МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ПРОФИССЕОНАЛЬНОГО ОБРАЗОВАНИЯ

«РЫБИНСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ ИМ. П. А. СОЛОВЬЕВА»

Факультет заочного отделения

Кафедра вычислительных систем

Контрольная работа

по дисциплине «Администрирование в сетевых ОС»

на тему: «Обзор операционных систем Windows Server и Linux»

Выполнила Ловецкая К. А. .

студент гр. МЗВП-14 , 2 курса

Преподаватель Малышев Р. А. .

Оценка .

Подпись преподавателя .

Дата .

Рыбинск 2015

Содержание

[Введение 3](#_Toc438816915)

[1 Первое знакомство с сетевыми подключениями в Windows Server 4](#_Toc438816916)

[1.1 Типы сетевых подключений 4](#_Toc438816917)

[1.2 Управление сетевыми подключениями 5](#_Toc438816918)

[1.3 Служба DNS. Возможности DNS-сервера в Windows Server. 9](#_Toc438816919)

[1.3.1 Пошаговая настройка DNS-сервера в Windows Server 11](#_Toc438816920)

[1.3.2 Установка DNS-сервера 15](#_Toc438816921)

[1.4 Служба DHCP 17](#_Toc438816922)

[1.4.1 Установка и настройка DHCP-сервера 18](#_Toc438816923)

[1.4.2 Авторизация DHCP-сервера 18](#_Toc438816924)

[1.4.3 Пошаговая настройка DCHP-сервера в Windows Server 21](#_Toc438816925)

[1.5 FTP-сервер в Windows Server 23](#_Toc438816926)

[1.5.1 Установка FTP-сервера 23](#_Toc438816927)

[1.5.2 Пошаговая настройка FTP-сервера 24](#_Toc438816928)

[1.6 Пошаговая установка Windows Server 27](#_Toc438816929)

[1.7 Достоинства и недостатки 28](#_Toc438816930)

[2 Назначение, область применения, архитектура ОС Linux. 30](#_Toc438816931)

[2.1 Архитектура ОС Linux 30](#_Toc438816932)

[2.2 Настройка DHCP в Linux 31](#_Toc438816933)

[2.3 Настройка DNS в linux 31](#_Toc438816934)

[2.4 Пошаговая установка Linux 32](#_Toc438816935)

[2.5 Достоинства и недостатки Linux 42](#_Toc438816936)

[2.5.1 Недостатки 42](#_Toc438816937)

[2.5.2 Преимущества 43](#_Toc438816938)

[Заключение 44](#_Toc438816939)

[Список использованных источников 45](#_Toc438816940)

# Введение

В настоящее время любая операционная система, ориентированная на корпоративный рынок, должна включать в себя компоненты, обеспечивающие возможность ее функционирования в рамках вычислительной сети. Не является исключением и Windows Server. Более того, данная операционная система позиционируется разработчиками, как основа для реализации основных сетевых сервисов в корпоративной вычислительной сети.

Linux – название ядра операционной системы, несмотря на то, что это ядро имеет монолитную архитектуру и не считается прогрессивным, оно поддерживает большинство современных технологий, является многопользовательским и многозадачным. Эта операционная система является третьей по популярности на сегодняшний день. Она установлена на огромном количестве компьютеров и составляет достойную конкуренцию операционным системам разрабатываемым гигантскими корпорациями, несмотря на то, что разрабатывается, в основном, добровольцами-энтузиастами.

# 1 Первое знакомство с сетевыми подключениями в Windows Server

Под сетевым подключением (**network connection**) в Windows Server понимается точка соединения компьютера с сетью (независимо от способа – подключение к локальной сети, серверу удаленного доступа или соединение двух компьютеров посредством нуль-модемного кабеля). Если говорить о том, какая сторона из участников обмена данными инициирует связь, сетевые подключения можно разделить на два вида: исходящие (**outgoing connections**) и входящие (**incoming connections**).

Исходящие подключения используются для соединения компьютера с вычислительной сетью или сервером удаленного доступа. Входящие подключения используются для поддержки подключений, инициализируемых другими компьютерами. В этом случае компьютер, на котором созданы входящие подключения, рассматривается в качестве сервера удаленного доступа (**remote access server**).

Каждое сетевое подключение рассматривается самостоятельно и независимо от других подключений. Это означает, что каждое сетевое подключение имеет индивидуальную конфигурацию. Перечень параметров, подлежащих настройке, зависит от того, к какому типу относится сетевое подключение.

# 1.1 Типы сетевых подключений

Типы сетевых подключений, поддерживаемых Windows Server, перечислены в таблице 1.1.

Таблица 1.1 – Типы сетевых подключений.

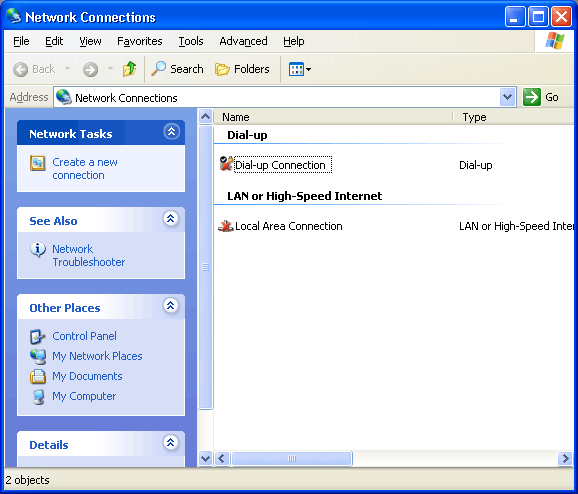
| Тип подключения | Технология связи | Пример |
| --- | --- | --- |
| Подключение к локальной сети (Local area connection) | Ethernet, xDSL, FDDI, IP no ATM, системы беспроводной связи, Е1/Т1 и т. п. | Типичный корпоративный пользователь |
| Телефонное, или коммутируемое, подключение (Dial-up connection) | Модем, ISDN, X.25 | Соединение с корпоративной сетью или Интернетом с использованием модемного подключения |
| Подключение в рамках виртуальной частной сети (Virtual Private Network connection) | Виртуальные частные сети по протоколам РРТР или L2TP, объединяющие или Подключающие к корпоративным сетям через Интернет или другую сеть общего пользования (public network) | Защищенное соединение удаленных филиалов корпорации через Интернет |
| Прямое подключение (Direct Connection) | Соединение нуль-модемным кабелем через последовательный порт (СОМ-порт), инфракрасная связь, параллельный кабель (DirectParallel) | Соединение двух ноутбуков через интерфейсы инфракрасной связи |
| Входящее подключение (Incoming connection) | Коммутируемая связь, VPN или прямое подключение | Подключение к удаленному компьютеру или корпоративному серверу удаленного доступа |

Следует заметить, что из всех перечисленных в таблице типов только подключение к локальной сети создается системой автоматически. В процессе загрузки Windows Server автоматически обнаруживает установленные сетевые адаптеры и для каждого сетевого адаптера создает соответствующее сетевое подключение.

В случае если на компьютере установлено более одного сетевого адаптера, администратор может устранить возможный беспорядок в именах подключений, переименовав каждое локальное подключение в соответствии с функциональным назначением или расположением сети, с которой это соединение связывает компьютер.

# 1.2 Управление сетевыми подключениями

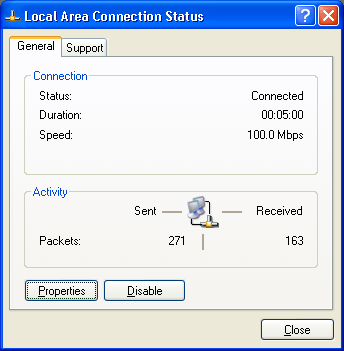
Все операции по конфигурированию сетевых средств осуществляются в папке **Network Connections** (Сетевые подключения) (рисунке 1.1). В этой папке создаются все поддерживаемые операционной системой подключения. Папка располагается на панели управления или может быть выведена непосредственно в меню **Start** (Пуск).

**Рисунок 1.1 –** Окно Network Connections

Вне зависимости от того, является ли связь локальной (ЛВС) или удаленной (телефонная линия, ISDN и т. п.), подключения можно настроить так, чтобы они могли полноценно выполнять все требуемые функции. Например, используя сетевое подключение любого типа, пользователь может распечатывать документы на сетевых принтерах, получать доступ к сетевым дискам и файлам, просматривать другие сети или получать доступ к Интернету (разумеется, если в рамках подключения используются соответствующие протоколы).

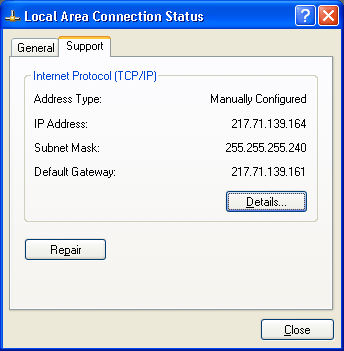
Все службы и методы связи настраиваются непосредственно в окне свойств сетевого подключения. Поэтому для конфигурирования параметров подключения не требуется обращаться к внешним инструментам управления. Например, параметры телефонного подключения при помощи модема включают те, которые нужно использовать до, в течение и после создания подключения: тип модема для связи, используемая при соединении схема аутентификации, а также используемые для передачи данных протоколы.

Для получения информации о состоянии интересующего подключения (продолжительность и эффективность использования) необходимо дважды щелкнуть на соответствующем подключении или в его контекстном меню выбрать пункт **Status** (Состояние). Информация о состоянии подключения приводится на вкладке **General** (Общие) открывшегося окна (рисунок 1.2). Чтобы перейти к настройке выбранного подключения, достаточно щелкнуть на кнопке **Properties** (Свойства).



**Рисунок 1.2 –** Получение информации о состоянии подключения

Для получения дополнительной информации о подключении необходимо перейти на вкладку **Support** (Поддержка) (рисунок 1.3). На этой вкладке приводится информация о настройке стека протоколов TCP/IP для данного подключения: IP-адрес и способ его назначения, а также маска подсети и шлюз по умолчанию. Нажав кнопку **Details** (Подробности), можно также получить информацию о физическом адресе (МАС-адресе), используемом подключением, DNS- и WINS-серверах.



**Рисунок 1.3 –** Получение вспомогательной информации о соединении

Установка дополнительных сетевых компонентов

В процессе развертывания операционной системы администратор может установить базовый набор сетевых компонентов, предоставляющих возможность создания сетевых подключений. В составе Windows Server поставляется значительное число дополнительных сетевых компонентов, расширяющих функциональность операционной системы (таблица 1.2) [4].

Эти компоненты организованы в три группы:

* Management and Monitoring Tools. В этой группе представлены компоненты, ориентированные на решение задач мониторинга сети и управления ею;
* Networking Services. Данная группа объединяет компоненты, осуществляющие установку основных сетевых служб, реализованных в рамках стека протоколов TCP/IP;
* Other Network File and Print Services. Компоненты этой группы позволяют предоставить возможность доступа к файлам и принтерам пользователям, работающим в других средах (Macintosh и UNIX).

Эти компоненты не устанавливаются автоматически непосредственно в ходе развертывания операционной системы. В случае необходимости администратор должен установить нужные сетевые компоненты вручную.

Таблица 1.2 – Сетевые компоненты Windows Server

| Компонент | Группа компонентов | Описание компонента |
| --- | --- | --- |
| Connection Manager Administration Kit | Management and Monitoring Tools | Компонент позволяет установить на сервере мастер Connection Manager Administration Kit Wizard |
| Connection Point Services | Management and Monitoring Tools | Данный компонент используется в процессе развертывания диспетчера соединений (Connection Manager) для публикации телефонных книг (phone book) |
| Network Monitor Tools | Management and Monitoring Tools | Компонент, позволяющий осуществлять анализ сетевого трафика |
| Simple Network Management Protocol | Management and Monitoring Tools | Компонент, обеспечивающий функционирование на сервере протокола SNMP |
| WMI SNMP Provider | Management and Monitoring Tools | Компонент, позволяющий приложениям осуществлять доступ к информации SNMP посредством технологии WMI (Windows Management Information) |
| Domain Name System (DNS) | Networking Services | Компонент устанавливает службу разрешения доменных имен в IP-адреса (DNS) |
| Dynamic Host Configuration Protocol (DHCP) | Networking Services | Компонент устанавливает службу, осуществляющую динамическое выделение IP-адресов (DHCP) |
| Internet Authentication Service | Networking Services | Служба аутентификации через Интернет. Включает в себя поддержку протокола аутентификации удаленных пользователей RADIUS |
| RPC over HTTP Proxy | Networking Services | Компонент, позволяющий осуществлять вызовы RPC/DCOM поверх протокола HTTP, используя службы Internet Information Services (IIS) |
| Simple TCP/IP Services.' | Networking Services | Устанавливаются дополнительные службы TCP/IP |
| Windows Internet Name Service (WINS) | Networking Services | Устанавливает службу разрешения NetBIOS-имен в IP-адреса (WINS) |
| File Services for Macintosh | Other Network File and Print Services | Служба, позволяющая пользователям Macintosh получить доступ к ресурсам на Windows-сервере |
| Print Services for Macintosh | Other Network File and Print Services | Служба, позволяющая пользователям Macintosh отправлять задания на печать на принтеры, подключенные к Windows-серверу |
| Print Services for Unix | Other Network File and Print Services | Служба, позволяющая пользователям UNIX отправлять задания на печать на принтеры, подключенные к Windows-серверу |

Рекомендуется устанавливать только действительно необходимые компоненты. Для обслуживания каждого компонента система затрачивает определенную часть системных ресурсов (память, процессорное время, дисковое пространство) и пропускной способности сети (для передачи служебного трафика сетевых компонентов).

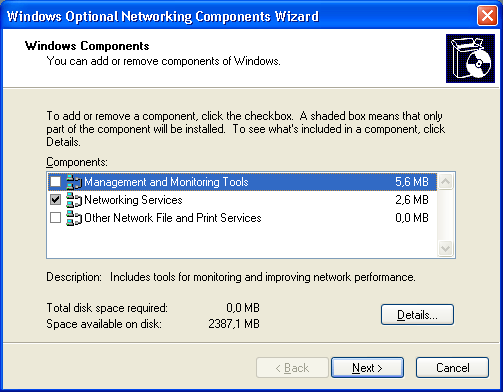


Рисунок 1.4 – Выбор сетевых компонентов для установки

Для установки дополнительных сетевых компонентов в меню Advanced (Дополнительно) окна Network Connections (Сетевые подключения) необходимо выбрать пункт Optional Networking Components (Дополнительные сетевые компоненты). В открывшемся окне (рисунок 1.4) система предлагает выбрать для установки требуемые группы сетевых компонентов. Установка флажка напротив названия группы предписывает установку всех компонентов данной группы. Для установки только отдельных компонентов некоторой группы необходимо выбрать группу и щелкнуть на кнопке Details (Подробности). При этом система предложит список компонентов, входящих в состав выбранной группы [4].

# 1.3 Служба DNS. Возможности DNS-сервера в Windows Server.

Служба доменных имен, **Domain Name System**, DNS, является одним из важнейших компонентов сетевой инфраструктуры Windows Server. Служба доменных имен осуществляет разрешение, или преобразование, символьных имен в IP-адреса. Клиенты доменов на базе Active Directory используют службу DNS для обнаружения контроллеров домена.

Доменная структура каталога отображается на пространство имен DNS. Поэтому процесс проектирования доменной структуры каталога должен происходить одновременно с формированием пространства имен DNS. Ошибки, допущенные при проектировании пространства имен DNS, могут стать причиной недостаточной производительности сети и, возможно, даже привести к ее отказу.

Возможности DNS-сервера в Windows Server

Служба DNS в Windows Server обладает общими функциональными возможностями, перечисленными ниже.

* **DNS-сервер, полностью соответствующий стандартам RFC**. Служба DNS базируется на открытых протоколах и полностью соответствует промышленным стандартам (RFC).
* **Способность взаимодействия с другими реализациями DNS-серверов**. Поскольку служба DNS построена на основе существующих стандартов, она успешно взаимодействует совместно с большинством других реализаций DNS, например, использующих программное обеспечение **Berkeley Internet Name Domain** (BIND).
* **Поддержка Active Directory**. Как уже упоминаюсь ранее, служба DNS является обязательным условием развертывания Active Directory. Служба DNS используется как основной механизм обнаружения ресурсов в Active Directory-доменах. В свою очередь, DNS-серверы могут использовать каталог Active Directory для размещения баз данных зон. При этом процесс репликации зон осуществляется непосредственно средствами Active Directory.
* **Интеграция с другими сетевыми службами Microsoft**. Служба DNS обеспечивает интеграцию с другими службами Windows и содержит функции, не описанные в RFC. Это касается интеграции со службами WINS и DHCP.
* **Улучшенные административные инструменты**. Для управления DNS-серверами администратор может использовать специальную оснастку с улучшенным графическим интерфейсом. Кроме того, в составе операционной системы имеется целый ряд мастеров конфигурации, позволяющих выполнять повседневные задачи по администрированию сервера. Также имеется ряд дополнительных утилит, помогающих управлять и поддерживать серверы DNS и клиентов в сети.
* **Поддержка протокола динамического обновления в соответствии с RFC**. Служба DNS позволяет клиентам динамически обновлять ресурсные записи при помощи динамического протокола обновления DNS (стандарт RFC 2136). Это облегчает администрирование DNS, избавляя от необходимости вносить эти записи вручную. Компьютеры под управлением Windows 2000, Windows XP и Windows Server могут динамически регистрировать свои доменные имена.
* **Поддержка инкрементных передач зоны между серверами**. Передача зоны осуществляется между DNS-серверами в качестве средства синхронизации отдельных экземпляров базы данных зоны. Стандартная процедура передачи зоны предполагает копирование всей базы данных зоны с одного сервера на другой. Инкрементная передача зоны позволяет копировать только сведения об изменениях.
* **Поддержка новых типов ресурсных записей**. Служба DNS обеспечивает поддержку нескольких новых типов ресурсных записей (RR): записи SRV (расположение службы) и АТМА (адрес ATM), что значительно расширяет возможности использования DNS в глобальных сетях.
* Кроме того, реализация службы DNS в Windows Server имеет несколько новых функциональных возможностей, отличающих ее от реализации в предыдущих версиях Windows (в частности Windows 2000).
* **Выборочное перенаправление запросов** (Conditional forwarding). Данный механизм позволяет осуществлять перенаправление запросов клиентов на различные DNS-серверы, основываясь на информации о доменном имени, содержащемся в запросе. Механизм выборочного перенаправления может быть использован как средство организации взаимодействия двух лесов доменов, реализующих собственные пространства имен DNS.
* **Упрощенные зоны** (Stub Zones). Упрощенная зона представляет собой фрагмент зоны, содержащий только те ресурсные записи, что необходимы для нахождения DNS-серверов, являющихся носителями полной версии зоны. Основное назначение упрощенной зоны – идентификация DNS-серверов, которые способны выполнить разрешение доменных имен, принадлежащих к этой зоне.
* **Новые способы хранения базы данных зоны в каталоге Active Directory**. В случае, когда DNS-сервер установлен на контроллере домена, для размещения содержимого зоны могут использоваться специальные разделы приложений (**application partitions**). При этом указанные разделы приложений могут размещаться только на тех контроллерах домена, которые являются DNS-серверами.
* **Улучшенные механизмы обеспечения безопасности службы DNS**. Система доменных имен (DNS) разрабатывалась как открытый протокол, что делает ее достаточно чувствительной к разнообразным атакам. В связи с этим в Windows Server разработчиками в реализацию службы DNS был добавлен целый ряд функциональных возможностей, направленных на защиту этой службы от различных атак (в том числе и от атак типа "отказ в обслуживании" – Denial of Services, DoS).
* **Расширенные возможности протоколирования событий, связанных с функционированием DNS-сервера**. В Windows Server администратор может получить в свое распоряжение более подробную аналитическую информацию о функционировании DNS-сервера. Эти сведения позволят ему, с одной стороны, получить информацию о режиме работы сервера, а с другой стороны, выявить причины неполадок в случае их возникновения.
* **Поддержка протокола DNSSEC (DNS Security Extensions)**. Протокол DNSSEC определен в стандарте RFC 2535. Реализованная в Windows Server поддержка этого протокола позволяет DNS-серверам выступать в качестве дополнительных носителей DNSSEC-совместимых защищенных зон. Поддерживаются ресурсные записи типа KEY, SIG и NXT.
* **Поддержка механизма EDNSO (Extension Mechanisms for DNS)**. Механизм EDNSO позволяет использовать UDP-пакеты размером больше 512 октетов.
* **Управление процессом автоматической регистрации серверов имен в базе данных зоны**. В Windows Server администратор может запретить автоматическую регистрацию серверов имен (что фактически равносильно запрещению автоматического создания ресурсных записей NS-типа) в базе данных зоны.
* **Новые групповые политики** для управления настройками DNS на клиентских компьютерах и контроллерах домена.

# 1.3.1 Пошаговая настройка DNS-сервера в Windows Server

1. Выберите объект DNS из папки Администрирование (Administrative Tools), чтобы открыть консоль управления DNS-сервером [9].
2. Выделите имя вашего компьютера и нажмите Действие (Action) | Конфигурация DNS-сервера (Configure a DNS Server), чтобы запустить Мастера настройки DNS-сервера.
3. Нажмите Далее (Next) и выберите объект настройки: зона прямого просмотра (forward lookup zone), зоны прямого и обратного просмотра (forward and reverse lookup zone ), только корневые ссылки (root hints only) (рисунок 1.5).
4. Нажмите Далее (Next) и потом Да (Yes) для того, чтобы создать зону прямого просмотра (рисунок 1.6).
5. Отметьте желаемый тип зоны (рисунок 1.7).
6. Нажмите Далее (Next) и введите имя создаваемой зоны.
7. Нажмите Далее (Next) и потом Да (Yes) для того, чтобы создать зону обратного просмотра.
8. Повторите шаг 5.
9. Выберите протокол зоны обратного просмотра: IPv4 или IPv6 (рисунок 1.8).
10. Нажмите Далее (Next) и ведите идентификатор зоны обратного просмотра (рисунок 1.9).
11. Можно создать новый или использовать копию уже существующего файла DNS (рисуков 1.10).
12. В окне Динамические обновления (Dynamic Update), выберите способ обновления DNS: безопасный (secure), небезопасный (nonsecure), неполучать динамических обновлений (no dynamic updates).
13. При желании можно включить перенаправляющий DNS-сервер в окне Перенаправление (Forwarders) (рисунок 1.11).
14. Нажмите Готово (Finish) (рисунок 1.12).

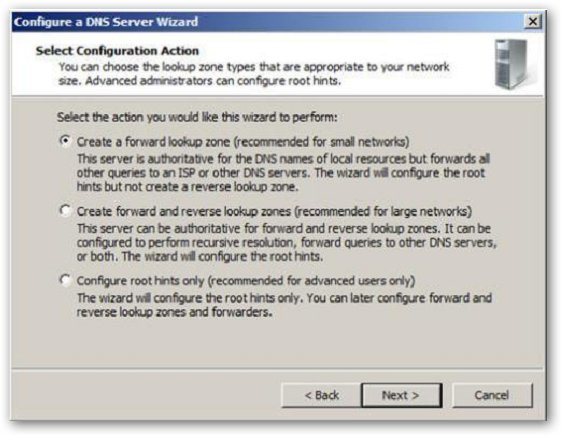
[](http://system-administrators.info/wp-content/uploads/2008/05/dns5.jpg)

Рисунок 1.5 – Настройка DNS-сервера

[](http://system-administrators.info/wp-content/uploads/2008/05/dns6.jpg)

Рисунок 1.6 – Зона прямого просмотра

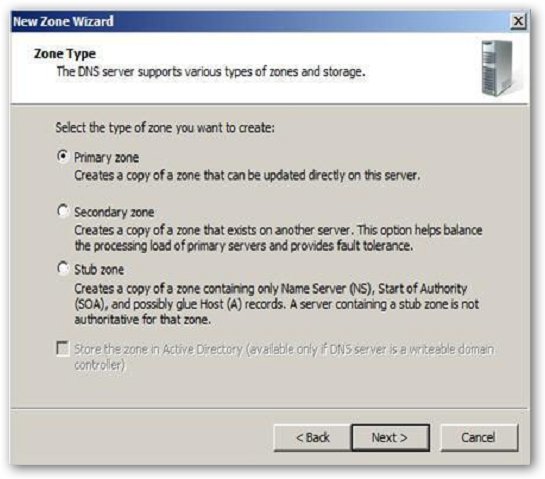
[](http://system-administrators.info/wp-content/uploads/2008/05/dns7.jpg)

Рисунок 1.7 – Желаемая зона

[](http://system-administrators.info/wp-content/uploads/2008/05/dns81.jpg)

Рисунок 1.8 – IPv4 или IPv6

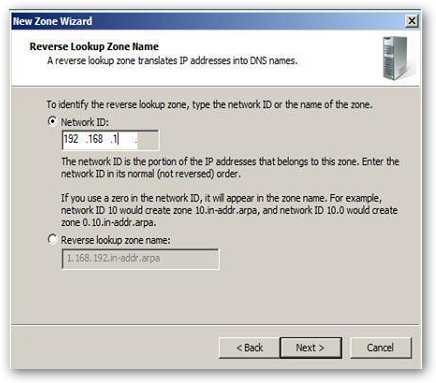
[](http://system-administrators.info/wp-content/uploads/2008/05/dns9.jpg)

Рисунок 1.9 – Зона обратного просмотра

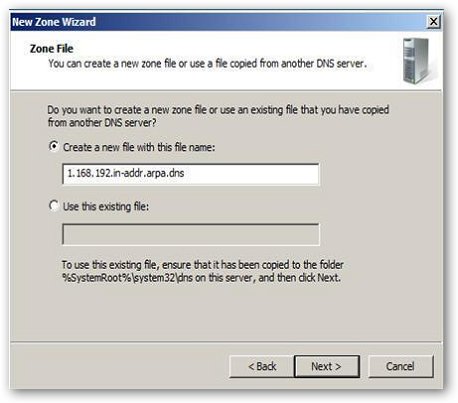
[](http://system-administrators.info/wp-content/uploads/2008/05/dns10.jpg)

Рисунок 1.10 – Новый или существующий файл DNS

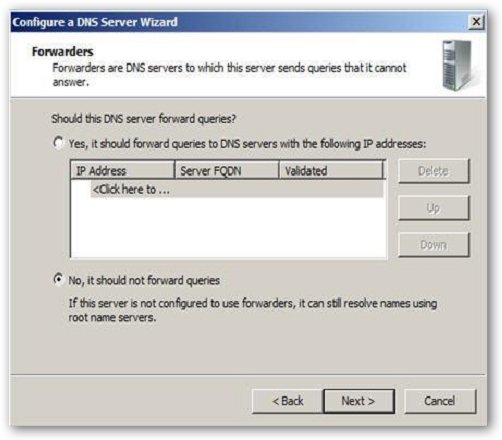
[](http://system-administrators.info/wp-content/uploads/2008/05/dns11.jpg)

Рисунок 1.11 – Окно «Перенаправление»

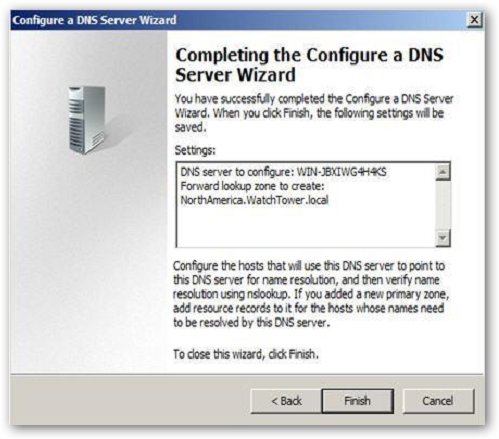
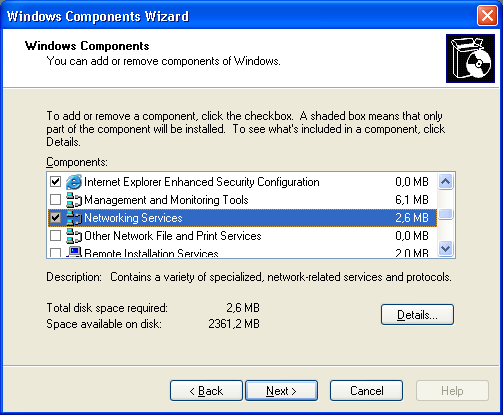
[](http://system-administrators.info/wp-content/uploads/2008/05/dns12.jpg)

Рисунок 1.12 – Завершение

# 1.3.2 Установка DNS-сервера

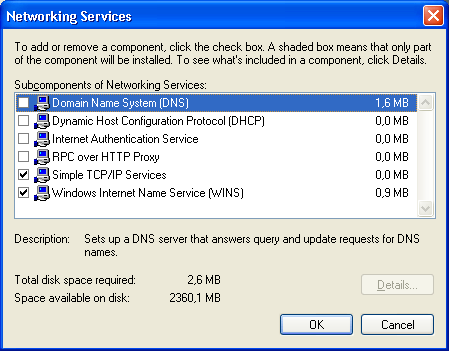
Можно воспользоваться мастером установки компонентов Windows. Для этого необходимо открыть панель управления, запустить утилиту **Add/Remove Programs** (Добавить/удалить приложения) и нажать кнопку **Add/Remove Windows Component** (Добавить/удалить компоненты Windows). В окне мастера (рисунок 1.13) следует выбрать компоненты Windows для установки. Администратор может одновременно установить множество компонентов, для этого достаточно установить соответствующие флажки [4].



**Рисунок 1.13 –** Выбор компонентов Windows для установки

Выберите в списке пункт **Networking Services** (Сетевые службы) и нажмите кнопку **Details** (Подробнее). В открывшемся окне (рисунок 1.14) установите флажок около компонента **Domain Name System** (DNS). Вернитесь в окно выбора устанавливаемых компонентов и щелкните на кнопке **Next** (Далее), чтобы приступить к установке. В процессе установки потребуется доступ к дистрибутивным файлам Windows Server.

По окончании работы мастера служба DNS будет установлена на выбранный компьютер. Требуемые файлы будут скопированы на жесткий диск, программное обеспечение сервера можно использовать после перезапуска системы. В группе программ **Administrative Tools** (Средства администрирования) появится новый инструмент: оснастка DNS. Однако мастер производит установку на сервер только системных файлов. Чтобы служба DNS-сервера начала выполнять свои функции, необходимо должным образом ее сконфигурировать.



**Рисунок 1.14 –** Выбор сетевых компонентов для установки

Установив сервер DNS, необходимо решить, как будут управляться сервер и файлы зон базы данных DNS. Хотя изменения в файлах базы данных можно вносить и при помощи текстового редактора, этот метод не рекомендуется. Лучше обслуживать сервер DNS и файлы зон базы данных средствами оснастки DNS.

# 1.4 Служба DHCP

Каждому хосту, подключенному к сети на базе TCP/IP, должен быть назначен уникальный IP-адрес. Протокол DHCP (Dynamic Host Configuration Protocol, протокол динамической конфигурации хоста) был разработан как средство динамического выделения хостам IP-адресов. Протокол DHCP является открытым промышленным стандартом, упрощающим управление сетями на базе TCP/IP. Этот протокол может быть использован для централизованного управления процессом настройки стека протокола TCP/IP на клиентских машинах (речь идет о таких параметрах, как адрес шлюза по умолчанию или адрес DNS-сервера).

В спецификации протокола DHCP определяются два участника: DHCP-сервер и DHCP-клиенты. Служба клиента DHCP запрашивает у DHCP-сервера параметры для настройки стека протоколов TCP/IP. Служба сервера DHCP обрабатывает клиентские запросы, осуществляя выдачу в аренду IP-адреса из некоторого диапазона. Каждый адрес выделяется на определенный срок. По окончании этого срока хост должен либо продлить срок аренды, либо освободить адрес. Все удовлетворенные запросы пользователя фиксируются службой сервера DHCP в собственной базе данных. Подобное решение позволяет предотвратить выделение одного IP-адреса двум хостам. Одновременно с выдачей IP-адреса DHCP-сервер может также предоставить клиенту дополнительную информацию о настройках стека протоколов TCP/IP, такую как маска подсети, адрес шлюза и адреса серверов DNS и WINS [2].

Кажется совершенно очевидным, что поддержка этого протокола была реализована в операционной системе Windows Server. В составе Windows Server реализован как DHCP-клиент (который устанавливается по умолчанию), так и DHCP-сервер (который может быть установлен и сконфигурирован администратором при необходимости). Реализованная в Windows Server поддержка протокола DHCP обладает характеристиками, перечисленными ниже.

* Интеграция с DNS. DNS-серверы обеспечивают разрешение имен для сетевых ресурсов и тесно связаны со службой DHCP. DHCP-серверы и DHCP-клиенты могут осуществлять динамическую регистрацию выдаваемых IP-адресов и ассоциированных с ними доменных имен в базе данных DNS-сервера. При этом в базе данных DNS-сервера создаются ресурсные записи типа PTR (указатель) и А (адрес).
* Улучшенное управление и мониторинг. Новая возможность обеспечивает уведомление об уровне использования пула IP-адресов. Оповещение производится при помощи соответствующего значка либо при помощи передачи сообщения. Сервер DHCP поддерживает SNMP и MIB, что обеспечивает графическое представление статистических данных. Это помогает администратору отслеживать состояние сети, например, число доступных и занятых адресов, число арендных договоров, обрабатываемых за секунду, и т. п..
* Распределение групповых адресов. DHCP-сервер может быть использован для выделения клиентам групповых (multicast) адресов. В последнее время появляется большое количество корпоративных приложений, требующих использования групповых адресов (например, видео – или аудио-конференции).
* Защита от подмены серверов. Одним из обязательных условий функционирования DHCP-сервера является требование его авторизации в каталоге Active Directory. При каждом запуске служба DHCP-сервера пытается обнаружить в каталоге запись, подтверждающую авторизацию службы. Если подобная запись не найдена, служба сервера не запускается.
* Автоматическая настройка клиентов. Служба DHCP-клиента в случае отсутствия в сети DHCP-сервера может выполнить необходимую настройку самостоятельно. Используя для работы временную конфигурацию стека протоколов TCP/IP, клиент продолжает попытки связаться с DHCP-сервером в фоновом режиме каждые 5 минут. При этом автоматическое назначение адреса всегда прозрачно для пользователей. Адреса для такого рода клиентов выбираются из диапазона частных сетевых адресов TCP/IP, которые не используются в Интернете.
* Новые специализированные опции и поддержка классов опций. Администратор может создавать собственные классы DHCP (используемые для конфигурации клиентов) в соответствии с необходимостью. Механизм пользовательских классов позволяет применять DHCP в заказных приложениях для сетей масштаба предприятия. Классы поставщиков (vendor classes) могут использоваться для настройки различных функций сетевого аппаратного обеспечения.

Следует также отметить функциональные возможности, которые были впервые добавлены в реализацию службы DHCP в Windows Server.

* Возможность резервного копирования базы данных DHCP. В базе данных DHCP-сервера хранится информация о выданных клиентам IP-адресах, включая информацию о времени окончания аренды. Регистрация этой информации позволяет избежать повторного выделения уже выданных адресов. Повреждение этой базы данных может привести к тому, что работоспособность сети окажется под угрозой. Администратор может выполнять резервное копирование базы данных DHCP-сервера. Созданная резервная копия может использоваться впоследствии для восстановления работоспособности DHCP-сервера.
* Возможность задания альтернативной конфигурации DHCP-клиента. Для DHCP-клиента может быть задана альтернативная конфигурация TCP/IP, что позволяет перемещать компьютер между различными подсетями.

# 1.4.1 Установка и настройка DHCP-сервера

После установки сервера в меню **Administrative Tools** (Администрирование) будет добавлен новый инструмент: **оснастка DHCP**.

Эта утилита используется для настройки DHCP-сервера. Непосредственно после установки службы DHCP-сервера необходимо запустить ее при помощи оснастки **Services** (Службы). В случае если DHCP-сервер подключен к нескольким сетям, необходимо отключить привязку службы к тем подключениям, которым не требуется поддержка DHCP.

Компьютер, выбранный на роль DHCP-сервера, должен быть сконфигурирован со статическим IP-адресом.

# 1.4.2 Авторизация DHCP-сервера

Прежде чем DHCP-сервер сможет приступить к процессу выделения адресов DHCP-клиентам, он предварительно должен быть авторизован. Авторизация DHCP-сервера является обязательным условием его нормального функционирования. Иными словами, в каталоге Active Directory должен быть создан объект, соответствующий установленному DHCP-серверу. Только после этого клиенты смогут работать с данным сервером. Все обязанности по осуществлению контроля над авторизацией DHCP-серверов возложены непосредственно на сами DHCP-серверы. Осуществляется это следующим образом. Служба DHCP-сервера при запуске обращается к Active Directory, чтобы просмотреть список IP-адресов авторизованных серверов. Если она не обнаруживает свой адрес в этом списке, она останавливает свою работу [2].

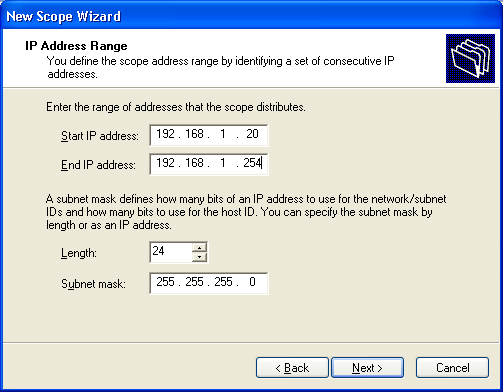
Для авторизации DHCP-сервера необходимо запустить оснастку DHCP и в контекстном меню объекта, расположенного в корне пространства имен утилиты, выбрать пункт **Manage authorized servers** (Управление авторизованными серверами). Система покажет список уже авторизованных DHCP-серверов. Нажав кнопку **Authorize** (Авторизовать) и указав имя авторизуемого DHCP-сервера или его IP-адрес, выбранный сервер будет немедленно добавлен в список авторизованных серверов.

Создание области действия

Для настройки службы DHCP сначала следует определить необходимые области действия. Запустите оснастку **DHCP**, которая находится в меню **Administrative Tools** (Администрирование). В результирующей панели оснастки вызовите контекстное меню объекта, ассоциированного с конфигурируемым DHCP-сервером, и выберите пункт **New Scope** (Новая область действия). Будет запущен мастер конфигурирования области действия.

Первое окно мастера традиционно предоставляет информацию о его назначении. Поэтому необходимо сразу же перейти во второе окно, в котором требуется определить имя для создаваемой области действия и дать ей краткое описание. В качестве имени можно использовать IP-адрес подсети. Это поможет легко ориентироваться в ситуации, когда на DHCP-сервере создано множество областей действия. В этом случае всегда можно точно идентифицировать необходимую область.

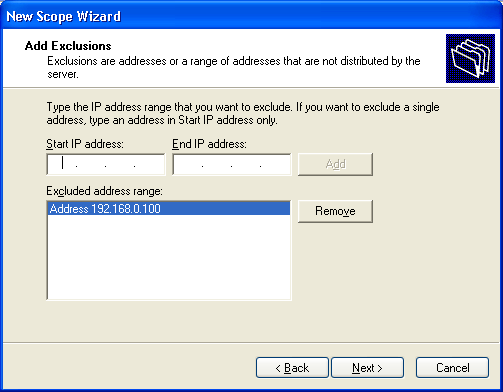
В третьем окне мастера следует определить пул IP-адресов, для которых создается область действия. Пул задается путем указания начального и конечного адреса диапазона. Потребуется также предоставить информацию о маске подсети (рисунок 1.15).



**Рисунок 1.15 –** Предоставьте информацию о диапазоне адресов

В следующем окне мастера администратор может определить исключения из только что определенного диапазона. Могут иметься различные причины для этого. Администратор может исключать как отдельные адреса, так и целые диапазоны. Для исключения одиночного IP-адреса необходимо указать его в поле **Start IP address** (Начальный IP-адрес). Поле **End IP address** (Конечный IP адрес) необходимо оставить в этом случае пустым. После нажатия кнопки **Add** (Добавить) введенный адрес будет добавлен в список исключенных из диапазона адресов (рисунок 1.16).

Перейдя к следующему окну мастера, необходимо определить для создаваемой области действия время аренды IP-адресов. Время аренды может быть определено на уровне дней, часов и даже минут. Хотя в стандарте протокола DHCP определена возможность аренды адреса на неопределенный срок (бесконечная аренда), реализация службы протокола в Windows Server не допускает сдачу адреса в бесконечную аренду.



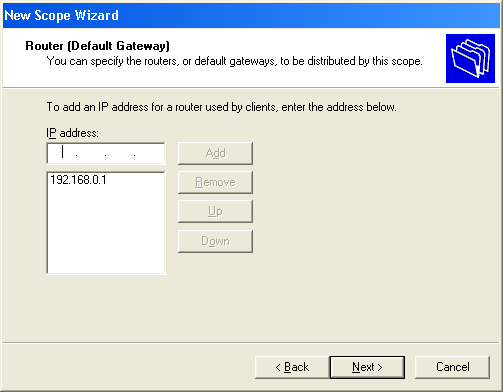
**Рисунок 1.16 –** Определение исключений из диапазона адресов

Определив время аренды, администратор фактически заканчивает конфигурирование области действия. В ходе работы мастера, однако, администратор может сразу определить опции **DHCP** для создаваемой области действия: будет задан вопрос – требуется ли определить опции непосредственно в ходе работы мастера или это будет сделано администратором впоследствии.

Если воспользоваться помощью мастера в определении опций, будет предложено определить несколько наиболее важных опций DHCP.

1. **Адрес шлюза по умолчанию**.

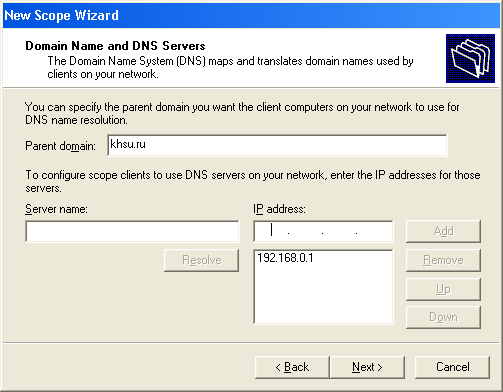
Шлюз по умолчанию используется для маршрутизации пакетов, адресованных хостам в других подсетях. Если хост не располагает информацией о шлюзе по умолчанию, он не будет способен взаимодействовать с подобными хостами. В данной опции требуется определить адрес маршрутизатора, который будет осуществлять доставку пакетов хостам в других подсетях (рисунок 1.17).



**Рисунок 1.17 –** Опция, позволяющая определить адреса шлюзов по умолчанию

1. **DNS-имя домена и адреса DNS-серверов**.

Эти опции используются для определения DNS-имени домена и DNS-серверов всех хостов, конфигурируемых посредством данной области действия. DNS-сервер может быть представлен как именем, так IP-адресом. Опция допускает указание нескольких DNS-серверов, что позволит обеспечить гарантированное разрешение имен в случае, если один из серверов выйдет из строя (рисунок 1.18).

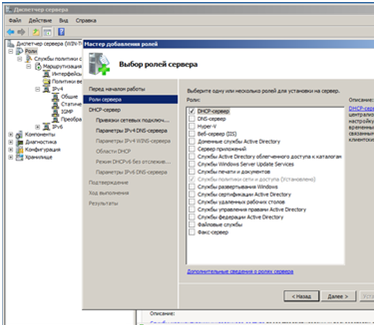


**Рисунок 1.18 –** Опция, позволяющая определить адреса DNS-серверов и

DNS-имени домена

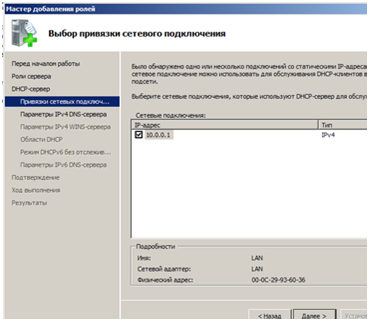
# 1.4.3 Пошаговая настройка DCHP-сервера в Windows Server

Для автоматической настройки сетевых параметров на клиентских машинах, ну не бегать же от места к месту вручную прописывая IP адреса, следует добавить роль DHCP сервера [10].



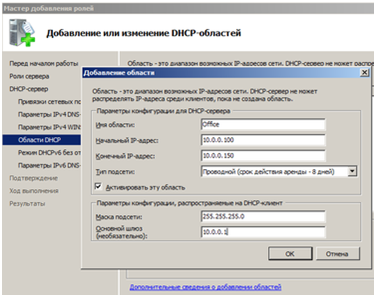
**Рисунок 1.19 –** Добавление ролей

Для этого выбираем **Добавить роль в Диспетчере сервера** и отмечаем необходимую нам опцию.



**Рисунок 1.20 –** Добавление ролей

Теперь нам предстоит ответить на ряд несложных вопросов. В частности выбрать для каких внутренних сетей следует использовать DHCP, при необходимости можно настроить различные параметры для разных сетей. Потом последовательно указать параметры DNS и WINS серверов. Последний, при его отсутствии, можно не указывать. Если в вашей сети отсутствуют старые рабочие станции под управлением ОС отличных от Windows NT 5 и выше (2000 / XP / Vista / Seven), то необходимости в WINS сервере нет.

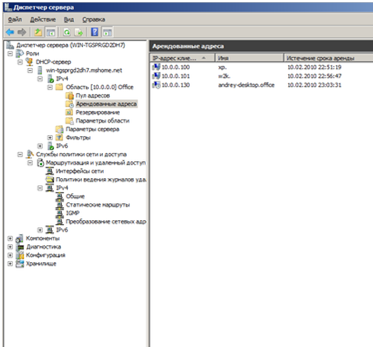


**Рисунок 1.21 –** Настройка параметров

К добавлению DHCP-области нужно отнестись с повышенной внимательностью, ошибка здесь может привести к неработоспособности всей сети. Ничего сложного здесь нет, просто внимательно вводим все необходимые параметры сети, следя, чтобы выделяемый диапазон IP не перекрывал уже выделенный для других устройств и не забываем правильно указывать маску и шлюз.

Отдельно следует обратить внимание на такой параметр как срок аренды адреса. По истечении половины срока аренды клиент посылает серверу запрос на продление аренды. Если сервер недоступен, то запрос будет повторен через половину оставшегося срока. В проводных сетях, где компьютеры не перемещаются в пределах сети, можно выставлять достаточно большой срок аренды, при наличии большого количества мобильных пользователей (например публичная Wi-Fi точка в кафе) срок аренды можно ограничить несколькими часами, иначе не будет происходить своевременное освобождение арендованных адресов и в пуле может не оказаться свободных адресов.

Следующим шагом отказываемся от поддержки IPv6 и после установки роли DHCP сервер готов к работе без каких либо дополнительных настроек. Можно проверять работу клиентских машин.



**Рисунок 1.22 –** Завершение настройки

Выданные IP адреса можно посмотреть в **Арендованных адресах**, относящихся к интересующей нас области. Здесь же можно настроить резервирование за определенным клиентом конкретного адреса (привязав по имени или MAC-адресу), при необходимости можно добавить или изменить параметры области. **Фильтры** позволяют создать разрешающие или запрещающие правила основываясь на MAC-адресах клиентов. Более полное рассмотрение всех возможностей DHCP-сервера Windows Server 2008 R2 выходит за рамки данной статьи и скорее всего мы посвятим им отдельный материал.

# 1.5 FTP-сервер в Windows Server

# 1.5.1 Установка FTP-сервера

FTP (от англ. File Transfer Protocol – протокол передачи файлов) – протокол, используемый для передачи файлов в ТСР-сетях. На сегодня, используется преимущественно для загрузки информации с клиентского устройства на хостинг-серверы. Рассмотрим FTP сервер Windows 7.

Протокол был создан в 1971, еще за долго до появления стека TCP/IP, который увидел свет лишь в конце 70-х годов. Изначально, в своей первой редакции, протокол использовал один и тот же канал для передачи команд и передачи данных. Но уже в 1972 протокол стал очень похожим, на тот, с которым мы имеем дело сегодня – для обмена между сервером и клиентом создается отдельный канал управления, который работает на 21 порту, передача данных осуществляется по каналу данных, для которого создается отдельное соединение. Последняя версия протокола была представлена в 1985 году.

Существенным недостатком FTP являются многочисленные уязвимости в защите, список которых был составлен и опубликован в 1999 году: проблема захвата портов, защиты имени пользователя, низкая стойкость к брутфорс-, спуф-, сниф-, скрытым атакам. Передача данных с использованием FTP осуществляется открытым текстом, без шифрования трафика, таким образом доступ к логинам, паролям, командам управления и пр. могут получить третьи лица, которые способны перехватить пакет по сети. Данная проблема характерна для всех ранних версий протоколов (например, почтовых SMTP, POP, IMAP), разработанных до появления механизмов шифрования SSL, TLS. Для решения этой проблемы рекомендуем использовать протокол передачи файлов с TLS-защитой – FTPS, при таком подходе шифруются два канала – канал управления и канал передачи данных.

В рамках этой статьи мы рассмотрим создание FTP-сервера на базе ОС Windows 7.

Шаг 1. Установка FTP-компонента

* + - 1. Пуск.
      2. В поле поиска вводим «Программы и компоненты», без кавычек.
      3. Выбираем соответствующий пункт меню.
      4. В появившемся окне, в левой колонке переходим в меню «Включение или отключение компонент Windows».
      5. Выбираем компоненты Windows, которые следует установить – FTP-сервер и Консоль управления IIS.
      6. Нажимаем ОК.

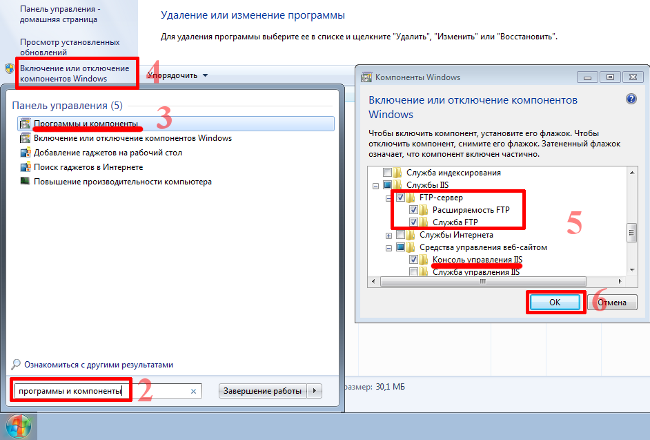
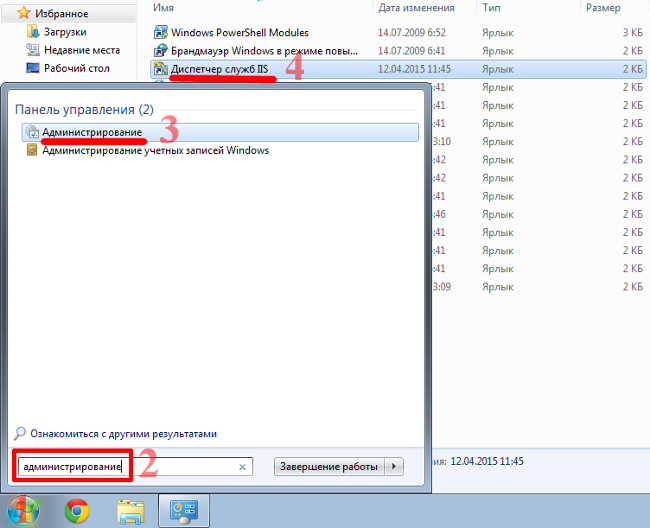
[](http://geek-nose.com/wp-content/uploads/2015/04/ftp-server-windows-7-01.png)

Рисунок 1.23 – Включение и отключение компонентов

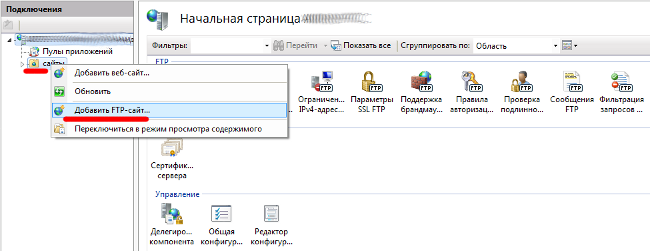
# 1.5.2 Пошаговая настройка FTP-сервера

1. Пуск.
2. В поле поиска вводим «Администрирование», без кавычек.
3. Выбираем соответствующий пункт меню.
4. В появившемся окне переходим в меню «Диспетчер служб IIS».

[](http://geek-nose.com/wp-content/uploads/2015/04/ftp-server-windows-7-02.png)

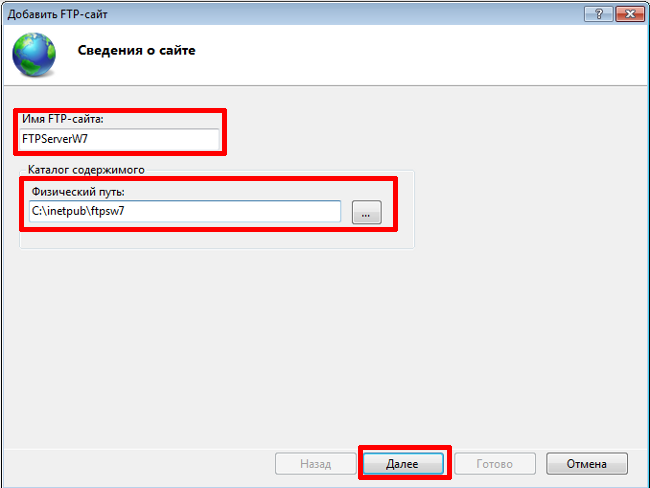
**Рисунок 1.24 –** Настройка FTP-сервера

1. Переходим на вкладку «сайты», нажимаем правой кнопкой мыши и выбираем «Добавить FTP-сайт» [11].

[](http://geek-nose.com/wp-content/uploads/2015/04/ftp-server-windows-7-03.png)

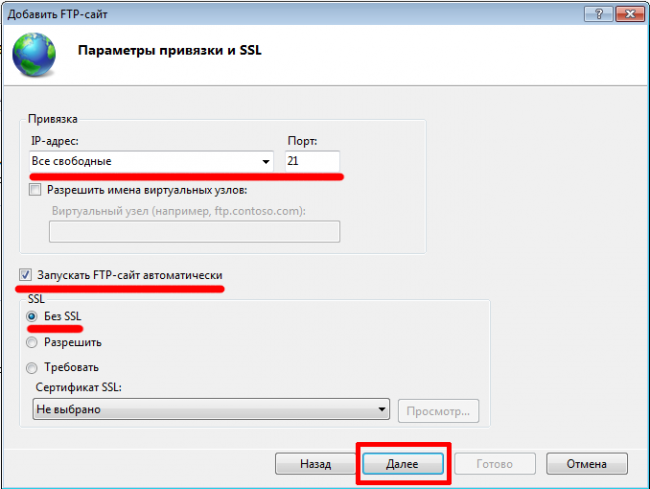
**Рисунок 1.25 –** Настройка FTP-сервера

1. Прописываем имя FTP-сервера и путь к папке, в которой будет хранится информация, переходим к следующему пункту настройки — «Далее». В качестве примера был создан подкаталог ftpsw7.

[](http://geek-nose.com/wp-content/uploads/2015/04/ftp-server-windows-7-04.png)

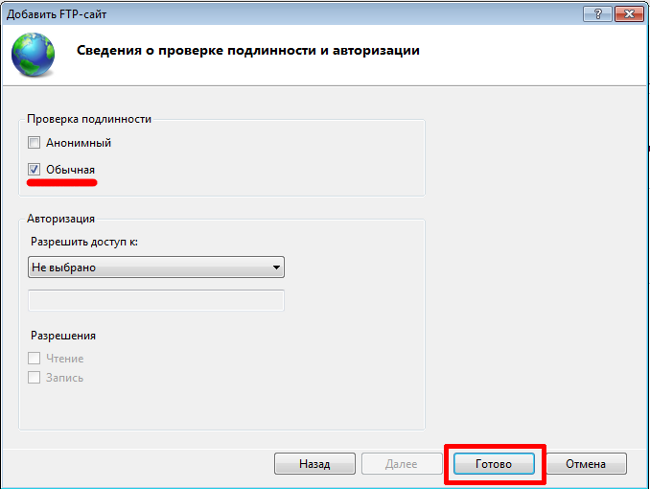
**Рисунок 1.26 –** Настройка FTP-сервера

1. В поле выбора IP-адреса выбираем нужный IP-адрес из списка. Если нужно расшарить папку для всех доступных подсетей выбираем пункт «Все свободные». Стандартный порт (21) оставляем без изменений. Если планируется использование FTP-сервера на постоянной основе – ставим галочку «Запускать FTP-сайт автоматически». Выбираем «Без SSL».

[](http://geek-nose.com/wp-content/uploads/2015/04/ftp-server-windows-7-05.png)

**Рисунок 1.27 –** Настройка FTP-сервера

1. Выбираем обычную проверку подлинности, поле авторизации оставляем без изменений. На этом настройка FTP-сервера завершена.

[](http://geek-nose.com/wp-content/uploads/2015/04/ftp-server-windows-7-06.png)

**Рисунок 1.28 –** Завершение настройки FTP-сервера

После настройки в меню «сайты» появится только что созданный FTP-сервер.

# 1.6 Пошаговая установка Windows Server

1. Выбор компьютера является для сервера самым главным решением поскольку Windows в отличии от Linux очень плотно привязывается к аппаратным средствам. Именно поэтому отнеситесь к подбору аппаратных средств вашего сервера [8].
2. Окно выбора привода для загрузки. Начинаем установку. Прежде всего нужно в BIOSe поставить загрузку с компакт диска. После этого перезагрузить ПК.
3. Во время перезагрузки компьютера надо вставить CD, после появится окно загрузки и выбрать установка Windows Server.
4. После этого появиться установки системы (экран синего цвета) с надписью Установка Windows Server и система начнет проверять файлы на установочном диске. Затем нажимаем Enter
5. После этого появиться окно разбиения диска в котором отобразятся все имеющиеся логические диски на всех винчестерах. Нам необходимо создать разделы. Главное создать системные разделы. именно поэтому можно разбить диск следующим образом:1 раздел 10237 МБ (или примерно 10 Гб), 2 раздел 36868 МБ (или примерно 35 Гб), 3 раздел 31416 Мб (или примерно 30 Гб). После этого нажать Enter на первый раздел, и выбрать пункт форматировать в NTFS. После этого программа установки начнет копировать пакеты на жесткий диск. Этот процесс может занять до 10 минут. После копирования компьютер сам перезагрузится.
6. После перезагрузки установка продолжится уже в графическом режиме. Установка в графическом режиме займет примерно 30-35 минут.
7. Первое, что потребует система во время установки это сверить часы и выставить страну и часовой пояс где мы находимся.
8. После этого система попросит ввести имя и организацию.
9. Затем появится окно лицензирования, где надо будет ввести пароль и указать метод лицензирования, здесь ни чего не выбираем, Windows по умолчанию выставляет те данные, которые необходимы.
10. И в заключений у вас появится окошко где Windows попросит ввести имя сервера и пароль администратора, обязательно необходимо ввести пароль администратора.
11. Дальше появится окошко выбора сетевых параметров. выбираем обычные параметры, их мы перенастроим позже, следующее окно попросит ввести имя рабочей группы.
12. Все после этого Windows сам окончит установку. После установки необходимо установить все драйвера. Что бы узнать какие драйвера нам надо установить, нужно зайти в диспетчер устройств. Что бы туда попасть, надо правой кнопкой нажать на ярлык «Мой компьютер» и выбрать пункт свойства, там переключится на вкладку «Оборудование» и там нажать на кнопку «Диспетчер устройств». Все устройства, которые помечены восклицательным знаком не имеют драйверов. И их надо установить.

# 1.7 Достоинства и недостатки

Как и у одноранговой сети, у сети с выделенным сервером имеются свои досто­инства и недостатки. Основное преимущество заключается в централизованном управлении ресурсами и возможности с легкостью найти нужный ресурс. В Windows Server управление общими папками, жесткими дисками, принтерами и даже пользователями осуществляется с помощью специальной службы Active Directory.

Служба Active Directory используется для добавления и удаления пользователей из сети и может даже объединять в группы пользователей, получивших доступ к одному и тому же ресурсу. Такие средства, как Active Directory, позволяет администраторам управлять доступом в сеть и различными уровнями допуска, которые присваиваются пользователям или группам пользователей [5].

Однако возможность управлять пользователями сети и ресурсами имеет высокую цену, и одним из главнейших недостатков сети с выделенным сервером является стоимость сервера и сетевой операционной системы, которую необ­ходимо установить на нем. Также это обычно означает появление в штате компании новой должности, а следовательно, и дополнительных расходов.

И все же суммарная стоимость программного обеспечения и компьютерной техники в наше время стала ниже, чем когда бы то ни было, а сети с выделенным сервером устанавливаются повсеместно даже в мелких компаниях. Средства за­щиты, входящие в состав сетевой операционной системы, позволяют системно­му администратору защитить корпоративную информацию от угроз извне, а так­же отслеживать секретные данные и доступ к ним внутри сети.

Представим достоинства и недостатки сетей с выделенным сервером в виде  
двух списков. Сначала перечислим достоинства:

* для получения доступа к сетевым ресурсам пользователь вводит только одно регистрационное имя и пароль;
* управление безопасностью в сети и сетевыми ресурсами осуществляется централизованно;
* централизованное размещение каталогов и файлов позволяет с легкостью выполнять резервное копирование;
* специализированные мощные серверы обеспечивают быстрый доступ к ресурсам;
* сеть с выделенным сервером можно легко расширить.

А теперь поговорим о недостатках:

* мелким компаниям стоимость сетевого оборудования, сетевой операцион­ной системы и соответствующих клиентских лицензий может оказаться не по карману;
* кому-то приходится осуществлять, настройку и управление ресурсами в сети. То есть, необходим системный администратор;
* при сбое главного сервера доступ к сетевым ресурсам прекращается.

# 2 Назначение, область применения, архитектура ОС Linux.

Операционная система Linux, разработанная в начале 90-х годов по инициативе энтузиаста-одиночки, в настоящее время превратилась в полноценную, высокоэффективную и надежную серверную ОС, получившую признание и широкое распространение во всем мире. Одной из важнейших отличительных особенностей Linux является открытость исходного кода, что дает возможность контролировать ее использование и при необходимости вносить изменения.

Операционная система Linux (любые дистрибутивы и версии) распространяется на основе генеральной общественной лицензии GPL (General Public License), позволяющей свободно использовать, модифицировать и распространять программные продукты в первоначальном или измененном виде, как на коммерческой, так и на некоммерческой основе. Благодаря участию в разработке и тестировании ОС Linux сотен тысяч программистов во всем мире, программный код системы быстро развивается и совершенствуется. Это создало предпосылки для признания Linux в качестве системы с высокой степенью надежности и безопасности, подтвержденной международным сертификатом Common Criteria (ISO/IEC 15408). Данный сертификат свидетельствует о возможности использования Linux при решении критически важных задач, например, в банковских и военных системах.

# 2.1 Архитектура ОС Linux

Linux создавалась как UNIX-подобная операционная система, поэтому принципы ее архитектуры мало чем отличаются от стандартной UNIX. Базовым элементом Linux является ядро (kernel), которое непосредственно взаимодействует с аппаратной частью компьютера, изолируя прикладные программы от особенностей его архитектуры. Ядро обеспечивает выполнение основных функций операционной системы, включая управление процессами и памятью, поддержку файловой системы и управление вводом-выводом. Процессами в Linux называют находящиеся в стадии выполнения программы, которые претендуют на получение имеющихся аппаратных ресурсов и данных [6].

Управление процессами осуществляется планировщиком процессов (scheduler), который создает процессы и управляет распределением ресурсов между ними. В частности, планировщик управляет выделением квантов процессорного времени и осуществляет диспетчеризацию процессов, выбирая для выполнения процесс с наивысшим приоритетом. Для взаимодействия между процессами поддерживается механизм обмена управляющими сигналами, а также обеспечивается возможность обмена данными между различными процессами.

 Управление памятью основано на методе страничной организации виртуальной памяти, реализуемом в соответствии с аппаратными особенностями той или иной платформы.

Файловая система Linux обеспечивает унифицированный интерфейс доступа к данным, расположенным на дисковых накопителях и других периферийных устройствах. Файловая система имеет иерархическую организацию, с возможностью объединения файлов в соподчиненные каталоги. Логически данная организация в точности соответствует файловой системе HFS UNIX. Файловая система контролирует права доступа к файлу при выполнении различных операций, основываясь на статусе и привилегиях пользователя и запущенных им приложений. Следует отметить, что все периферийные устройства рассматриваются как элементы единой файловой системы Linux.

 Управление вводом-выводом заключается в выполнении запросов файловой системы и модуля управления процессами на доступ к различным периферийным устройствам (дискам, принтерам, пользовательским терминалам, сетевым адаптерам и т.п.). При выполнении операций ввода-вывода организуется разделяемый доступ к устройствам и обеспечивается необходимая буферизация данных. Программную основу ввода-вывода составляют драйверы устройств.

 Помимо ядра Linux включает набор утилит и вспомогательных программ, предназначенных для администрирования системы, обслуживания устройств, реализации дополнительных сервисов, разработки приложений и т.д. Особое место здесь занимают средства поддержки пользовательского интерфейса Linux, включающие как традиционные для UNIX-систем версии командного интерпретатора shell, так и графические оболочки (KDE, Gnome). Взаимодействие вспомогательных программ (так же, как и пользовательских приложений) с ядром происходит посредством стандартного интерфейса системных вызовов. Интерфейс системных вызовов (API) представляет собой набор услуг ядра и определяет формат запросов на услуги. Процесс запрашивает услугу посредством системного вызова определенной процедуры ядра, внешне похожего на вызов обычной библиотечной функции.

# 2.2 Настройка DHCP в Linux

DHCP в Linux реализован в виде домена сервера (dhcpd) и демона клиента (dhcpcd или pump (в Red Hat)). Демон dhcpd запускается на сервере и непосредственно отвечает за назначение и отбор IP-адресов клиентам, при входе и выходе их из сети. Клиентский демон, как явствует из названия, запускается на стороне клиента.

DHCP при установке Linux обычно не устанавливается, однако входит в состав дистрибутивов. В любом случае можно скачать последнюю версию с сайта. Установить пакет dhcp и включить поддержку динамических IP-адресов командой echo «1» > /proc/sys/net/ ipv4/ip\_dynaddr.

Конфигурационным файлом для dhcpd является /etc/dhcpd.conf. При запуске DHCP-сервера происходит выделение IP-адресов согласно содержащимся в файле /etc/dhcpd.conf установкам. Выделенные адреса dhcpd регистрирует в файле dhcpd. leases, который обычно находится в каталоге /var/dhcpd [3].

# 2.3 Настройка DNS в linux

После активизации интерфейсов и установки маршрутов компьютер может обмениваться пакетами, как с компьютерами локальной сети, так и с любыми другими компьютерами, с которыми он соединен системой шлюзов. Для указания адреса назначения пакета используются IP-адреса. Такая адресация естественна для маршрутизаторов, но чрезвычайно неудобна для пользователей. Преобразование символьных имен (например, www. awl. com) в IP-адреса, используемые при маршрутизации пакетов, осуществляет система доменных имен (DNS - Domain Name System). Кроме того, DNS может также осуществлять обратное преобразование.

DNS поддерживает глобальную распределенную базу данных, для работы с которой используется большое количество серверов. Для того чтобы пользоваться этой базой, компьютер должен знать адрес лишь одного сервера DNS. Большинство организаций и провайдеров Internet устанавливают у себя один или несколько серверов. Чтобы узнать адрес такого сервера, надо обратиться к администратору сети. Получив эти сведения, надо включить их в файл /etc/resolv. conf. В данном файле может содержаться до трех строк, начинающихся с ключевого слова name serveг, за которым следует IP-адрес сервера DNS. В этом файле также указывается домен по умолчанию (для этого используется ключевое слово domain) и произвольное число доменов, в которых выполняется поиск имени. Поиск проводится в том случае, если указано лишь имя компьютера, а имя домена пропущено (например, если вместо mail. threeroomco. com пользователь задал имя mail).

# 2.4 Пошаговая установка Linux

Для начала скачайте последний дистрибутив [Linux](http://mintlinux.ru/catalog/1003) , если вы еще не сделали это ранее. Теперь загружаемся с диска [7].

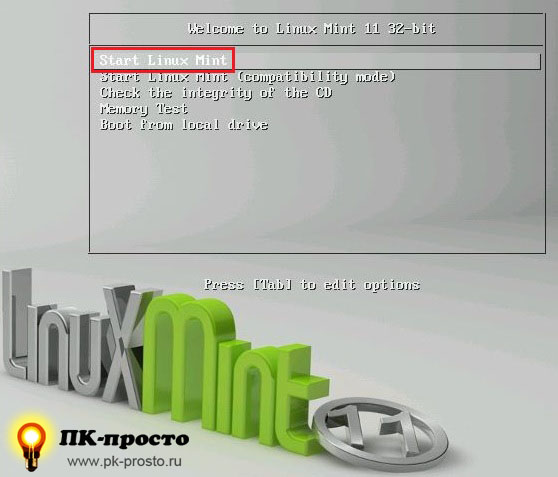
[](http://pk-prosto.ru/wp-content/uploads/2011/09/1.jpg)

Рисунок 1.29 – Пошаговая установка ОС Linux

Когда система загрузиться, мы увидим рабочий стол окружения Gnome. Нужно нажать на значок **Install Linux,** и начинаем установку.

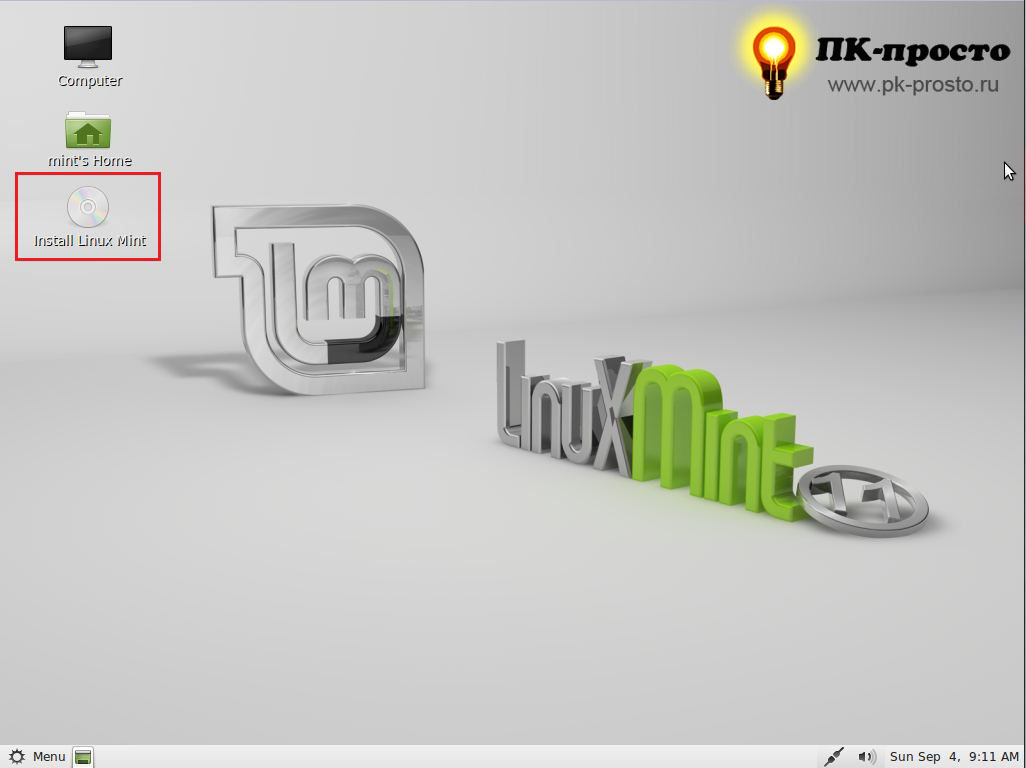
[](http://pk-prosto.ru/wp-content/uploads/2011/09/2.jpg)

Рисунок 1.30 – Пошаговая установка ОС Linux

Выбираем язык системы и нажимаем вперед.

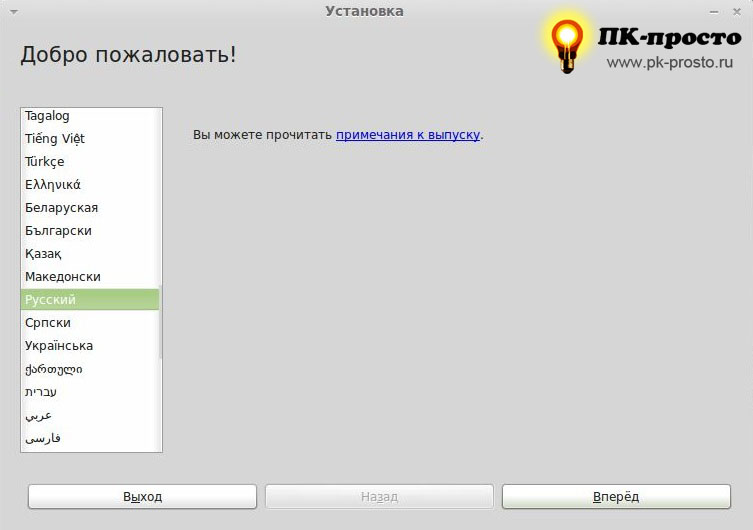
[](http://pk-prosto.ru/wp-content/uploads/2011/09/3.jpg)

Рисунок 1.31 – Выбор языка при установке

Проверяем компьютер на соответствия требованиям, и нажимаем вперед.

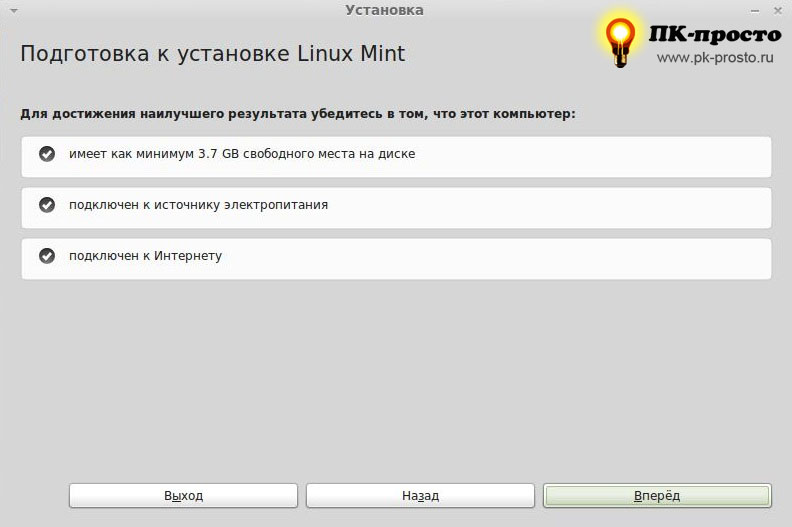
[](http://pk-prosto.ru/wp-content/uploads/2011/09/4.jpg)

Рисунок 1.32 – Проверка соответствия требованиям

Далее предлагается распределить место на жестком диске. Если установка системы впервые и на винчестере еще нет никаких данных можно довериться установщику и разрешить ему самостоятельно распределить жесткий диск.

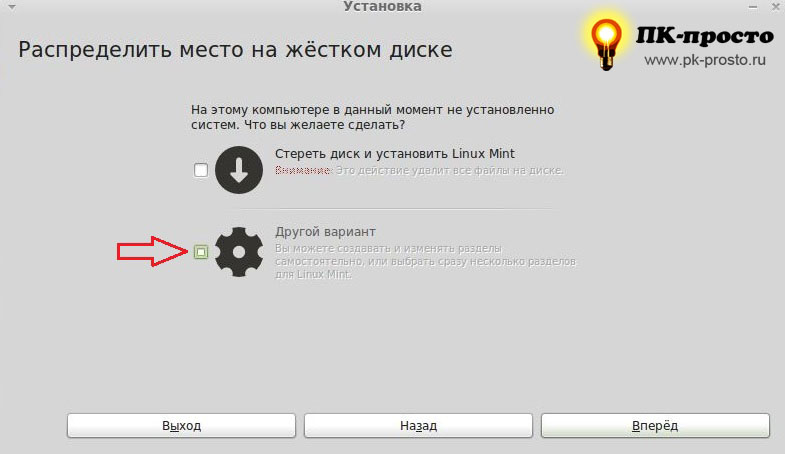
[](http://pk-prosto.ru/wp-content/uploads/2011/09/5.jpg)

Рисунок 1.33 – Разделение места на жестком диске

Структура хранения данных в Linux отличается от таковой в Windows. Здесь нет привычных локальных дисков C:, D: и прочих. Выбираем свободное место на жестком диске и распределяем его по такому принципу: 1. Пространство под систему и программы: 5 Гб — минимум, 10 — Гб достаточно, 15 Гб — с запасом. 2. Раздел подкачки: если мало оперативной памяти (от 512 Мб до 4 Гб), то раздел подкачки делаем в два раза больше ее объема. Если большой объем оперативной памяти (от 8 Гб) — подкачку можно не использовать. 3. Все оставшееся пространство отдаем под хранение пользовательских данных.

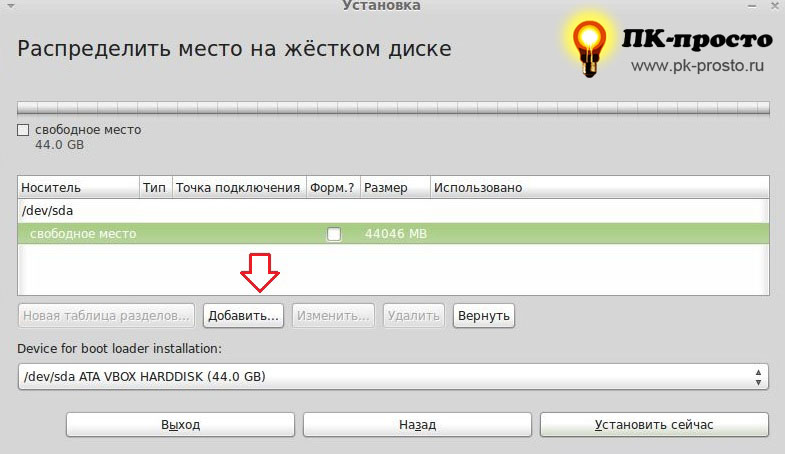
[](http://pk-prosto.ru/wp-content/uploads/2011/09/6.jpg)

Рисунок 1.34 – Разделение места на жестком диске

После нажатия на кнопку «Добавить» создаем разделы. Размер корневого (системного) раздела установим 15000 Мб (почти 15 Гб). Файловую систему выбираем Ext4. Точка монтирования — «/».

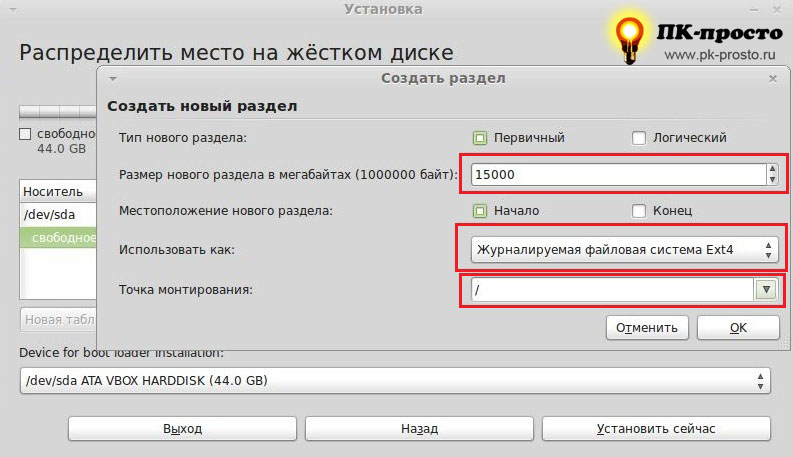
[](http://pk-prosto.ru/wp-content/uploads/2011/09/7.jpg)

Рисунок 1.35 – Разделение места на жестком диске

Выбираем оставшееся свободное пространство и нажимаем «Добавить». Теперь создаем раздел подкачки, а для этого выбираем его размер (например 2 Гб, так объем оперативной памяти на тестовой машине всего 1 Гб) и в поле «Использовать как» указываем раздел подкачки.

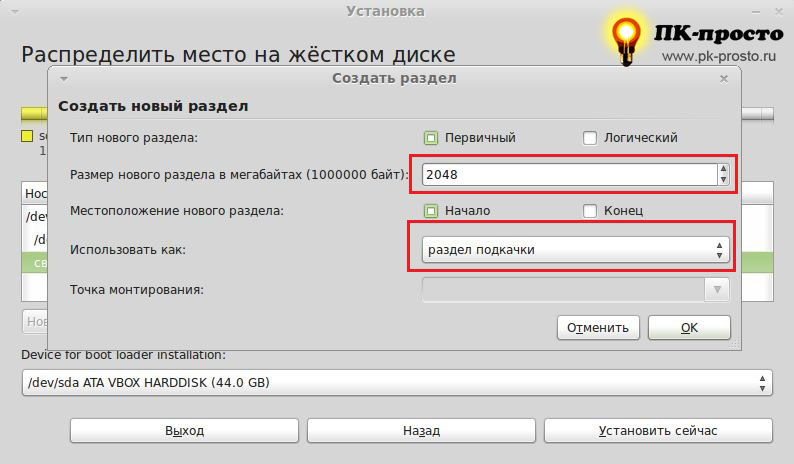
[](http://pk-prosto.ru/wp-content/uploads/2011/09/8.jpg)

Рисунок 1.36 – Создание нового раздела

Теперь оставшееся место всецело отдаем под Домашнюю папку.

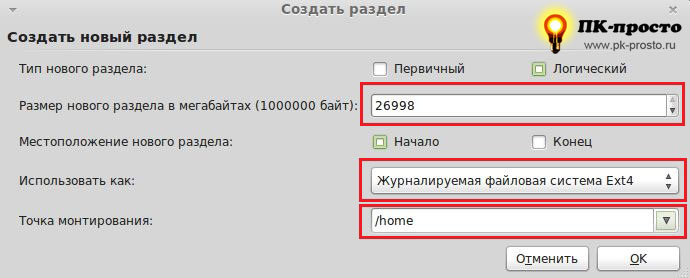
[](http://pk-prosto.ru/wp-content/uploads/2011/09/9.jpg)

Рисунок 1.37 – Создание нового раздела

Конечно есть и другие способы разбивки диска (с отведением отдельных разделов под каталоги **/boot**, **/var** и **/usr** и т.д.), которые используют профессионалы и продвинутые пользователи Linux, но для не подготовленного пользователя указанной разбивки будет достаточно.

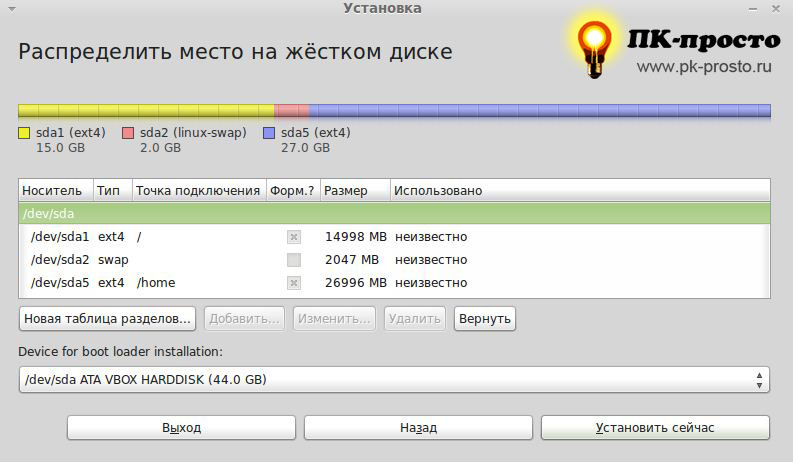
[](http://pk-prosto.ru/wp-content/uploads/2011/09/10.jpg)

Рисунок 1.38 – Установка операционной системы

Теперь нажимаем «Установить сейчас» и приступаем к заполнению пользовательских данных, а система тем временем будет копировать файлы с оптического диска на винчестер.

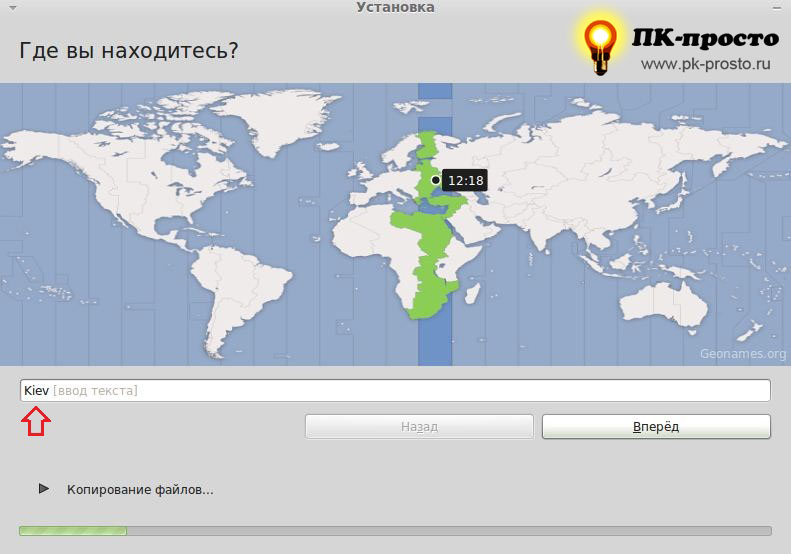
[](http://pk-prosto.ru/wp-content/uploads/2011/09/11.jpg)

Рисунок 1.39 – Установка некоторых параметров

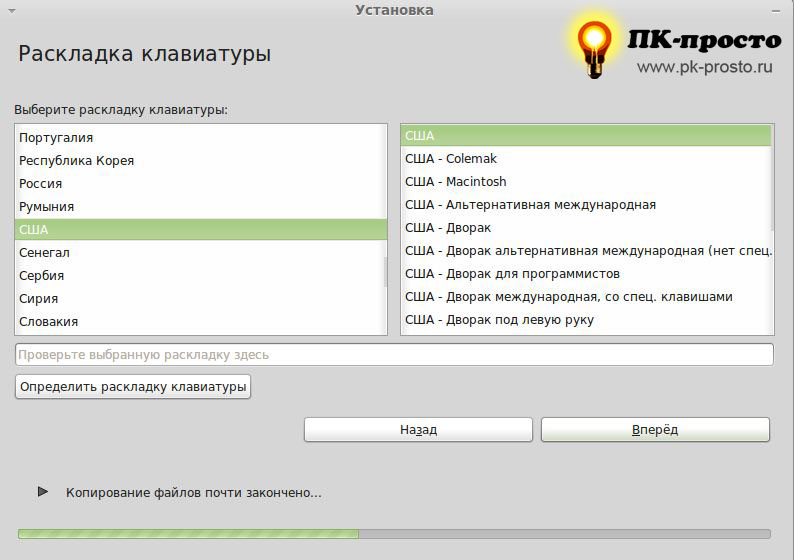
[](http://pk-prosto.ru/wp-content/uploads/2011/09/12.jpg)

Рисунок 1.40 - Установка некоторых параметров

Внимательно заполняйте следующие поля:

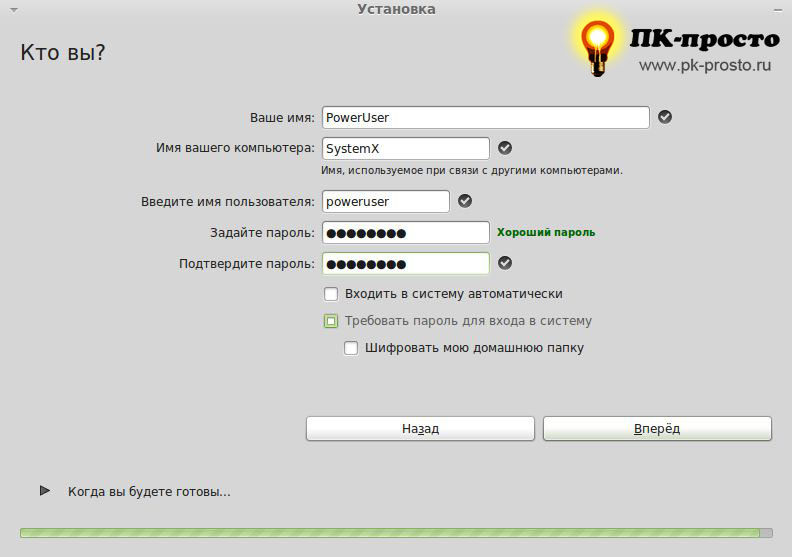
[](http://pk-prosto.ru/wp-content/uploads/2011/09/13.jpg)

Рисунок 1.41 – Установка данных пользователя

После этого нажимаем «Вперед» и система начнет устанавливаться.

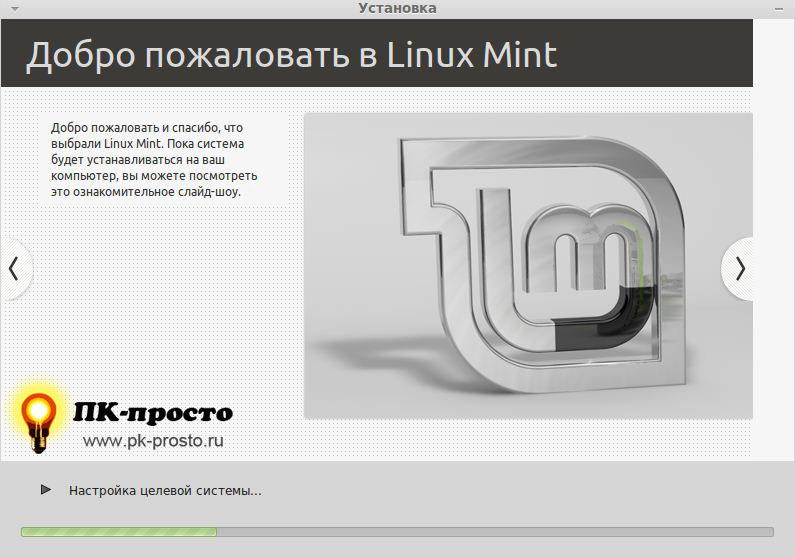
[](http://pk-prosto.ru/wp-content/uploads/2011/09/14.jpg)

Рисунок 1.42 – Завершение установки

По завершению вам предложат перезагрузиться и начать использовать **установленную Linux**.

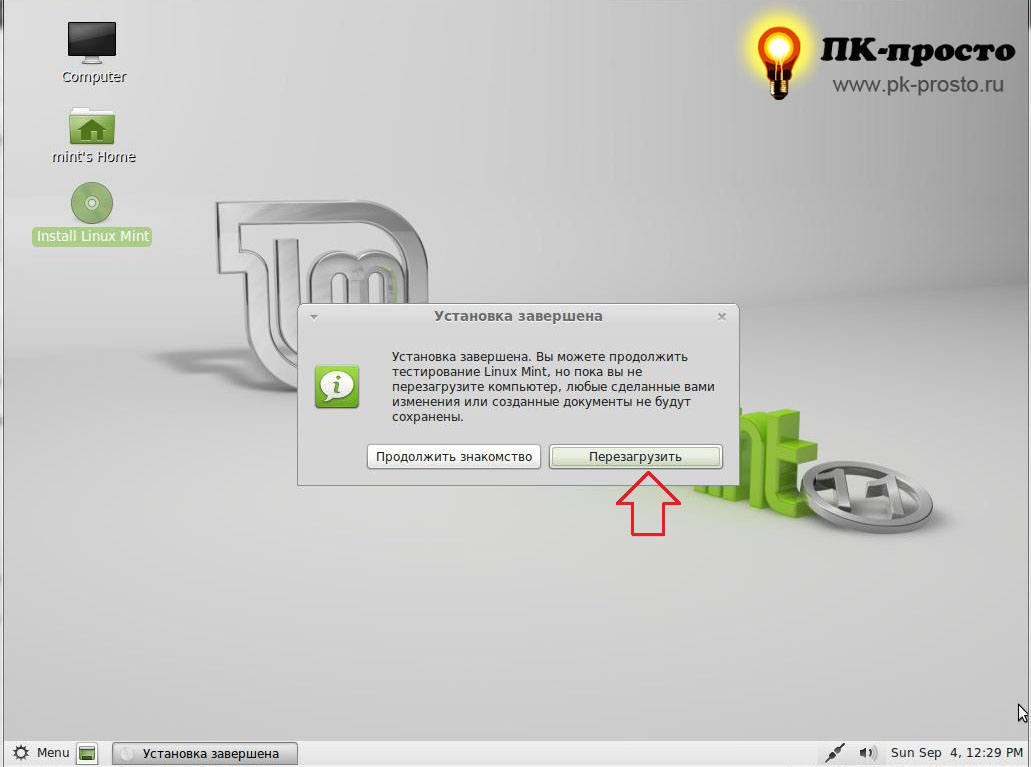
[](http://pk-prosto.ru/wp-content/uploads/2011/09/15.jpg)

Рисунок 1.43 – Выбор параметров

Перезагружаем компьютер, не забыв при этом извлечь диск из системного блока, когда система попросит сделать это. Теперь выбираем свой логин и вводим пароль.

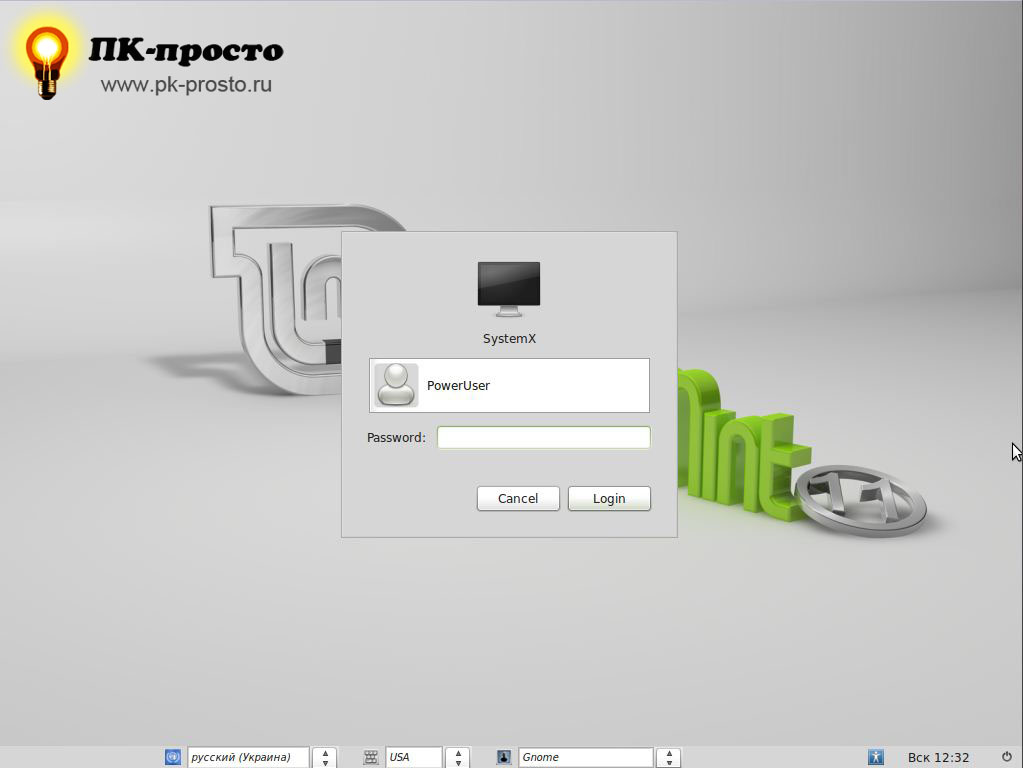
[](http://pk-prosto.ru/wp-content/uploads/2011/09/16.jpg)

Рисунок 1.44 – Авторизация пользователя

Вот мы и в системе и, казалось бы, можно приступать к изучению и работе, но рекомендуют сделать некоторую донастройку.

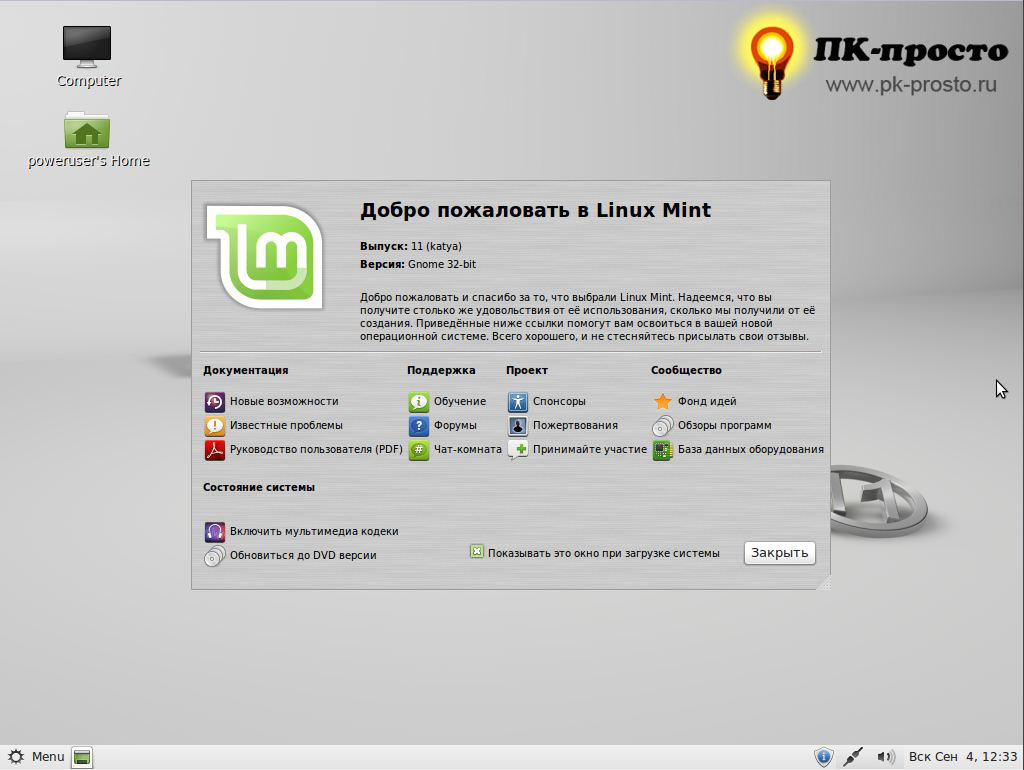
[](http://pk-prosto.ru/wp-content/uploads/2011/09/17.jpg)

Рисунок 1.45 – Донастройка операционной системы

Во первых нужно проверить соединение с Интернетом. Если у вас IP адрес раздается автоматически, то система будет подключена к сети еще в процессе установки. Если же адрес нужно прописывать вручную, то сделать это вы можете, нажав на значок с двумя кабелями, который расположен возле часов, и выбрав пункт «Изменить соединения». В окне «Сетевые соединения» переходим на вкладку своего типа подключения и выбираем текущее соединение, после чего нажимаем кнопку «Изменить».

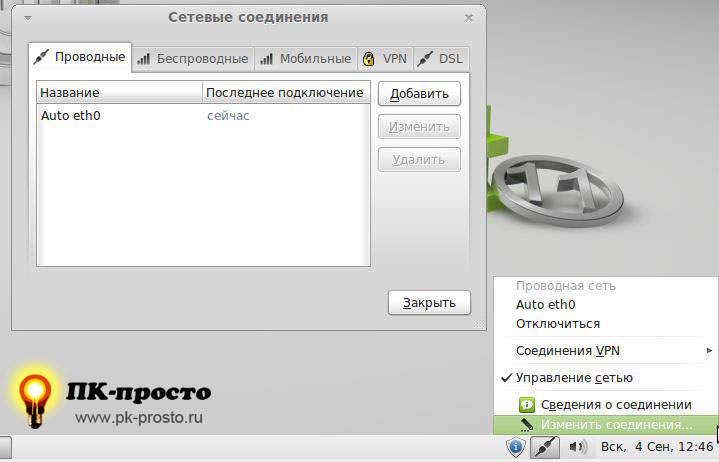
[](http://pk-prosto.ru/wp-content/uploads/2011/09/18.jpg)

Рисунок 1.46 – Настройка сетевых соединений

Здесь переходим на вкладку «Параметры IPv4» и вместо профиля «Автоматически (DHCP)» выбираем профиль «Вручную». Теперь в поле адреса нужно будет вбить настройки провайдера, которые обычно указаны в договоре на предоставления услуг, и нажать кнопку «Сохранить».

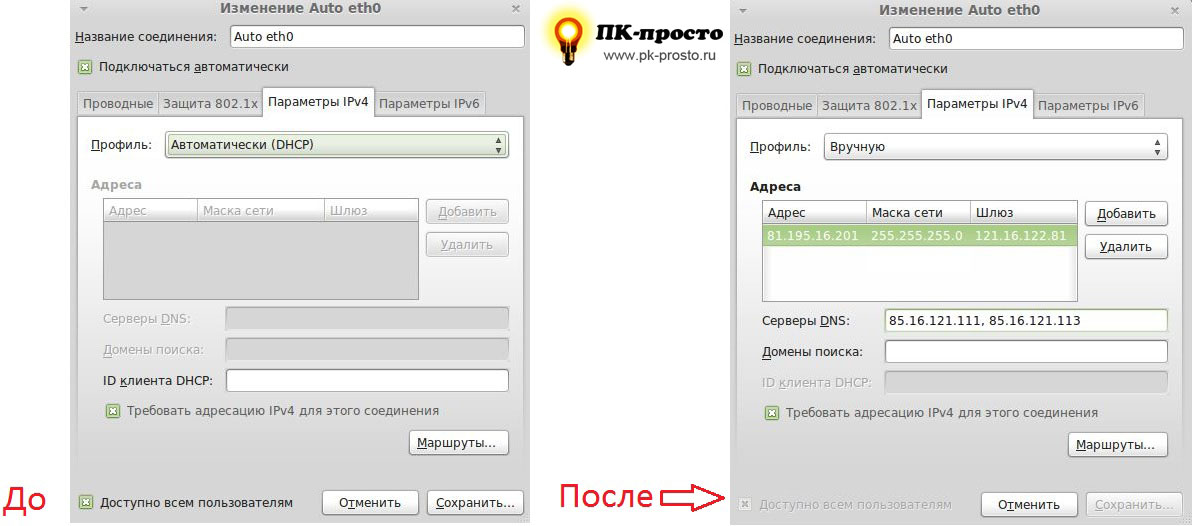
[](http://pk-prosto.ru/wp-content/uploads/2011/09/19.jpg)

Рисунок 1.47 – Установка настроек провайдера

Теперь, когда есть подключение к Интернет, нужно установить полную поддержку русского языка. Дело в том, что на диске физически не могут быть расположены полные файлы всех языковых пакетов, поэтому при выборе языка во время установки система русифицируется частично. Нажимаем «Menu>Центр управления(аналог Панели управления в Windows)>раздел System>пункт Язык системы». После этого система сообщит о том, что поддержка языка установлена не полностью и предложить скачать и доустановить недостающие пакеты. Соглашаемся, вводим пароль. В Linux запуск любых операций или действий требующих прав Администратора системы (здесь он называется **root**) сопровождается обязательным вводом пароля. После его ввода нажимаем на кнопку с надписью Authenticate.

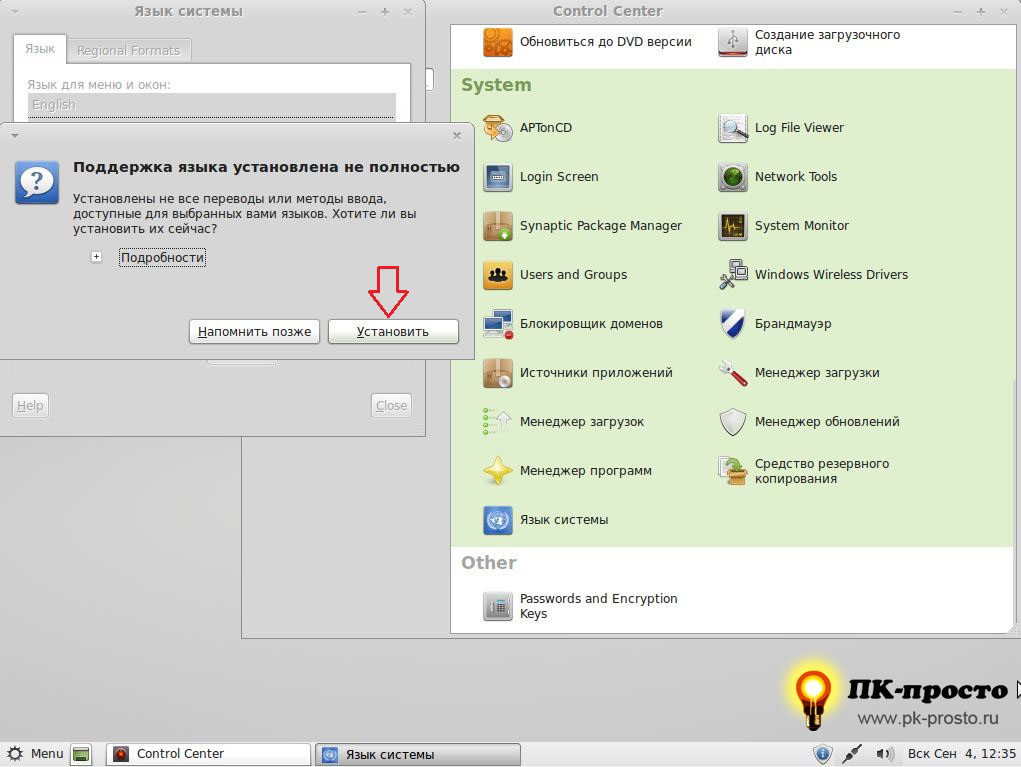
[](http://pk-prosto.ru/wp-content/uploads/2011/09/20.jpg)

Рисунок 1.48 – Донастройка поддержки языка

Для того, чтобы увидеть изменения нужно будет выйти из текущего сеанса и зайти заново.

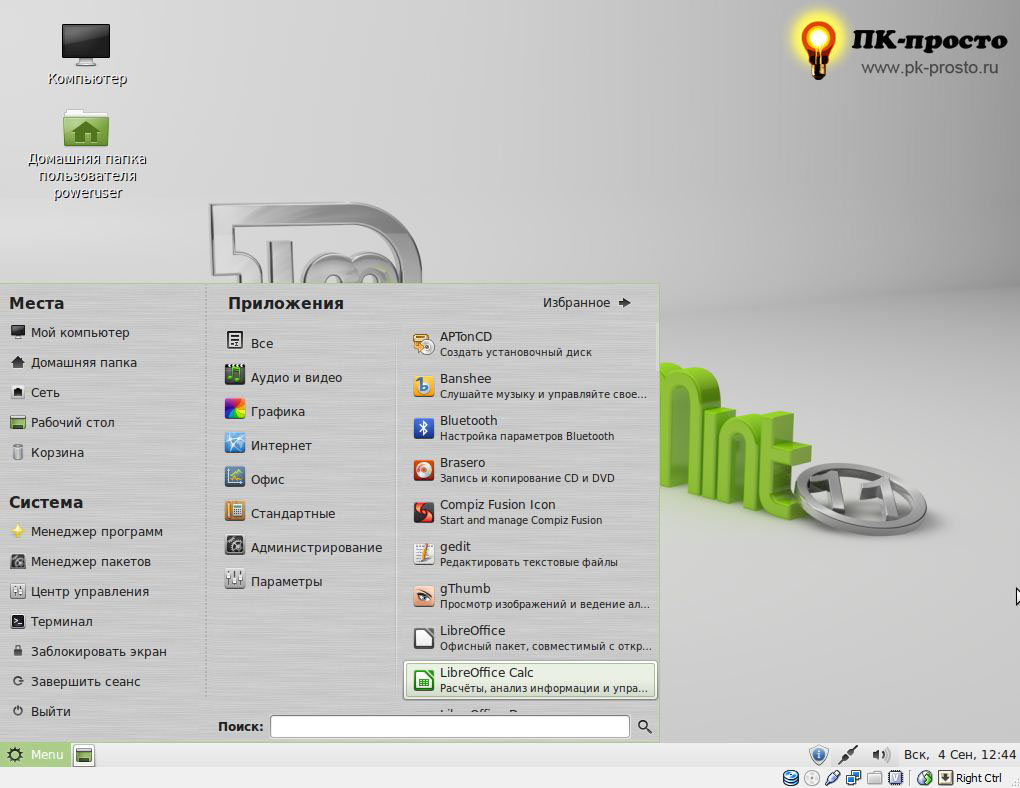
[](http://pk-prosto.ru/wp-content/uploads/2011/09/21.jpg)

Рисунок 1.49 – Перезапуск системы

# 2.5 Достоинства и недостатки Linux

# 

# 2.5.1 Недостатки

У Linux, как и у любой ОС, есть свои недостатки. Наиболее значительные из них:

1. Система все еще слишком сложна для непрофессиональных пользователей. Этот недостаток не может быть решен за счет создания средств конфигурирования системы с графическим или web-интерфейсом, поскольку разработчики прикладных программ в большинстве не заинтересованы в таких конфигураторах. А разработчики этих средств конфигурирования не могут успеть за развитием других частей системы. Добавление элементов управления в программу-конфигуратор обходится несравнимо дороже, чем добавление пары строчек в текстовый файл. Создание документации может только частично сгладить проблему, так как прочтение очень большого объема документации отнимает много времени.
2. Разработка драйверов устройств для Linux пока отстает от Windows. Она затрудняется тем, что драйверы под Linux пишутся самими пользователями оборудования, вместо фирм-производителей. Поддерживаются только самые популярные устройства. Для написания драйвера под Linux от производителей требуется открыть детали интерфейса с их оборудованием. Многие производители считают, что это может привести к разглашению их ноу-хау и нанести ущерб их бизнесу. Разработка бинарных (без исходных текстов) драйверов для Linux затруднена, поскольку модули ядра, в виде которых обычно распространяются драйверы, не предназначены для переносимости между разными версиями Linux, а новые версии выходят очень часто.
3. Разработчики популярного коммерческого ПО пока не торопятся портировать свои приложения под Linux. Они ожидают момента, когда Linux наберет "критическую массу", т.е. пока расходы на портирование не станут меньше доходов от продажи продукта пользователям Linux. Но, в то же время, многие пользователи не спешат переходить на Linux, поскольку под ним нет привычного им программного обеспечения.
4. Linux разрабатывается интернациональной командой и их языком общения является английский. Вся документация также создается на этом языке. Только небольшая часть этой документации переведена на русский язык, что создает трудности для пользователей, не читающих по-английски. Система слишком сложна, чтобы в ней можно было разобраться без документации, а найти что-то на русском языке на тему бывает очень трудно.

5. Различия между дистрибутивами Linux создает трудности при поддержке. Стандартизация необходима, но дистрибутивы различаются и будут различаться программами установки, процедурами установки ПО. К тому же производители ПО нередко тестируют свои продукты только на одном дистрибутиве Linux – на самом распространенном. Дистрибутивы, конечно, все совместимы между собой, но иногда бывают трудности, связанные с тем, что различаются версии библиотек, ядра, процедура начальной загрузки, а иногда даже пути к каким-либо ключевым файлам. Все эти проблемы решаемые, но лучше бы их не было [1].

# 2.5.2 Преимущества

Конечно же, Linux имеет и черты, которые отличают его от других ОС. Наиболее выделяющиеся:

1. Командная строка.

В Unix пользовательский интерфейс командной строки приближен к совершенству, в комплекте с системой идет множество полезных утилит, которые можно использовать с командной строки, а скрипты позволяют автоматизировать множество задач. Даже графический интерфейс Unix - X Window System не предполагает отказа от командной строки и никогда ей не противопоставлялся, как в Windows.

Под Linux существуют и программы типа Norton-а - Midnight Commander.

1. "Понятность" системы.

Можно ткнуть пальцем в любой файл в любом каталоге и, при желании, узнать, зачем он нужен и почему находится именно в этом каталоге. Можно оставить только необходимые для какого-то конкретного приложения файлы и запускать Linux с одной дискеты или использовать эту систему во встраиваемых приложениях.

Linux предоставляет развитые возможности для диагностики проблем, такие как лог-файлы, утилита strace и встроенные во многие программы средства отладки. Эти же средства позволяют составить представление о том, как работает та или иная программа, даже если нет желания или возможности изучать ее исходные тексты.

Систематизация файлов тоже помогает разбираться в файловой системе.

1. Удаленное управление.

Linux имеет очень развитые средства удаленного управления. Причем управлять машиной под управлением Linux можно с любой другой системы, где есть программа эмулятор терминала (в отличие, например, от Windows NT).

1. Многопользовательская работа.

Пользовательские настройки отделяются от системных, т.е. от тех, которые относятся ко всем пользователям и к системе в целом. Такое разделение положительно сказывается на устойчивости и безопасности системы. Многопользовательский режим позволяет производить настройку системы, не прерывая работы пользователей.

1. Стабильность.

Возможность обновления системных библиотек, загрузки и выгрузки драйверов устройств, обновление практически любых программ на ходу позволяют месяцами обходиться без перезагрузки системы, а следовательно и без прерывания функционирования сервисов и работы пользователей.

Перезагрузка Linux требуется только в случае модернизации компьютера или обновления ядра.

1. Гибкая файловая система.

Файловая система Linux предусматривает такие средства, как точки монтирования, символьные и жесткие ссылки. Это позволяет эффективно распределять место на диске и решать проблемы, когда какая-либо программа требует файл в определенном каталоге, а он на самом деле в системе находится в другом месте [1].

# Заключение

В данной работе были рассмотрены две ОС: Windows Server и Linux, настройки в них служб DHCP и DNS, рассмотрены их достоинства и недостатки.

Windows Server обладает гибкостью, позволяющей расширять, сужать или распределять серверные системы без ущерба для многофункциональности и соотношения цена/быстродействие для платформы операционной системы.

Linux является надежной, гибкой и высокоэффективной ОС.

Данная тема имеет немаловажное значение. На сегодняшний день разработка и внедрение локальных информационных систем является одной из самых интересных и важных задач в области информационных технологий. Появляется потребность в использовании новейших технологий передачи информации. Интенсивное использование информационных технологий уже сейчас является сильнейшим аргументом в конкурентной борьбе, развернувшейся на мировом рынке.

# Список использованных источников

1. Преимущества и недостатки ОС Linux [электронный ресурс] – http http://works.doklad.ru/view/PNWsJdsbJOQ.html;
2. Анализ принципов администрирования операционных систем на примере Windows [электронный ресурс] – http http://bukvasha.ru/kursova/191284;
3. Настройка DHCP в Linux [электронный ресурс] – http://daybook.org.ua/linux/dhcp-2.html;
4. Иллюстрированный самоучитель по Windows Server [электронный ресурс] – http://samoucka.ru/document31673.html;
5. Преимущества и недостатки сетей с выделенным сервером [электронный ресурс] – http://studall.org/all2-49605.html;
6. Архитектура ОС Linux [электронный ресурс] – http http://s-nov.narod.ru/12.Operatsionnye/12.Operatsionnye.htm;
7. Пошаговая установка Linux [электронный ресурс] – http://pk-prosto.ru/ustanovka-linux-mint/;
8. Пошаговая установка Windows Server [электронный ресурс] – http://akak.ru/recipes/876-ustanovka-windows-2003-server;
9. Пошаговая установка DNS-сервера в Windows Server [электронный ресурс] – http://system-administrators.info/?p=1919;
10. Пошаговая установка DNS-сервера в Windows Server [электронный ресурс] – http://online-studies.ru/kak-ustanovit-dhcp-server-rol-na-windows-2008-i-kak-potom-upravlyat-dhcp/;
11. Пошаговая установка FTP-сервера в Windows Server [электронный ресурс] – http://geek-nose.com/ftp-server-windows-7-udobryj-sposob-xraneniya-i-peredachi-dannyx/.