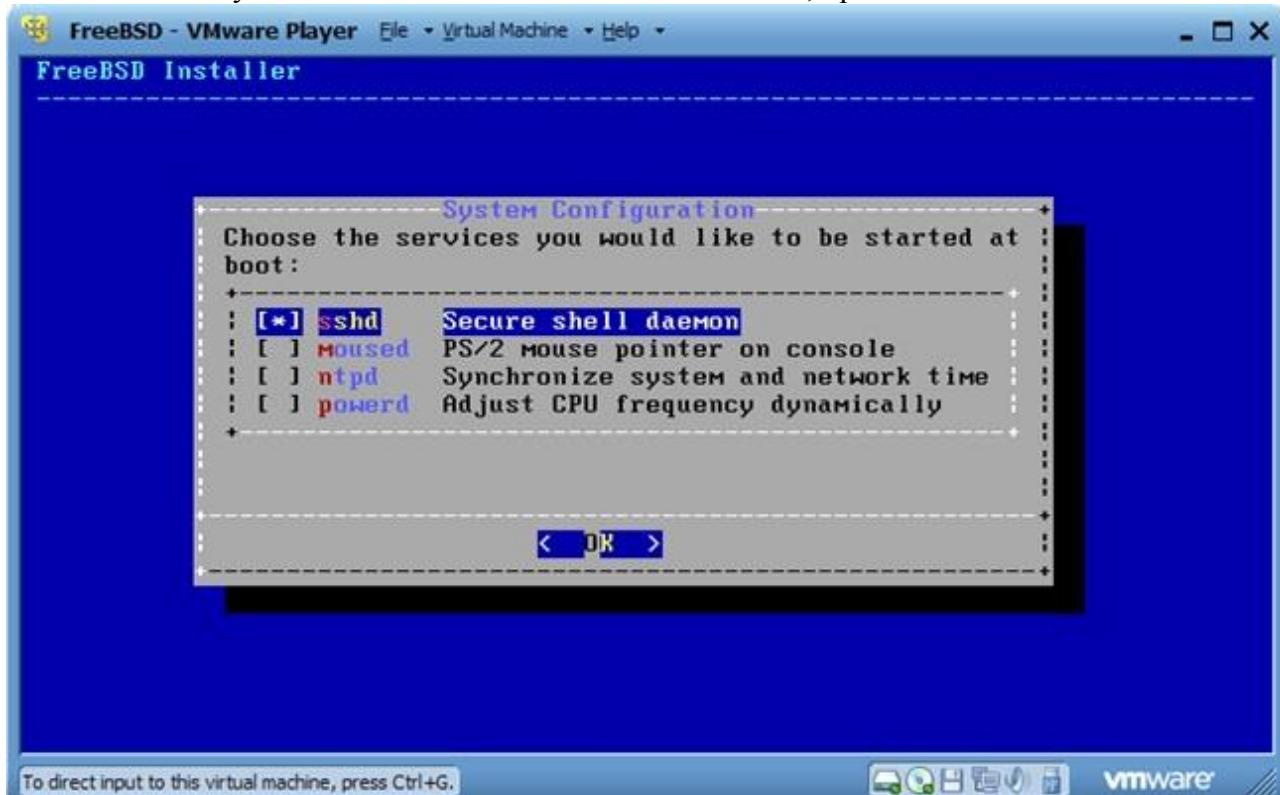


Рис. 25 Конфигурация системы

На данном этапе система сообщает: “Выберите службы, которые будут запускаться при запуске системы”. Предлагаемые варианты:

- sshd – это служба “безопасной оболочки”, работающая в фоновом режиме. (иными словами, режим шифрования данных во время работы с оболочкой системы).
- moused – это служба, позволяющая задействовать мышь, подключённую в PS/2 порт рабочей станции при работе в консоли.
- ntpd – это служба, периодически синхронизирующая системное время, сверяя его со временем в сети.
- powerd – это служба динамической настройки частоты центрального микропроцессора.

Выберите необходимые вам службы и нажмите Enter.

18. На следующем этапе появляется диалоговое окно, представленное на Рис. 26.



Рис. 26 Конфигурация сохранения информации о сбоях системы

На данном этапе система сообщает: “Вы бы хотели активировать сохранение информации о сбоях системы? Если у вас появятся какие-то проблемы с системой, это сможет помочь разработчикам FreeBSD исправить эти проблемы. Но информация о сбоях системы может занять большой объём дискового пространства в каталоге /var”. Если вам необходимо сохранять информацию о сбоях системы, выберите Yes и нажмите Enter. В противном случае ваш вариант – No.

19. На следующем этапе появляется диалоговое окно, представленное на Рис. 27.

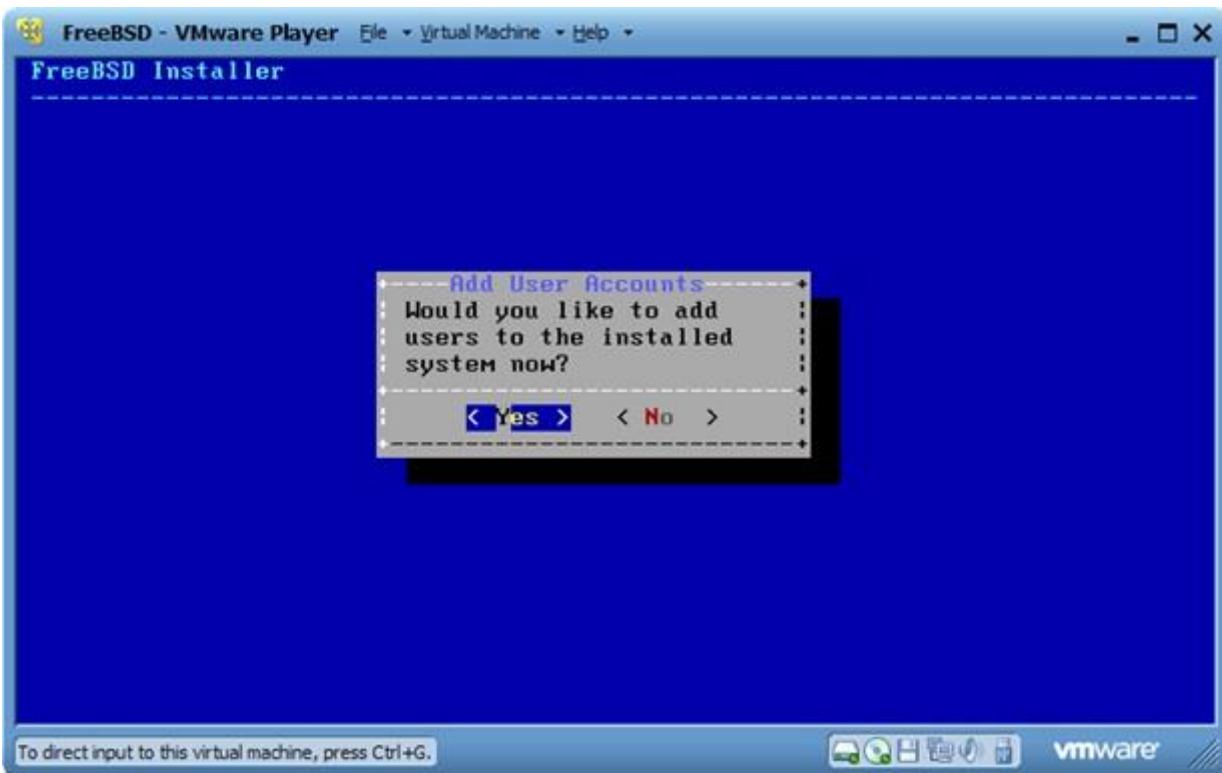


Рис. 27 Добавление учётных записей пользователя

На данном этапе система сообщает: “Вы бы хотели сейчас добавить пользователей в установленную систему?”. Если вам нет необходимости добавлять пользователей, см. пункт 24.

Выберите Yes и нажмите Enter.

20. На следующем этапе появляется диалоговое окно, представленное на Рис. 28.

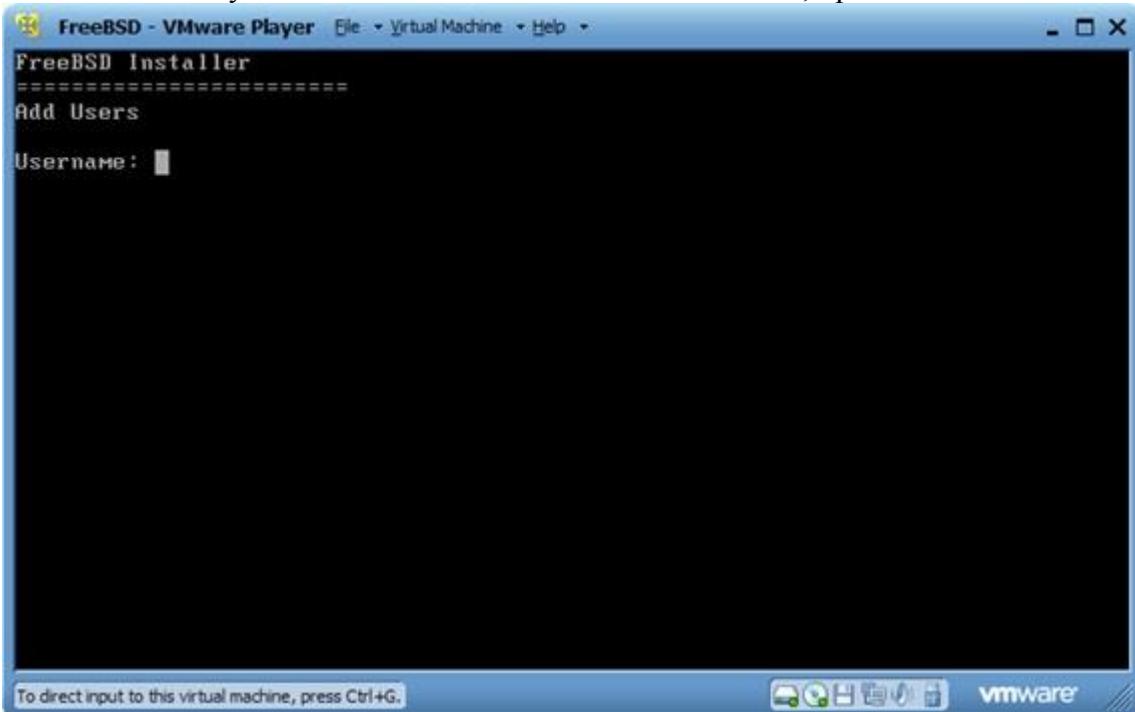
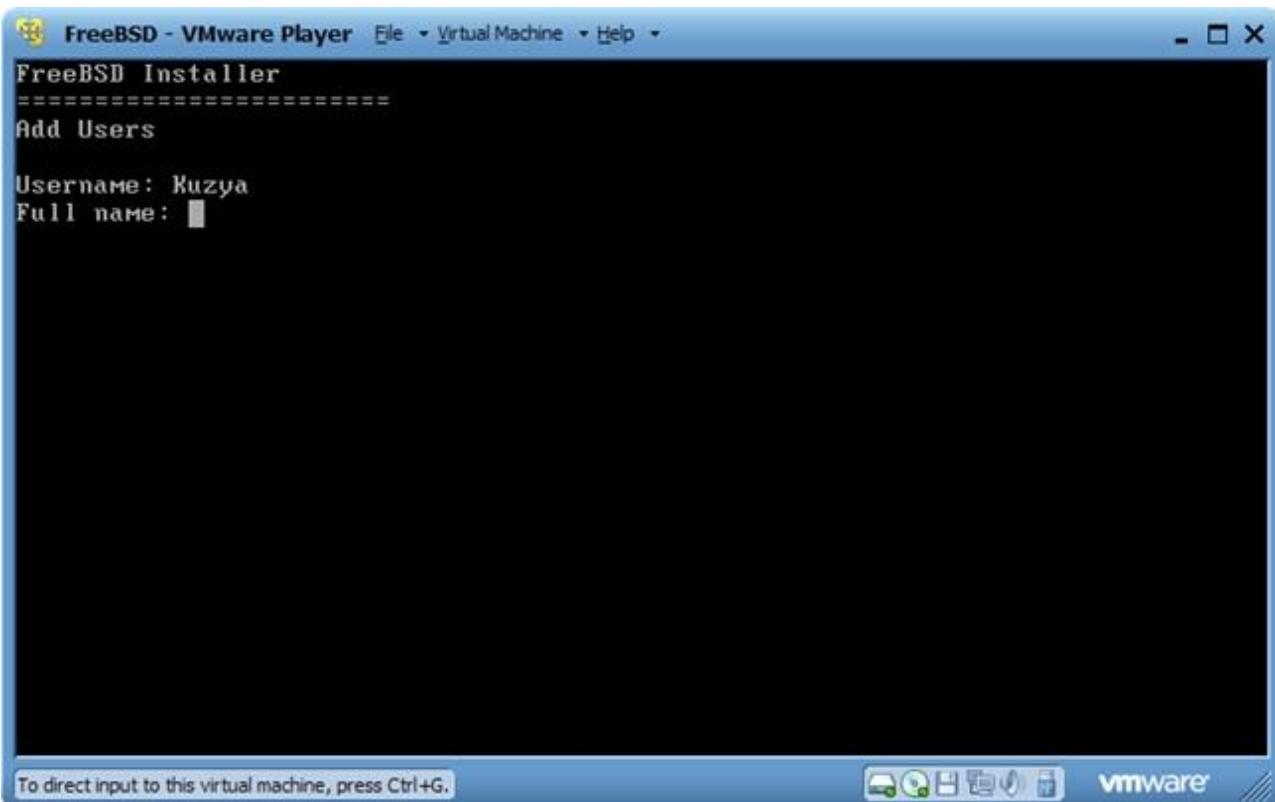
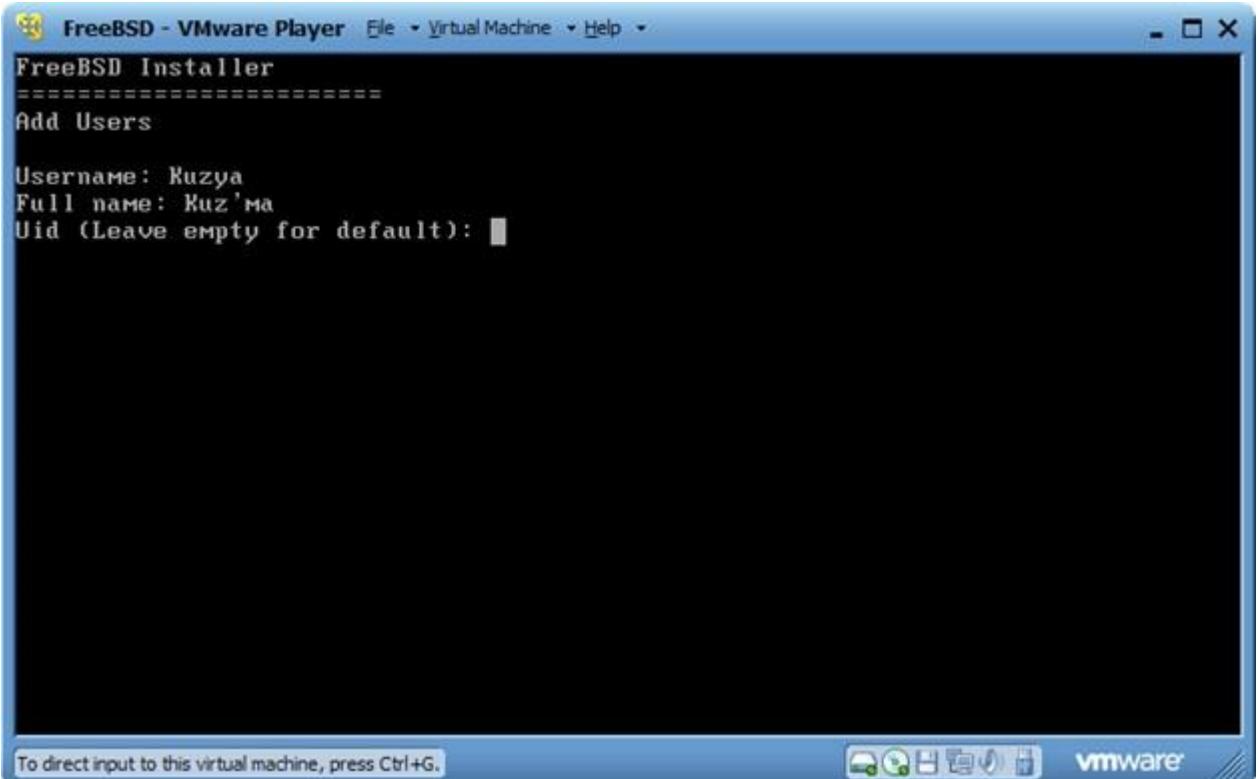


Рис. 28 Ввод имени пользователя

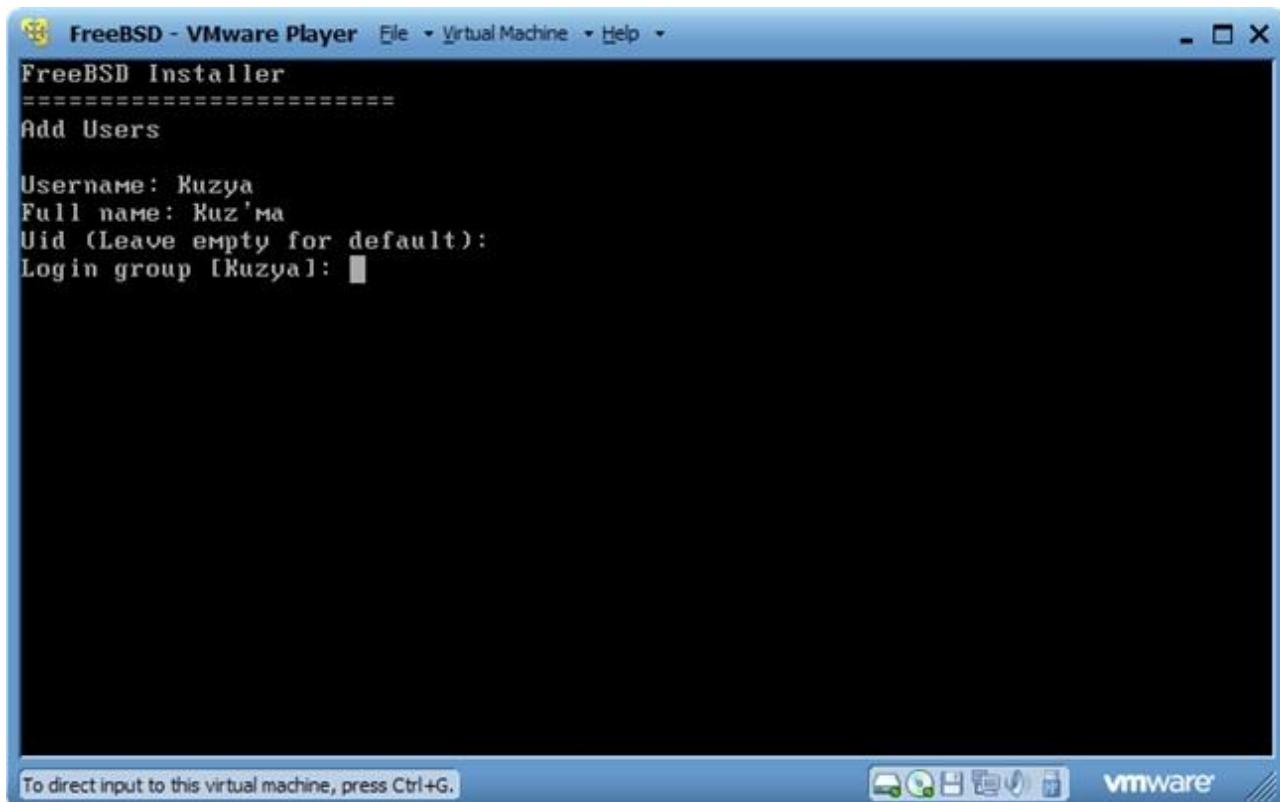
Введите имя пользователя и нажмите Enter.



Введите полное имя пользователя и нажмите Enter.



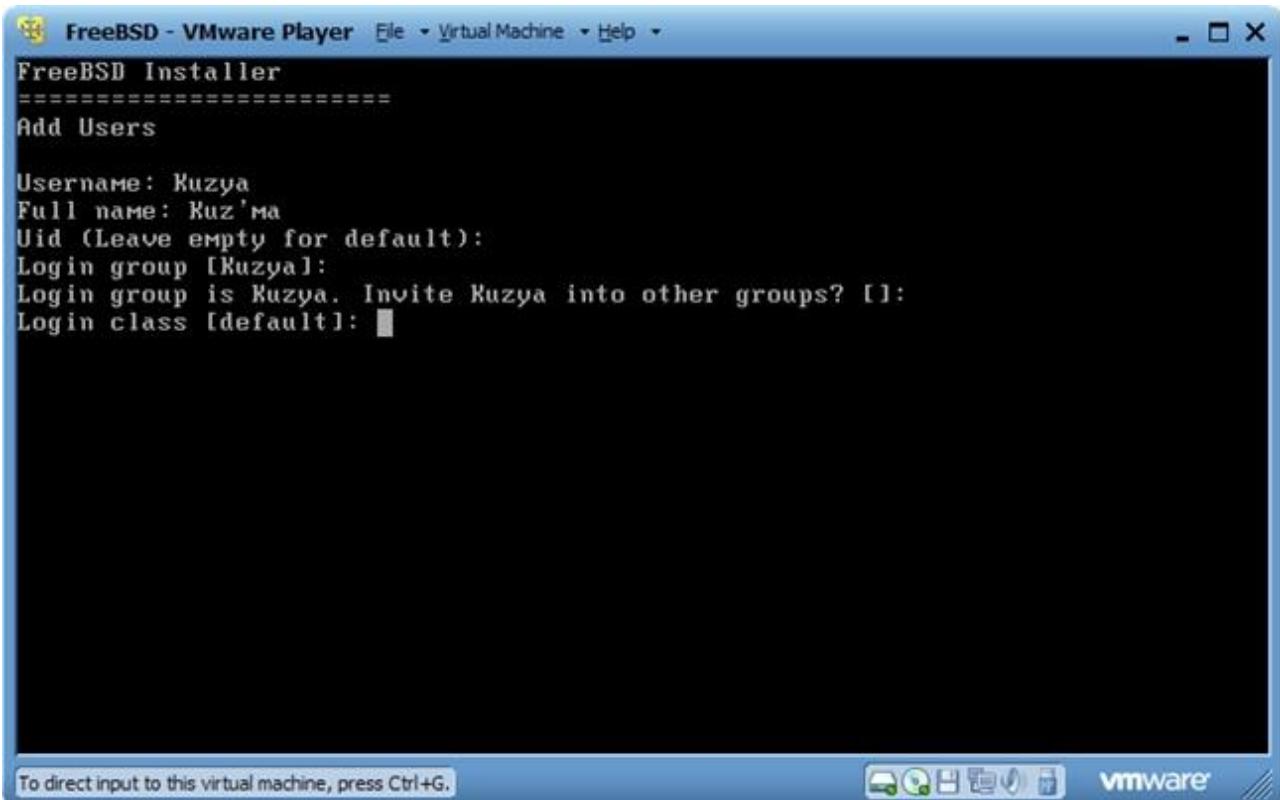
Введите идентификатор пользователя и нажмите Enter или оставьте поле пустым и нажмите Enter для установки идентификатора пользователя по умолчанию.



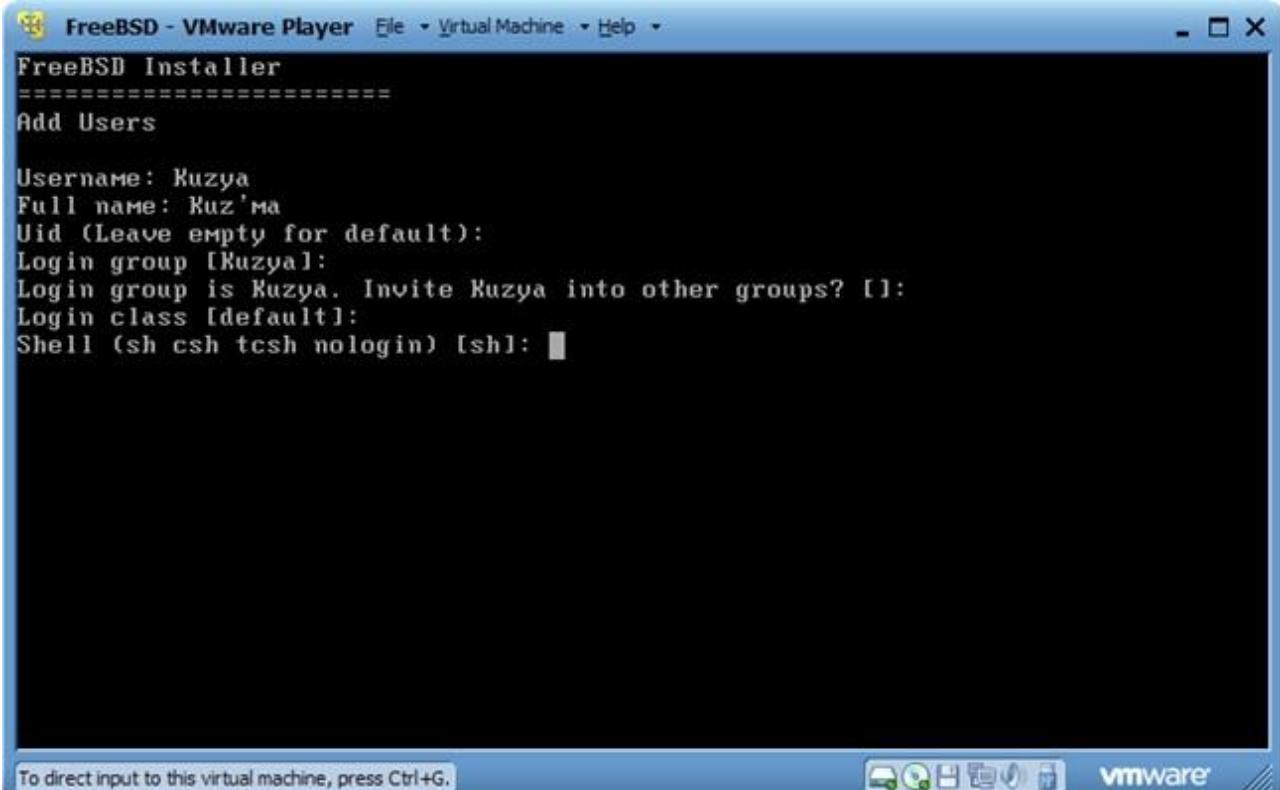
Введите название loginгруппы и нажмите Enter. В квадратных скобках указывается значение по умолчанию, которое можно ввести и которое будет присвоено атрибуту (в данном случае атрибутом является loginгруппа пользователя) в случае, если вы оставите поле пустым.



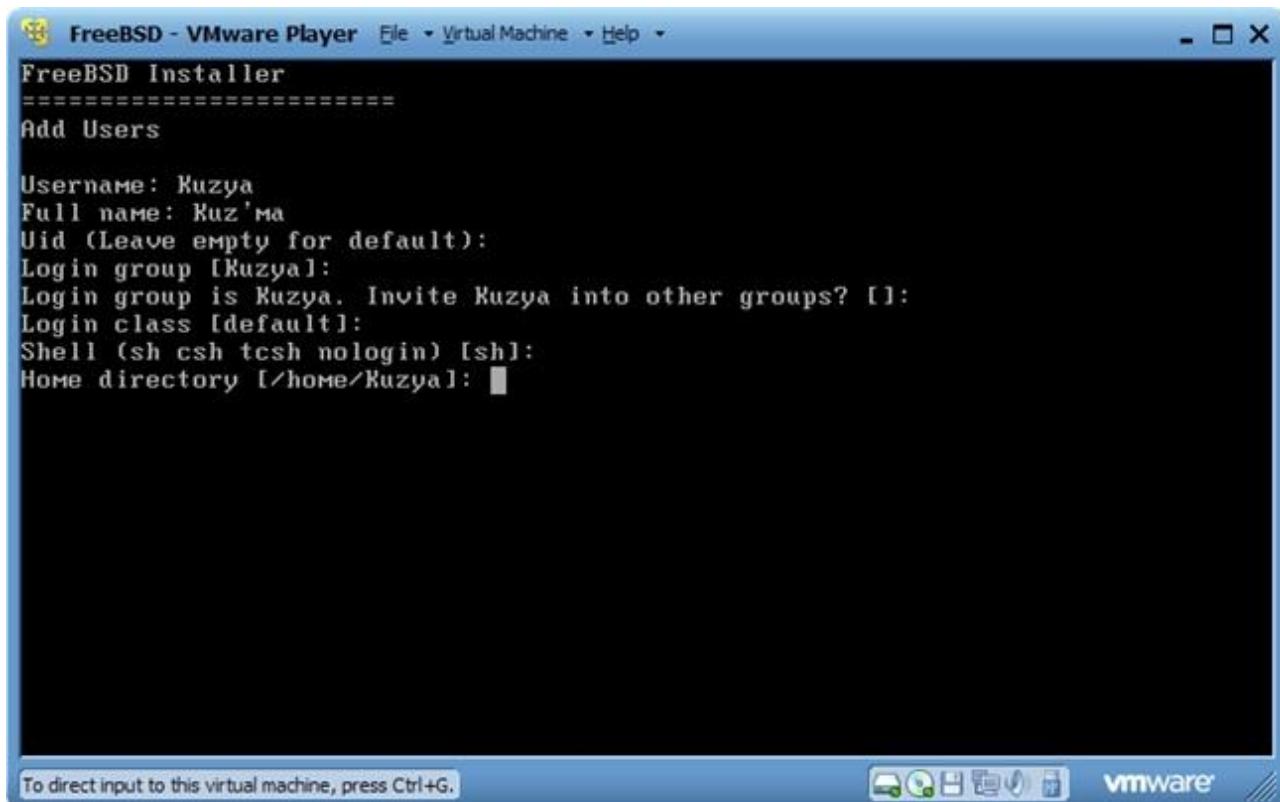
Система спрашивает, хотите ли вы сделать данного пользователя членом ещё каких-либо login групп. Введите необходимые вам группы и нажмите Enter.



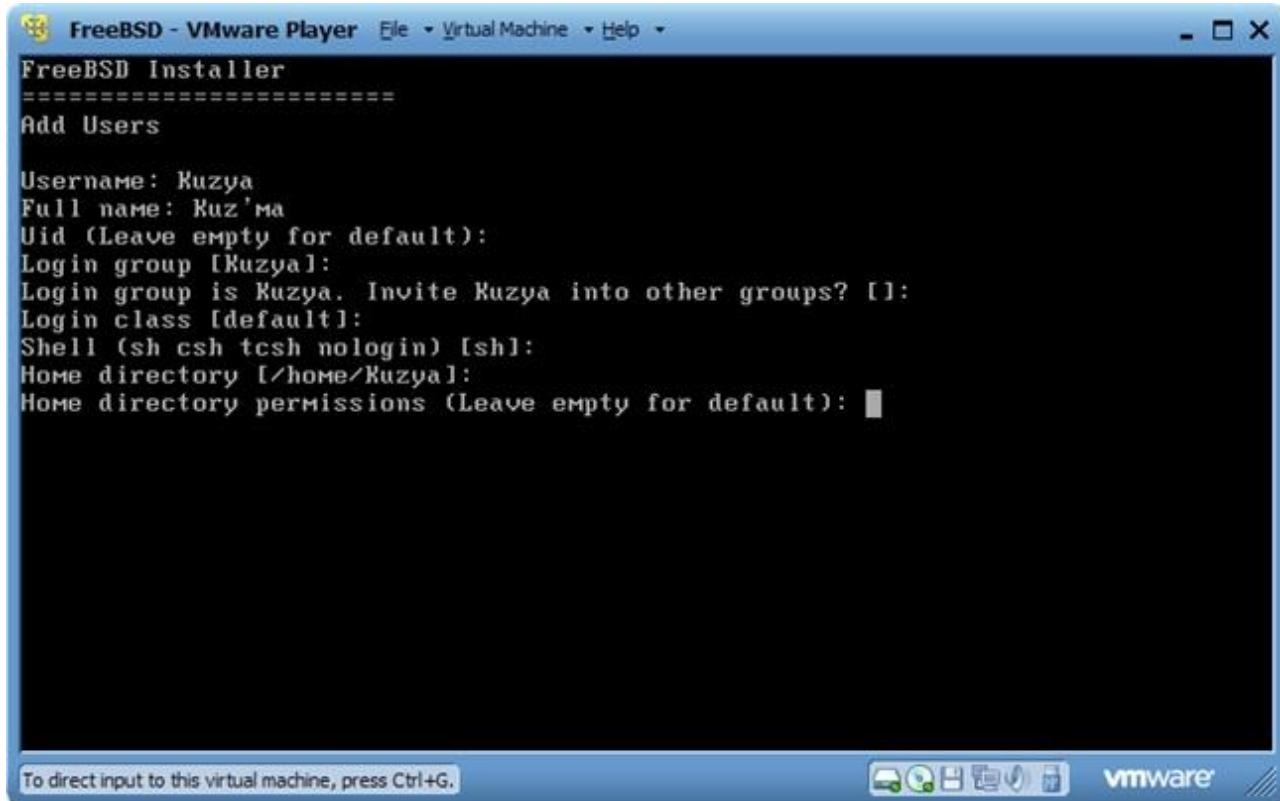
Введите название login класса для данного пользователя и нажмите Enter.



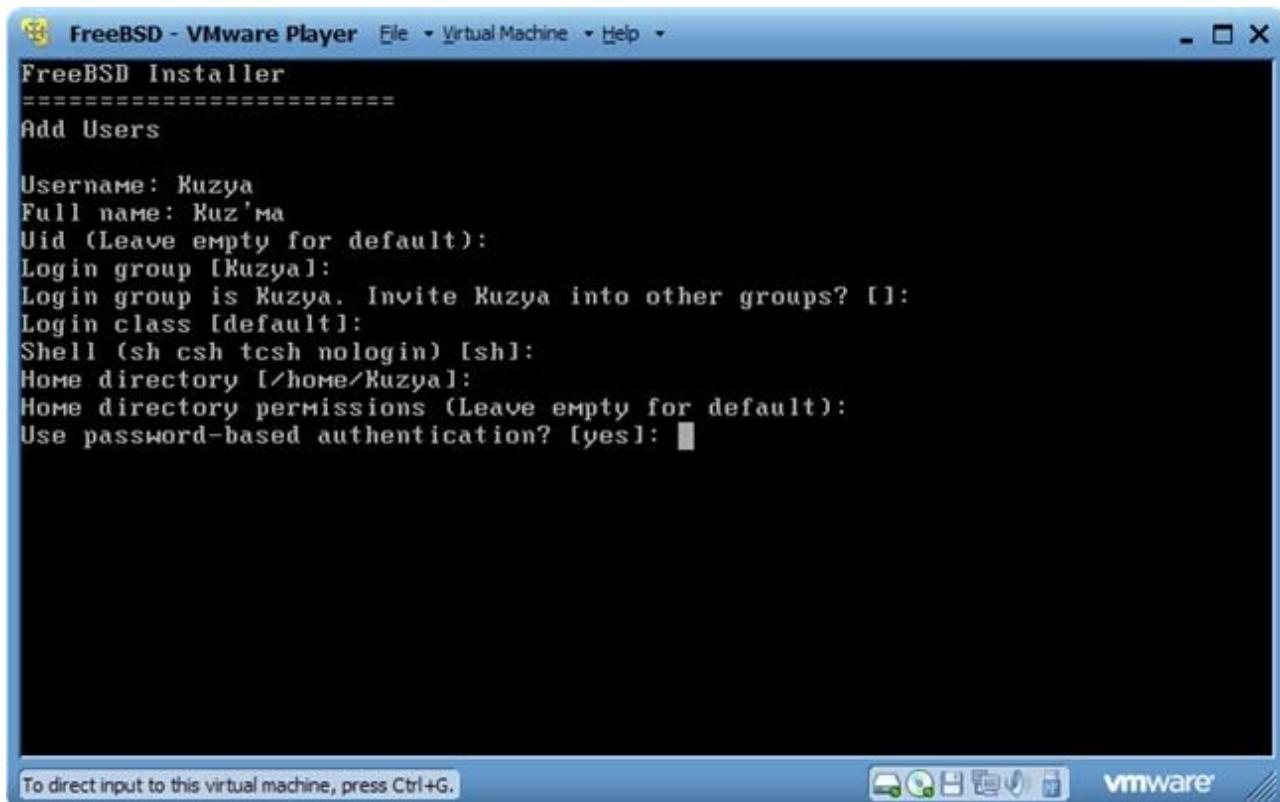
Введите название оболочки, которая будет использоваться для данного пользователя и нажмите Enter. В круглых скобках указывается подсказка (в данном случае это названия доступных для ввода оболочек).



Введите путь директории, которая будет являться домашней директорией данного пользователя и нажмите Enter.



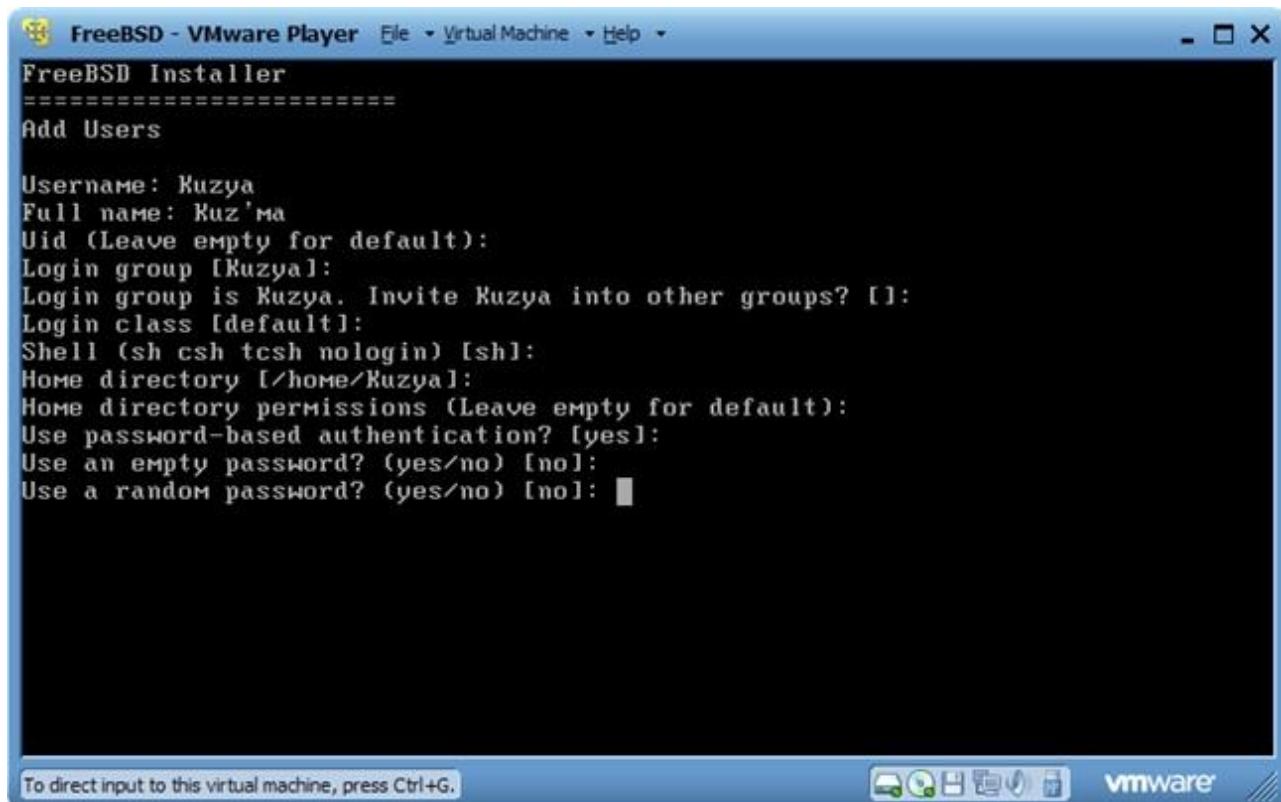
Введите разрешения для домашней директории данного пользователя и нажмите Enter или же оставьте поле пустым для значения разрешений по умолчанию и нажмите Enter.



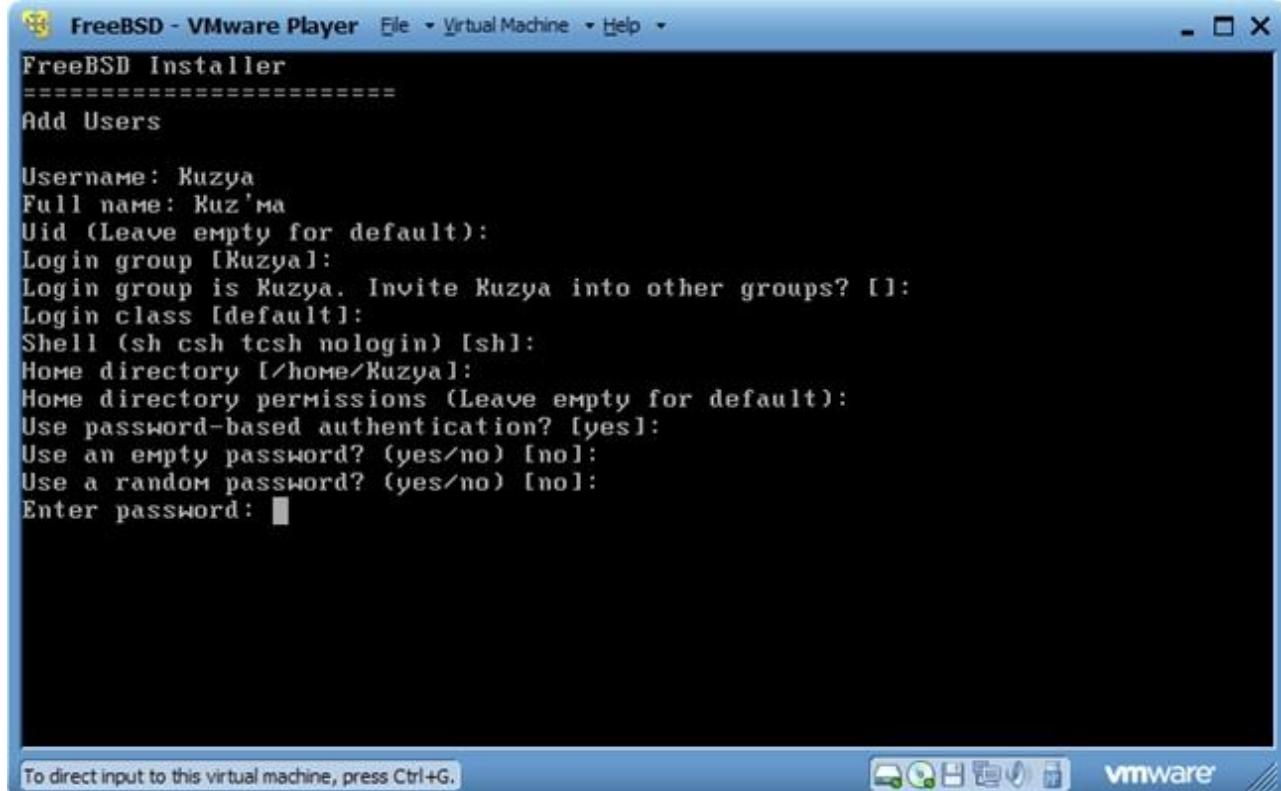
Система спрашивает, использовать ли пароль для аутентификации данного пользователя. Оставьте поле пустым для подтверждения и нажмите Enter или же введите no для отказа и нажмите Enter.



Использовать ли пустой пароль? Введите ответ и нажмите Enter.



Использовать ли случайным образом сгенерированный системой пароль? Введите ответ и нажмите Enter.



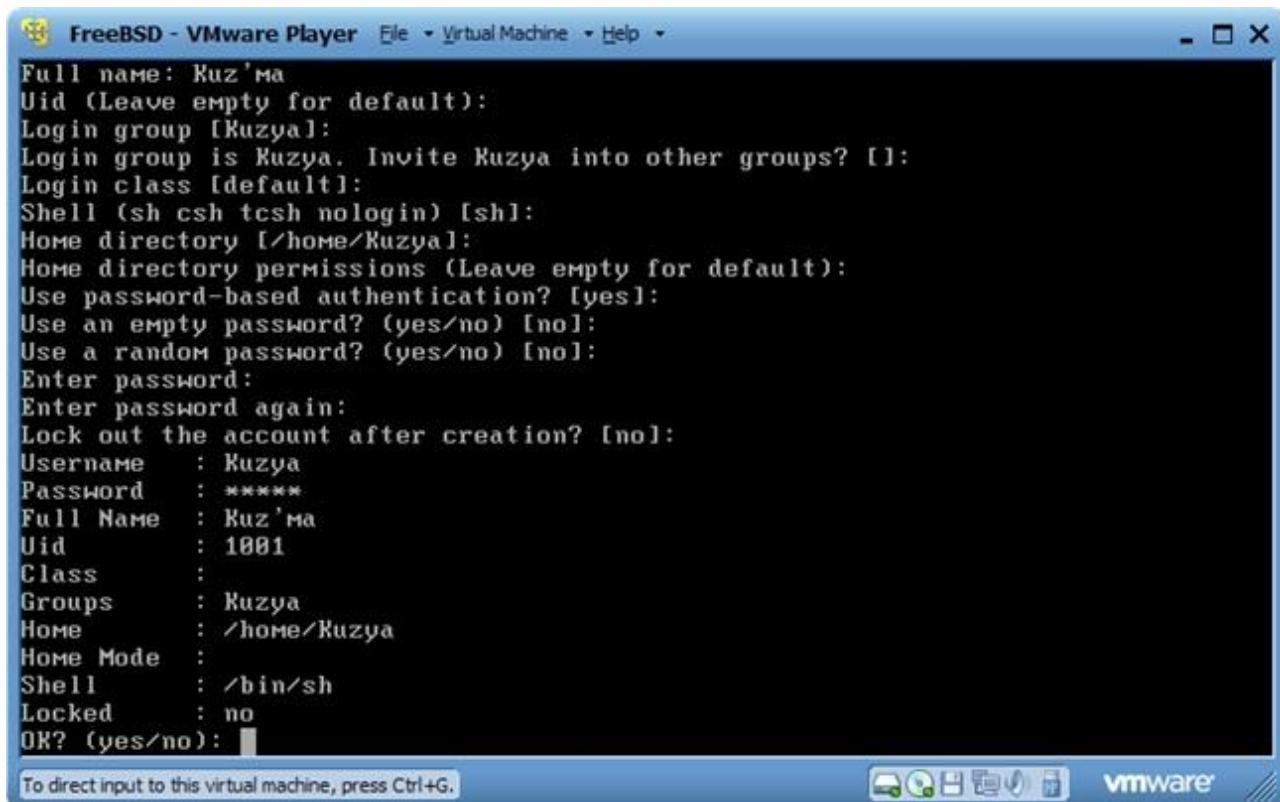
Введите необходимый вам пользовательский пароль и нажмите Enter.



Введите данный пароль ещё раз для подтверждения и нажмите Enter.



Заблокировать ли учётную запись после создания? Введите ответ и нажмите Enter.



FreeBSD - VMware Player File → Virtual Machine → Help

```

Full name: Kuz'ma
Uid (Leave empty for default):
Login group [Kuzya]:
Login group is Kuzya. Invite Kuzya into other groups? []:
Login class [default]:
Shell (sh csh tcsh nologin) [sh]:
Home directory [/home/Kuzya]:
Home directory permissions (Leave empty for default):
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
Use a random password? (yes/no) [no]:
Enter password:
Enter password again:
Lock out the account after creation? [no]:
Username : Kuzya
Password : *****
Full Name : Kuz'ма
Uid : 1001
Class :
Groups : Kuzya
Home : /home/Kuzya
Home Mode :
Shell : /bin/sh
Locked : no
OK? (yes/no): 

```

To direct input to this virtual machine, press Ctrl+G. vmware

Система выводит всю введённую ранее вами информацию для проверки её правильности. Убедитесь, что всё заполнено верно, если да, то введите yes и нажмите Enter. В противном же случае введите no и нажмите Enter.



FreeBSD - VMware Player File → Virtual Machine → Help

```

Login group [Kuzya]:
Login group is Kuzya. Invite Kuzya into other groups? []:
Login class [default]:
Shell (sh csh tcsh nologin) [sh]:
Home directory [/home/Kuzya]:
Home directory permissions (Leave empty for default):
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
Use a random password? (yes/no) [no]:
Enter password:
Enter password again:
Lock out the account after creation? [no]:
Username : Kuzya
Password : *****
Full Name : Kuz'ма
Uid : 1001
Class :
Groups : Kuzya
Home : /home/Kuzya
Home Mode :
Shell : /bin/sh
Locked : no
OK? (yes/no): yes
adduser: INFO: Successfully added (Kuzya) to the user database.
Add another user? (yes/no): 

```

To direct input to this virtual machine, press Ctrl+G. vmware

В случае подтверждения и правильности заполнения всей необходимой информации об учётной записи система выведет сообщение, представленное на рисунке выше. Затем система спрашивает: “Добавить ли нового пользователя?”. Процедура добавления каждого нового пользователя идентична. После добавления всех необходимых вам пользователей введите no и нажмите Enter.

На следующем этапе появляется диалоговое окно, представленное на Рис. 29.

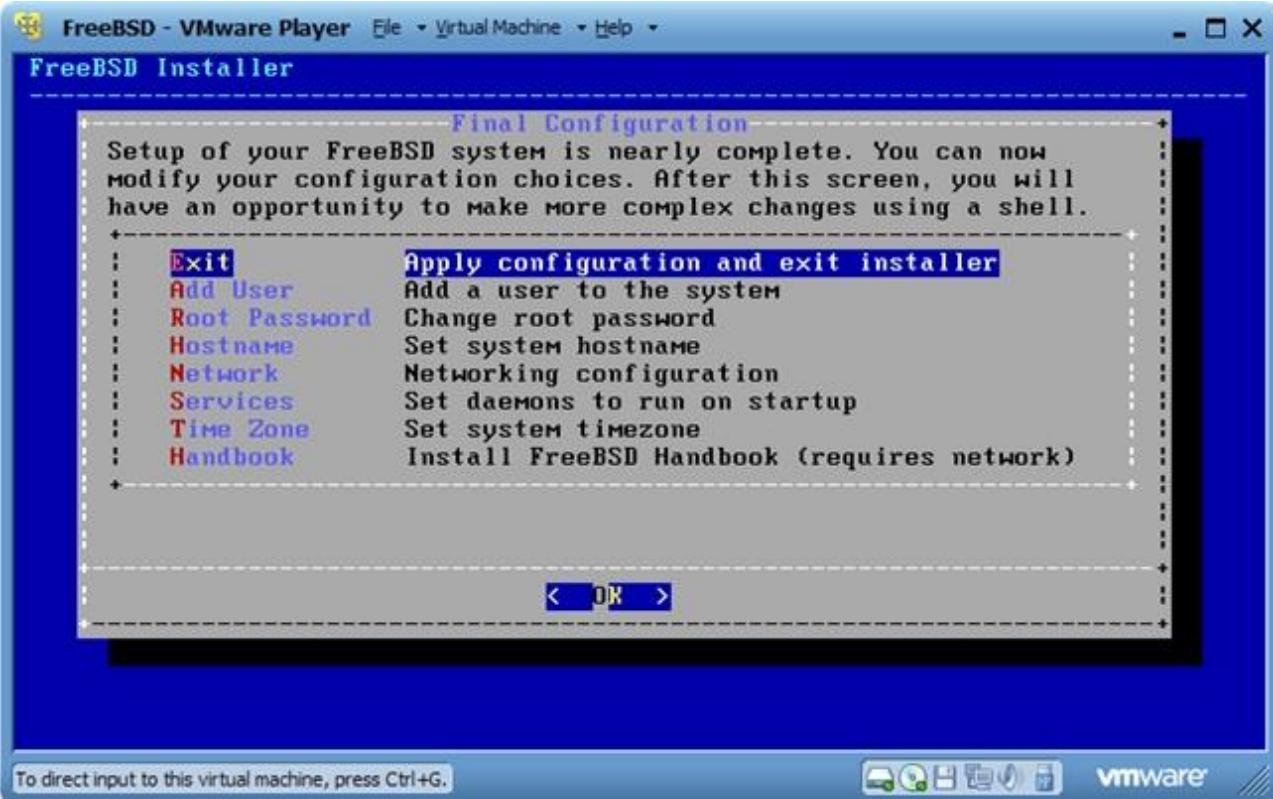


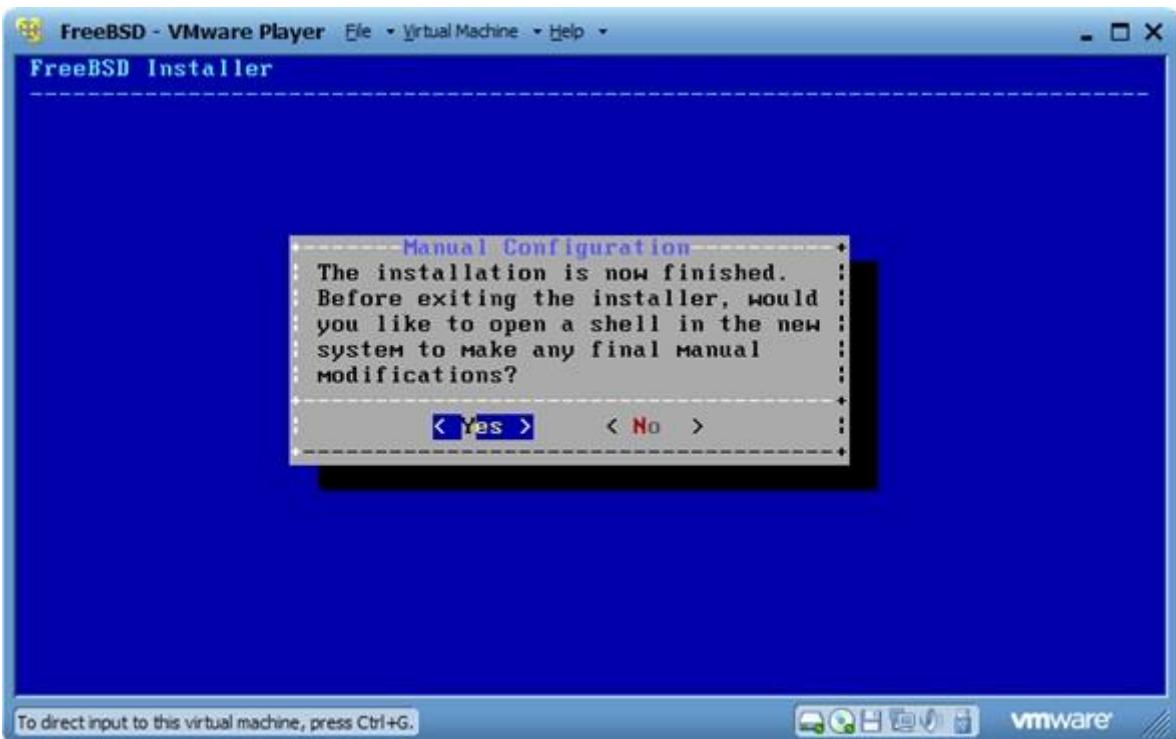
Рис. 29 Заключительная конфигурация

На данном этапе система сообщает: “**Установка вашей операционной системы FreeBSD** почти завершена. Сейчас вы можете настроить ранее вами выбранные конфигурации. После закрытия этого окна вы сможете реализовать более сложные настройки системы, используя оболочку”. Доступные действия:

- Exit – применить все настройки и выйти из установщика.
- AddUser – добавить пользователя в систему.
- RootPassword – изменить пароль root.
- Hostname – установить имя системы (компьютера).
- Network – настройка сети.
- Services – выбор служб, которые будут запускаться при запуске системы.
- TimeZone – установить временную зону системы.
- Handbook – установить руководство по FreeBSD (необходимо наличие сети (интернет)).

Если вам необходимо настроить один из этих компонентов, выберите его, нажмите Enter и обратитесь ещё раз к соответствующему разделу установки. Если вы настроили нужным вам образом, выберите Exit и нажмите Enter.

21. Установка FreeBSD закончена, если вы видите на экране следующее:



Система спрашивает, хотите ли вы запустить оболочку, чтобы вручную выполнить заключительные изменения. Выберите No и нажмите Enter.



Система сообщает: “**Установка FreeBSD успешно завершена!** Вы хотите перезагрузиться для работы в новой системе?”. Выберите Reboot для перезагрузки и начала работы в новой системе или же выберите Live CD для запуска соответствующей версии с носителя. Нажмите Enter.

2.2 Установка и настройка приложений

После загрузки система попросит ввести имя пользователя и пароль. Вводим «root» и пароль, указанный во время установки. Как видите, перед нами голая система — никакого графического интерфейса, поднятого веб-сервера и тд. Только терминал.

На самом деле терминалов не один, а восемь. Переключаться между ними можно с помощью комбинации клавиш **Ctrl+Alt+F1..F8** или, если вы используете VMWare Player, **Shift+Ctrl+Alt+F1..F8** (а иногда — **Alt+F1..F8**).

Когда мы установим графический интерфейс, он будет работать на девятом терминале (**F9**), и остальные 8 при этом будут по-прежнему доступны. Это так, информация к сведению.

Bo FreeBSD есть несколько способов установки программ. В рамках этой заметки мы будем использовать самый простой и быстрый способ — установку бинарных пакетов с DVD диска (если вы использовали для установки CD, то можете не искать на нем бинарных пакетов, их придется ставить по сети). Выполняем команду:

```
ls /dev | grep cd
```

Мы должны увидеть что-то вроде **acd0** или **cd0**. Это — имя, под которым система видит оптический накопитель. В отличие от Windows и Ubuntu «голая» FreeBSD не открывает диски и флешки автоматически. Также, в отличие от Windows, здесь нет «диска C:», «диска D:» и тп. Вся файловая система — это одно дерево каталогов. Чтобы увидеть содержимое DVD диска, нужно выделить для него пустой каталог и **примонтировать** к нему носитель. Вот как это сделать:

```
# создаем каталог mkdir /mnt/cdrom
# монтируем диск mount -t cd9660 /dev/acd0 /mnt/cdrom
# смотрим содержимое диска ls /mnt/cdrom
# также /mnt/cdrom должен быть в списке точек монтирования df -h
```

Если все сделано правильно, в каталоге **/mnt/cdrom** мы увидим содержимое DVD диска. Интересующие нас бинарные пакеты находятся в **/mnt/cdrom/packages/All**, но их там довольно много, так что для просмотра каталога нужно использовать связку **ls + less** или **ls + grep**. На самом деле, нас интересуют только два пакета:

```
ls /mnt/cdrom/packages/All | grep gnome2
ls /mnt/cdrom/packages/All | grep xorg
```

На моем диске версии пакетов были **gnome2-2.26.3** и **xorg-7.4_2**.

Установка пакетов производится с помощью команды **pkg_add**. Но перед установкой мы должны присвоить значение переменной окружения **PKG_PATH**, чтобы программа знала, где искать пакеты.

```
setenv PKG_PATH /mnt/cdrom/packages/All
```

Затем приступаем к самой установке:

```
pkg_add gnome2-2.26.3
```

xorg-7.4_2

Это займет какое-то время. Вместе с нужными нам программами также будут установлены все пакеты, от которых они зависят. Во время установки мы увидим различные сообщения — это комментарии к устанавливаемым пакетам. Можете не обращать на них внимания.

Раньше перед тем, как использовать Xorg, его следовало настроить. Но начиная с версии Xorg 7.3 это не обязательно.

Большинство настроек FreeBSD хранит в файле **/etc/rc.conf**. Сейчас нам предстоит его отредактировать, чтобы при загрузке системы запускался GDM (Gnome Desktop Manager). Это та программа, которая выводит окошко с просьбой ввести логин и пароль, а затем, если данные введены правильно, запускает Gnome. Редактировать будем с помощью утилиты под названием ее (**easy editor**):

```
ee /etc/rc.conf
```

Использовать редактор не сложнее, чем «Блокнот». Дописываем в конец файла следующие строки:

```
gnome_enable="YES"
```

```
# Следующие две строчки нужно закомментировать с помощью знака решетки
```

```
# если во время работы Gnome возникают какие-то проблемы.
```

```
# Например, не заработает мышка или клавиатура.
```

```
# После внесения изменений следует перезагрузиться.
```

```
halld_enable="YES"
```

```
dbus_enable="YES"
```

```
gdm_enable="YES"
```

```
gdm_lang="ru_RU.UTF-8"
```

Затем сохраняемся и выходим. Последний этап — это создание пользователя для постоянной работы. Сидеть под пользователем root небезопасно, хотя бы потому что одна неверная команда, введенная случайно, может убить всю систему.

Говорим «adduser», после чего отвечаем на простые вопросы вроде «укажите имя» или «введите пароль». На непонятные вопросы можно просто ответить нажатием клавиши Enter. На вопрос «Invite user to another groups?» обязательно ответьте «wheel», иначе созданный пользователь не сможет выполнять команду su для получения прав root'a.

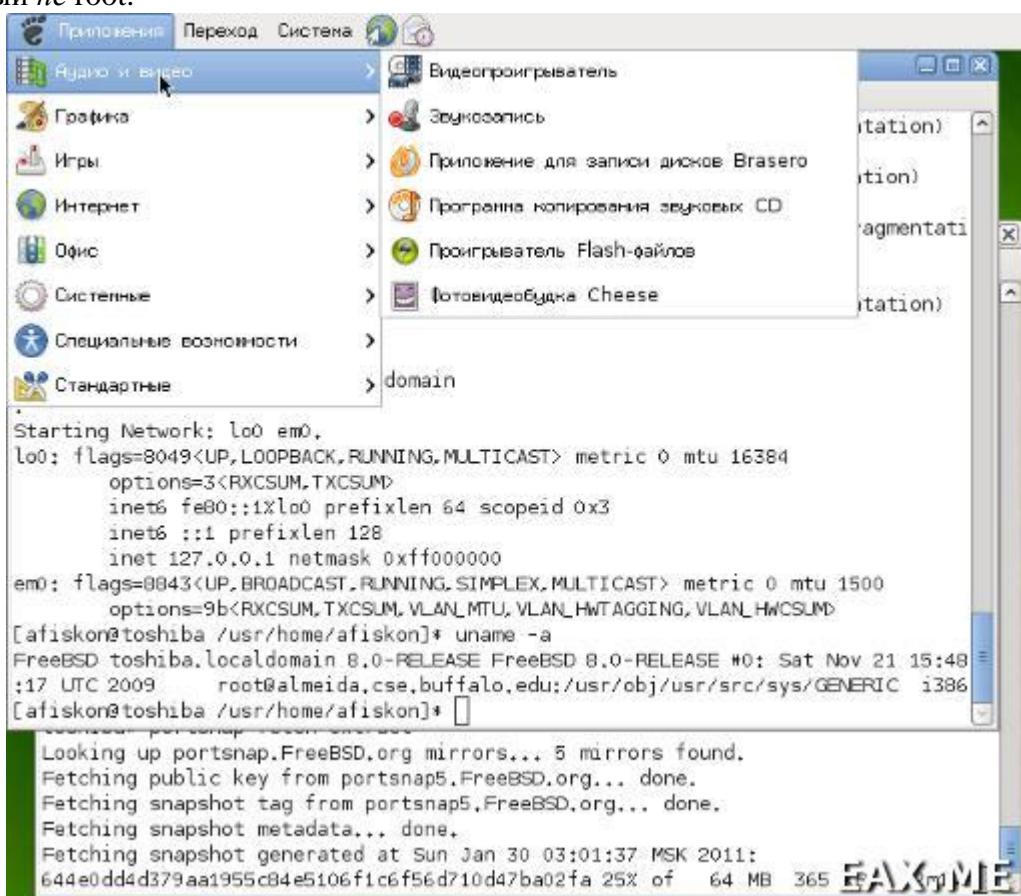
Если вы где-то допустили ошибку, просто выполните команду «rmuser имя_пользователя» и повторите попытку.

Для перезагрузки и выключения системы используйте следующие команды:

```
# перезагрузка - [R]eboot system shutdown -r now
```

```
# завершение работы - halt system and turn [P]ower off shutdown -p now
```

Выполняем перезагрузку. Если все сделано правильно, мы должны увидеть окошко с предложением ввести логин и пароль. Заходим под последним созданным пользователем. Тем, который *не* root.



На самом деле, настройка системы не закончена. Во-первых, клавиатура еще не умеет вводить русские буквы. Исправить это, а также настроить клавиши переключения раскладки, можно в «Система → Параметры → Клавиатура».

Во-вторых, вам наверняка хотелось бы установить еще парочку приложений или сменить шрифты на что-нибудь более симпатичное. Однако эти вопросы я оставлю вам для самостоятельного изучения.

References

- http://interface31.ru/tech_it/2012/05/windows-server-nastraivaem-veb-server-iis.html
- <http://litl-admin.ru/freebsd/ustanovka-freebsd-9-s-nulya.html#ixzz2wvGZUU9R>