

Политика безопасности Windows

Настройка политики безопасности в Windows 10 будет состоять из 3 основных пунктов:

- 1 Локальная политика безопасности
- 2 Ограничение политики выполнения скриптов
- 3 Настройка Брандмауэра

Они позволят оптимизировать и обезопасить систему от несанкционированных действий вредоносного ПО или пользователей.



1 Локальная политика безопасности

Политика безопасности Windows — это набор правил, которые определяют, как система защищает себя от угроз, и могут быть настроены администраторами для управления доступом пользователей и другими настройками.

- 1.1. Выполните сочетание клавиш Win + R для открытия программы “Выполнить”. Введите “secpol.msc” и нажмите “OK”.

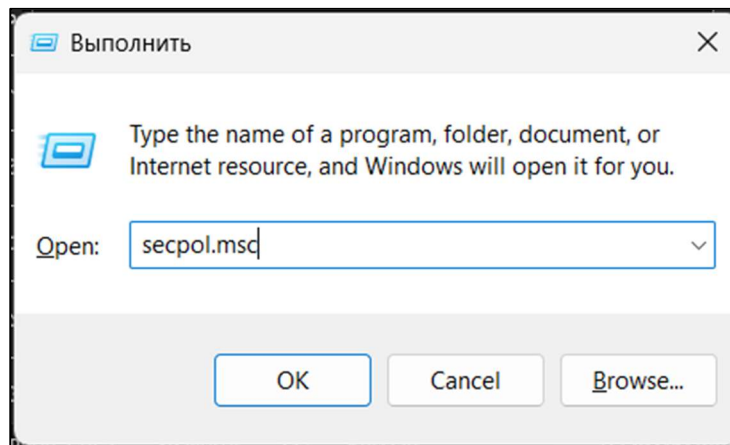


Рисунок 1 – Окно программы “Выполнить”

- 1.2. Перейдите в Параметры безопасности - Политики учетных записей - Политика паролей.

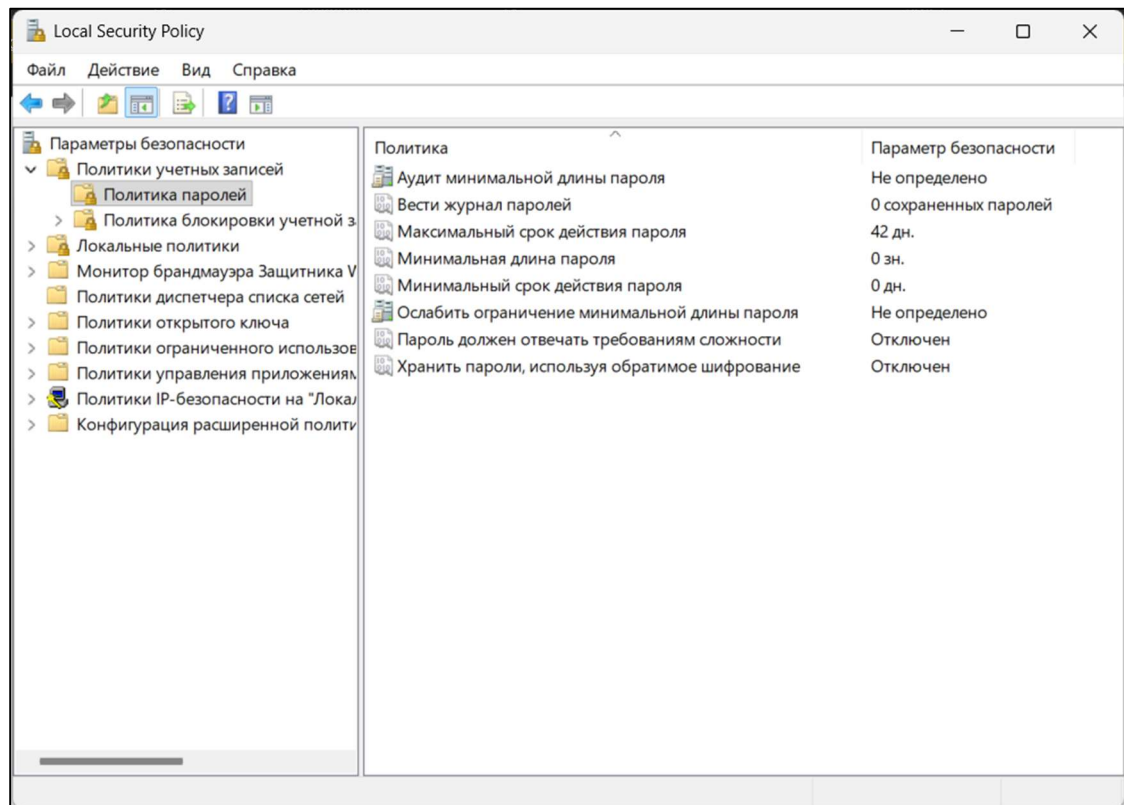


Рисунок 2 – Окно локальной политики безопасности

- 1.3. Изменим следующие параметры безопасности:
— минимальная длина пароля - 8 символов;

- максимальный срок действия пароля - 42 дня;
- минимальный срок действия пароля - 1 день;
- включите параметр “Пароль должен отвечать требованиям сложности”;
- включите параметр “Хранить пароли, используя обратимое шифрование”.

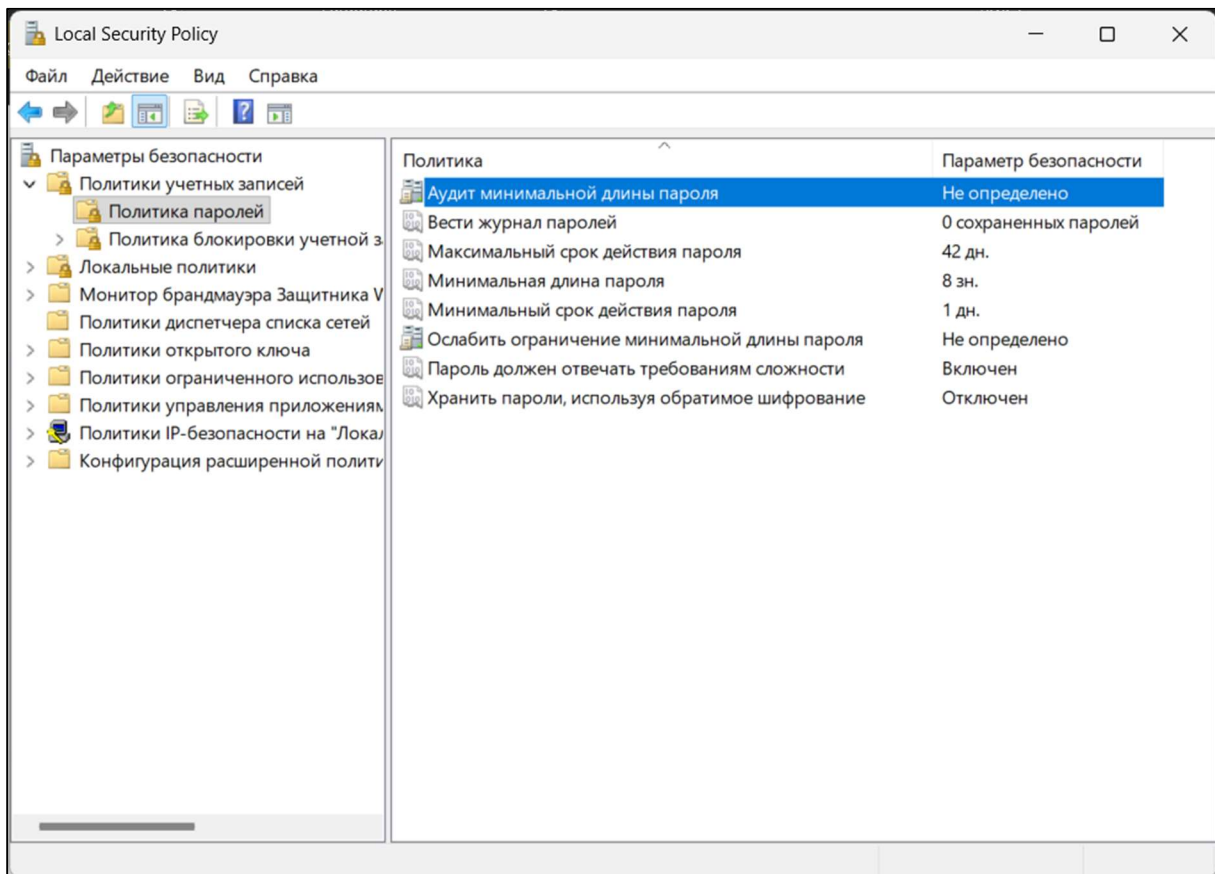


Рисунок 3 – Вкладка “Политика паролей” с измененными параметрами

2 Ограничение политики выполнения скриптов

Политика выполнения скриптов Windows — это встроенный механизм безопасности, предназначенный для защиты системы от несанкционированных и вредоносных скриптов.

2.1. Выполните сочетание клавиш Win + Si введите powershell.

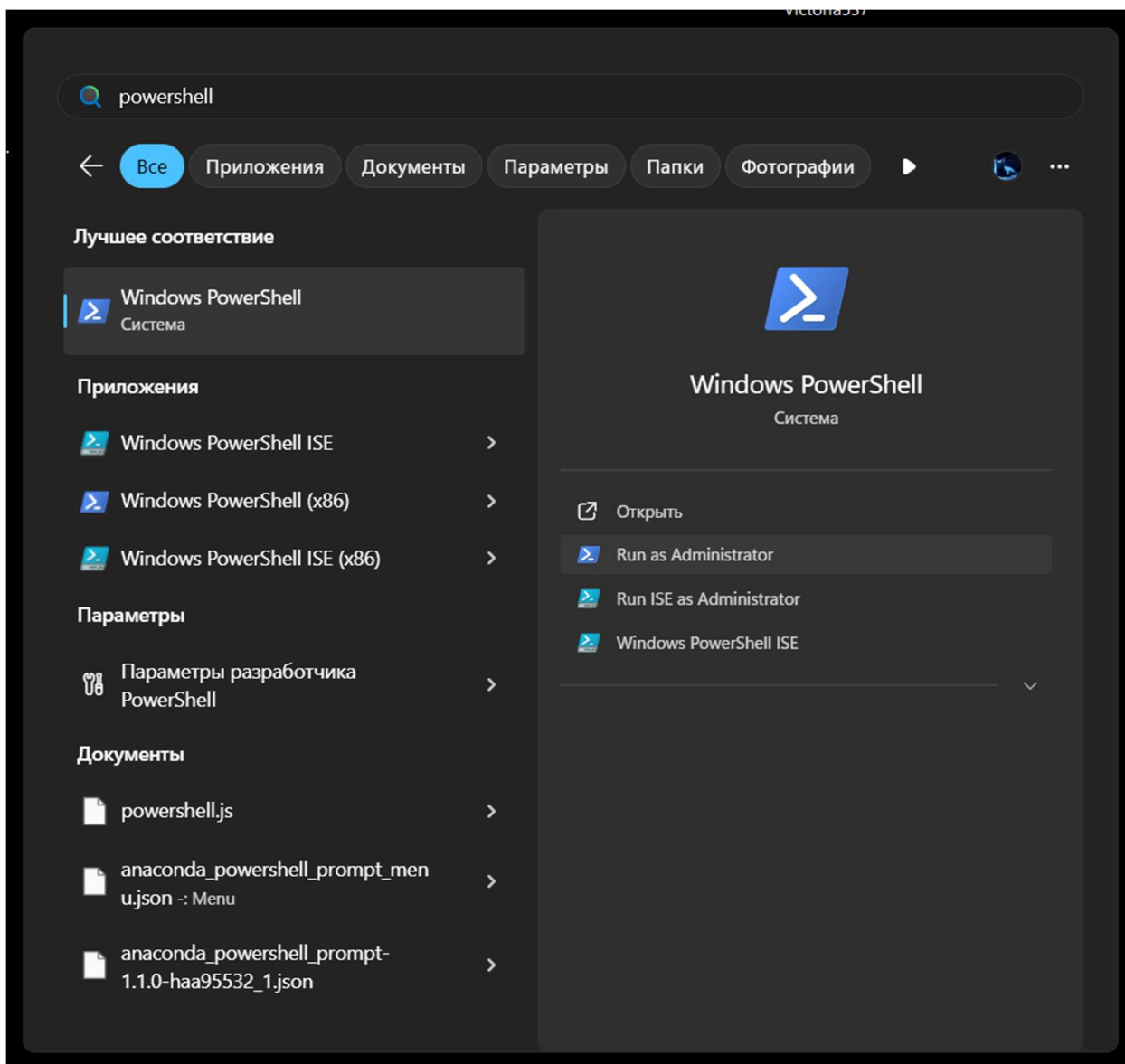


Рисунок 4 – Окно поиска

2.2. Запустите Windows Powershell от имени администратора

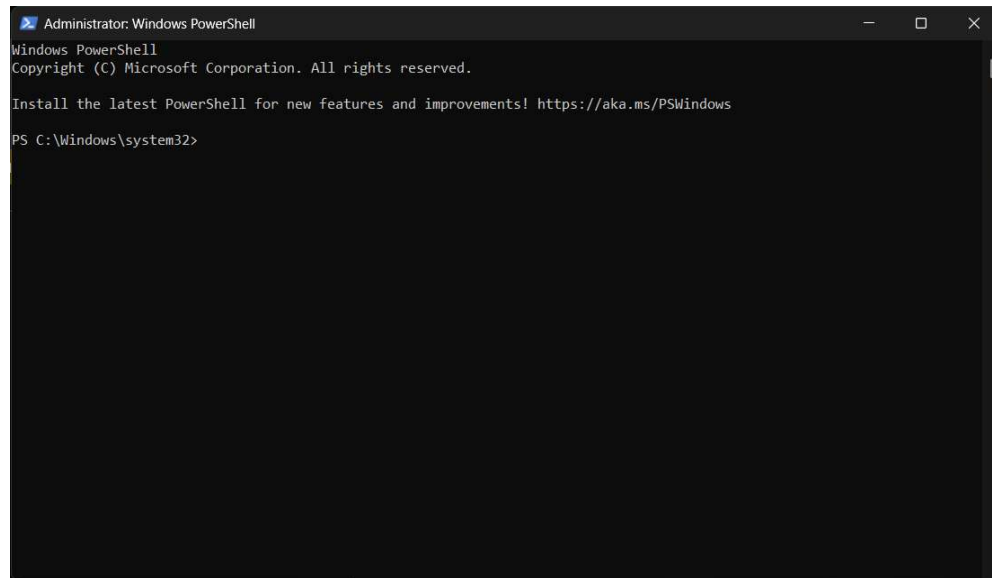


Рисунок 5 – Окно Windows PowerShell

- 2.3. Введите команду `Get-ExecutionPolicy -List` для получения настройки выполнения скриптов для всех областей

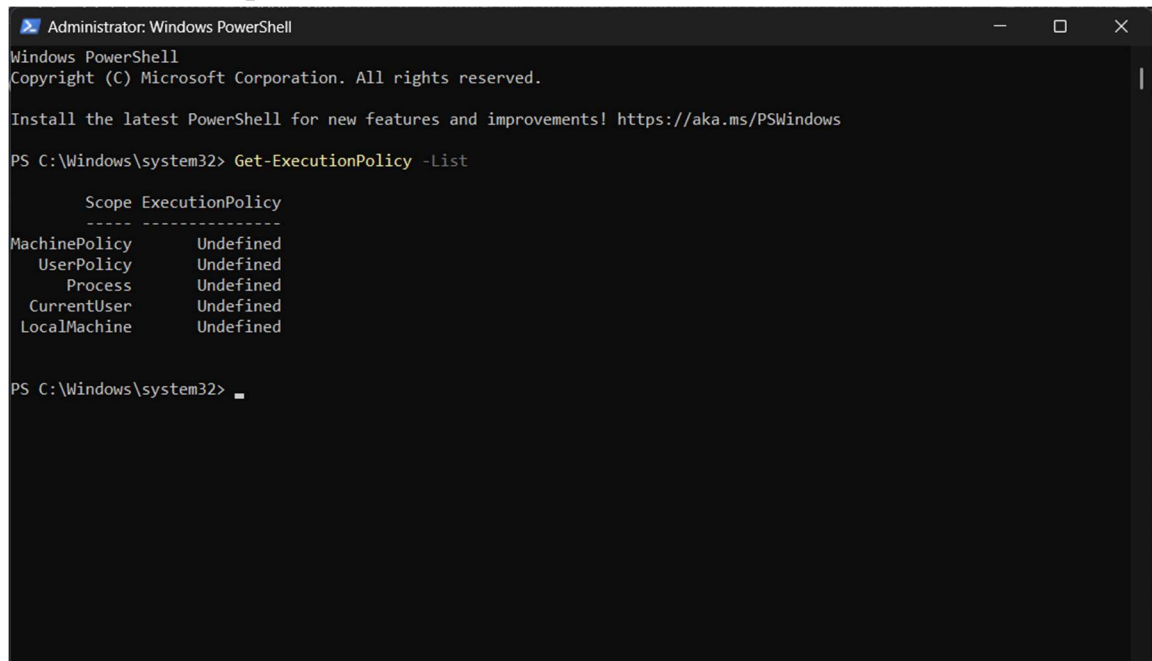


Рисунок 6 – Результат выполнения команды “`Get-ExecutionPolicy -List`”

- 2.4. Введите команду `Set-ExecutionPolicy RemoteSigned -Force` для разрешения выполнения только подписанных скриптов

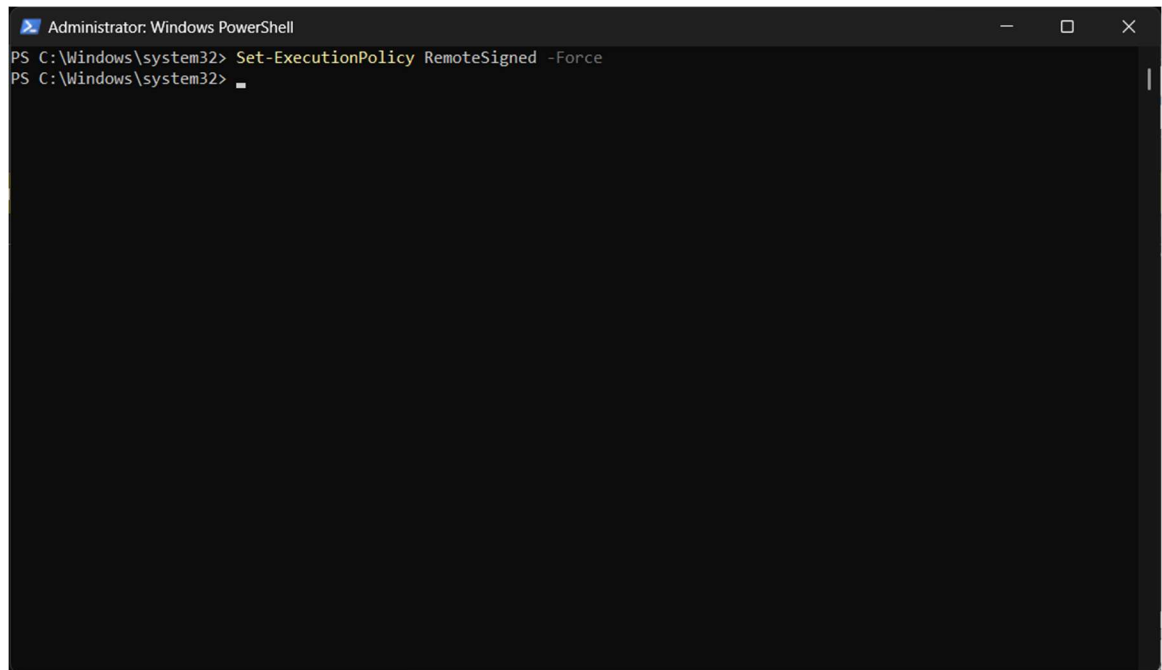


Рисунок 7 – Результат выполнения команды “Set-ExecutionPolicy RemoteSigned -Force”

3 Настройка Брандмауэра

Брандмауэр Windows — это функция безопасности, которая помогает защитить устройство, фильтруя сетевой трафик, который входит в устройство и выходит из нее.

- 3.1. Выполните сочетание клавиш Win + R для открытия программы “Выполнить”. Введите “firewall.cpl” и нажмите “ОК”.

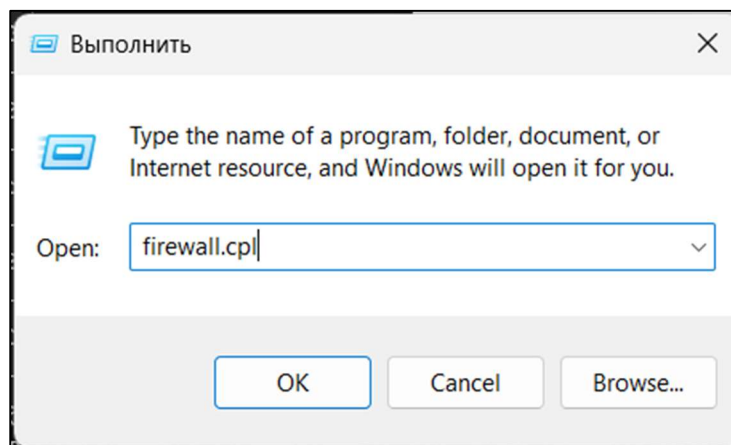


Рисунок 8 – Окно программы “Выполнить”

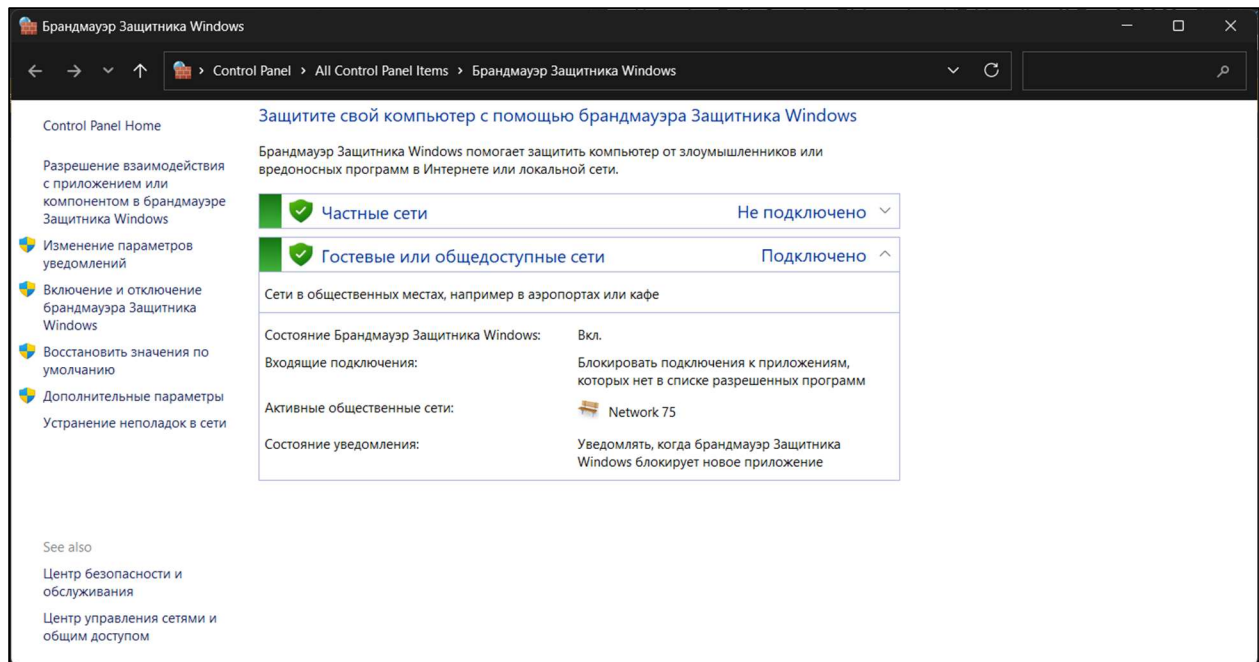


Рисунок 9 – Окно брандмауэра Windows

3.2. Нажмите кнопку “Дополнительные параметры”. Выберите пункт “Правила для входящих подключений” и нажмите “Создать правило”.

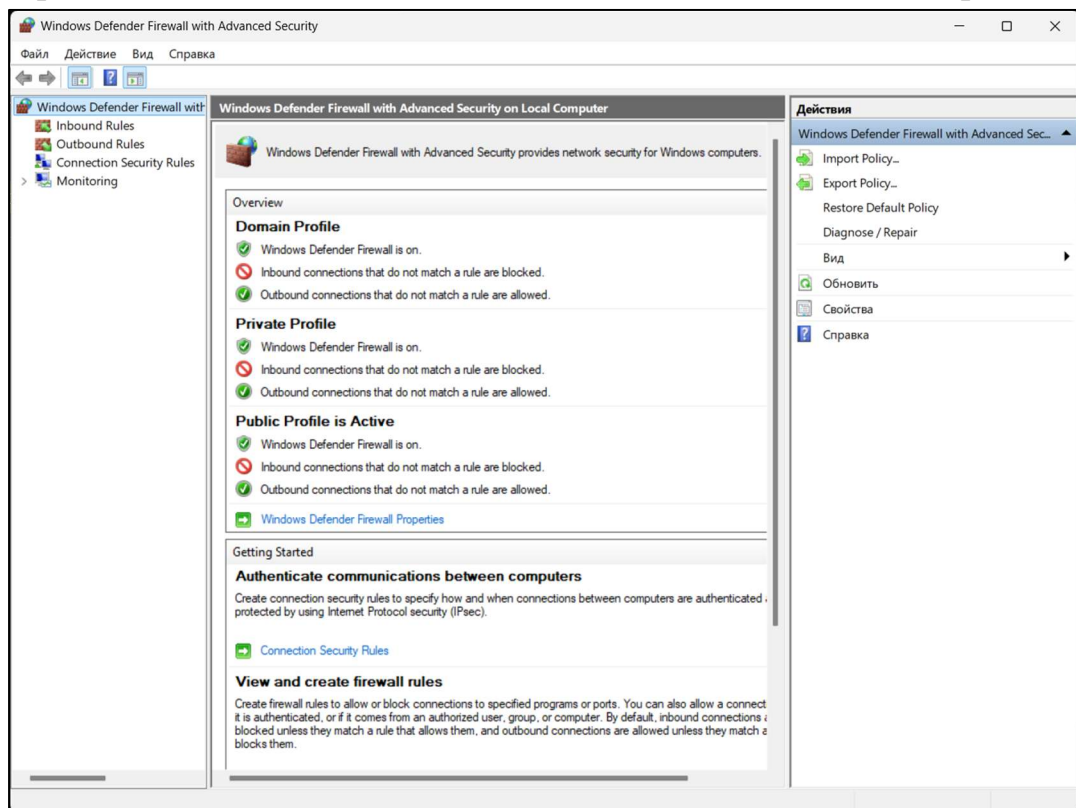


Рисунок 10 – Окно дополнительных параметров

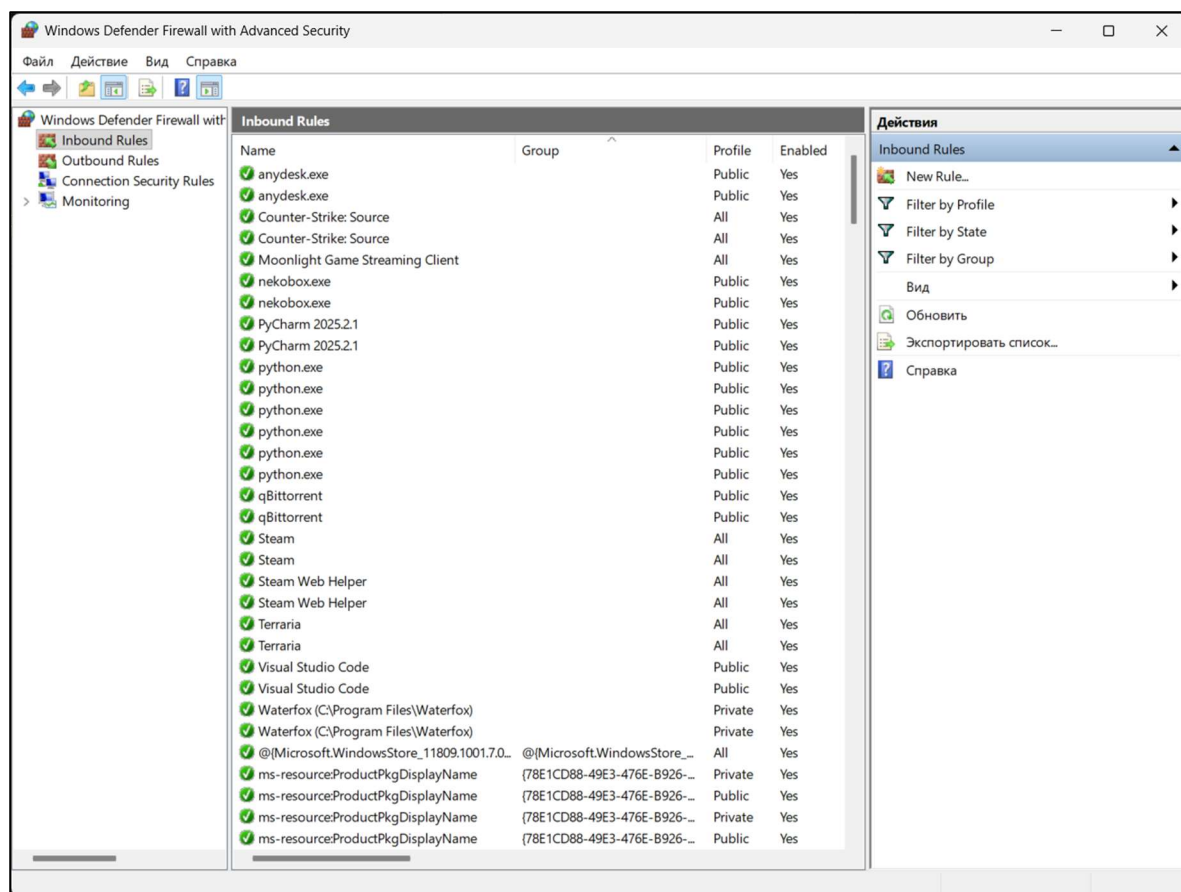


Рисунок 11 – Вкладка “Правила для входящих подключений”

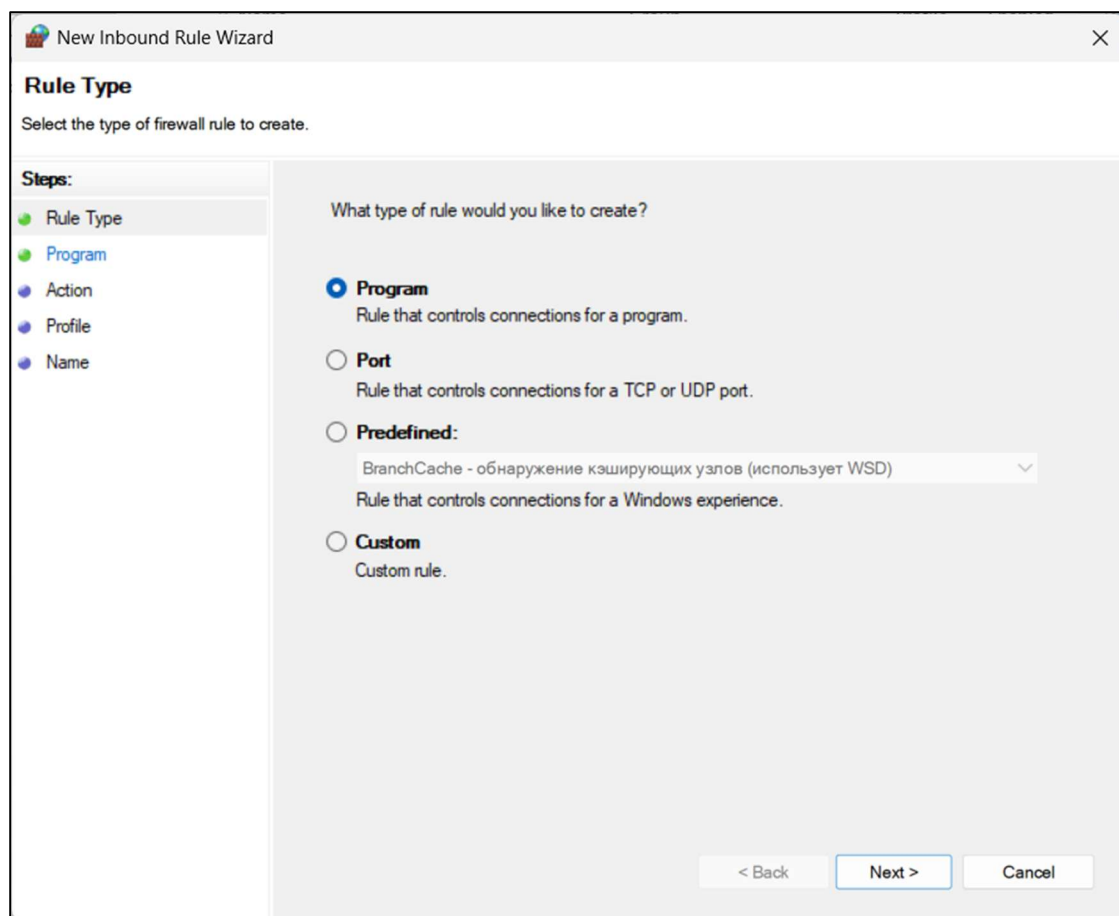


Рисунок 12 – Окно создания правила

- 3.3. Выберем тип правила “Порт”. Выберем протокол TCP и введем порт 445.

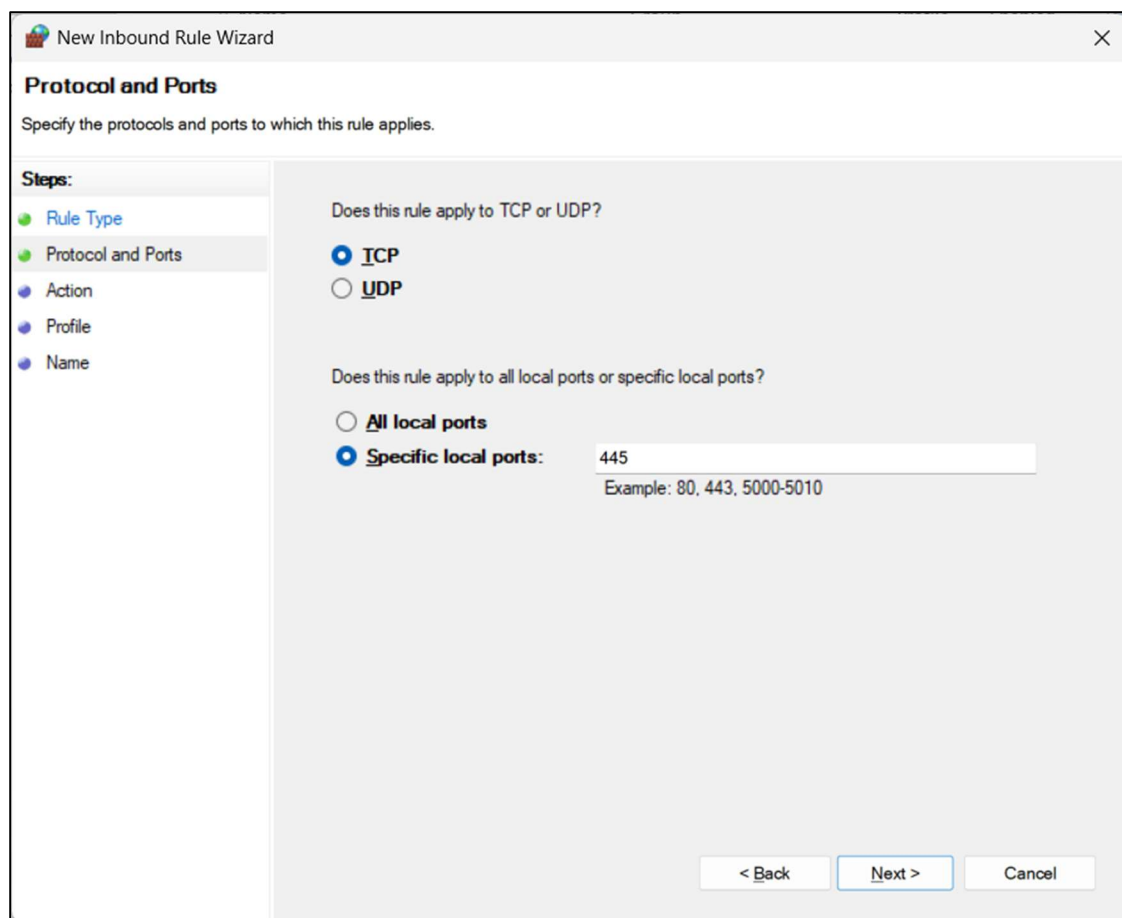


Рисунок 13 – Окно создания правила – пункт “Протокол и порты”

3.4. Заблокируем данный порт. Выбираем пункт “Блокировать подключение”.

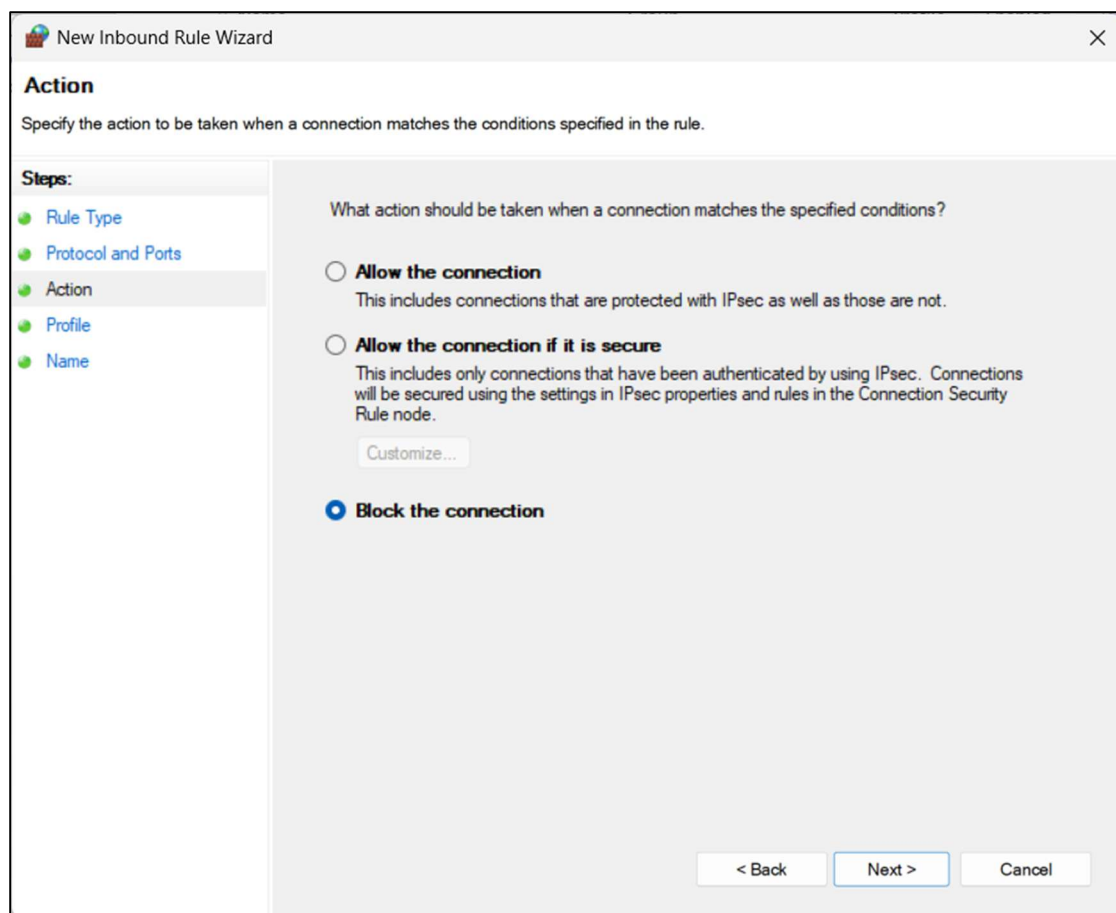


Рисунок 14 – Окно создания правила – пункт “Действие”

3.5. Необходимо дать название новому правилу. Введем его в поле “Имя”

The screenshot shows a Windows-style dialog box titled "New Inbound Rule Wizard" with a close button (X) in the top right corner. The main heading is "Name", followed by the instruction "Specify the name and description of this rule." On the left, a "Steps:" sidebar lists five steps: "Rule Type", "Protocol and Ports", "Action", "Profile", and "Name". The "Name" step is currently selected and highlighted. The main area contains a "Name:" label with a text input field containing "new_rule", and a "Description (optional):" label with a larger, empty text area below it. At the bottom right, there are three buttons: "< Back", "Finish" (which is highlighted with a blue border), and "Cancel".

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name**

Name:
new_rule

Description (optional):

< Back Finish Cancel

Рисунок 15 - Окно создания правила – пункт “Имя”