

## Настройка политики безопасности Windows

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

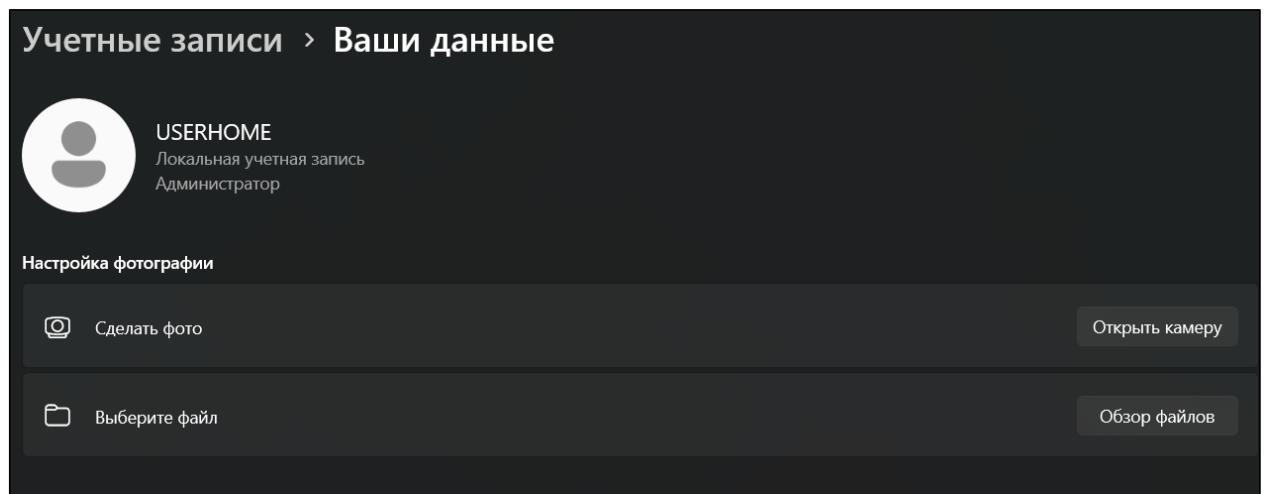
1. Настройка реестра
2. Оптимизация служб Windows
3. Настройка Брандмауэра

Они позволяют 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. Команда в командной строке и реестр Windows представлены на рисунке 1.1.1 и 1.1.2.

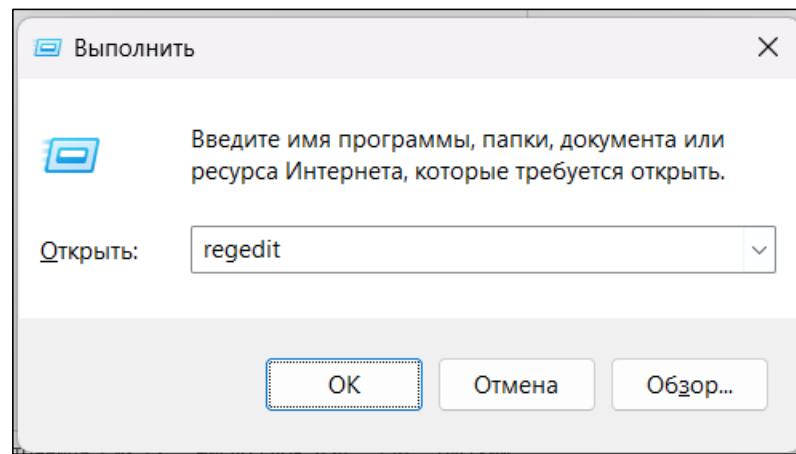


Рисунок 1.1.1 – Ввод команды “regedit”

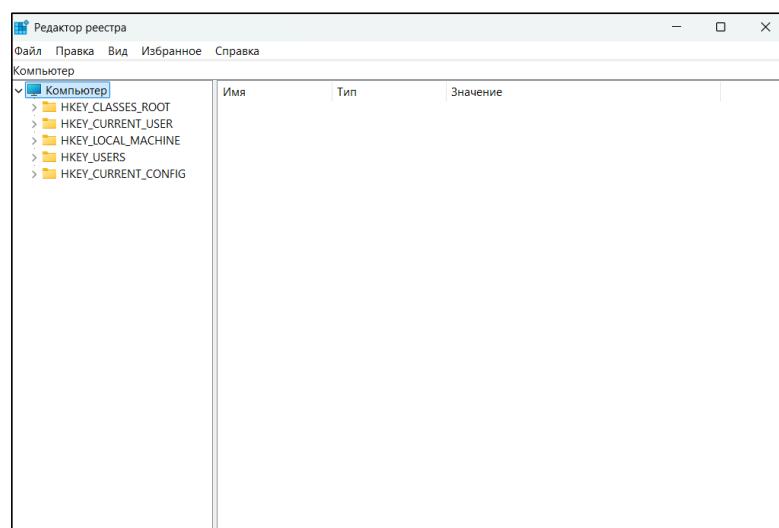


Рисунок 1.1.2 – Реестр Windows

1.2 Создание сохранения файла реестра. Нажать пункт “Файл”, и из выпадающего списка выбрать пункт “Экспорт”. Верхнее меню с выбором сохранения реестре представлено на рисунке 1.2.

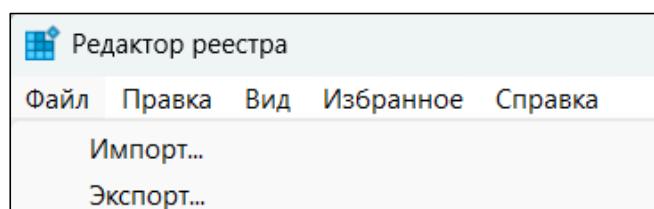


Рисунок 1.2 – Верхнее меню

1.3 Дать название файлу и выбрать путь сохранения. Окно экспорта реестра представлено на рисунке 1.3.

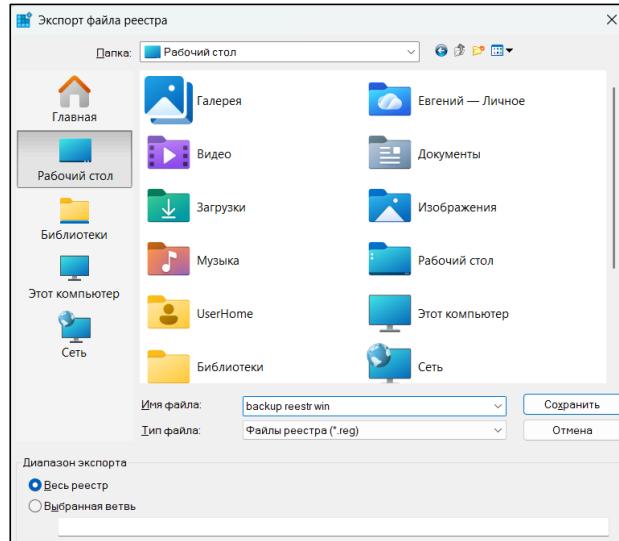


Рисунок 1.3 – Окно экспорта реестра

1.4 Проверить файл экспорта реестра. Файл экспорта реестра представлен на рисунке 1.4.

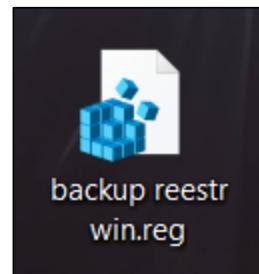


Рисунок 1.4 – Файл экспорта реестра

1.5 Отключение меню “Поделиться” в проводнике”. Перейти к HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions и создать раздел Blocked. Этап создания раздела blocked представлен на рисунке 1.5.

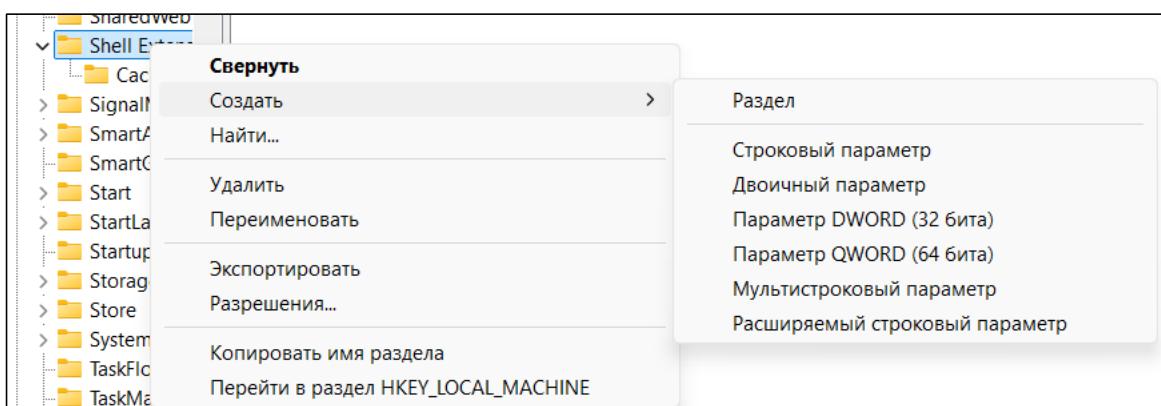


Рисунок 1.5 – Создание раздела blocked

1.6 Создать строковый раздел с именем “{e2bf9676-5f8f-435c-97eb-11607a5bedf7}”. Строковый раздел для блокировки представлен на рисунке 1.6.

Имя	Тип
ab(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”. Заблокированное меню после перезагрузки представлено на рисунке 1.6.

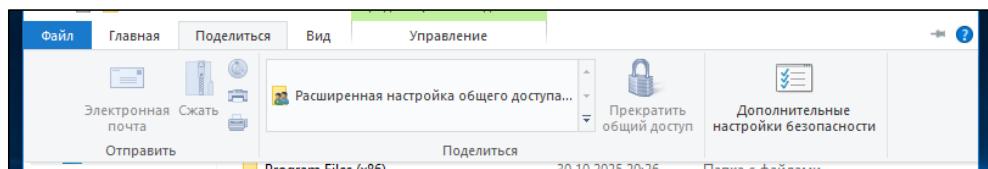


Рисунок 1.6 – Заблокированное меню “поделиться”

## 2 Оптимизация служб Windows.

2.1 Открыть командную строку и ввести команду “services.msc” для открытия служб Windows. Команда для открытия служб Windows и сами службы Windows представлены на рисунках 2.1.1 и 2.1.2.

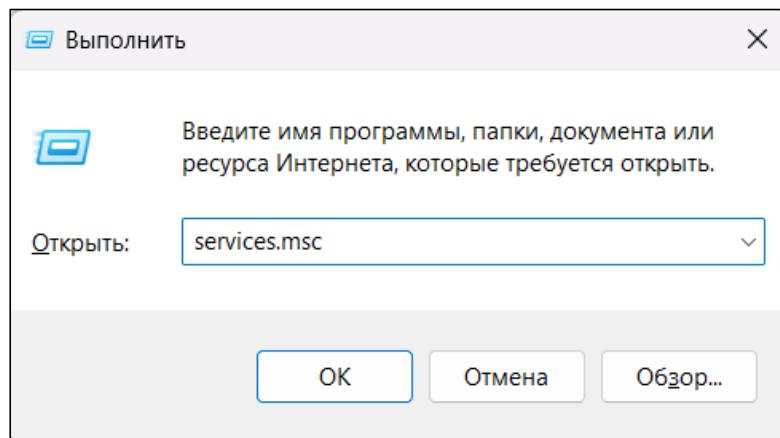


Рисунок 2.1.1 – Командная строка

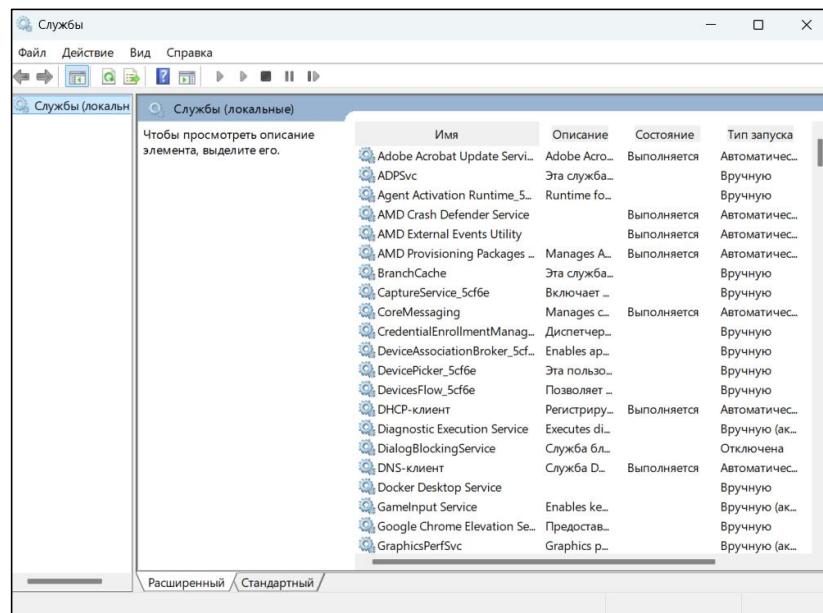


Рисунок 2.1.2 – Службы Windows

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

Перечень служб Windows представлены на рисунке 2.2.

Имя	Описание	Состояние	Тип запуска	Вход от имени
Время в сети мобильной св...	Эта служба...	Вручную (ак...	Локальная слу...	
Вспомогательная служба IP	Обеспечив...	Выполняется	Автоматичес...	Локальная сист...
Вспомогательная служба Z...	Вспомогат...	Вручную	NT AUTHORITY\...	
Встроенный режим	Служба "Вс...	Вручную (ак...	Локальная сист...	
Вторичный вход в систему	Позволяет ...	Вручную	Локальная сист...	
Готовность приложений	Подготовк...	Вручную	Локальная сист...	
Диспетчер автоматических...	Создает по...	Вручную	Локальная сист...	
Диспетчер локальных сеан...	Основная ...	Выполняется	Автоматичес...	Локальная сист...
Диспетчер настройки устр...	Включени...	Вручную (ак...	Локальная сист...	
Диспетчер печати	Запустить	Инвектируетс...	Автоматичес...	Локальная сист...
Диспетчер платеж	Остановить	Инвектируетс...	Вручную (ак...	Локальная слу...
Диспетчер подклы	Приостановить	Инвектируетс...	Автоматичес...	Локальная слу...
Диспетчер подклы	Продолжить	Инвектируетс...	Вручную	Локальная слу...
Диспетчер польз	Перезапустить	Инвектируетс...	Автоматичес...	Локальная слу...
Диспетчер скажан	Все задачи	Инвектируетс...	Вручную	Сетевая служба
Диспетчер учетн	Обновить	Инвектируетс...	Вручную	Локальная слу...
Диспетчер учетн	Свойства	Инвектируетс...	Автоматичес...	Локальная слу...
Доступ к устройст	Справка	Инвектируетс...	Вручную (ак...	Локальная слу...
Журнал событий		Инвектируетс...	Автоматичес...	Локальная слу...
Журналы и опове		Инвектируетс...	Вручную	Локальная слу...
Защита программного обе...	Разрешает ...	Инвектируетс...	Автоматичес...	Сетевая служба

Рисунок 2.2 – Перечень служб

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

Свойства службы Windows представлены на рисунке 2.3.

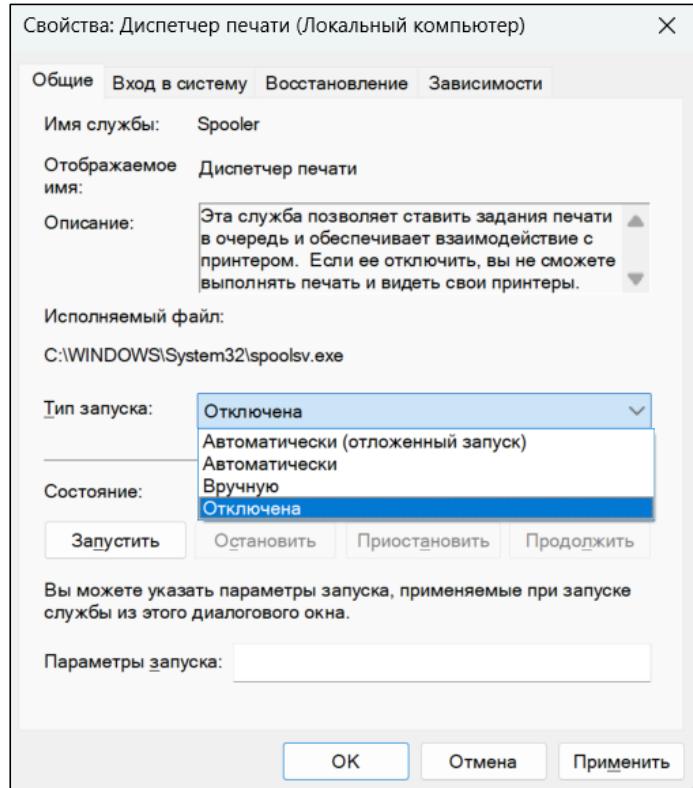


Рисунок 2.3 – Свойства службы

### 3 Настройка Брандмауэра

3.1 Открыть командную строку и ввести команду “firewall.cpl” для открытия Брандмауэра Windows. Команда для командной строки Брендмауэра и сам Брендмауэр Windows представлены на рисунках 3.1.1 и 3.1.2.

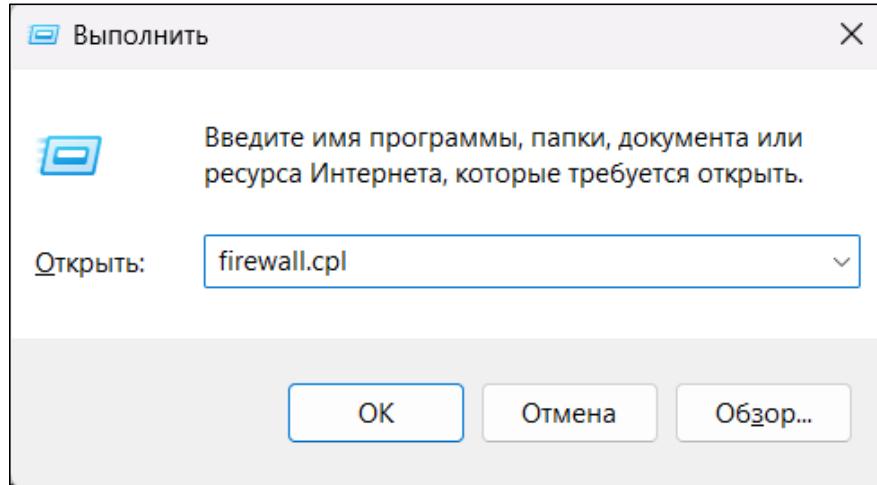


Рисунок 3.1.1 – Командная строка

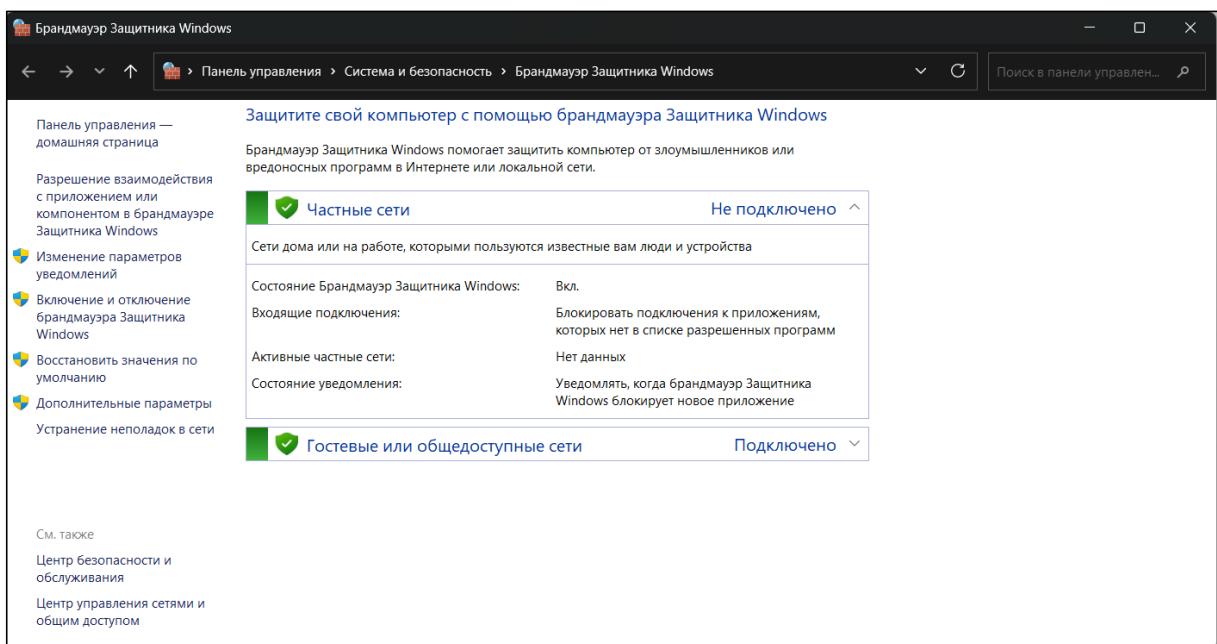


Рисунок 3.1.2 – Брандмауэр Windows

3.2 Разрешить подключение к веб-серверу. Нажать кнопку “Дополнительные параметры”. Кнопка «Дополнительные параметры» представлена на рисунке 3.2.



Рисунок 3.2 – Кнопка “Дополнительные параметры”

3.3 Выбрать пункт “Правила для входящих подключений” и нажать “Создать правило...”. Пункты дополнительных параметров и кнопка для создания правил представлены на рисунках 3.3.1 и 3.3.2.

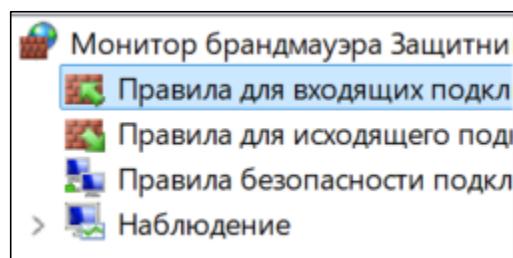


Рисунок 3.3.1 – Пункты дополнительных параметров

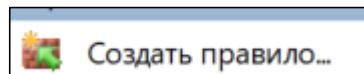


Рисунок 3.3.2 – Кнопка “Создать правило”

3.4 Ввести параметры для правила (порт: 80). Окно для создания типа правила, для указания протокола, для указания действия, для названия правила и окно с созданным правилом представлены на рисунках 3.4.1 – 3.4.5.

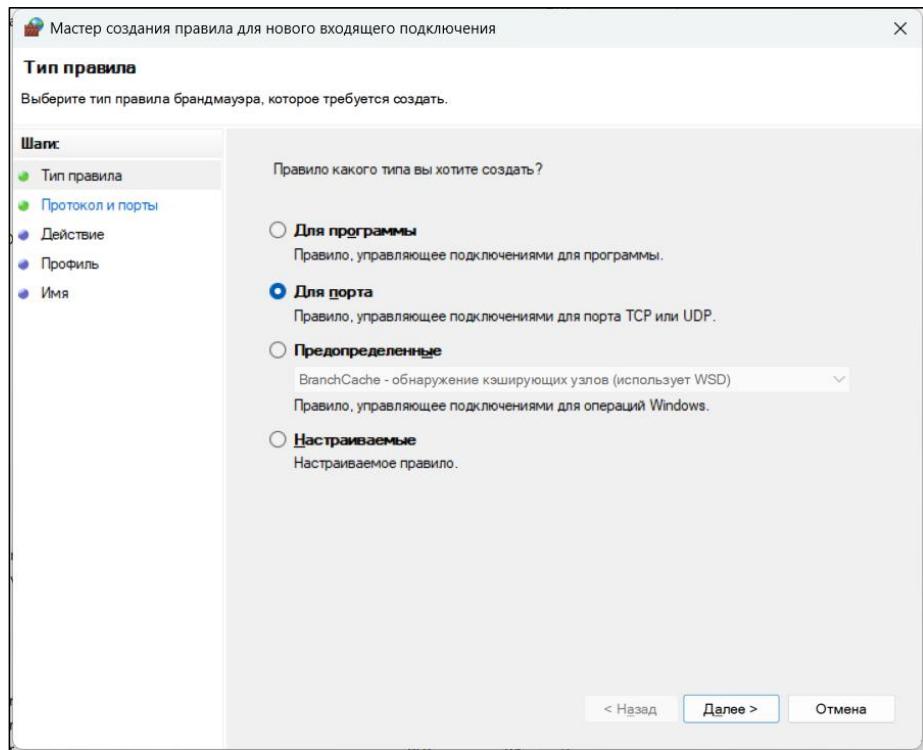


Рисунок 3.4.1 – Окно создания правила – тип правила

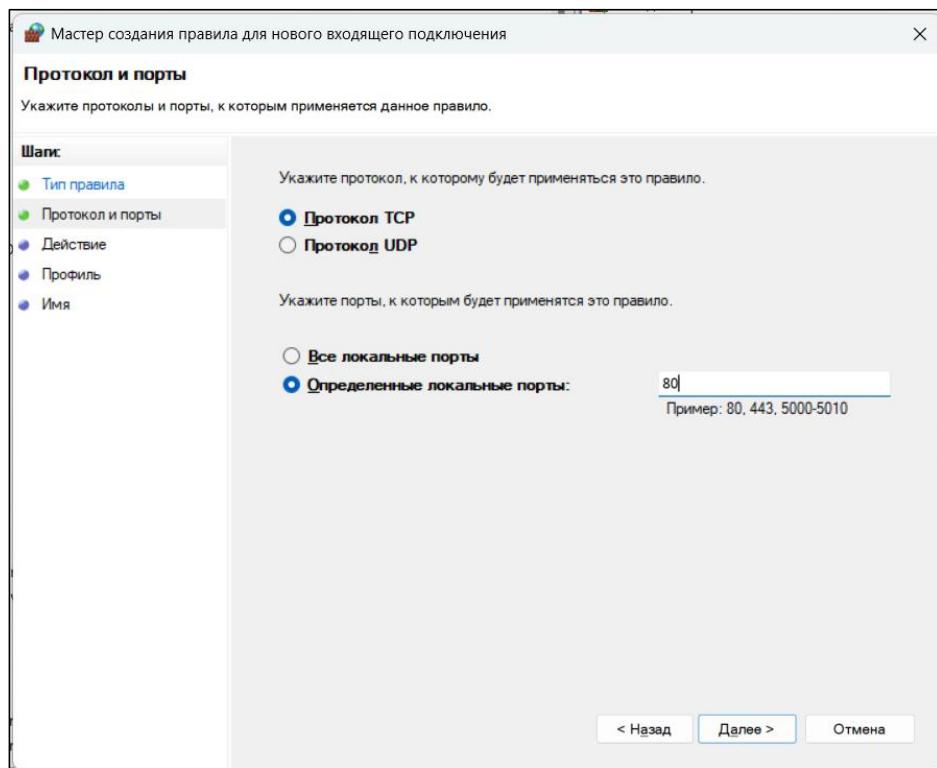


Рисунок 3.4.2 – Окно создания правила – протоколы и порты

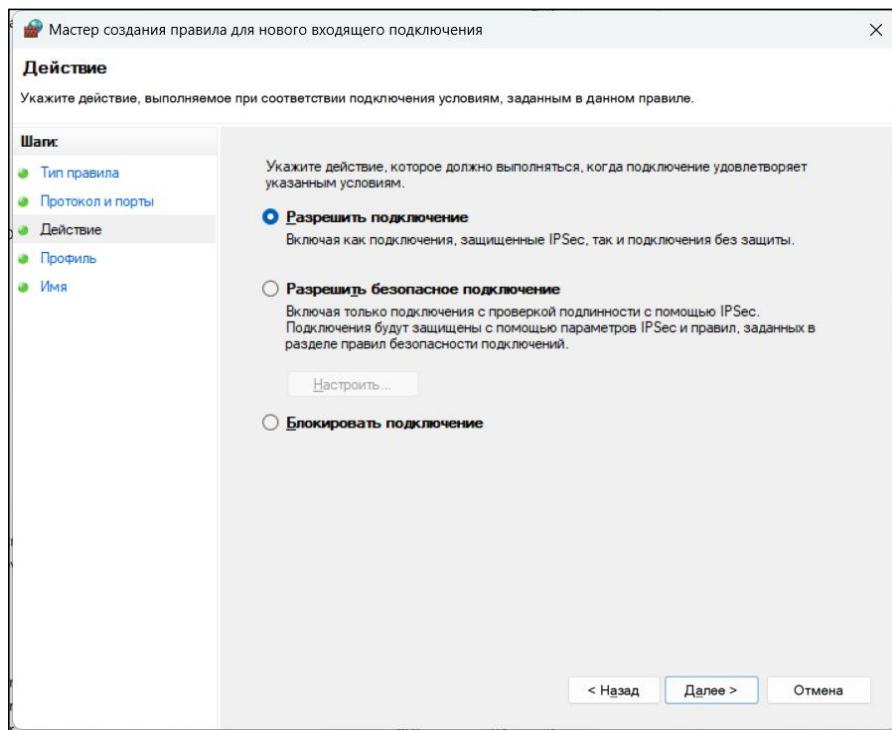


Рисунок 3.4.3 – Окно создания правила – действие

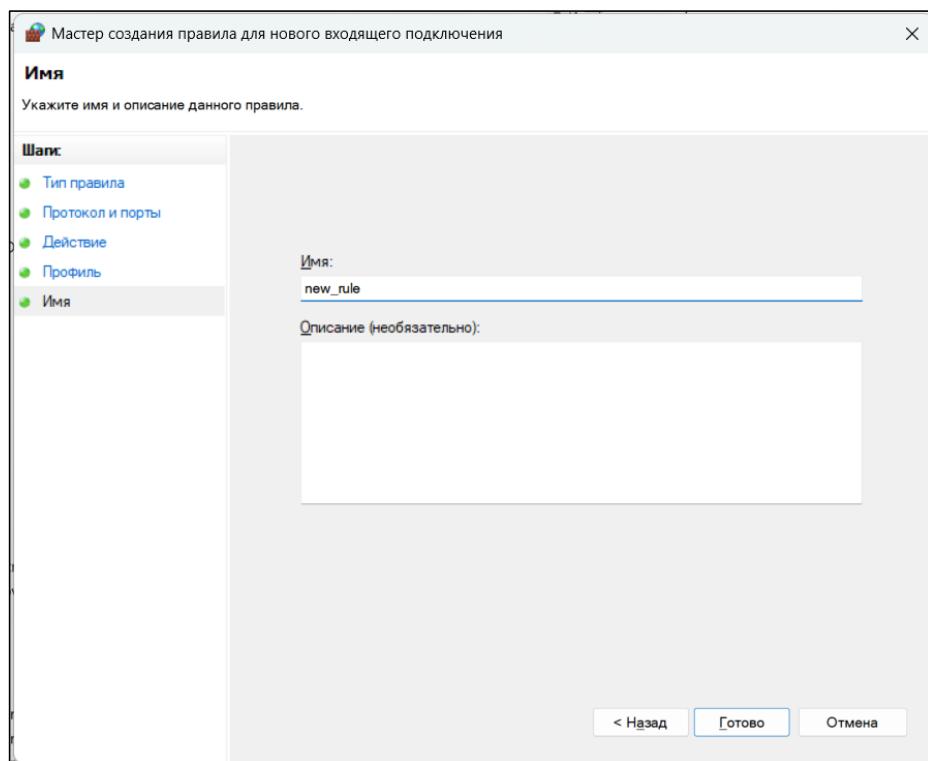


Рисунок 3.4.4 – Окно создания правила – имя

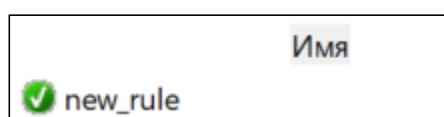


Рисунок 3.4.5 – Созданное новое правило

3.5 Ограничение работы браузера. Выбрать пункт “Правила для исходящего трафика” и нажать кнопку “Создать правило...”. Пункт дополнительных параметров и кнопка для создания правила представлены на рисунках 3.5.1 и 3.5.2.

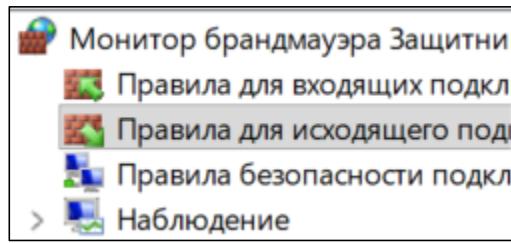


Рисунок 3.5.1 – Пункты дополнительных параметров

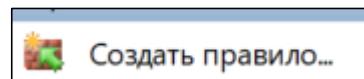


Рисунок 3.5.2 – Кнопка “Создать правило”

3.6 Ввести параметры для правила (путь к браузеру). Okno для создания типа правила, указания пути к программе, для указания действия, для названия правила и с созданным правилом представлены на рисунках 3.6.1 – 3.6.5.

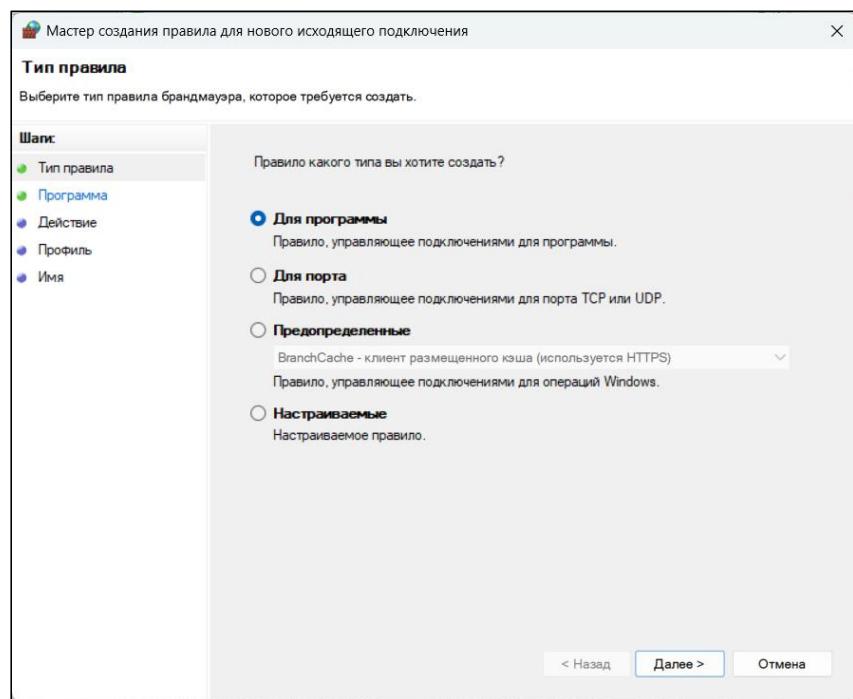


Рисунок 3.6.1 – Окно создания правила – тип программы

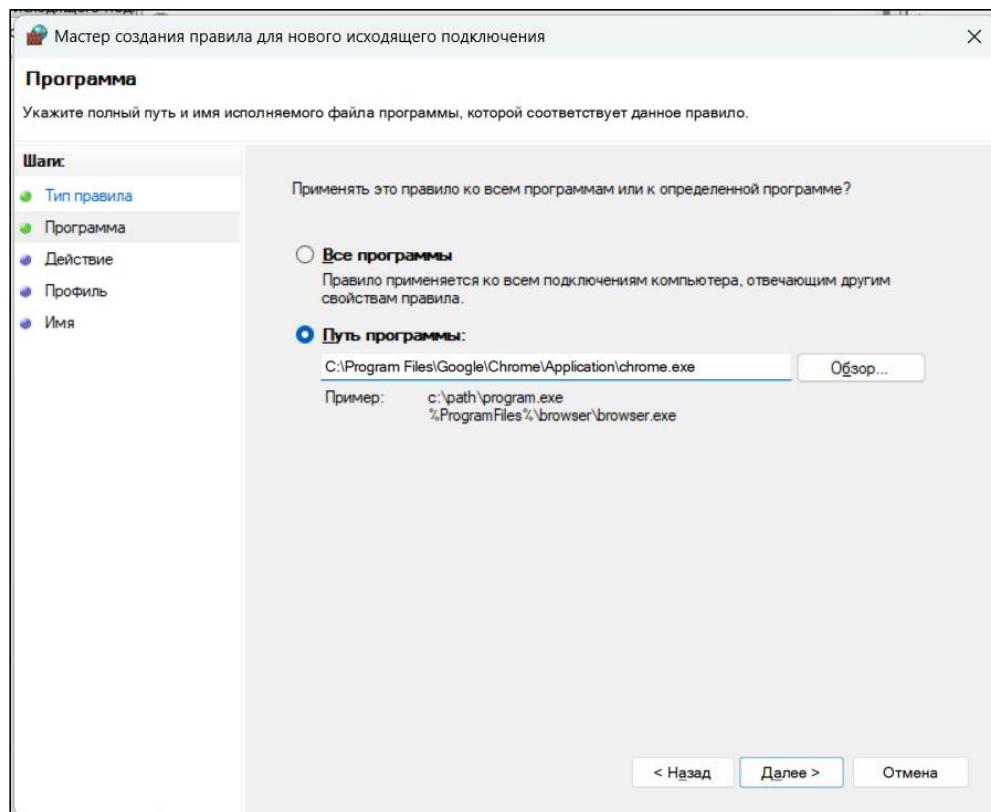


Рисунок 3.6.2 – Окно создания правила – программа

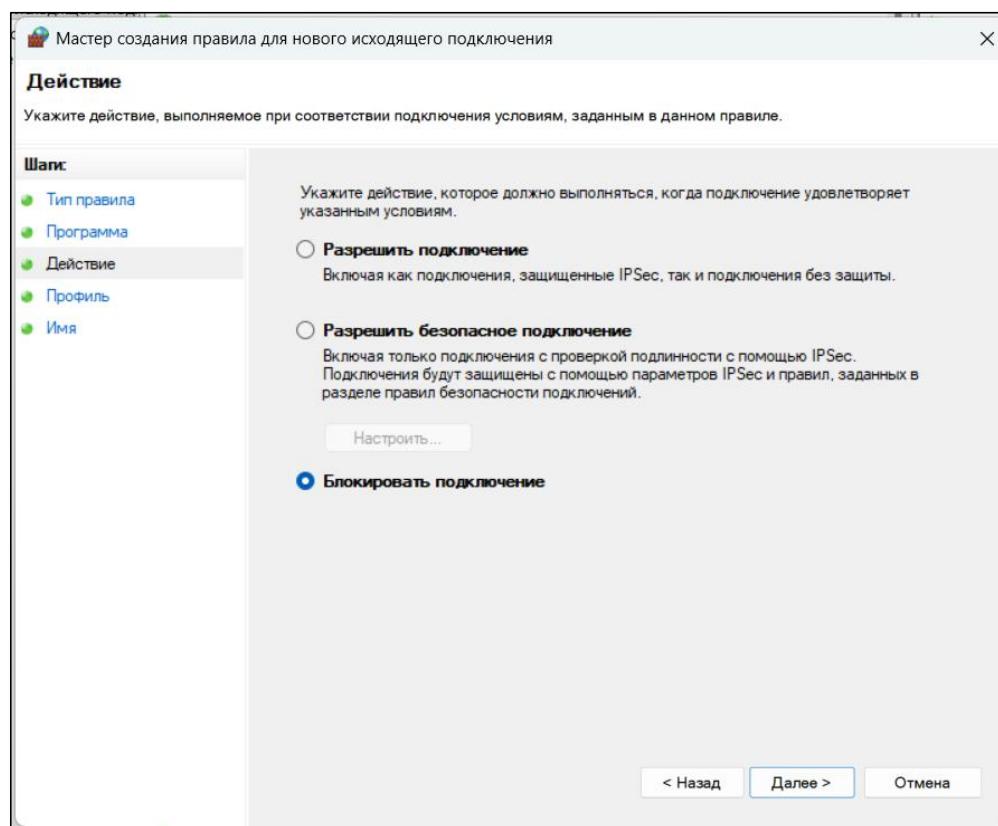


Рисунок 3.6.3 – Окно создания правила – действие

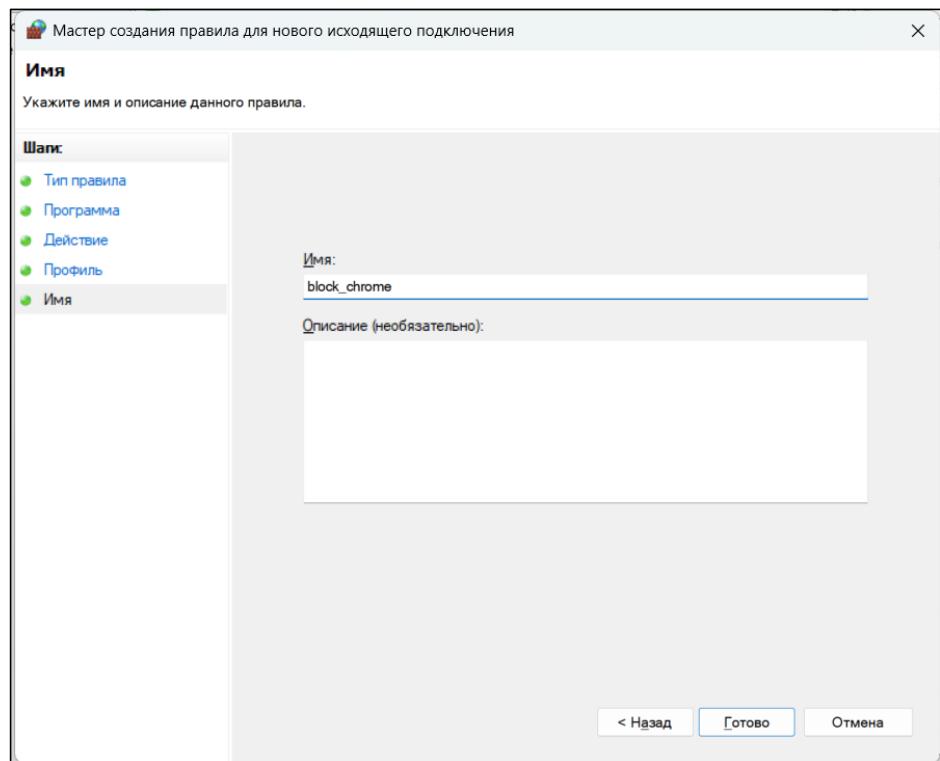


Рисунок 3.6.4 – Окно создания правила – имя

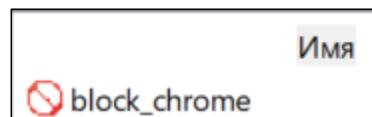
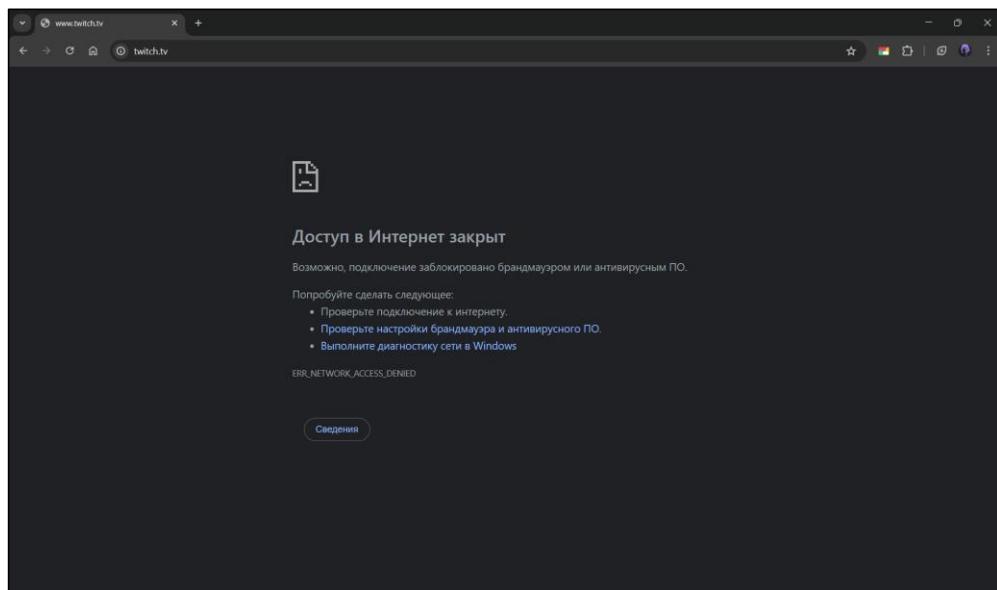


Рисунок 3.6.5 – Созданное новое правило

3.7 Проверим доступ в интернет через заблокированный правилом Google Chrome. Сообщение о блокировке доступа в интернет представлено на рисунке 3.7.



### 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.