МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

**С.Э. Хоружников, В.В. Прыгун**

# Администрирование сетей Windows

## Учебное пособие


**Санкт-Петербург**

**2012**

УДК 004.655, 004.657, 004.62

С.Э. Хоружников, В.В. Прыгун

Администрирование Windows Server 2008 - СПб: НИУ ИТМО, 2012. – 61 с.

В пособии излагаются методические указания к выполнению лабораторных работ по дисциплине «Администрирование сетей Windows».

Предназначено для студентов, обучающихся по всем профилям подготовки бакалавров направления: 210700 Инфокоммуникационные технологии и системы связи.

Рекомендовано к печати Ученым советом факультета Инфокоммуникационных технологий, протокол № 4 от 13 декабря 2011г.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

# Оглавление

# Введение

Обучение данному курсу позволит получить фундаментальные знания и навыки, связанные с обеспечением безопасности, управлением сетями и администрированием в Windows Server 2008 R2. Курс проводится для студентов с целью приобретения новых навыков в области технологий Windows Server

**Задачи дисциплины**

После изучения данного курса студенты смогут выполнять перечисленные ниже задачи:

- Выбрать соответствующие технологии хранения и настроить систему хранения в Windows Server.
- Выполнить установку Windows Server 2008 R2 с локального носителя.
- описывать роли сервера.
- Реализовать и настроить лес доменных служб Active Directory®.
- Описать понятие многоуровневой защиты и определить способ реализации этой модели в Windows Server.
- Определить компоненты системы безопасности Windows Server, которые помогут обеспечить многоуровневую защиту.
- Определить сетевые компоненты системы безопасности Windows Server, которые позволят устранить угрозы безопасности сети.
- Определить и реализовать дополнительные программные компоненты для повышения уровня безопасности организации.
- Обеспечить наблюдение за сервером для определения уровня производительности.
- Определить доступные средства Windows Server, которые можно использовать для обслуживания и устранения неполадок Windows Server.

# Лабораторная работа 1. Установка Windows Server

Чтобы иметь эффективно и согласованно работающий сервер, соответствующий потребностям организации, необходимо рассмотреть определенные вопросы и предпринять надлежащие действия. Для обеспечения удобства использования сервера операционной системы Windows Server 2008 R2 очень важно надлежащим образом выполнить начальные установку и настройку. Функциональные возможности и эффективность реализации системы Windows Server зависит от выпусков Windows Server 2008 R2, параметров установки, оптимальной конфигурации служб и устройств и общей послеустановочной конфигурации.

**Сценарий**

Первой задачей администратора сервера на новой работе является выполнение начальных установки и настройки нового сервера для отдела исследований и разработок компании. В данном случае компания решила, что установку необходимо выполнить с локального носителя. Когда установка будет завершена, выполните настройки, которые нужно выполнить после установки, в соответствии с прилагаемой документацией. Кроме того, требуется настроить параметры запуска для некоторых служб и тестировать новый драйвер устройства на предмет надлежащей функциональности.

Для установки нового сервера используйте следующие параметры установки:

Язык: Английский
Формат времени и денежных единиц: Английский (США)
Раскладка клавиатуры или метод ввода: США
Продукт: Windows Server 2008 R2 Enterprise (полная установка)
Пароль администратора: Pa$$w0rd
Параметры настройки после установки:
Часовой пояс: (UTC+03:00)
IP-адрес: 192.168.0.1
Маска подсети: 255.255.255.0
Шлюз: 192.168.0.100
DNS-серверы: 192.168.0.1 и 127.0.0.1
Разрешить автоматическое обновление из Центра обновления Windows
Имя сервера: SERVER
Имя домена: domain.local

## Упражнение 1. Установка на локальный носитель

1. Подключите установочный DVD Windows Server 2008 R2

2. В диалоговом окне Install Windows (Установка Windows) в списке Language to install (Устанавливаемый язык) щелкните English (Английский).

3. В списке Time and currency format (Формат времени и денежных единиц) выберите English (United States) (Американский).

4. В списке Keyboard or input method (Раскладка клавиатуры или метод ввода) выберите Russian и нажмите кнопку Next (Далее).

5. В диалоговом окне Install Windows (Установка Windows) щелкните Install now (Установить).

6. В списке Operating system (Операционная система) выберите Windows Server 2008 R2 Enterprise (Full Installation) (полная установка) и нажмите кнопку Next (Далее).

7. На странице Please read the license terms (Прочтите условия лицензионного соглашения) установите флажок I accept the license terms (Я принимаю условия лицензионного соглашения) и нажмите кнопку Next (Далее).

8. На странице Which type of installation do you want? (Выберите тип установки) щелкните Custom (advanced) (Полная установка (дополнительные параметры)).

9. На странице Where do you want to install Windows? (Выберите раздел для установки Windows) нажмите кнопку Next (Далее). Примечание. Программа установки продолжает работу: копирует и распаковывает файлы, устанавливает компоненты и обновления и завершает установку. Эта фаза займет около двадцати минут. В это время ваш преподаватель может продолжать выполнение других задач.

10. При отображении сообщения The user’s password must be changed before logging on the first time (Перед первым входом в систему пользователь должен сменить свой пароль) нажмите кнопку ОК.

11. В поле New password (Новый пароль) введите Pa$$w0rd.

12. В поле Confirm password (Подтверждение) введите Pa$$w0rd и нажмите клавишу ВВОД.

13. При отображении сообщения Your password has been changed (Пароль был изменен) нажмите кнопку ОК.

Примечание. В процесс установки входит копирование и извлечение файлов, установка компонентов и обновлений, а также завершение установки. Эта фаза занимает от двадцати минут до часа.

Результаты. В ходе этого упражнения вы установили новый сервер Windows Server 2008 R2.

## Упражнение 2. Настройка Windows Server

### Сценарий

Вас попросили настроить только что установленный сервер отдела исследований и разработки в соответствии с инструкциями приведенными выше.

### Задание 1. Используйте «Задачи начальной настройки» для настройки часового пояса.

1. Щелкните Установить часовой пояс.
2. В диалоговом окне Дата и время нажмите кнопку Изменить часовой пояс....
3. Выберите (UTC+04:00), нажмите кнопку ОК.
4. В диалоговом окне Дата и время нажмите кнопку ОК.

### Задание 2. 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

- 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».

**Задание 3. Используйте «Задачи начальной настройки» для настройки параметров автоматического обновления и обратной связи.**

1. Щелкните Включить автоматическое обновление и обратную связь.
2. В окне «Включить автоматическое обновление Windows и сбор отзывов и предложений» выберите Включить автоматическое обновление Windows и сбор отзывов и предложений.

**Задание 4. Используйте «Задачи начальной настройки» для настройки имени компьютера и параметров домена, как указано в задании к лабораторной работе.**

1. В окне «Свойства системы» нажмите кнопку Изменить.
2. В окне «Изменение имени компьютера или домена» введите SERVER в поле Имя компьютера.
3. При появлении запроса на перезагрузку для применения изменений нажмите кнопку ОК.
4. В окне «Свойства системы» щелкните Закрыть.
5. При появлении запроса на перезагрузку щелкните Перезагрузить сейчас.

**Результаты.** В ходе этого упражнения вы настроили параметры, настраиваемые после установки, с помощью мастера задач начальной настройки.

## Упражнение 3. Настройка служб

### Сценарий

Новый сервер для отдела исследований и разработок установлен и настроен. Чтобы подготовить сервер к новой роли, необходимо внести дополнительные изменения в некоторые службы. Чтобы не допустить установки и использования принтеров на этом сервере, службу очереди печати необходимо остановить и отключить, чтобы она не запускалась после перезагрузки сервера. В рамках данного упражнения необходимо выполнить следующую основную задачу.

### Задание 1. Настройте параметры диспетчера очереди печати

1. Войдите на установленный Windows Server 2008 R2.
2. В диспетчере сервера разверните узел Configuration (Конфигурация) в левом столбце и выберите Services (Службы).
3. Прокрутите список до элемента Диспетчер печати. Обратите внимание, что состояние диспетчера очереди печати — Started (Работает), а режим запуска — Automatic (Автоматически).
4. Щелкните правой кнопкой мыши Диспетчер печати и выберите пункт Свойства.
5. Щелкните раскрывающийся список Startup (Автозагрузка) и выберите Disabled (Отключена).
6. Нажмите кнопку Stop (Стоп) для остановки очереди печати, затем нажмите кнопку ОК.
7. Закройте диспетчер сервера.

**Результаты.** В ходе этого упражнения вы использовали диспетчер сервера для изменения параметров запуска службы.

## Упражнение 4. Настройка устройств

### Сценарий

Необходимо проверить правильность работы нового драйвера клавиатуры, подключенной к серверу отдела исследований и разработок, прежде чем его можно будет настроить для постоянного использования. Используемая стандартная клавиатура PS/2 будет заменена расширенной клавиатурой PS/2 PC/AT. Вас попросили проверить правильность обновления драйвера новой расширенной клавиатуры PS/2 PC/AT. После проверки

правильности работы вас попросили выполнить откат к предыдущей версии драйвера.

В рамках данного упражнения необходимо выполнить следующие основные задачи:

1. Обновите драйвер стандартной клавиатуры PS/2.
2. Выполните откат к предыдущей версии драйвера.

**Задание 1. Обновите драйвер стандартной клавиатуры PS/2**

1. Откройте диспетчер сервера.
2. В диспетчере сервера разверните узел Диагностика в левом столбце и выберите Диспетчер устройств.
3. В окне «Диспетчер устройств» разверните Клавиатуры, щелкните правой кнопкой мыши Стандартная клавиатура PS/2 и выберите пункт Обновить драйверы.
4. В диалоговом окне Update Driver Software – Standard PS/2 Keyboard (Обновление драйверов — Стандартная клавиатура PS/2) щелкните Browse my computer for driver software (Выполнить поиск драйверов на этом компьютере).
5. На странице Browse for driver software on your computer (Поиск драйверов на этом компьютере) щелкните Let me pick from a list of device drivers on my computer (Выбрать драйвер из списка уже установленных драйверов).
6. В списке Show compatible hardware list (Только совместимые устройства) щелкните PC/AT Enhanced PS/2 Keyboard (101/102 Key) (Расширенная клавиатура PS/2 PC/AT (101/102 клавиши)) и нажмите кнопку Next (Далее).
7. Нажмите кнопку Close (Закрыть).
8. Перезапустите компьютер, когда будет предложено сделать это.

**Задание 2. Выполните откат к предыдущей версии драйвера**

1. Войдите на сервер под учетной записью Администратор с паролем Pa$$w0rd.

2. Нажмите кнопку Start (Пуск), щелкните правой кнопкой мыши Computer (Компьютер) и выберите пункт Свойства (Управление).

3. В диспетчере сервера разверните узел Диагностика в левом столбце и выберите Диспетчер устройств.

4. В окне диспетчера устройств разверните Keyboards (Клавиатуры), щелкните правой кнопкой мыши PC/AT Enhanced PS/2 Keyboard (101/102 Key) (Расширенная клавиатура PS/2 PC/AT (101/102 клавиши)) и выберите пункт Properties (Свойства).

5. В диалоговом окне PC/AT Enhanced PS/2 Keyboard (101/102 Key) Properties (Свойства: расширенная клавиатура PS/2 PC/AT (101/102 клавиши)) перейдите на вкладку Driver (Драйвер).

6. Щелкните Откатить.

7. В диалоговом окне Driver Package rollback (Откат пакета драйверов) нажмите кнопку Yes (Да).

8. Нажмите кнопку Close (Закрыть), затем в диалоговом окне System Settings Change (Изменение параметров системы) нажмите кнопку Yes (Да), чтобы перезапустить компьютер.

9. После перезагрузки, когда отобразится окно «Задачи начальной настройки», нажмите кнопку Закрыть, чтобы закрыть окно. Нажмите кнопку Start (Пуск), щелкните правой кнопкой мыши Computer (Компьютер) и выберите пункт Свойства (Управление).

10. В окне «Управление компьютером» щелкните Диспетчер устройств. Разверните узел Keyboards (Клавиатуры) и щелкните Standard PS/2 Keyboard (Стандартная клавиатура PS/2).

11. Проверьте, что вы успешно выполнили откат драйвера.

12. Закройте диспетчер сервера.

Результаты. В ходе этого упражнения вы выполнили операции обновления и отката драйвера устройства.

# Лабораторная работа 2. Реализация ролей сервера

## План лабораторной работы

Ваша компания развернула клиентские компьютеры в ряде новых филиалов, занимающихся исследованиями и разработкой. Планируется установить новые серверные компьютеры в этих филиалах для включения компонентов сетевой инфраструктуры, поддержки пользовательских приложений и включения служб доступа к файлам и принтерам для поддержки офисных приложений на клиентских компьютерах. Ваша задача — прочитать документ с требованиями и определить, какие роли сервера необходимы для поддержки потребностей пользователей в филиалах.

## Упражнение 1. Определение соответствующих ролей для развертывания

### Сценарий

Вашей организации необходимо, чтобы все филиалы могли продолжать работу в нормальном режиме, даже если связь с головными офисами отсутствует. В компании используется база данных; филиалы периодически синхронизируют свои данные с базой данных головного офиса. Все сотрудники филиалов используют стандартное офисное ПО; Microsoft Office Word 2007, Microsoft Office Excel® 2007 и другие компоненты Office. Они сохраняют результаты своей работы на сервере. Всем пользователям филиалов доступны общие принтеры. К нам часто приходят посетители с ноутбуками, а пользователи могут перемещаться между филиалами; они должны иметь возможность подключаться к сети без участия пользователя или администратора.

*Технический обзор филиала*

В результате интервью с сотрудниками и дополнительного изучения каждого из филиалов были выработаны следующие требования:

- клиентские компьютеры должны быть настроены на автоматическое получение IPv4-адресов;
- пользователи должны иметь возможность входа в сеть, даже если связь с головным офисом потеряна;
- пользователи хранят файлы централизованно, используя для этого общие папки;
- всем пользователям филиалов доступны общие принтеры;
- в каждом филиале имеется сервер баз данных, содержащий подмножество данных всего исследовательского отдела; синхронизация с головным офисом происходит автоматически;

- важно, чтобы обновления компьютеров загружались не напрямую из Интернета, а с локального сервера.

**Задание 1. Прочтите сопроводительную документацию**

1. Прочтите сопроводительную документацию, чтобы определить требования к серверам в филиалах.

**Задание 2. Выполните рекомендации по развертыванию серверов в филиалах**

1. Ответьте на вопросы, изложенные в рекомендациях по развертыванию серверов в филиалах.
2. Выполните предложения по развертыванию из соответствующего раздела документа.

**Рекомендации по развертыванию серверов в филиалах**

**Обзор требований**

Выполните развертывание требуемых серверных ролей в филиалах, чтобы удовлетворить потребности пользователей.

**Предложения**

1. Как вы выполните требование автоматического получения конфигурации IPv4, если связь с головным офисом потеряна?
2. Как вы выполните требование, чтобы все пользователи могли войти в сеть, если связь с головным офисом потеряна?
3. Как вы выполните требование, чтобы пользователи имели возможность получить доступ к общим файлам?
4. Как вы выполните требование, чтобы пользователи имели возможность использовать общие принтеры?
5. Какой тип сервера наилучшим образом обеспечивает поддержку приложения базы данных?
6. Какие роли поддерживают такой тип сервера?
7. Как вы выполните требование, чтобы компьютеры могли получать обновления от локального сервера обновлений?
8. Какие роли требуются на серверах филиалов?

**Результаты.** В ходе этого упражнения вы выполнили рекомендации

по развертыванию серверов в филиалах.

## Упражнение 2. Развертывание определенных ранее ролей сервера

### Сценарий

Вы изучили сопроводительную документацию, и руководство попросило вас развернуть часть необходимых ролей на тестовом сервере в лабораторной среде. Предположим, в лабораторной среде все прошло удачно, и вы будете развертывать эти роли на рабочих серверах в филиалах.

В рамках данного упражнения необходимо выполнить следующие основные задачи:

1. Выполните развертывание инфраструктурных ролей.
2. Выполните развертывание ролей, имеющих отношение к файлам и печати.
3. Выполните развертывание ролей сервера приложений.
4. Выполните развертывание вспомогательных ролей и компонентов.

### Задание 1. Выполните развертывание инфраструктурных ролей

1. Откройте **Диспетчер сервера**.
2. Добавьте следующие роли сервера:
   - **DHCP-сервер**
   - **DNS-сервер**
3. Примите значения по умолчанию для всех страниц **Мастера добавления ролей**, чтобы завершить процесс установки. На странице **Привязки сетевых подключений** снимите флажок около **192.168.0.1**.
4. Добавьте роль **Доменные службы Active Directory**.
5. **Примечание.** Роль доменных служб Active Directory необходимо добавлять отдельно от роли DNS-сервера.
6. Примите значения по умолчанию для всех страниц **Мастера добавления ролей**, чтобы завершить процесс установки.
7. **Примечание.** Вам не требуется настраивать доменные службы Active Directory.

### Задание 2. Выполните развертывание ролей, имеющих отношение к файлам и печати

1. В диспетчере сервера добавьте следующие роли сервера:

- **Файловые службы**
- **Службы печати и документов**

2. Примите значения по умолчанию для всех страниц **Мастера добавления ролей**, чтобы завершить процесс установки.

**Задание 3. Выполните развертывание ролей сервера приложений**

1. В диспетчере сервера добавьте роль сервера **Сервер приложений**.
2. В ответ на запрос выберите службу роли **Поддержка вебсервера (IIS)**.

**Задание 4. Проверьте вспомогательные роли и компоненты**

1. Почему в окне «Сводка по ролям» некоторые роли помечены красным крестиком?
2. На панели навигации щелкните **Компоненты**.
3. Проверьте установленные компоненты.
4. Когда они были установлены?
5. Закройте диспетчер сервера.

**Результаты.** В ходе этого упражнения вы выполнили развертывание всех требуемых ролей и компонентов.

## Лабораторная работа 3. Конфигурация протокола TCP/IP

Вам поставлена задача назначить клиентским компьютерам соответствующие IP-конфигурации, но сначала нужно выбрать наиболее подходящую схему IP-адресации для новых филиалов.

## Упражнение 1. Определение подходящей схемы IPv4адресации

### Сценарий

Вы ответственны за планирование установки новых сетевых компонентов в этих новых филиалах. Ваш начальник по ИТ посетил некоторые филиалы и подготовил план сети. Кроме того, у вас есть схема IP-адресации филиалов.

В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Прочтите сопроводительную документацию.
2. Ответьте на вопросы, изложенные в схеме IP-адресации филиала (Рис. 1).

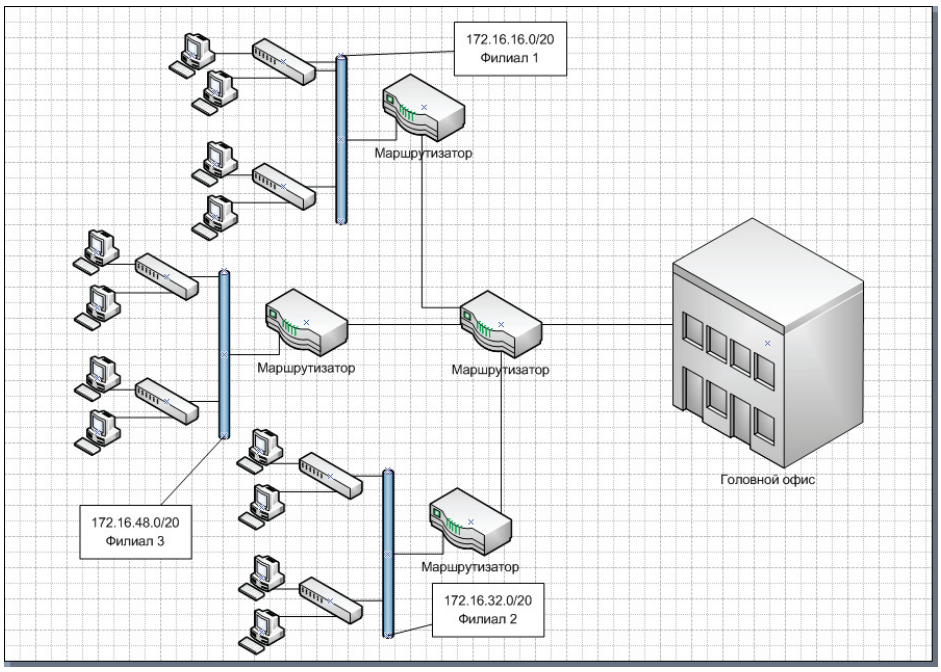


Рис. 1. Схема филиала

Один маршрутизатор связывает три филиала с головным офисом.

Есть три ссылки глобальной сети. Есть три филиала, каждый из которых может быть настроен как отдельная подсеть.

Сетевые адреса 172.16.0.0/16 выделены филиалам, в то время как головной офис использует адреса 10.10.0.0/16.

1. Сколько сетевых адресов необходимо для соблюдения этих требований?
2. К какому классу относятся адреса 172.16.0.0/16?
3. Это публичные или частные адреса?
4. Ваш руководитель выделил первый блок адресов для первого филиала: 172.16.16.0/20. Какова следующая логическая подсеть при такой первоначальной подсети?
5. Каковы первый и последний узлы этой подсети?
6. Какова будет маска подсети для узлов этой подсети?

## Упражнение 2. Настройка протокола IPv4 в Windows Server 2008

### Сценарий

Пока рассматривается схема адресации филиалов, ваш руководитель попросил вас настроить новый DHCP-сервер для головного офиса. В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Настройка области DHCP.
2. Настройте клиентский компьютер на динамическое получение IPадреса.
3. Проверьте, что клиентский компьютер получил адрес.
4. Определите IP-адрес клиентского компьютера.

### Задание 1. Настройте область протокола DHCP

1. Откройте окно DHCP из окна Администрирование.
2. Удалите существующую область.
3. Создайте новую область, выполнив следующие действия.
4. Щелкните правой кнопкой мыши IPv4 и выберите команду Создать область.
5. Имя области: Office1
6. Описание области: Адреса клиентских компьютеров

7. На странице Диапазон IP-адресов введите следующие сведения.
    - Начальный IP-адрес: 192.168.0.150
    - Конечный IP-адрес: 192.168.0.160
    - Длина: 16
    - Маска подсети: 255.255.255.0
8. На странице Добавление исключений и задержка примите значения по умолчанию.
9. На странице Срок действия аренды адреса примите значения по умолчанию.
10. На странице Настройка параметров DHCP примите значения по умолчанию, и для настройки параметров области используйте следующие данные.
11. Адрес маршрутизатора: 192.168.0.100.
12. На странице Имя домена и DNS-серверы примите значения по умолчанию.
13. На странице WINS-серверы примите значения по умолчанию.
14. На странице Активировать область примите значения по умолчанию.
15. На странице Завершение мастера создания области нажмите кнопку Готово.
16. В консоли разверните узел Область [192.168.0.0] Office1 и выберите Арендованные адреса.

**Задание 2. Настройте клиентский компьютер на динамическое получение IP-адреса**

1. Переключитесь на компьютер CLIENT.
2. Откройте Панель управления.
3. Выберите Сеть и Интернет, а затем Центр управления сетями и общим доступом.
4. В левой области щелкните Изменение параметров адаптера.

5. Щелкните правой кнопкой мыши Подключение по локальной сети и выберите пункт Свойства.
6. Измените свойства элемента Протокол Интернета версии 4 (TCP/IPv4), указав следующие параметры.
7. Получить IP-адрес автоматически.
8. Получить адрес DNS-сервера автоматически.
9. Дважды нажмите кнопку ОК.

**Задание 3. Проверьте, что клиентский компьютер получил адрес**

1. Откройте командную строку.
2. В командной строке введите следующую команду и нажмите клавишу ВВОД.
3. Ipconfig /all
4. Вопрос. Каков текущий IPv4-адрес?
5. Вопрос. В поле «DHCP включен» указано значение «Да»?
6. Вопрос. Какой IP-адрес у DHCP-сервера?
7. Вопрос. Когда истекает аренда DHCP?

Результаты. В ходе этого упражнения вы создали область DHCP и выделили клиентский адрес.

## Упражнение 3. Проверка конфигурации

**Сценарий**

Начальник попросил вас проверить функциональность DHCP-сервера.
В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Остановите работу DHCP-сервера.
2. Попытайтесь обновить IPv4-адрес на клиентском компьютере.
3. Повторно запустите DHCP-сервер.
4. Обновите адрес клиента и проверьте IPv4.

**Задание 1. Остановите работу DHCP-сервера**

1. Переключитесь на компьютер SERVER.

2. В окне DHCP выберите Все задачи и щелкните Остановить.

**Задание 2. Попытайтесь обновить IPv4-адрес на клиентском компьютере**

1. Переключитесь на компьютер CLIENT и переключитесь в командную строку.

2. В командной строке введите следующую команду и нажмите клавишу ВВОД.

   Ipconfig /release

3. В командной строке введите следующую команду и нажмите клавишу ВВОД.

   Ipconfig /renew

   Примечание. Это может занять несколько минут, поскольку клиентский компьютер пытается подключиться к исходному DHCP-серверу, а затем к любому другому DHCP-серверу.

4. В командной строке введите следующую команду и нажмите клавишу ВВОД

   Ipconfig

   Вопрос. Какой IPv4-адрес отобразился?

   Вопрос. На что это указывает?

5. В командной строке введите следующую команду и нажмите клавишу ВВОД.

   Ping nyc-dc1.contoso.com

   Примечание. Попытка была неудачной.

**Задание 3. Повторно запустите DHCP-сервер**

1. Переключитесь на компьютер CLIENT и перезапустите службу DHCP.

**Задание 4. Обновите адрес клиента и проверьте IPv4**

1. Переключитесь на компьютер NYC-CL1 и в командной строке введите следующую ниже команду, после чего нажмите клавишу ВВОД:

Ipconfig /renew

Вопрос. Какой IPv4-адрес отобразился?

Вопрос. На что это указывает?

2. В командной строке введите следующую команду и нажмите клавишу ВВОД.

   Ping nyc-dc1.contoso.com

   Примечание. Попытка была удачной.

**Результаты**. В ходе этого упражнения вы успешно проверили ункциональность DHCP-сервера в головном офисе.

## Упражнение 4. Настройка и тестирование разрешения имен

### Сценарий

Ваш руководитель хочет разместить веб-сервер на узле SERVER. Однако вместо префикса server он бы хотел использовать префикс www. Вы создадите необходимые записи в службе DNS, чтобы удовлетворить этот запрос.

В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Просмотрите текущие DNS-записи.
2. Выполните принудительное динамическое обновление.
3. Добавьте новую запись DNS.
4. Проверьте запись.

### Задание 1. Просмотрите текущие записи DNS

1. Переключитесь на сервер SERVER.
2. Откройте диспетчер DNS.

Вопрос. Какой IP-адрес сейчас отображается для записи узла (A) для SERVER?

### Задание 2. Выполните принудительное динамическое обновление

3. Переключитесь на компьютер CLIENT .
4. В окне «Сетевые подключения» щелкните правой кнопкой мыши значок Подключение по локальной сети и выберите пункт Свойства.

5. Измените свойства элемента Протокол Интернета версии 4 (TCP/IPv4), указав следующие параметры.

   - IP-адрес: 192.168.0.2
   - Маска подсети: 255.255.255.0
   - Шлюз по умолчанию: 192.168.0.100
   - Предпочитаемый DNS-сервер: 192.168.0.1

6. Дважды нажмите кнопку ОК.
7. Переключитесь на виртуальную машину CLIENT.
8. Обновите экран.

Вопрос. Какой IP-адрес сейчас отображается напротив записи узла (A) для CLIENT?

**Задание 3. Добавьте новую запись DNS**

1. Переключитесь на компьютер CLIENT и в командной строке введите следующую ниже команду, после чего нажмите клавишу ВВОД.

   Ipconfig /displaydns

Вопрос. Какие записи отображаются?

2. В командной строке введите следующую команду и нажмите клавишу ВВОД.

   Ping www.domaijn.local

Примечание. Попытка была неудачной.

3. Переключитесь на виртуальную машину SERVER.
4. Создайте новую запись в диспетчере DNS.

   - Тип: новый псевдоним (CNAME)
   - Псевдоним (если не указан, используется имя род. домена): www
   - Полное доменное имя (FQDN) конечного узла: server.domain.local

**Задание 4. Проверьте запись**

1. В командной строке введите следующую команду и нажмите клавишу ВВОД.
2. Выполните команду

   Ping www.domain.local

   Примечание. Попытка была неудачной.
3. В командной строке введите следующую команду и нажмите клавишу ВВОД.

   Ipconfig /flushdns
4. В командной строке введите следующую команду и нажмите клавишу ВВОД.

   Ping www.domain.local

   Примечание. Попытка была удачной.
5. В командной строке введите следующую команду и нажмите клавишу ВВОД.

   Ipconfig /displaydns

Вопрос. Какая запись возвращается для www.domain.local?

**Результаты.** В ходе этого упражнения вы успешно добавили новую DNSзапись.

## Упражнение 5. Просмотр конфигурации IPv6

**Сценарий**

В настоящее время компания Contoso, Ltd. не планирует реализовывать поддержку IPv6, но Ed хочет знать текущие IPv6-адреса. Для определения текущих IPv6-адресов будет использоваться программа Ipconfig.

В рамках данного упражнения необходимо выполнить следующую основную задачу.

1. Определите текущий IPv6-адрес. На виртуальной машине CLIENT в командной строке введите следующую команду и нажмите клавишу ВВОД.

Ipconfig /all

Вопрос. Отобразился ли IPv6-адрес?

Вопрос. Какого типа этот адрес?

**Результаты.** В ходе этого упражнения вы определили, что на локальном узле задан только локальный IPv6-адрес канала

## Лабораторная работа 4. Установка доменных служб Active Directory

# Упражнение 1. Создание нового контроллера домена

### Задание 1. Создайте контроллер домена

1. Переключитесь на компьютер SERVER.
2. Запустите программу dcpromo и дождитесь установки двоичных файлов доменных служб Active Directory.
3. Выполните операции мастера установки доменных служб Active Directory, указав следующие сведения.
4. Совместимость операционных систем: примите значения по умолчанию
5. Выберите конфигурацию развертывания: новый лес, новй домен:
6. Сетевые учетные данные: примите значения по умолчанию
7. Выберите домен: domain.local (по умолчанию)
8. Расположение для базы данных, файлов журнала и SYSVOL: примите значения по умолчанию
9. Пароль администратора режима восстановления служб каталогов: Pa$$w0rd
10. Установите флажок Перезагрузить сейчас

Результаты. В ходе этого упражнения вы создали новый контроллер домена.

# Упражнение 2. Создание подразделения

### Задание 1. Создание подразделения

1. После перезапуска компьютера SERVER, выполните вход со следующими учетными данными:
   - Имя пользователя: Администратор
   - Пароль: Pa$$w0rd
   - Домен: domain.local
2. Выбрав на панели навигации «Active Directory - пользователи и компьютеры», щелкните domain.local.

3. Щелкните правой кнопкой мыши Contoso.com, выберите команду Создать и щелкните Подразделение

4. Создайте новое подразделение с именем Managers в домене domain.local.

**Результаты.** В ходе этого упражнения вы создали новый организационный список.

## Упражнение 3. Настройка учетных записей

### Сценарий

Руководство попросило вас создать необходимые учетные записи и группы пользователей и перенести учетные записи компьютеров пользователей в подразделение. Необходимо создать две группы: одну для менеджеров и вторую для руководителей. Затем следует предоставить руководителям возможность сбросить пароли всех учетных записей пользователей подразделения Managers.

В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Добавьте учетные записи пользователей.

2. Создайте группы.

3. Добавьте членов в группы.

4. Переместите учетную запись компьютера.

5. Делегируйте управление подразделению.

### Задание 1. Добавьте учетные записи пользователей

В оснастке «Active Directory - пользователи и компьютеры» создайте

указанные ниже учетные записи пользователей в подразделении Managers, используя для этого следующую информацию.

Настройте имена и фамилии пользователей.

Именем входа пользователя является его имя.

Пароль: Pa$$w0rd.

Снимите флажок Требовать смену пароля при следующем входе в систему.

Создайте следующих пользователей:

- Ivanov Ivan
- Petrov Ivan

- Sidorov Ivan

1. Выбрав «Active Directory - пользователи и компьютеры», щелкните правой кнопкой мыши Managers, выберите Создать, затем щелкните Пользователь.
2. В диалоговом окне Новый объект — Пользователь в поле Имя введите Ivan.
3. В поле Фамилия введите Ivanov.
4. В поле Имя входа пользователя введите Ivanov и нажмите кнопку Далее.
5. В полях Пароль и Подтверждение пароля введите Pa$$w0rd.
6. Снимите флажок Требовать смены пароля при следующем входе в систему и нажмите кнопку Далее.
7. Нажмите кнопку Готово.
8. Повторите пункты 1-7 для оставшихся пользователей

**Задание 2. Создание групп**

В подразделении Managers создайте следующие глобальные группы безопасности: Managers, Headers.

1. Выбрав «Active Directory - пользователи и компьютеры», щелкните правой кнопкой мыши Managers, выберите Создать, затем щелкните Группа.
2. В диалоговом окне Новый объект — Группа в поле Имя группы введите Managers.
3. Повторите пункты 1-2 для группы Headers

**Задание 3. Добавьте членов в группы**

1. Добавьте всех новых пользователей в группу Managers подразделения Managers.
2. Добавьте только пользователя Petrob Ivan в группу Headers.

**Задание 4. Делегируйте управление подразделением**

С помощью мастера делегирования управления дайте глобальной группе безопасности Headers право Переустановить пароли пользователей и установить изменение пароля при следующей перезагрузке в подразделении Managers.

1. На панели навигации щелкните правой кнопкой мыши по контейнеру Managers и щелкните Делегирование управления.
2. На странице Мастер делегирования управления мастера делегирования управления нажмите кнопку Далее.
3. На странице Пользователи или группы нажмите кнопку Добавить.
4. В диалоговом окне Выбор: «Пользователи», «компьютеры» или «группы» в поле Введите имена выбираемых обьектов (примеры): введите Headers, щелкните Проверить имена и нажмите кнопку ОК.
5. На странице Пользователи или группы нажмите кнопку Далее. На странице Делегируемые задачи установите флажок Переустановить пароли пользователей и установить изменение пароля при следующей перезагрузке и нажмите кнопку Далее.
6. Нажмите кнопку Готово.

## Упражнение 4. Создание объекта групповой политики

### Задание 1. Создание объекта групповой политики

1. Нажмите кнопку Пуск, укажите пункт Администрирование и выберите оснастку Управление групповой политикой.
2. Последовательно разверните узлы Лес: domain.local, Домены и domain.local.
3. На панели навигации щелкните правой кнопкой мыши Объекты групповой политики, затем щелкните Создать.
4. В диалоговом окне Новый объект групповой политики в поле Имя введите Объект групповой политики Managers и нажмите кнопку ОК.
5. Разверните узел Объекты групповой политики, щелкните правой кнопкой мыши Объект групповой политики Managers и выберите пункт Правка.
6. В редакторе управления групповыми политиками последовательно разверните узлы Конфигурация пользователя, Политика и Конфигурация Windows, затем щелкните Сценарии (вход/выход из системы).
7. В области результатов дважды щелкните Вход в систему.
8. В диалоговом окне Свойства: Вход в систему нажмите кнопку Добавить.
9. В диалоговом окне Добавление сценария нажмите кнопку Обзор.

10. В диалоговом окне Обзор щелкните правой кнопкой мыши поле Нет элементов, удовлетворяющих условиям поиска, выберите Создать и Текстовый документ.

11. Выделите имя файла целиком, включая расширение, введите logon.vbs и нажмите клавишу ВВОД.

12. В диалоговом окне Переименование нажмите кнопку Да.

13. Щелкните правой кнопкой мыши файл logon.vbs и выберите пункт Изменить.

14. В диалоговом окне Открыть файл - Предупреждение о безопасности нажмите кнопку Открыть.

15. В «Блокноте» введите msgbox «Welcome».

16. В меню Файл выберите команду Сохранить.

17. Закройте Блокнот.

18. В диалоговом окне Обзор нажмите кнопку Открыть.

19. В диалоговом окне Добавление сценария нажмите кнопку ОК.

20. В диалоговом окне Свойства: Вход в систему нажмите кнопку ОК.

21. Закройте Редактор управления групповыми политиками.

**Задание 2. Свяжите объект групповой политики**

1. На панели навигации консоли управления групповыми политиками щелкните правой кнопкой мыши Managers и выберите команду Связать существующий объект групповой политики.

2. В диалоговом окне Выбор объекта групповой политики в списке Объекты групповой политики выберите Объект групповой политики Managers.

**Задание 3. Проверьте объект групповой политики**

1. Переключитесь на компьютер CLIENT и выйдите из системы.

2. Войдите с использованием следующих учетных данных:

   - Имя пользователя: ivanov
   - Пароль: Pa$$w0rd
   - Домен: domain

Вопрос. Сценарий запускается?

**Результаты.** В ходе этого упражнения вы создали объект групповой политики и связали его с подразделением.

## Лабораторная работа 5. Реализация уровней безопасности ИТ

В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Проверьте текущие параметры безопасности Internet Explorer.
2. Измените параметры безопасности для зоны интрасети.
3. Протестируйте изменения безопасности.

### Задание 1. Проверьте текущие параметры безопасности Internet Explorer

1. Откройте **Internet Explorer**.
2. В меню **Сервис** выберите пункт **Свойства** обозревателя.
3. В диалоговом окне **Свойства** обозревателя перейдите на вкладку **Безопасность**.
4. В списке **Выберите зону** для настройки ее параметров безопасности щелкните **Местная интрасеть**.
5. Каков текущий уровень безопасности для зоны местной интрасети?

### Задание 2. Измените параметры безопасности для зоны интрасети

1. Измените уровень безопасности для зоны местной интрасети на **Высокий**.
2. Включите для зоны местной интрасети **Защищенный режим**.
3. Закройте Internet Explorer.

### Задание 3. Протестируйте изменения безопасности

**Примечание.** Если отображается диалоговое окно **Вас приветствует Internet Explorer 8**, щелкните **Отложить этот вопрос**.

1. Откройте **Internet Explorer**.
2. Перейдите на страницу **http://localhost**
3. К какой зоне безопасности относится данный веб-сайт?

## Лабораторная работа 6. Реализация безопасности Windows Server

## Упражнение 1. Настройка политики учетных записей

### Сценарий

Вас попросили реализовать политику паролей в соответствии с требованиями новых политик безопасности компании. Ваш руководитель попросил вас настроить параметры в соответствии со следующими критериями; в ситуациях, когда параметры не определяются политикой компании явным образом, должны применяться рекомендации.

### Рекомендации

- Длина пароля должна быть не менее восьми знаков.
- Пароли должны содержать знаки по крайней мере трех из четырех следующих типов: строчные буквы (a-z), прописные буквы (A-Z), цифры (0-9), небуквенные символы (например, ! @ # $).
- Пароли должны меняться каждые 60 дней.
- Пользователи не могут повторно использовать пароль, пока они не сменили пять других различных паролей.
- После повторной неудачной попытки входа пользователи должны блокироваться в системе.

В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Настройте параметры политики паролей в соответствии с политикой компании.
2. Настройте параметры политики блокировки учетных записей в соответствии с политикой компании.

### Задание 1. Настройка политики паролей

1. Откройте консоль управления групповыми политиками.
2. Нажмите кнопку Пуск, укажите пункт Администрирование и выберите оснастку Управление групповой политикой.
3. Последовательно разверните узлы Лес:domain.local, Домены и domain.local. Правой кнопкой мыши щелкните элемент Default Domain Policy и выберите команду Изменить....

4. В разделе Конфигурация компьютера последовательно разверните Политики, Конфигурация Windows и Параметры безопасности, затем щелкните Политики учетных записей.

5. В окне результатов дважды щелкните Политика паролей.

6. Дважды щелкните Вести журнал паролей и введите 5 в поле Вести журнал для:. Нажмите кнопку ОК.

7. Дважды щелкните Максимальный срок действия пароля и введите 60 в поле Срок истечения действия пароля:. Нажмите кнопку ОК.

8. Дважды щелкните Минимальная длина пароля и введите 8 в поле Длина пароля не менее:. Нажмите кнопку ОК.

9. Дважды щелкните Пароль должен отвечать требованиям сложности и проверьте, что выбрано значение Включен. Нажмите кнопку ОК.

10. Измените политику **Default Domain Policy**.

11. Измените параметры **политики паролей**, обновив соответствующие параметры с помощью представленной выше информации.

**Задание 2. Настройка параметров политики блокировки учетной записи**

1. Измените параметры **политики блокировки учетных записей**, обновив соответствующие параметры с помощью представленной выше информации.

2. Щелкните Политика блокировки учетной записи в левой области окна редактора управления групповыми политиками.

3. Дважды щелкните Пороговое значение блокировки и введите 3 в поле Учетная запись не будет блокирована.

4. В диалоговом окне Свойства: Пороговое значение блокировки нажмите кнопку ОК.

5. В окне «Предлагаемые изменения значений» нажмите кнопку ОК, чтобы принять предложенные значения.

6. Закройте окно редактора управления групповыми политиками.

7. Закройте консоль управления групповыми политиками

**Результаты.** В ходе этого упражнения вы настроили параметры политик паролей и блокировки учетных записей в окне «Политики учетных записей».

## Упражнение 2. Безопасность файлов и папок в NTFS

### Сценарий

Исследовательская команда попросила создать на сервере новую папку для хранения общей информации об исследованиях, а также информации о проектах и засекреченной информации. Эта папка и все ее содержимое должны быть полностью доступны для всей исследовательской команды, кроме засекреченной информации, которая должна быть доступна только Администратору (он должен иметь полный доступ к ней). Члены исследовательской команды будут обращаться к файлам и папкам только по сети.

Руководитель попросил вас создать структуру общих папок, соответствующую запросу исследовательской команды.

В рамках данного упражнения необходимо выполнить следующие основные задачи:

1. Создайте структуру папки C:\Исследования.
2. Назначьте соответствующие разрешения NTFS файлам и папкам этой структуры.
3. Предоставьте доступ к папке C:\Исследования по сети и задайте соответствующие разрешения для общей папки.

### Задание 1. Создайте структуру папки C:\Исследования

1. Создайте новую папку с именем **C:\Исследования**.
2. Создайте в папке **C:\Исследования** две вложенные папки с именами **Секретно** и **Проекты**.

### Задание 2. Назначьте соответствующие разрешения NTFS файлам и папкам этой структуры

- Заблокируйте наследование для папки **C:\Исследования**.
- Назначьте группе **Исследователи** разрешение **Полный доступ** для папки **C:\Исследования**.

  **Примечание.** Если группы **Исследователи** не существует, то ее предварительно необходимо создать.

- Заблокируйте наследование для папки **C:\Исследования\Секретно**.
- Назначьте разрешение **Полный доступ** для папки **C:\Исследования\Секретно** только пользователю Администратор.

1. В диалоговом окне Свойства: **Исследования** перейдите на вкладку Безопасность и щелкните Дополнительно.

2. В диалоговом окне Дополнительные параметры безопасности для папки **Исследования** нажмите кнопку Изменить разрешения.

3. В диалоговом окне Дополнительные параметры безопасности для папки **Исследования** снимите флажок Добавить разрешения, наследуемые от родительских объектов и щелкните кнопку Добавить во всплывающем диалоговом окне Безопасность Windows.

4. В диалоговом окне Дополнительные параметры безопасности для папки **Исследования** нажмите кнопку ОК.

5. В диалоговом окне Дополнительные параметры безопасности для папки **Исследования** снова нажмите кнопку ОК.

6. В диалоговом окне Свойства: папки **Исследования** перейдите на вкладку Безопасность и щелкните Изменить.

7. В диалоговом окне Разрешения для группы папки **Исследования** в области Группы или пользователи последовательно щелкните Пользователи (Users) и Удалить.

8. В диалоговом окне Разрешения для группы «Исследования» нажмите кнопку Добавить.

9. В диалоговом окне Выбор: «Пользователи», «Компьютеры», «Учетные записи служб» и «группы» в поле Введите имена выбираемых объектов (примеры) введите **Исследования**, щелкните Проверить имена и нажмите кнопку ОК.

10. В поле Группы или пользователи выберите **Исследования**.

11. В диалоговом окне Разрешения для группы **Исследования** рядом с элементом Полный доступ установите флажок Разрешить и нажмите кнопку ОК.

12. В окне «Свойства: **Исследования**» нажмите кнопку ОК.

13. Дважды щелкните Исследования, затем щелкните правой кнопкой мыши папку Секретно и выберите пункт Свойства.

14. В диалоговом окне Свойства: Секретно перейдите на вкладку Безопасность и щелкните Дополнительно.

15. В диалоговом окне Дополнительные параметры безопасности для папки **Секретно** нажмите кнопку Изменить разрешения.

16. В диалоговом окне Дополнительные параметры безопасности для папки **Секретно** снимите флажок Добавить разрешения, наследуемые от родительских объектов и щелкните кнопку Добавить во всплывающем диалоговом окне Безопасность Windows.

    Примечание. Кнопка «Удалить» удаляет все разрешения NTFS для данной папки, включая разрешения вашего пользователя Administrator. В результате вам будет запрещено производить любые изменения с этой папкой, включая назначение разрешений.

17. В диалоговом окне Дополнительные параметры безопасности для папки **Секретно** нажмите кнопку ОК.

18. В диалоговом окне Дополнительные параметры безопасности для папки **Секретно** снова нажмите кнопку ОК.

19. В диалоговом окне Свойства: **Секретно** перейдите на вкладку Безопасность и щелкните Изменить.

20. В диалоговом окне Разрешения для папки Секретно в области Группы или пользователи щелкните группу Иследователи и нажмите кнопку Удалить.

**Задание 3. Предоставьте доступ к папке C:\Исследования по сети и задайте соответствующие разрешения для общей папки**

1. Откройте общий доступ к папке **C:\Исследования** в сети.

2. Назначьте группе **Исследователи** разрешение **Полный доступ** для папки **C:\Исследования**.

3. Нажмите кнопку Назад, затем щелкните правой кнопкой мыши папку Исследования и выберите пункт Свойства.

4. В диалоговом окне Свойства: **Исследования** перейдите на вкладку Доступ и щелкните Расширенная настройка....

5. Установите флажок Открыть общий доступ к этой папке, имя общего ресурса Исследования оставьте без изменений, затем щелкните Разрешения.

6. В диалоговом окне Разрешения для группы **Исследователи** в области Группы или пользователи последовательно щелкните Все и Удалить.

7. В диалоговом окне Разрешения для группы **Исследователи** нажмите кнопку Добавить.

8. В диалоговом окне Выбор: «Пользователи», «Компьютеры», «Учетные записи служб» и «группы» в поле Введите имена

выбираемых объектов (примеры) введите **Исследователи**, щелкните Проверить имена и нажмите кнопку ОК.

9. В поле Группы или пользователи выберите **Исследователи**.

10. В диалоговом окне Разрешения для группы **Исследователи** рядом с элементом Полный доступ установите флажок Разрешить и нажмите кнопку ОК.

11. В диалоговом окне Расширенная настройка общего доступа нажмите кнопку ОК.

12. В диалоговом окне Свойства: **Исследования** нажмите кнопку Закрыть.

13. Закройте проводник Windows.

**Результаты.** В ходе этого упражнения вы обеспечили безопасность папок NTFS и общих папок.

## Упражнение 3. Шифрование файлов

**Сценарий**

Ваш начальник попросил, чтобы на сервере определенные файлы с конфиденциальной информацией в подпапке **Секретно** общей папки **Исследования** были зашифрованы с целью предотвратить неавторизованный доступ. Вас попросили проверить шифрование папки **Секретно**. В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Зашифруйте файлы и папки с помощью EFS.

2. Проверьте, что файлы зашифрованы.

3. Расшифруйте файлы и папки.

### Задание 1. Зашифруйте файлы и папки с помощью шифрующей файловой системы (EFS)

- При необходимости войдите на сервер под учетной записью **Администратор**.
- Создайте тестовый файл **Личное.txt** в папке **C:\Исследования\Секретно**.
- Зашифруйте папку **C:\Исследования\Секретно** и содержащиеся в ней файлы.

1. В правой области дважды щелкните папку Исследования.

2. В правой области дважды щелкните папку Секретно.

3. Щелкните правой кнопкой мыши в правой области и последовательно выберите пункты Создать и Текстовый документ.

4. Переименуйте файл Новый текстовый документ в Личное.txt.

5. В левом столбце дважды щелкните Локальный диск (C:), затем щелкните папку Исследования.

6. В правом столбце щелкните правой кнопкой мыши папку Секретно и выберите пункт Свойства.

7. В диалоговом окне Свойства: Секретно нажмите кнопку Другие....

8. В диалоговом окне Дополнительные атрибуты установите флажок Шифровать содержимое для защиты данных и нажмите кнопку ОК.

9. В диалоговом окне Свойства: Секретно нажмите кнопку ОК.

10. Во всплывающем диалоговом окне Подтверждение изменения атрибутов проверьте, выбран ли переключатель К данной папке и ко всем вложенным папкам и файлам, затем нажмите кнопку ОК.

11. Выполните операцию выхода из системы.

**Задание 2. Проверьте, что файлы зашифрованы**

1. Войдите на сервер под учетной записью отличной от учетной записи **Администратор**

**Примечание.** При необходимости создайте учетную запись нового пользователя.

2. Убедитесь, что папка **Секретно** и содержащиеся в ней файлы зашифрованы, попытавшись открыть файл **Личное.txt** из папки **C:\Исследования\Секретно**. Имена зашифрованных файлов и папок должны отображаться зеленым.

**Задание 3. Расшифровка файлов и папок**

1. Войдите на сервер под учетной записью **Администратор**.

2. Расшифруйте содержимое папки **C:\Исследования\Секретно**.

**Результаты.** В ходе этого упражнения вы выполнили шифрование и расшифровку файлов и папок с помощью системы EFS.

## Упражнение 4. Настройка брандмауэра Windows в режиме повышенной безопасности

**Сценарий**

Необходимо создать правило брандмауэра, блокирующее входящий трафик ICMPv4, чтобы злоумышленники не могли использовать программу ping.exe.

В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Проверьте связь с помощью команды Ping.
2. Настройте новое правило брандмауэра.
3. Проверьте правило.
4. Отключите новое правило.

**Задание 1. Проверьте связь с помощью команды Ping**

1. Переключитесь на компьютер SERVER.
2. Откройте командную строку.
3. В командной строке введите следующую команду и нажмите клавишу ВВОД.

   Ping CLENT

4. Проверьте связь с компьютером CLENT.

Вопрос. Попытка была удачной?

**Задание 2. Настройте новое правило брандмауэра**

1. На компьютере CLIENT откройте брандмауэр Windows в режиме повышенной безопасности.
2. Создайте новое правило для входящих подключений, используя для завершения процесса следующую информацию.

   - Тип правила: Настраиваемые
   - Программа: Все программы
   - Тип протокола: ICMPv4
   - Область: значение по умолчанию
   - Действие: Блокировать подключение
   - Профиль: значение по умолчанию
   - Имя: Правило ICMPv4

3. Щелкните правой кнопкой мыши Правила для входящих подключений и выберите пункт Создать правило.

4. В окне мастера создания правила для нового входящего подключения на странице Тип правила щелкните Настраиваемые и нажмите кнопку Далее.

5. На странице Программа выберите Все программы и нажмите кнопку Далее.

6. На странице Протокол и порты в списке Тип протокола щелкните ICMPv4 и нажмите кнопку Далее.

7. На странице Область нажмите кнопку Далее.

8. На странице Действие выберите Блокировать подключение и нажмите кнопку Далее.

9. На странице Профиль нажмите кнопку Далее.

10. На странице Имя в поле Имя введите Правило ICMPv4 и нажмите кнопку Готово.

Вопрос. Отображается ли новое правило в узле «Наблюдение» раздела брандмауэра?

**Задание 3. Проверьте правило**

1. Снова переключитесь на компьютер SERVER.

2. В командной строке введите следующую команду и нажмите клавишу ВВОД.

   Ping CLIENT

Вопрос. Удается ли проверить связь с CLENT?

**Задание 4. Отключите новое правило**

Снова переключитесь на компьютер CLIENT.

1. В оснастке «Брандмауэр Windows в режиме повышенной безопасности» щелкните Правила для входящих подключений.

2. Отключите Правило ICMPv4.

3. Закройте окно «Брандмауэр Windows в режиме повышенной безопасности».

4. Снова переключитесь на компьютер SERVER.

Вопрос. Удается ли проверить связь с CLIENT?

**Результаты**. В ходе этого упражнения вы создали и проверили правило брандмауэра для входящих подключений.

## Упражнение 5. Настройка соответствия защите доступа к сети (NAP)

### Сценарий

Необходимо включить принудительное использование NAP с DHCP для достижения второй цели — контроля того, что на подключающихся к сети клиентских компьютерах запущено антивирусное ПО.

В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Установите роль сервера политики сети.
2. Настройте роль DHCP-сервера.
3. Настройте средство проверки работоспособности системы.
4. Отключите неважные сетевые политики.
5. Создайте обязательные политики работоспособности.
6. Создайте обязательные сетевые политики.
7. Настройте параметры NAP клиентов.
8. Настройте клиентский компьютер на динамическое получение IPv4адреса.
9. Проверьте защиту доступа к сети.

### Задание 1. Установите роль сервера сетевых политик

1. На панели задач щелкните Диспетчер сервера.
2. В диспетчере сервера щелкните Роли.
3. На панели действий щелкните Добавить роли.

4. В мастере добавления ролей на странице Перед началом работы нажмите кнопку Далее и затем на странице Выбор ролей сервера установите флажок Службы политики сети и доступа и нажмите кнопку Далее.

5. На странице Службы политики сети и доступа нажмите кнопку Далее.

6. На странице Выбор служб ролей установите флажок Сервер политики сети и нажмите кнопку Далее.

7. На странице Подтверждение выбранных элементов для установки щелкните Установить.

8. На странице Результаты установки щелкните Закрыть.

**Задание 2. Настройка роли DHCP-сервера**

1. Откройте окно DHCP из окна Администрирование.

2. Просмотрите Свойства области.

3. На вкладке Защита доступа к сети выберите Включить для этой области.

4. На панели навигации щелкните Параметры области.

5. Щелкните правой кнопкой мыши Параметры области и выберите команду Настроить параметры.

6. На вкладке Дополнительно в списке Класс пользователя выберите Класс защиты доступа к сети по умолчанию.

7. В списке Доступный параметр настройте для параметра 006 DNSсерверы IP-адрес 192.168.0.100.

8. Настройте для 015 DNS-имя домена строковое значение restricted.domain.local.

9. Закройте DHCP.

**Задание 3. Настройте средство проверки работоспособности системы**

1. На компьютере SERVER откройте Сервер политики сети в окне Администрирование.

2. На панели навигации последовательно разверните узлы Защита доступа к сети, Средства проверки работоспособности системы и Средство проверки работоспособности системы безопасности Windows, затем щелкните Параметры.

3. В области результатов дважды щелкните Конфигурация по умолчанию.

4. В диалоговом окне Средство проверки работоспособности системы безопасности Windows снимите все флажки, кроме флажка Антивирусная программа включена, и нажмите кнопку ОК.

**Задание 4. Отключите неважные сетевые политики**

1. На панели навигации консоли «Сервер сетевых политик» разверните узел Политики и щелкните Сетевые политики.

2. В области результатов щелкните правой кнопкой мыши каждую из двух отображаемых политик и для каждой из них выберите Выключить.

**Задание 5. Создайте обязательные политики работоспособности**

1. На панели навигации щелкните Политики работоспособности.

2. Создайте новую политику работоспособности со следующими свойствами:

3. Имя политики: Работоспособный клиент

4. Клиенты, проверяемые SHV: Клиент проходит все проверки SHV

5. Средство проверки работоспособности: Средство проверки работоспособности системы безопасности Windows

6. Создайте новую политику работоспособности со следующими свойствами:

7. Имя политики: Неработоспособный клиент

8. Клиенты, проверяемые SHV: Клиент не проходит одну или несколько проверок SHV

9. Средство проверки работоспособности: Средство проверки работоспособности системы безопасности Windows

**Задание 6. Создайте обязательные сетевые политики**

1. На панели навигации щелкните Сетевые политики.
2. Щелкните правой кнопкой мыши Сетевые политики и выберите команду Новый документ.
3. В мастере создания политик сетей на странице Укажите имя политики сети и тип подключения в поле Имя политики введите Работоспособный клиент без ограничений и нажмите кнопку Далее.
4. На странице Укажите условия щелкните Добавить.
5. В диалоговом окне Выбор условия щелкните Политики работоспособности и нажмите кнопку Добавить.
6. В диалоговом окне Политики работоспособности в списке Политики работоспособности выберите Работоспособный клиент и нажмите кнопку ОК.
7. На странице Укажите условия нажмите кнопку Далее.
8. На странице Укажите разрешение доступа нажмите кнопку Далее.
9. На странице Настройка методов проверки подлинности снимите все флажки, установите только флажок Выполнять только проверку работоспособности компьютера и нажмите кнопку Далее.
10. На странице Настройка ограничений нажмите кнопку Далее.
11. На странице Настройка параметров в списке Параметры выберите Принудительное использование NAP.
12. В области результатов щелкните Разрешить полный доступ к сети и нажмите кнопку Далее.
13. На странице Завершение создания политики сети нажмите кнопку Готово.
14. Щелкните правой кнопкой мыши Сетевые политики и выберите команду Новый документ. В мастере создания политик сетей на странице Укажите имя политики сети и тип подключения в поле Имя политики введите Неработоспособный клиент с ограничениями и нажмите кнопку Далее.
15. На странице Укажите условия щелкните Добавить.

16. В диалоговом окне Выбор условия щелкните Политики работоспособности и нажмите кнопку Добавить.
17. В диалоговом окне Политики работоспособности в списке Политики работоспособности выберите Неработоспособный клиент и нажмите кнопку ОК. На странице Укажите условия нажмите кнопку Далее.
18. На странице Укажите разрешение доступа нажмите кнопку Далее.
19. На странице Настройка методов проверки подлинности снимите все флажки, установите только флажок Выполнять только проверку работоспособности компьютера и нажмите кнопку Далее.
20. На странице Настройка ограничений нажмите кнопку Далее.
21. На странице Настройка параметров в списке Параметры выберите Принудительное использование NAP.
22. В области результатов щелкните Разрешить ограниченный доступ и нажмите кнопку Далее.
23. На странице Завершение создания политики сети нажмите кнопку Готово.

**Задание 7. Настройте параметры NAP клиентов**

1. Переключитесь на компьютер CLIENT.
2. Запустите программу napclcfg.msc.
3. Включите клиент принудительного карантина для DHCP.
4. Закройте napclcfg.msc.
5. Запустите программу services.msc.
6. Настройте агент защиты доступа к сети для автоматического запуска, а затем вручную запустите этот агент.
7. Закройте services.msc.
8. Запустите mmc.exe.
9. Добавьте оснастку Редактор объектов групповой политики в консоль, используя значения по умолчанию.

10. В дереве консоли последовательно разверните узлы Политика «Локальный компьютер»/Конфигурация компьютера/Административные шаблоны/Компоненты Windows/Центр обеспечения безопасности. Дважды щелкните Включить центр обеспечения безопасности (только для компьютеров в домене), щелкните Включить и нажмите кнопку ОК.

11. Закройте консоль.

**Задание 8. Настройте клиентский компьютер на динамическое получение IPv4-адреса**

1. Нажмите кнопку Пуск, в поле Найти программы и файлы введите Сеть и в списке Панель управления (3) щелкните Центр управления сетями и общим доступом.

2. В левой области центра управления сетями и общим доступом щелкните Изменение параметров адаптера.

3. Щелкните правой кнопкой мыши Подключение по локальной сети и выберите пункт Свойства.

4. Настройте для адаптера следующие параметры.

5. Получить IP-адрес автоматически.

6. Получить адрес DNS-сервера автоматически.

Примечание. Настройте протокол TCP/IPv4.

**Задание 9. Проверьте защиту доступа к сети**

1. На  компьютере CLIENT откройте командную строку.

2. Введите команду ipconfig /release и нажмите клавишу ВВОД.

3. Введите команду ipconfig /renew и нажмите клавишу ВВОД.

4. Введите команду ipconfig /all и нажмите клавишу ВВОД.

Вопрос. Укажите DNS-суффикс для этого подключения.

Вопрос. Каково текущее состояние карантина?

**Результаты.** В ходе этого упражнения вы включили принудительное использование NAP для DHCP.

## Упражнение 6. Ограничение на приложения с помощью AppLocker

### Сценарий

Вас попросили заблокировать запуск WordPad на компьютерах пользователей исследовательского отдела.

В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Создайте объект групповой политики, чтобы применить правила исполняемых файлов AppLocker® по умолчанию.
2. Примените объект групповой политики к домену.
3. Проверьте правило AppLocker.

### Задание 1. Создайте объект групповой политики, чтобы применить правила исполняемых файлов AppLocker по умолчанию

1. Переключитесь на компьютер SERVER.
2. Последовательно разверните узлы Лес: domain.local и Домены.
3. Разверните узел domain.local.
4. Щелкните Объекты групповой политики.
5. Щелкните правой кнопкой мыши Объекты групповой политики и выберите Создать.
6. Назовите новый объект групповой политики Политика ограниченного использования WordPad и нажмите кнопку ОК.
7. Правой кнопкой мыши щелкните элемент Политика ограниченного использования WordPad и выберите команду Изменить.
8. Последовательно разверните Конфигурация компьютера, Политики, Конфигурация Windows и Параметры безопасности, Политики управления приложениями и AppLocker.
9. Выберите Правила исполняемых файлов, затем щелкните правой кнопкой мыши и выберите команду Создать новое правило.
10. Нажмите кнопку Далее.

11. На экране Разрешения выберите Запретить и нажмите кнопку Далее.
12. На экране Условия выберите Издатель и нажмите кнопку Далее.
13. Нажмите кнопку Обзор..., затем щелкните Компьютер.
14. Дважды щелкните значок Локальный диск (C:).
15. Последовательно дважды щелкните Program Files, Windows NT, Стандартные, выберите wordpad.exe и нажмите кнопку Открыть.
16. Переместите ползунок вверх на Имя файла: и нажмите кнопку Далее.
17. Еще раз нажмите кнопку Далее и щелкните Создать.
18. При запросе на создание правил по умолчанию нажмите кнопку Да.
19. В редакторе групповых политик последовательно разверните узлы Конфигурация компьютера, Конфигурация Windows и Параметры безопасности.
20. Разверните узел Политики управления приложениями.
21. Щелкните AppLocker, затем щелкните правой кнопкой мыши и выберите пункт Свойства.
22. На вкладке Применение в разделе Правила исполняемых файлов установите флажок Настроено и выберите Принудительное применение правил.
23. Нажмите кнопку ОК.
24. В редакторе групповых политик последовательно разверните узлы Конфигурация компьютера, Конфигурация Windows и Параметры безопасности.
25. Щелкните Системные службы, затем дважды щелкните Удостоверение приложения.
26. В диалоговом окне Свойства: удостоверение приложения установите флажок Определить следующий параметр политики
27. Выберите значение автоматически в поле Выберите режим запуска службы и нажмите кнопку ОК.

28. Закройте редактор управления групповыми политиками.

**Задание 2. Примените объект групповой политики к домену**

1. В окне управления групповыми политиками разверните Лес: domain.local.
2. Разверните узел Домены.
3. Разверните domain.local
4. Разверните Объекты групповой политики.
5. Перетащите Политика ограниченного использования WordPad к верхней части контейнера домена Contoso.com.
6. Нажмите кнопку ОК, чтобы связать объект групповой политики с доменом.
7. Закройте Консоль управления групповыми политиками.
8. Нажмите кнопку Пуск, в поле Найти программы и файлы введите cmd и нажмите клавишу ВВОД.
9. В окне командной строки введите gpupdate /force и нажмите клавишу ВВОД. Подождите, пока политика обновится.

**Задание 3. Проверьте правило AppLocker**

1. Войдите на компьютер CLIENT.
2. Обновите групповую политику, выполнив команду gpudate /force из командной строки.
3. Попытайтесь запустить программу Пуск – Все программы – Стандартные – WordPad.

Примечание. Политика AppLocker должна запрещать вам запуск этого приложения. Если приложение запустится, выйдите из компьютера CLIENT и войдите снова. Ограничение использования приложения включается после применения политики.

**Результаты**. В ходе этого упражнения вы заблокировали приложение с помощью AppLocker.

## Упражнение 7. Использование мастера настройки безопасности

**Сценарий**

Вас попросили с помощью мастера настройки безопасности создать политику безопасности для котроллеров домена contoso.com на основании конфигурации сервера NYC-DC1. Затем эта политика безопасности будет

преобразована в объект групповой политики, который будет развертываться на контроллерах домена с помощью групповой политики.

В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Создайте политику безопасности.
2. Преобразуйте политику безопасности в объект групповой политики.

**Задание 1. Создайте политику безопасности**

1. На компьютере SERVER нажмите кнопку Пуск, Администрирование и запустите Мастер настройки безопасности.
2. На странице Мастер настройки безопасности нажмите кнопку Далее.
3. На странице Действие настройки выберите Создать новую политику безопасности и нажмите кнопку Далее.
4. На странице Выбор сервера примите имя сервера по умолчанию SERVER и нажмите кнопку Далее.
5. На странице Обработка базы данных настройки безопасности можно щелкнуть Просмотр базы данных и просмотреть обнаруженную конфигурацию сервера.
6. Нажмите кнопку Далее.
7. На начальной странице раздела Настройка служб на основе ролей нажмите кнопку Далее.
8. На странице Выбор ролей сервера можно просмотреть обнаруженные параметры сервера, однако изменять их не следует. Нажмите кнопку Далее.
9. На странице Выбор клиентских возможностей можно просмотреть обнаруженные параметры сервера, однако изменять их не следует. Нажмите кнопку Далее.
10. На странице Выбор управления и других параметров можно просмотреть обнаруженные параметры, однако изменять их не следует. Нажмите кнопку Далее.
11. На странице Выбор дополнительных служб можно просмотреть обнаруженные параметры сервера, однако изменять их не следует. Нажмите кнопку Далее.

12. На странице Обработка неопределенных служб не изменяйте параметр по умолчанию Не изменять режим запуска этой службы. Нажмите кнопку Далее.

13. На странице Подтверждение изменений для служб в списке Просмотреть выберите Все службы.

14. Просмотрите параметры в столбце Текущий режим запуска, отражающем режимы запуска служб на компьютере SERVER, и сравните их с параметрами в столбце Режим запуска политики.

15. В списке Просмотреть выберите Измененные службы.

16. Нажмите кнопку Далее.

17. На начальной странице раздела Сетевая безопасность нажмите кнопку Далее.

18. На странице Правила сетевой безопасности можно проверить правила брандмауэра, полученные из конфигурации. Не меняйте никакие параметры. Нажмите кнопку Далее.

19. На начальной странице раздела Параметры реестра нажмите кнопку Далее.

20. На каждой из страниц раздела Параметры реестра проверьте параметры, не изменяя их, и нажмите кнопку Далее. Нажимайте кнопку Далее на всех страницах, пока не появится страница Сводка параметров реестра, просмотрите параметры и нажмите кнопку Далее.

21. На начальной странице раздела Политика аудита нажмите кнопку Далее.

22. На странице Политика аудита системы проверьте параметры, но не изменяйте их. Нажмите кнопку Далее.

23. На странице Сводка политики аудита проверьте параметры в столбцах Текущее значение и Параметр политики. Нажмите кнопку Далее.

24. На начальной странице раздела Сохранение политики безопасности нажмите кнопку Далее.

25. В поле Имя файла политики безопасности щелкните конец пути к файлу и введите Политика безопасности контроллера домена.
26. Нажмите кнопку Просмотр политики безопасности.
27. Нажмите кнопку Да.
28. Завершив изучение политики, закройте окно.
29. В мастере настройки безопасности нажмите кнопку Далее.
30. На странице Применение политики безопасности примите параметр по умолчанию Применить позже и нажмите кнопку Далее.
31. Нажмите кнопку Готово.

**Задание 2. Преобразуйте политику безопасности в объект групповой политики**

1. На компьютере SERVER нажмите кнопку Пуск, в поле Найти программы и файлы введите cmd и нажмите клавишу ВВОД.
2. Введите команду cd c:\windows\security\msscw\policies и нажмите клавишу ВВОД.
3. Введите команду scwcmd transform /p:”Политика безопасности контроллера домена.xml” /g:”DC Security Policy” и нажмите клавишу ВВОД.
4. Закройте окно командной строки.
5. Нажмите кнопку Пуск, щелкните Администрирование, затем Управление групповой политикой.
6. В дереве консоли последовательно разверните узлы Лес:domain.local, Домены, domain.local и Объекты групповой политики и щелкните DC Security Policy. Это объект групповой политики, созданный командой Scwcmd.exe.
7. Перейдите на вкладку Параметры, чтобы просмотреть параметры объекта групповой политики.
8. Закройте Консоль управления групповыми политиками.

## Лабораторная работа 7. Наблюдение за производительностью сервера

### Сценарий

Несколько новых серверов успешно развернуты в филиалах компании. Перед вводом системы в эксплуатацию вы решили определить базовый уровень производительности, чтобы иметь возможность сравнить будущую рабочую нагрузку с предполагаемой рабочей нагрузкой.

## Упражнение 1. Определение базового уровня производительности

### Сценарий

Вы загрузите на сервере системный монитор и рассчитаете базовый уровень с использованием обычных счетчиков производительности.

В рамках данного упражнения необходимо выполнить следующие основные задачи:

1. Создайте группу сборщиков данных.
2. Запустите группу сборщиков данных.
3. Обеспечьте нагрузку на сервер.
4. Проанализируйте собранные данные.

### Задание 1. Создайте группу сборщиков данных

1. Откройте системный монитор.
2. Создайте новую пользовательскую группу сборщиков данных, используя для завершения процесса следующую информацию.
    - Имя: **Производительность *имя_сервера***
    - Создать: **Создать вручную (для опытных)**
    - Тип данных: **Счетчик производительности**
    - Выберите следующие счетчики:
        - Процессор, % загруженности процессора.
        - Память, Обмен страниц/с
        - Физический диск, % активности диска
        - Физический диск, средняя длина очереди диска
        - Система, длина очереди процессора

- Сетевой интерфейс, Всего байт/с

- Интервал выборки: **1 секунда**

- Где хранить данные: значение по умолчанию

3. Сохраните и закройте группу сборщиков данных.

**Задание 2. Запустите группу сборщиков данных**

1. В области результатов системного монитора щелкните правой кнопкой мыши **Производительность *имя_сервера*** и щелкните **Пуск**.

**Задание 3. Обеспечьте нагрузку на сервер**

1. Откройте командную строку и выполните следующие команды,нажимая после каждой клавишу ВВОД.

   - Fsutil file createnew bigfile 104857600

   - Copy bigfile *имя_сервера*\c$

   - Copy \\ *имя_сервера*\c$\bigfile bigfile2

   - Del bigfile*.*

   - Del \\ *имя_сервера*\c$\bigfile*.*

2. Не закрывайте командную строку.

**Задание 4. Проанализируйте собранные данные**

1. Переключитесь на **Системный монитор**.

2. Остановите работу группы сборщиков данных **Производительность *имя_сервера***.

3. На панели навигации окна «Системный монитор» щелкните **Системный монитор**.

4. На панели инструментов щелкните **Просмотр данных журнала**.

5. В диалоговом окне **Свойства: Системный монитор** на вкладке **Источник** щелкните **Файлы журнала** и нажмите кнопку **Добавить**.

6. В диалоговом окне **Выбор файла журнала** дважды щелкните **Admin**.

7. Последовательно дважды щелкните **Производительность**, папку **имя_сервера_date-000001** и файл **DataCollector01**.

8. Перейдите на вкладку **Данные** и нажмите кнопку **Добавить**.
9. Выберите следующие счетчики:
    - Процессор, % загруженности процессора.
    - Память, Обмен страниц/с
    - Физический диск, % активности диска
    - Физический диск, средняя длина очереди диска
    - Система, длина очереди процессора
    - Сетевой интерфейс, Всего байт/с
10. Нажмите на панели инструментов стрелку вниз и выберите пункт **Отчет**.
11. Запишите значения, перечисленные в отчете, чтобы проанализировать их позже.

    **Записанные значения:**

    - Процессор, % загруженности процессора.
    - Память, Обмен страниц/с
    - Физический диск, % активности диска
    - Физический диск, средняя длина очереди диска
    - Система, длина очереди процессора
    - Сетевой интерфейс, Всего байт/с

**Результаты.** В ходе этого упражнения вы рассчитали базовый уровень.

## Упражнение 2. Сбор дополнительных данных о производительности

### Сценарий

Пользователи жалуются на низкую производительность сервера, а вы разбираетесь, в чем дело, используя созданную ранее группу сборщиков данных.

### Задание. Снова запустите группу сборщиков данных

1. Переключитесь на **Системный монитор**.
2. Запустите группу сборщиков данных **Производительность *имя_сервера***.

3. Подождите одну минуту, пока записываются данные.

**Результаты.** В ходе этого упражнения вы записали дополнительные данные о производительности.

## Упражнение 3. Определение возможных «узких мест» в производительности

### Сценарий

Результаты, полученные под новой нагрузкой, сравниваются с результатами при изначальном развертывании сервера.

В рамках данного упражнения необходимо выполнить следующие основные задачи.

1. Остановите работающую программу.
2. Просмотрите данные производительности.
3. Проанализируйте результаты и сделайте вывод.

### Задание 1. Остановите работающую программу

1. В командной строке нажмите комбинацию клавиш CTRL + C и закройте командную строку.

### Задание 2. Просмотрите данные производительности

1. Переключитесь на **Системный монитор**.
2. Остановите группу сборщиков данных.
3. На панели навигации окна «Системный монитор» щелкните **Системный монитор**.
4. На панели инструментов щелкните **Просмотр данных журнала**.
5. В диалоговом окне **Свойства: Системный монитор** на вкладке **Источник** щелкните **Файлы журнала** и нажмите кнопку **Удалить**.
6. Нажмите кнопку **Добавить**.
7. В диалоговом окне **Выбор файла журнала** щелкните **На один уровень вверх**.
8. Последовательно дважды щелкните папку **SERVER_date-000002** и файл **DataCollector01**.
9. Перейдите на вкладку **Данные** и нажмите кнопку **ОК**.

**Примечание.** Если в этот момент вы получили ошибку или в отчете содержатся нулевые значения, повторите действия 4–9.

**Записанные значения:**

- Процессор, % загруженности процессора.
- Память, Обмен страниц/с
- Физический диск, % активности диска
- Физический диск, средняя длина очереди диска
- Система, длина очереди процессора
- Сетевой интерфейс, Всего байт/с

**Задание 3. Проанализируйте результаты и сделайте вывод**

1. Какие значения изменились по сравнению с предыдущим отчетом?
2. Что бы вы порекомендовали?

**Результаты.** В ходе этого упражнения вы обнаружили потенциальное «узкое место».

## Список литературы


1. Митч Таллоч. Знакомство с Windows Server 2008. – Изд-во «Русская Редакция», БХВ-Петербург. – 2008.
2. Митч Таллоч. Windows Server 2008 Server Core. Справочник администратора. - Изд-во «Русская Редакция», БХВ-Петербург. – 2010.
3. Уильям Р. Станек Windows Server 2008. Справочник администратора. - Изд-во «Русская Редакция», БХВ-Петербург. – 2008.
4. Дж. К. Макин, Анил Десаи. Развертывание и настройка Windows Server 2008. Учебный курс Microsoft. - Изд-во «Русская Редакция». – 2008.
5. Роберт Ларсон, Жаник Карбон. Платформа виртуализации Hyper-V. Ресурсы Windows Server 2008. - Изд-во «Русская Редакция», БХВ-Петербург. – 2010.
6. Джеспер М. Джоханссон. Обеспечение безопасности. Ресурсы Windows Server 2008. - Изд-во «Русская Редакция», БХВ-Петербург. – 2009.
7. Орин Томас, Джон Поличелли, Йен Маклин, Дж. К. Макин, Пол Менкьюзо, Дэвид Р. Миллер. Администрирование корпоративных сетей на основе Windows Server 2008. - Изд-во «Русская Редакция». – 2009.
8. Дэн Холме, Нельсон Рест, Даниэль Рест. Настройка Active Directory. Windows Server 2008. - Изд-во «Русская Редакция». – 2009.
9. Рэнд Моримото, Майкл Ноэл, Омар Драуби, Росс Мистри, Крис Амарис. Microsoft Windows Server 2008 R2. Полное руководство - Изд-во «Вильямс». – 2010.
10. #10712 Основы Windows 2008 Server. Официальный курс Microsoft.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

---

## КАФЕДРА ПРОГРАММНЫХ СИСТЕМ

Кафедра **Программных систем** входит в состав нового факультета **Инфокоммуникационные технологии**, созданного решением Ученого совета университета 17 декабря 2010 г. по предложению инициативной группы сотрудников, имеющих большой опыт в реализации инфокоммуникационных проектов федерального и регионального значения.

На кафедре ведется подготовка бакалавров и магистров по направлению **210700 «Инфокоммуникационные технологии и системы связи»:**
**210700.62.10 – ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ (Бакалавр)**
**210700.68.10 – ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ (Магистр)**

Выпускники кафедры получают фундаментальную подготовку по: математике, физике, электронике, моделированию и проектированию инфокоммуникационных систем (ИКС), информатике и программированию, теории связи и теории информации.

В рамках профессионального цикла изучаются дисциплины: архитектура ИКС, технологии программирования, ИКС в Интернете, сетевые технологии, администрирование сетей Windows и UNIX, создание программного обеспечения ИКС, Web программирование, создание клиент-серверных приложений.

**Область профессиональной деятельности бакалавров и магистров включает:**

- сервисно-эксплуационная в сфере современных ИКС;
- расчетно-проектная при создании и поддержке сетевых услуг и сервисов;

- экспериментально-исследовательская;
- организационно-управленческая – в сфере информационного менеджмента ИКС.

**Знания выпускников востребованы:**

- в технических и программных системах;
- в системах и устройствах звукового вещания, электроакустики, речевой, и мультимедийной информатики;
- в средствах и методах защиты информации;
- в методах проектирования и моделирования сложных систем;
- в вопросах передачи и распределения информации в телекоммуникационных системах и сетях;
- в методах управления телекоммуникационными сетями и системами;
- в вопросах создания программного обеспечения ИКС.

**Выпускники кафедры Программных систем обладают компетенциями:**

- проектировщика и разработчика структур ИКС;
- специалиста по моделированию процессов сложных систем;
- разработчика алгоритмов решения задач ИКС;
- специалиста по безопасности жизнедеятельности ИКС;
- разработчика сетевых услуг и сервисов в ИКС;
- администратора сетей: UNIX и Windows;
- разработчика клиентских и клиент-серверных приложений;
- разработчика Web – приложений;
- специалиста по информационному менеджменту;
- менеджера проектов планирования развития ИКС.

**Трудоустройство выпускников:**

1. ОАО «Петербургская телефонная сеть»;
2. АО «ЛЕНГИПРОТРАНС»;
3. Акционерный коммерческий Сберегательный банк Российской Федерации;
4. ОАО «РИВЦ-Пулково»;
5. СПБ ГУП «Петербургский метрополитен»;
6. ООО «СоюзБалтКомплект»;
7. ООО «ОТИС Лифт»;
8. ОАО «Новые Информационные Технологии в Авиации»;
9. ООО «Т-Системс СиАйЭс» и др.

**Кафедра** сегодня имеет в своем составе высококвалифицированный преподавательский состав, в том числе:

- 5 кандидатов технических наук, имеющих ученые звания профессора и доцента;
- 4 старших преподавателя;
- 6 штатных совместителей, в том числе кандидатов наук, профессиональных IT - специалистов;

- 15 Сертифицированных тренеров, имеющих Западные Сертификаты фирм: Microsoft, Oracle, Cisco, Novell.

Современная техническая база; лицензионное программное обеспечение; специализированные лаборатории, оснащенные необходимым оборудованием и ПО;качественная методическая поддержка образовательных программ; широкие Партнерские связи существенно влияют на конкурентные преимущества подготовки специалистов.

Авторитет специализаций кафедры в области компьютерных технологий подтверждается Сертификатами на право проведения обучения по методикам ведущих Западных фирм - поставщиков аппаратного и программного обеспечения.

Заслуженной популярностью пользуются специализации кафедры ПС по подготовке и переподготовке профессиональных компьютерных специалистов с выдачей **Государственного Диплома** о профессиональной переподготовке по направлениям: **"Информационные технологии (инженер-программист)"** и **"Системный инженер"**, а также Диплома о дополнительном (к высшему) образованию с присвоением квалификации: **"Разработчик профессионально-ориентированных компьютерных технологий "**. В рамках этих специализаций высокопрофессиональные преподаватели готовят компетентных компьютерных специалистов по современным в России и за рубежом операционным системам, базам данных и языкам программирования ведущих фирм: Microsoft, Cisco, IBM, Intel, Oracle, Novell и др.

Профессионализм, компетентность, опыт, и качество программ подготовки и переподготовки IT- специалистов на кафедре ПС неоднократно были удостоены **высокими наградами «Компьютерная Элита» в номинации лучший учебный центр России**.

**Партнеры:**

1. **Microso**ft Certified Learning Solutions;
2. **Novell** Authorized Education Center;
3. **Cisco** Networking Academy;
4. **Oracle** Academy;
5. **Sun Java** Academy и др;
6. **Prometric**;
7. **VUE**.

**Мы готовим квалифицированных инженеров в области инфокоммуникационных технологий с новыми знаниями, образом мышления и способностями быстрой адаптации к современным условиям труда.**

Сергей Эдуардович Хоружников
Виктор Викторович Прыгун

# Администрирование сетей Windows

**УЧЕБНОЕ ПОСОБИЕ**

В авторской редакции
Редакционно-издательский отдел НИУ ИТМО
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

**Редакционно-издательский отдел**
Санкт-Петербургского национального
исследовательского университета
информационных технологий, механики
оптики
197101, Санкт-Петербург, Кронверкский пр., 49