Практическое занятие №4

НАСТРОЙКА БРАНДМАУЭРА WINDOWS

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель занятия**

Овладеть навыками настройки и использования брандмауэра Windows для обеспечения безопасности системы.

**Краткие теоретические сведения**

Брандмауэр (межсетевой экран) — это программное или аппаратное средство, которое контролирует входящий и исходящий трафик на основе заданных правил безопасности. Он позволяет предотвратить несанкционированный доступ к компьютеру и защищает его от различных угроз.

**Принципы работы брандмауэра:**

1. **Фильтрация трафика:** Брандмауэр проверяет пакеты данных и принимает решение о их разрешении или блокировке.
2. **Правила доступа:** Настройки брандмауэра определяют, какие приложения могут получать доступ к сети и какие соединения могут быть установлены.
3. **Мониторинг активности:** Брандмауэр ведет учет сетевой активности, что позволяет выявлять подозрительные действия.

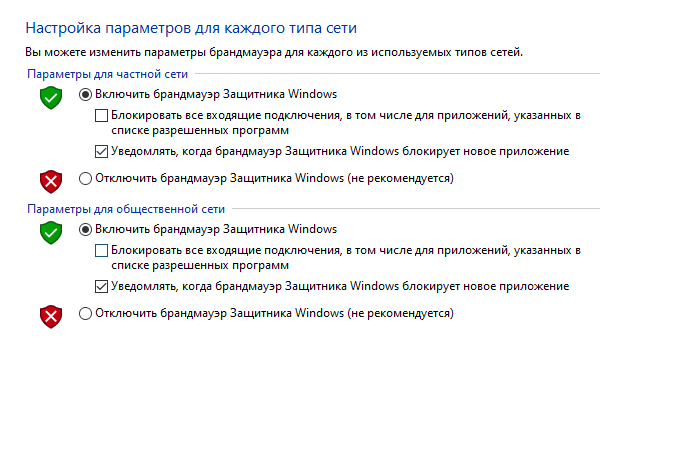
**Условие задания**

1. Включить брандмауэр Windows.
2. Настроить правила для входящих и исходящих подключений.
3. Создать правила для блокировки и разрешения подключения для выбранной программы.

**Исполнительская часть**

**Шаг 1: Включение брандмауэра Windows**

1. Откройте «Панель управления» через меню «Пуск».
2. Перейдите в раздел «Система и безопасность».
3. Выберите «Брандмауэр Windows».
4. В левой части окна выберите «Включение и отключение брандмауэра Windows».
5. Убедитесь, что брандмауэр включен для всех сетевых подключений.



**Шаг 2: Настройка правил для входящих и исходящих подключений**

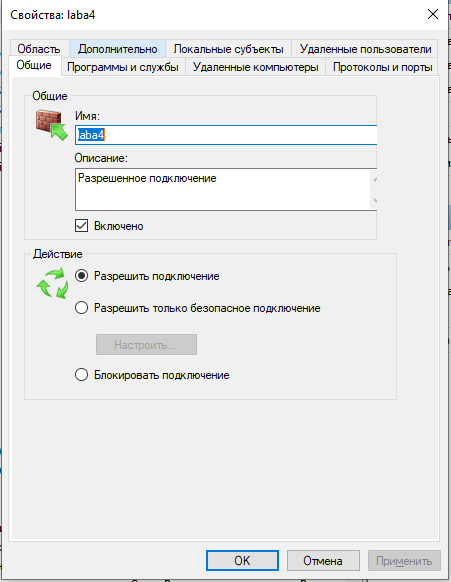
1. В меню «Брандмауэр Windows» выберите «Дополнительные параметры».
2. В разделе «Правила для входящих подключений» создайте новое правило:
   * Нажмите «Создать правило».
   * Выберите «Для программы» и укажите путь к исполняемому файлу.
   * Выберите действие (разрешить или блокировать).
   * Завершите настройку правила

**Блокировка входящего подключения:**

.Изображение выглядит как текст, электроника, снимок экрана, дисплей

Контент, сгенерированный ИИ, может содержать ошибки.

**Разрешение входящего подключения:**



**Правила для входящего подключения:**

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

**Блокировка исходящего подключения**

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Контент, сгенерированный ИИ, может содержать ошибки.

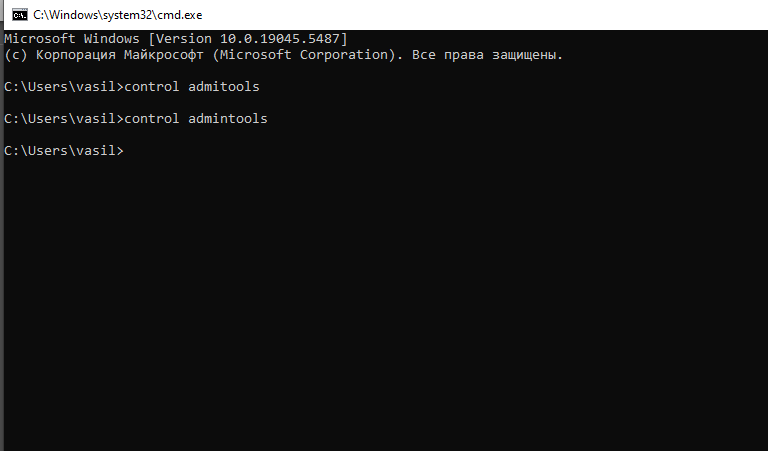
**Разрешение исходящего подключения:**  
Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

**Правила для исходящего подключения:**

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

**Выполнение команды control admintools:**  


При выполнении открывается следующее окно:  
Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Контент, сгенерированный ИИ, может содержать ошибки.

**Выполнение команды dxdiag:**

Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Открывается следующее окно:  
Изображение выглядит как текст, электроника, снимок экрана, дисплей

Контент, сгенерированный ИИ, может содержать ошибки.

**Выполнение команды diskmgmt.msc:**  
Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Открывает следующее окно:  
Изображение выглядит как текст, электроника, снимок экрана, дисплей

Контент, сгенерированный ИИ, может содержать ошибки.

**Заключение**

В ходе выполнения практической работы была успешно настроена работа брандмауэра Windows. Были созданы правила для входящих и исходящих подключений, обеспечивающие защиту системы от несанкционированного доступа. Овладение навыками работы с брандмауэром является важным шагом в обеспечении информационной безопасности.

**Использованные источники**

1. Документация Microsoft по настройке брандмауэра Windows.
2. Учебное пособие по основам защиты информации.