Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новгородский государственный университет имени Ярослава Мудрого»
МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ
ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ
Учебно-методическая документация

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

ОП.10 АДМИНИСТРИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ

Специальность:
09.02.03 Программирование в компьютерных системах
Квалификация выпускника: техник-программист

Разработчики: Карпинский Виктор Болеславович, к.т.н.
Сазонова Наталья Владимировна, преподаватель высшей категории

Методические приняты на заседании предметной цикловой комиссия профессионального цикла Политехнического колледжа протокол № 1 от 05. 09. 2016 г.

Председатель предметной (цикловой) комиссии _____ Н.В. Сазонова

Содержание

1. Пояснительная записка

Методические рекомендации по организации и выполнению самостоятельной работы, являющиеся частью учебно-методического комплекса по дисциплине «Администрирование компьютерных сетей» ОП.10 составлены в соответствии с:

1. Федеральным государственным образовательным стандартом по специальности 09.02.03 «Программирование в компьютерных системах»;
2. Рабочей программой учебной дисциплины;
3. Положением о планировании, организации и проведении лабораторных работ и практических занятий студентов, осваивающих основные профессиональные образовательные программы среднего профессионального образования в колледжах НовГУ.

Методические рекомендации включают внеаудиторную работу студентов, предусмотренную рабочей программой учебной дисциплины «Администрирование компьютерных сетей» в объёме 46 часов.

Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя и при методическом руководстве преподавателя, но без его непосредственного участия.

Формами внеаудиторной самостоятельной работы являются:

- поиск источников информации по заданной теме;
- изучение литературы по проблемам дисциплины;
- конспектирование, написание рефератов;
- подготовку к практическим работам, работа со справочниками;
- выполнение домашних практических заданий.

Преобладающим типом самостоятельной работы является подготовка сообщений и рефератов для выступления на занятиях с целью отработки навыков публичных выступлений, умений грамотно излагать материал, рассуждать.

Написание реферата является необходимым компонентом профессиональной подготовки студента в рамках освоения курса «Администрирование компьютерных сетей». Основная его задача состоит в том, чтобы на примере рассмотрения одной из актуальных тем развить навыки самостоятельной работы с информационно-аналитической литературой. В тексте реферата его автор должен продемонстрировать достаточный уровень логико-методологической культуры мышления, творческий подход к исследованию конкретной научной проблемы в контексте её понимания и интерпретации.

В результате выполнения самостоятельной работы обучающийся должен:

уметь:

- настраивать и администрировать Windows Server 2008;
- использовать методы и средства мониторинга и конфигурирования сетевых служб и систем;
- использовать средства защиты и восстановления системы и данных.

- **знать:**

- принципы построения открытых системы и «клиент-серверных» технологий;
- основные типы сетевых топологий;
- основные сетевые протоколы администрирования вычислительных сетей;
- информационные ресурсы компьютерных сетей;
- технологии передачи и обмена данными в компьютерных сетях;

- методы и средства информационных и телекоммуникационных технологий,
- основы защиты информации и обеспечения сетевой безопасности;
- основы администрирования в операционной системе Windows Server 2008

2. Тематический план и содержание учебной дисциплины «Администрирование компьютерных сетей»

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Раздел 1.	**Основные сведения о компьютерных сетях**	**18**	
Тема 1.1. Назначение и классификация компьютерных сетей.	**Содержание учебного материала**	2	**1**
	Назначение и классификация компьютерных сетей. Типы компьютерных сетей. Понятие топологии сетей. Основные сетевые устройства.		
	Практические занятия: Практическая работа № 1. Построение диаграммы сети, используя базовые топологии.	1	**2**
	Практическая работа № 2. Локально- вычислительные сети (ЛВС). Типы ЛВС.	1	
	Практическая работа № 3. Логическая структуризация сети с помощью мостов и коммутаторов.	2	
Тема 1.2. Основные понятия семиуровневой модели сетевого взаимодействия OSI.	**Содержание учебного материала**	2	**1**
	Основные понятия семиуровневой модели сетевого взаимодействия OSI. Процесс передачи информации между стеками OSI для компьютеров, объединенных в сеть. Применение модели OSI. Сравнение семиуровневой модели OSI с моделью TCP/IP.		
Тема 1.3. Среды передачи информации	**Содержание учебного материала**	2	**1**
	Понятие пропускной способности и полосы пропускания. Физические основы распространения сигналов. Типы коммуникационной среды. Типы медных кабелей. Оптические кабели. Беспроводные коммуникации.		
	Практические занятия: Практическая работа № 4. Построение организационной диаграммы предприятия. Диаграммы информационных потоков в сети подразделения	2	**2**
Тема 1.4. Методы передачи	**Содержание учебного материала**		
	Методы передачи данных в локальных сетях: Ethernet, Token Ring, FDDI.	2	**1**

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
данных в локальных сетях: Ethernet, Token Ring, FDDI.	**Практические занятия:** Практическая работа № 5. Проектирование и создание ЛВС в организации с помощью программы MS Visio 2003.	2	**2**
Тема 1.5. Протоколы стека TCP/IP. Принципы IP адресации.	**Содержание учебного материала**	2	**1**
	Протоколы стека TCP/IP. Принципы IP адресации. Роль маски подсети.		
Раздел 2.	**Администрирование операционной системы Windows Server 2008.**	**60**	
Тема 2.1. Семейство серверных операционных систем Windows.	**Содержание учебного материала**	1	**1**
	Сетевые операционные системы. Одноранговые операционные системы и ОС с выделенными серверами. Сравнение версий Windows Server. Основные возможности систем Windows Server 2008. Обязанности системного администратора.		
	Практические занятия: Практическая работа №6. Диагностические команды Windows XP TCP/IP.	2	**2**
Тема 2.2 Консоль управления MMC. Удаленное управление компьютерами с помощью консоли.	**Содержание учебного материала**	2	**1**
	Практические занятия: Практическая работа №7. Создание и сохранение консолей. Добавление компьютера для удаленного управления.		
	Практическая работа №8. Управление серверами с помощью программы Удаленный рабочий стол для администрирования.	2	**2**
Тема 2.3 Средства мониторинга и	**Содержание учебного материала**	2	**1**
	Средства мониторинга и оптимизации. Диспетчер задач Task Manager. Мониторинг процессов. Мониторинг сети. Просмотр системных событий.		

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
оптимизации Windows Server 2008.	Оснастка Event Viewer. Мониторинг производительности компьютера. Оснастка Performance. Оснастка Performance Logs and Alerts.		
	Практические занятия: Практическая работа № 9. Мониторинг производительности системы. Просмотр создание и настройка параметров журналов. Мониторинг производительности компьютера. Настройка счетчиков.	2	**2**
	Практическая работа № 10. Мониторинг производительности системы. Просмотр создание и настройка параметров журналов. Мониторинг производительности компьютера. Настройка счетчиков.	2	
Тема 2.4 Работа с дисковыми ресурсами.	**Содержание учебного материала**		
	Работа с дисковыми ресурсами. Оснастка Disk Management. Управление общими дисковыми ресурсами.	2	**1**
	Практические занятия: Практическая работа №11. Управление дисковой памятью в Windows Server 2008. Работа с динамическими дисками. Дефрагментация дисков. Управление общими дисковыми ресурсами.	2	**2**
Тема 2.5. Проектирование доменов и развертывание службы Active Directory.	**Содержание учебного материала**		
	Проектирование доменов. Формирование пространства имен. Функциональные уровни доменов и леса доменов. Установка контроллеров домена, Служба каталогов Active Directory. Администрирование доменов. Оснастки Active Directory - Users and Computers, Active Directory – Sites and Services, Active Directory -Domain and Trusts.	2	**1**
	Практические занятия: Практическая работа № 12. Служба каталогов Active Directory.	2	**2**
Тема 2.6. Серверы DHCP,	**Содержание учебного материала**		
	Знакомство с сервером DHCP. Установка и конфигурирование DHCP –	2	**1**

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
DNS и WINS	сервера. Знакомство с сервером DNS. Пространство имен DNS. Понятие и конфигурирование зон. Установка и конфигурирование DNS–сервера. Назначение WINS – сервера		
	Практические занятия: Практическая работа № 13. Сетевые адреса. Установка и авторизация службы DCHP Server.	2	**2**
	Практическая работа № 14. Сетевые адреса. Установка и авторизация службы DCHP Server.	2	
	Практическая работа №15. Обслуживание базы данных службы DCHP Server.	2	
	Практическая работа №16. Служба DNS. Создание и настройка зон авторизации службы DNS	2	
	Практическая работа № 17. Проверка работоспособности службы DNS Server.	2	
Тема 2.7 Создание и управление объектами пользователей. Управление профилями пользователей	**Содержание учебного материала**		
	Создание и управление объектами пользователей в консоли Active Directory - Users and Computers. Использование средств командной строки Active Directory. Управление профилями пользователей.	2	**1**
	Практические занятия: Практическая работа № 18. Создание и управление объектами пользователей из консоли Active Directory – пользователи и компьютеры.	2	**2**
	Практическая работа №19. Управление профилями пользователей.	2	
Тема 2.8 Понятие типа группы и области	**Содержание учебного материала**		
	Понятие типа группы и области действия группы. Управление учетными записями групп. Автоматизация управления учетными записями групп.	1	**1**

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
действия группы. Управление учетными записями групп	**Практические занятия:** Практическая работа №20. Учетные записи групп.	2	**2**
Тема 2.9 Службы печати.	**Содержание учебного материала**	1	**1**
	Службы печати. Удаленная печать в Windows Server 2008. Управление доступом к принтерам.		
	Практические занятия: Практическая работа №21. Управление доступом к принтерам. Опубликование информации об общих принтерах в Active Directory.	2	**2**
Тема 2.10 Использование групповых политик.	**Содержание учебного материала**	1	**1**
	Использование групповых политик. Настройка безопасности проверки подлинности при помощи политик. Аудит проверки подлинности.		
Тема 2.11 Создание и управление учетными записями компьютеров	**Содержание учебного материала**	2	**2**
	Практические занятия: Практическая работа № 22. Управление учетными записями компьютеров.		
Тема 2.12 Управление общими ресурсами.	**Содержание учебного материала**	1	**1**
	Настройка и управление общими папками. Оснастка Shared Folders.Настройка разрешений доступа к общему ресурсу. Настройка разрешений файловой системы. Наследование. Права владения ресурсом. Аудит доступа к файловой системе. Настройка параметров аудита Администрирование служб IIS**.**		
	Практические занятия: Практическая работа № 23. Настройка общих папок.	2	**2**

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
	Практическая работа № 24. Настройка разрешений файловой системы. Аудит доступа к файловой системе.	2	
	Практическая работа № 25. Проверка подлинности: безопасность и устранение неполадок.	2	
	Практическая работа № 26. Администрирование служб IIS.	2	
Тема2.13. Основы архивации данных.	**Содержание учебного материала**		
	Основы архивации данных. Определение стратегии архивации. Восстановление данных.	1	**1**
	Практические занятия: Практическая работа № 27. Различные типы архивации.	2	**2**
Раздел 3.	**Средства безопасности Windows Server 2008.**	**10**	
Тема 3.1. Основы и методы защиты информации.	**Содержание учебного материала**		
	Основы и методы защиты информации: источники и виды угроз информационной безопасности. Методы и средства защиты информации.	2	**1**
	Практические занятия: Практическая работа № 28 Настройка брандмауэра.	1	
	Практическая работа №29. Управление подключениями и безопасностью в Internet Explorer.	1	
	Практическая работа №30. Управление конфигурацией безопасности компьютера. Шаблоны безопасности.	2	**2**
	Практическая работа №31. Настройка протокола IPSec.	2	
	Практическая работа №32. Центры сертификации. Работа с EFS ((Encrypting File System).	2	
Самостоятельная работа. **Примерная тематика внеаудиторной самостоятельной работы:**		46	

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Подготовка рефератов по темам: «Принципы построения и архитектура ЭВМ и ВС». Изучение модели OSI. Выбор сетевой топологии и метода передачи данных для компании. Изучить теоретический материал «Локальные вычислительные сети (ЛВС)». Изучить теоретический материал «Программное обеспечение ЭВМ». Спроектировать структуру активного каталога Active Directory. Изучить основы безопасности при работе в сетях, научиться настраивать групповые политики для обеспечения дополнительной функциональности контроллеров домена, продумывать обеспечение безопасности контроллеров домена.			
	Всего по разделам	134	
	Обязательная учебная нагрузка, часов	88	
	Лекции	28	
	Практические занятия	60	
	Самостоятельная работа обучающихся	46	

3. Тематика самостоятельных работ

Название темы	Количество часов, отведенных на выполнение работы
1. Принципы построения и архитектура ЭВМ и ВС.	8
2. Изучение модели OSI. Выбор сетевой топологии и метода передачи данных для компании.	8
3. Локальные вычислительные сети (ЛВС).	6
4. Программное обеспечение ЭВМ. Структура программного обеспечения ЭВМ. Операционные системы	6
5. Проектирование домена.	8
6. Защита информации в компьютерных системах. Защита контроллеров домена Windows Server 2008. Защита информации от несанкционированного доступа	10

4. Содержание самостоятельной работы

Самостоятельная внеаудиторная работа № 1. Принципы построения и архитектура ЭВМ и ВС.

Раздел 1. Основные сведения о компьютерных сетях.

Тема 1.1. Назначение и классификация компьютерных сетей.

Самостоятельная внеаудиторная работа– 8ч.

1. **Цель работы:** изучить архитектуру персонального компьютера вычислительной сети.
2. **Задание к работе**

Написать реферат по теме «Принципы построения и архитектура ЭВМ и ВС».

Примерное содержание:

1. Общие принципы построения современных ЭВМ;
2. История развития ВТ (ЭВМ);
3. Модульность построения, магистральность, иерархия управления;
4. Архитектура вычислительных систем;
5. Назначение, область применения и способы оценки производительности многопроцессорных вычислительных систем.

.**Требования к результатам работы**

- ✓ соответствие выполненного задания предлагаемой теме;
- ✓ глубина и качество проработки основных разделов темы;
- ✓ оригинальность предлагаемых решений;
- ✓ качество оформления материала.

Методические указания к написанию реферата представлены в приложении

3. **Форма контроля и критерии оценки**

Оценка **«отлично»** ставится студенту, если;

- работа оформлена аккуратно, без помарок, ответы конкретные, лаконичные;

Оценка **«хорошо»** ставится студенту если:

- ответы конкретные и лаконичные, но могут быть незначительные неточности;

Оценка **«удовлетворительно»** ставится если:

- задание не выполнено до конца, ответы содержат некоторые неточности;

Оценка **«неудовлетворительно»** ставится если:

- допущены принципиальные ошибки, работа оформлена небрежно;

4. Список рекомендуемой литературы:

Основная литература:

1. Кузин А.В. Компьютерные сети: учебное пособие / А.В. Кузин. – 3-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА – М, 2014. – 192 с.: ил. – (Профессиональное образование).
2. Эксплуатация объектов сетевой инфраструктуры: учебник для студентов учреждений сред. проф. Образования / [А.В. Назаров, В.П. Мельников, А.И. Куприянов, А.Н. Енгалычев]; под редакцией А.В. Назарова. – М.: Издательский центр «Академия», 2014. – 368 с.

Дополнительная литература:

3. Клейменов С.А. Администрирование в информационных системах: учеб.пособие для вузов.- М.:Академия, 2008.- 272 с.
4. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, программы. - СПб:Питер, 2008.-672 с.
5. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс

Самостоятельная внеаудиторная работа № 2. Изучение модели OSI. Выбор сетевой топологии и метода передачи данных для компании.

Раздел 1. Основные сведения о компьютерных сетях.

Тема 1.4. Методы передачи данных в локальных сетях: Ethernet, Token Ring, FDDI.

Самостоятельная внеаудиторная работа – 8ч.

1. **Цель работы:** закрепить теоретический материал по теме, изучить функции уровне модели OSI, изучить основные компоненты локальной сети типа Ethernet и маркерное кольцо.
2. **Задание к работе**

Задание 1.

В предлагаемом сценарии необходимо выбрать метод передачи данных и топологию сети для компании «Мастер чертежа», которая является клиентом вашего работодателя – фирмы «Сетевой консультант». Также вам нужно будет помочь своему новому коллеге лучше понять модель OSI.

В компании «Мастер чертежа» работают 20 чертежников, реализующих схемные решения или схематические изображения, поступающие от инженеров – электротехников. Большинство заказчиков компании – фирмы, входящие в состав компании «Фортуна 2009» и сотрудничающие с ней в сфере разработки электрических схем, которые входят в пакет документации на серийные изделия. Компания «Мастер чертежа» заинтересована в реализации сети, связывающей отдельные рабочие станции чертежников, при этом особое внимание должно уделяться надежности и скоростным характеристикам, обеспечивающим передачу очень больших графических файлов.

Какой метод передачи данных – Ethernet или маркерное кольцо – вы посоветуете для реализации в новой сети? Почему?

Какую базовую топологию вы посоветуете (с учетом ваших знаний) данной компании?

Ваш новый коллега по компании «Сетевой консультант» не уверен в понимании некоторых аспектов модели OSI. У него есть к вам список вопросов, и он просит вас нарисовать таблицу, которую он смог бы использовать для ответов на свои вопросы. Создайте таблицу, имеющую два столбца и семь строк. Озаглавьте левый столбец «Сетевая функция», а правый – «Уровень OSI». Впишите каждую из перечисленных ниже функций в клетку левого столбца, а в правом столбце укажите уровень OSI, реализующий эту функцию. Итак, ваш коллега задает следующие вопросы.

- ✓ Какой уровень изменяет размер фреймов так, чтобы они соответствовали конечной сети?
- ✓ Какой уровень выполняет сжатие данных?
- ✓ Какой уровень гарантирует прием данных в том порядке, в каком они были посланы?
- ✓ Какой уровень управляет сигналом, передающим данные?
- ✓ Какой уровень поддерживает службы передачи файлов?
- ✓ Какой уровень реализует маршрутизацию?
- ✓ Какой уровень обеспечивает передачу подтверждения от принимающего узла?

Вашему коллеге понравилась таблица, и у него есть еще вопрос. Он хочет, чтобы вы объяснили ему принципы MAC – адресации.

Компания «Мастер чертежа» просит помочь в разработке способа электронного приема и передачи файлов своим заказчикам. Расскажите о трех возможностях

использования глобальных коммуникаций для этой цели. Какую из трех возможностей вы порекомендуете в данной ситуации.

Задание 2.

Компания «Наша торговля» хочет связать локальные сети, расположенные в принадлежащих ей пяти магазинах, находящихся в пяти населенных пунктах одной области. Расстояние между магазинами от 20 до 100 км. Предложите наилучший способ объединения локальных сетей магазинов в глобальную сеть.

Несколько консультантов вашей компании интересуются, как реализация доступа к Интернету соотносится с моделью OSI. Сделайте презентацию для других консультантов. В презентации предусмотрите пример, показывающий, как пользователь с помощью веб – браузера может обратиться к Интернету. Проследите взаимосвязи браузера и Интернета с уровнями OSI. Для лучшей иллюстрации вашего объяснения можно использовать таблицы или диаграммы.

3. Требования к результатам работы

Задание самостоятельной работы выполняется в два этапа:

1. изучение теоретического материала по заявленной теме и ответы на поставленные в заданиях вопросы;
2. написание отчета и создание презентации о проделанной работе.

Каждый этап оценивается определенным количеством баллов и выполняется в рамках отведенного времени на выполнение каждого задания. На выполнение работ первого этапа отводится неделя с момента получения самостоятельного задания. На выполнение работ второго этапа – две недели с момента завершения работ первого этапа. Несвоевременное выполнение отдельных этапов и работ в целом приводит к уменьшению количества баллов.

Работа над заданиями проводится вне учебного заведения и завершается представлением файла с отчетом о выполнении задания, а также файла - презентации.

4. Форма контроля и критерии оценки

Оцениваются:

- ✓ Правильность ответов, на поставленные в заданиях вопросы;
- ✓ Подробность и понятность отчета о проделанной работе;
- ✓ Качество презентаций.

За несвоевременное выполнение этапа и работы в целом баллы снижаются на 1 балл в неделю.

-если на поставленные в заданиях вопросы даны подробные, четко сформулированные ответы, отчет оформлен аккуратно, а презентации имеют продуманную структуру и отражают всю необходимую информацию, ставится оценка «5»;

- если на поставленные в заданиях вопросы даны подробные, четко сформулированные ответы, отчет оформлен неаккуратно, структура презентаций продумана, но в ней не отражена вся необходимая информация, ставится оценка «4»;

- если ответы на поставленные в заданиях вопросы плохо структурированы, отчет оформлен неаккуратно, презентация не полностью отражает проделанную работу, ставится оценка «3»;

- если ответы на поставленные в заданиях вопросы плохо структурированы и содержат явные ошибки, отчет оформлен неаккуратно, презентация не полностью отражает проделанную работу или не представлена, ставится оценка «2».

5. Список рекомендуемой литературы:

Основная литература:

1. Кузин А.В. Компьютерные сети: учебное пособие / А.В. Кузин. – 3-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА – М, 2014. – 192 с.: ил. – (Профессиональное образование).
2. Эксплуатация объектов сетевой инфраструктуры: учебник для студентов учреждений сред. проф. Образования / [А.В. Назаров, В.П. Мельников, А.И. Куприянов, А.Н. Енгалычев]; под редакцией А.В. Назарова. – М.: Издательский центр «Академия», 2014. – 368 с.

Дополнительная литература:

3. Майкл Палмер, Роберт Брюс Синклер Проектирование и внедрение компьютерных сетей. Санкт – Петербург «БХВ - Петербург», 2005, 740с.
4. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, программы. - СПб:Питер, 2008.-672 с.
5. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс

Самостоятельная внеаудиторная работа № 3. Локальные вычислительные сети (ЛВС)»

Раздел 1. Основные сведения о компьютерных сетях.

Тема 1.5. Протоколы стека TCP/IP. Принципы IP адресации.

Самостоятельная внеаудиторная работа – 6ч.

1. **Цель работы:** изучить топологии и оборудование ЛВС, протоколы передачи данных и методы доступа к передающей среде, программное обеспечение ЛВС.
2. **Задание к работе**

   Написать реферат по теме «Локальные вычислительные сети (ЛВС)».

   Примерное содержание:

   1. Типы и характеристики ЛВС;
   2. Протоколы передачи данных и методы доступа к передающей среде;
   3. Сетевое оборудование ЛВС;
   4. Программное обеспечение ЛВС;
   5. Функционирование ЛВС.

3. **Требования к результатам работы**
   - ✓ соответствие выполненного задания предлагаемой теме;
   - ✓ глубина и качество проработки основных разделов темы;
   - ✓ оригинальность предлагаемых решений;
   - ✓ качество оформления материала.

   Методические указания к написанию реферата представлены в приложении

4. **Форма контроля и критерии оценки**

   Оценка **«отлично»** ставится студенту, если;

   - работа оформлена аккуратно, без помарок, ответы конкретные, лаконичные;

   Оценка **«хорошо»** ставится студенту если:

   - ответы конкретные и лаконичные, но могут быть незначительные неточности;

   Оценка **«удовлетворительно»** ставится если:

   - задание не выполнено до конца, ответы содержат некоторые неточности;

   Оценка **«неудовлетворительно»** ставится если:

   - допущены принципиальные ошибки, работа оформлена небрежно;

5. **Список рекомендуемой литературы:**

Основная литература:

1. Кузин А.В. Компьютерные сети: учебное пособие / А.В. Кузин. – 3-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА – М, 2014. – 192 с.: ил. – (Профессиональное образование).
2. Эксплуатация объектов сетевой инфраструктуры: учебник для студентов учреждений сред. проф. Образования / [А.В. Назаров, В.П. Мельников, А.И. Куприянов, А.Н. Енгалычев]; под редакцией А.В. Назарова. – М.: Издательский центр «Академия», 2014. – 368 с.

Дополнительная литература:

3. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, программы. - СПб:Питер, 2008.-672 с.

4. Майкл Палмер, Роберт Брюс Синклер Проектирование и внедрение компьютерных сетей. Санкт – Петербург «БХВ - Петербург», 2005, 740с.
5. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс

Самостоятельная работа № 4. Программное обеспечение ЭВМ.

Раздел 2. Сетевые операционные системы. Базовая настройка сети.

Тема 2.1. Сетевые операционные системы.

Самостоятельная внеаудиторная работа – 6ч.

1. **Цель работы:** изучить структуру программного обеспечения, клиентские и серверные сетевые ОС.
2. **Задание к работе**

   Написать реферат по теме «Программное обеспечение ЭВМ».

   Примерное содержание:

   1. Структура программного обеспечения ЭВМ;
   2. Виды системного программного обеспечения;
   3. Операционные системы.

3. **Требования к результатам работы**

   соответствие выполненного задания предлагаемой теме;
   глубина и качество проработки основных разделов темы;
   оригинальность предлагаемых решений;
   качество оформления материала.

Методические указания к написанию реферата представлены в приложении

4. **Форма контроля и критерии оценки**

   Оценка **«отлично»** ставится студенту, если;

   - работа оформлена аккуратно, без помарок, ответы конкретные, лаконичные;

   Оценка **«хорошо»** ставится студенту если:

   - ответы конкретные и лаконичные, но могут быть незначительные неточности;

   Оценка **«удовлетворительно»** ставится если:

   - задание не выполнено до конца, ответы содержат некоторые неточности;

   Оценка **«неудовлетворительно»** ставится если:

   - допущены принципиальные ошибки, работа оформлена небрежно;

5. **Список рекомендуемой литературы:**

Основная литература:

1. Кузин А.В. Компьютерные сети: учебное пособие / А.В. Кузин. – 3-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА – М, 2014. – 192 с.: ил. – (Профессиональное образование).
2. Эксплуатация объектов сетевой инфраструктуры: учебник для студентов учреждений сред. проф. Образования / [А.В. Назаров, В.П. Мельников, А.И. Куприянов, А.Н. Енгалычев]; под редакцией А.В. Назарова. – М.: Издательский центр «Академия», 2014. – 368 с.

Дополнительная литература:

3. В.Г. Олифер Сетевые операционные системы.-СПб., 2002
4. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс

Самостоятельная работа № 5. Проектирование домена.

Раздел 3. Администрирование операционной системы Windows Server 2008.

Тема 3.6. Проектирование доменов и развертывание службы Active Directory.

Самостоятельная внеаудиторная работа– 8ч.

1. **Цель работы:** научиться проектировать структуру активного каталога Active Directory.
2. **Задание к работе**

«Сталелитейные технологии» - это компания, которая будет заниматься выпуском специальных легированных сплавов. Сплавы предполагается использовать в авиационных двигателях, тяжелом машиностроении, строительстве и других областях.

В составе компании имеются завод и заводоуправление, сеть которых нужно модернизировать. У компании имеется сервер, работающий под управлением операционной системы Windows Server 2008, расположенный в заводоуправлении и пять серверов, размещенных по всему заводу. Кроме этого, компания планирует создать учебную лабораторию, имеющую сервер и 25 клиентских рабочих станций. Эта лаборатория будет использоваться для постоянного обучения работников новым производственным технологиям. При этом обычно лаборатория будет загружена полностью. Лаборатория должна быть соединена с главной сетью завода.

Вы приняты на работу в качестве сетевого администратора, и вам необходимо развернуть Active Directory.

Соберите информацию об организационной структуре и состоянии сетевых коммуникаций предприятия.

Оцените общее количество пользователей вашей сети.

Оцените возможность увеличения числа пользователей.

Оцените состояние корпоративной вычислительной сети на физическом уровне. Соберите информацию о существующих коммуникационных линиях.

Продумайте:

- ✓ доменную структуру каталога (создание структуры доменов);
- ✓ логическую структуру каталога (создание подразделений);
- ✓ физическую структуру каталога (создание подсетей и сайтов).

Подготовьте схему, в которой будет отражаться доменная структура вашего предприятия.

3. **Требования к результатам работы**

Задание самостоятельной работы выполняется в два этапа:

1. изучение теоретического материала по заявленной теме и ответы на поставленные в заданиях вопросы;
2. написание отчета и создание презентации о проделанной работе.

Каждый этап оценивается определенным количеством баллов и выполняется в рамках отведенного времени на выполнение каждого задания. На выполнение работ первого этапа отводится неделя с момента получения самостоятельного задания. На выполнение работ второго этапа – две недели с момента завершения работ первого этапа. Несвоевременное выполнение отдельных этапов и работ в целом приводит к уменьшению количества баллов.

Работа над заданиями проводится вне учебного заведения и завершается представлением файла с отчетом о выполнении задания, а также файла - презентации

4. **Форма контроля и критерии оценки**

Оцениваются:

- ✓ Правильность ответов, на поставленные в заданиях вопросы;
- ✓ Подробность и понятность отчета о проделанной работе;
- ✓ Качество презентаций.

За несвоевременное выполнение этапа и работы в целом баллы снижаются на 1 балл в неделю.

-если на поставленные в заданиях вопросы даны подробные, четко сформулированные ответы, отчет оформлен аккуратно, а презентации имеют продуманную структуру и отражают всю необходимую информацию, ставится оценка «5»;

- если на поставленные в заданиях вопросы даны подробные, четко сформулированные ответы, отчет оформлен неаккуратно, структура презентаций продумана, но в ней не отражена вся необходимая информация, ставится оценка «4»;

- если ответы на поставленные в заданиях вопросы плохо структурированы, отчет оформлен неаккуратно, презентация не полностью отражает проделанную работу, ставится оценка «3»;

- если ответы на поставленные в заданиях вопросы плохо структурированы и содержат явные ошибки, отчет оформлен неаккуратно, презентация не полностью отражает проделанную работу или не представлена, ставится оценка «2».

5. Список рекомендуемой литературы:

Основная литература:

1. Кузин А.В. Компьютерные сети: учебное пособие / А.В. Кузин. – 3-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА – М, 2014. – 192 с.: ил. – (Профессиональное образование).
2. Эксплуатация объектов сетевой инфраструктуры: учебник для студентов учреждений сред. проф. Образования / [А.В. Назаров, В.П. Мельников, А.И. Куприянов, А.Н. Енгалычев]; под редакцией А.В. Назарова. – М.: Издательский центр «Академия», 2014. – 368 с.

Дополнительная литература:

3. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
4. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)
5. Майкл Палмер, Роберт Брюс Синклер Проектирование и внедрение компьютерных сетей. Санкт – Петербург «БХВ - Петербург», 2005, 740с.
6. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008/2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.

Самостоятельная № 6. Защита информации в компьютерных системах. Защита контроллеров домена Windows Server 2008. Защита информации от несанкционированного доступа

Раздел 4. Средства безопасности Windows Server 2008.

Тема 4.1. Основы и методы защиты информации.

Самостоятельная внеаудиторная работа– 10ч.

1. **Цель работы:** изучить основы безопасности при работе в сетях, научиться настраивать групповые политики для обеспечения дополнительной функциональности контроллеров домена, продумывать обеспечение безопасности контроллеров домена.
2. **Задание к работе**

Контроллеры домена в сети — центральный элемент службы каталогов Active Directory. Они содержат сведения об учетных данных всех имеющихся пользователей, без которых последние не смогут войти в сеть и получить доступ к ресурсам, необходимым для выполнения повседневной работы.

Для повышения безопасности среды следует применять групповую политику, которая является технологией управления изменениями и конфигурацией, включенной в службу Active Directory на используемых контроллерах домена. Изучите инструкции по выполнению следующих задач:

- Защита контроллеров домена с помощью групповой политики.
- Настройка групповой политики для обеспечения дополнительной функциональности контроллеров домена.
- Защита службы DNS-сервера.
- Обеспечение безопасности контроллеров домена.
- Можно повысить безопасность контроллеров домена с помощью групповой политики. Для настройки групповой политики контроллеров домена выполните следующие задачи:
- Создание нового объекта групповой политики (GPO) и привязывание его к организационному подразделению (OU) контроллеров домена.
- Импорт основных параметров безопасности в новый объект GPO с помощью шаблона безопасности, который содержится в данном руководстве.
- Проверка новых параметров с помощью просмотра журнала приложений на контроллерах домена.

1. Развертывание базовой политики для контроллеров домена.

Необходимо один раз выполнить перечисленные ниже действия. Безопасность всех контроллеров домена будет повышена одновременно после настройка базовой политики контроллеров домена.

Для того чтобы базовая политика контроллеров домена вступила в силу, нужно перезапустить все контроллеры домена. Выполняйте все эти действия в нерабочее время, чтобы свести к минимуму неблагоприятные последствия для пользователей.

Требования:

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена».
- Средства. Active Directory — пользователи и компьютеры. Для доступа к этому средству нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools**

(Администрирование), а затем — **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).

- Файлы. Необходимо загрузить файл **Enterprise Client — Domain Controller.inf**, который поставляется вместе с руководством по безопасности Windows Server 2008. После загрузки этого файла скопируйте его в папку systemroot\Security\Templates на контроллере домена, для которого выполняются эти действия. (Например, в обычной конфигурации файл INF копируется в папку C:\Windows\Security\Templates.)

Задание 1. Загрузка файла Enterprise Client — Domain Controller.inf

1. На контроллере домена откройте окно веб-обозревателя и перейдите на страницу Windows Server 2008 Security Guide центра загрузки «Майкрософт» по адресу http://go.microsoft.com/fwlink/?LinkId=14846.
2. В нижней части страницы в разделе **Files in This Download** (Файлы для загрузки) щелкните файл **Windows_Server_2003_Security_Guide.exe**.
3. В диалоговом окне **File Download** (Загрузка файла) нажмите кнопку **Save** (Сохранить).
4. При выводе запроса о месте загрузки разверните поле со списком **Save in** (Сохранить в), выберите **Desktop** (Рабочий стол), а затем создайте новую папку для сохранения файла после загрузки, выполнив следующие действия:
5. Щелкните правой кнопкой мыши белое пространство в диалоговом окне **Save As** (Сохранить как), укажите на **New** (Создать), а затем выберите параметр **Folder** (Папка).
6. Введите описательное имя папки (замените выделенный текст *Новая папка* на описательное имя), дважды щелкните новую папку, чтобы выделить ее в списке **Save in** (Сохранить в), а затем нажмите кнопку **Save** (Сохранить).
7. После завершения загрузки в окне **Download complete** (Загрузка завершена) выберите команду **Close** (Закрыть).
8. В новой папке на рабочем столе дважды щелкните файл **Windows_Server_2003_Security_Guide.exe**, чтобы открыть WinZip Self-Extractor.
9. В диалоговом окне **WinZip Self-Extractor**:
10. Нажмите кнопку **Browse**, затем выберите папку, созданную для загрузки, щелкните папку, чтобы открыть ее, а затем нажмите кнопку **ОК**.
11. В диалоговом окне **WinZip Self-Extractor** нажмите кнопку **Unzip**. Будет выведено сообщение об успешной распаковке файлов.
12. В комплекте распакованных файлов и папок дважды щелкните на папке **Windows Server 2008 Security Guide**, чтобы открыть ее, откройте папки **Tools and Templates** (Средства и шаблоны), **Security Guide** (Руководство по безопасности), а затем откройте папку **Security Templates** (Шаблоны безопасности).
13. В папке **Security Templates** (Шаблоны безопасности) щелкните правой кнопкой мыши файл **Enterprise Client — Domain Controller.inf** и скопируйте его в папку *systemroot*\Security\Templates контроллера домена, на котором выполняются эти действия.

Задание 2. Создание нового объекта групповой политики в организационном подразделении контроллеров домена.

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры), а затем дважды щелкните домен для развертывания дерева домена.
2. Щелкните правой кнопкой мыши организационное подразделение **Domain Controllers** (Контроллеры домена) и выберите команду **Properties** (Свойства).

3. В диалоговом окне свойств откройте вкладку **Group Policy** (Групповая политика), а затем выберите команду **New** (Создать) для создания нового объекта групповой политики.
4. Назовите политику **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а затем нажмите кнопку **Close** (Закрыть).

Задание 3. Импорт основных параметров безопасности в базовую политику котроллеров домена

1. Щелкните правой кнопкой мыши организационное подразделение **Domain Controllers** (Контроллеры домена) и выберите команду **Properties** (Свойства).
2. В диалоговом окне свойств откройте вкладку **Group Policy** (Групповая политика), а затем выберите **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена).
3. Выберите команду **Up** (Вверх) для перемещения нового объекта групповой политики в начало списка, а затем нажмите кнопку **Edit** (Изменить).
4. Убедитесь, что изменения выполняются для параметра **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а не **Default Domain Controllers Policy** (Политика по умолчанию для контроллеров домена). Неправильные изменения параметра **Default Domain Controllers Policy** (Политика по умолчанию для контроллеров домена) могут неблагоприятно повлиять на используемую среду, и их последствия трудно будет устранить.
5. В разделе **Computer Configuration** (Конфигурация компьютера) дважды щелкните папку **Windows Settings** щелкните правой кнопкой мыши **Security Settings** (Параметры безопасности), а затем выберите **Import Policy** (Импорт политики).
6. В диалоговом окне **Import Policy From** (Импорт политики из) выберите файл **Enterprise Client — Domain Controller.inf**, а затем — команду **Open** (Открыть).
7. Закройте окно **Group Policy Object Editor** (Редактор объектов групповой политики), нажмите кнопку **OK**, чтобы закрыть диалоговое окно, и выйдите из окна **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).
8. Перезапустите по одному контроллеры доменов.

Не перезапускайте все контроллеры доменов одновременно, поскольку пользователи могут испытывать трудности при доступе в сеть или к сетевым ресурсам, если не будет доступен ни один контроллер домена.

После настройки параметров безопасности групповой политики убедитесь, что параметры были успешно применены.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена».
- Средства. Средство «Просмотр событий» и службы.
- Убедитесь, что журнал событий приложения на каждом из контроллеров домена содержит код события 1704.

Задание 4. Проверка журнала событий приложения.

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), щелкните **Administrative Tools** (Администрирование), а затем —**Event Viewer** (Просмотр событий).
2. В окне **Event Viewer** (Просмотр событий) выберите **Application** (Приложение), а затем найдите самое последнее событие:
   a) **Type** (Тип): Данные;
   b) **Source** (Источник): SceCli;
   c) **Event ID** (Событие): 1704;

3. Если дважды щелкнуть это событие, появится окно **Event Properties** (Свойство: Событие), похожее на следующее:
4. Нажмите кнопку **OK** и закройте окно Event Viewer (Просмотр событий).
5. Затем убедитесь, что на контроллерах домена отключены ненужные службы.

Задание 5. Проверка отключенных служб.

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), а затем — **Services** (Службы).
2. Убедитесь, что отключены **Alerter** (Оповещатель), **Messenger** (Служба сообщений) и **Task Scheduler** (Планировщик заданий) и в качестве типа запуска для них указано значение **Disabled** (Отключено).
   Примечание. Три службы, перечисленные при описании шага 2, включены по умолчанию в Microsoft Windows Server 2008. Не только эти службы отключаются с помощью базовой политики контроллеров доменов, но проверка их конфигурации позволит убедиться, что параметры новой групповой политики вступили в действие.
3. Закройте средство **Services** (Службы).

Задание 6. Включение дополнительных служб на контроллерах домена.

Базовая политика контроллеров домена, которая была применена в предыдущем разделе, отключает несколько служб, которые не используются для обеспечения основных функциональных возможностей контроллера домена. Такое изменение конфигурации позволяет повысить безопасность контроллеров домена, однако оно мешает правильной работе отдельных служб, которую контроллеры домена обычно обеспечивают в организациях малого и среднего бизнеса.

Описанные далее шаги показывают, как можно изменить групповую политику для повторного включения дополнительных служб. Изучите перечисленные ниже задачи и выполните их на контроллерах домена, только если для работы сети требуются дополнительные функции, обеспечиваемые этими службами:

- Включение служб DHCP;
- Включение служб WINS;
- Включение служб печати;
- Включение служб IAS;
- Включение служб сертификатов;
- Включение и защита службы «Планировщик задач»;

Если один из контроллеров домена настроен как DHCP-сервер, нужно изменить параметры групповой политики контроллера домена для обеспечения работы служб DHCP в имеющейся среде. В этом разделе содержатся инструкции по настройке групповой политики для повторного включения служб DHCP.

Для повторного включения службы DHCP-сервера нужно изменить параметр **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена) на контроллерах домена. Выполнение этих действий позволяет включить службу DHCP-сервера на всех контроллерах домена, которые обеспечивают службы DHCP.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена».
- Анализ последствий для пользователей. Необходимо перезапустить контроллеры домена для выполнения этих действий. Следует выполнять все эти действия в нерабочее время, чтобы свести к минимуму неблагоприятные последствия для пользователей.

Настройка групповой политики для включения служб DHCP.

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры), а затем дважды щелкните домен для развертывания дерева домена.
2. Щелкните правой кнопкой мыши организационное подразделение **Domain Controllers** (Контроллеры домена) и выберите команду **Properties**(Свойства).
3. В диалоговом окне свойств откройте вкладку **Group Policy** (Групповая политика), выберите **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а затем нажмите кнопку **Edit** (Изменить).
2. Убедитесь, что изменения выполняются для параметра **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а не **Default Domain Controllers Policy**(Политика по умолчанию для контроллеров домена). Неправильные изменения параметра **Default Domain Controllers Policy** (Политика по умолчанию для контроллеров домена) могут неблагоприятно повлиять на используемую среду, и их последствия трудно будет устранить.
1. В разделе **Computer Configuration** (Конфигурация компьютера) дважды щелкните папку **Windows Settings**, щелкните правой кнопкой мыши **Security Settings** (Параметры безопасности), а затем выберите **System Services** (Системные службы).
2. В разделе сведений (правый раздел) дважды щелкните **DHCP Server** (DHCP-сервер), выберите параметр **Automatic** (Автоматически), а затем нажмите кнопку **OK**.
3. Закройте окно **Group Policy Object Editor** (Редактор объектов групповой политики), нажмите кнопку **OK**, чтобы закрыть диалоговое окно, и выйдите из окна **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).
4. Перезапустите по одному контроллеры доменов.

После изменения параметров групповой политики для включения службы DHCP убедитесь, что служба работает.

Задание 7. Проверка работы DHCP-службы.

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), а затем — **Services** (Службы).
2. Убедитесь, что DHCP-служба работает и настройте ее автоматический запуск.

Задание 8. Включение служб WINS.

Если контроллер домена настроен как WINS-сервер, нужно изменить параметры групповой политики контроллера домена для обеспечения работы служб WINS в имеющейся среде. В этом разделе содержатся инструкции по настройке групповой политики для повторного включения служб WINS.

Для повторного включения службы WINS на контроллерах домена нужно изменить объект групповой политики **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена). Выполните следующие действия для включения службы WINS на всех контролерах домена.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена».
- Анализ последствий для пользователей. Необходимо перезапустить контроллеры домена для выполнения этих действий. Следует выполнять все эти действия в нерабочее время, чтобы свести к минимуму неблагоприятные последствия для пользователей.

Настойка групповой политики для включения службы WINS.

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), **Active Directory Users and Computers** Active Directory — пользователи и компьютеры), а затем дважды щелкните домен для развертывания дерева домена.
2. Щелкните правой кнопкой мыши организационное подразделение **Domain Controllers** (Контроллеры домена) и выберите команду **Properties** (Свойства).
3. В диалоговом окне свойств откройте вкладку **Group Policy** (Групповая политика), выберите **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а затем нажмите кнопку **Edit** (Изменить).
4. Убедитесь, что изменения выполняются для параметра **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а не **Default Domain Controllers Policy**(Политика по умолчанию для контроллеров домена). Неправильные изменения параметра **Default Domain Controllers Policy** (Политика по умолчанию для контроллеров домена) могут неблагоприятно повлиять на используемую среду, и их последствия трудно будет устранить.
5. В разделе **Computer Configuration** (Конфигурация компьютера) откройте папку **Windows Settings**, щелкните **Security Settings** (Параметры безопасности), а затем выберите **System Services** (Системные службы).
6. В разделе сведений дважды щелкните **WINS**, выберите параметр **Automatic** (Автоматически), а затем нажмите кнопку **OK**.
7. Закройте окно **Group Policy Object Editor** (Редактор объектов групповой политики), нажмите кнопку **OK**, чтобы закрыть диалоговое окно, и выйдите из окна **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).
8. Перезапустите по одному контроллеры домена, которые обеспечивают работу служб WINS, убедившись, что они перезапускаются по очереди.

После изменения параметров групповой политики для включения службы WINS убедитесь, что служба работает.

Задание 9. Проверка работы WINS.

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), а затем — **Services** (Службы).
2. Убедитесь, что служба **Windows Internet Name Service (WINS)** работает и настройте ее автоматический запуск.

Задание 10. Включение файловых служб и служб печати.

Доступ к общим файлам на контроллерах домена не затрагивается базовой политикой контроллеров домена, развернутой после выполнения инструкций предыдущих разделов. Для безопасного доступа к файловым службам не требуются никакие изменения контроллеров домена.

Однако если один из контроллеров домена настроен как сервер печати, нужно настроить параметры групповой политики для включения службы диспетчера очереди печати, чтобы контроллеры домена могли обеспечить работу служб печати в имеющейся среде.

Для включения службы диспетчера очереди печати на контроллерах домена нужно изменить объект групповой политики **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена). Выполните следующие действия для включения службы диспетчера очереди печати на всех контролерах домена.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена».

- Анализ последствий для пользователей. Необходимо перезапустить контроллеры домена для выполнения этих действий. Следует выполнять все эти действия в нерабочее время, чтобы свести к минимуму неблагоприятные последствия для пользователей.

Настройка групповой политики для включения служб печати на контроллерах домена

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), **Active Directory Users and Computers**(Active Directory — пользователи и компьютеры), а затем дважды щелкните домен для развертывания дерева домена.
2. Щелкните правой кнопкой мыши организационное подразделение **Domain Controllers** (Контроллеры домена) и выберите команду **Properties** (Свойства).
3. В диалоговом окне свойств откройте вкладку **Group Policy** (Групповая политика), выберите **Domain Controllers Baseline Policy**(Базовая политика контроллеров домена), а затем нажмите кнопку **Edit** (Изменить).
4. Убедитесь, что изменения выполняются для параметра **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а не **Default Domain Controllers Policy** (Политика по умолчанию для контроллеров домена). Неправильные изменения параметра **Default Domain Controllers Policy** (Политика по умолчанию для контроллеров домена) могут неблагоприятно повлиять на используемую среду, и их последствия трудно будет устранить.
5. В разделе **Computer Configuration** (Конфигурация компьютера) дважды щелкните папку **Windows Settings**, щелкните правой кнопкой мыши **Security Settings** (Параметры безопасности), а затем выберите **System Services** (Системные службы).
6. В разделе сведений дважды щелкните **Print Spooler** (Диспетчер очереди печати), выберите параметр **Automatic** (Автоматически), а затем нажмите кнопку **OK**.
7. Закройте окно **Group Policy Object Editor** (Редактор объектов групповой политики), нажмите кнопку **OK**, чтобы закрыть диалоговое окно, и выйдите из окна **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).
8. Перезапустите по одному контроллеры домена, которые обеспечивают работу служб печати, убедившись, что они перезапускаются по очереди.

После изменения параметров групповой политики для включения службы диспетчера очереди печати убедитесь, что служба работает.

Задание 11. Проверка работы службы диспетчера очереди

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), а затем — **Services** (Службы).
2. Убедитесь, что служба диспетчера очереди печати работает, и настройте ее автоматический запуск.

Задание 12. Включение служб IAS.

Если один из контроллеров домена настроен как IAS-сервер, нужно изменить параметры групповой политики контроллера домена для обеспечения работы служб IAS в имеющейся среде. В этом разделе последовательно описываются инструкции по настройке групповой политики для повторного включения служб IAS.

Для повторного включения служб IAS на контроллерах домена нужно изменить параметр Domain Controllers Baseline Policy (Базовая политика контроллеров домена). Выполнение этих действий позволяет включить службы сертификатов на всех контроллерах домена, которые обеспечивают работу служб IAS.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена».
- Анализ последствий для пользователей. Необходимо перезапустить контроллеры домена для выполнения этих действий. Следует выполнять все эти действия в нерабочее время, чтобы свести к минимуму неблагоприятные последствия для пользователей.

Настройка групповой политики для включения служб IAS.

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), **Active Directory Users and Computers**(Active Directory — пользователи и компьютеры), а затем дважды щелкните домен для развертывания дерева домена.
2. Щелкните правой кнопкой мыши организационное подразделение **Domain Controllers** (Контроллеры домена) и выберите команду **Properties** (Свойства).
3. В диалоговом окне свойств откройте вкладку **Group Policy** (Групповая политика), выберите **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а затем нажмите кнопку **Edit** (Изменить).
4. Убедитесь, что изменения выполняются для параметра **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а не **Default Domain Controllers Policy**(Политика по умолчанию для контроллеров домена). Неправильные изменения параметра **Default Domain Controllers Policy** (Политика по умолчанию для контроллеров домена) могут неблагоприятно повлиять на используемую среду, и их последствия трудно будет устранить.
5. В разделе **Computer Configuration** (Конфигурация компьютера) дважды щелкните папку **Windows Settings**, щелкните правой кнопкой мыши **Security Settings** (Параметры безопасности), а затем выберите **System Services** (Системные службы).
6. В разделе сведений (правый раздел) дважды щелкните **IAS**, выберите параметр **Automatic** (Автоматически), а затем нажмите кнопку **OK**.
7. Закройте окно **Group Policy Object Editor** (Редактор объектов групповой политики), нажмите кнопку **OK**, чтобы закрыть диалоговое окно, и выйдите из окна **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).
8. Перезапустите по одному контроллеры домена, на которых используется IAS, убедившись, что они перезапускаются поочередно.

После изменения параметров групповой политики для включения служб IAS убедитесь, что службы работают.

Задание 13. Проверка работы службы IAS.

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), а затем — **Services** (Службы).
2. Убедитесь, что служба IAS работает и настройте ее автоматический запуск.

Задание 14. Включение служб сертификатов.

Если один из контроллеров домена настроен как центр сертификации, нужно изменить параметры групповой политики контроллера домена для обеспечения работы служб сертификатов в имеющейся среде.

Для повторного включения служб сертификатов на контроллерах домена нужно изменить параметр Domain Controllers Baseline Policy (Базовая политика контроллеров домена). Выполнение этих действий позволяет включить службы сертификатов на всех контроллерах домена, которые обеспечивают работу этих служб.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена».

- Анализ последствий для пользователей. Необходимо перезапустить контроллеры домена для выполнения этих действий. Следует выполнять все эти действия в нерабочее время, чтобы свести к минимуму неблагоприятные последствия для пользователей.

Настройка групповой политики для включения служб сертификатов.

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), **Active Directory Users and Computers**(Active Directory — пользователи и компьютеры), а затем дважды щелкните домен для развертывания дерева домена.
2. Щелкните правой кнопкой мыши организационное подразделение **Domain Controllers** (Контроллеры домена) и выберите команду **Properties** (Свойства).
3. В диалоговом окне свойств откройте вкладку **Group Policy** (Групповая политика), выберите **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а затем нажмите кнопку **Edit** (Изменить).
4. Убедитесь, что изменения выполняются для параметра **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а не **Default Domain Controllers Policy** (Политика по умолчанию для контроллеров домена). Неправильные изменения параметра **Default Domain Controllers Policy** (Политика по умолчанию для контроллеров домена) могут неблагоприятно повлиять на используемую среду, и их последствия трудно будет устранить.
5. В разделе **Computer Configuration** (Конфигурация компьютера) дважды щелкните папку **Windows Settings**, щелкните правой кнопкой мыши **Security Settings** (Параметры безопасности), а затем выберите **System Services** (Системные службы).
6. В разделе сведений дважды щелкните **CertSvc**, выберите параметр **Automatic** (Автоматически), а затем нажмите кнопку **OK**.
7. Закройте окно **Group Policy Object Editor** (Редактор объектов групповой политики), нажмите кнопку **OK**, чтобы закрыть диалоговое окно, и выйдите из окна **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).
8. Перезапустите по одному контроллеры доменов.

После изменения параметров групповой политики для включения служб сертификатов убедитесь, что служба работает.

Задание 15. Проверка работы служб сертификатов.

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), а затем — **Services** (Службы).
2. Убедитесь, что служба сертификатов работает, и настройте ее автоматический запуск.

Задание 16. Включение и защита служб «Планировщик задач».

Если один из контроллеров домена использует назначенные задачи для автоматического запуска сценариев или программ, нужно изменить параметры групповой политики контроллера домена для обеспечения работы службы «Планировщик задач».

Чтобы повысить безопасность контроллеров домена, после повторного включения службы планировщика задач ограничьте любые задачи, которые назначены с помощью AT-команд при использовании локальной системной учетной записи. При сохранении конфигурации учетной записи по умолчанию контроллеры домена открыты для атак злонамеренных пользователей.

Это задание содержит поэтапные инструкции для выполнения следующих действий:

- Настройка групповой политики для включения службы планировщика заданий.
- Защита службы планировщика заданий с помощью изменения учетной записи AT-службы.

Для включения службы планировщика заданий на контроллерах домена нужно изменить объект групповой политики **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена). Выполните следующие действия для включения службы планировщика заданий на всех контролерах домена.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена».
- Анализ последствий для пользователей. Необходимо перезапустить контроллеры домена для выполнения этих действий. Одновременная перезагрузка контроллеров домена может создать временные трудности для пользователей при доступе в сеть или к сетевым ресурсам. Следует выполнять все эти действия в нерабочее время, чтобы свести к минимуму неблагоприятные последствия для пользователей.

Настройка групповой политики для включения службы планировщика заданий

1. Нажмите кнопку **Start** (Пуск), выберите последовательно **Settings** (Настройка), **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры), а затем дважды щелкните домен для развертывания дерева домена.
2. Щелкните правой кнопкой мыши организационное подразделение **Domain Controllers** (Контроллеры домена) и выберите команду **Properties** (Свойства).
3. В диалоговом окне свойств откройте вкладку **Group Policy** (Групповая политика), выберите **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а затем нажмите кнопку **Edit** (Изменить).
4. Убедитесь, что изменения выполняются для параметра **Domain Controllers Baseline Policy** (Базовая политика контроллеров домена), а не **Default Domain Controllers Policy** (Политика по умолчанию для контроллеров домена). Неправильные изменения параметра **Default Domain Controllers Policy** (Политика по умолчанию для контроллеров домена) могут неблагоприятно повлиять на используемую среду, и их последствия трудно будет устранить.
5. В разделе **Computer Configuration** (Конфигурация компьютера) дважды щелкните папку **Windows Settings**, щелкните правой кнопкой мыши **Security Settings** (Параметры безопасности), а затем выберите **System Services** (Системные службы).
6. В разделе сведений дважды щелкните **Task Scheduler** (Планировщик заданий), выберите параметр **Automatic** (Автоматически), а затем нажмите кнопку **OK**.
7. Закройте окно **Group Policy Object Editor** (Редактор объектов групповой политики), нажмите кнопку **OK**, чтобы закрыть диалоговое окно, и выйдите из окна **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).
8. Перезапустите по одному контроллеры домена, на которых используется планировщик заданий, убедившись, что они перезапускаются поочередно.

После изменения параметров групповой политики для включения службы планировщика заданий убедитесь, что служба работает.

Задание 17. Проверка работы службы планировщика заданий.

1. Нажмите кнопку **Start** (Пуск), выберите последовательно **Settings** (Настройка), **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), а затем —**Services** (Службы).
2. Убедитесь, что служба планировщика заданий работает, и настройте ее автоматический запуск.

Задание 18. Защита службы планировщика заданий с помощью изменения учетной записи АТ-службы.

Для назначения задач в планировщике заданий можно также использовать AT-команды. По умолчанию задачи, назначенные с помощью AT-команд, выполняются с локальной системной учетной записью, вне зависимости от того, какой пользователь вошел в систему компьютера. Очень часто эти задачи выполняются в фоновом режиме и остаются незамеченными для администраторов.

Локальная системная учетная запись — это специальная предустановленная учетная запись, которая используется для запуска и выполнения многих служб на контроллерах домена. Эта учетная запись обеспечивает полный доступ ко всем контроллерам домена, а также к сетевым ресурсам. Следовательно, при многих видах атак на систему безопасности делается попытка воспользоваться службами, которые выполняются с помощью локальной системной учетной записи.

Для повышения безопасности контроллеров домена можно ограничить возможности злонамеренных пользователей по запуску программ, использующих локальную системную учетную запись. Рекомендуется изменить конфигурацию планировщика заданий таким образом, чтобы любые задачи, назначенные с помощью AT-команд, не выполнялись с использованием локальной системной учетной записи.

После выполнения следующих действий любые задачи, назначенные с помощь AT-команд, смогут выполняться только при использовании явно указанной учетной записи.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена».
- Повторите следующие действия. Необходимо выполнить эти действия на каждом из контроллеров домена.

Изменение конфигурации учетной записи службы AT.

1. Нажмите кнопку **Start** (Пуск), выберите последовательно **Settings** (Настройка), **Control Panel** (Панель управления) и дважды щелкните значок **Scheduled Tasks** (Назначенные задания).
2. В меню **Advanced** (Дополнительно) выберите **AT Service Account** (Учетная запись службы «AT»).
3. Выберите вариант **This Account** (Учетная запись), введите имя и пароль для учетной записи, которые не дают прав администратора контроллеру домена, а затем нажмите кнопку **OK**.

Убедитесь, что используемая учетная запись не принадлежит ни одной из административных групп (например, «Администраторы предприятия», «Администраторы домена» или «Администраторы»). Для этой цели рекомендуется создать специальную учетную запись службы и периодически проверять членство в группе учетной записи.

Если требуется выполнить задачу, в которой используются учетные права администратора, необходимо назначить ее с помощью мастера добавления заданий в «Планировщике задач».

Задание 19. Защита службы DNS-сервера.

Для правильной работы Active Directory необходимо наличие DNS-сервера. В интернете и других сетях TCP/IP именование DNS используется для поиска компьютеров и служб с помощью удобных для пользователя имен. Когда пользователь вводит имя DNS в приложении, DNS-службы разрешают имя в IP-адрес.

Для поддержки Active Directory можно использовать DNS-службу, которая предоставлена поставщиком услуг, или разместить собственную систему DNS в Windows Server 2008. При размещении собственной службы DNS-сервера можно повысить его безопасность с помощью параметров:

- Ограничение IP-адресов, на которых слушает служба DNS-сервера.
- Отключение рекурсии для DNS-серверов, которые не обеспечивают услуги разрешения для сетевых клиентов.

- Настройка корневых ссылок для обеспечения защиты частного пространства имен DNS.

Многосетевой компьютер — это компьютер, имеющий несколько сетевых адаптеров или настроенный с несколькими IP-адресами для одного сетевого адаптера. По умолчанию служба DNS-сервера выполняется на многосетевом компьютере, настроенном для слушания запросов DNS с использованием всех его IP-адресов.

С помощью ограничения IP-адресов, на которых слушает служба DNS-сервера, можно сократить угрозу атаки на DNS-сервер. Следует настраивать DNS-серверы только для слушания запросов DNS на IP-адресах, указанных как предпочтительные DNS-серверы в конфигурации компьютеров текущей среды. Используйте следующую процедуру для ограничения IP-адресов, на которых выполняет прослушивание служба DNS-сервера.

Требования

- Учетные данные. Необходимо войти в систему на DNS-сервере с правами члена группы администраторов DNS, администраторов домена или предприятия.
- Конфигурация. DNS-сервер должен иметь несколько IP-адресов.
- Средства. Оснастка DNS консоли управления MMC.

Ограничение IP-адресов, на которых выполняет прослушивание служба DNS-сервера

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), а затем— **DNS**.
2. В дереве консоли (левая область) щелкните DNS-сервер, который требуется настроить.
3. В меню **Action** (Действие) выберите пункт **Properties** (Свойства).
4. На вкладке **Interfaces** (Интерфейсы) выберите вариант **Only the following IP addresses** (Только следующие IP-адреса).
5. В поле **IP address** (IP-адрес) введите IP-адрес, который должен быть разрешен для использования данным DNS-сервером, и нажмите кнопку **Add** (Добавить).
6. При необходимости повторите предыдущее действие, чтобы указать другие IP-адреса сервера, которые должны быть разрешены для использования этим DNS-сервером.
7. Для каждого из IP-адресов в списке, которые не используются в качестве предпочтительного DNS-сервера DNS-клиентами, щелкните IP-адрес, а затем нажмите кнопку **Remove** (Удалить).
8. Нажмите кнопку **OK**.

Задание 20. Отключение рекурсии для отдельных DNS – серверов.

Клиент отправляет запрос на DNS-сервер, когда требуется узнать IP-адрес конкретного компьютера. Рекурсивный запрос — это запрос, который сделан на DNS-сервер с требованием принять ответственность за предоставление полного ответа на запрос, а не просто обратиться на другой DNS-сервер. Затем DNS-сервер выполняет отдельные итеративные запросы на другие DNS-серверы от лица автора запроса, чтобы получить полный ответ на запрос. Рекурсия включена по умолчанию для службы DNS-сервера.

Несмотря на то, что рекурсия позволяет DNS-серверу выполнять циклические запросы для DNS-клиентов и серверов, от которых они получены, она может быть также использована злоумышленниками для перегрузки имеющихся ресурсов DNS-сервера, что приводит к отказу в обслуживании законных пользователей. Если имеющийся DNS-сервер обеспечивает разрешение служб для сетевых клиентов, а не для других DNS-серверов, рекурсию следует включить. Однако если DNS-сервер не обеспечивает услуги разрешения для сетевых клиентов, используйте описанную ниже процедуру для отключения рекурсии.

Если нет уверенности в том, оказывает DNS-сервер услуги разрешения сетевым клиентам или нет, лучше не менять используемый по умолчанию параметр.

Требования

- Учетные данные. Необходимо войти в систему на DNS-сервере с правами члена группы администраторов DNS, администраторов домена или предприятия.
- Средства. Оснастка DNS консоли MMC.

Отключение рекурсии

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), а затем — **DNS**.
2. В дереве консоли (левая область) щелкните DNS-сервер, который требуется настроить.
3. В меню **Action** (Действие) выберите пункт **Properties** (Свойства).
4. Откройте вкладку **Advanced** (Дополнительно).
5. В разделе **Server options** (Параметры сервера) выберите пункт **Disable recursion (also disables forwarders)** (Отключить рекурсию (также отключить отправителей)), а затем нажмите кнопку **OK**.

Задание 21. Настройка корневых ссылок для предотвращения незащищенности данных.

Внутренний корень DNS используется для обеспечения частного пространства имен DNS для данной организации, которое не находится под действием общедоступного интернета. Корневые ссылки помогают DNS-серверу находить сведения о домене DNS верхнего уровня (например, .net, .org или .com).

Если в используемой инфраструктуре DNS имеется внутренний корень DNS, нужно настроить корневые ссылки на внешние DNS-серверы, чтобы указать на те из них, на которых размещен корневой домен, а не на те, на которых размещен корневой домен интернета. Это позволяет предотвратить отправку DNS-серверами личных данных через интернет при разрешении имен.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена» или «Администраторы предприятия».
- Средства. Оснастка DNS консоли MMC.

Эту процедуру следует выполнять только на DNS-серверах, которые разрешают имена для внутреннего корня DNS.

Настройка корневых ссылок для предотвращения незащищенности данных

1. Нажмите кнопку **Start** (Пуск), выберите последовательно **Control Panel** (Панель управления), **Administrative Tools** (Администрирование), а затем — **DNS**.
2. В дереве консоли (левая область) щелкните DNS-сервер, который требуется настроить.
3. В меню **Action** (Действие) выберите пункт **Properties** (Свойства).
4. Откройте вкладку **Root Hints** (Корневые ссылки).
5. Выделите имя каждого сервера, который перечислен в группе **Name servers** (Серверы имен), а затем нажмите кнопку **Remove** (Удалить).
6. Для каждого DNS-сервера, на котором размещен внутренний корень DNS, нажмите кнопку **Add** (Добавить), а затем укажите имя и IP-адрес DNS-сервера.

Задание 22. Проверка новых параметров.

Чтобы убедиться в применении нужных параметров для DNS-сервера, используйте следующую процедуру.

Требования

- Учетные данные. Необходимо войти в систему на DNS-сервере с правами члена группы администраторов DNS, администраторов домена или предприятия.
- Средства. Оснастка DNS консоли MMC.

Проверка настройки корневых ссылок

1. Нажмите кнопку **Start** (Пуск), выберите последовательно **Control Panel** (Панель управления), **Administrative Tools** (Администрирование), а затем — **DNS**.
2. В дереве консоли (левая область) щелкните DNS-сервер, который требуется проверить.
3. В меню **Action** (Действие) выберите пункт **Properties** (Свойства).
4. Откройте вкладку **Root Hints** (Корневые ссылки).
5. Убедитесь, что DNS-серверы, на которых размещен внутренний корень DNS, перечислены в списке раздела **Name servers** (Серверы имен).

Задание 23. Обеспечение безопасности контроллеров домена

Поскольку контроллеры домена содержат важные данные, которые должны быть защищены, необходимо изучить имеющиеся функции безопасности контроллеров домена и применить те из них, которые подходят для используемой среды. Затем убедитесь в обеспечении защиты с помощью установки последних обновлений безопасности «Майкрософт».

В этом задании рассматривается процедура настройки, которая поможет лучше защитить контроллеры домена:

- Установка последних обновлений безопасности «Майкрософт».
- Создание резервного файла, обеспечивающего восстановление после атак на дисковое пространство.
- Отключение автоматического создания 8.3 имен файлов, чтобы уменьшить уязвимость для вирусов и атак злоумышленников.
- Использование служебной программы System Key для защиты контроллеров домена от ПО, взламывающего пароли.
- Отключение анонимного доступа к Active Directory в тех средах, где приложения не требуют анонимных подключений.

Установка последних обновлений безопасности “Microsoft”.

Для обеспечения работы контроллеров домена необходимо регулярно загружать и устанавливать последние обновления безопасности «Майкрософт». Эти обновления помогают разрешать известные проблемы и устранять известные уязвимые места компьютера.

Выполнение перечисленных ниже действий позволит автоматически и вручную обновлять контроллеры домена с помощью установки имеющихся обновлений безопасности. Необходимо выполнить следующие задачи:

- Настройка автоматических обновлений для автоматической загрузки и установки обновлений безопасности по заданному расписанию.
- Изучение способов использования Windows Update для загрузки и установки обновлений безопасности вручную.

Необходимо устанавливать последние обновления безопасности на все компьютеры в сети. Настройка автоматических обновлений и программы Windows Update для обновления котроллеров домена распространяется только на контроллеры домена, но не затрагивает остальные серверы и клиенты сети. Убедитесь, что автоматические обновления и программа Windows Update настроены для использования на всех компьютерах текущей сети, работающих под управлением Windows Server 2008, Windows 2000 и Windows XP.

Настройка автоматических обновлений

Можно настроить контроллеры домена Windows Server 2008 для автоматического обновления и установки последних исправлений безопасности «Майкрософт», когда компьютер подключен к интернету.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена».

- Повторите следующие действия. Необходимо выполнить эти действия на каждом из контроллеров домена.

Настройка контроллера домена для автоматической загрузки и установки обновлений безопасности

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Control Panel** (Панель управления), дважды щелкните **Administrative Tools** (Администрирование), а затем — **System** (Система).
2. Откройте вкладку **Automatic Updates** (Автоматическое обновление), а затем установите флажок **Keep my computer up-to-date. With this setting enabled, Windows Update software may be automatically updated prior to applying any other updates** (Помогите защитить мой компьютер. Автоматическое обновление сначала обновит программное обеспечение Windows Update, а затем применит остальные обновления).
3. Выберите вариант **Automatically download the updates, and install them on the schedule that I specify** (Автоматически загружать и устанавливать на компьютер рекомендуемые обновления).
4. Выберите день и время для выполнения обновления, а затем нажмите кнопку **OK**, чтобы закрыть окно **System Properties** (Свойства системы).

Обновления безопасности часто требуют перезапуска контроллеров домена. Выберите день и время, когда отрицательные последствия для пользователей будут минимальными.

Задание 24. Использование Windows Update.

Программа Windows Update представляет собой сетевое расширение системы Windows, которое следит за обновлением компьютеров, подключенных к интернету. Можно запустить программу Windows Update, чтобы проверить, были ли установлены все последние обновления безопасности с помощью автоматического обновления. Программа Windows Update может быть полезна, если корпорация «Майкрософт» присылает уведомления о новой проблеме безопасности и требуется немедленно проверить, были или нет обновлены имеющиеся компьютеры.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Операторы сервера» или «Администраторы домена».
- Повторите следующие действия. Необходимо выполнить эти действия на каждом из контроллеров домена.

Внимание! Обновления безопасности часто требуют перезапуска контроллеров домена. При запуске Windows Update следует помнить о последствиях перезапуска контроллеров домена для пользователей.

Запуск Windows Update для загрузки и установки обновлений безопасности вручную

1. Нажмите кнопку **Start** (Пуск), выберите пункт **All Programs** (Все программы), а затем щелкните значок **Windows Update**.
2. В окне Internet Explorer, выберите команду **Scan for updates** (Поиск обновлений), а затем подождите, пока проверка не будет выполнена на 100 процентов.
3. Программа Windows Update автоматически выбирает все необходимые важные обновления, которые отсутствуют на контроллерах домена. Если доступны какие-либо обновления, выберите последовательно **Review and Install Updates** (Просмотр и установка обновлений), **Install Now** (Установить) и следуйте инструкциям на экране.
4. Повторяйте эти действия, пока не останется никаких важных обновлений для котроллера домена.

Задание 25. Создание резервного файла, обеспечивающего восстановление после атак, затрагивающих дисковое пространство.

Многие атаки на систему безопасности включают попытку использования системных ресурсов атакуемой системы. Один из наиболее часто затрагиваемых системных ресурсов — свободное дисковое пространство. Во время атак на дисковое пространство злоумышленники используют все пространство диска за счет добавления в каталог огромного количества объектов.

Можно ускорить восстановление после атаки, затрагивающей дисковое пространство, заранее создав резервный файл на диске, который содержит базу данных Active Directory (Ntds.dit). Резервный файл — это просто большой файл, который занимает (сохраняет) свободное дисковое пространство. Если злоумышленник переполняет свободное дисковое пространство, добавляя в каталог большое количество неразрешенных объектов, можно удалить резервный файл для освобождения свободного пространства и начала восстановления нормальной работы.

Если атака, затрагивающая дисковое пространство, происходит на контроллере домена, помимо удаления резервного файла нужно также удалить неразрешенные объекты, которые заполняют дисковое пространство. Для получения дополнительных сведений об удалении неразрешенных объектов после атаки, затрагивающей дисковое пространство.

Описанная далее процедура позволяет сохранить дисковое пространство с помощью создания файла на том же диске, где расположена база данных Active Directory. Резервный файл должен быть больше 250 МБ или 1% от объема логического диска, на котором хранится база данных Active Directory. По умолчанию резервный файл размещается в папке systemroot\Ntds. Эту процедуру следует выполнить на каждом котроллере домена в сети.

Требования

- Учетные данные. Необходимо войти в систему контроллера домена с правами члена группы «Администраторы домена» или «Администраторы предприятия».
- Повторите следующие действия. Эту процедуру следует выполнить на каждом котроллере домена в сети.
- Средства. Fsutil.exe.

Создание резервного файла, обеспечивающего восстановление после атак, затрагивающих дисковое пространство

1. Нажмите кнопку **Start**Start (Пуск), выберите пункт **Run** (Выполнить), введите команду **cmd** и нажмите кнопку **OK**.
2. В командной строке введите следующую команду и нажмите клавишу «Ввод»: **fsutil file createnew %systemroot%\ntds\reservefile 256000000**

Эта команда приводит к созданию резервного файла под названием Reservefile (размером 250 МБ) в каталоге, где хранится база данных Active Directory на контроллере домена. Если служба Active Directory перестает работать из-за нехватки свободного места на диске, можно удалить этот файл, чтобы создать свободное дисковое пространство.

Задание 26. Проверка создания резервного файла на контроллере домена**.**

Требования

- Учетные данные. Необходимо войти в систему контроллера домена с правами члена группы «Администраторы домена» или «Администраторы предприятия».
- Средства. «Мой компьютер».
- Повторите следующие действия. Если имеется несколько контроллеров домена, следует проверить создание резервного файла на каждом из них.

1. Нажмите кнопку **Start** (Пуск) и выберите команду **My Computer** (Мой компьютер).
2. В окне **My Computer** (Мой компьютер) перейдите в папку Ntds (обычно по адресу C:\Windows\Ntds).
3. Дважды щелкните папку Ntds, найдите файл Reservefile и убедитесь, что его размер не менее 250 МБ.

Задание 27. Отключение автоматического создания 8.3 имен файлов.

Многие вирусы и служебные программы, используемые злоумышленниками, являются 16-разрядными приложениями, которые ожидают, что имена файлов имеют формат, используемый при автоматическом создании 8.3 имен файлов. Защищенные контроллеры домена выполняют 16-разрядные приложения локально. Следовательно, нужно отключить автоматическое создание 8.3 имен, чтобы предотвратить угрозу безопасности контроллеров домена со стороны таких вирусов и служебных программ.

Для отключения автоматического создания 8.3 имен можно установить для записи реестра **NtfsDisable8dot3NameCreation** значение **1**. Следует отключить автоматическое создание имен файлов формата 8.3 на всех контроллерах домена.

Ошибка при изменении реестра может серьезно повредить систему. Прежде чем вносить изменения в реестр, следует выполнить архивацию важных данных, имеющихся на компьютере.

Требования

- Учетные данные. Необходимо войти в систему с правами члена группы «Администраторы домена»;
- Повторите следующие действия. Необходимо выполнить эти действия на каждом из контроллеров домена;
- Средства. Regedit.exe (редактор реестра).

Отключение автоматического создания 8.3 имен файлов на контроллерах домена

1. Нажмите кнопку **Start** (Пуск), выберите пункт **Run** (Выполнить), введите команду **regedit.exe** и нажмите кнопку **OK**.
2. В окне редактора реестра перейдите к параметру **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem**
3. Выберите запись реестра **NtfsDisable8dot3NameCreation**.
4. В меню **Edit** (Правка) выберите команду **Modify** (Изменить).
5. В поле **Value data** (Значение) введите отключение автоматического создания 8.3 имен файлов на данном контроллере домена.
6. Закройте редактор реестра.

Для получения дополнительных сведений об отключении автоматического создания 8.3 имен файлов см. Защита контроллеров домена от перезапуска с помощью Syskey.

На контроллерах домена данные пароля хранятся в Active Directory. Программы, взламывающие пароли, часто выбирают своей целью базу данных Security Accounts Manager (SAM) или Active Directory для доступа к паролям пользовательских учетных записей. Служебная программа System Key (Syskey) позволяет защитить контроллеры домена от ПО, взламывающего пароли. В Syskey используется технология сильного шифрования, которая помогает защитить данные о пароле учетной записи, сохраненные в базе данных SAM или в Active Directory.

Параметры Syskey

Параметр System Key	Уровень безопасности	Описание
Режим 1. Пароль, генерируемый системой: Store Startup Key Locally (Сохранение ключа запуска локально)	Безопасно	В качестве системного ключа используется создаваемый компьютером случайный ключ. Сохраняется также зашифрованная версия ключа для локального компьютера. Этот параметр обеспечивает сильное шифрование пароля в реестре, что дает возможность пользователям перезапускать компьютер без необходимости ввода пароля

		администратором или вставки диска.
Режим 2. Пароль, создаваемый администратором: Password Startup (Запуск по паролю)	Повышенная безопасность	В качестве системного ключа используется создаваемый компьютером случайный ключ. Сохраняется также зашифрованная версия ключа для локального компьютера. Кроме того, ключ защищен выбранным администратором паролем. При начальном запуске компьютера у пользователя запрашивается пароль системного ключа. Пароль системного ключа не хранится на компьютере.
Режим 3. Пароль, генерируемый системой: Store Startup Key on Floppy Disk (Сохранение ключа запуска на дискете)	Повышенная безопасность	Используется создаваемый компьютером случайный ключ, который сохраняется на дискете. Для запуска системы требуется дискета, на которой хранится системный ключ — ее нужно вставить по запросу во время начальной загрузки. Системный ключ не хранится на компьютере.

Программа Syskey включена на всех серверах Windows Server 2008 в режиме 1 (скрытый ключ). Использование Syskey в режиме 2 (пароль для консольного входа) и режиме 3 (пароль Syskey, хранящийся на дискете) рекомендуется только для контроллера домена, который подвержен физическим угрозам безопасности.

Отключение анонимного доступа к Active Directory.

По умолчанию Active Directory не предоставляет явных разрешений на доступ к объектам каталога для учетных данных «Анонимный вход», которые соответствуют анонимным подключениям. Однако при включении на контроллерах домена под управлением Windows Server 2008 совместимости с системами, предшествующими Windows 2000, в группу совместимого доступа с системами, предшествующими Windows 2000, добавляется член со специальными учетными данными «Анонимный вход». Поскольку данная группа имеет разрешения только для чтения в корне домена, а также в приложениях и службах пользователей, компьютеров и групповых объектов, использующих анонимный доступ, ее члены могут только считывать эти объекты.

В средах, где приложения не требуют установки анонимных подключений для доступа к данным Active Directory, рекомендуется отключить анонимный доступ.

Анонимный доступ можно отключить, если имеется один лес Active Directory с рядовыми серверами и контроллерами домена под управлением только Windows Server 2008 и Microsoft Windows 2000 Server и рабочими станциями под управлением Microsoft Windows 2000 Professional или Windows XP Professional.

Можно отключить анонимный доступ, выполнив следующие действия:

- При создании нового домена примите параметр установки по умолчанию **Permissions compatible only with Windows 2000 or Windows Server 2008 servers** (Разрешения, совместимые только с Windows 2000 или Windows Server 2008).
- В текущем домене Windows Server 2008, где включен доступ, совместимый с системами, предшествующими Windows 2000, удалите параметры Everyone (Все) и Anonymous Logon (Анонимный вход) из группы Windows 2000 Compatible Access и сохраните в качестве членов только пользователей, прошедших проверку подлинности.

1. Требования к результатам работы

Задание самостоятельной работы также выполняется в два этапа:

1. выполнение практических заданий;
2. написание отчета о проделанной работе.

Каждый этап оценивается определенным количеством баллов и выполняется в рамках отведенного времени на выполнение каждого задания. На выполнение работ первого этапа отводится неделя с момента получения самостоятельного задания. На выполнение работ второго этапа – две недели с момента завершения работ первого этапа. Несвоевременное выполнение отдельных этапов и работ в целом приводит к уменьшению количества баллов.

Работа над заданиями проводится вне учебного заведения и завершается представлением файла с отчетом о выполнении задания, а также файла - презентации.

2. Форма контроля и критерии оценки

Оцениваются:

- ✓ Подробность и понятность отчета о проделанной работе;
- ✓ Качество презентаций.

За несвоевременное выполнение этапа и работы в целом баллы снижаются на 1 балл в неделю.

-если на поставленные в заданиях вопросы даны подробные, четко сформулированные ответы, отчет оформлен аккуратно, а презентации имеют продуманную структуру и отражают всю необходимую информацию, ставится оценка «5»;

- если на поставленные в заданиях вопросы даны подробные, четко сформулированные ответы, отчет оформлен неаккуратно, структура презентаций продумана, но в ней не отражена вся необходимая информация, ставится оценка «4»;

- если ответы на поставленные в заданиях вопросы плохо структурированы, отчет оформлен неаккуратно, презентация не полностью отражает проделанную работу, ставится оценка «3»;

- если ответы на поставленные в заданиях вопросы плохо структурированы и содержат явные ошибки, отчет оформлен неаккуратно, презентация не полностью отражает проделанную работу или не представлена, ставится оценка «2».

3. Список рекомендуемой литературы:

Основная литература:

1. Кузин А.В. Компьютерные сети: учебное пособие / А.В. Кузин. – 3-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА – М, 2014. – 192 с.: ил. – (Профессиональное образование).
2. Эксплуатация объектов сетевой инфраструктуры: учебник для студентов учреждений сред. проф. Образования / [А.В. Назаров, В.П. Мельников, А.И. Куприянов, А.Н. Енгалычев]; под редакцией А.В. Назарова. – М.: Издательский центр «Академия», 2014. – 368 с.

Дополнительная литература:

3. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
4. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

5. Майкл Палмер, Роберт Брюс Синклер Проектирование и внедрение компьютерных сетей. Санкт – Петербург «БХВ - Петербург», 2005, 740с.
6. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008/2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.

5. Информационное обеспечение обучения

Основная литература:

1. Кузин А.В. Компьютерные сети: учебное пособие / А.В. Кузин. – 3-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА – М, 2014. – 192 с.: ил. – (Профессиональное образование).
2. Эксплуатация объектов сетевой инфраструктуры: учебник для студентов учреждений сред. проф. Образования / [А.В. Назаров, В.П. Мельников, А.И. Куприянов, А.Н. Енгалычев]; под редакцией А.В. Назарова. – М.: Издательский центр «Академия», 2014. – 368 с.

Дополнительная литература:

3. Клейменов С.А. Администрирование в информационных системах: учеб.пособие для вузов.- М.:Академия, 2008.- 272 с.
4. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
5. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)
6. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс
7. Майкл Палмер, Роберт Брюс Синклер Проектирование и внедрение компьютерных сетей. Санкт – Петербург «БХВ - Петербург», 2005.
8. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
9. Колисниченко Д.Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. Изд. 2-ое, переработанное и дополненное – СПб.: Наука и Техника,2006.-448с.: ил.
10. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.
11. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, программы. - СПб:Питер, 2008.-672 с.
12. В.Г. Олифер Сетевые операционные системы.-СПб., 2002.
13. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

Интернет – ресурсы:

1. http://www.mkgt.ru/files/material-static/552/tema2/index.htm
2. www.microsoft.com/rus/education/higher-education/faculty/resource-center.aspx

Приложение

Указания для написания реферата по дисциплине

Содержание разделов реферата

Реферат должен включать план, введение, основную часть и заключение. Пример оформления плана (оглавления, содержания) работы:

Содержание
Введение
1.
1.1
1.2
2.
2.1
2.2
Заключение
Список литературы
Приложения

1. Во **введении** необходимо отразить актуальность, степень разработанности проблемы, ее место в системе операционных систем, цель и задачи работы.
2. В **основной** части выделяются несколько (не менее двух) разделов, формулировка названий которых должна соответствовать пунктам плана. Проблематика, рассматриваемая в разделах реферата, должна быть теоретически и логически взаимосвязанной, а ее рассмотрение должно способствовать содержательному освещению темы.
3. В **заключении** необходимо подвести итоги анализа и сделать основные выводы.
4. Реферат завершается **списком использованной литературы**, включая оригинальные тексты, монографические исследования, статьи, учебные пособия и др.
5. **Приложения** являются необязательными и могут включать: сведения справочного характера; документальные источники информации необходимой для решения задачи. Допускается содержание разделов иллюстрировать поясняющими примерами, таблицами, схемами, графиками.

Требования к оформлению реферата

Реферат должен соответствовать следующим теоретико-методическим требованиям:

1. Объем реферата должен составлять **15-25** страниц печатного текста (формат **А4**; поля: левое **3 см**, правое – **1 см**, верхнее и нижнее **2 см**; шрифт – **Times New Roman, 14 пт.**; междустрочный интервал **одинарный**; **выравнивание по ширине**; **отступ первой строки 1,25 см**). Работа выполняется на русском языке.

2. Титульный лист оформляется в соответствии с **образцом**, представленным ниже**.**

3. Текст должен быть тщательно выверен, соответствовать нормам научного литературного языка.

Защита реферата

В установленные сроки реферат представляется преподавателю.

Собеседование по теме реферата (его защита студентом) включается в структуру экзамена в качестве одного из экзаменационных вопросов.

Для защиты реферата материалы предоставляются в распечатанном виде и в виде демонстрационных материалов (презентации в программе PowerPoint) на накопителе электронных данных – дискете, флешке. Титульный лист набирается тем же шрифтом в соответствии с образцом.

Образец оформления реферата

Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
Высшего профессионального образования

«Новгородский государственный университет имени Ярослава Мудрого»

Многопрофильный колледж

Политехнический колледж

РЕФЕРАТ

по дисциплине «Администрирование компьютерных сетей»

для специальности **09.02.03 Программирование в компьютерных системах**

ПРИЧИНЫ, ОБУСЛОВИВШИЕ ПОЯВЛЕНИЕ ЛОКАЛЬНЫХ И ГЛОБАЛЬНЫХ СЕТЕЙ

Выполнил:
Студент
Ф.И.О.
Группа _____

Руководитель:
_____ /*Ф.И.О.*

Оценка:_____

Великий Новгород
год

6. Лист регистрации изменений.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изме-нения	Номер листа				Всего листов в документе	ФИО и подпись ответственного за внесение изменения	Дата внесения изменения	Дата введения изменения
	измененного	замененного	нового	изъятого				