image001

**НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«МОСКОВСКИЙ ФИНАНСОВО-ПРОМЫШЛЕННЫЙ УНИВЕРСИТЕТ «СИНЕРГИЯ»**

**Институт информационных технологий**

(наименование факультета/института)

**Направление/специальность подготовки:** 09.03.02 Информационные системы и технологии

(код и наименование направления /специальности подготовки)

**Профиль/специализация:** Разработка, сопровождение и обеспечение безопасности информационных систем

(наименование профиля/специализации)

**Форма обучения*:*** очная

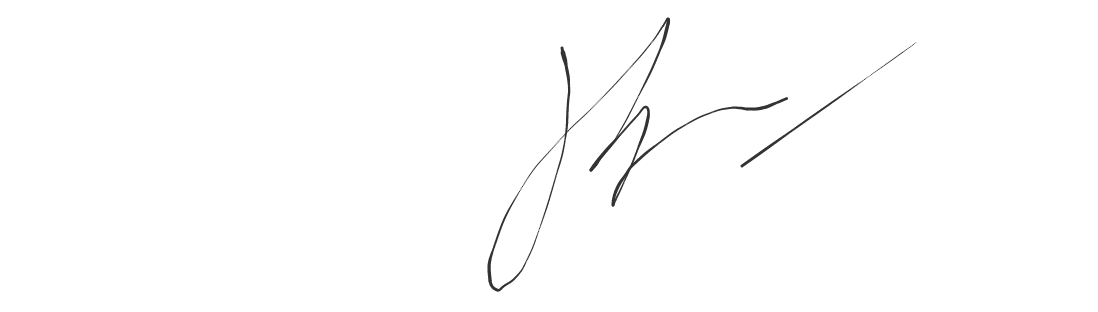
(очная, очно-заочная, заочная)

***Лабораторный практикум №3.***

**На тему *Базовые средства администрирования Microsoft Windows Server 2012. Администрирование сетей передачи данных. Сетевые службы и протоколы.***

(наименование темы)

**По дисциплине Администрирование информационных систем**



|  |  |  |  |
| --- | --- | --- | --- |
| **Обучающийся** | Рунов Алексей Алексеевич |  |  |
|  | (ФИО) |  | (подпись) |

**Москва 2024г**

### ***Задача:***

***Лабораторный практикум №3. Базовые средства администрирования Microsoft Windows Server 2012. Администрирование сетей передачи данных. Сетевые службы и протоколы.***

1. Провести настройку средств администрирования служб маршрутизации в Microsoft RRAS Microsoft Windows Server 2012 R2.

2. Провести настройку средств удаленного доступа в Microsoft RRAS Microsoft Windows Server 2012 R2.

3. Настроить параметры политики безопасности Windows 2012 Server.

### ***Пошаговое решение:***

### 1. Настройка средств администрирования служб маршрутизации в Microsoft RRAS

Что делаем: Настроим службу маршрутизации и удалённого доступа (RRAS) для маршрутизации трафика в сети.

#### Шаги:

1. Устанавливаем роль RRAS:
   * Открываем Диспетчер серверов.
   * Переходим в раздел Управление и выбираем Добавить роли и компоненты.
   * В мастере добавления ролей выбираем Маршрутизация и удалённый доступ (RRAS).
   * Устанавливаем необходимые компоненты, такие как Маршрутизация (Routing) и Мостовая служба (Routing and Remote Access Service).
2. Настраиваем RRAS для маршрутизации:
   * После установки открываем Диспетчер маршрутизации и удалённого доступа.
   * Выбираем сервер, нажимаем правой кнопкой и выбираем Настроить и включить маршрутизацию.
   * В мастере настроек маршрутизации выбираем Маршрутизация (Routing) и активируем необходимые параметры маршрутизации, например, статическую маршрутизацию или динамическую маршрутизацию с использованием протокола RIP.
3. Добавляем статические маршруты:
   * В Диспетчере маршрутизации и удалённого доступа переходим к разделу Маршруты IP (IP Routes).
   * Добавляем необходимые статические маршруты для подключения различных подсетей и сетевых интерфейсов.
4. Проверяем маршрутизацию:
   * Используем команду ping или tracert с других машин в сети, чтобы проверить корректность маршрутизации.

### 2. Настройка средств удалённого доступа в Microsoft RRAS

Что делаем: Настроим удалённый доступ для пользователей с использованием Microsoft RRAS.

#### Шаги:

1. Настраиваем RRAS для удалённого доступа:
   * В Диспетчере маршрутизации и удалённого доступа выбираем сервер и нажимаем правой кнопкой, затем выбираем Настроить и включить маршрутизацию и удалённый доступ.
   * В мастере выбираем Удалённый доступ (Dial-up or VPN) и продолжаем настройку.
2. Настроиваем VPN-сервер:
   * В мастере настройки выбираем Виртуальная частная сеть (VPN).
   * Настроиваем VPN-сервер для использования протоколов, например, PPTP, L2TP или SSTP (Secure Socket Tunneling Protocol).
   * Указываем параметры IP-адресации для клиентов VPN и выбираем способ аутентификации, например, MS-CHAP v2 или EAP.
3. Настраиваем пользователей для доступа:
   * В Пользователи и компьютеры Active Directory добавляем пользователей в группу, которая будет иметь доступ к VPN, например, VPN-Users.
   * Убедимся, что для этих пользователей включён доступ к VPN-серверу.
4. Проверяем подключение клиентов:
   * На клиентских компьютерах настраиваем соединение через VPN.
   * Используем клиент VPN для подключения и проверяем, что соединение с VPN-сервером работает корректно.

### 3. Настройка параметров политики безопасности Windows Server 2012

Что делаем: Настроим параметры политики безопасности для защиты серверов и сетевых ресурсов на Windows Server 2012.

#### Шаги:

1. Настраиваем политику безопасности через групповую политику (Group Policy):
   * Открываем gpedit.msc или Group Policy Management Console (для контроллера домена).
   * Переходим в Конфигурация компьютера -> Политики -> Административные шаблоны -> Система -> Безопасность.
2. Настроим основные параметры политики безопасности:
   * Параметры блокировки учетных записей: Настроим политику блокировки учетных записей для защиты от несанкционированных входов. Например:
     + Блокируем учетную запись после 3 неудачных попыток входа.
     + Устанавливаем срок действия блокировки — 30 минут.
   * Парольная политика: Устанавливаем политику сложных паролей, например:
     + Минимальная длина пароля — 8 символов.
     + Требуем использование букв верхнего и нижнего регистра, цифр и специальных символов.
   * Аудит безопасности: Включаем аудит безопасности для отслеживания всех успешных и неуспешных попыток входа в систему, изменений в системе и доступа к критическим данным.
3. Настроим брандмауэр Windows:
   * Открываем Брандмауэр Windows с расширенными параметрами безопасности.
   * Настроим правила входящего и исходящего трафика, включая блокировку нежелательных портов и протоколов.
   * Убедимся, что разрешены только необходимые порты для работы серверных служб, таких как RDP (порт 3389), HTTP (порт 80), HTTPS (порт 443) и т.д.
4. Настроим доступ к сетевым ресурсам:
   * Убедимся, что для доступа к файлам и принтерам настроены соответствующие разрешения. Для этого используем вкладки Безопасность в свойствах файлов или папок.
5. Проверяем безопасность:
   * Для проверки безопасности используем утилиту Microsoft Baseline Security Analyzer (MBSA) или PowerShell команды, чтобы выявить потенциальные уязвимости и настройки, требующие улучшения.
   * Также используем команду secpol.msc для запуска редактора локальной безопасности и проверяем параметры безопасности системы.

### Резюме:

1. Маршрутизация (RRAS) — настраиваем службу маршрутизации для передачи данных между подсетями и настраиваем маршруты для сети.
2. Удалённый доступ (RRAS) — настраиваем сервер для предоставления удалённого доступа пользователям с помощью VPN-соединений.
3. Политики безопасности — настраиваем параметры безопасности с помощью групповых политик, брандмауэра, контроля паролей и блокировки учетных записей.