**НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

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

|  |  |  |
| --- | --- | --- |
| **Факультет/Институт** |  | Информационных технологий |
|  |  | (наименование факультета/ Института) |
| **Направление/специальность** |  | Разработка, сопровождение и обеспечение безопасности информационных систем |
| **подготовки:** |  | (код и наименование направления /специальности подготовки) |
| **Форма обучения:** |  | очная |
|  |  | (очная, очно-заочная, заочная) |
|  |  |  |

**Лабораторный практикум № 2**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **по дисциплине** |  | Администрирование информационных систем | | |
|  | | |  | (наименование дисциплины) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Обучающийся** |  | **Низомов Рустам С** |  |  |
|  |  | (ФИО) |  | (подпись) |
| **Группа** |  | **Вбио-305-рсоб** |  |
|  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Преподаватель** |  | Сибирев Иван Валерьевич |  |  |
|  |  | (ФИО) |  | (подпись) |

**Москва 2024 г**

1. Настройка Средств Администрирования Служб Маршрутизации в RRAS:

\* Установка роли RRAS:

\* Открыть диспетчер сервера.

\* Выбрать "Добавить роли и компоненты".

\* Установить роль "Маршрутизация и удаленный доступ".

\* Настройка интерфейсов:

\* Открыть консоль "Маршрутизация и удаленный доступ".

\* Выбрать сервер и настроить интерфейсы, участвующие в маршрутизации.

\* Создание IP-маршрутов:

\* Создать статические или динамические маршруты для направления трафика по определенным путям.

\* Настройка NAT:

\* Конфигурировать NAT для маскировки внутренних IP-адресов при выходе в интернет.

\* Настройка DHCP-сервера:

\* Если необходимо, настроить DHCP-сервер для автоматической раздачи IP-адресов.

2. Настройка Средств Удаленного Доступа в RRAS:

\* Выбор типа VPN:

\* Выбрать тип VPN (PPTP, L2TP/IPsec) в зависимости от требований безопасности и совместимости клиентов.

\* Создание VPN-подключения:

\* Создать новое VPN-подключение, указав настройки аутентификации, авторизации и шифрования.

\* Настройка разрешений доступа:

\* Определить, какие пользователи или группы могут подключаться к VPN и какие ресурсы им доступны.

\* Конфигурация политики VPN:

\* Настроить политики VPN для управления подключением и доступом.

3. Настройка Параметров Политики Безопасности:

\* Обзор локальной политики:

\* Использовать оснастку "Локальная политика безопасности" для просмотра и изменения настроек.

\* Настройка политик паролей:

\* Установить требования к сложности паролей, минимальной длине и частоте смены.

\* Конфигурация политик учетных записей:

\* Настроить параметры блокировки учетных записей, время жизни паролей и другие параметры.

\* Управление политиками аудита:

\* Конфигурировать аудит событий безопасности для отслеживания действий пользователей и систем.

\* Использование групповых политик:

\* Для централизованного управления политиками безопасности использовать групповые политики.

Дополнительные Рекомендации:

\* Изучение документации:

\* Подробные инструкции и примеры конфигурации можно найти в официальной документации Microsoft.

\* Использование графического интерфейса:

\* В большинстве случаев для настройки RRAS и политик безопасности достаточно использовать графический интерфейс.

\* Тестирование и отладка:

\* После внесения изменений тщательно протестируйте работу сети и служб.

\* Обеспечение безопасности:

\* Используйте сильные пароли, регулярно обновляйте программное обеспечение и следите за последними угрозами безопасности.

Важно:

\* Конкретные команды и настройки могут варьироваться в зависимости от версии Windows Server и требований вашей сети.

\* Для более сложных задач может потребоваться использование командной строки или PowerShell.

\* При внесении изменений в конфигурацию рекомендуется создать резервную копию.

Дополнительные Тематики для Изучения:

\* IPsec: Протокол для обеспечения безопасности IP-трафика.

\* DirectAccess: Технология для удаленного доступа к корпоративной сети.

\* Network Access Protection (NAP): Механизм для обеспечения соответствия клиентов сетевым требованиям.

\* Windows Firewall: Брандмауэр Windows для защиты от несанкционированного доступа.