**Министерство науки и высшего образования Российской Федерации** ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий Дисциплина:**

«Организация и обеспечение аудита настроек средств защиты информации»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5**

«**Защита информации при работе с каналами связи.**»

**Выполнили:**

Молитвин Илья Алексеевич, студент группы N3345

(подпись)

**Проверил:**

Пенин Андрей Семенович

(отметка о выполнении)

(подпись)

Содержание

Оглавление

[Этап 1 4](#_Toc195685439)

[Этап 2 6](#_Toc195685440)

[Этап 3 8](#_Toc195685441)

[**Заключение** 11](#_Toc195685442)

**ХОД РАБОТЫ**

**Цели:**

**Цели работы:**

Необходимо установить, настроить и протестировать несколько ключевых компонентов безопасности на виртуальной машине. Эти компоненты включают межсетевой экран (фаервол), средства анализа сетевого трафика, шифрованный канал передачи данных и систему цифровых подписей. Каждый из этих компонентов играет важную роль в обеспечении защиты данных и сетевой безопасности, и в ходе работы будет продемонстрирована их настройка и функционирование.

**Этапы работы:**

**Этап 1. Установка и настройка межсетевого экрана (фаервол)**

* Установить и настроить межсетевой экран (например, iptables для Linux, pfSense или Windows Firewall).
* Настроить правила фильтрации трафика, разрешив доступ только к необходимым портам (например, порт 1194 для OpenVPN), и заблокировать все остальные порты.
* Провести тестирование: попытаться подключиться к заблокированным портам (например, с использованием telnet или nmap) и зафиксировать результат блокировки.

**Этап 2. Установка и настройка средств анализа сетевого трафика и шифрованного канала**

* Установить средство анализа сетевого трафика (например, Wireshark или tcpdump) для мониторинга сетевых соединений.
* Настроить фильтры для отслеживания трафика на виртуальной машине (например, по порту OpenVPN).
* Установить и настроить OpenVPN для создания защищенного шифрованного канала передачи данных между виртуальными машинами. Использовать сертификаты для аутентификации.
* Провести тестирование: перехватить трафик до и после включения шифрования и продемонстрировать, что данные в канале зашифрованы (например, сравнив содержимое пакетов).

**Этап 3. Настройка и демонстрация использования цифровой подписи**

* Установить программное обеспечение для создания и проверки цифровых подписей (например, OpenSSL, GPG или встроенные средства Windows).
* Настроить систему: сгенерировать пару ключей (открытый и закрытый) для цифровой подписи и подписать тестовый файл с использованием закрытого ключа.
* Провести тестирование: проверить подлинность подписанного файла с использованием открытого ключа, а затем изменить файл и убедиться, что проверка подписи не проходит.

# Этап 1

Этап 1: **Установка и настройка межсетевого экрана (фаервол)**

1. **Устанавливаем Firewall**

Включим UFW,разрешим openvpn,и запрещаем все остальное sudo ufw default deny incoming

sudo ufw default allow outgoing  
получаем на вывод статус sudo ufw status verbose

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.  
Статус ufw enable,firewall is active

Рисунок 1 - firewall is active

Настроен firewall На убунту

# Этап 2

Этап 2: становка и настройка средств анализа сетевого трафика и шифрованного канала

Устанавливаем OpenVPN,настариваем конфиг сервера,конфиг клиента,генерируем ключи через easy-rsa  
Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 2 – файлы опенвпн

Получаем файлы.Настраиваем конфиги клиента и сервера,запускаем вайршарк на ens33,потом запускаем опенвпн,проверяем,что появились пакеты зашифрованные.  
**Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.**

Рисунок 3 – client.ovpnИзображение выглядит как текст, снимок экрана, программное обеспечение, число

Контент, сгенерированный ИИ, может содержать ошибки.Рисунок 4 –слушаем ens33

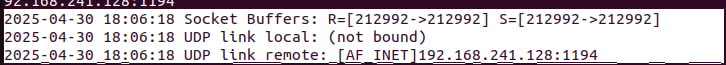


Рисунок 5 – врубаем openvpn,видим зашифрованные пакеты

# Этап 3

Этап 3. Настройка и демонстрация использования цифровой подписи

Устанавливаем OpenSSl,генерируем ключи,извлекаем открытый ключь,создаем текстовый файл и подписываем с помощью открытого ключа.Проверяем подлинность.  
Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.  
Рисунок 6 – генерируем ключ  
Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 7 – проверка,что все работает

Теперь нужно проверить,что будет,если мы добавим доп строку,проверяем,что верификация не пройдет.  
Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.  
Рисунок 8 – Верификация не пройдена

## **Заключение**

В ходе выполнения лабораторной работы были успешно реализованы ключевые меры по обеспечению информационной безопасности на виртуальной машине. На первом этапе был настроен файрвол,что позволило ограничить сетевую активность и допустить подключение только к разрешённым портам, включая порт шифрованного соединения. На втором этапе были установлены и протестированы средства анализа трафика и защищённый VPN-канал с использованием OpenVPN, что позволило убедиться в шифровании передаваемых данных и невозможности их перехвата в открытом виде. На третьем этапе была настроена система цифровой подписи, включая генерацию ключевой пары, подписание и проверку целостности данных. Проведённые тесты подтвердили корректность настройки: при изменении подписанного файла проверка подписи не проходила. Таким образом, были продемонстрированы базовые, но важные средства защиты данных при передаче, хранении и проверке подлинности информации