ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Петербургский государственный университет путей сообщения Императора Александра I»
(ФГБОУ ВО ПГУПС)

Петрозаводский филиал ПГУПС

ОДОБРЕНО
на заседании цикловой комиссии
протокол № 11 от 23 06 2017
Председатель цикловой комиссии:
_____ (Камынов)

УТВЕРЖДАЮ
Начальник УМО
_____ А.В. Калько
«23» 06 2017 г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по организации и проведению практических занятий

По учебной практике: УП.02.01. Администрирование сетей

Специальность: 09.02.02 Компьютерные сети

Выполнил:

2017г.

ВВЕДЕНИЕ

Методическое пособие по проведению учебной практики, входящей в состав ПМ.02. Организация сетевого администрирования составлено в соответствии с требованиями Федерального государственного образовательного стандарта по специальности среднего профессионального образования (далее СПО) 09.02.02 Компьютерные сети

Настоящее методическое пособие рассчитано на самостоятельную работу обучающихся в учебном кабинете под руководством преподавателя, а также является руководством для преподавателей при подготовке к проведению учебной практики.

Для успешного прохождения учебной практики могут быть использованы теоретические знания, полученные обучающимися при изучении ПМ.02.Организация сетевого администрирования

УП.02.01. Администрирование сетей направлена на:

- приобретение студентами профессиональных навыков и первоначального опыта в профессиональной деятельности;
- формирование основных профессиональных компетенций, соответствующих виду профессиональной деятельности (ВПД): Организация сетевого администрирования;
- воспитание сознательной трудовой и производственной дисциплины;
- усвоение студентами основ законодательства об охране труда, системы стандартов безопасности труда, требований правил гигиены труда и производственной санитарии, противопожарной защиты, охраны окружающей среды в соответствии с новыми нормативными и законодательными актами.

Результатом освоения учебной практики является овладение обучающимися видом профессиональной деятельности (ВПД): Организация деятельности коллектива исполнителей, в том числе профессиональными (ПК) компетенциями:

Код	Наименование результата обучения
ПК 2.1.	Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.
ПК 2.2.	Администрировать сетевые ресурсы в информационных системах.
ПК 2.3.	Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.
ПК 2.4.	Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

Каждый студент обязан оформлять отчет о проделанной работе. Отчет должен содержать:

- титульный лист;

- цель работы;

- задание;

- выполненное практическое занятие в соответствии с заданием;

- вывод;

Правила охраны труда при проведении учебной практики.

1. Общие требования охраны труда.

1.1. К работе в учебном кабинете допускаются студенты, прошедшие инструктаж по охране труда, знающие правила пожарной безопасности.

1.2. При работе в кабинете должны соблюдаться правила поведения, расписание учебных занятий, установленный режим труда и отдыха.

1.3. При проведении занятий возможно воздействие на студентов следующих опасных факторов:

- нарушение осанки, искривление позвоночника, развитие близорукости при неправильном подборе мебели;

- нарушение остроты зрения при недостаточной освещенности в кабинете;

- поражение электрическим током при неисправном оборудовании кабинета;

1.4. В процессе занятий студенты должны соблюдать правила личной гигиены, содержать в чистоте рабочее место.

2. Требования безопасности перед началом занятия.

2.1. Включить полностью освещение в кабинете, убедиться в правильности работы светильников. Наименьшая освещенность в кабинете должна быть не менее 300Лк (20ВТ/м^2) при люминесцентных лампах.

2.2. Убедиться в исправности электрооборудования кабинета: коммуникационные коробки выключателей и розеток не должны иметь трещин, сколов, а также оголенных контактов.

2.3. Проверить санитарное состояние кабинета, убедиться в целостности стекол в окнах и провести сквозное проветривание кабинета.

3.Требование безопасности во время занятия.

3.1. Используемые в кабинете демонстрационные электрические приборы должны быть исправны и иметь заземление и зануление.

4. Требования безопасности в аварийных ситуациях.

4.1. При возникновении аварийных ситуаций немедленно эвакуировать студентов и сообщить администрации учреждения.

5. Требования безопасности по окончании занятия.

5.1. Выключить демонстрационные электрические приборы;

5.2. Закрыть окна и выключить свет

Практическое занятие №1.

Определение требований заказчика к сети. Сбор данных для анализа использования программно-технических средств компьютерных сетей.

Цель: Определить требования заказчика к сети.

Требования к проектированию аппаратных (серверных комнат) Кроссовых комнат

Аппаратная – помещение, занимаемое телекоммуникационным и/или серверным оборудованием, обслуживающим пользователей в здании. Часто аппаратные являются помещениями специального назначения. Аппаратные соединяются с магистралями и обычно считаются средствами обслуживания здания.

Размещение в здании

- Помещение аппаратной не должно быть проходным. Желательно, чтобы оно не имело окон и не примыкало вплотную к внешним стенам здания. Если же в техническом помещении предусмотрены окна, то рекомендуется располагать аппаратную на северной или северо-восточной стороне здания. Крайне нежелательно размещать аппаратную рядом с теми внутренними конструкциями здания, которые ограничивают ее возможное расширение в будущем: лифтовые шахты, лестничные марши, вентиляционные камеры и т.д.
- Запрещается располагать аппаратную рядом с помещениями для хранения пожароопасных или агрессивных химических материалов.
- Не рекомендуется выделять помещение для аппаратной на верхних этажах здания, т.к. они наиболее подвержены повреждениям в случае пожара и могут заливаться при протечках крыши.
- Не допускается размещение аппаратной под помещениями, связанными с потреблением воды (туалеты, душевые, столовые, буфеты и т.д.). При размещении аппаратной в подвале, необходимы дополнительная гидроизоляция и тщательный выбор трасс прокладки трубопроводов. Через аппаратную не должны прокладываться транзитом трубопроводы инженерных систем здания.
- Предпочтительно размещать аппаратную недалеко от грузовых или грузопассажирских лифтов, используемых для транспортировки тяжелого оборудования, например ИБП. В тоже время, следует избегать близкого размещения мощных источников электрических и магнитных полей, а также

оборудования, которое может вызвать повышенную вибрацию.

- Многие источники рекомендуют располагать аппаратную в геометрическом центре здания хотя бы потому, что это позволяет существенно сэкономить на прокладке кабеля.

Помещение аппаратной

- Минимальный допустимый размер аппаратной - 14 квадратных метров.
- Минимальная высота потолка аппаратной должна составлять 2,44 м.
- Пол в аппаратной должен быть ровным и иметь антистатическое покрытие

Размещение кроссовых

- В соответствии с классификацией, кроссовые подразделяются на кроссовые внешних магистралей (КВМ), здания (КЗ) и этажа (КЭ).
- КЭ представляет собой служебное помещение, в которое вводятся кабели подсистемы внутренних магистралей СКС и кабели горизонтальной подсистемы. В этом помещении монтируются коммутационные панели, сетевые приборы и другие вспомогательные устройства. В кроссовых нельзя размещать оборудование, которое не имеет непосредственного отношения к тем функциям, для выполнения которых организуется данное техническое помещение, например силовые распределительные щиты электропитания этажа.
- В небольших СКС с количеством портов до 150-200 согласно накопленной статистике кроссовая зачастую является единственным техническим помещением и естественным образом совмещается с аппаратной.

Задание:

1. Ознакомится с требованиями заказчика:
    a. Скорость передачи данных не ниже 5000 Мбит/с;
    b. В каждом рабочем помещении по 2 ПК + 1 резервная розетка;
    c. На каждом этаже по 2 сетевых принтера;
    d. Серверная на 2 этаже здания;
    e. Кроссовые этажей на 1 и 3 этажах с возможностью расширения;
    f. Требования к оборудованию:
        - ПК: корпус miniTower с блоком питания не менее 350 Вт, HDD не менее 320 Гб, ОП не менее 4 Гб, DVD-привод, процессор не менее Intel Core i3, ОС + офисное ПО;
        - Монитор не менее 18” + клавиатура + мышь + сетевой фильтр;

- ♦ Коммутаторы не менее 24 портов + патч-панели не менее 24 портов;
- ♦ Сервер выполняет функции файл-сервера и принт-сервера
- ♦ Стойка серверная 8 U
- ♦ ИБП (серверный) минимум 1 час работы сервера и коммутаторов

g. Файл сервер доступен всем но с разными правами: 3 группы допуска (администраторы, руководство, сотрудники)
h. Доступ в Интернет всех пользователей
i. Минимальные затраты при вышеуказанных требованиях
j. Доступ к сетевым принтерам с любого ПК

2. Ознакомится с планировкой здания.
3. Проанализировать требования заказчика.
4. Выбрать места расположения серверной и кроссовых.

Практическое занятие №2

Выбор среды и скорости передачи.

Цель: научиться правильно, выбирать среду и скорость передачи.

Существует выбор между кабельной и беспроводной средой. В случае выбора кабельной среды выбор необходимо выбрать между витой парой и оптоволокном, так как выбранная ранее технология передачи данных использует именно эти среды.

Рассмотрим вкратце достоинства и недостатки каждой среды.

Витая пара -- вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой.

Витая пара бывает нескольких типов: неэкранированная витая пара UTP (Unscreened Twisted Pair), фольгированная FTP (foiled), фольгированная экранированная FBTP (foiled braided) и защищенная STP (shielded).

Достоинства:

- Такой кабель легко монтировать;
- Невысокая цена;
- Достаточная скорость передачи данных;
- Возможность передавать данные на достаточные для офиса расстояния.

Недостатки:
- Сильное воздействие внешних электромагнитных наводок;
- Возможность утечки информации;
- Сильное затухание сигналов.

Оптическое волокно -- нить из оптически прозрачного материала (стекло, пластик), используемая для переноса света внутри себя посредством полного внутреннего отражения.

Достоинства:
- Высокая скорость передачи информации (до 1000 Мбит/с и выше);
- Диапазон пролетов линии связи до 15 км;
- Надежность и долговечность использования;
- Невосприимчивость к воздействию атмосферного электричества.

Недостатки:
- Высокая цена кабеля;
- Высокая цена и сложность монтажа.

Wi-fi, беспроводная среда передачи данных

Достоинства:
- Позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развёртывания и/или расширения сети.
- Позволяет иметь доступ к сети мобильным устройствам.

Недостатки:
- Неполная совместимость между устройствами разных производителей;
- Ограниченный радиус действия;
- Высокое потребление энергии;
- Невысокий уровень безопасности.

Задание:
1.Выбрать среду для передачи данных
2.Определить скорость передачи данных необходимую для нормальной работы.

Практическое занятие №3

Выбор и размещение сетевых ресурсов: рабочих станций, периферии, кабелей, устройств связи, серверов.

Цель: Разместить сетевые ресурсы

Для совместной работы с файлами, необходим отдельный компьютер, выполняющий роль файлового сервера, который предназначается для хранения документации, доступ к которой обеспечен компьютерам сети. Кроме этого понадобится коммутатор, чтобы соединить несколько компьютеров в один сегмент. Далее стоит отметить, что одним из требований к ЛВС является наличие Wi-Fi. Чтобы его обеспечить, необходимо использовать Wi-Fi роутер. Кроме того для прокладки сети необходим сам кабель и розетки, а также короба, чтобы защитить провода от повреждений. Для сетевого оборудования понадобится шкаф.

Итак, для создания локальной сети потребуется следующее оборудование:

- компьютер, являющийся файловым сервером;

- коммутатор;

- Wi-Fi роутер;

- сетевой кабель;

- короба для прокладки;

- информационные розетки;

- коммутационный шкаф;

- конечное сетевое оборудование - компьютеры и ноутбуки.

Подбор маршрутизатора

Маршрутизатор (роутер) - сетевое устройство, используемое в компьютерных сетях, которое, на основании информации о топологии сети (таблицы маршрутизации) и определённых правил, принимает решения о пересылке пакетов сетевого уровня модели OSI их получателю. Обычно применяется для связи нескольких сегментов сети.

Существует 2 вида маршрутизаторов: программный и аппаратный. В первом случае он является частью операционной системы одного из компьютеров сети, во втором случае - специальным вычислительным устройством.

Аппаратный маршрутизатор - специализированное устройство, собранное на узкоспециализированном процессоре RISC или ARM, объединяющее в отдельном корпусе множество маршрутизирующих модулей.

Программный маршрутизатор - это рабочая станция или выделенный сервер, имеющий несколько сетевых интерфейсов и снабженный специальным программным обеспечением, настроенным на маршрутизацию.

Не смотря на то, что программный маршрутизатор обладают более гибким функционалом, чем аппаратный, в данном проекте он применяться не будет, так является менее надежным и более сложным в использовании. К тому же для него пришлось бы докупать адаптер Wi-Fi. Программный маршрутизатор требует того, чтобы компьютер, на котором он установлен был включенным, а это влечет лишние затраты на электроэнергию.

В отличие от коммутаторов и мостов, в таблицах маршрутизации этих устройств записываются номера подсетей, а не MAC-адреса. Вторым отличием является активный обмен с другими маршрутизаторами информацией о топологии связей в подсетях, их пропускная способность и состояние каналов.

Основные требования, которые предъявляются к маршрутизатору в проекте - это функциональность и скорость работы.

Требование скорости работы маршрутизатора важно, так как к нему будет подключено одновременно несколько компьютеров.

Функциональность характеризуется набором поддерживаемых сетевых протоколов, протоколов маршрутизации, портов, наличие Wi-fi. Она достигается с помощью использования модульной конструкции, когда в одно шасси устанавливается несколько блоков с портами определенного типа.

Благодаря технологии Wi-Fi можно осуществляется выход с ноутбуков, КПК, сотовых телефонов и других устройств, оборудованных приемниками Wi-Fi в интернет без подключения сетевого кабеля.

После определения места установки сервера и рабочих станций можно сразу определить, какое количество кабеля потребуется.

Размещение сервера

На выбор места влияет несколько факторов:

- из-за высокого уровня шума сервер желательно установить отдельно от остальных рабочих станций;

- необходимо обеспечить постоянный доступ к серверу для технического обслуживания;

- по соображениям защиты информации требуется ограничить доступ к серверу.

Таким образом, было выбрано единственное, возможное место установки сервера, не требующее перестройки внутренних помещений. Сервер было решено установить в отдельном помещении, которое используется как архив, так как только это помещение удовлетворяет требованиям, то есть уровень шума в помещении архива минимален, помещение архива изолированно от других, следовательно, доступ к серверу будет ограничен (Приложение Г). В то же время в помещении архива более удобно проводить обслуживание сервера, так как при установке сервера в кабинете директора или зам. директора обслуживание будет затрудненно в связи с выполнением ими своих служебных обязанностей, а в кабинете отдела кадров доступ к серверу посторонних лиц не сильно затруднен. Размещение же сервера в других кабинетах не отвечает ни одному условию.

Практическое занятие №4.
Проектирование логической схемы сетевой инфраструктуры.
Цель: Спроектировать логическую схему сетевой инфраструктуры

Адресная схема должна быть разработана в соответствии с иерархическим принципом проектирования компьютерных сетей.

Рассматриваемая сеть имеет четыре уровня иерархии. Вся сеть разбивается на 3 филиала. В каждом филиале содержится 50 корпусов. В корпусах есть 10 подразделений, на каждое из которых выделяется подсеть. На нижнем уровне иерархии располагаются адреса хостов. На каждый уровень иерархии выделено количество бит, достаточное для адресации содержащихся на данном уровне элементов и учитывающее возможное расширение сети.

Для раздачи адресов внутри корпоративной сети использован частный диапазон 10.0.0.0/8, обладающий наибольшей емкостью (24 бита адресного пространства).

Таблица 1.1 - Распределение бит для адресации подсетей и соответствующие маски подсетей

Уровень	Количество	Мин. необх.	Отведенное	Маска

структурной единицы	элементов для нумерации	число бит для нумерации	число бит для нумерации	
Филиал	3	2	3	/11
Корпус	50	6	7	/18
Подразделение	10	4	6	/24
Хосты	200	8	8	
Итого			24	

Таблица 1.2 - Распределение бит IP-адреса

0 0 0 0 1 0 1 0	X X X	X X X X X	X X	X X X X X X	X X X X X X X X
Сеть	Филиал	Корпус	Подразделение		

Таблица 1.3 - Распределение IP-адресов по филиалам

Номер филиала	Двоичный код	Диапазон адресов	Адрес подсети	Маска
1	001	10.32.0.1 - 10.63.255.254	10.32.0.0/11	255.224.0.0
2	010	10.64.0.1 - 10.95.255.254	10.64.0.0/11	255.224.0.0
3	100	10.96.0.1 - 10.127.255.254	10.128.0.0/11	255.224.0.0

Таблица 1.4 - Распределение диапазонов IP-адресов по корпусам для 1-го филиала

№ кампуса	Двоичный код	Диапазон адресов	Адрес подсети кампуса	Маска
1	0000001	10.33.0.1 - 10.33.255.254	10.33.0.0/18	255.255.192.0
2	0000010	10.34.0.1 - 10.34.255.254	10.34.0.0/18	255.255.192.0
3	0000011	10.35.0.1 - 10.35.255.254	10.35.0.0/18	255.255.192.0
4	0000100	10.36.0.1 - 10.36.255.254	10.36.0.0/18	255.255.192.0
5	0000101	10.37.0.1 - 10.37.255.254	10.37.0.0/18	255.255.192.0
…	…	…	…	…
50	0110010	10.82.0.1 -	10.82.0.0/18	255.255.192.0

		10.82.255.254		

Для остальных филиалов адреса корпусов подсчитываются аналогично.

От подсетей корпусов перейдем на более низкий уровень, то есть к подсетям подразделений, в качестве примера рассмотрим подсети подразделений первого корпуса первого филиала.

Таблица 1.5 - Распределение диапазонов IP-адресов по подразделениям для 1-го корпуса 1-го филиала.

№ подразделения	Двоичный код	Диапазон адресов	Адрес подсети подразделения	Маска
1	000001	10.33.1.1 - 10.33.1.254	10.33.1.0/24	255.255.255.0
2	000010	10.33.2.1 - 10.33.2.254	10.33.2.0/24	255.255.255.0
…	…	…	…	…
10	001010	10.33.10.1 - 10.33.10.254	10.33.10.0/24	255.255.255.0

Сети, не вписывающиеся в иерархическую схему адресации, называют "служебными".

Задание:

1.Разработать логическую схему сети и рассчитать IP –адреса.

Практическое занятие №5

Проектирование физической схемы сетевой инфраструктуры.

Цель: Спроектировать физическую схему сетевой инфраструктуры.

Физическая схема локальной сети должна содержать коммутирующее оборудование, физические линии связи между ними, а также компьютеры, как конечные узлы сети.

Самым простым коммутирующим оборудованием уровня доступа являются коммутаторы рабочих групп, к которым присоединяются

автоматизированные рабочие места сотрудников организации (АРМы). В нашей сети из-за большого количества АРМов коммутаторы уровня рабочих групп разделены на два уровня. Коммутаторы рабочих групп верхнего (второго) уровня объединяются в единую сеть с помощью коммутаторов зданий, которые в рамках одного корпуса соединяются в кольцо оптоволоконными линиями связи. В каждом корпусе содержится по три здания, а, следовательно, и коммутаторов зданий в них тоже будет три. Через коммутатор корпуса сеть соединена с маршрутизатором корпуса и серверами корпуса.

Задание:

1.Спроектировать физическую схему сетевой инфрасткурты в MS Visio

Практическое занятие №6.

Составление технического задания.

Цель: Составить техническое задание.

Техническое задание нужно для того, чтобы заказчик точно узнал чего он хочет, а исполнитель понял, что ему нужно для этого делать .Если в техническом задании вы напишете примерный перечень действий и фразу "хочу, чтобы все работало хорошо!", все будет работать хорошо, но так, как решит программист. Идеальное техническое задание - какое оно?

Во-первых, в техническом задании должны быть четко прописаны общие положения. Это нужно для того, чтобы исполнитель понимал, что он делает. В общих положениях могут быть прописаны характеристики оборудования, на котором должна выполняться работа, разъяснения спорных моментов, глоссарий и т.п.

Второй пункт - это четко сформулированные цели, которых нужно достичь в процессе работы. Написание этого раздела поможет заказчику понять, чего он действительно хочет, а исполнителю - впоследствии предложить решения описанных проблем.

Третий пункт - это требования, которые заказчик предъявляет к выполнению задания. Без этого пункта не обходится ни одно техническое задание. В нем должно быть четко прописано, что именно, и в какой срок хочет получить заказчик. Не нужно думать, что опуская сроки выполнения задания вы даете "свободу" исполнителю. Работать в условиях неизвестности очень сложно. Техническое задание не должно быть слишком расплывчатым - ведь исполнитель может понять его неверно или не так, как требуется заказчику.

В то же время, техническое задание не должно быть слишком подробным - в любом проекте должно быть место творчеству

Практическое занятие №7

Планирование адресного пространства.

Цель: Спланировать адресное пространство.

Ip-адрес - это 32х битное двоичное значение, которое обычно выражается в виде 4-х 8-ми битных десятичных чисел, разделенных точками. Это называется десятичным представлением.

Каждое из 4-ч 8-ми битных чисел называется октетом

Компоненты Ip-адреса.

Ip-адрес идентифицирует конкретное устройство - хост. Так же Ip-адрес идентифицирует сеть, в котором находится данное устройство. Это возможно т.к. Ip-адрес состоит из 2-х частей: идентификатора сети и идентификатора хоста.

Идентификатор сети стоит перед идентификатором хоста, но «линии раздела» могут находится между любыми битами 32-х битного пространства.

Именно такая 2-х уровневая организация характерна для Интернета. Каждый Пк в Интернете должен иметь уникальный Ip-адрес.

Разделение адресов на сети и хосты позволяет осуществить Ip - маршрутизацию. Маршрутизатор не должен знать где находится конкретный хост, он должен знать где находится нужная сеть.

Сетевая маска - это 32-х битное двоичное значение. Определяет сколько бит Ip-адрес относится к Ip-сети, а сколько к Ip-хоста. 1 к сети, 0 к хосту.

Классы адресов:

A,B,C - основные

D,E - дополнительные

D - адреса для групповой рассылки, идентифицирует какую-либо группу ПК по общему признаку

E - экспериментальный, пока не используется

Существует 2 типа адресов:

-) зарегистрированные (общие)

-могут использоваться в интернете

- регулируются организацией IANA

-) не регистрированные (частные)

- могут использоваться только в частных сетях

-могут использоваться в совместимых схемах нумерации

Ip- адрес используется для идентификации ПК в сети. Каждый пакет передаваемый в сети Ip содержит адрес получателя. Маршрутизатор использует этот адрес для пересылки пакета в точку назначения. Для правильного функционирования Ip-адреса должны быть уникальны. В частных сетях за уникальность Ip отвечает администратор.

Сеть Интернет много больше и процессом распределения ID управляет IANA - официальный регистратор сетевых адресов.

IANA - выделяет большие куски ID адресного пространства региональным, национальным регистратором, которые в свою очередь выделяют конкретные сети ISD - провайдер услуг Интернет.

Использование зарегистрированных адресов: используются только для ПК, которые должны быть доступны в Интернете. Защита ПК с общими адресами - очень важный процесс для администратора. Если в сети есть ПК с открытыми и частными Ip, то рекомендуется выделить ПК с открытым Ip в отдельный сегмент сети - демилитаризованная зона.

Использование не зарегистрированных адресов: для работы внутри сети рекомендуется использовать частные Ip адреса, которые не регистрируются в IANA => невидимы доя Интернета, их нельзя атаковать => они более защищены, но подвержены другим видам атак.

Планирование IP адресации:

1. Определить тип доступа к сети Интернет - если пользователь является только клиентом интернета, то используются частные адреса в сочетании с технологиями NAT и PROXY

2. Определить количество сегментов в сети и способов их соединения. Если сеть состоит из нескольких сегментов , то для каждого сегмента нужно использовать различные подсети. Если сегмент соединяется коммутаторами, то мы получаем одну большую подсеть с большим количеством хостов

=>нужно правильно подобрать класс ID, который будет использоваться для сети.

Получение сетевых адресов: сетевые адреса можно получить у вашего ISD - провайдер услуг Интернет.

Если ПК надо взаимодействовать между собой, то потребуется выделение подсети. Если вам нужно вывести в Интернет много устройств, то тогда потребуется отдельная сеть.

Разбитие IP адресов на подсети:

Определив типы Ip адресов, число сегментов и способы их соединения можно приступать к расчету Ip адресного пространства.

Разбитие на подсети - процесс создания адресов отдельных сетей из адреса большой сети. Позволяет более рационально использовать адресное пространство, например класса A=16 млн. хостов.

Задание: Рассчитать ip- адреса для заданной сети.

Практическое занятие №8.

Установка серверной операционной системы.

Цель: Установить Windows Server 2008

Перед началом установки нужно выполнить подготовительную работу. Вот основные пункты:
1) Определитесь с редакцией операционной системы (standard, enterprise, datacenter и т.д.);
2) Проверьте, соответствует ли ваш сервер минимальным системным требованиям выбранной редакции операционной системы;
3) Подготовьте носитель с файлами для установки (в нашем случае USB-флэшка).

Если вы планируете использовать данный сервер для хранения или обработки данных, лучше установить дополнительный жесткий диск для операционной системы. Также желательно убедиться в правильной организации работы сервера и инфраструктуры.
Желательно после установки операционной системы Windows Server установить драйвера.

Подготовка окончена. Можно приступать к установке. В среднем по времени она займет примерно 15-20 минут, всё зависит от производительности вашего сервера.

Ниже описаны ключевые этапы:
1) Вставляем флэшку в рабочий USB разъём сервера;
2) Включаем сервер;
3) Путем нажатия кнопки F2 или DEL (зависит от модели материнской платы) попадаем в БИОС и выбираем загрузку с нашей флэшки. Сохраняем изменения и перезагружаемся.

Содержание

Далее запустится процесс установки и мы будем работать с довольно простыми диалоговыми окнами

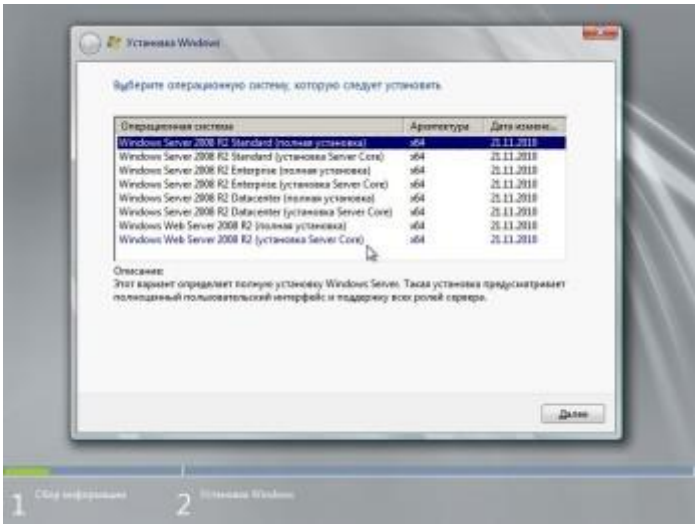
1. Первоначально нам предложено выбрать языковые настройки и параметры местоположения:

Выбираем необходимые настройки и нажимаем кнопку ДАЛЕЕ.

2. В следующем диалоговом окне нам предлагается на выбор несколько пунктов, но нас на данный момент интересует только установка:

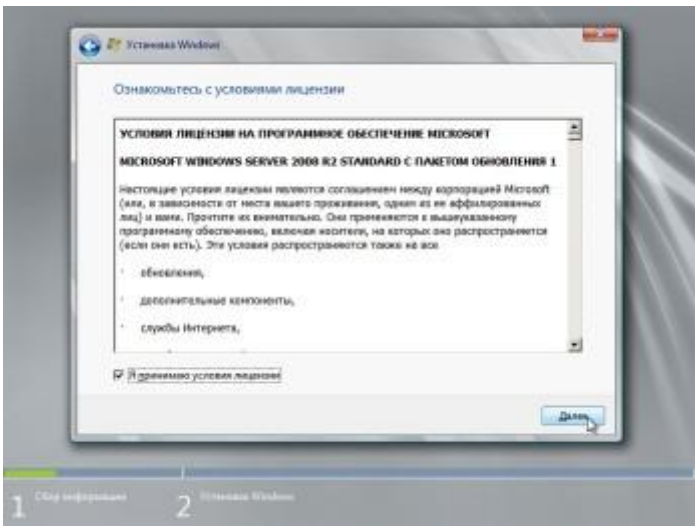
Нажимаем кнопку УСТАНОВИТЬ.

С редакцией операционной системы мы определились ранее:



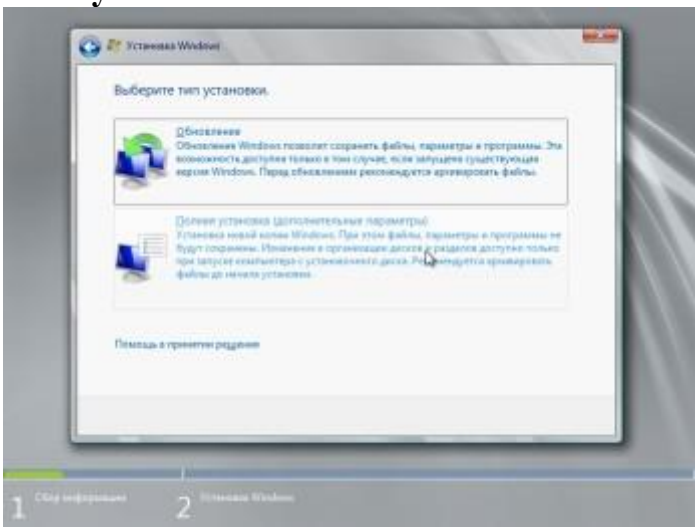
Выбираем необходимую и нажимаем кнопку ДАЛЕЕ.

3. Окно с условиями лицензионного соглашения:



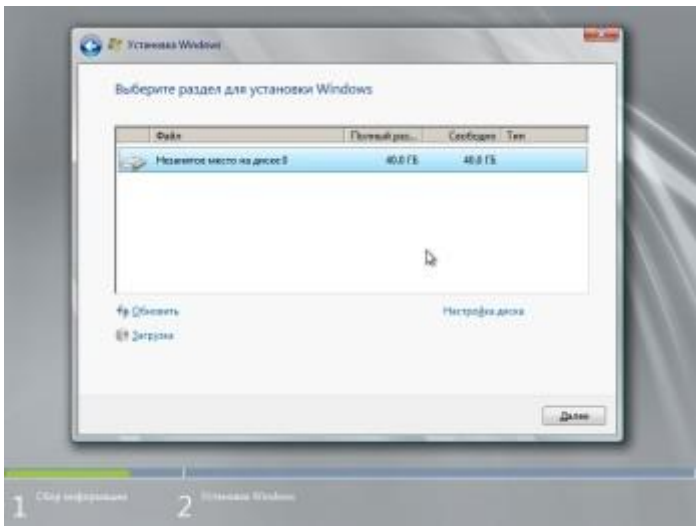
Ставим галочку «Я принимаю условия лицензии» и нажимаем кнопку ДАЛЕЕ.

4. Тип установки:

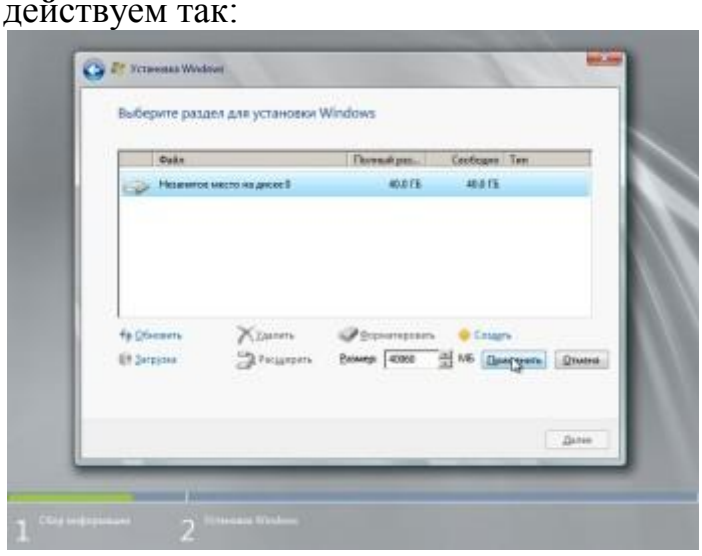


Нажимаем «Полная установка».

5. Выбор раздела для установки:

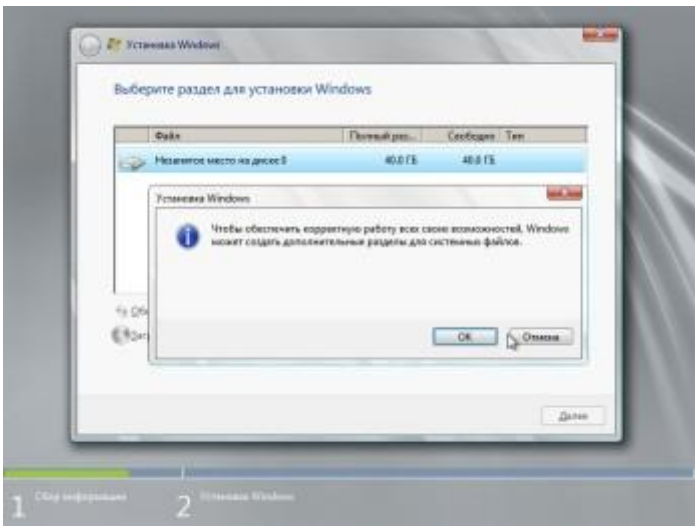


На этом пункте остановимся поподробнее.
Возможно, появится ошибка типа: «невозможно определить жесткий диск» и предложит отменить установку либо выбрать дополнительный драйвер. Вставляем флэшку либо диск нажимаем кнопку ЗАГРУЗКА и выбираем нужный драйвер. Обычно просит данный драйвер при установке на динамический жесткий диск.
В случае, если производим установку на отдельный жесткий диск, действуем так:



Выделяем строку «Незанятое место на диске», нажимаем кнопку СОЗДАТЬ, далее кнопку ПРИМЕНИТЬ.

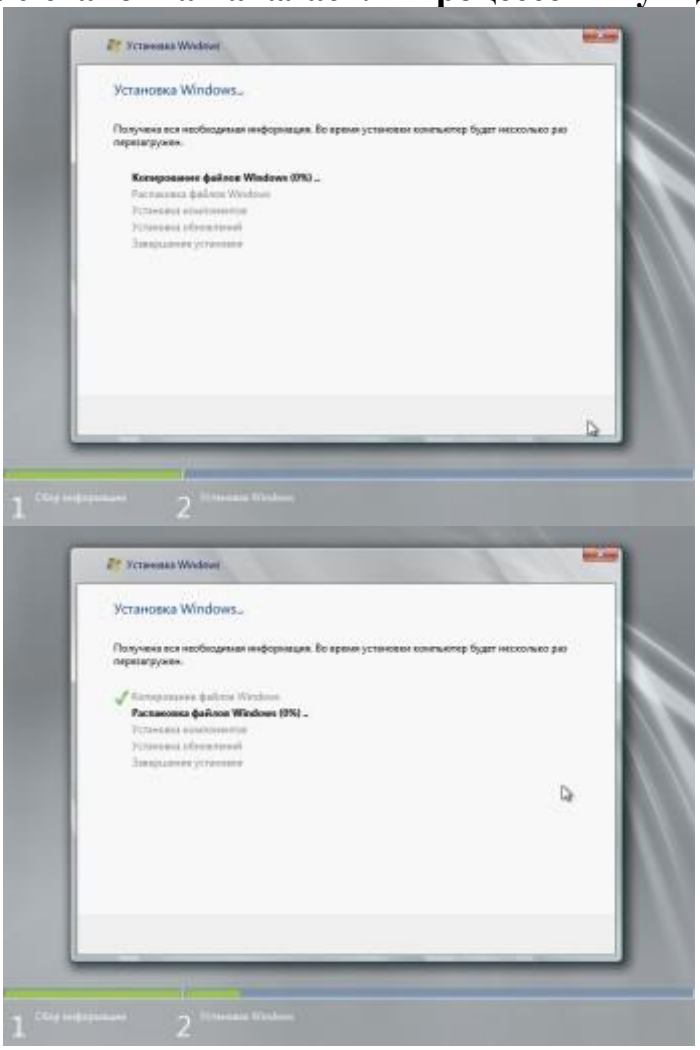
Появляется следующее окно:

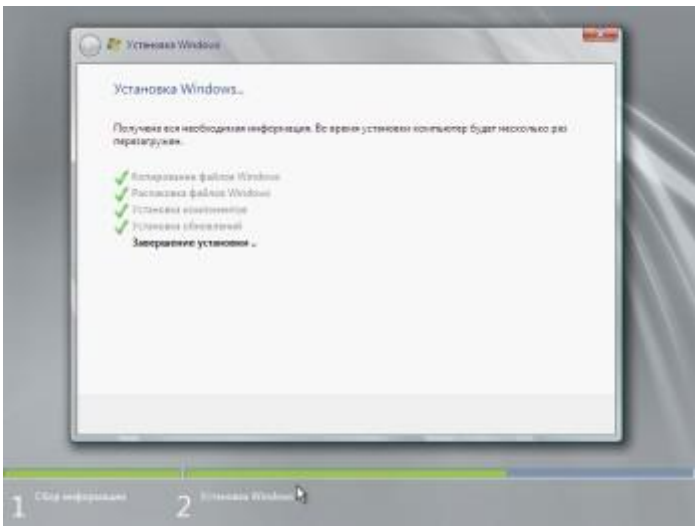


Нажимаем кнопку ОК, далее кнопку ДАЛЕЕ.

Всегда удаляйте старые системные разделы и создавайте новые, чтобы избежать дальнейших проблем.

6. Установка началась. В процессе мы увидим следующие окна:

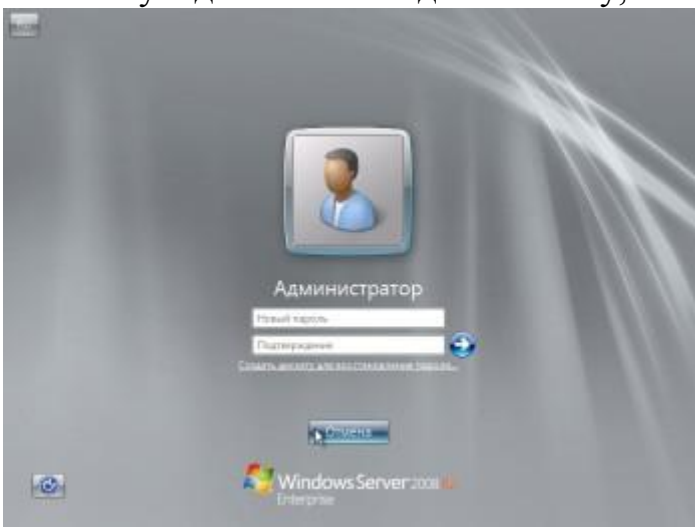




7. Во время установки компьютер перезагрузится

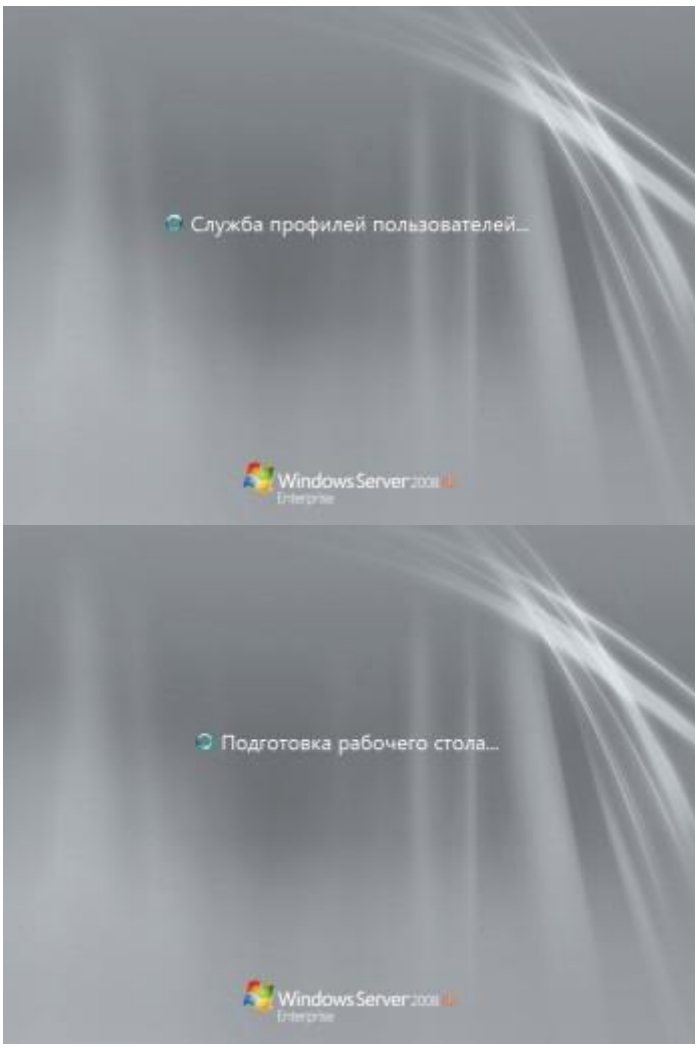
Если в настройках загрузки компьютера по умолчанию вы выбирали флэшку, то теперь нам нужно выбрать жесткий диск, на который мы производим установку. В противном случае мы опять вернемся к первоначальному этапу.

Если вы увидели окно входа в систему, то всё прошло удачно:



Вводим пароль и его подтверждение и нажимаем кнопку «Стрелка вправо». Пароль должен содержать буквы разного регистра, цифры и быть длинной не менее восьми символов. Запишите пароль, чтобы не забыть, он понадобится после каждой перезагрузки системы.

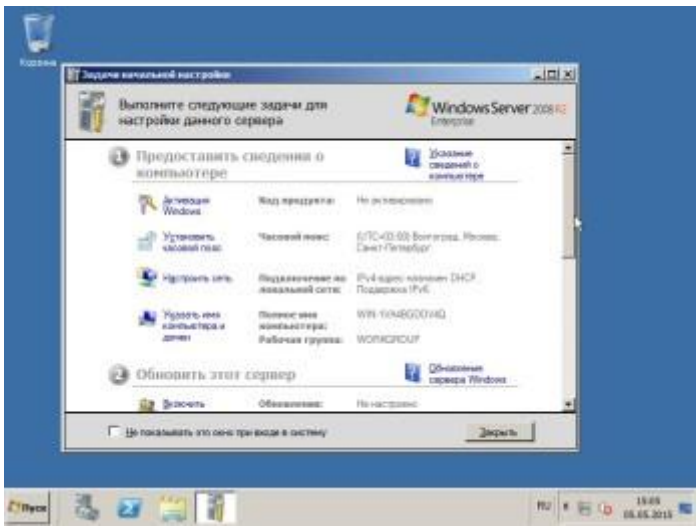
8. Дожидаемся применения параметров:



В части установки операционной системы мы закончили.

9. Теперь требуется минимальная первоначальная настройка

Устанавливаем драйвера и перезагружаемся. После перезагрузки появится окно первоначальной настройки:

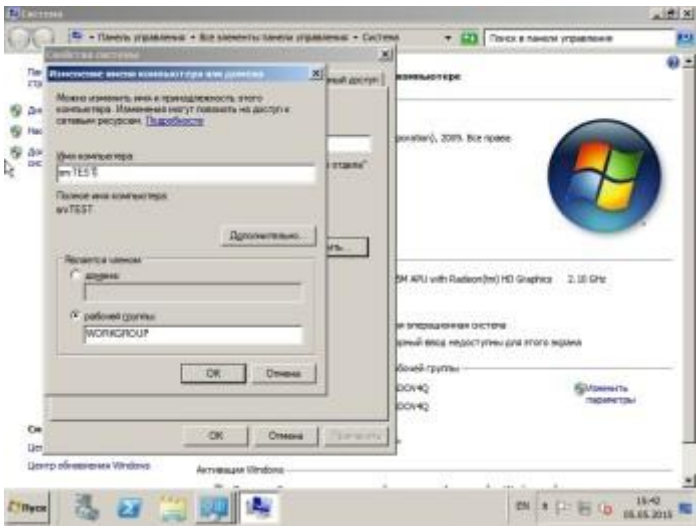


Здесь приведены основные пункты первоначальной настройки:

a) Нам нужно активировать систему. Существует много способов это сделать. Про это читайте отдельно.

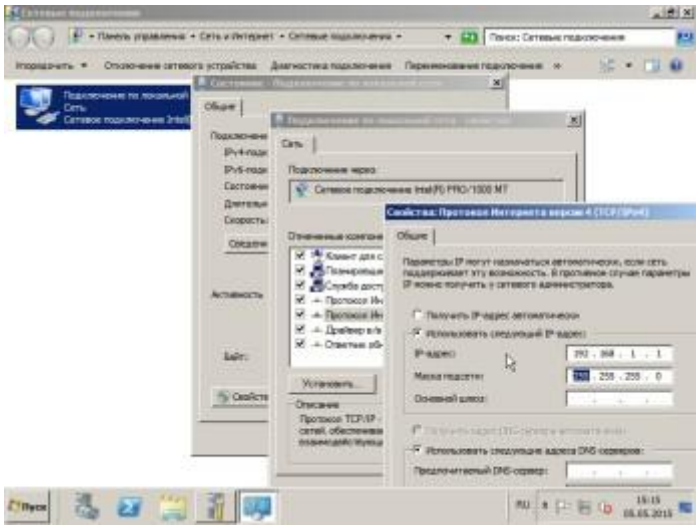
b) Установите нужный часовой пояс.

c) Поменяйте имя сервера на нужное (пример srvTEST).

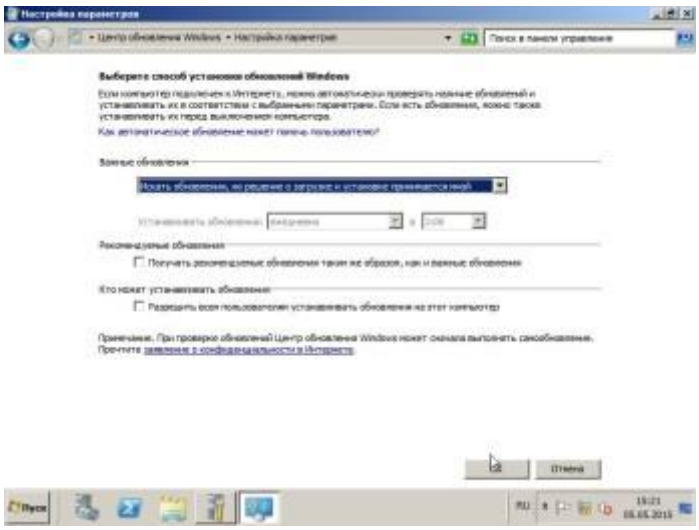


Перезагрузку можно произвести после всех остальных настроек.

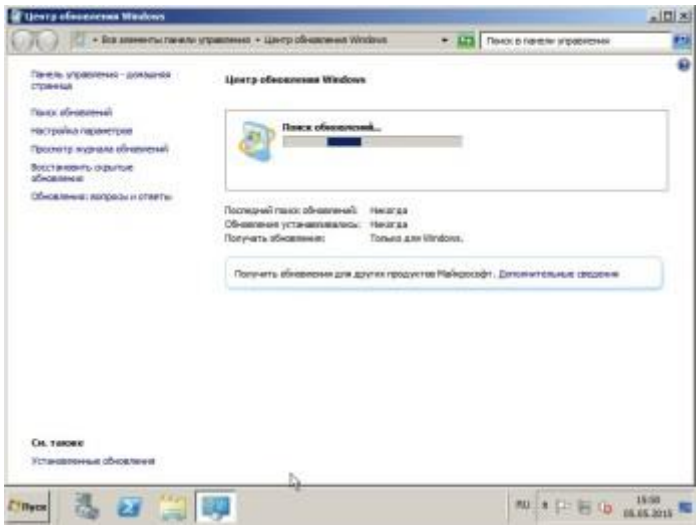
d) В настройках сети пропишите IP-адрес и маску подсети (пример 192.168.1.1, 255.255.255.0).



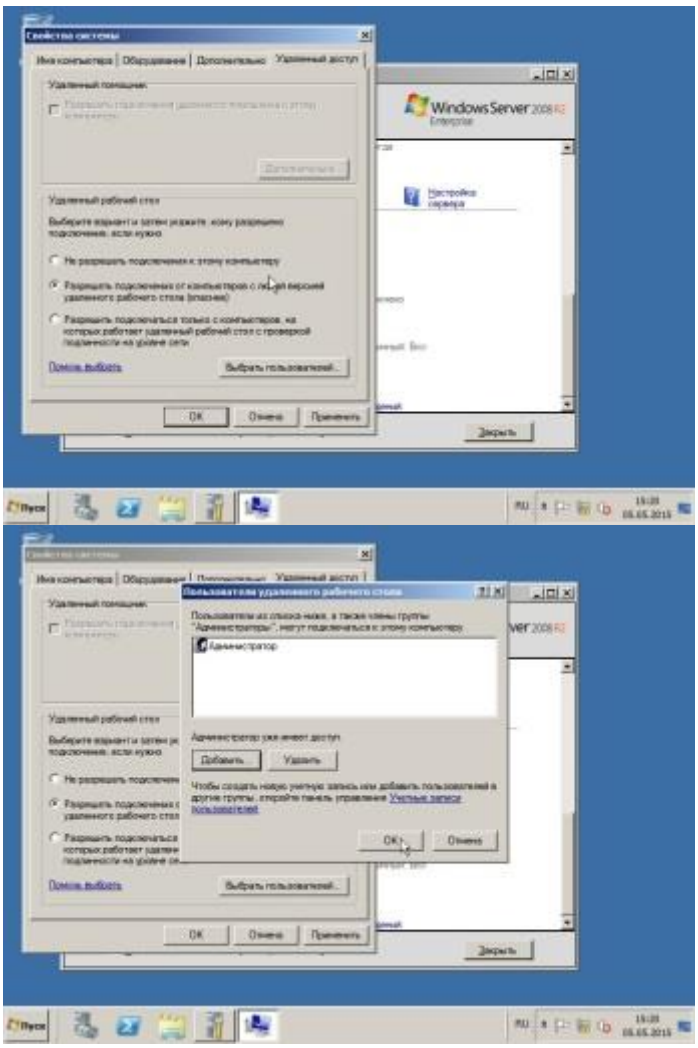
e) Установите необходимые обновления из центра обновления Windows:



В способе установки обновлений выберите пункт: «Искать обновления, но решение о загрузке и установке принимается мной».



f) Для удобства дальнейшего администрирования настраиваем службу удаленных рабочих столов



g) Добавьте пользователя для подключения.

10. Первоначальная настройка операционной системы завершена

Практическое занятие № 9.

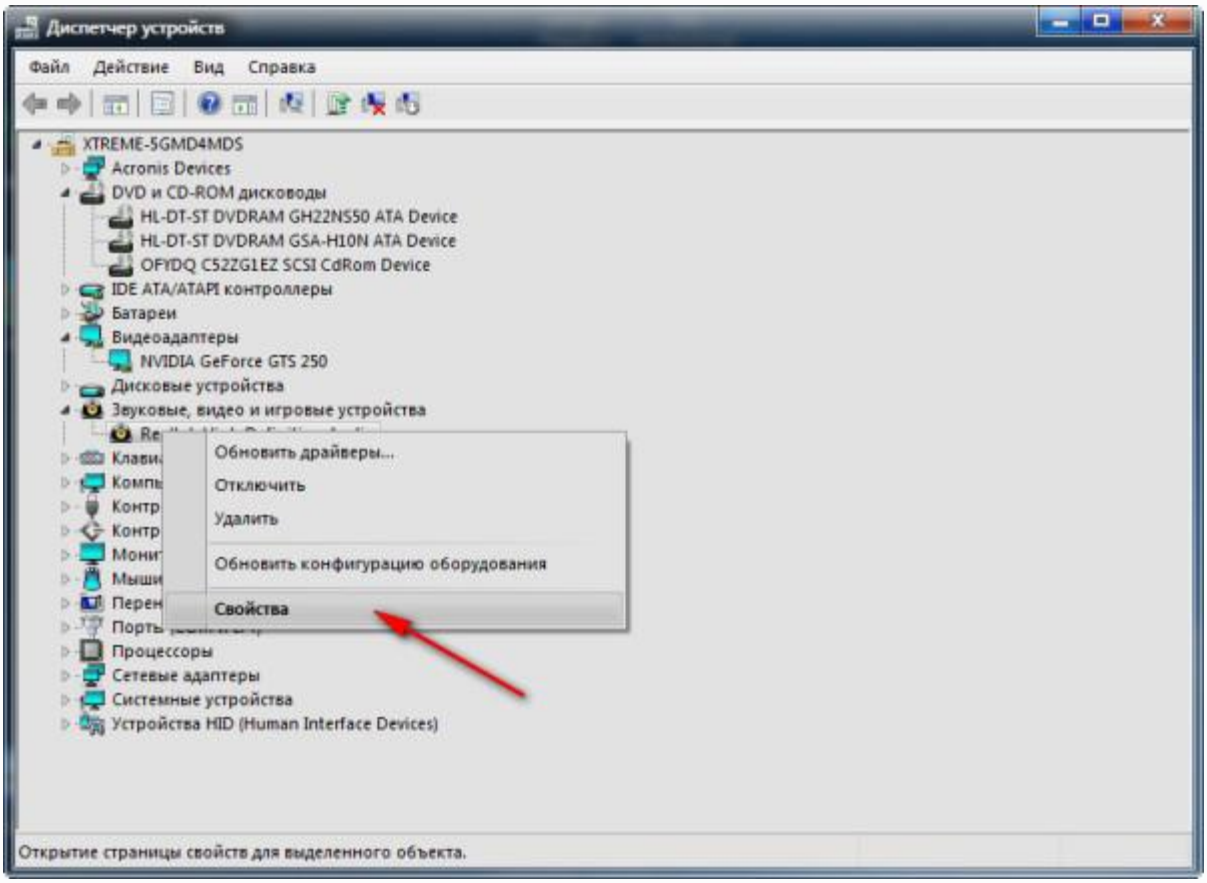
Установка драйверов, исправлений и обновлений.

Цель: Научится устанавливать драйвера и обновления.

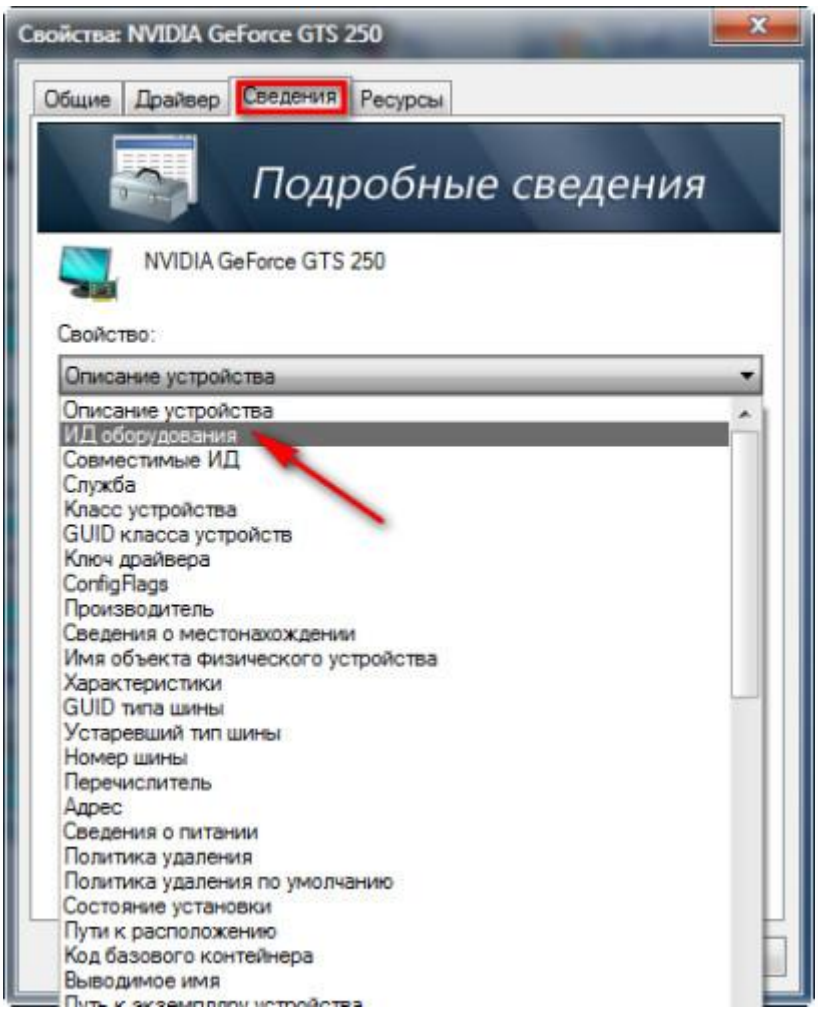
Ручная установка драйверов

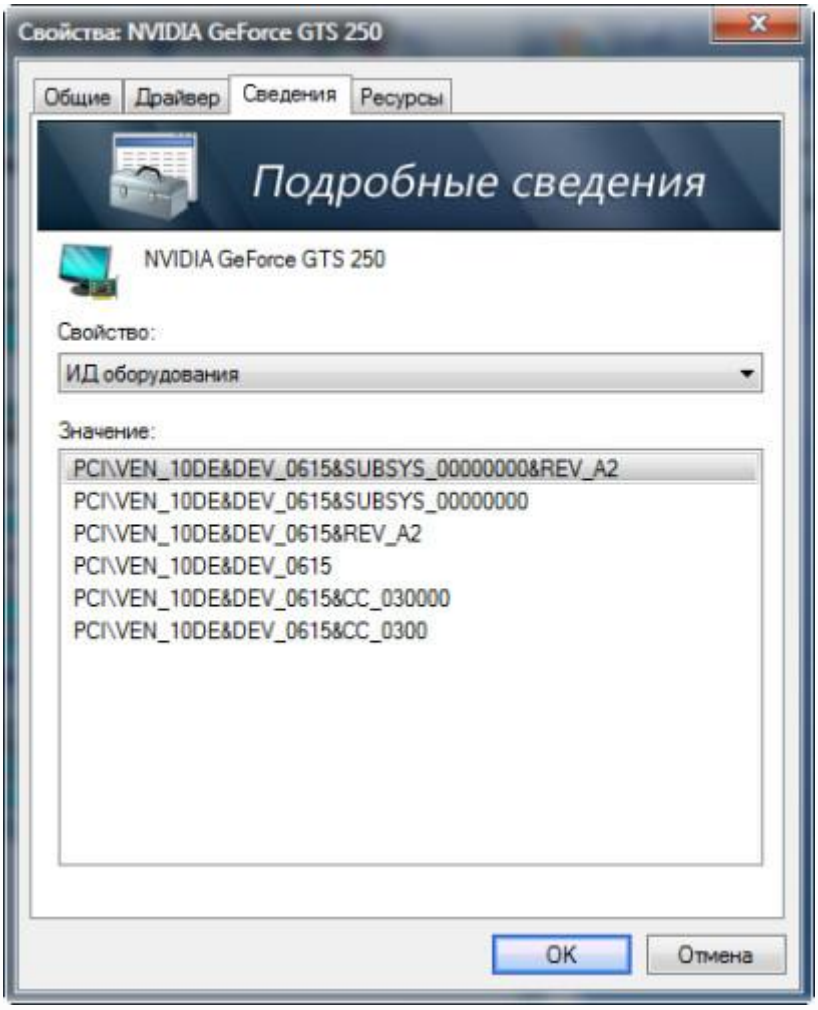
Вся процедура начинается с поиска устройства, для которого необходим драйвер. Например, пусть это будет видеокарта.

• Необходимо зайти в «Диспетчер устройств» и нажать на «Видеоадаптеры».
• Выбрать устройство и щелкнуть по нему правой кнопкой мыши с последующим выбором «Свойства».



• Откроется окно. Здесь нужно перейти на вкладку «Сведения». В меню «Свойство» нужно выбрать «ИД оборудования».


Свойства: NVIDIA GeForce GTS 250
Общие
Драйвер
Сведения
Ресурсы
Подробные сведения
NVIDIA GeForce GTS 250
Свойство:
Описание устройства
Описание устройства
ИД оборудования
Совместимые ИД
Служба
Класс устройства
GUID класса устройств
Ключ драйвера
ConfigFlags
Производитель
Сведения о местонахождении
Имя объекта физического устройства
Характеристики
GUID типа шины
Устаревший тип шины
Номер шины
Перечислитель
Адрес
Сведения о питании
Политика удаления
Политика удаления по умолчанию
Состояние установки
Пути к расположению
Код базового контейнера
Выводимое имя

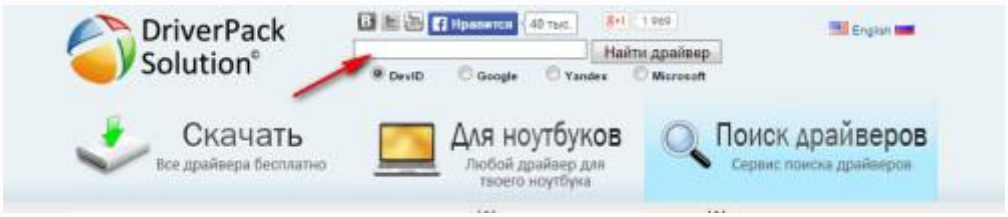


Все, что находится до символа «&» является названием оборудования. По нему осуществляется поиск драйвера.

Для этого используются два основных сайта:

1. http://devid.drp.su;
2. http://devid.info/ru.

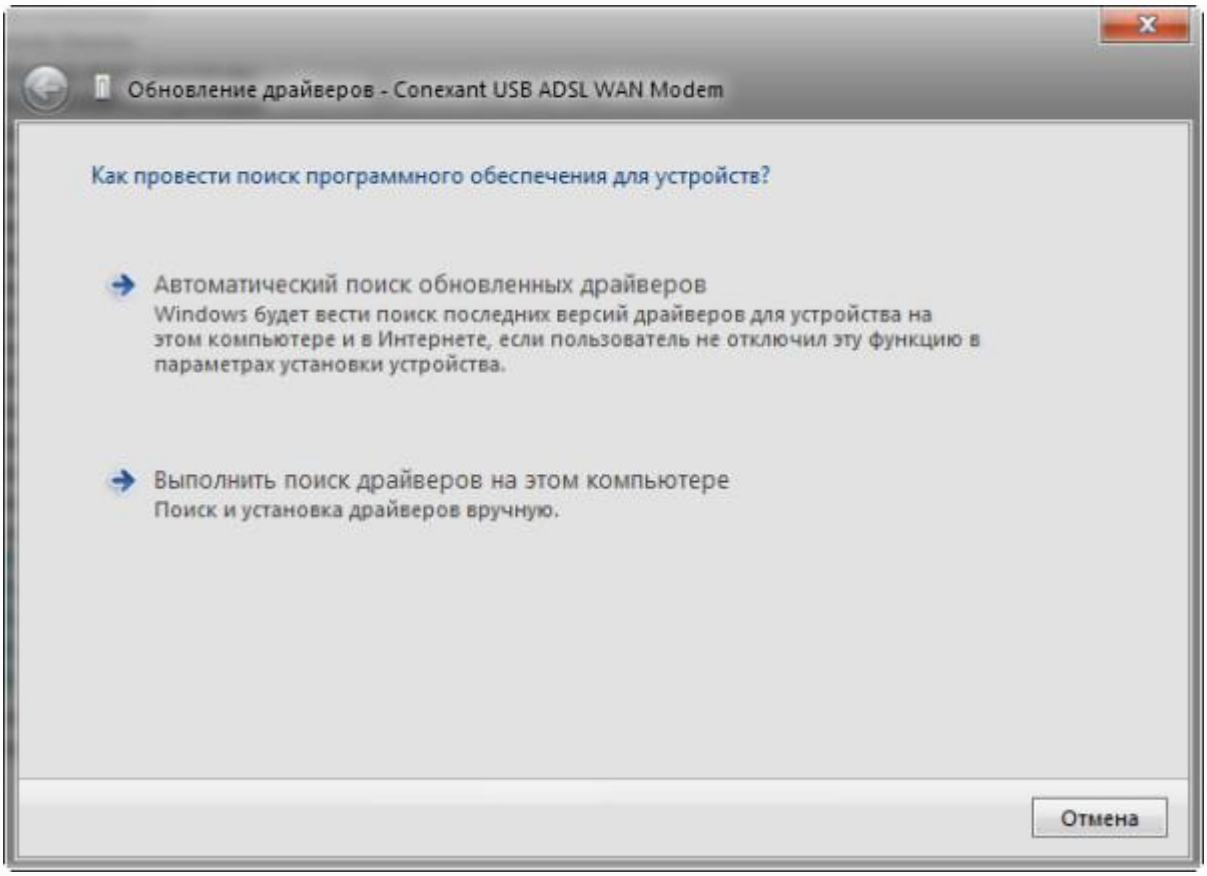
Для первого сайта ИД оборудования вводится в следующее поле:



Для второго сайта ИД оборудования вводится в следующее окно:

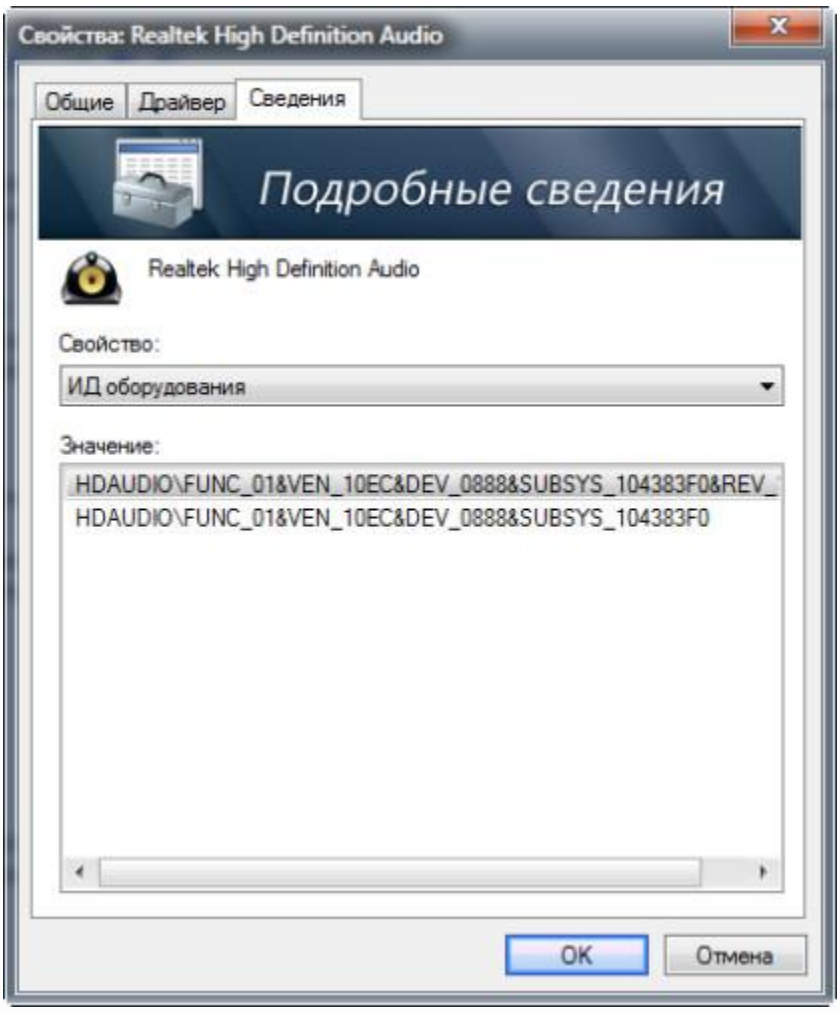
После нахождения драйверов необходимо их скачать и установить. Если это exe-файлы, то они инсталлируются как обычная программа. Если файл имеет

другое расширение, например, *.ini, то установку драйверов нужно выполнять из «Диспетчера устройств».



Здесь выбирается 2-ой пункт «Выполнить поиск драйверов на этом компьютере». Далее указывается место, где сохранен файл *.ini.

Бывает так, что ИД отображен непонятно.



Здесь нет привычных слов PCI\VEN. Как же искать драйвера? Чтобы поиск дал результаты, убираются все символы в запросе до слова VEN, и удаляются все символы, начиная с «&».

Остается только «VEN_10EC&DEV_0888». Эту фразу вводят на сайтах, где ищут драйвера.

Обновление драйверов, используя стандартные средства операционной

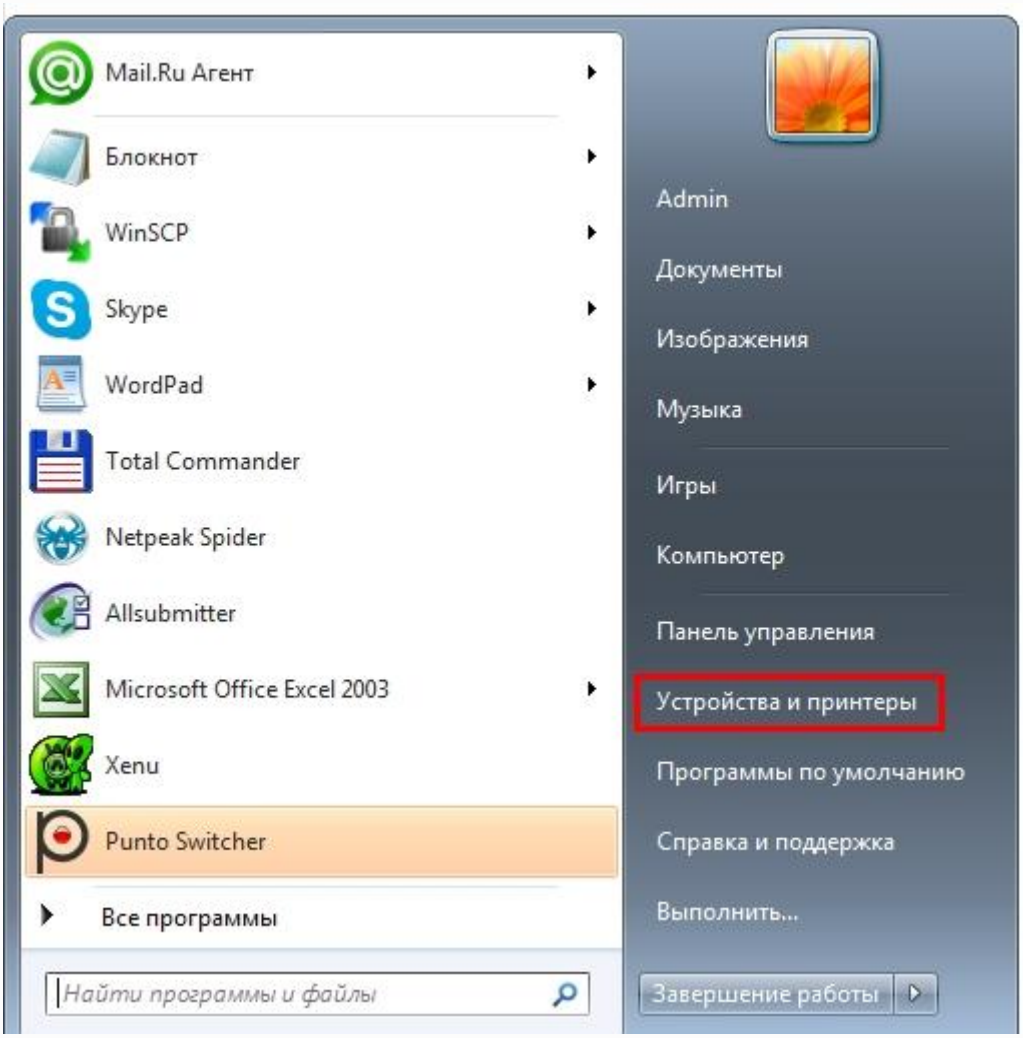
системы

При покупке компьютера с ним вместе идет диск с драйверами. Он понадобится в конце установки Windows. Но они, скорее всего, будут устаревшими, хотя компьютер с ними будет работать. Нужно регулярно обновлять драйвера. Такой процесс осуществляется несколькими способами.

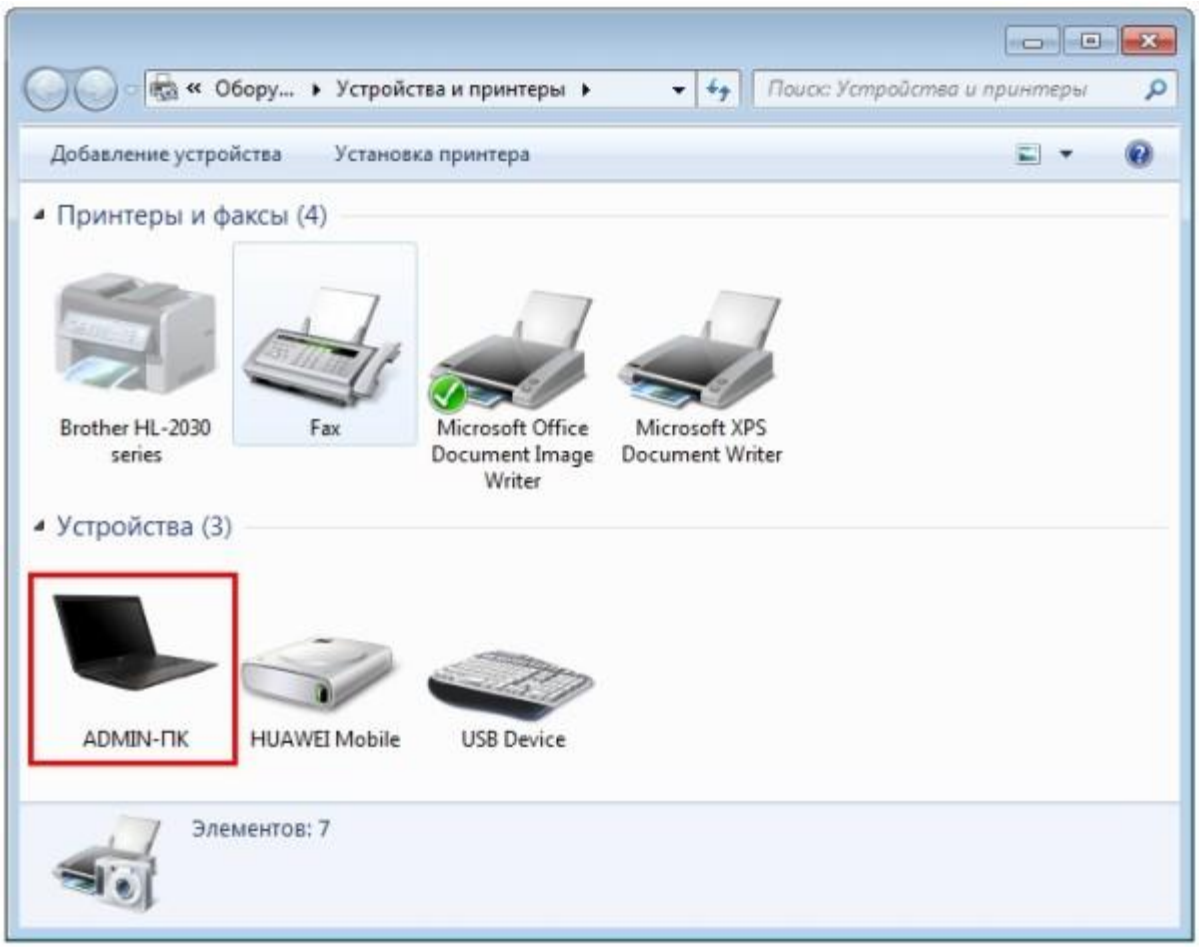
В самой ОС Windows 7 имеется возможность обновления драйверов без стороннего ПО.

Способ №1

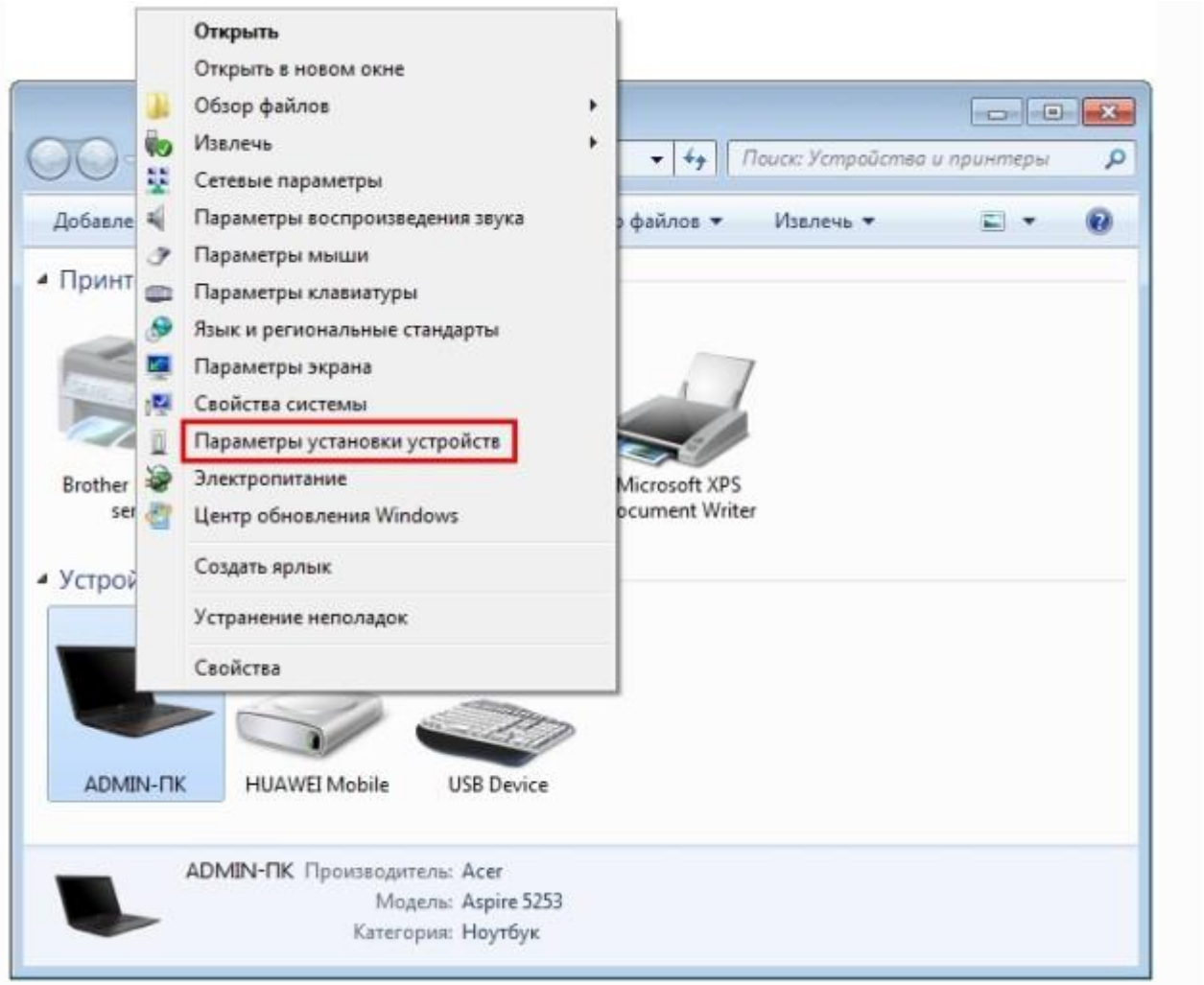
Нужно открыть меню «Пуск», а затем выбрать в нем «Устройства и принтеры».



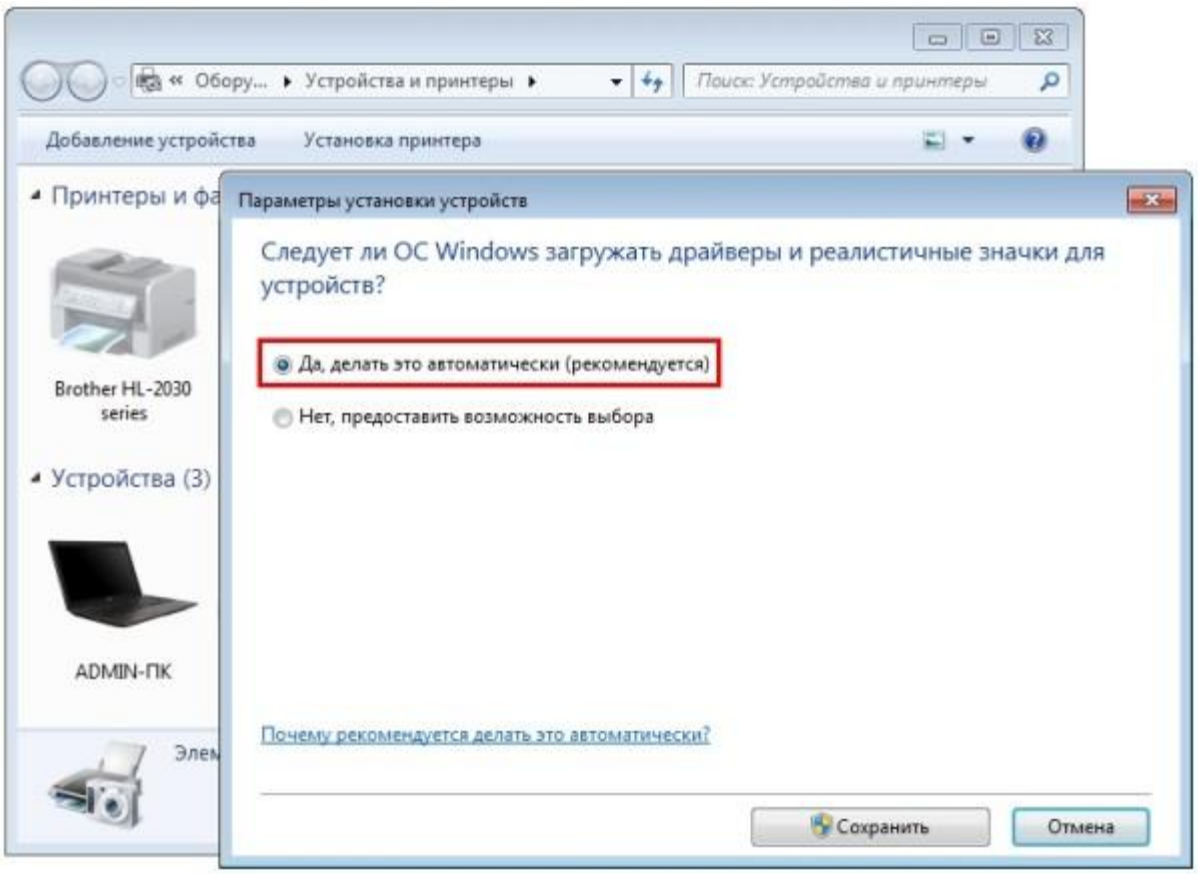
Откроется окно, с различными устройствами. Нужно найти пиктограмму, напоминающую своим видом компьютер, системный блок или жесткий диск. Эта иконка будет иметь имя компьютера.



Нажав правой кнопкой мыши по значку, откроется меню. Здесь выбирается пункт «Параметры установки устройств».



Следуем указаниям на скриншоте. После этого сохраняем все изменения кнопкой «Сохранить».



Теперь ОС сама будет искать обновленные или неустановленные драйвера на компьютер.

Задание:

1.Установить драйвера.

Практическое занятие №10

Установка и привязка сетевых протоколов. Настройка протоколов.

Цель: Установить сетевые протоколы.

Используйте «Задачи начальной настройки» для настройки параметров сети.

1. Щелкните Настроить сети.

2. В окне Сетевые подключения правой кнопкой мыши щелкните значок Подключение по локальной сети и выберите пункт Свойства.

3. Щелкните Протокол Интернета версии 4 (TCP/IPv4) и нажмите кнопку Свойства. В окне свойств протокола Интернета версии 4 (TCP/IPv4) выберите Использовать следующий IP-адрес.

4. Введите следующие значения: • IP-адрес: 192.168.0.1 • Маска подсети: 255.255.255.0 8 • Основной шлюз: 192.168.0.100

5. Должен быть выбран вариант Использовать следующие адреса DNS-серверов. Введите следующие значения: • Предпочитаемый DNS-сервер: 192.168.0.1 • Альтернативный DNS-сервер: 127.0.0.1

6. В окне свойств протокола Интернета версии 4 (TCP/IPv4) нажмите кнопку ОК.

7. В диалоговом окне свойств подключения по локальной сети нажмите кнопку ОК.

8. Закройте окно «Сетевые подключения».

Практическое занятие №11.

Установка службы каталога. Начальное администрирование службы каталога. Создание структуры подразделений.

Цель: Установить службу каталога.

Установка роли доменной службы Acvtive Directory в Microsoft Server 2008 R2

1. Открываем Диспетчер сервера и заходим во вкладку Роли:

Нажимаем «Добавить роли».

2. Откроется Мастер добавления ролей:

Здесь размещается краткая справочная информация: рекомендуется использовать надежный пароль Администратора, установить последние обновления сервера и проверить корректность сетевых настроек. Чтобы в дальнейшем при вызове Мастера добавления ролей не отображалась данная страница необходимо активировать пункт «Пропустить данную страницу по умолчанию». Для продолжения нажимаем Далее.

3. Окно Выбор ролей сервера:

Выбираем пункт Доменные службы Active Directoryи нажимаем Далее.

Если нажать на ссылку «Дополнительные сведения о ролях сервера», то откроется встроенная справочная система:

Здесь доступны описания служб сервера Microsoft Server 2008 R2.

4. В этом окне можно ознакомиться с основной информацией об Active Directory:

Также здесь сообщается, что Active Directory требует установленного DNS-сервера, который в случае отсутствия будет установлен. Внизу под надписью «Дополнительные сведения» доступны 3 ссылки на встроенную справочную систему: Обзор AD DS, Установка доменных служб Active Directory и Общие конфигурации доменных служб Active Directory. Для перехода к следующему этапу нажимаем Далее.

5. Подтверждение установки роли Active Directory:

Компания Microsoft еще раз напоминает о необходимости после установки роли Active Directory запустить утилиту dcpromo.exe, чтобы назначить данный сервер контроллером домена. Нажимаем «Установить».

6. Ход выполнения установки:

Происходит установка роли доменных служб Active Directory. Данный процесс занимает несколько минут.

7. Если установка ролей Active Directory завершится успешно, то вы увидите следующее окно:

Для выхода из Мастера добавления ролей нажмите кнопку «Закрыть». Чтобы назначить данный сервер контроллером домена необходимо запустить утилиту dcpromo.exe или нажать ссылку «Закройте этот мастер и запустите установки доменных служб Active Directory (dcpromo.exe)».

8. После закрытия Мастера добавления ролей можно зайти в Диспетчер сервера, открыть вкладку Роли и убедиться, что роль доменной службы Active Directory установлена успешно:

Если нажать на надпись «Доменные службы Active Directory» (обведена красным прямоугольником), то откроется новое окно, где сообщается о том, что данный сервер не работает в качестве контроллера домена:

Чтобы сделать данный сервер контроллером домена необходимо запустить утилиту dcpromo.exe или нажать ссылку «Запустить мастер установки доменных служб Active Directory (dcpromo.exe)».

Установка доменной службы Active Directory в Microsoft Server 2008 R2

1. Запускаем Мастер установки доменных служб Active Directory:

В этом стартовом окне можно активировать пункт «Использовать

расширенный режим установки». Прочитать справочную информацию о нем можно пройдя по ссылке «Подробнее о дополнительных параметрах, доступных в расширенном режиме установки». Мы не будем использовать расширенный режим, т. к. при установке первого (корневого) контроллера домена можно обойтись «обычным» режимом. Если вы хотите прочитать встроенную справку о службах AD, то пройдите по ссылке «Подробности о доменных службах Active Directory». Для продолжения установки Active Directory выбираем Далее.

2. Информация о совместимости операционных систем:

Данное окно содержит информацию о совместимости операционных систем. Для продолжения нажимаем Далее.

3. Выбираем пункт «Создать новый домен в новом лесу» и нажимаем Далее:

Также вы можете почитать справочную информацию по ссылке «Подробности о возможных конфигурациях развертывания».

4. Указываем имя корневого домена леса:

В качестве тестового имени я выбрал «denis.local».

5. Начнется проверка уникальности имени нового леса:

Затем будет проверяться имя NetBIOS:

Оба процесса длятся считанные секунды.

6. Выбор режима работы леса:

Доступные значения: Windows 2000, Windows Server 2003 и Windows Server 2008. Для каждого режима работы отображается краткая справочная информация.

Пример работы леса в режиме Windows 2000:

Пример работы леса в режиме Windows 2003:

Пример работы леса в режиме Windows 2008:

Мы устанавливаем корневой контроллер домена, поэтому здесь наиболее предпочтительнее выбрать режим работы леса Windows 2008.

7. Проверка конфигурации DNS:

Будет запущена проверка конфигурации DNS, которая займет несколько секунд.

8. Дополнительные параметры контроллера домена:

Будет предложено установить DNS-сервер. Соглашаемся на установку и нажимаем Далее.

9. Назначение статического IP-адреса:

Если ваш сервер имеет динамический IP-адрес, то вы увидите данное окно. Для надежной работы DNS рекомендуется в свойствах сетевой карты назначить статический IP-адрес. Таким образом, если выбрать пункт «Да, компьютер будет использовать динамически назначаемый IP-адрес (не рекомендуется).», то процесс установки доменных служб Active Directory будет продолжен. Если выбрать «Нет, я назначу статические IP-адреса всем физическим сетевым адаптерам.», то перед продолжением установки доменных служб Active Directory вам необходимо будет прописать в свойствах всех сетевых карт данного сервера статические IP-адреса.

10. Делегирование для DNS-сервера:

Выбираем «Да».

11. Выбор расположения базы данных, файла журнала и SYSVOL:

Можно оставить значения по умолчанию или указать другие. Для продолжения нажимаем Далее.

12. Установка пароля администратора для режима восстановления служб каталогов:

Пароль администратора режима восстановления служб каталогов должен включать в себе как минимум 1 букву верхнего регистра, 1 букву нижнего регистра и 1 цифру. Таким образом, минимальная длина такого пароля составляет 3 символа. Но рекомендуется придумать более надежный пароль. Подробную информацию можно прочитать во встроенной справочной системе по ссылке «Подробности о пароле режима восстановления служб каталогов».

13. Сводка:

В данном окне можно посмотреть все выбранные на предыдущих этапах параметры Active Directory. Для продолжения нажмите Далее.

При необходимости прочитайте встроенную справочную систему по ссылке «Подробнее об использовании файла ответов». Допускается экспортировать все параметры в файл ответов, который можно использовать в будущем для быстрого развертывания контроллера домена. Для этого нажмите кнопку «Экспортировать параметры»:

Укажите имя файла, в который экспортируются все параметры. По умолчанию он будет сохранен а папку Администратор\Документы. Если вы хотите сохранить файл с параметрами в другом месте, то нажмите кнопку

«Обзор папок»:

Файл с автоматическими установками может быть сохранен в форматах TXT или INI.

При успешном экспорте вы увидите следующее окно с информацией об имени файла ответов и месте его сохранения:

Чтобы использовать файл ответов для установки службы Active Directory наберите в командной строке: dcpromo /answer[: имя_файла], где «имя_файла» - это имя файла ответов.

Содержимое файла ответов в моем случае выглядит следующим образом:

14. Настройка доменных служб Active Directory состоит из нескольких этапов и может занимать от нескольких минут до нескольких часов. Приведу несколько примеров.

Завершение установки DNS:

Проверка необходимости установки консоли управления групповыми политиками:

Установка консоли управления групповыми политиками:

На моем сервере данный процесс длился примерно 40 минут. По завершении установки доменных служб Active Directory для вступления изменений в силу требуется перезагрузка компьютера. Чтобы ПК перезагрузился автоматически, поставьте галочку «Перезагрузка по завершении».

Если все прошло без ошибок, то вы увидите окно об успешном завершении мастера установки доменных служб Active Directory:

Нажмите «Готово» для закрытия данного окна.

Если галочка «Перезагрузка по завершении» не была поставлена, то потребуется перезагрузить компьютер:

Для немедленной перезагрузки сервера нажмите «Перезагрузить сейчас».

15. После загрузки Windows Server 2008 открывает Диспетчер сервера и проверяем корректность установки доменной службы Active Directory и DNS-сервера:

Роли (Главное окно):

Роли (DNS-сервер):

Роли (Доменные службы Active Directory):

Задание: 1.Установить Active Directory

Практическое занятие №12.

Создание учетных записей компьютеров в домене. Управление учетными записями компьютеров в домене.

Цель: Создать учетные записи в домене.

1. Чтобы открыть оснастку "Active Directory - пользователи и компьютеры", нажмите кнопку **Пуск**, щелкните **Панель управления,** дважды щелкните **Администрирование**, а затем дважды щелкните **Active Directory - пользователи и компьютеры**.
   Чтобы открыть оснастку "Active Directory - пользователи и компьютеры" в , **dsa.msc**.
2. В дереве консоли щелкните правой кнопкой мыши **Компьютеры**.
   Расположение

   - Active Directory - пользователи и компьютеры*узел домена*\Компьютеры

   Или щелкните правой кнопкой мыши папку, в которую требуется добавить компьютер.
3. Выберите команду **Создать**, а затем щелкните **Компьютер**.
4. Введите имя компьютера.

Дополнительные рекомендации

- Для выполнения этой процедуры необходимо быть членом группы "Операторы учета", "Администраторы домена" или "Администраторы предприятия" в доменных службах Active Directory либо вам должны быть делегированы соответствующие полномочия. По соображениям безопасности для выполнения этой процедуры рекомендуется использовать команду **Запуск от имени.**

- По умолчанию члены группы "Операторы учета" могут создавать учетные записи компьютеров в контейнере **Компьютеры** и новых подразделениях.

- По умолчанию прошедшим проверку пользователям в домене назначается **право пользователя "Добавление рабочих станций в домен**, и они могут создавать в домене до 10 учетных записей компьютеров.

- Существует два дополнительных способа предоставления пользователю или группе разрешения на добавление компьютера в домен:
    - используйте объект групповой политики, чтобы предоставить разрешение **Добавление пользователя компьютера**;
    - предоставьте пользователю или группе разрешение **Создание объектов-компьютеров** в подразделении.
- Если компьютер, который использует данную учетную запись, работает под управлением какой-либо из предшествующих Windows 2000 операционных систем, установите флажок **Назначить учетной записи статус пред-Windows 2000 компьютера**.
- Задачу этой процедуры можно также выполнить, используя Модуль Active Directory для Windows PowerShell. Чтобы открыть Модуль Active Directory, нажмите кнопку **Пуск**, щелкните **Администрирование**, а затем щелкните **Модуль Active Directory для Windows PowerShell**.

  Чтобы открыть Модуль Active Directory в , откройте **Диспетчер серверов**, щелкните **Сервис**, а затем щелкните **Модуль Active Directory для Windows PowerShell**.

  Дополнительные сведения см. в статье "Создание учетной записи компьютера" (http://go.microsoft.com/fwlink/?LinkId=138384). Дополнительные сведения о Windows PowerShell см. в статье "Windows PowerShell" (http://go.microsoft.com/fwlink/?LinkID=102372).

Дополнительные материалы

- Управление компьютерами

Создание учетной записи компьютера с помощью командной строки

1. Чтобы открыть командную строку, нажмите кнопку **Пуск**, щелкните **Выполнить**, введите **cmd**, а затем нажмите кнопку **ОК**. Чтобы открыть командную строку в , **cmd**, а затем нажмите кнопку **ОК**.
2. Введите следующую команду и нажмите клавишу ВВОД.
3. dsadd computer <ComputerDN>

Параметр	**Описание**

<ComputerDN>	Задает различающееся имя добавляемого компьютера. Различающееся имя указывает местоположение каталога.

Для просмотра полного синтаксиса данной команды, а также сведений о вводе в командную строку информации учетной записи пользователя введите следующую команду, а затем нажмите клавишу ВВОД.
dsadd computer /?

Дополнительные рекомендации

- Для выполнения этой процедуры необходимо быть членом группы "Операторы учета", "Администраторы домена" или "Администраторы предприятия" в доменных службах Active Directory либо получить соответствующие полномочия путем делегирования. По соображениям безопасности для выполнения этой процедуры рекомендуется использовать команду **Запуск от имени.**
- По умолчанию члены группы "Операторы учета" могут создавать учетные записи компьютеров в контейнере **Компьютеры** и новых подразделениях.
- По умолчанию прошедшим проверку пользователям в домене назначается **право пользователя "Добавление рабочих станций в домен"**, и они могут создавать в домене до 10 учетных записей компьютеров.
- Существует два дополнительных способа предоставления пользователю или группе разрешения на добавление компьютера в домен:
    - используйте объект групповой политики, чтобы предоставить разрешение **Добавление пользователя компьютера;**
    - предоставьте пользователю или группе разрешение **Создание объектов-компьютеров** в подразделении.
    - Задачу этой процедуры можно также выполнить, используя Модуль Active Directory для Windows PowerShell. Чтобы открыть Модуль Active Directory, нажмите кнопку **Пуск**, щелкните **Администрирование**, а затем щелкните **Модуль Active Directory для Windows PowerShell.**

      Чтобы открыть Модуль Active Directory в , откройте **Диспетчер серверов**, щелкните **Сервис**, а затем щелкните **Модуль Active Directory для Windows PowerShell.**

Задание: 1.Создать Учетные записи

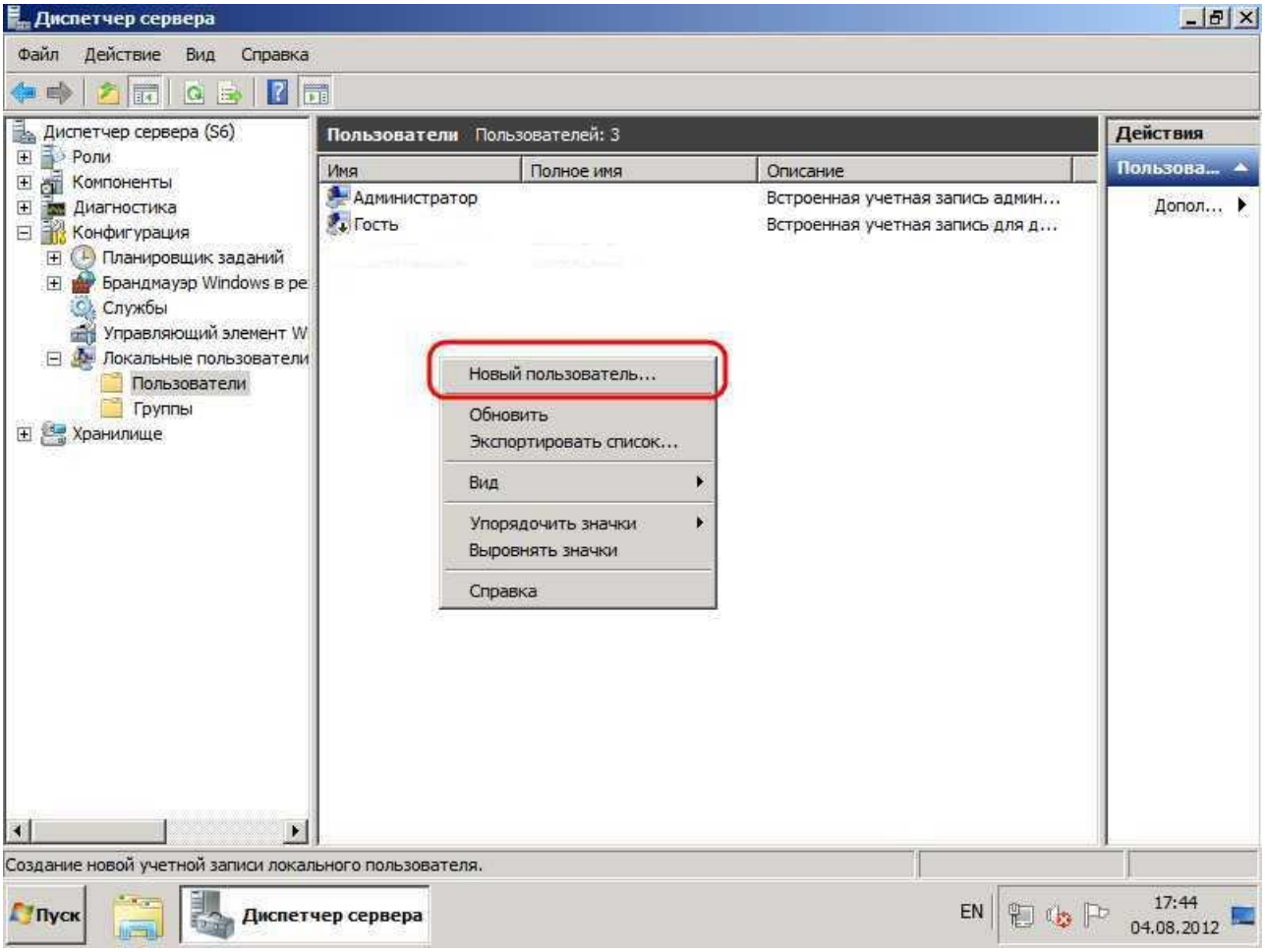
Практическое занятие №13.

Создание и настройка учетных записей пользователей. Управление локальными и глобальными группами. Использование шаблонов.

Цель: Создать новых пользователей.

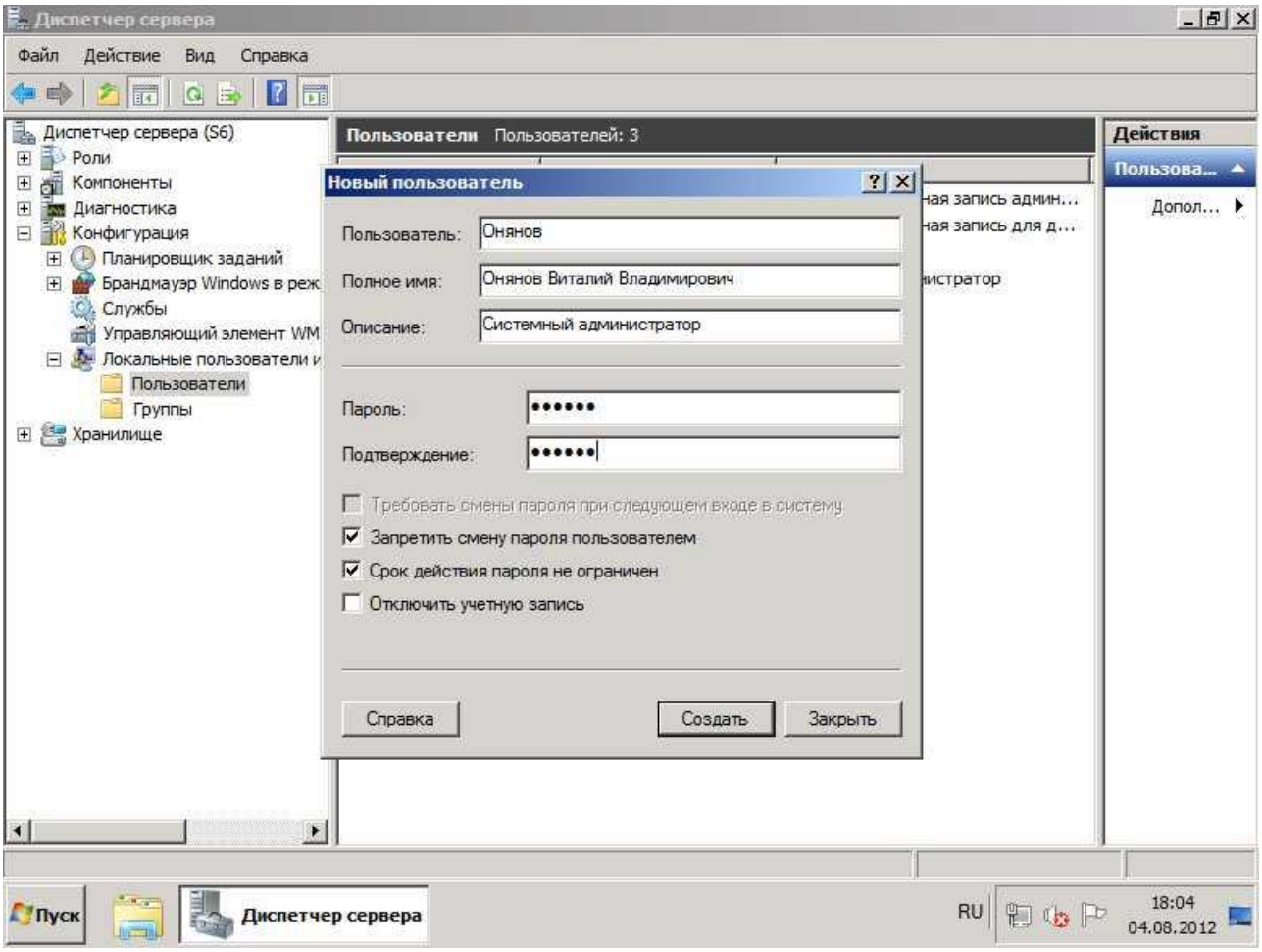
Создание нового пользователя

Запускаем диспетчер сервера («*Пуск*» — «*Администрирование*» — «*Диспетчер сервера*»). Раскрываем вкладку «*Конфигурация*» , затем «*Локальные пользователи и группы*» и выбираем оснастку «*Пользователи*» . В таблице справа мы видим уже существующих пользователей. Кликаем в свободном месте таблицы правой кнопкой мыши и выбираем «*Новый пользователь*» .

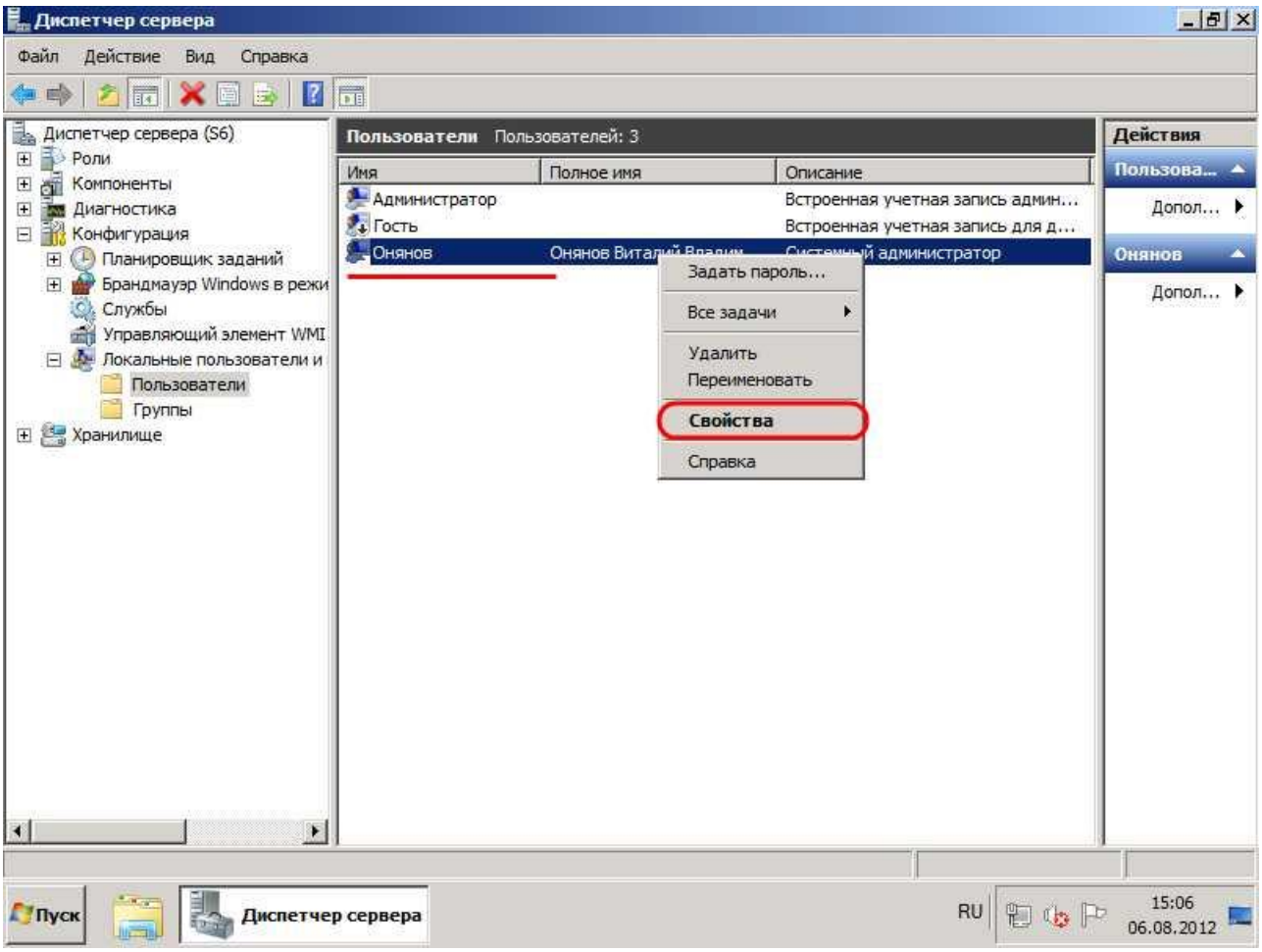


Откроется окно ввода данных пользователя. В поле «*Пользователь*» необходимо указать то имя, под которым пользователь будет логиниться на сервер, поля «*Полное имя*» и «*Описание*» могут быть любыми. Далее вводим 2 раза пароль. По умолчанию пароль должен отвечать требованиям сложности. О том как изменить политику паролей в Windows 2008 можно прочитать здесь. Рекомендую сразу записать пароль в отведенное для этого дела места. Удобно использовать специальные менеджеры паролей, например бесплатную программу KeePass. Если оставить галочку

«*Требовать смены пароля при следующем входе в систему*» , то, соответственно, при первом входе пользователя система попросит его ввести новый пароль. Здесь также можно вообще запретить пользователю менять свой пароль. И, наконец, если не ставить галочку «*Срок действия пароля не ограничен*» то через количество дней, указанных в политике безопасности паролей, система потребует у пользователя ввести новый пароль. После того как все настройки определены (их можно поменять в любое время) жмем «*Создать*» .



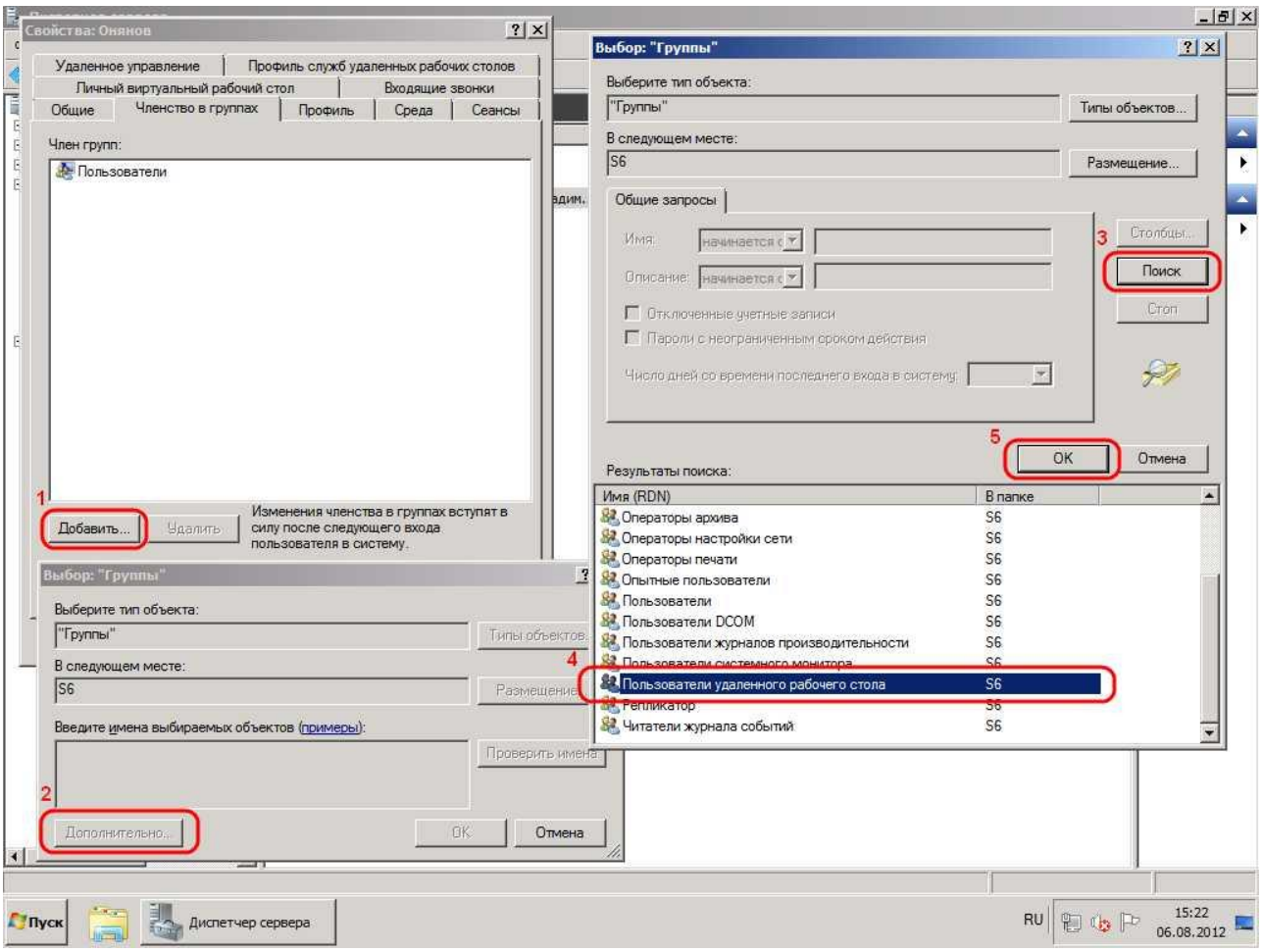
В списке должен появиться только что созданный пользователь. Кликнув по нему правой кнопкой мыши, видно, что из этого меню можно изменить пароль пользователя, удалить, переименовать пользователя, а также отредактировать его свойства.



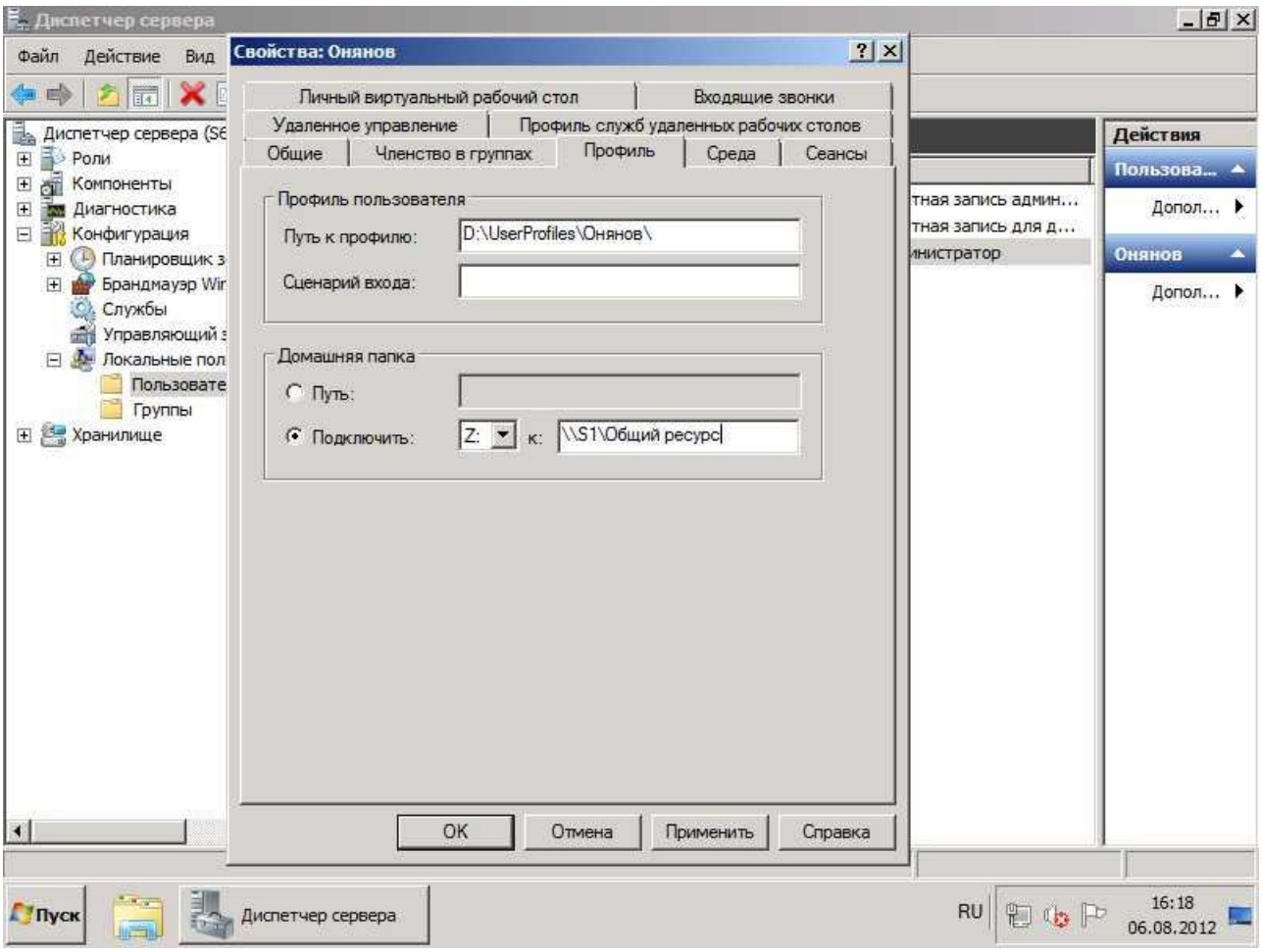
2. Редактирование свойств пользователя

Рассмотрим некоторые из свойств пользователя:

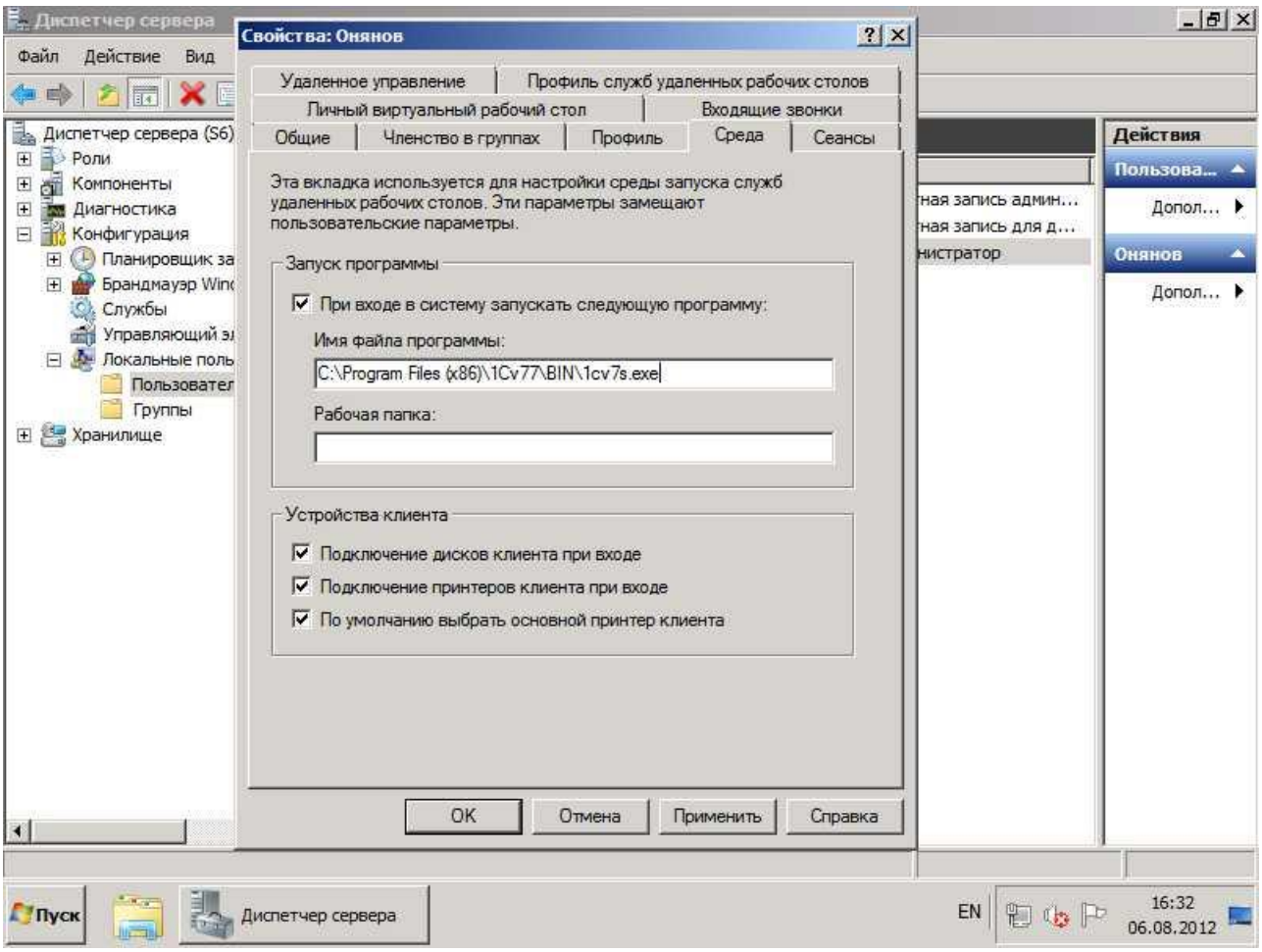
- Вкладка «*Общие*» — здесь можно изменить начальные данные пользователя. О них было сказано выше.
- «*Членство в группах*» — здесь можно определить в какие группы будет входить пользователь. Например, если предполагается, что пользователь будет работать через удаленный рабочий стол, то его нужно добавить в группу «*Пользователи удаленного рабочего стола*» . Для этого нажимаем кнопку «*Добавить*» , затем «*Дополнительно*» , в окне выбора группы жмем «*Поиск*» , выбираем нужную группу из списка и кликаем «*ОК*» 3 раза.



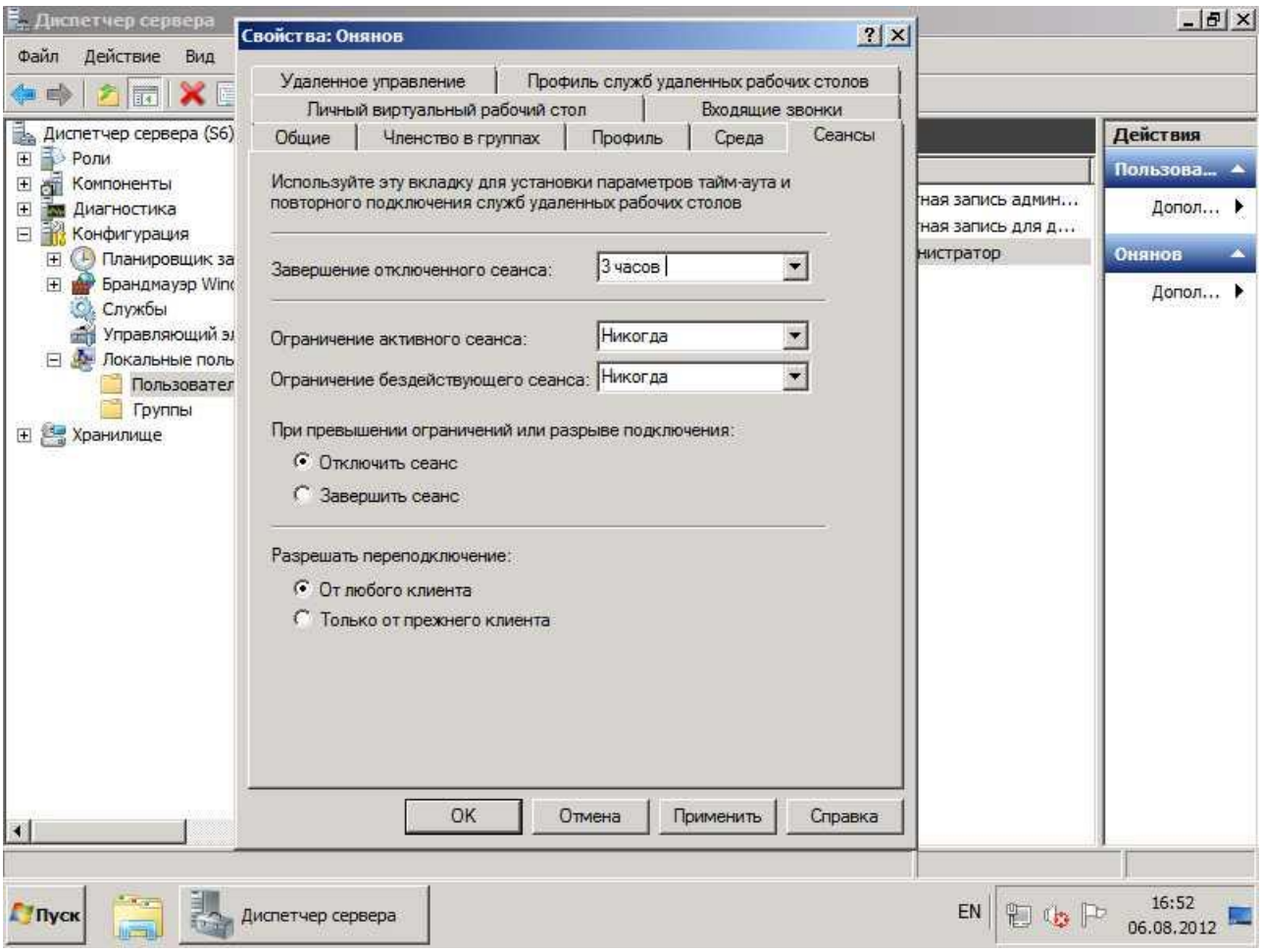
- На вкладке «*Профиль*» можно изменить путь хранения профиля (По умолчанию это **C:\Users**), указать сценарий входа, а так же задать сетевой диск, который будет подключаться при входе пользователя.



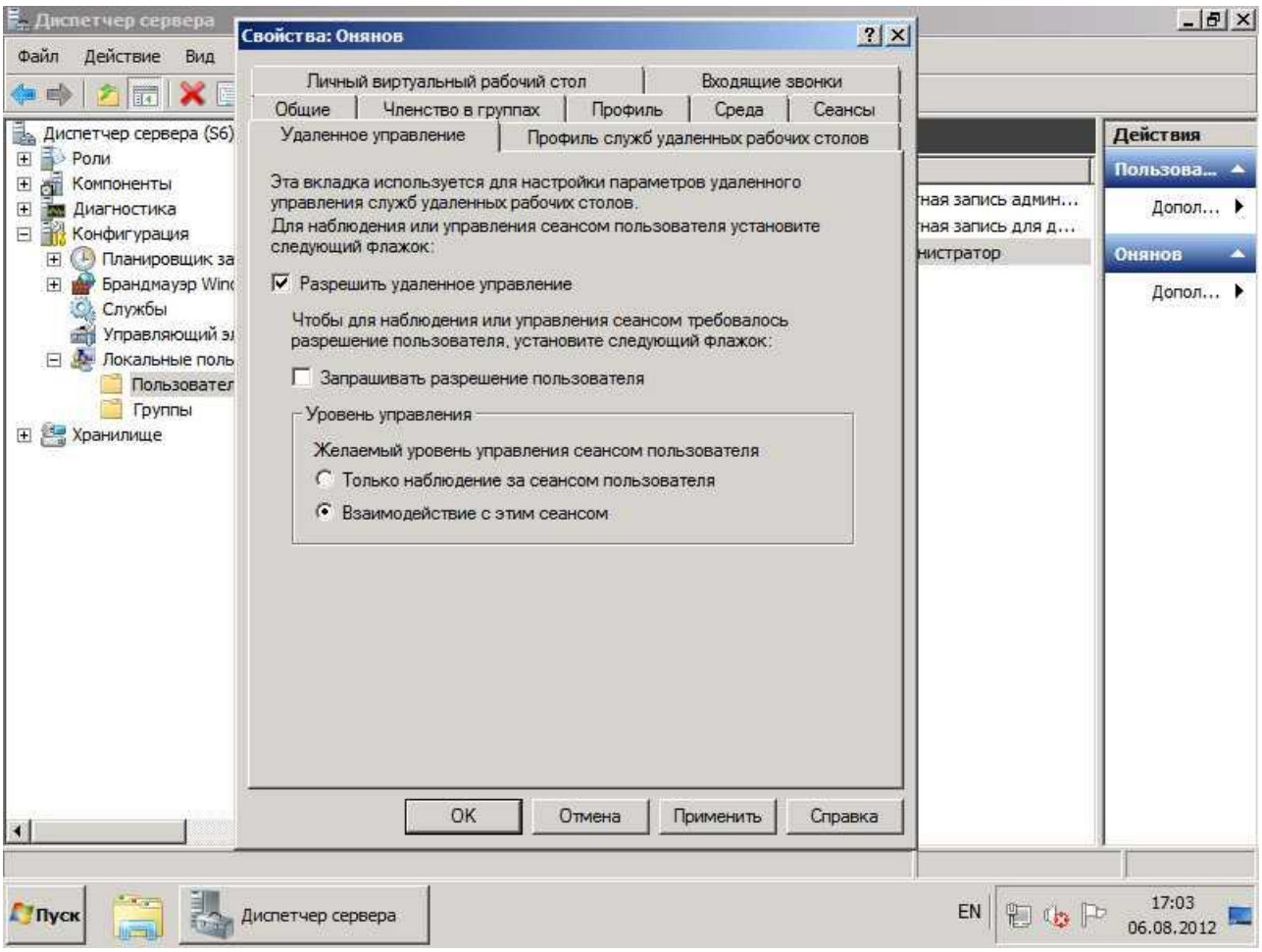
- «*Среда пользователя*» — здесь можно задать программу, которая будет запускаться при входе пользователя на удаленный рабочий стол. В этом случае пользователю будут недоступен рабочий стол, панель задач, а также другие программы сервера. При закрытии этой программы также будет выгружаться и учетная запись. Грубо говоря, пользователь сможет работать только с этой программой и ни с чем больше. Также на этой влкдаке можно разрешить/запретить подключение устройств при работе через удаленный рабочий стол.



- Вкладка «*Сеансы*» отвечает за установку параметров тайм-аута и повторного подключения к удаленному рабочему столу. Очень часто на практике я сталкивался с ситуацией, когда пользователь не отключался от удаленного рабочего стола, просто закрывая терминал «крестиком» . Учетная запись в этом случае продолжает «висеть» на сервере. Помогает в данной ситуации выставление тайм-аута отключения сеанса.



- Вкладка «*Профиль служб терминалов*» аналогична вкладке «*Профиль*» , с той лишь разницей, что относится к профилю пользователя, загружаемому при входе на сервер через удаленный рабочий стол. Также здесь можно запретить данное подключение.
- На вкладке «*Удаленное управление*» можно включить/отключить удаленное управление учетной записью пользователя при работе через удаленный рабочий стол. Обычно здесь я снимаю галочку «*Запрашивать разрешение пользователя*» т. к. если пользователь отключился от сеанса службы терминалов, то управлять этой учеткой уже не получится.



Практическое занятие №14.

Автоматизация процедур администрирования. Утилиты командной строки.

Службы Службы Reporting Services поддерживают использование сценариев для автоматизации стандартных задач по установке, развертыванию и администрированию. Развертывание сервера отчетов является многошаговым процессом. Чтобы настроить развертывание, необходимо использовать несколько средств и процессов. Для автоматизации всех задач не существует единой программы или единого подхода.

Не все шаги следует автоматизировать. В некоторых случаях выполнение шага вручную или с помощью графического средства является самым простым и эффективным подходом. Например, если требуется развернуть большое количество отчетов и моделей, проще скопировать базу данных сервера отчетов, чем писать программный код, который воссоздаст среду сервера отчетов.

Некоторые шаги требуют специального программного кода. Например, автоматизировать настройку URL-адресов для веб-службы и диспетчера отчетов можно только путем написания специального кода, который обращается к Инструментарию управления Windows (WMI) сервера

отчетов. Избежать написания программного кода на этом шаге можно. Для этого примените средство настройки служб Службы Reporting Services. Чтобы выполнить скрипт, настраивающий сервер отчетов, необходимо иметь права локального администратора на настраиваемом компьютере.
Этот раздел описывает рекомендуемые подходы для автоматизации определенных шагов. Упомянуты несколько программ и программных интерфейсов; описания каждого предоставлены далее в разделе.

Задачи развертывания и способы их автоматизации

В следующей таблице обобщены задачи по установке и настройке сервера отчетов, необходимые для его развертывания.Эту таблицу можно использовать для сверки конкретной задачи с подходом, позволяющим ее автоматизировать или выполнить полностью автоматически.

Задача	**Подход**
Установить службы Службы Reporting Services.	Для выполнения автоматической установки программу установки можно запустить из командной строки. Программу установки можно использовать как для установки, так и для настройки сервера отчетов, но только в случае, если указаны параметры конфигурации по умолчанию и система соответствует всем требованиям для этого типа установки. Если установка конфигурации по умолчанию невозможна, необходимо установить только файлы.
Настройте учетную запись службы.	Начальная конфигурация этой учетной записи службы выполняется программой установки. Чтобы автоматизировать сделанные в учетной записи службы изменения как задачу, которая будет выполнена после установки, необходимо написать пользовательский код, выполняющий вызовы к поставщику WMI сервера отчетов. Для программной настройки учетной записи службы не существует специальных программ командной строки или шаблонов скриптов. Если автоматизировать этот шаг путем создания программного кода невозможно, то учетную запись можно настроить вручную при помощи средства настройки служб Службы Reporting Services.

Настройте URL-адреса веб-службы сервера отчетов и диспетчера отчетов.	Необходимо написать специальный программный код, обращающийся к поставщику WMI сервера отчетов. Для настройки URL-адресов не существует специальных программ командной строки или шаблонов скриптов. Если вы хотите избежать написания кода, то URL-адреса можно настроить вручную при помощи средства настройки служб Службы Reporting Services.
Создание базы данных сервера отчетов.	Необходимо написать специальный программный код, обращающийся к поставщику WMI сервера отчетов. Для создания баз данных сервера отчетов и роли RSExecRole не существует специальных программ командной строки или шаблонов скриптов. Если вы хотите избежать написания кода, то базу данных можно создать вручную при помощи средства настройки служб Службы Reporting Services. .
Настройка подключения к базе данных сервера отчетов.	При изменении строки подключения, учетной записи, пароля или типа проверки подлинности следует запустить программу **rsconfig** для настройки соединения. Программу rsconfig.exe нельзя использовать для создания или обновления базы данных. База данных и роль RSExecRole должны быть созданы ранее.
Настройка масштабного развертывания.	Для настройки масштабного развертывания выберите один из следующих подходов. • Для соединения экземпляров сервера отчетов с существующим экземпляром запустите программу rskeymgmt.exe. • Напишите специальный программный код, обращающийся к поставщику WMI сервера отчетов.
Резервное копирование ключей шифрования.	Для автоматизации резервного копирования ключей шифрования выберите один из следующих подходов.

	• Для создания резервной копии ключей шифрования запустите программу rskeymgmt.exe. • Напишите специальный программный код, обращающийся к поставщику WMI сервера отчетов.
Настройка электронной почты сервера отчетов.	Напишите пользовательский программный код, обращающийся к поставщику WMI служб Службы Reporting Services. Поставщик поддерживает подмножество установок конфигурации электронной почты. Хотя файл RSReportServer.config содержит все установки, не используйте этот файл автоматически. В особенности не используйте пакетный файл для копирования файла на другой сервер отчетов. Каждый файл конфигурации содержит значения, определенные для текущего экземпляра. Эти значения не будут допустимыми на других экземплярах сервера отчетов.
Настройка учетной записи автоматического выполнения.	Для автоматизации настройки учетной записи автоматического выполнения выберите один из следующих подходов. • Запустите программу rsconfig.exe для настройки учетной записи. • Напишите специальный программный код, обращающийся к поставщику WMI сервера отчетов.
Развертывание существующего содержимого на другом сервере отчетов, включая иерархию папок, назначение ролей, отчеты, подписки, расписания, источники данных и ресурсы.	Лучший способ повторно создать существующую среду сервера отчетов — скопировать базу данных сервера отчетов в новый экземпляр сервера отчетов. Альтернативный подход заключается в написании специального кода, который программным путем заново создает существующее содержимое сервера отчетов.Однако учтите, что подписки, моментальные снимки отчетов и журнал отчетов невозможно создать повторно

	программным способом. В некоторых случаях развертывание может выиграть от применения обоих методов (то есть можно восстановить базу данных сервера отчетов, а затем написать программный код, изменяющий ее для конкретного экземпляра).

Инструменты и технологии для автоматизации развертывания сервера

В следующем списке обобщаются программы и интерфейсы, которые могут использоваться для автоматизации задач развертывания и обслуживания.

- Программа установки может запускаться в автоматическом режиме для установки и (в некоторых случаях) настройки компонентов сервера отчетов. Чтобы программа установки настроила экземпляр сервера отчетов, следует использовать параметр установки «Только файлы».
- Поставщик WMI служб Службы Reporting Services и программы командной строки служб Службы Reporting Services можно использовать для локальной и удаленной настройки сервера. Поставщик WMI служб Службы Reporting Services предоставляет классы, свойства и методы, реализующие управление всеми аспектами установки служб Службы Reporting Services, — задание учетной записи службы, настройка URL-адресов, создание и настройку базы данных сервера отчетов или настройку сервера отчетов для доставки отчетов по электронной почте. Для использования поставщика WMI необходимо написать специальный программный код или скрипт. Альтернативой написанию программного кода является использование программ командной строки (rsconfig.exe и rskeymgmt.exe). Можно написать пакетный файл, запускающий эти программы. Программы могут использоваться для автоматизации не всех задач настройки.
- Средство сервера скриптов сервера отчетов (rs.exe) может выполнять пользовательский программный код на языке Microsoft Visual Basic, предназначенный для повторного создания или перемещения существующего содержимого с одного сервера отчетов на другой. При этом подходе скрипт создается на языке Visual Basic, сохраняется в виде RSS-файла и с помощью программы rs.exe запускается на сервере отчетов. Написанный скрипт может обращаться к веб-службе сервера отчетов по протоколу SOAP. При создании скриптов развертывания данный подход позволяет повторно создавать пространство имен и содержимое папок сервера отчетов, а также политики безопасности на основе ролей.
- В выпуске SQL Server 2012 появились командлеты PowerShell для режима интеграции с SharePoint. PowerShell можно использовать для настройки и администрирования интеграции с SharePoint.

Миграция содержимого и папок сервера отчетов с помощью скриптов

Можно написать скрипт, дублирующие среду сервера отчетов на другом экземпляре сервера отчетов. Скрипты развертывания, как правило, пишутся на языке Visual Basic, а затем выполняются с помощью сервера скриптов сервера отчетов.
Скрипты позволяют копировать с одного сервера на другой папки, общие источники данных, ресурсы, отчеты, назначение ролей и настройки. Если есть необходимость воссоздания пространства имен сервера отчетов, они пишутся для одного экземпляра сервера отчетов, а затем выполняются на другом. Если развертывание служб Службы Reporting Services выполняется на нескольких серверах отчетов, то для одинаковой их настройки один и тот же скрипт выполняется на каждом из серверов.
Следующий перечень описывает шаги, необходимые для перемещения отчетов с одного сервера на другой.

1. Присвойте переменной скрипта URL-адрес исходного сервера отчетов.
2. Воспользуйтесь методами GetItemDefinition и GetProperties для получения определения и свойств отчета.
3. Присвойте URL-адресу значение, указывающее на целевой сервер.
4. Воспользуйтесь методом CreateCatalogItem, передав ему свойства, возвращенные методом GetProperties, и определение отчета, возвращенное методом GetItemDefinition.

Пользуясь методами get и create, можно выполнить аналогичные шаги для переноса настроек, папок, общих источников данных и ресурсов.

Примечание
Если учетные данные не указаны явным образом, то скрипты выполняются от имени пользователя Microsoft Windows, запустившего скрипт.

Настройка свойств сервера с помощью сценариев
Можно написать сценарии, которые зададут системные свойства на сервере отчетов. Следующий скрипт Visual Basic .NET иллюстрирует один из способов установки свойств. Этот сценарий отключает элемент управления RSClientPrint ActiveX, но можно заменить
значения **EnableClientPrinting** и **False** любым допустимым именем свойства и значением.
Чтобы использовать скрипт, сохраните его в файл с расширением RSS, а затем воспользуйтесь программой командной строки rs.exe для запуска файла на сервере отчетов. Скрипт не компилируется, поэтому необязательно иметь установку Visual Basic. В этом примере предполагается, что пользователь имеет необходимые разрешения на локальном компьютере, на котором находится сервер отчетов. Если пользователь не вошел в систему под учетной записью, имеющей необходимые разрешения, необходимо указать сведения об учетной записи с помощью дополнительных аргументов командной строки.
Public Sub Main()

```
        Dim props(0) As [Property]
        Dim setProp As New [Property]
        setProp.Name = "EnableClientPrinting"
        setProp.Value = “False”
        props(0) = setProp
        Try
           rs.SetSystemProperties(props)
        Catch ex As System.Web.Services.Protocols.SoapException
           Console.Write(ex.Detail.InnerXml)
        Catch e as Exception
           Console.Write(e.Message)
        End Try
End Sub
```

Практическое занятие №15.

Средства удаленного доступа.

Цель: Научиться работать с удаленным доступом.

Инструментарий, позволяющий выполнить команду или работать с приложениями на удаленных системах, существенно упрощает работу как пользователя, так и администратора. Не покидая рабочего места, на удаленной системе можно запустить сервис, изменить настройки, диагностировать и исправить проблему, создать документ, обработать данные.

Функции удаленного управления, реализованные в Windows NT, были весьма ограничены, в результате большинство операций администрирования приходилось выполнять в локальной консоли. Но с каждой новой версией операционной системы Windows и обновлением возможности расширялись, и в настоящее время количество доступных решений возросло на порядок. Администратор может управлять системами при помощи штатных средств Windows — консоли MMC, PowerShell, командной строки WinRS (Windows Remote Shell), групповых политик, средств удаленного доступа к Рабочему столу RDP (Remote Desktop Protocol Protocol — протокол удаленного Рабочего стола) и некоторых других. Этот список можно дополнить инструментами и утилитами сторонних разработчиков, но мы остановимся именно на штатных возможностях, заложенных в операционных системах, поскольку их функционал достаточен для решения большинства административных и пользовательских задач в малых и средних сетях.

Удаленный Рабочий стол

В операционной системе Windows, начиная с NT (точнее NT 4.0 Terminal Server Edition), появилась поддержка RDP — протокола, который предоставляет возможность подключаться к Рабочему столу удаленной системы или сервису терминальных подключений. Пользователь, подключившийся к удаленному компьютеру по RDP, получает практически те же возможности, что и при работе в локальной системе: доступ к установленным программам, дискам, сети, печати, звуковым устройствам и т. д. Иными словами, он видит перед собой Рабочий стол удаленной системы, которым управляет как обычно, а физически находится от него далеко. Вариант взаимодействия с системой при помощи графических инструментов очень популярен, так как не требует дополнительной подготовки пользователя и изучения команд, ведь все настройки производятся в обычном визуальном режиме. Самое главное то, что в этом случае мощность клиентского компьютера роли не играет, ведь все вычисления производятся на удаленной системе. А компьютер пользователя просто выводит результат на экран.

Клиенты для подключения по RDP имеются в большинстве популярных операционных систем — они встроены в Windows (в том числе Windows CE и Mobile), Linux, FreeBSD, OpenBSD, Mac OS X и некоторые другие. Что, по сути, снимает все ограничения.

В Windows Server 2008 R2 и Windows 7 доступен протокол RDP версии 7.0, получившая поддержку Aero, Direct2D и Direct3D в приложениях, улучшена мультидисплейная конфигурация и работа с мультимедиа. В Windows серверных и клиентских версий поддерживается два режима работы:

удаленное управление Рабочим столом — используется для удаленного управления компьютером администраторами, его обычно используют для устранения неполадок или настройки компьютера;

службы удаленных Рабочих столов (Remote Desktop Services, RDS) — предназначен для подключения пользователей к удаленному Рабочему столу или приложениям.

В предыдущих версиях Windows служба удаленных Рабочих столов называлась сервер терминалов.

В исправлении Windows Server 2008 R2 с пакетом обновления SP1, появилось новое расширение — RemoteFX. Оно предоставляет большие возможности для работы по протоколу удаленного Рабочего стола — RDP,

включая полную поддержку видео, Silverlight и 3D-анимаций. Технология RemoteFX позволяет использовать рабочую среду Aero на виртуальном Рабочем столе. Но для использования всех возможностей необходима специальная версия клиента RDP.
В первом режиме Windows Server 2008 R2 поддерживает только два одновременных RDP-подключения, к тому же не прерывается локальное. И такая работа не требует дополнительного лицензирования. Клиентские версии операционных систем, в том числе Windows 7, поддерживают работу только одного пользователя (локального или подключившегося через RDP). В итоге при удаленном подключении к компьютеру пользователь, который работает локально, будет автоматически отключен, и получить доступ к системе в это же время не сможет. Иными словами, при помощи функции удаленного управления Рабочим столом показать, как правильно выполнить некоторую операцию, весьма проблематично, можно лишь произвести действия по настройке, после чего отдать управление обратно пользователю.

Для помощи в настройках удаленному пользователю и одновременной консультации в режиме чата или голосового общения следует использовать Remote Assistance (Удаленный помощник). Он также позволяет взять управление системой, но с разрешения пользователя.

Система и щелкнуть кнопкой мыши на ссылке Настройка удаленного доступа. В результате появитя окно Свойства системы, открытое на вкладке Удаленный доступ.4Чтобы разрешить удаленное управление Рабочим столом, достаточно в окне Диспетчера сервера перейти по ссылке Настроить удаленный рабочий стол или открыть Панель управления, выбрать Система и безопасность

Разрешаем подключение к удаленному рабочему столу в Windows Server 2008 R2

В области Удаленный рабочий стол устанавливаем переключатель в одно из следующих положений.

Разрешать подключения от компьютеров с любой версией удаленного рабочего стола (опаснее) — позволит подключаться с клиентских компьютеров, работающих под управлением более ранних версий операционных систем Windows (или клиентов в других операционных системах — GNU/Linux, Mac OS X), которые не поддерживают новую

версию протокола RDP. Такой вариант считается менее безопасным, хотя это не значит, что нужно отказаться от его использования.

Разрешать подключаться только с компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне сети — выбираем, если в организации в наличии только Windows 7 или Windows Server 2008 R2.

Нажав кнопку Выбрать пользователей, указываем учетные записи, которым разрешено подключаться удаленно (Администратор, как правило, уже имеет удаленный доступ).
В Windows 7 настройки подключения аналогичны.
Естественно, для каждого компьютера вручную разрешать подключение к удаленному Рабочему столу долго, поэтому лучше воспользоваться возможностями групповых политик. Переходим в окно Диспетчера сервера, выбираем Конфигурация компьютера — Административные шаблоны — Компоненты Windows — Службы терминалов и активизируем параметр Разрешать удаленное подключение с помощью служб терминалов.
Чтобы подключиться к удаленной системе, выбираем меню Пуск- Все программы — Стандартные — Подключение к удаленному рабочему столу.
В появившемся окне необходимо ввести имя или IP-адрес удаленной системы и в нескольких вкладках настроить параметры подключения — размер экрана, глубину цвета, локальные ресурсы, которые будут подключены во время сеанса и др.

Программа подключения к удаленному Рабочему столу

Чтобы не вводить параметры сеанса каждый раз, их можно сохранить, нажав соответствующую кнопку.
В процессе подключения будет запрошен пароль учетной записи, используемой для входа в удаленную систему, и потребуется принять сертификат сервера. После этого получим доступ к удаленному Рабочему столу.

Удаленный сеанс Windows 7 в Windows Server 2008 R2

Режим службы удаленных Рабочих столов уже требует дополнительного

лицензирования и предназначен для удаленной работы пользователей с приложениями, а не для администрирования систем.

Практическое занятие №16.

Мониторинг серверной операционной системы. Интерфейсы мониторинга.

Цель: Изучить мониторинг серверной операционной системы.

Мощные производственные серверы требуют постоянного контроля за тем, какие события на них происходят. Неверный ввод паролей, попытки доступа к административным ресурсам, внезапные остановки служб, отсутствие свободного места на жестких дисках – информация обо всех этих и других событиях необходима системному администратору для обеспечения рабочего функционирования промышленных серверов.

Теперь настало время поговорить о том, как реализованы средства сбора сообщений о событиях в новой операционной системе Windows Server 2008.

Нововведения

Как и многие другие функции Windows Server 2008, журналы событий были существенно переделаны и дополнены новыми возможностями. Но обо всем по порядку. Для начала рассмотрим, как новшества были внесены в средства получения и обработки событий Event Viewer.

По определению Microsoft [1], событие – это любое значительное проявление в операционной системе или приложении, требующее отслеживания информации. Событие не всегда негативно, поскольку успешный вход в сеть, успешная передача сообщений или репликация данных также могут генерировать события в Windows. В каждом журнале с его событиями связаны общие свойства.

- **Level (уровень)** – это свойство определяет важность события;
- **Date and Time (дата и время)** – это свойство содержит информацию о дате и времени возникновения события;
- **Source (источник)** – это свойство указывает источник события: приложение, удаленный доступ, служба и т. д.;
- **Event ID (код события)** – каждому событию назначен идентификатор события ID, число, сгенерированное источником и уникальное для всех типов событий;

- **Task Category (категория задачи)** – это свойство определяет категорию события, например Security или System.

На основе данных свойств событий можно осуществлять выборку и фильтрацию, выполнять поиск.

Внешний вид

Интерфейс утилиты Event Viewer также существенно изменился. Информация, содержащаяся в системных собщениях, во многом осталась прежней, переработанный интерфейс теперь позволяет более эффективно работать с событиями, осуществлять их поиск, фильтрацию и другие функциональные возможности. Внешний вид утилиты аналогичен реализации MMC 3.0. Навигационное дерево на левой панели окна утилиты просмотра событий отображает список системных собщений и журналов, доступных для просмотра, а также содержит новые папки, предназначенные для создания настраиваемых представлений событий и подписок с удаленных систем.

Фильтры

Настраиваемые представления – это специальные фильтры, созданные либо автоматически системой Windows Server 2008 во время добавления в систему новых ролей сервера или приложений, таких как Active Directory Certificate Services (службы сертификатов каталогов), сервер DHCP, либо администраторами вручную. Для администраторов одной из важнейших функций при работе с журналами событий является возможность создавать фильтры, позволяющие просматривать только интересующие события, чтобы можно было быстро диагностировать и устранять проблемы в системе.

В качестве примера рассмотрим папку Custom Views в навигационной панели утилиты просмотра событий. Если в этой папке щелкнуть правой кнопкой мыши по Administrative Events и затем указать Properties, то после нажатия Edit Filter получаем набор отфильтрованных по критерию сообщений.

Настраиваемые представления оснастки Administrative Events фиксируют все критические события, а события ошибок и предупреждений фиксируются для всех журналов событий (в отличие от предыдущих версий Windows). Таким образом, с помощью данного фильтра администратор может обращаться к единственному источнику для быстрой проверки потенциальных проблем, присутствующих в системе.

Теперь в качестве примера попробуем создать собственное представление. Для этого щелкнем правой кнопкой мыши на папке Custom View и в контекстном меню выберем пункт Create Custom View (создать настраиваемое представление).

Если требуемые события необходимо фильтровать по дате, то в списке Logged выберите диапазон дат. Затем необходимо указать критерий Event Level (уровень событий) для включения в настраиваемое представление. Возможные значения:

- **Critical** –критическое;
- **Error** – ошибка;
- **Warning** – предупреждение;
- **Information** – информация;
- **Verbose** – подробности.

После указания уровня событий необходимо перейти к разделам By Log и By Source. Используя соответствующие раскрывающиеся списки, укажите журнал события и источники журнала событий, которые должны быть включены в данный настраиваемый фильтр.

При необходимости вы также можете указать конкретные коды событий, категории задач и другие параметры. Но помните, что включение слишком большого числа событий в настраиваемое представление может отрицательно сказаться на производительности и использовании ресурсов системы.

Созданные настраиваемые представления можно экспортировать в XML-файл для последующего распространения на другие машины.

Журналы

Теперь рассмотрим типы журналов, появившиеся в Windows Server 2008. Здесь тоже произошли некоторые изменения. В папке журналов Windows Logs находятся как традиционные журналы безопасности, приложений и системы, так и два новых журнала – Setup (настройка) и Forwarded Events (пересланные события).

Первые три типа событий уже присутствовали в предыдущих версиях системы, поэтому рассказывать о них нет смысла. А о последних двух следует рассказать подробнее.

Журнал Setup фиксирует информацию, связанную с установкой приложений, ролями сервера и их характеристиками. Так, например, сообщения о добавлении на сервере роли DHCP будет отражены в этом журнале.

В журнале Forwarded Events собираются сообщения, присланные с других машин в сети. Наличие такой функции позволяет облегчить решение проблем, возникших сразу на нескольких машинах в сети.

Папка Applications and Services Logs (журналы приложений и служб) представляют собой новый способ логической организации, представления и сохранения событий, связанных с конкретным приложением, компонентом или службой Windows, вместо использовавшейся ранее регистрации событий, которые оказывают влияние на всю систему. Эти журналы включают четыре подтипа:

- **Admin** – события, предназначенные для конечных пользователей и администраторов;
- **Operational** – рабочий журнал событий, также предназначенный для администраторов;
- **Analytic** – журнал позволяет отслеживать цепочку возникновения проблемы и часто содержит большое количество записанных событий;
- **Debug** – используется для отладки приложений.

По умолчанию журналы Analytic и Debug скрыты и отключены. Для того чтобы их просмотреть, щелкните правой кнопкой мыши на папке Applications and Services Logs, а затем в контекстном меню выберите пункт View, Show Analytic and Debug Logs

Подписки на события

Рассмотрим еще одно нововведение в Windows Server 2008. Это Subscriptions (подписки). Эта долгожданная функция аналогична службе Syslog в UNIX. Данная функциональная возможность позволяет удаленным компьютерам пересылать сообщения о событиях, в результате чего их можно просматривать централизованно. Например, если у вас имеется несколько серверов и вам необходимо следить за состоянием каждого из них. Теперь вместо того чтобы переключаться из одной консоли Event Viewer в другую, вы можете наблюдать все события в одной консоли. Это позволит сэкономить время и облегчить процесс решения проблем.

В качестве примера настроим подписку событий. Для этого нам потребуются два компьютера: один будет выступать в качестве источника событий, второй будет получать события от первого. Зайдите на сервер-источник под учетной записью, обладающей административными правами. Введите в окне командной строки:

winrm quickconfig

Добавьте компьютер, собирающий сообщения о событиях, в группу локальных администраторов на источнике. Затем войдите на компьютер, собирающий сообщения, и также выполните:

winrm quickconfig

После этого выполните на нем же следующую команду:

wecutil qc

При необходимости вы можете изменять параметры оптимизации доставки событий. Например, вы можете изменить параметр Minimize Bandwidth (минимизация пропускной способности) для удаленных серверов с ненадежным каналом связи.

Реагируем на события

Еще одной интересной функцией, о которой хотелось бы упомянуть, является возможность ответной реакции на события. Другими словами, если в журнал событий поступило сообщение о том, что на жестком диске осталось слишком мало свободного места, вы можете автоматически запустить сценарий, выполняющий архивацию данных. Аналогично в случае получения сообщения об ошибке какого-либо критически важного приложения, вы можете отправить уведомление администратору по электронной почте или смс. Данная функция является долгожданным решением проблем с автоматизацией работы серверов, так как раньше требовалось устанавливать дополнительное программное обеспечение или писать сценарии, для того чтобы заставить сервер автоматически реагировать на определенные события.

В качестве примера настроим отправку сообщения администратору в случае неудачного входа пользователя в систему. Обратите внимание на то, что теперь это событие имеет другой ID, отличный от использовавшегося в Windows 2003 ID 528.

Для этого необходимо зайти в журнал событий Event Viewer, открыть раздел Windows Logs, затем Security, выбрать нужное событие, нажать правую кнопку мыши и указать Attach Task To This Event… (прикрепить задачу к этому событию)

В открывшемся окне необходимо выбрать название события и его описание. На следующем шаге указываются используемый журнал, источник и номер события. Содержимое этого журнала нельзя изменить. Потом выбирается тип ответного действия. Это может быть выполнение какого-либо приложения, отправка электронного письма или вывод сообщения на экран. Выберем отправку письма. На следующем шаге нужно указать, от кого и на чей адрес отправлять письмо, тему письма, его текст. Можно также прикрепить какой-либо файл к данному сообщению. Не забудьте указать IP-адрес SMTP-сервера. На следующем шаге поставьте галочку в соответствующем поле, для того чтобы после создания задачи открылось окно с ее свойствами

Свойства задач

Окно свойств задачи аналогично интерфейсу Scheduled Tasks для заданий, выполняющихся по расписанию. Здесь можно указать учетную запись, под которой выполняется задача, при необходимости ее можно выполнять только когда пользователь работает на машине.

В закладке Triggers вы можете добавлять или изменять условия выполнения задачи. В Actions вы можете добавлять различные действия. В закладке Conditions прописаны условия, при которых выполняется задача. В Settings можно прописать, какие действия должны быть выполнены при различных условиях. Например, что нужно делать в случае, если такая задача уже выполняется. Наконец, в закладке History вы можете наблюдать все события, которые вызвали выполнение задачи.

Практическое занятие №17.
Изучение журналов мониторинга. Создание и просмотр оповещений. Мониторинг сетевой активности.

Цель: Изучить журналы мониторинга

Чтение журналов событий является неотъемлемой частью работы любого администратора безопасности. Сетевое оборудование, операционные системы и практически все бизнес приложения осуществляют журналирование событий безопасности, таких как, удачный/неудачный вход в систему, запуск/остановка системы, обращение к закрытому порту для межсетевых экранов и другие события. Однако при наличии в сети даже десяти серверов, чтение журналов событий на каждом из них становится довольно трудоемкой задачей, требующей затраты большой части рабочего времени. Для того, чтобы автоматизировать процесс обработки журналов событий, например в части поиска попыток неудачного входа в систему, существует множество различных решений. Для Unix систем существует множество бесплатных сценариев на Перл, позволяющих осуществлять автоматический поиск заданного события в журнале и реакцию на данное событие, например отправку почтового сообщения администратору. Для Windows есть множество коммерческих продуктов, таких как ArcSight, Symantec Information Manager или Tivoli Security Operations Manager, которые умеют не только собирать события от различных источников, но и проверять данные события на соответствие различным моделям угроз (например подбор пароля или DDoS атака), реагировать на события, строить отчеты и многое другое. Но эти мощные средства мониторинга стоят очень недешево и в нынешних непростых экономических условиях многим организациям просто не по карману.

Однако, если в вашей сети на серверах используется операционная система Windows Server 2008, то вы можете самостоятельно организовать

централизованный мониторинг событий безопасности. Для начала поговорим о том, какие нововведения появились в системе журналирования в Windows Server 2008.

Как и многие другие функции Windows 2008 журналы событий были существенно переделаны и дополнены новыми возможностями. По определению Майкрософт [1] событие это любое значительное проявление в операционной системе или приложении, требующее отслеживания информации. Событие не всегда негативно, поскольку успешный вход в сеть, успешная передача сообщений, или репликация данных также могут генерировать события в Windows. В каждом журнале с его событиями связаны общие свойства.

Level (уровень) – Это свойство определяет важность события.

Date and Time (дата и время) – Это свойство содержит информацию о дате и времени возникновения события.

Source (источник) – Это свойство указывает источник события: приложение, удаленный доступ, служба и так далее.

Event ID (Код события) – Каждому событию назначен идентификатор события ID, число, сгенерированное источником и уникальное для всех типов событий.

Task Category (Категория задачи) – Это свойство определяет категорию события. Например Security или System. .

Итак, мы разобрались с тем, что представляет из себя событие в журнале Windows Event Log. Теперь нам необходимо сначала настроить аудит событий информационной безопасности. Далее будем предполагать, что у нас используется домен Active Directory и все сервера входят в этот домен. Для настройки аудита необходимо зайти на контроллер домена и открыть редактор групповых политик Start->Administrative Tools->Group Policy Management. Далее выбираем домен и нажав правую кнопку мыши указываем Create a GPO in this domain… Вообще, для включения аудита можно воспользоваться политиками домена по умолчанию, но лучше создать отдельную политику с соответствующим названием, так как это упрощает администрирование. Далее в новой политике идем в Computer Configuration-> Windows Settings -> Security Settings -> Local Policies -> Audit Policy. Откроется список возможных параметров настройки аудита. Включать все подряд параметры нет особого смысла, так как в таком случае журнал событий наполнится огромным количеством малоинформативных сообщений. Рекомендую следующий набор параметров:

Категория аудита	Тип аудита	Примечание
Audit account logon events	No auditing	
Audit account management	success/failure	

Audit directory service access	No auditing	
Audit logon events	success/failure	
Audit object access	No auditing	включить, только если необходимо отслеживать доступ к определенным объектам (например, каталогам на диске).
Audit policy change	success/failure	
Audit privilege use	success/failure	
Audit process tracking	No auditing	
Audit system events	success/failure	

Теперь мы настроили аудит в нашем домене. Открыв журнал событий Security можно убедиться в том, какое количество событий сыпется в него ежесекундно. Для того, чтобы не нагружать контроллеры домена и другие сервера задачами по обработке событий мы должны сначала переслать события безопасности на выделенный сервер, на котором и будет осуществляться автоматическая обработка всех полученных событий. Данный выделенный сервер также должен работать под управлением операционной системы Windows Server 2008 и входить в домен Active Directory. Для пересылки событий нам необходимо воспользоваться Subscriptions, подписками на события.

Подписки на события

Эта функция аналогична службе Syslog в Unix. Данная функциональная возможность позволяет удаленным компьютерам пересылать сообщения о событиях, в результате чего их можно просматривать локально из центральной системы.

Настроим пересылку событий с нескольких серверов на выделенный сервер сбора событий. Для этого на каждый из серверов источников событий

необходимо зайти под учетной записью, обладающей административными правами. В окне командной строки ввести:
winrm quickconfig
Сервер, собирающий сообщения о событиях необходимо добавить в группу локальных администраторов на каждом из серверов источников событий. Затем войдите на сервер, собирающий сообщения, и также выполните:
winrm quickconfig
После этого, выполните на нем же следующую команду:
wecutil qc
При необходимости, вы можете изменять параметры оптимизации доставки событий. Например, вы можете изменить параметр Minimize Bandwidth (минимизация пропускной способности) для удаленных серверов, с ненадежным каналом связи.
Теперь необходимо собственно создать подписку, указав события, которые должны извлекаться из логов серверов источников. Для этого на собирающем сервере запустите утилиту просмотра событий с учетной записью, обладающей административными привилегиями. Затем щелкните на папке Subscriptions в дереве консоли и выберите команду Create Subscription (Создать подписку). В поле Subscription Name нужно указать имя подписки. При необходимости в поле Description можно привести описание. Затем, в поле Destination Log (журнал назначения) выберите файл журнала, в котором будут храниться собранные события. По умолчанию эти события будут храниться в журнале перенаправленных событий в папке Windows Logs дерева консоли. После этого, щелкните на кнопке Select Computers, чтобы выбрать исходные сервера, которые будут перенаправлять события. Как уже упоминалось ранее, данные сервера должны находиться в домене. Затем выберите события, нажав на кнопке Select Events. Сконфигурируйте журналы и типы событий, предназначенные для сбора. Щелкните ОК чтобы сохранить подписку.
Журналы
Теперь зайдем на выделенный сервер сбора событий и рассмотрим типы журналов, появившиеся в Windows Server 2008. В папке журналов Windows Logs находятся как традиционные журналы безопасности, приложений и системы, так и два новых журнала – Setup (настройка) и Forwarded Events (Пересланные события). Первые три типа событий уже присутствовали в предыдущих версиях системы, поэтому о них рассказывать нет смысла. А о последних двух следует рассказать подробнее. Журнал Setup фиксирует информацию, связанную с установкой приложений, ролями сервера и их характеристиками. Так, например, сообщения о добавлении на сервере роли DHCP будет отражены в этом журнале. В журнале Forwarded Events собираются сообщения, присланные с других машин в сети.
Папка Applications and Services Logs (журналы приложений и служб) представляют собой новый способ логической организации, представления и сохранения событий, связанных с конкретным приложением, компонентом или службой Windows вместо использовавшейся ранее, регистрации

событий, которые оказывают влияние на всю систему. Эти журналы включают четыре подтипа: Admin (события, предназначенные для конечных пользователей и администраторов), Operational (Рабочий журнал событий, также предназначенный для администраторов), Analytic (журнал позволяет отслеживать цепочку возникновения проблемы и часто содержит большое количество записанных событий), Debug (используется для отладки приложений). По умолчанию журналы Analytic и Debug скрыты и отключены. Для того, чтобы их просмотреть, щелкните правой кнопкой мыши на папке Applications and Services Logs, а затем в контекстном меню выберите пункт View, Show Analytic and Debug Logs.

Фильтры

Настраиваемые представления – это специальные фильтры, созданные либо автоматически системой Windows 2008, во время добавления в систему новых ролей сервера или приложений, таких как Directory Certificate Services (Службы сертификатов каталогов), сервер DHCP, либо администраторами вручную. Для администраторов одной из важнейших функций при работе с журналами событий является возможность создавать фильтры, позволяющие просматривать только интересующие события, чтобы можно было быстро диагностировать и устранять проблемы в системе. В качестве примера, рассмотрим папку Custom Views в навигационной панели утилиты просмотра событий. Если в этой папке щелкнуть правой кнопкой мыши по Administrative Events и затем выбрать Properties, то после нажатия Edit Filter, можно увидеть как информация из журнала событий преобразуется в набор отфильтрованных событий. Настраиваемые представления оснастки Administrative Events фиксируют все критические события, а события ошибок и предупреждений фиксируются для всех журналов событий (в отличие от предыдущих версий Windows). Таким образом, с помощью данного фильтра администратор может обращаться к единственному источнику для быстрой проверки потенциальных проблем, присутствующих в системе. Это средство может пригодиться при обработке событий, приходящих с серверов источников событий.

Созданные настраиваемые представления можно экпортировать в XML-файл для последующего распространения на другие машины.

Реагируем на события

Еще одной интересной функцией, о которой хотелось бы упомянуть, является возможность ответной реакции на события. Например, если у вас пользователь указал неверные учетные данные для аккаунта, имеющего административные привилегии, то на появление данного события в журнале необходимо отреагировать, послав уведомление администратору безопасности. Данная функция является долгожданным решением проблем с автоматизацией работы серверов, так как раньше требовалось устанавливать дополнительное программное обеспечение или писать сценарии для того чтобы заставить сервер автоматически реагировать на определенные события.

В качестве примера настроим отправку сообщения администратору в случае неудачного входа пользователя в систему (Обратите внимание на то, что теперь это событие имеет другой ID 4625, отличный от использовавшегося в Windows 2003 ID 529).
Для этого необходимо зайти в журнал событий Event Viewer, открыть раздел Windows Logs, затем Security, выбрать нужное событие, нажать правую кнопку мыши, и указать Attach Task To This Event… (прикрепить задачу к этому событию).

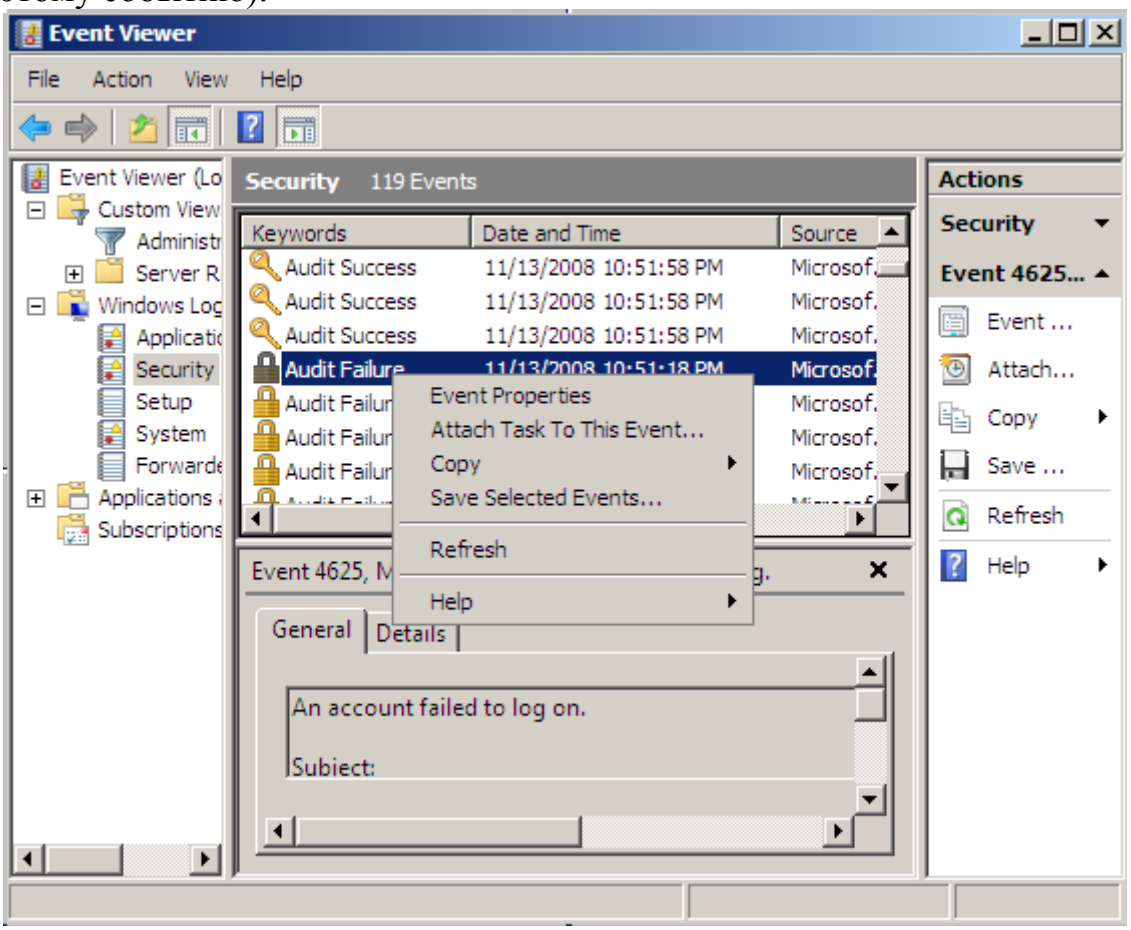


Рисунок 2.
Настройка ответной реакции на событие

В открывшемся окне необходимо выбрать название события и его описание. На следующем шаге указывается используемый журнал, источник и номер события. Содержимое этого журнала нельзя изменить. Потом выбирается тип ответного действия. Это может быть выполнение какого-либо приложения, отправка электронного письма или вывод сообщения на экран. Выберем отправку письма. На следующем шаге нужно указать, от кого и на чей адрес отправлять письмо, тему письма, его текст. Можно также прикрепить какой-либо файл к данному сообщению. Не забудьте указать IP-адрес SMTP сервера. На следующем шаге поставьте галочку в соответствующем поле, для того, чтобы после создания задачи, открылось окно с ее свойствами.

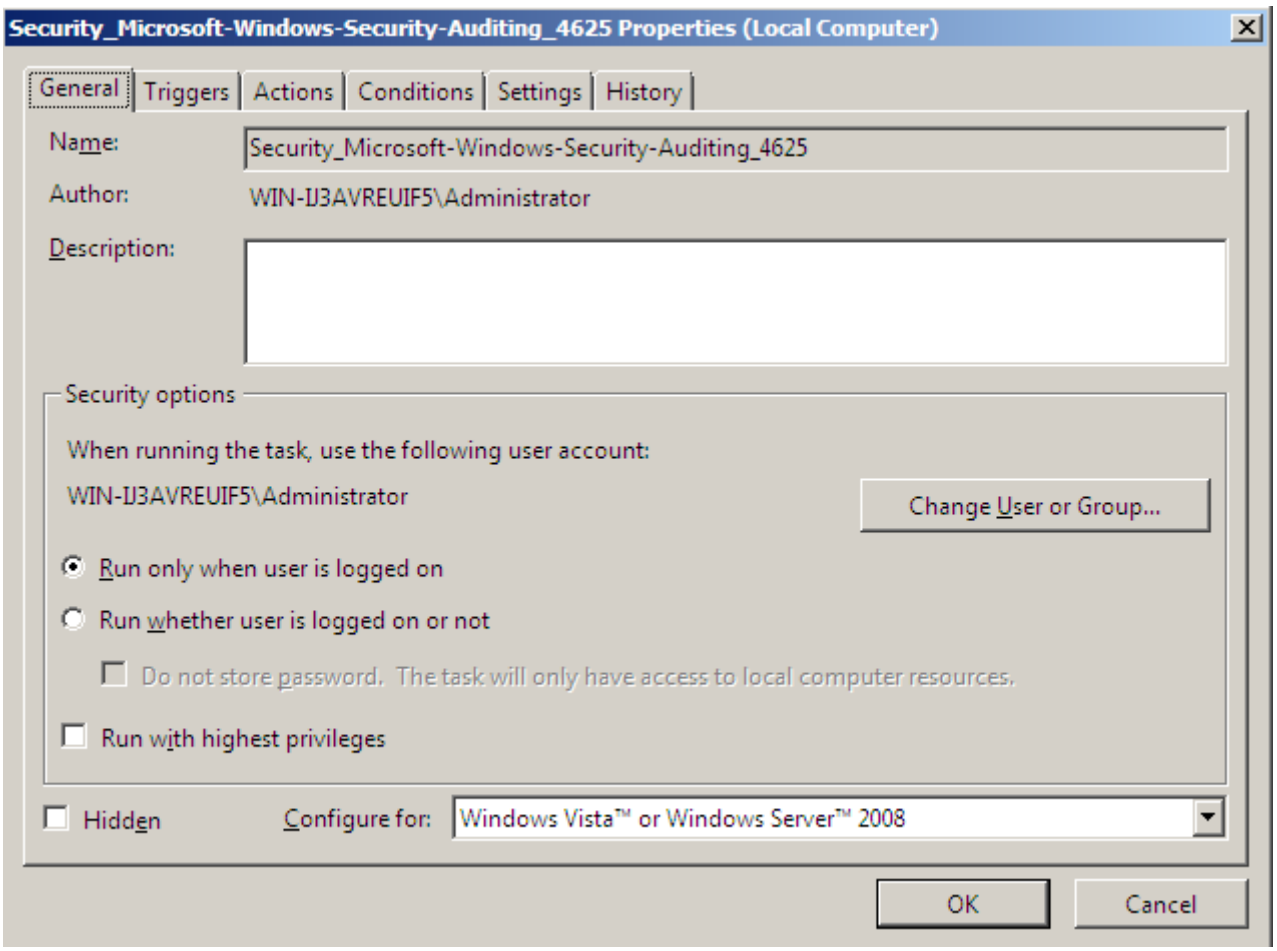


Рисунок 3.
Свойства задач

Окно свойств задачи аналогично интерфейсу Scheduled Tasks, для заданий, выполняющихся по расписанию. Здесь можно указать учетную запись, под которой выполняется задача, при необходимости ее можно выполнять только когда пользователь работает на машине.

В закладке Triggers, вы можете добавлять или изменять условия выполнения задачи. В Actions вы можете добавлять различные действия. В закладке Conditions прописаны условия, при которых выполняется задача. В Settings можно прописать, какие действия должны быть выполнены при различных условиях. Например, что нужно делать в случае, если такая задача уже выполняется. Наконец, в закладке History вы можете наблюдать все события, которые вызвали выполнение задачи.

Немного о построении отчетов

Иногда возникает необходимость в построении отчетов о событиях информационной безопасности. Например, руководители различного уровня очень любят, когда им предоставляют распечатки отчетов, в которых представлена информация, о том сколько попыток несанкционированного проникновения было осуществлено, к примеру за месяц. Благодаря отчетам многие руководители ИТ-отделов выбивают бюджеты на развитие, так что не стоит пренебрегать отчетами.

Итак, нам нужно осуществить выборку событий из журнала. Делать мы это будем с помощью средств PowerShell.

Для начала построим отчет о неудачных входах в систему. Для этого нам необходимо выбрать все события с кодом 4625.

```
get-eventLog -LogName Security -Newest 100 | Where-Object { $_.EventID -eq 4625 }
```

Еще один пример. Узнаем, сколько пользователей осуществляло вход в систему в нерабочее время. Код события Success Logon – 4624.

```
get-eventlog security | where
 {$_.EventId -eq 4624 -and
 ($_.TimeGenerated.TimeOfDay
 -gt '20:00:00' -or
 $_.TimeGenerated.TimeOfDay
 -lt '08:00:00' )}
```

В завершении, узнаем, сколько удачных входов систему было осуществлено пользователем administrator.

```
get-eventLog -LogName Security | Where-Object { $_.message -match 'administrator' -AND $_.EventID -eq 4624 }
```

Здесь приведены только простейшие сценарии работы с журналом событий в Windows Server 2008. При необходимости на их основе можно построить более сложные запросы для релшения соответствующих задач информационной безопасности.

Практическое занятие №18

Установка и настройка локального принтера. Настройка общего доступа к принтеру. Подключение к принтеру. Наблюдение и управление очередью печати. Создание пула принтеров.

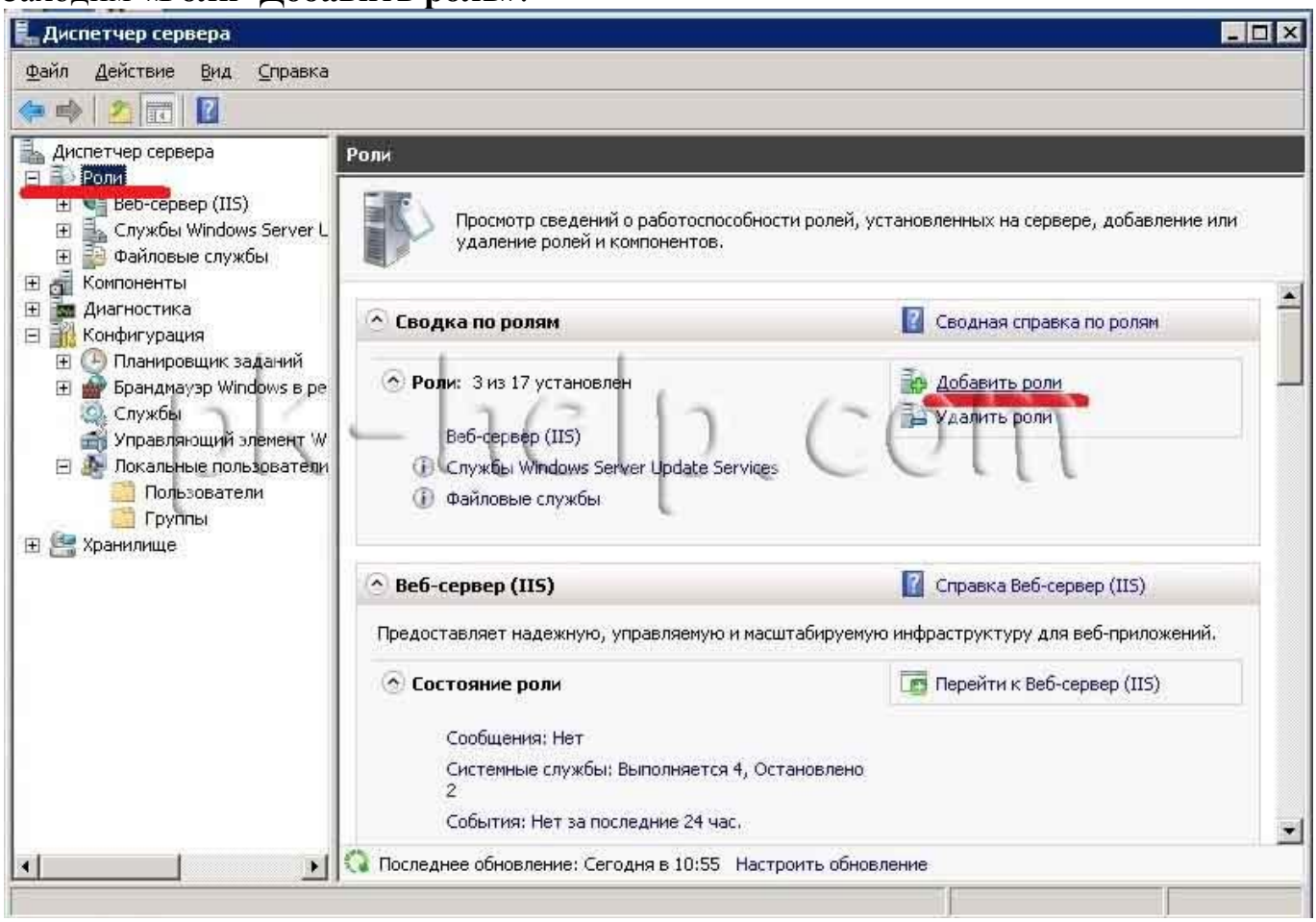
Цель: Установить и настроить принтер.

Настроить сетевой принтер через рабочую станцию весьма просто и легко , но у этого метода использования общего принтера есть свои минусы, например человек к которому локально подключен принтер и через который все печатают- выключил компьютер (или перезагрузил его)- всё!!!- сетевой принтер не доступен. К тому же, если к одному компьютеру подключено несколько принтеров и ими активно пользуются, возможно замедление работы компьютера к которому подключены принтеры, возможны сбои\ ошибки в работе принтеров. Исходя из этого, лучше использовать выделенный сервер (или компьютер с серверной операционной системой, например Windows Server 2003, 2008 (R2)). Зачастую маленькие организации используют **расшаривание принтеров, через рабочие станции**, а средние и крупные используют- выделенные сервера.

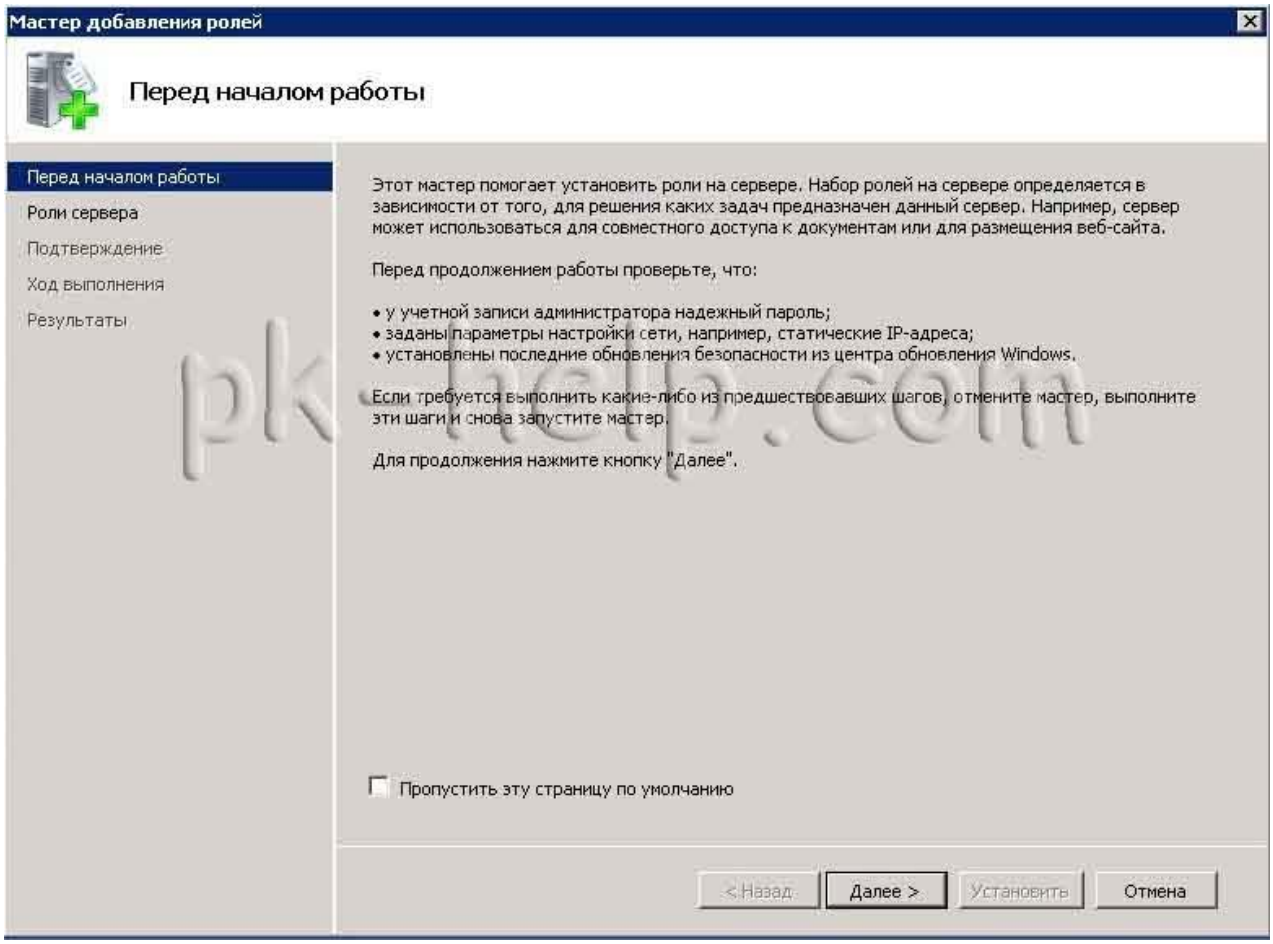
В этой статье я пошагово опишу, как настроить сетевой принтер на Windows Server 2008 R2.

Первым делом, для безотказной работы сетевых принтеров, необходимо установить роль печати. Для этого заходим в **«Диспетчер сервера»**, для этого нажимаем на панели на значок диспетчера сервера.

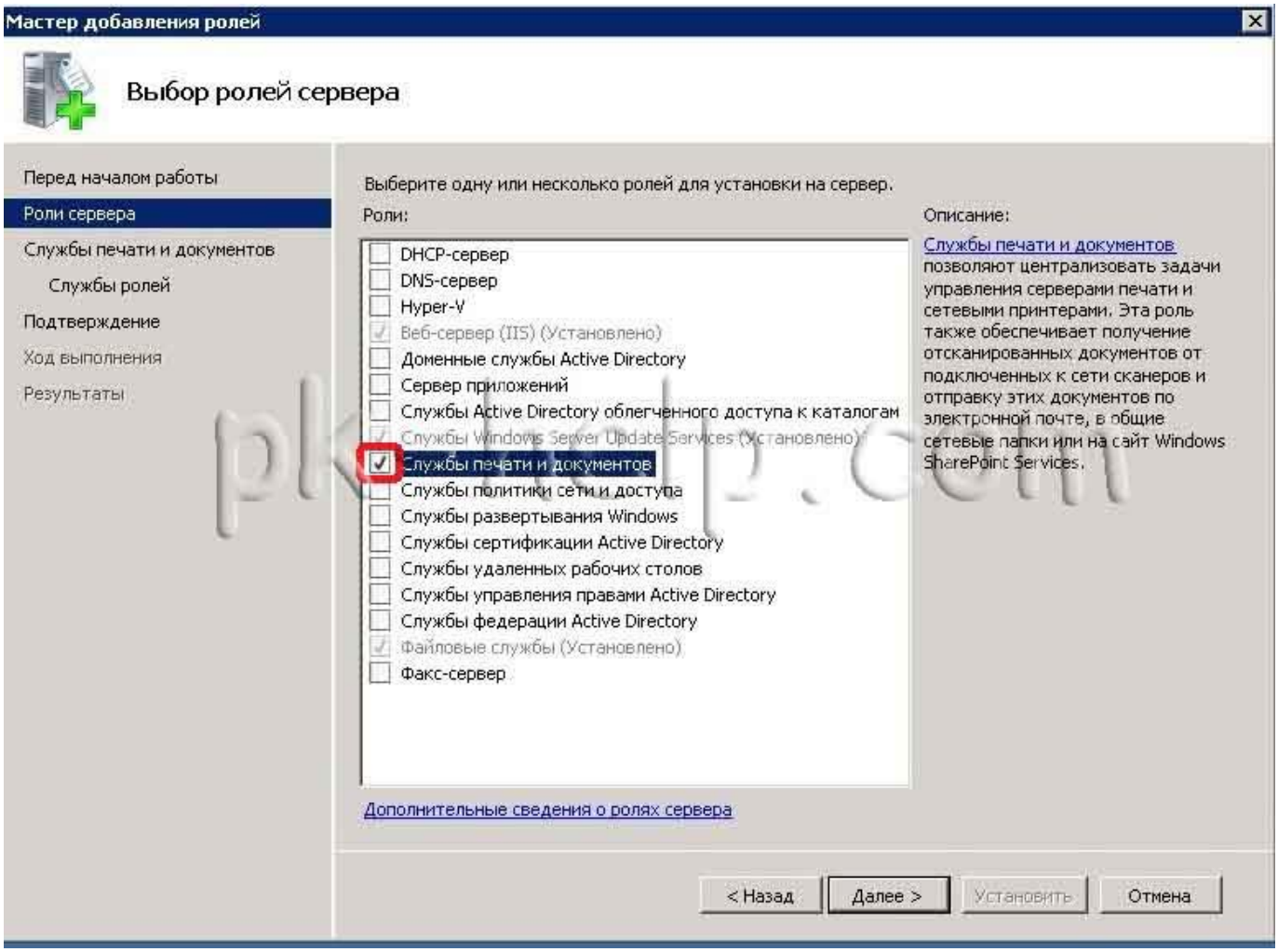
Заходим **«Роли- Добавить роль»**.



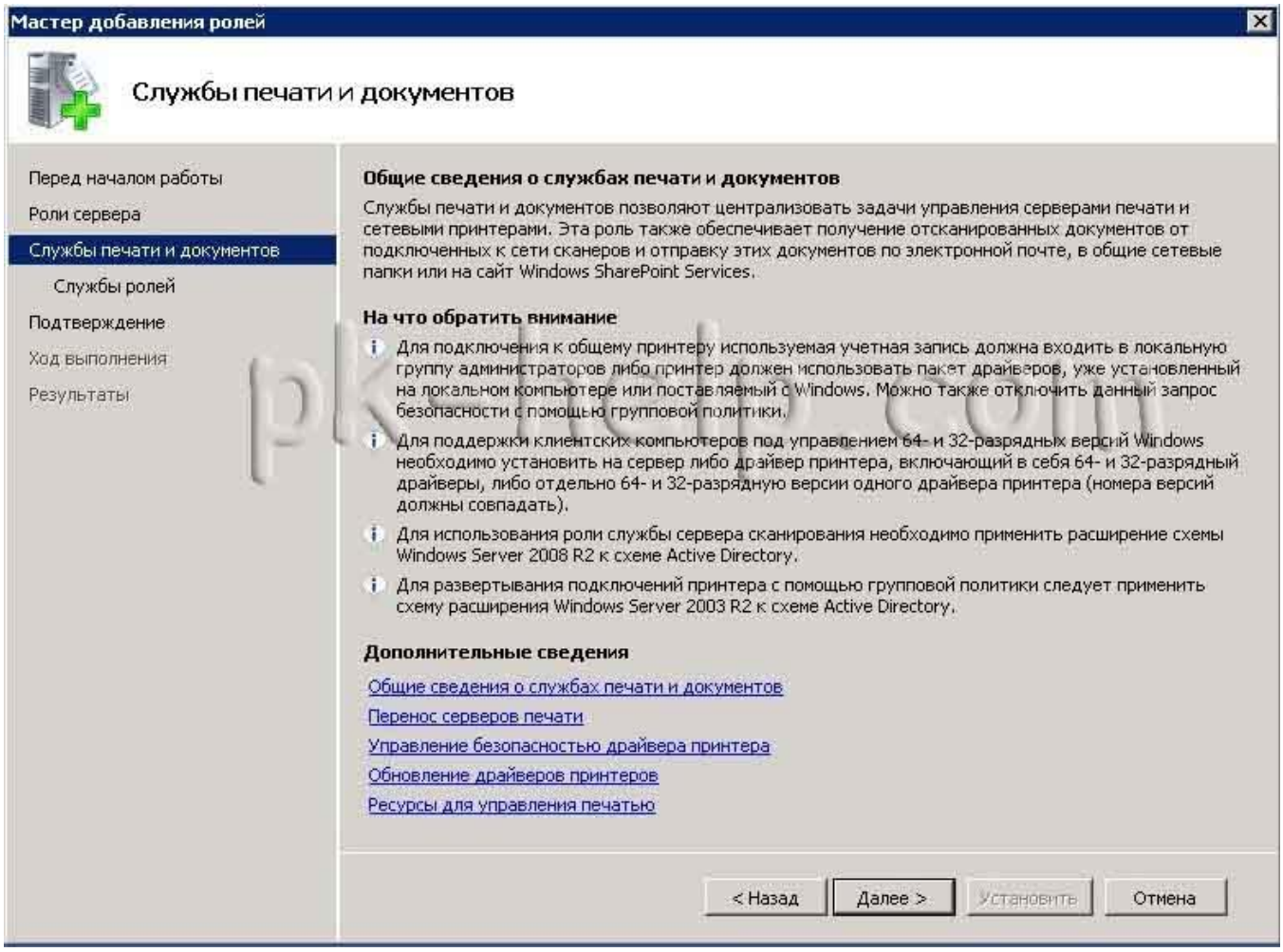
В следующем окне читаем служебную информацию, нажимаем **«Далее»**.



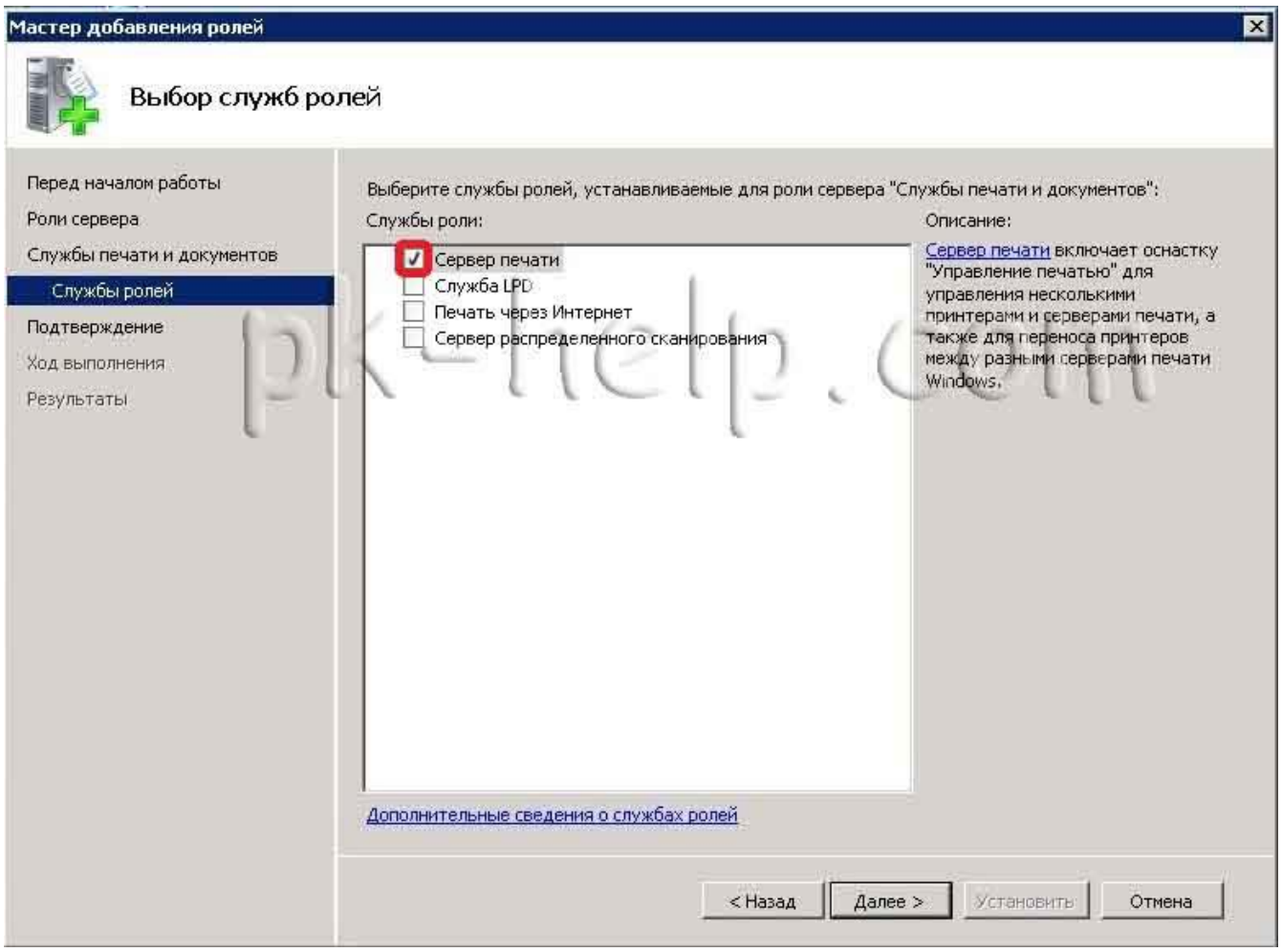
Выбираем интересующую нас роль **«Служба печати и документов»** и нажимаем **«Далее»**.



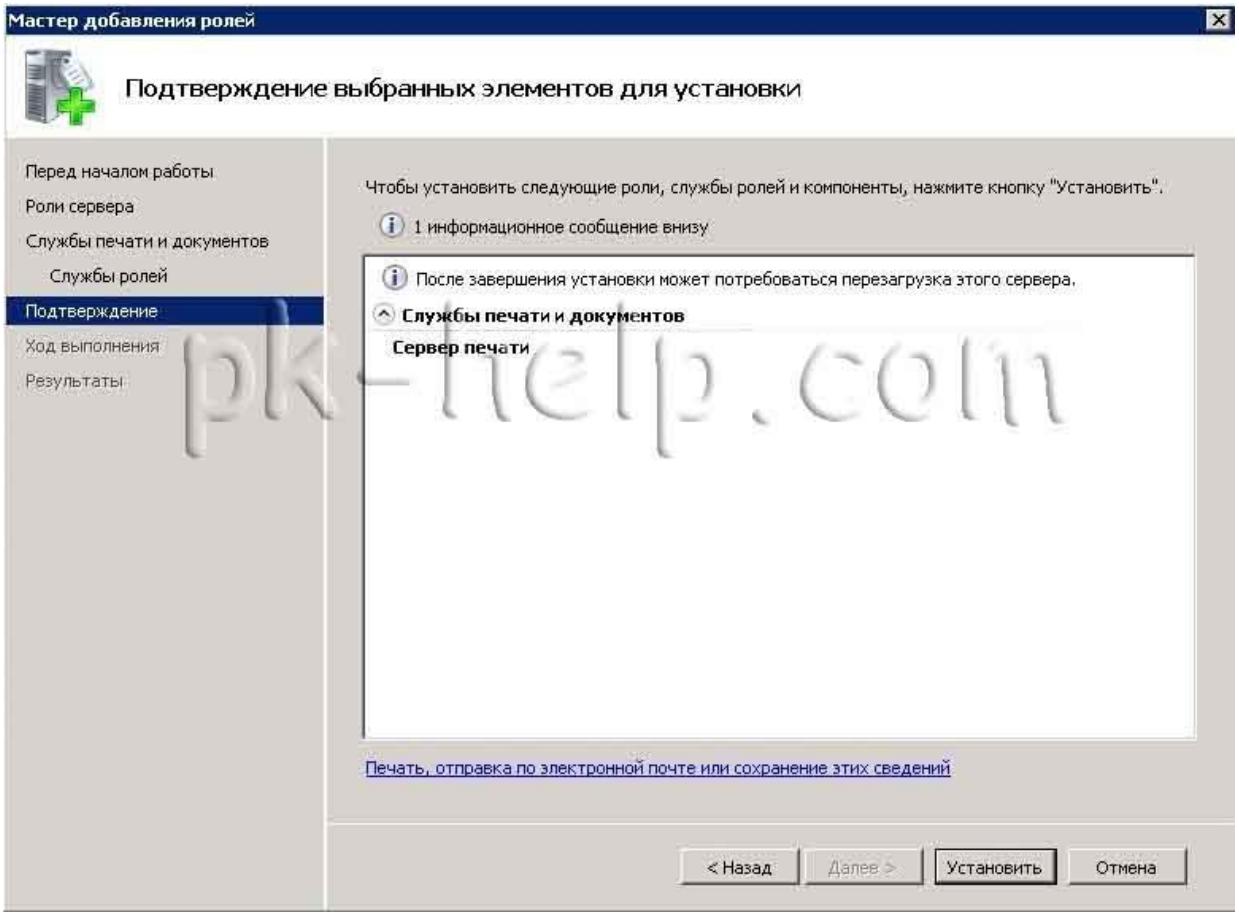
Читаем общую информацию о службе и нажимаем **«Далее»**.



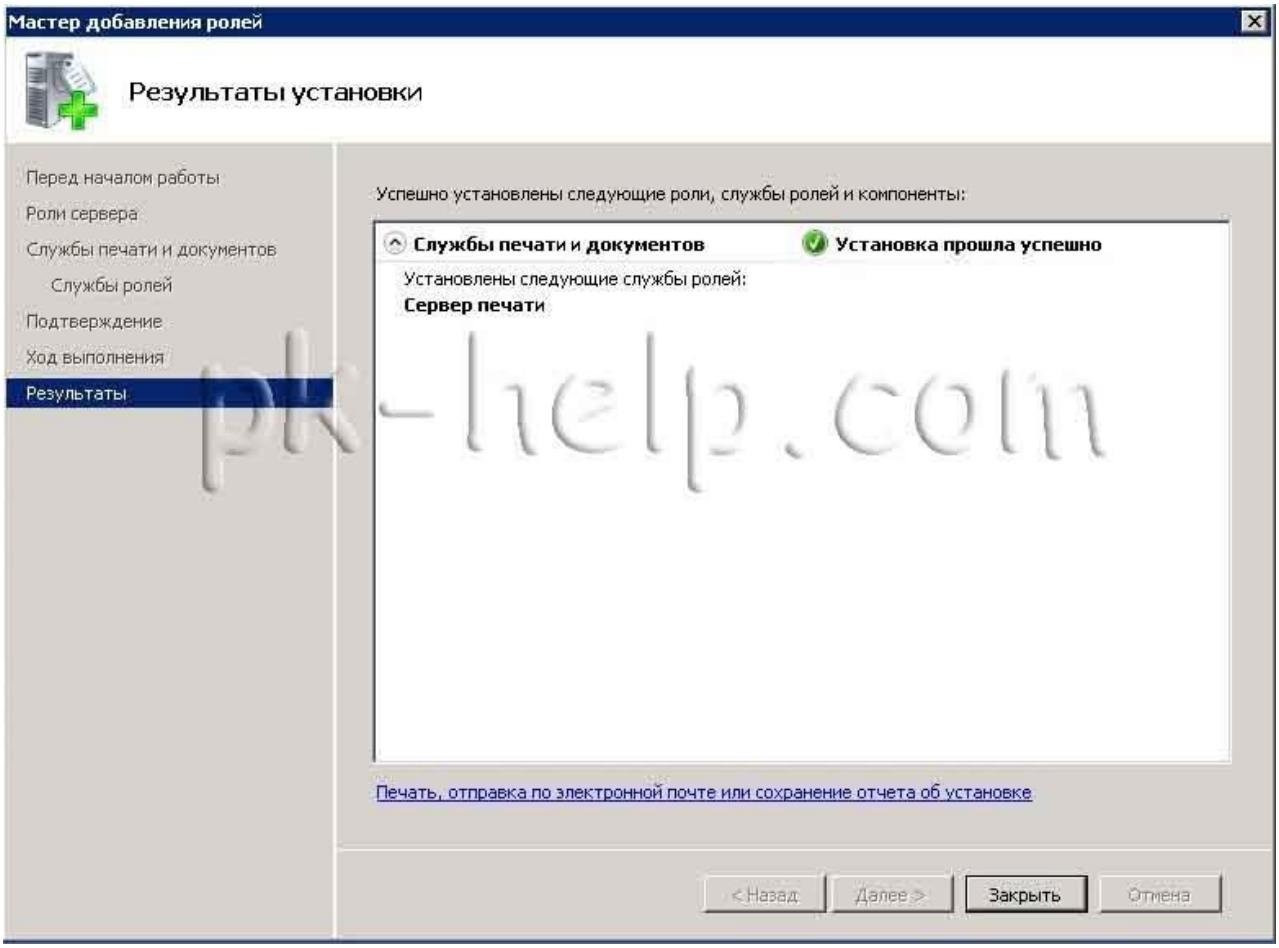
В следующем окне выбираем необходимые службы ролей, в данном примере нам хватит **«Сервера печати»**, выбираем его, нажимаем **«Далее»**.



Подтверждаем свой выбор нажатием кнопки **«Установить»**.

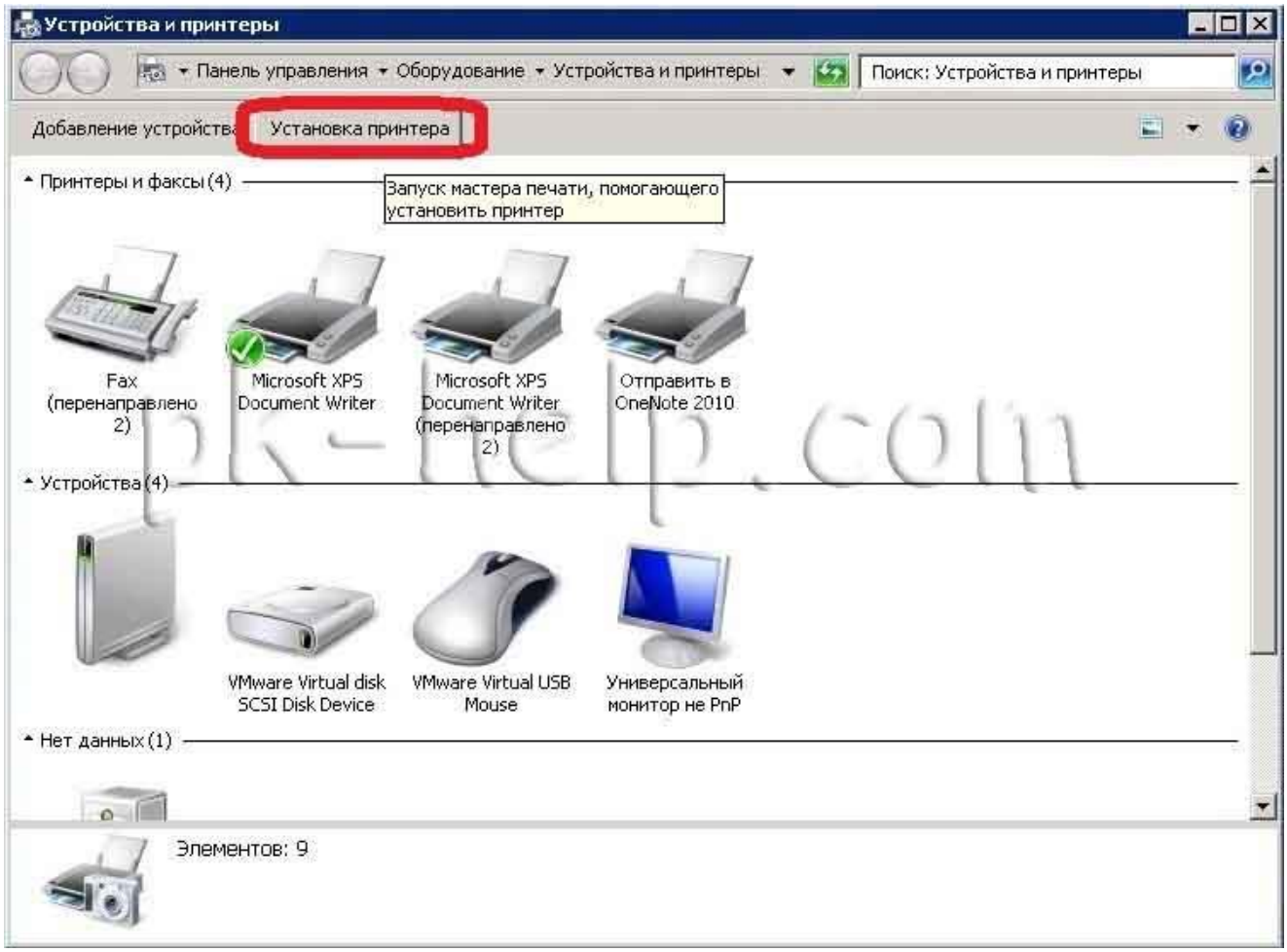


После этого идет процесс установки роли, ждем… если роль успешно установлена нажимаем **«Закрыть»**, иначе разбираемся почему не установилась роль и повторяем процедуру установки роли печати.

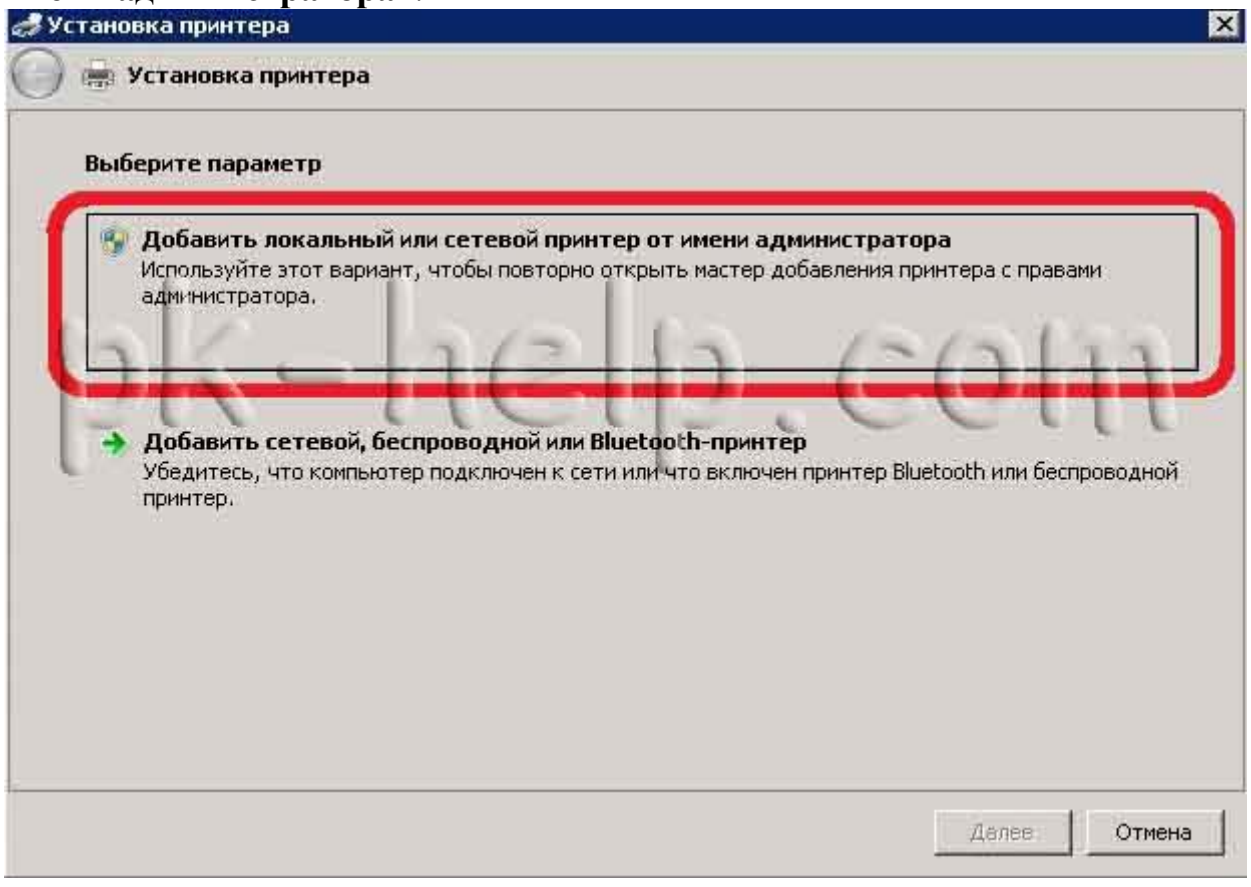


Теперь необходимо физически (с помощью сетевого кабеля или принт-сервера) подключить принтер к серверу и настроить работу принтера на сервере, для этого заходим **«Пуск- Устройства и принтеры»**.

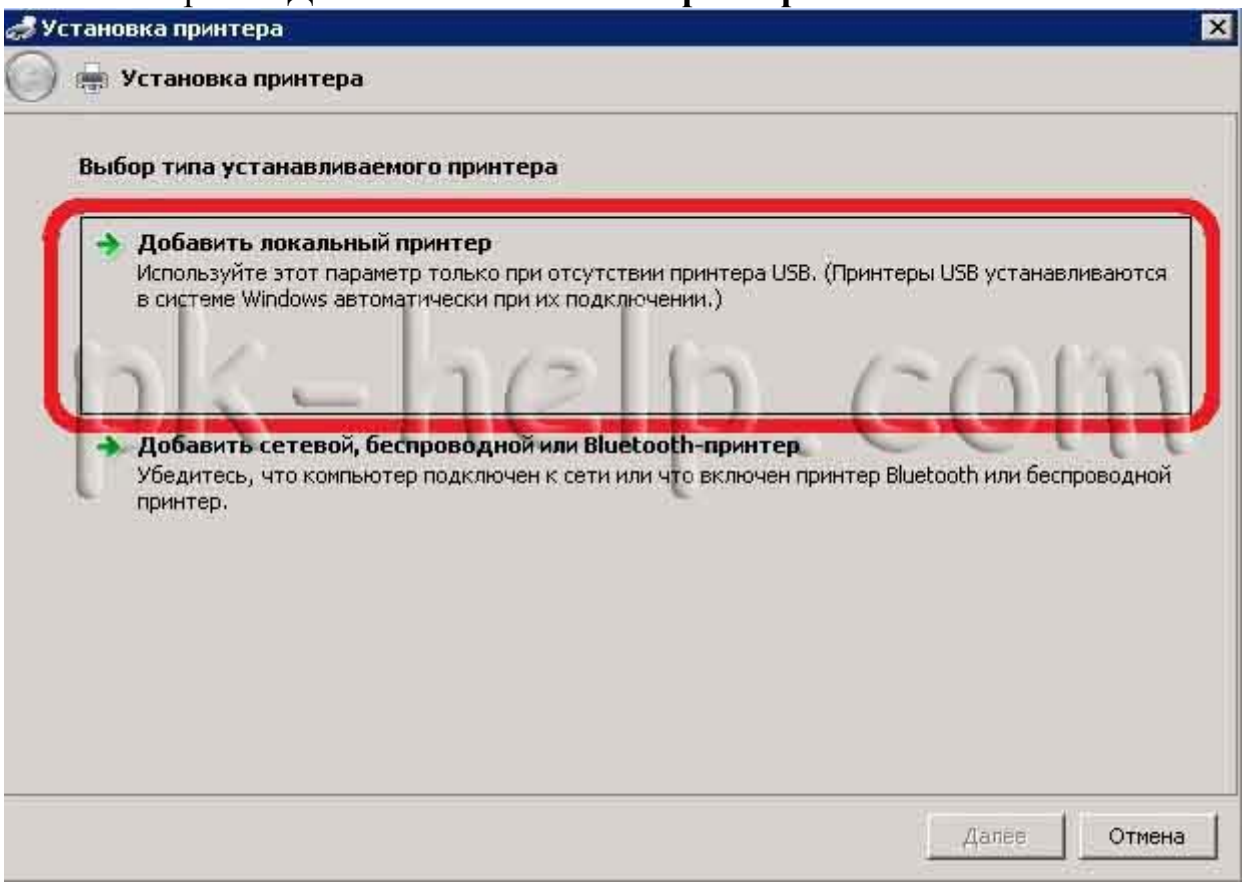
В окне Устройства и принтеры нажимаем **«Установка принтера»**.



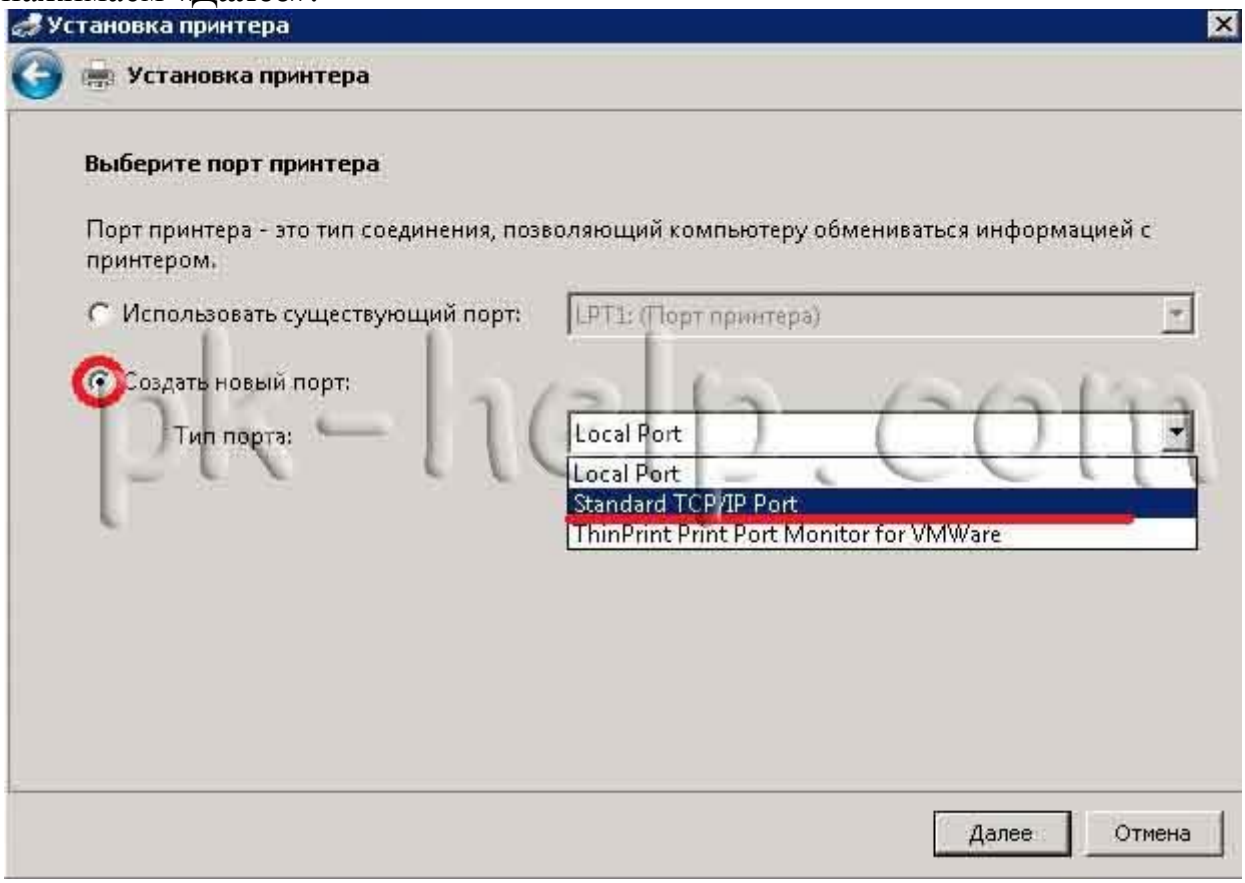
В следующем окне выбираем «**Добавить локальный или сетевой принтер от имени администратора**».



Затем выбираем **«Добавить локальный принтер»**.



Выбираем **«Создать новый порт» «Standard TCP/IP port»** и нажимаем **«Далее»**.



Прописываем IP адрес принтера. Если у вас возник вопрос – Как узнать IP

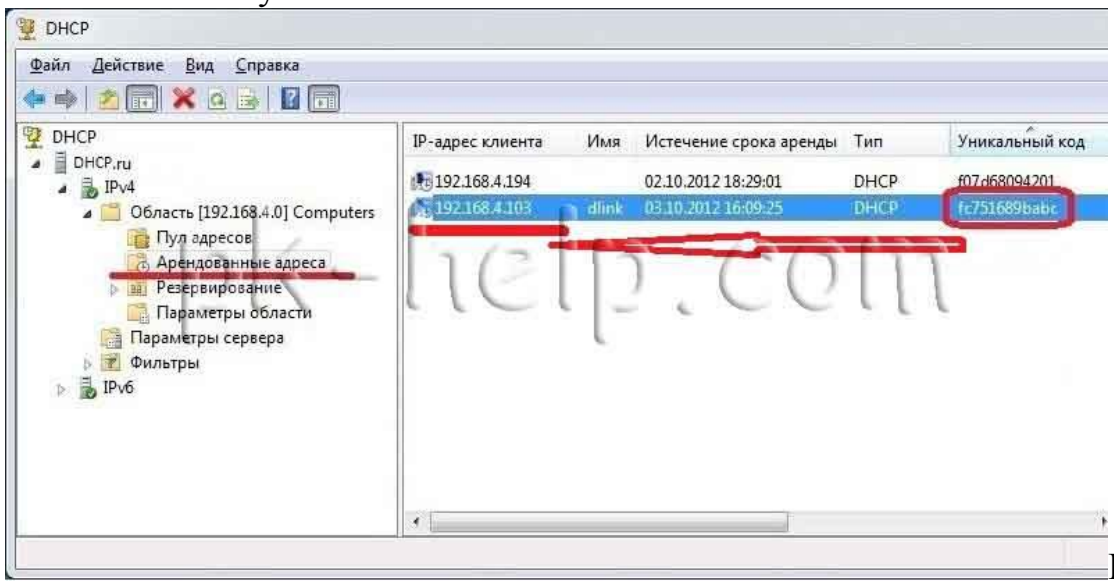
адрес принтера? Немного поясню. Сетевые принтеры подключаются двумя способами:

1) С помощью сетевого кабеля LAN (или Wi-Fi).
2) С помощью принт-сервера

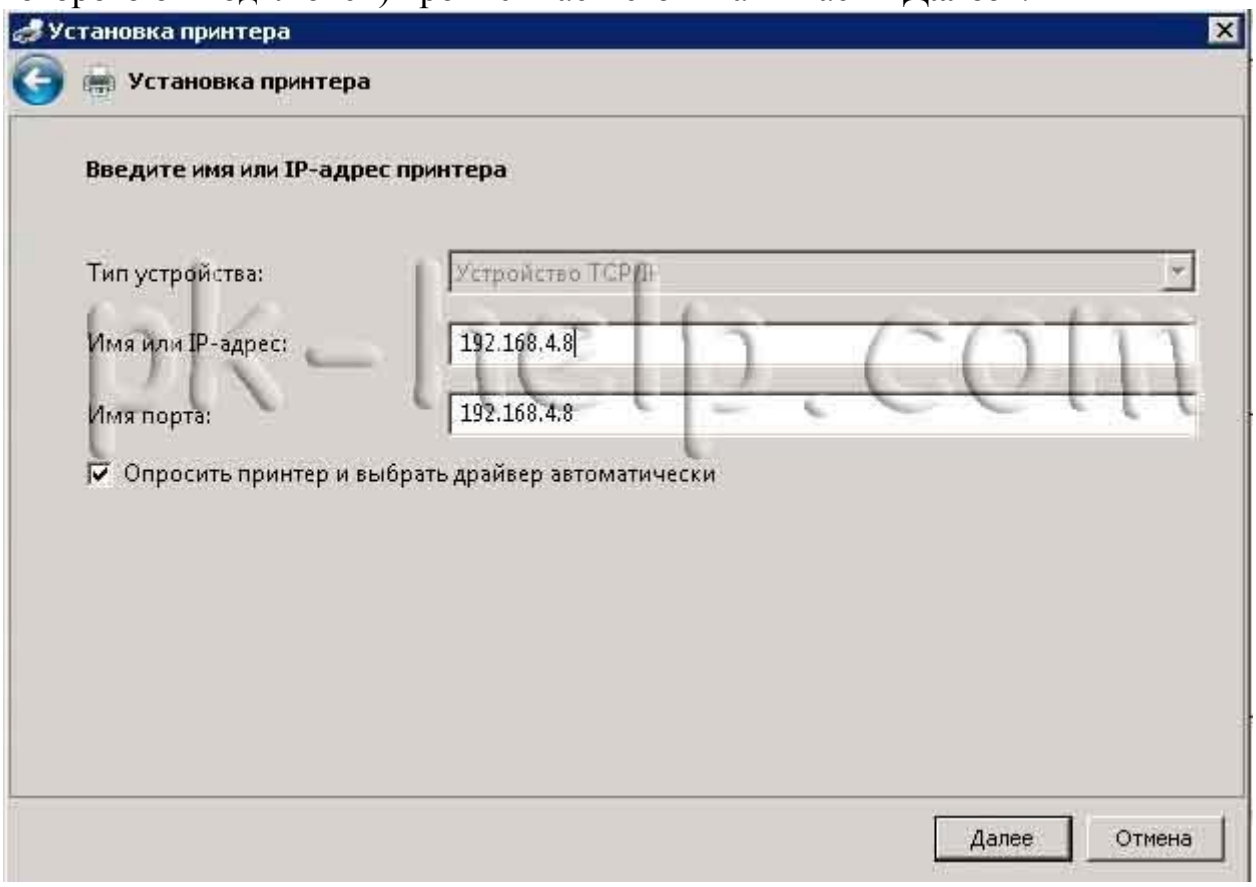
В первом способе IP адрес вручную прописывается в принтере (или принтер получает IP с помощью DHCP), соответственно узнать IP, можно на дисплее принтера, в настройках, либо нажав клавишу конфигурации? принтер распечатает всю служебную информацию в том числе и IP.
Во втором случае у вас должен быть DHCP сервер, что бы принт-сервер получил IP. После того как вы подключите принт-сервер в сеть и подключите к нему питание, посмотрите его MAC адрес на корпусе.


ACN 052 202 838
Z576
AR46
This Class B digital apparatus complies with Canada ICES-00
Cet appareil numérique de la class B est conforme à la norm
NMB-003 du Canada
P/N: RPR1020A2B...A2
S/N: PVUD2B9000300
H/W Ver.: A2 F/W Ver.: 1.00
MAC ID: FC751689BABC
Input: 5V/2.5A
Made in China
WARRANTY IS V
IF SEAL IS BR

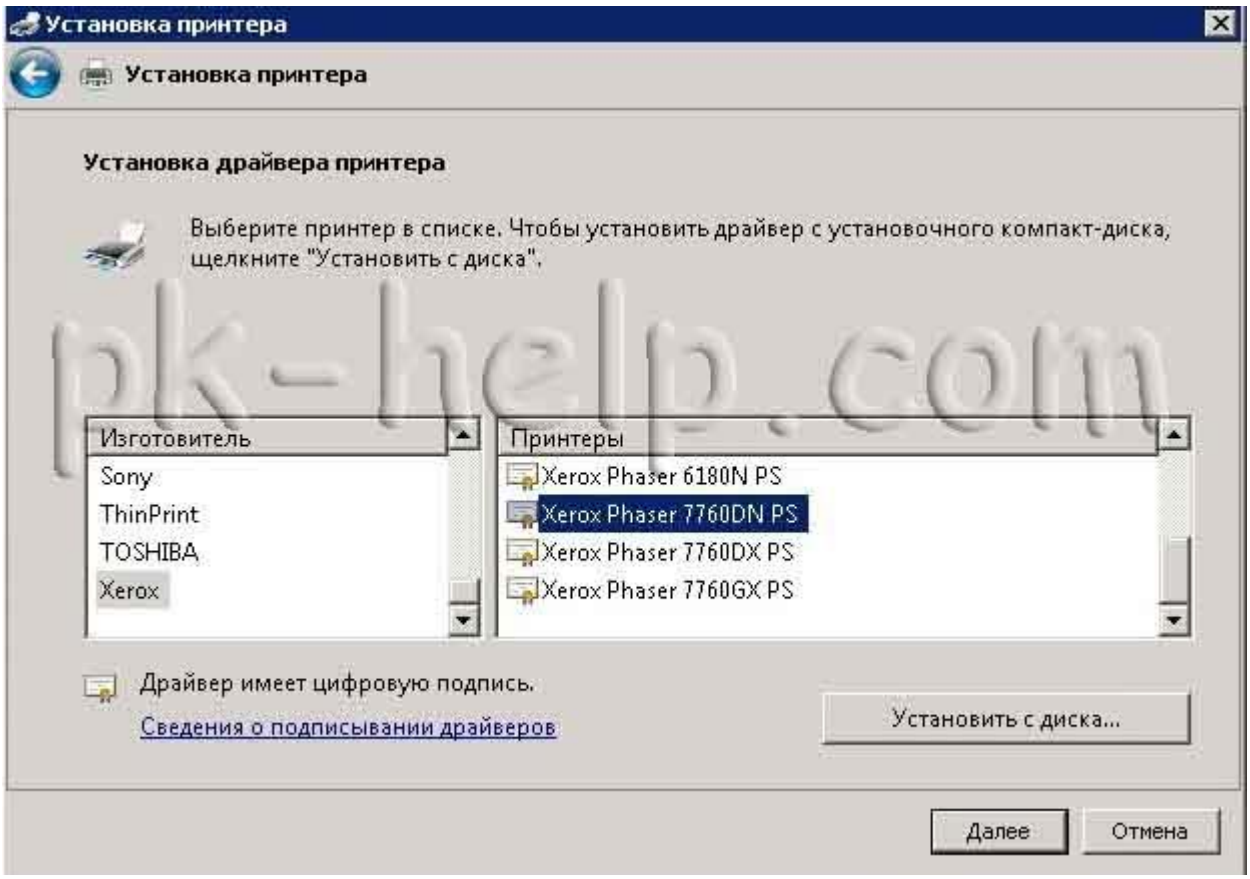
Зайдите на DHCP сервер и найдите ваш принт-сервер по MAC адресу и соответственно узнаете его IP.



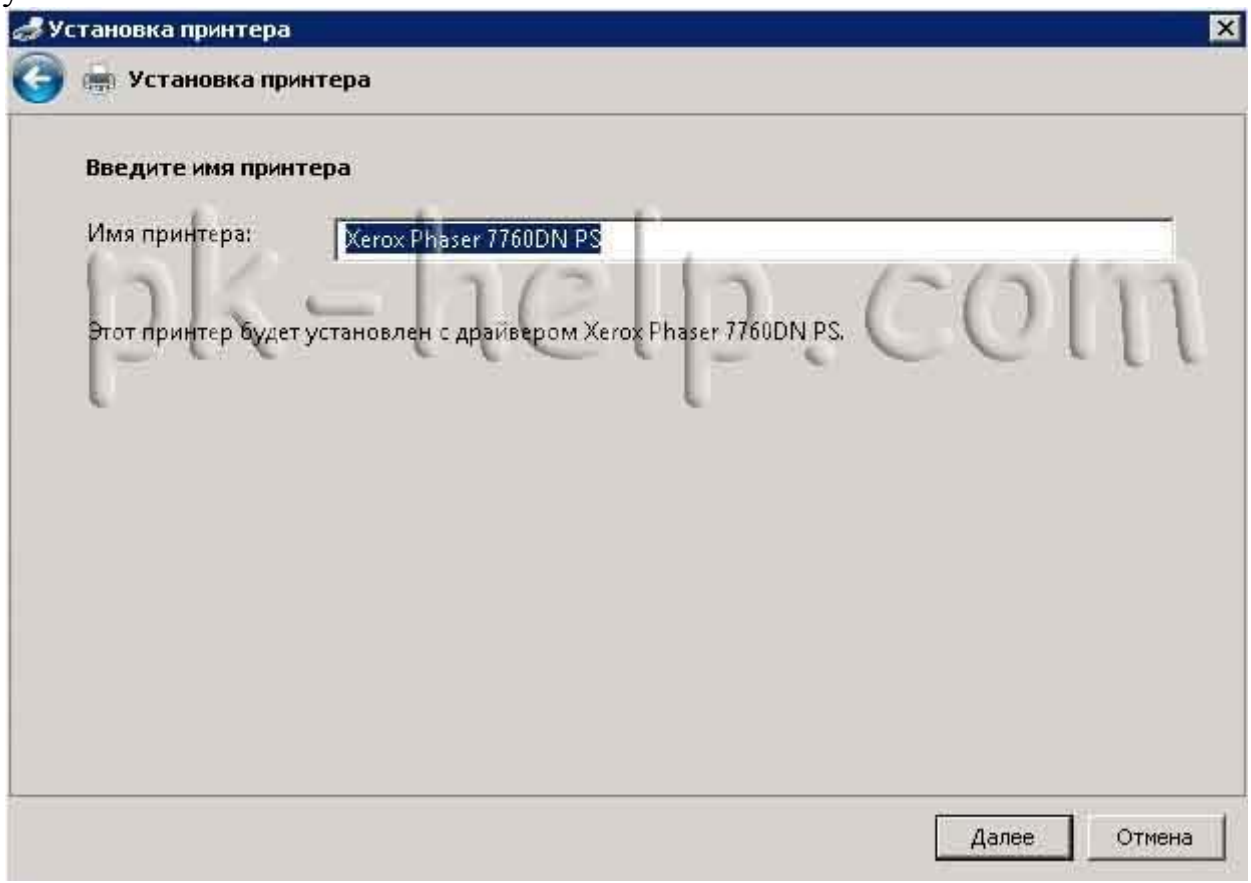
После того как вы узнали IP адрес принтера (или принт-сервера с помощью которого он подключен) прописываем его и нажимаем **«Далее»**.



После этого необходимо выбрать драйвер. В списке скорее всего не будет драйвера для вашего принтера (если есть, я вас поздравляю :)), драйвер необходимо скачать с сайта производителя принтера, установить его и выбрать его окне **«Установка драйвера принтера»**.

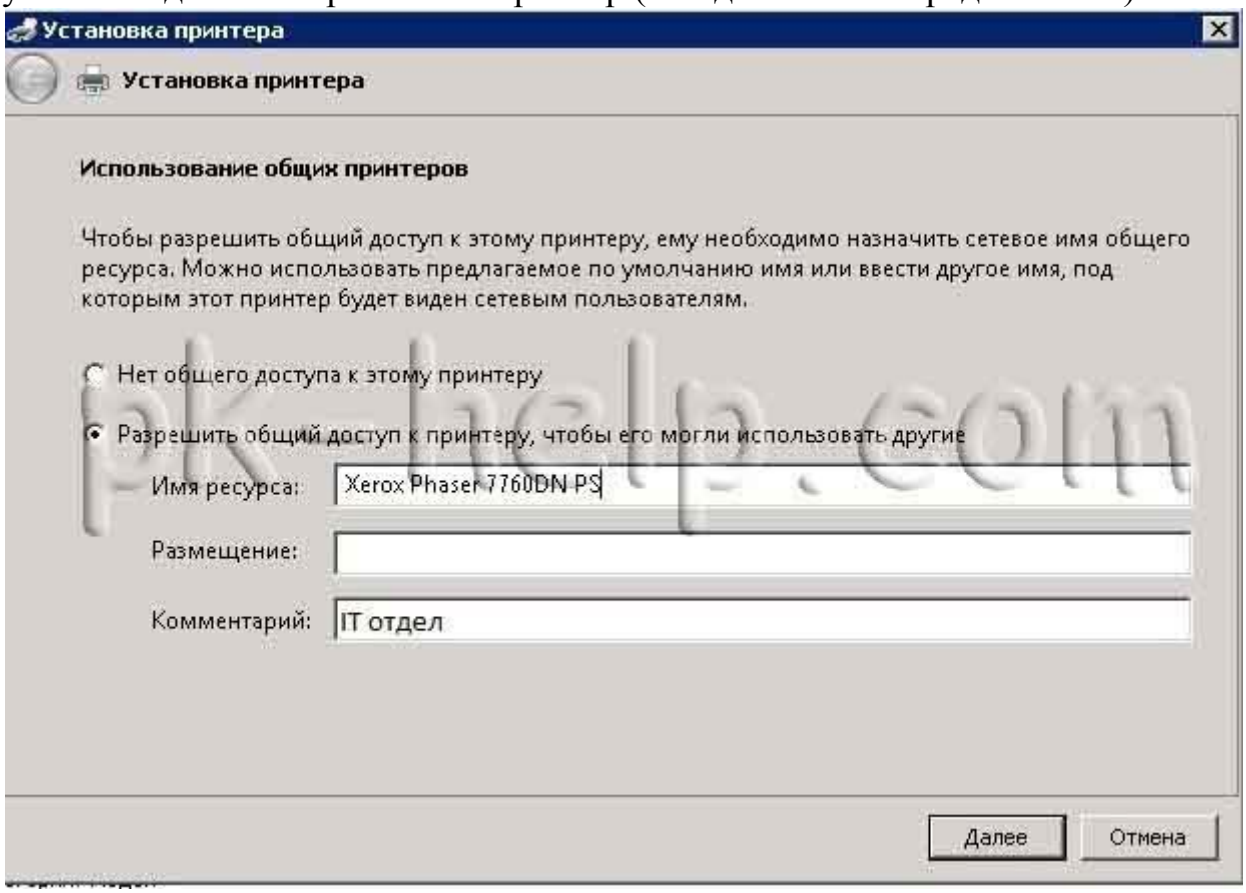


Указываем имя принтера или оставляем имя, которое пропишется по умолчанию.

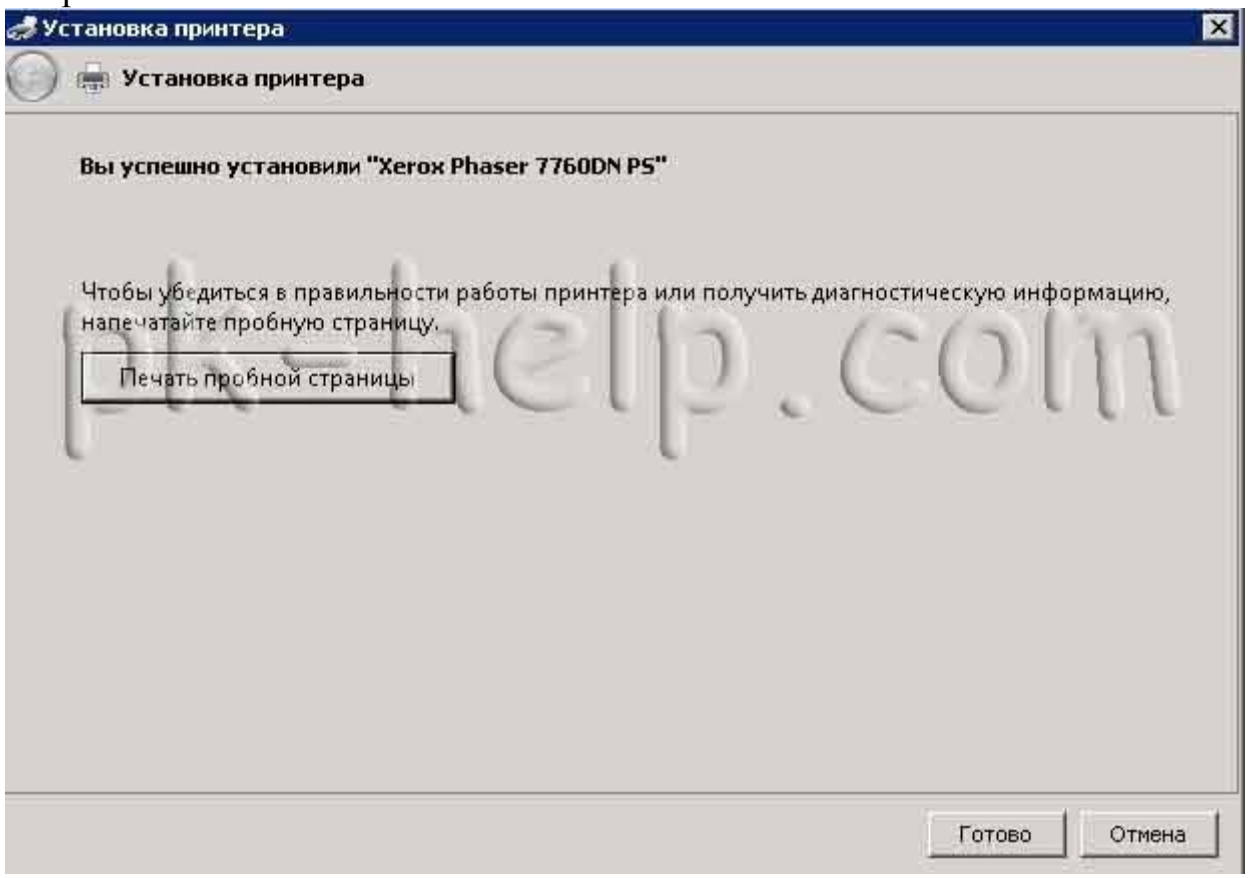


В следующем окне оставляем **«Разрешить общий доступ к принтеру, чтобы его могли использовать другие»** , если у вас будет несколько

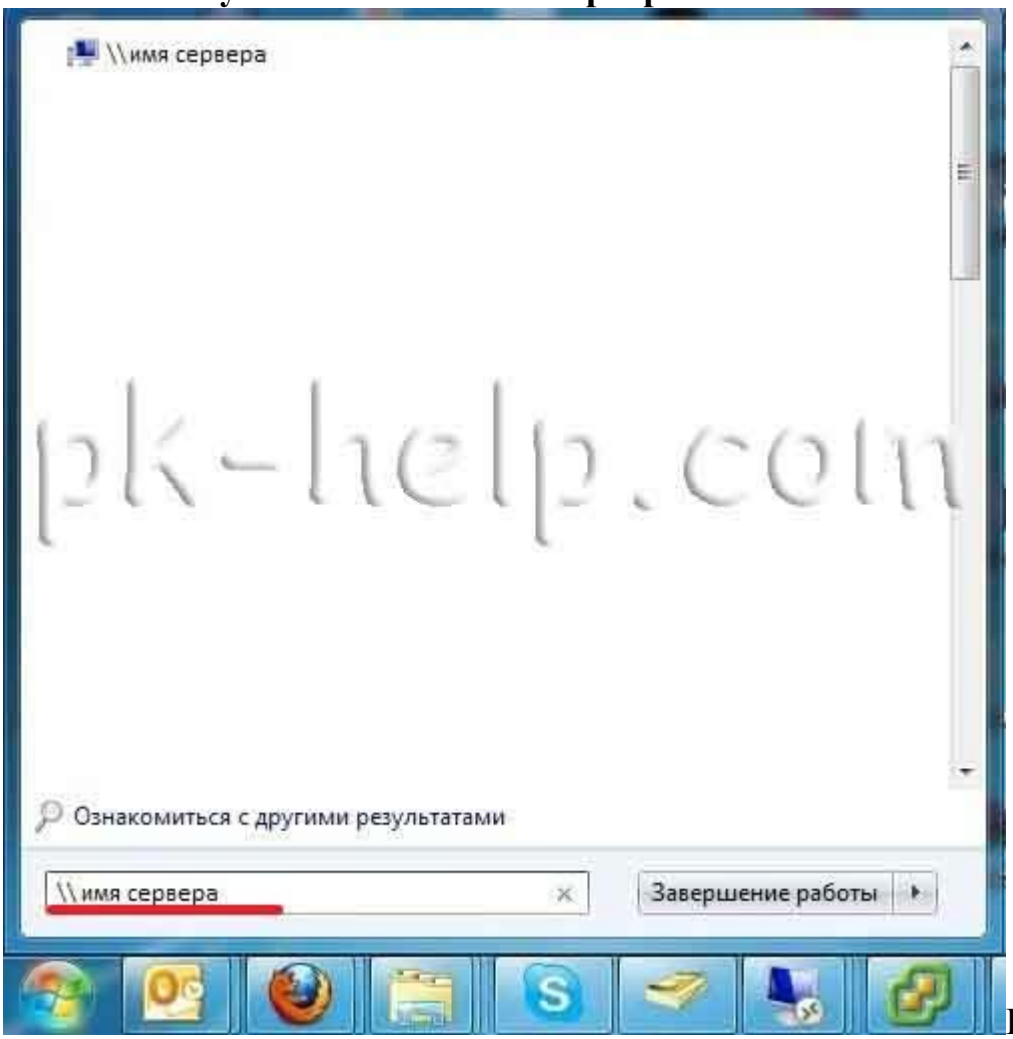
принтеров подключено к этому серверу, рекомендуется в комментарии указать отдел в котором стоит принтер (или для кого он предназначен).



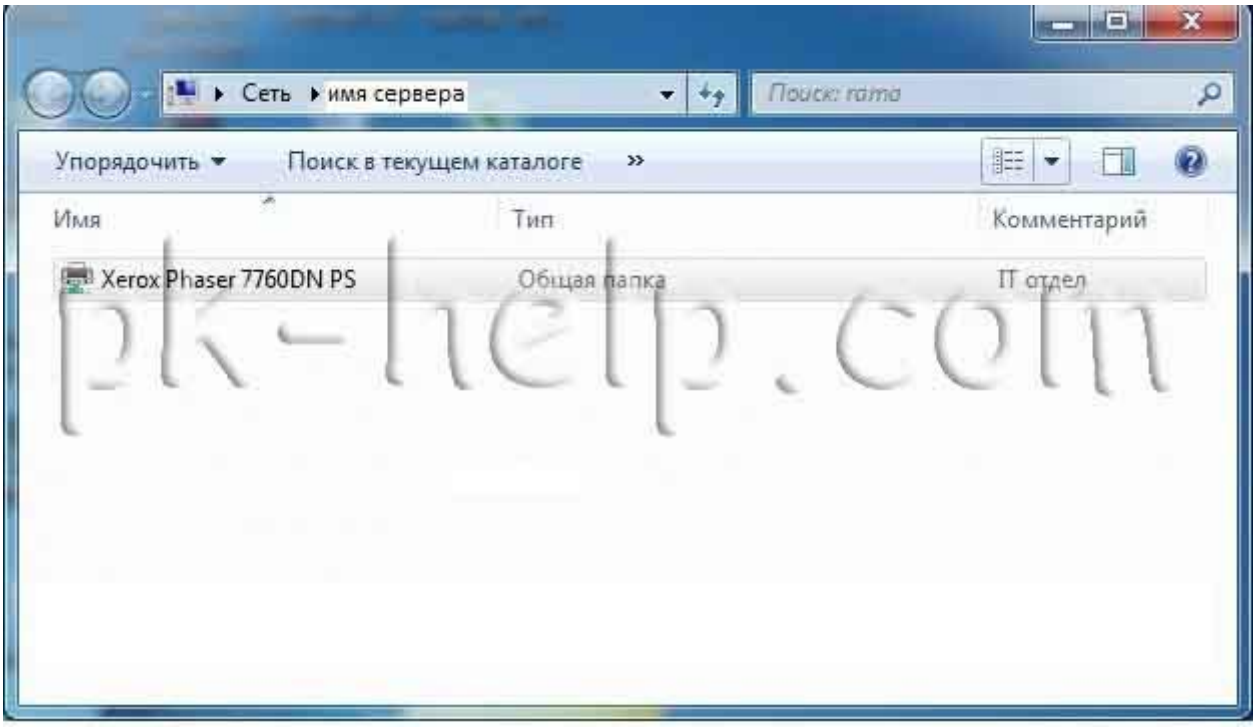
Печатаем пробную страницу, в качестве проверки, что драйвер подходит и все работает и нажимаем **«Готово»**.



Для того, что бы подключить принтер на компьютер (рабочую станцию), нажимаем **«Пуск» «\\имя вашего сервера»**.



Выбираем принтер, который необходимо подключить и кликаем на нем двумя кликами мыши.



После того как автоматически установились драйвера, заходим **«Пуск-Устройства и принтеры»** и видим сетевой принтер.

Практическое занятие №19.

Организация подключения созданной сети к сети Интернет.

Цель: Подключить компьютер к сети Интернет.

Чтобы любой компьютер (и виртуальный тоже) домашней сети, имел доступ в Интернет, необходим DNS-сервер и маршрутизатор для этой сети. DNS-сервер транслирует доменные имена в реальные IP адреса. А маршрутизатор пересылает пакеты из локальной сети во внешнюю сеть - Интернет.

Примечание. Маршрутизатор это русское название роутера.

В Интернет компьютер выходит через DNS сервер и маршрутизатор которые находятся в сети провайдера. Можно нескольким компьютерам обеспечить выход в Интернет через ресурсы провайдера но для этого необходимо заключить соответствующий договор с провайдером. Чтобы использовать только одно подключение к провайдеру для выхода в Интернет нескольких компьютеров необходимо иметь свой собственный маршрутизатор с двумя сетевыми интерфейсами - один подключённый к сети провайдера, второй - к локальной сети. В этом случае провайдер видит только наш маршрутизатор, а структура локальной сети для него закрыта.

В качестве маршрутизатора может использоваться готовое устройство (роутер) или компьютер с настроенными соответствующими службами.

Готовый роутер хорош для небольших сетей тем, что очень лёгок в настройке и стоит намного дешевле отдельного компьютера. Для сетей которым требуется большая производительность необходим отдельный сервер, например на Linux / Unix.

Компьютеры, подключенные к одной локальной сети, должны иметь одну и ту же маску (например, 255.255.255.0), тогда как IP-адрес у каждого компьютера должен быть свой, например, адрес может иметь следующий вид: 192.168.x.x, где x - цифра от 0 до 254. Оптимальная последовательность использования адресов для подключения компьютеров - 192.168.0.1, 192.168.0.2 и т.д.

Примечание: Не используйте IP-адрес 127.0.0.1, т.к. при обращении к нему вы фактически обращаетесь к своему компьютеру. Это так называемый "адрес-петля".

Пример сети показан на Рис. 1. Домашняя сеть - 192.168.1.0/255.255.255.0. Роутер - 192.168.1.1, выступает DNS-сервером и маршрутизатором сети. Параметры Интернет, которые дал провайдер, настраиваются внутри роутера. Они зависят от провайдера и типа подключения. А у всех компьютеров локальной сети они будут одинаковыми:

IP адрес - 192.168.1.2-254

Маска подсети - 255.255.255.0

DNS - 192.168.1.1

Шлюз, роутер - 192.168.1.1

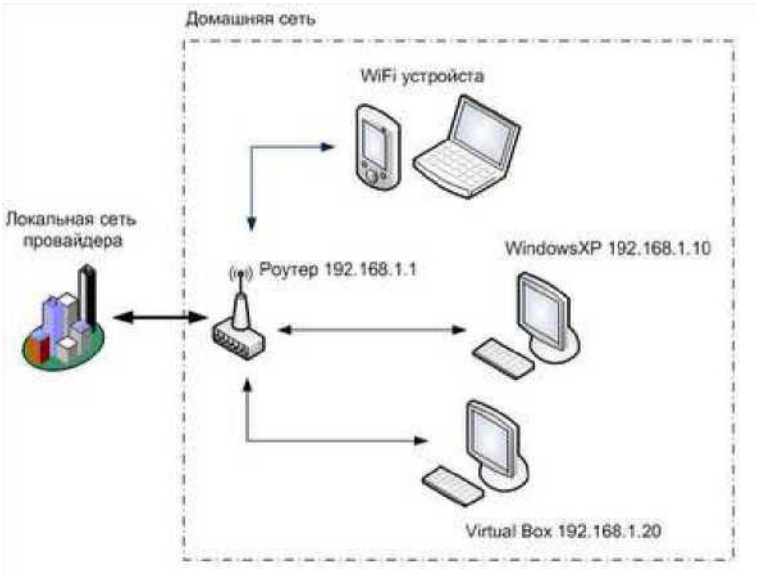


Рис. 1. Пример сети с маршрутизатором.

Можно и не настраивать у всех компьютеров параметры вручную, почти все роутеры имеют DHCP сервер.

Без использования роутера компьютеры два или несколько компьютеров можно объединить в локальную сеть, один из которых может иметь доступ в

Интернет напрямую, а остальные - через первый компьютер. Эти варианты и рассматривается в этой работе.

НАЗНАЧЕНИЕ DNS СЕРВЕРА.

DNS-сервер предназначен для того чтобы по имени домена определить IP-адрес сервера на котором находится сайт, связанный с этим доменом. Собственно информация о привязке имени к IP указывается в настройках DNS-сервера. Если основной DNS-сервер (master dns) по каким-то причинам окажется неработоспособен, то обращение для определения IP-адреса по имени будет производиться к дополнительному DNS-серверу (slave dns), что повышает надежность при определении IP-адреса сайта. Теоретически чем больше (но не менее двух) DNS-серверов хранит данные об IP-адресе сайта, тем лучше. Однако если не работает сервер на котором находится сайт, обилие DNS не поможет увидеть сайт.

Предположим у сайта есть доменное имя, например: forum.searchengines.ru. Для того чтобы создать сетевое соединение с тем сервером на котором находится forum.searchengines.ru, необходимо знать IP-адрес этого сервера. При обращении из браузера к сайту forum.searchengines.ru ОС вашего компьютера определяет IP-адрес сервера на котором расположен forum.searchengines.ru, обращаясь к DNS-серверу вашего Интернет-провайдера, который в свою очередь обращается к "авторитетному" DNS-серверу, отвечающему за зону forum.searchengines.ru (хранящему данные об IP-адресе, связанном с именем forum.searchengines.ru). После определения IP-адреса, браузер устанавливает сетевое соединение с сервером на котором живет forum.searchengines.ru. Браузер посылает HTTP- запрос web-серверу.

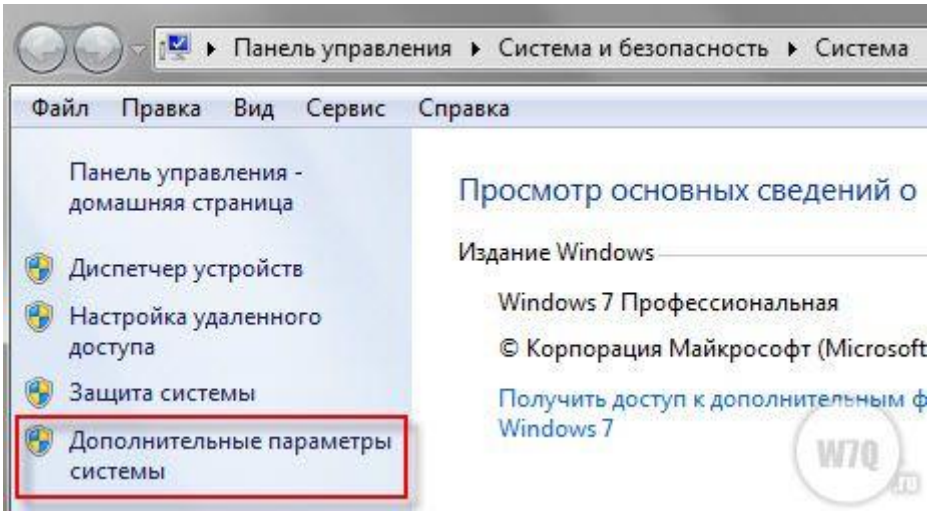
Практическое занятие №20.

Организация удаленного доступа из сети Интернет к информационным ресурсам, расположенным в созданной сети.

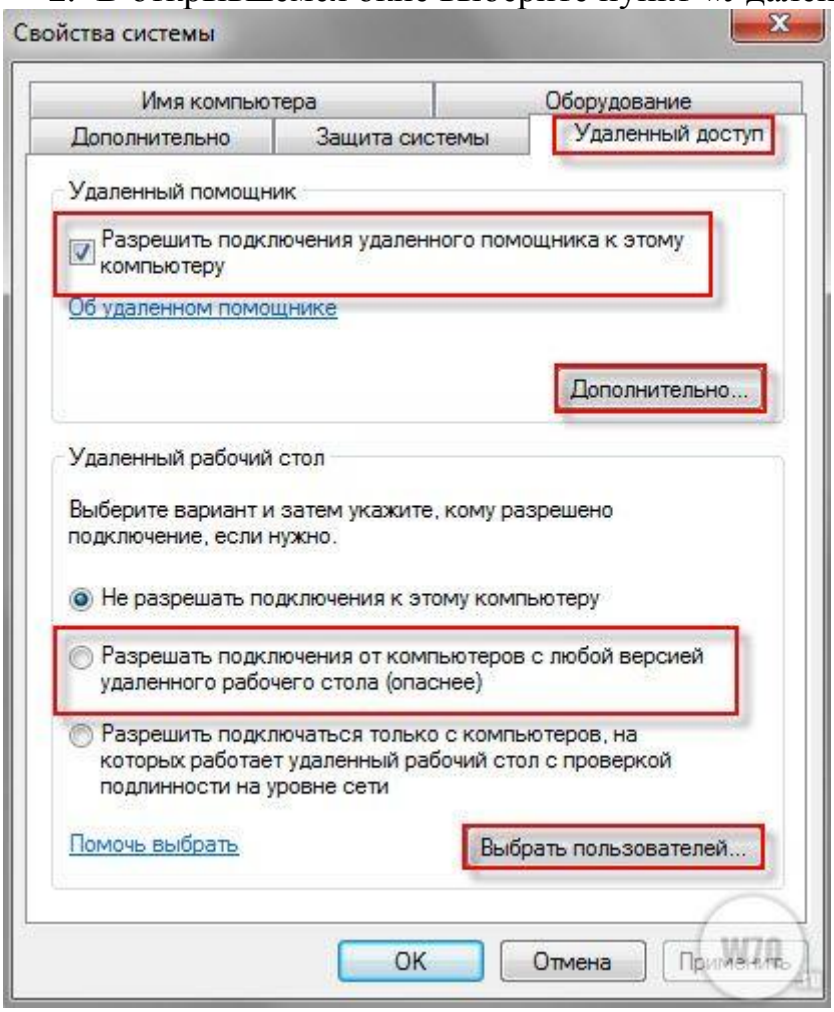
Цель: Организовать удаленный доступ.

Что бы включить удаленный доступ на компьютере под управлением Windows 7

1. Зайдите в свойства компьютера (или перейдите в «Панель управления» -> «Система») и выберите пункт «Дополнительные параметры системы»:



2. В открывшемся окне выберите пункт «Удаленный доступ»:



3. Поставьте галку напротив пункта «Разрешить подключение удаленного помощника к этому компьютеру». Это автоматически добавит исключение в брандмауэр Windows.

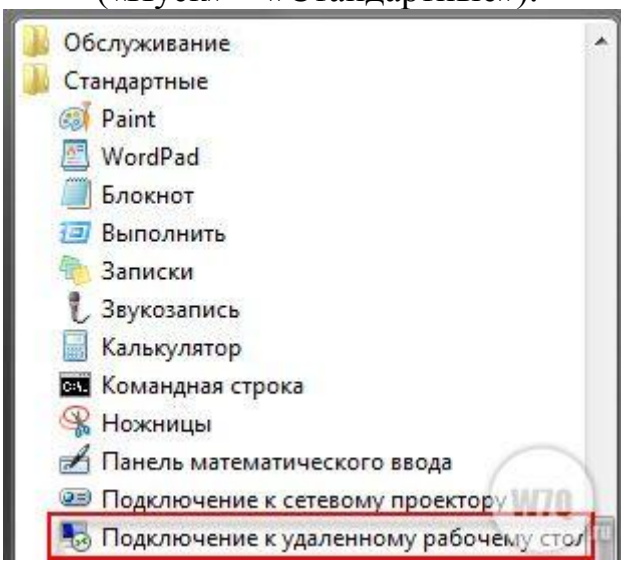
4. Выбрав «Дополнительно» вы можете настроить разрешать или нет удаленное управление компьютером (по-умолчанию «разрешать») и срок в течение которого будет поддерживаться подключение сеанса (по-умолчанию 6 часов).
   Если вы запретите удаленное управление компьютером, то после подключения вы не сможете никаким образом управлять содержимым компьютера, а будете только видеть переданное вам изображение.
5. В разделе «Удаленный рабочий стол» выберите «Разрешать подключения …».
6. Нажмите на кнопку «Выбрать пользователей» и добавьте пользователей, которые будут иметь удаленный доступ к компьютеру. Учтите: пользователям с «пустыми» паролями запрещены удаленные подключения не зависимо от установленных разрешений. Задайте такому пользователю пароль или создайте отдельного пользователя со сложным паролем для этих целей.
7. Нажмите «ОК» для завершения настроек.

Что бы подключиться к компьютеру с включенным удаленным доступом

Что бы подключиться к такому компьютеру, вам необходимо знать IP адрес компьютера или имя компьютера в сети.

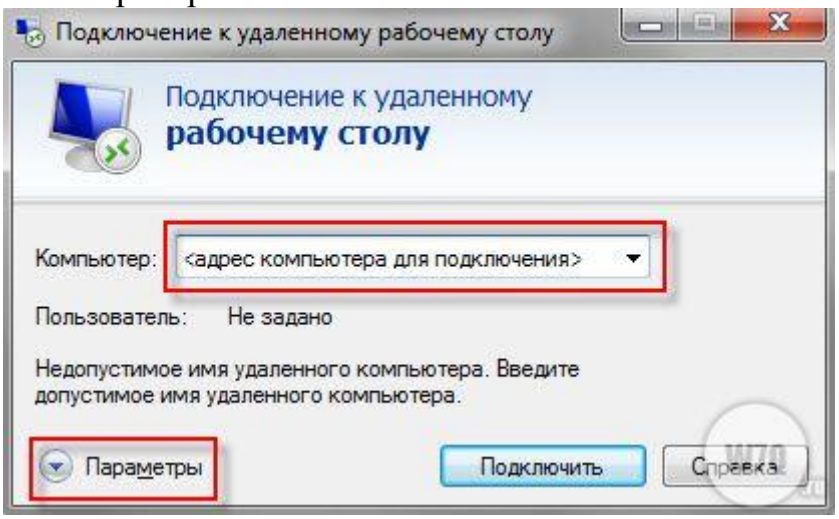
Что бы узнать IP адрес, запустите командною строку и в ней выполните команду «ipconfig». Найдите в появившемся списке ваше подключение (обычно «подключение по локальной сети» или «беспроводное подключение») и посмотрите IPv4-адрес — это и будет необходимый вам набор цифр.

1. Запустите на компьютере с которого хотите получить удаленный доступ, программу «Подключение к удаленному рабочему столу» («Пуск» ->»Стандартные»).



Настройка терминального доступа к Windows 7

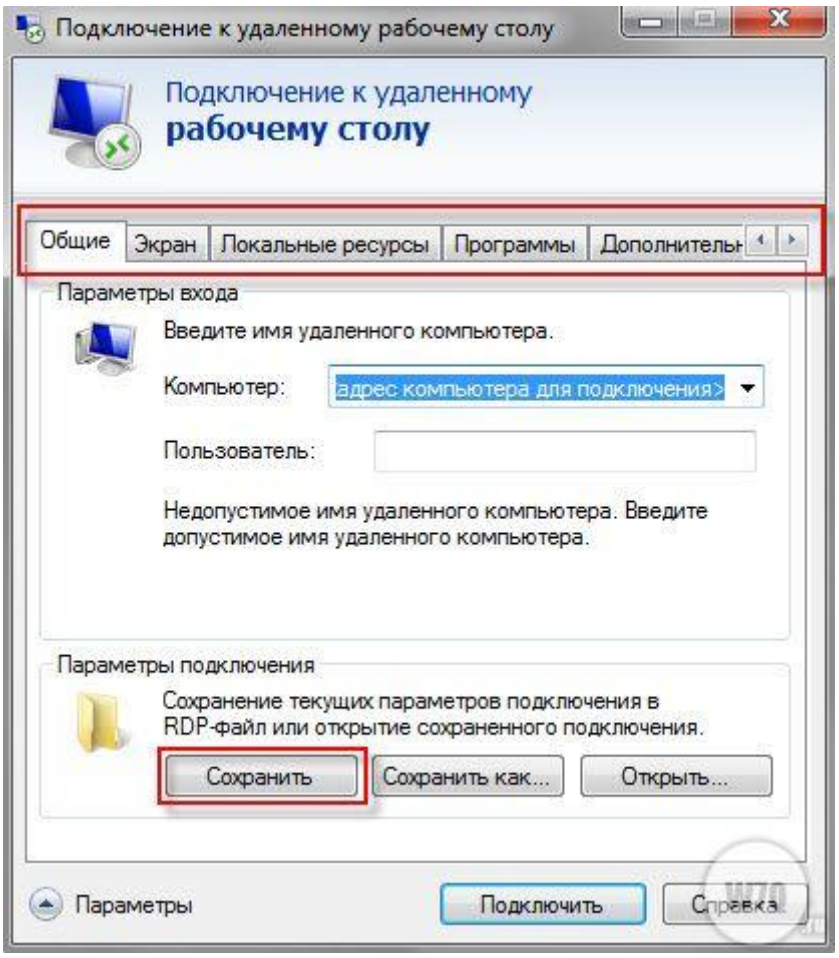
2. В открывшемся окне задайте адрес компьютера к которому планируете подключение (IP-адрес или имя) и нажмите «Подключить» для проверки связи.



Настройка терминального доступа к Windows 7

Если все нормально, вы увидите окно с предложением ввести логин и пароль для подключения к компьютеру.

3. Перед подключением вы можете настроить разнообразные параметры, нажав на соответствующую кнопку (см. рисунок выше). В этом случае откроется панель настроек удаленного доступа:



Настройка терминального доступа к Windows 7

Несколько слов о закладках:

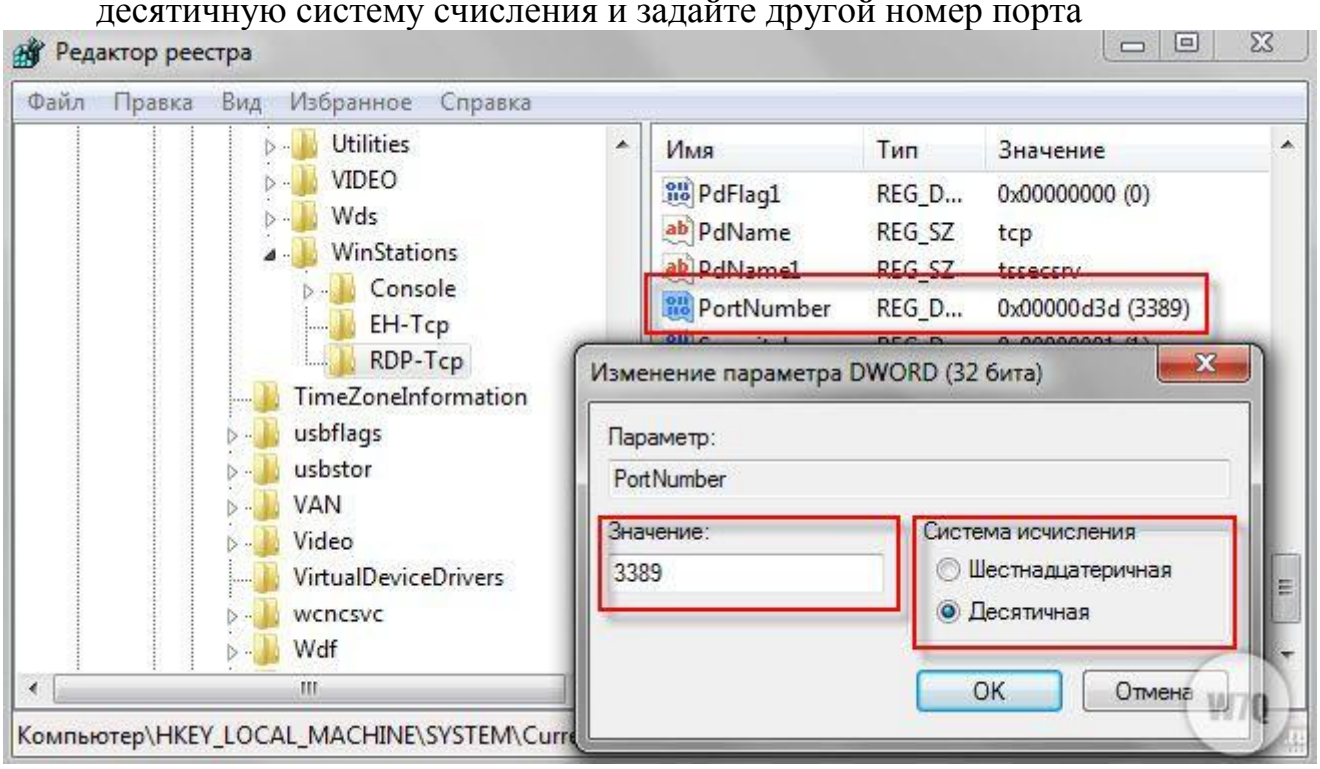
- **Общие**. Вы можете задать имя и адрес подключения, а так же сохранить настройки в виде файла. В последнем случае вам не придется каждый раз запускать программу, достаточно будет запустить сохраненный файл со всеми настройками.
- **Экран**. задаются свойства экрана: разрешение (по-умолчанию полный экран), количество цветов.
- В **локальных ресурсах** вы можете настроить передачу звука по сети (по-умолчанию разрешено), использование сочетания клавиш и самое интересное: доступ к локальным ресурсам компьютера с которого происходит подключение. В последнем случае вы можете разрешить доступ к принтерам, дисководам и жестким дискам, которые будут доступны вам при работе на удаленном компьютере (например, если вы разрешите доступ к диску C, то после установки соединения, он появится на удаленном компьютере в списке устройств и вы сможете обмениваться файлами с удаленным компьютером).
- **Программы** служат для настройки автоматического запуска программ после подключения.

- В закладке «**Дополнительно**» вы можете задать профили для подключений и вручную настроить визуальные эффекты, доступные вам после подключения.
- В закладке «**Подключение**» можно изменить настройки оповещений и безопасности.

Некоторые дополнительные не документированные настройки

Как я уже говорил выше, подключение происходит по протоколу RDP, а для подключения используется порт 3389. что бы изменить номер порта (а это может быть полезно, если ваш компьютер напрямую включен в интернет), необходимо сделать следующее:

1. Запустите редактор реестра «Regedit» (Win+R -> Regedit).
2. Перейдите в ветку реестра**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumber**
3. Дважды щелкните мышью по записи «PortNumber», переключитесь в десятичную систему счисления и задайте другой номер порта



Настройка терминального доступа к Windows 7

Крайне рекомендуется задавать номер больше 1024, а лучше в промежутке от 49152 до 65535 (максимально возможный номер).

4. Помните, что после изменения номера порта, необходимо:

- Внести изменения в фаервол, открыв доступ из внешней сети к новому порту.

- Подключение производить к адресу компьютера + :<новый номер порта>. Например: 192.168.1.100:55600. Это связано с тем, что если явно не указать номер порта, программа для удаленного доступа будет пытаться соединиться по порту 3389.

Практическое занятие №21.

Внедрение основных Интернет - сервисов (антивирусное ПО, обмен файлами, гипертекстовые и почтовые серверы).

Цель: Внедрить основные интернет - сервисы

Постоянное развитие информационных технологий приводит к появлению разнообразных информационных ресурсов, отличающихся друг от друга формами представления и методами обработки составляющих их информационных объектов. Поэтому в настоящее время в Интернет существует достаточно большое количество сервисов, обеспечивающих работу со всем спектром ресурсов. Наиболее известными среди них являются:

- электронная почта (E-mail), обеспечивающая возможность обмена сообщениями одного человека с одним или несколькими абонентами;
- телеконференции, или группы новостей (Usenet), обеспечивающие возможность коллективного обмена сообщениями;
- сервис FTP – система файловых архивов, обеспечивающая хранение и пересылку файлов различных типов;
- сервис Telnet, предназначенный для управления удаленными компьютерами в терминальном режиме;
- World Wide Web (WWW, W3) – гипертекстовая (гипермедиа) система, предназначенная для интеграции различных сетевых ресурсов в единое информационное пространство;
- сервис DNS, или система доменных имен, обеспечивающий возможность использования для адресации узлов сети мнемонических имен вместо числовых адресов;
- сервис IRC, предназначенный для поддержки текстового общения в реальном времени (chat);

Перечисленные выше сервисы относятся к стандартным. Это означает, что принципы построения клиентского и серверного программного обеспечения, а также протоколы взаимодействия сформулированы в виде международных стандартов. Следовательно, разработчики программного обеспечения при практической реализации обязаны выдерживать общие технические требования.

Наряду со стандартными сервисами существуют и нестандартные, представляющие собой оригинальную разработку той или иной компании. В

качестве примера можно привести различные системы типа Instant Messenger (своеобразные Интернет-пейджеры – ICQ, AOl, Demos on-line и т.п.), системы Интернет-телефонии, трансляции радио и видео и т.д. Важной особенностью таких систем является отсутствие международных стандартов, что может привести к возникновению технических конфликтов с другими подобными сервисами.

Для стандартных сервисов также стандартизируется и интерфейс взаимодействия с протоколами транспортного уровня. В частности, за каждым программным сервером резервируются стандартные номера TCP- и UDP-портов, которые остаются неизменными независимо от особенностей той или иной фирменной реализации как компонентов сервиса, так и транспортных протоколов. Номера портов клиентского программного обеспечения так жестко не регламентируются. Это объясняется следующими факторами:

- во-первых, на пользовательском узле может функционировать несколько копий клиентской программы, и каждая из них должна однозначно идентифицироваться транспортным протоколом, т.е. за каждой копией должен быть закреплен свой уникальный номер порта;
- во-вторых, клиенту важна регламентация портов сервера, чтобы знать, куда направлять запрос, а сервер сможет ответить клиенту, узнав адрес из поступившего запроса.

В приведенной ниже таблице перечислены стандартные номера портов для основных сервисов.

Компонент службы	**Номер порта**	**Транспортные протоколы**
Электронная почта		
SMTP-сервер	25	TCP
POP3-сервер	110	TCP
IMAP-сервер	143	TCP
Телеконференции		
NNTP-сервер	119	TCP
FTP		
FTP-сервер	20, 21	TCP
Telnet		
Telnet-сервер	23	TCP
WWW		
HTTP-сервер	80	TCP
DNS		

DNS-сервер	53	TCP, UDP