

Настройка политики безопасности Windows

Настройка политики безопасности в Windows 11 будет состоять из 3 основных пунктов:

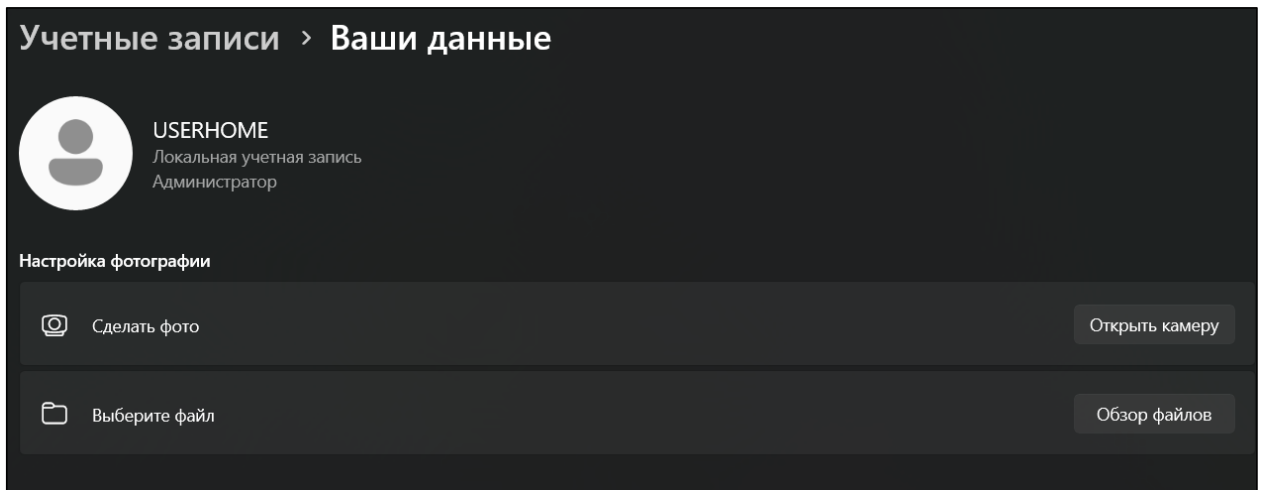
1. Настройка реестра
2. Оптимизация служб Windows
3. Настройка Брандмауэра

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

Версия Windows 11: 10.0.26100 “Pro”.

| | |
|------------|---------------------------------|
| Имя ОС: | Майкрософт Windows 11 Pro |
| Версия ОС: | 10.0.26100 Н/Д построение 26100 |

Профиль Windows



1. Настройка реестра

Реестр Windows представляет собой структурированную базу данных, в которой хранятся параметры и информация, используемая операционной системой, драйверами, службами и программами.

1.1 Открытие реестра Windows. Открыть командную строку и ввести команду “regedit” для открытия реестра Windows.

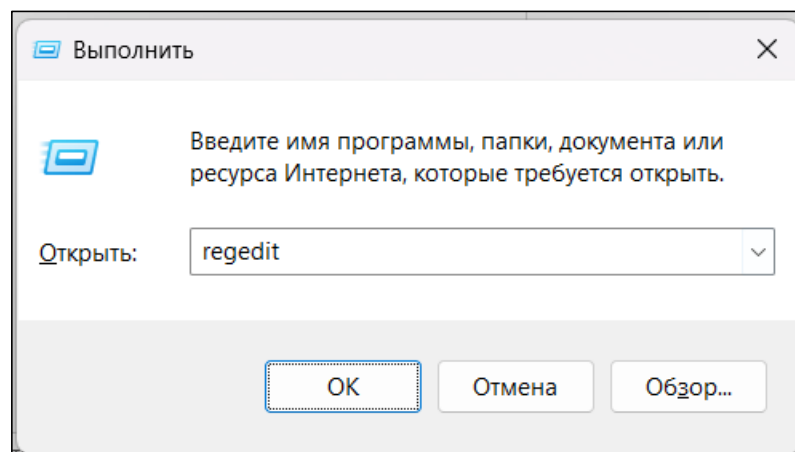


Рисунок 1.1.1 – Ввод команды “regedit”

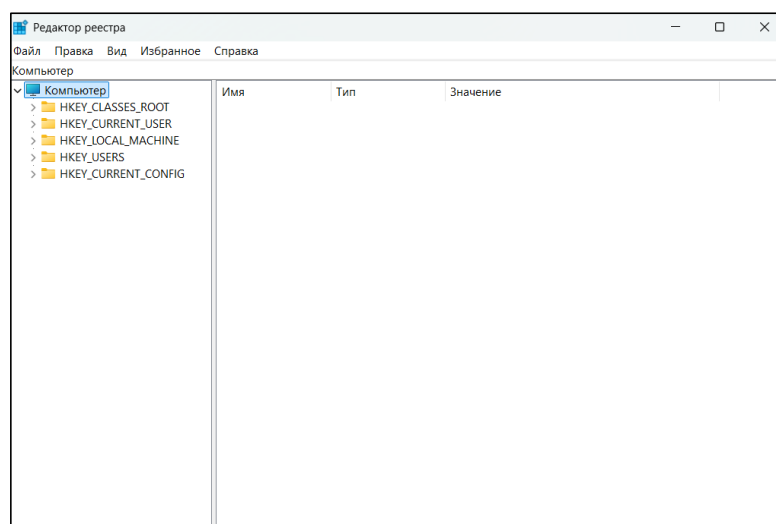


Рисунок 1.1.2 – Реестр Windows

1.2 Создание сохранения файла реестра. Нажать пункт “Файл”, и из выпадающего списка выбрать пункт “Экспорт”.

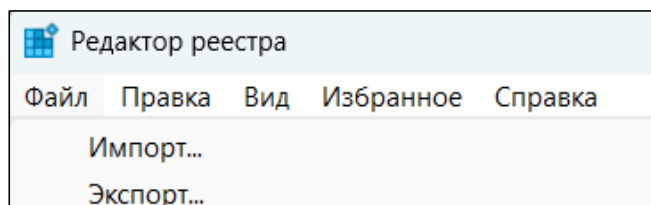


Рисунок 1.2 – Верхнее меню

1.3 Дать название файлу и выбрать путь сохранения.

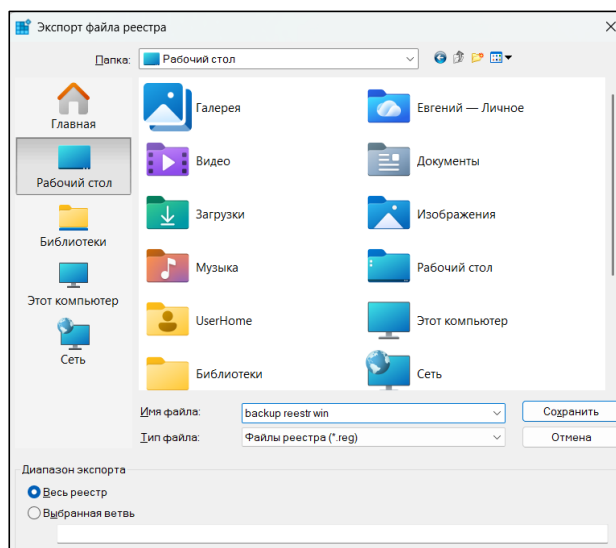


Рисунок 1.3 – Окно экспорта реестра

1.4 Проверить файл экспорта реестра

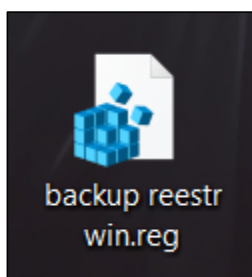


Рисунок 1.4 – Файл экспорта реестра

1.5 Отключение меню “Поделиться в проводнике”. Перейти к HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions и создать раздел Blocked.

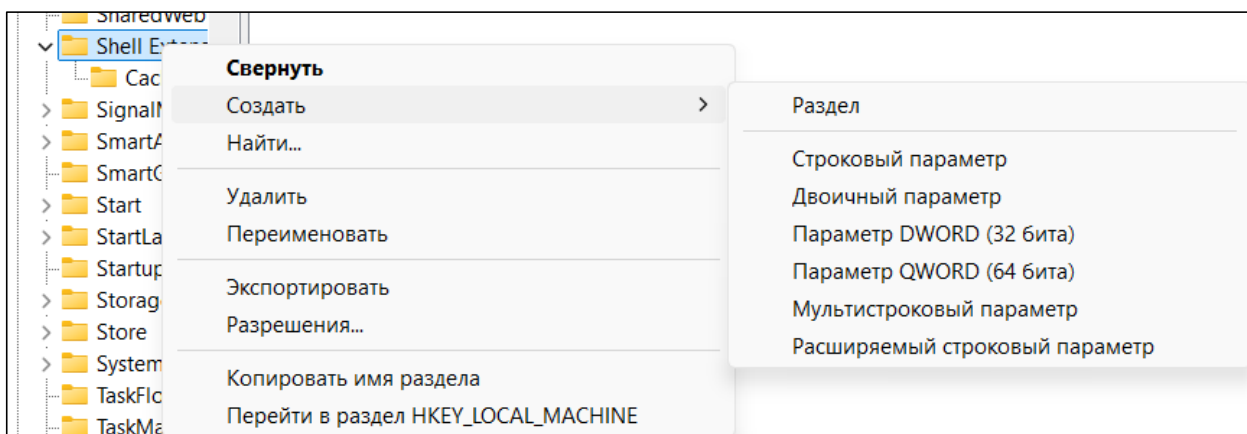


Рисунок 1.5 – Создание раздела blocked

1.6 Создать строковый раздел с именем “{e2bf9676-5f8f-435c-97eb-11607a5bedf7}”

| Имя | Тип |
|--|--------|
| (По умолчанию) | REG_SZ |
| {e2bf9676-5f8f-435c-97eb-11607a5bedf7} | REG_SZ |

Рисунок 1.6 – Раздел для блокировки “Поделиться”

1.7 Перезагрузить компьютер. Открыть проводник и проверить отсутствие пункта “поделиться”.

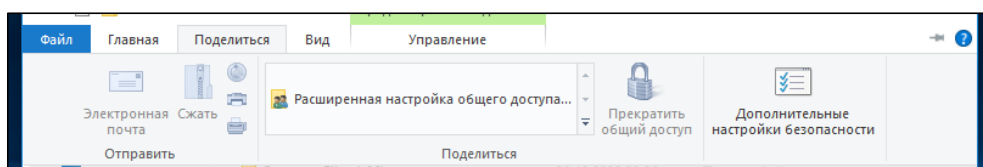


Рисунок 1.6 – Заблокированное меню “поделиться”

2. Оптимизация служб Windows.

2.1 Открыть командную строку и ввести команду “services.msc” для открытия служб Windows.

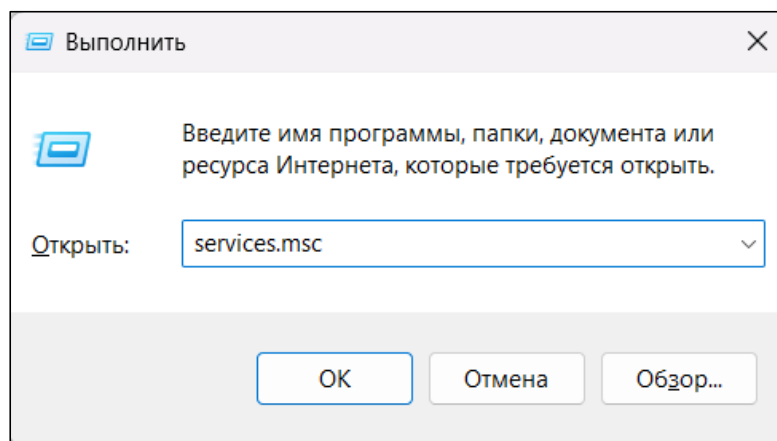


Рисунок 2.1.1 – Командная строка

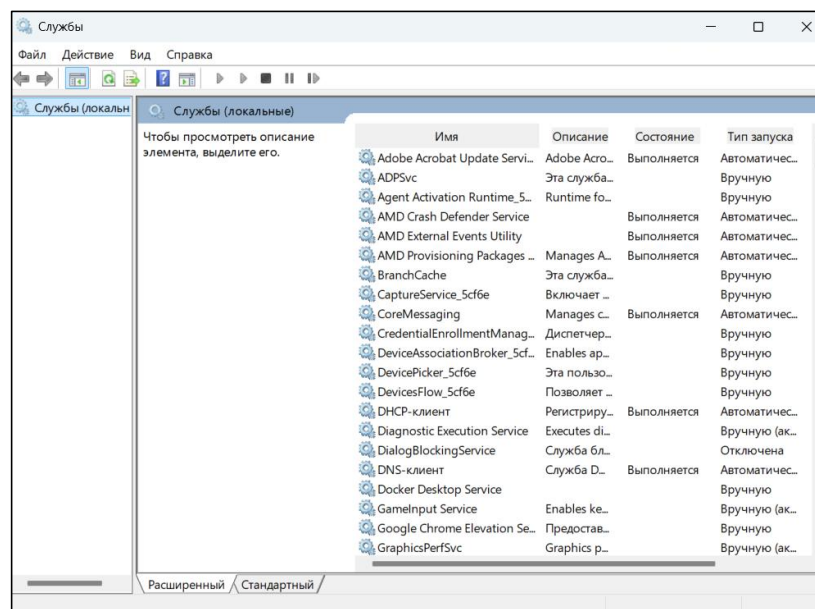


Рисунок 2.1.2 – Службы Windows

2.2 Отключить не нужные службы, такие как “Диспетчер печати”

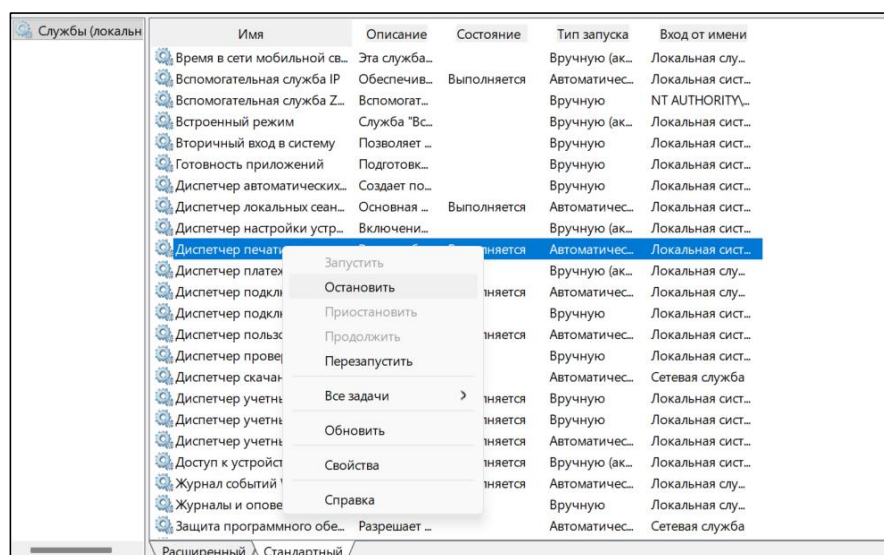


Рисунок 2.2 – Перечень служб

2.3 Нажать “Свойства” и изменить тип запуска на “Отключена”

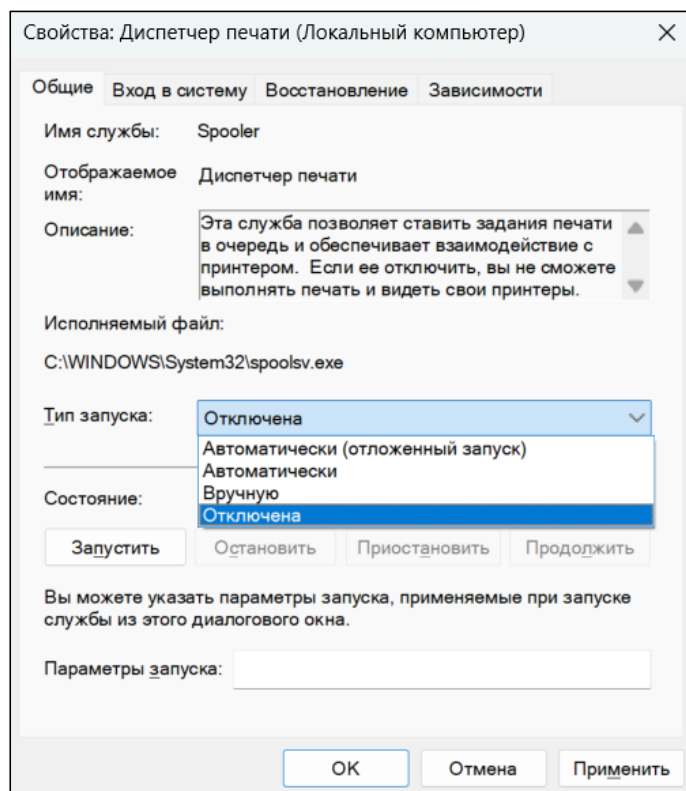


Рисунок 2.3 – Свойства службы

3. Настройка Брандмауэра

3.1 Открыть командную строку и ввести команду “ firewall.cpl” для открытия Брандмауэра Windows.

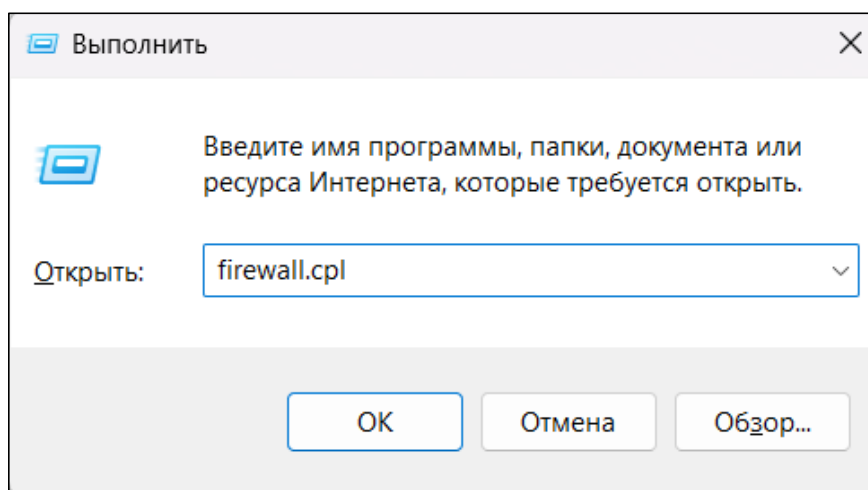


Рисунок 3.1.1 – Командная строка

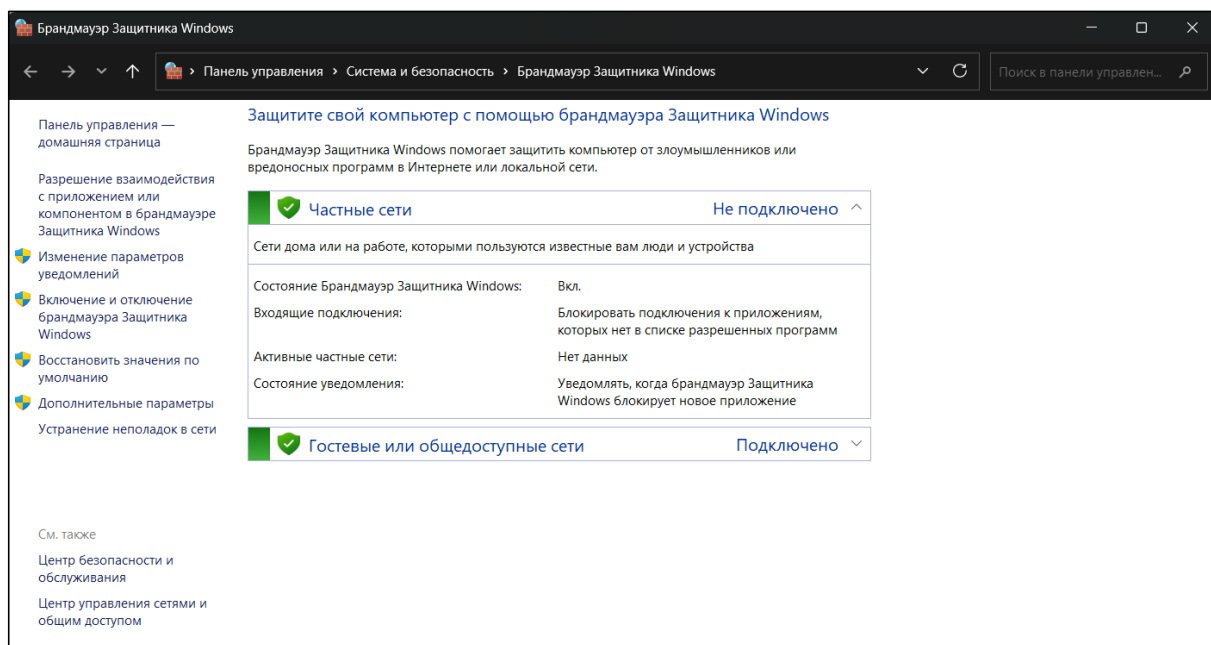


Рисунок 3.1.2 – Брандмауэр Windows

3.2 Разрешить подключение к веб-серверу. Нажать кнопку “Дополнительные параметры”.



Рисунок 3.2 – Кнопка “дополнительные параметры”

3.3 Выбрать пункт “Правила для входящих подключений” и нажать “Создать правило...”

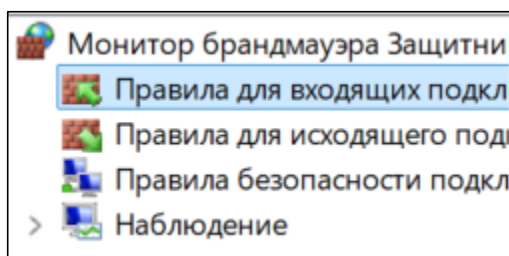


Рисунок 3.3.1 – Пункты дополнительных параметров

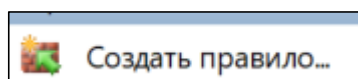


Рисунок 3.3.2 – Кнопка “Создать правило”

3.4 Ввести параметры для правила (порт: 80).

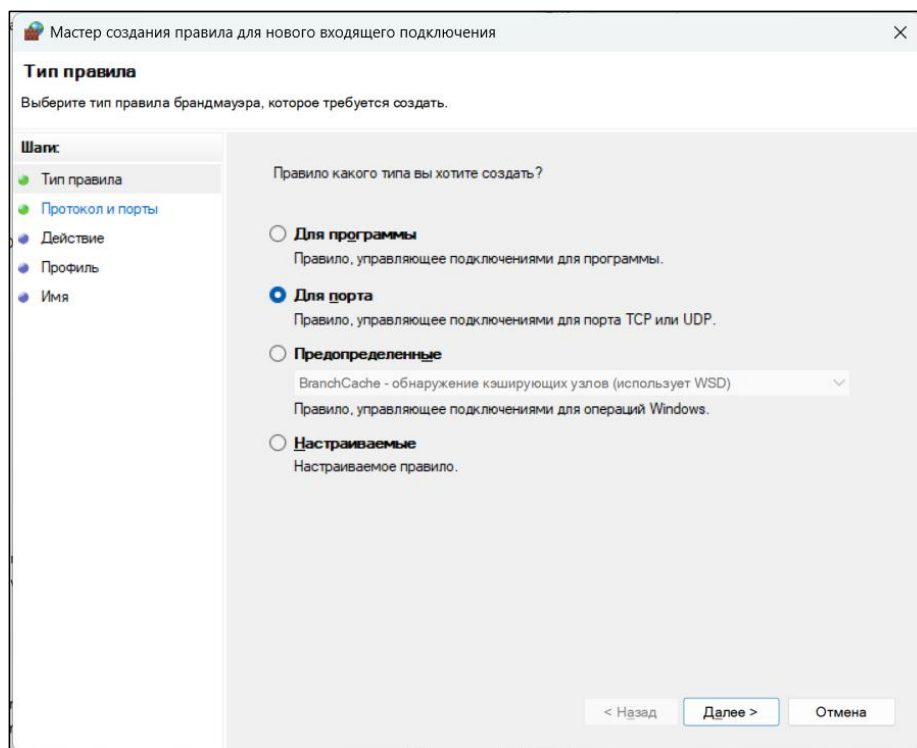


Рисунок 3.4.1 – Окно создания правила – тип правила

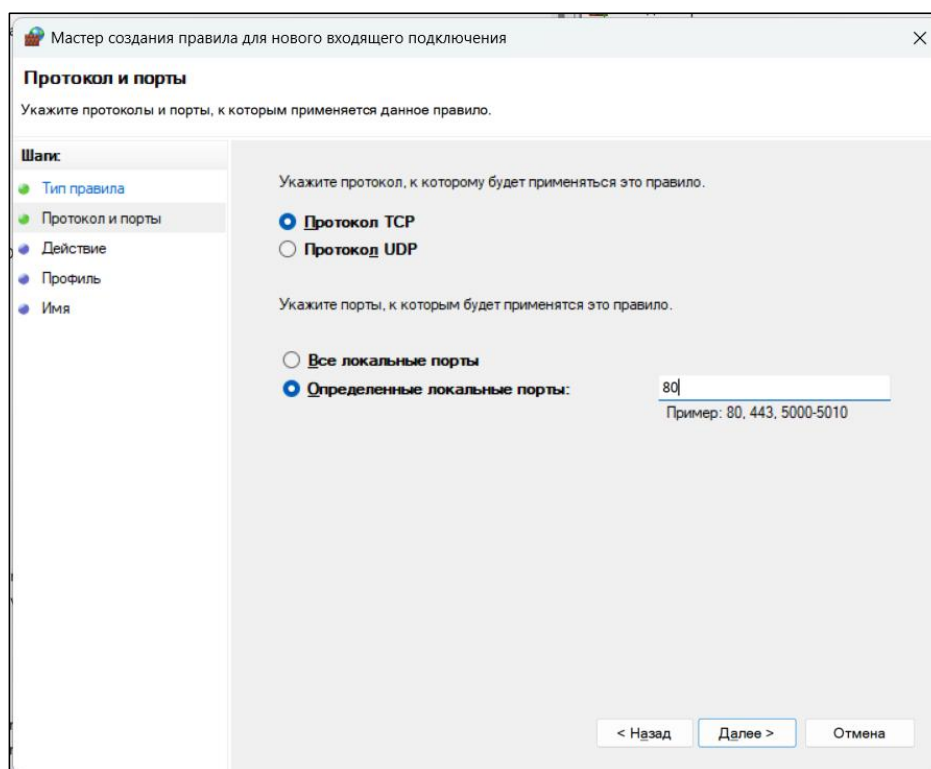


Рисунок 3.4.2 – Окно создания правила – протоколы и порты

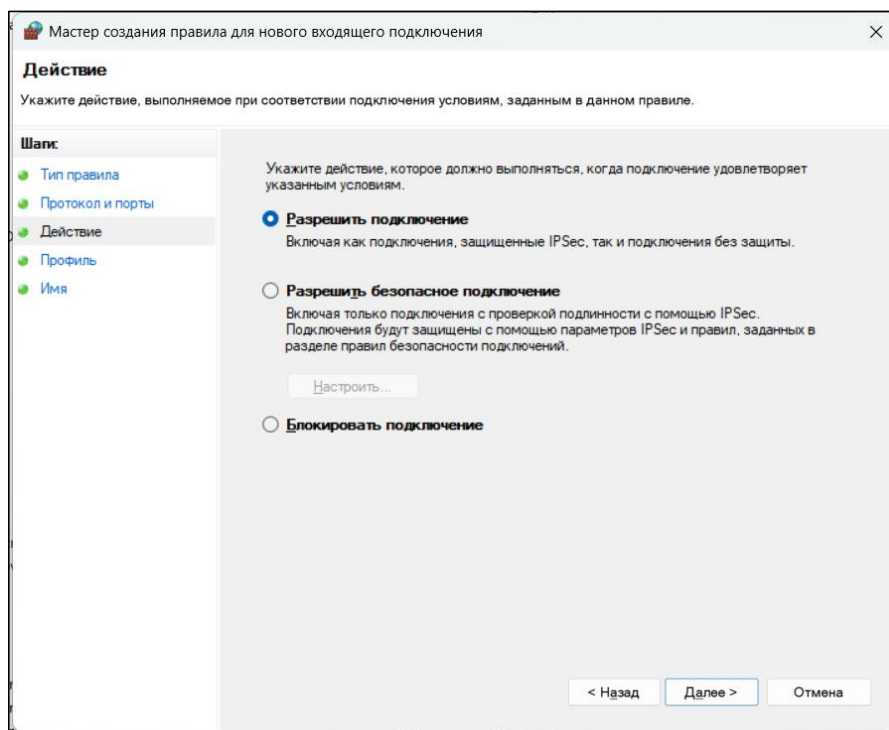


Рисунок 3.4.3 – Окно создания правила – действие

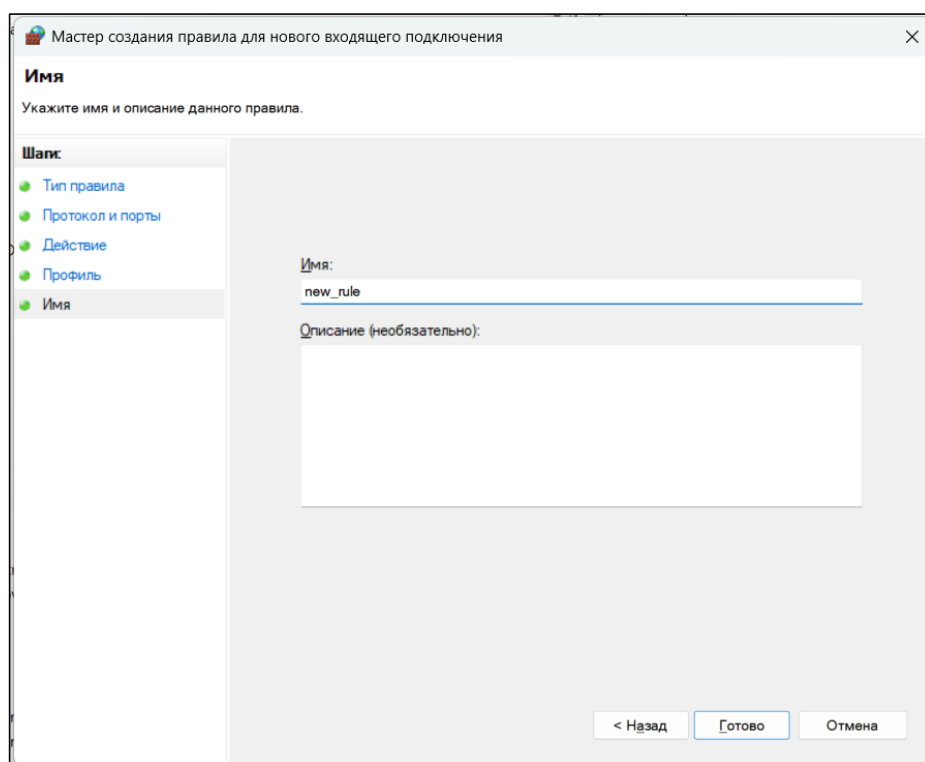


Рисунок 3.4.4 – Окно создания правила – имя

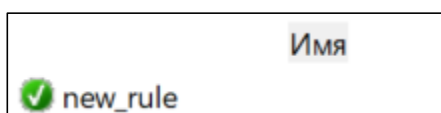


Рисунок 3.4.5 – Созданное новое правило

3.5 Ограничение работы браузера. Выбрать пункт “Правила для исходящего трафика” и нажать кнопку “Создать правило...”

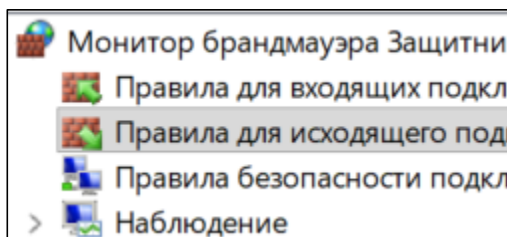


Рисунок 3.5.1 – Пункты дополнительных параметров

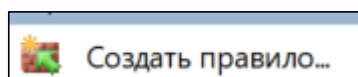


Рисунок 3.5.2 – Кнопка “Создать правило”

3.6 Ввести параметры для правила (путь к браузеру).

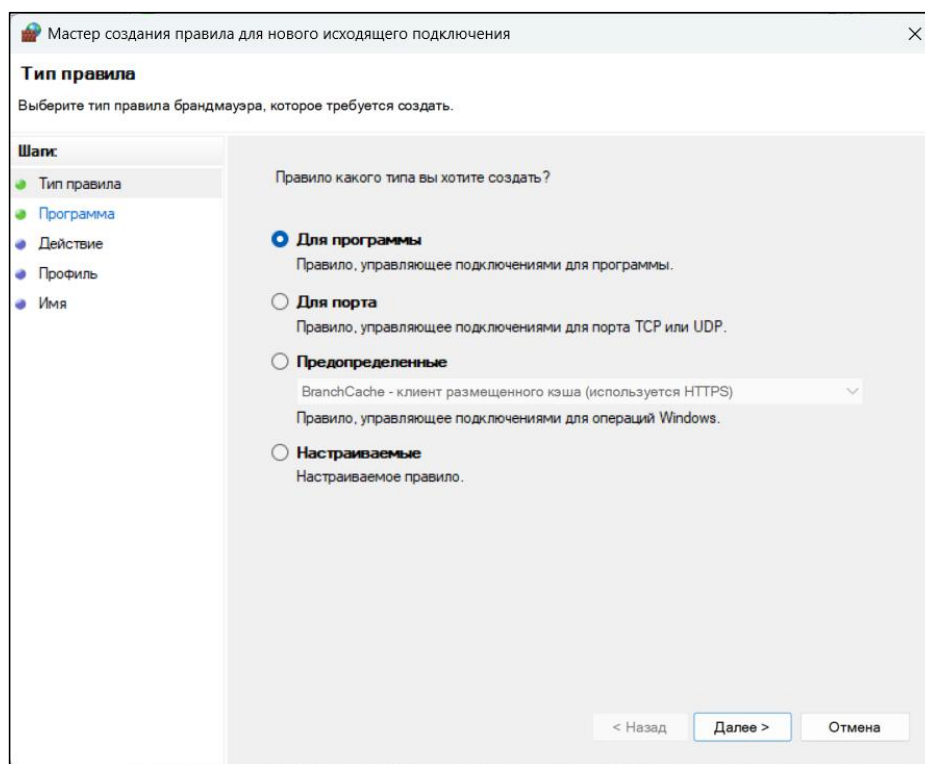


Рисунок 3.6.1 – Окно создания правила – тип программы

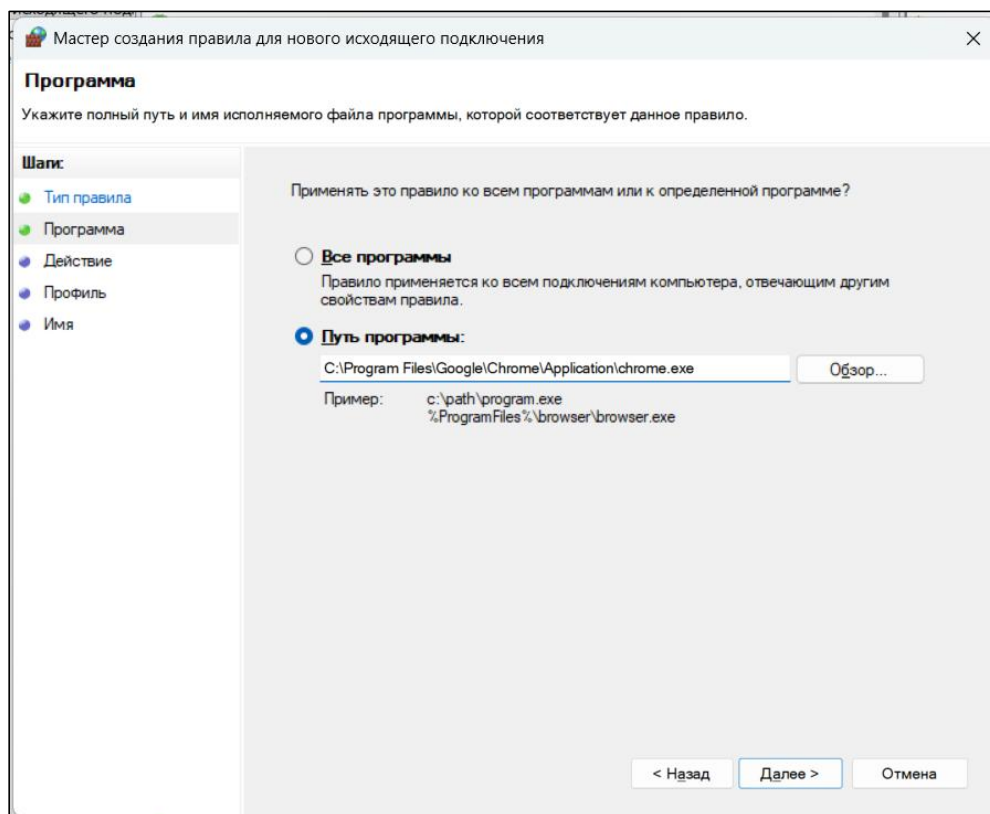


Рисунок 3.6.2 – Окно создания правила – программа

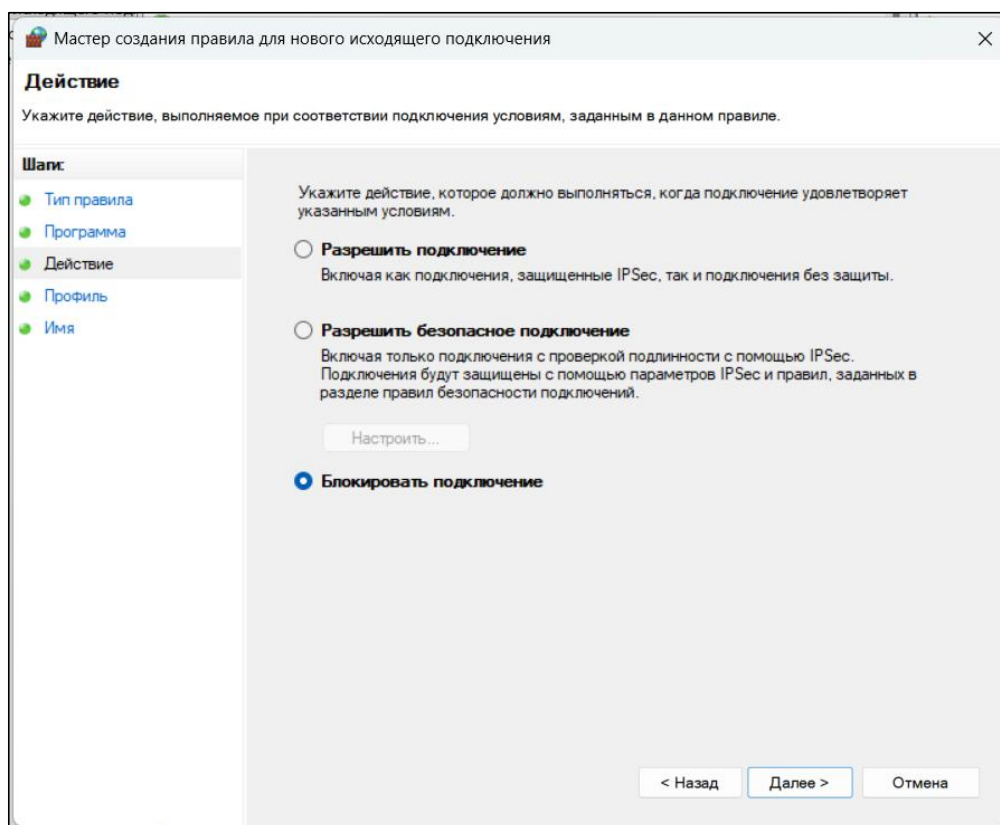


Рисунок 3.6.3 – Окно создания правила – действие

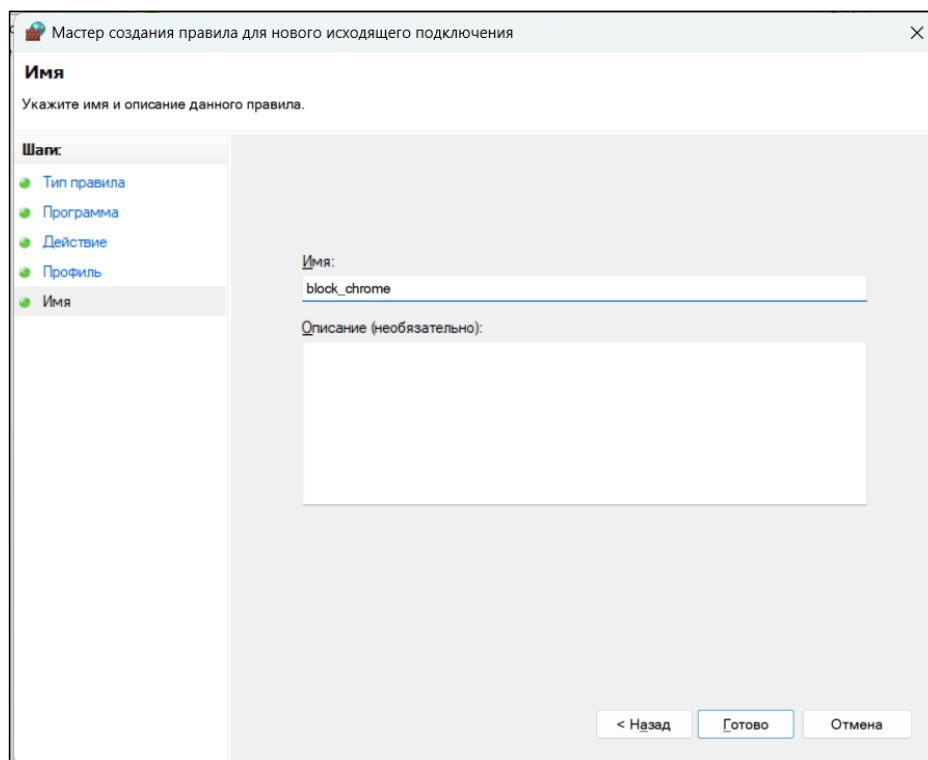


Рисунок 3.6.4 – Окно создания правила – имя

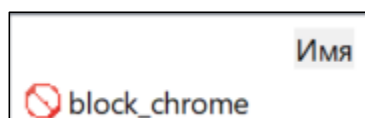


Рисунок 3.6.5 – Созданное новое правило

3.7 Проверим доступ в интернет через заблокированный правилом Google Chrome.

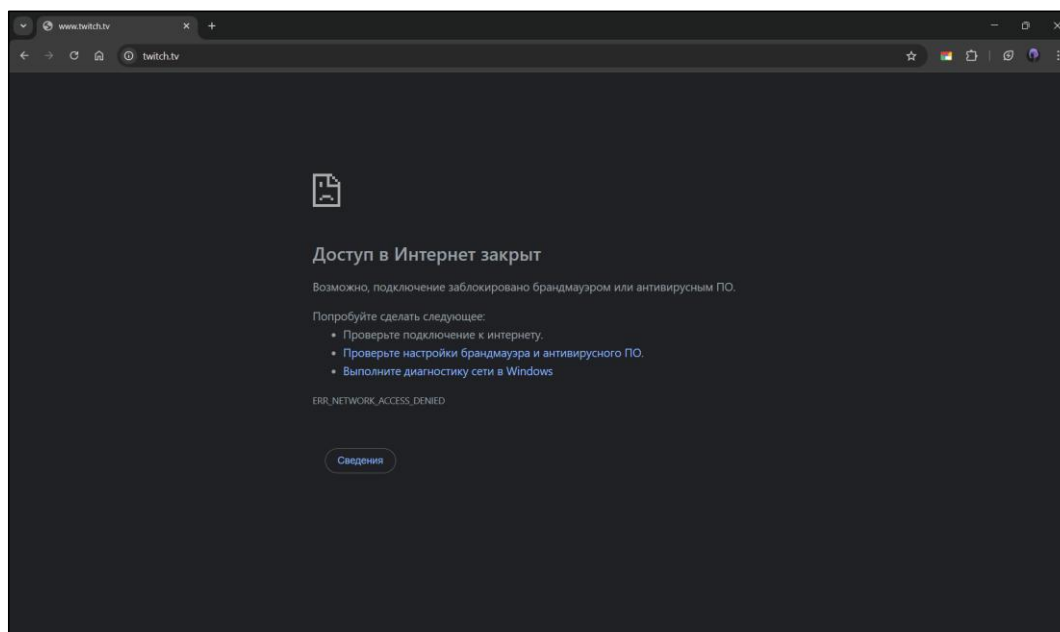


Рисунок 3.7 – Сообщение о заблокированном доступе в интернет

Вывод

У нас получилось настроить реестр, оптимизировать службы и сделать контролируемый доступ к сети брандмауэр. Мы смогли сделать контролируемый доступ к Windows 11.