

## Настройка безопасности политики Windows

Настройка будет проводиться в Windows 11 будет состоять из 2 пунктов:

1. Настройка редактора локальной групповой политики
2. Настройка Брандмауэра

С их помощью сможем обезопасить систему от неутвержденных действий пользователей или ПО.


Для начало узнаем данные пользователя вводим команду:

```
C:\Users\Пользователь>systeminfo
```

|                              |                                 |
|------------------------------|---------------------------------|
| Имя ОС:                      | Майкрософт Windows 11 Pro       |
| Версия ОС:                   | 10.0.26200 Н/Д построение 26200 |
| Изготовитель ОС:             | Microsoft Corporation           |
| Конфигурация ОС:             | Изолированная рабочая станция   |
| Тип сборки ОС:               | Multiprocessor Free             |
| Зарегистрированный владелец: | Пользователь                    |


## Профиль


### Учетные записи





**МАСТЕР DIPPER**  
kazyhanovdavid@gmail.com  
Администратор


#### Параметры учетной записи


 Ваши данные  
Фотография профиля





 Варианты входа  
Windows Hello, ключ безопасности, пароль, динамическая блокировка



 Связанные устройства  
Находите, восстанавливайте и администрируйте устройства, на которых выполнен вход с помощью учетной записи Майкрософт



 Email & accounts  
Учетные записи, используемые приложениями "Почта", "Календарь" и "Контакты"



1. Настройка редактора локальной групповой политики

Редактор локальной групповой политики — это инструмент для управления настройками ОС, безопасности и пользовательской среды на одном компьютере.

1.1 Открываем редактор через диалоговое окно “Выполнить” вводим команду secpol.msc.

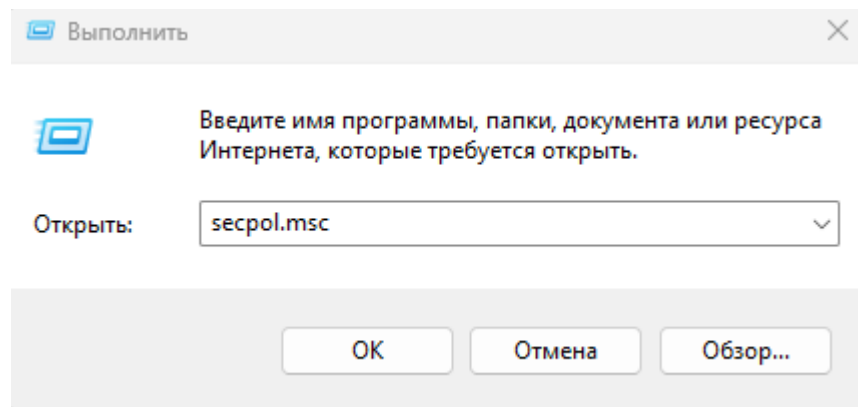


Рисунок 1.1 – Ввод команды “secpol.msc”.

1.2 Далее вкладке действие выбираем “Экспорт политики” на случай непредвиденных обстоятельств.

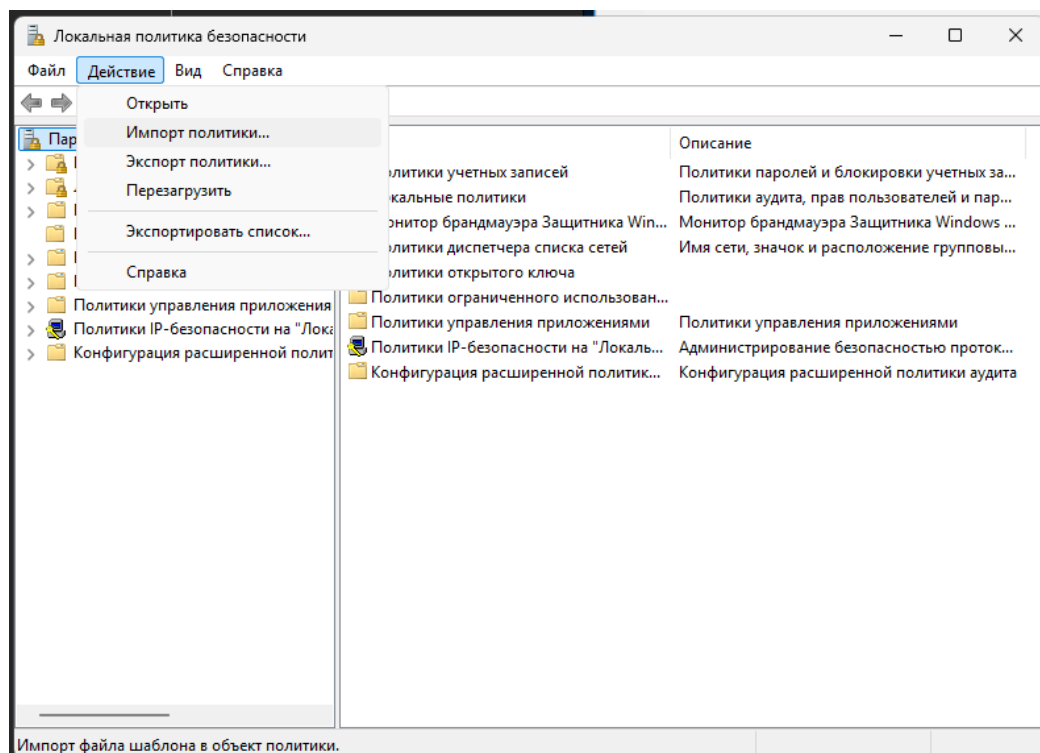


Рисунок 1.2 – Создание файл политики.

1.3 Далее настраиваем политику паролей. Заходим в раздел “политики учетных записей” – “политика паролей”. Изменяем значение параметров

| Политика                                       | Параметр безопасности |
|--|-----------------------|
| Аудит минимальной длины пароля                 | Не определено         |
| Вести журнал паролей                           | 0 сохраненных паролей |
| Максимальный срок действия пароля              | 60 дн.                |
| Минимальная длина пароля                       | 8 зн.                 |
| Минимальный срок действия пароля               | 24 дн.                |
| Ослабить ограничение минимальной длины пароля  | Не определено         |
| Пароль должен отвечать требованиям сложности   | Отключен              |
| Хранить пароли, используя обратимое шифрование | Отключен              |

Рисунок 1.3.1 – Создание файл политики.

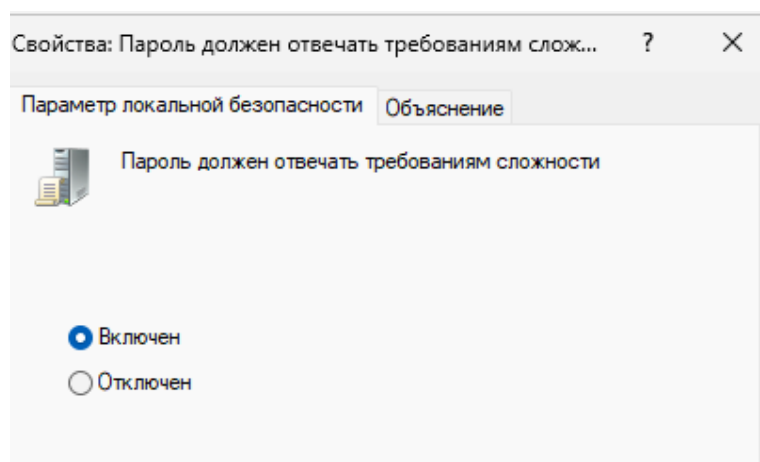


Рисунок 1.3.2 – включаем “Пароль должен отвечать требованиям сложности

1.4 Далее настраиваем политика блокировки учетной записей пользователей. Заходим в раздел “политики учетных записей” – “политика паролей”.

| Политика   | Параметр безопасности     |
|--|---------------------------|
| Время до сброса счетчика блокировки                | 5 мин.                    |
| Пороговое значение блокировки                      | 5 ошибок входа в систе... |
| Продолжительность блокировки учетной записи        | 5 мин.                    |
| Разрешить блокировку учетной записи администратора | Включен                   |

Рисунок 1.4 – Изменение значение параметров

1.5 Далее настраиваем политика аудита. Заходим в раздел “Локальные политики” – “Политика аудита”. Ставим галочки в 2 параметрах на Успех и Отказ.

| Политика                           | Параметр безопасности |
|------------------------------------|-----------------------|
| Аудит входа в систему              | Успех, Отказ          |
| Аудит доступа к объектам           | Нет аудита            |
| Аудит доступа к службе каталогов   | Нет аудита            |
| Аудит изменения политики           | Успех, Отказ          |
| Аудит использования привилегий     | Нет аудита            |
| Аудит отслеживания процессов       | Нет аудита            |
| Аудит системных событий            | Нет аудита            |
| Аудит событий входа в систему      | Нет аудита            |
| Аудит управления учетными записями | Нет аудита            |

Рисунок 1.5 – Изменение значение параметров

1.6 Создадим новую учетную запись для тестов назовем его

“Лемингтон”.

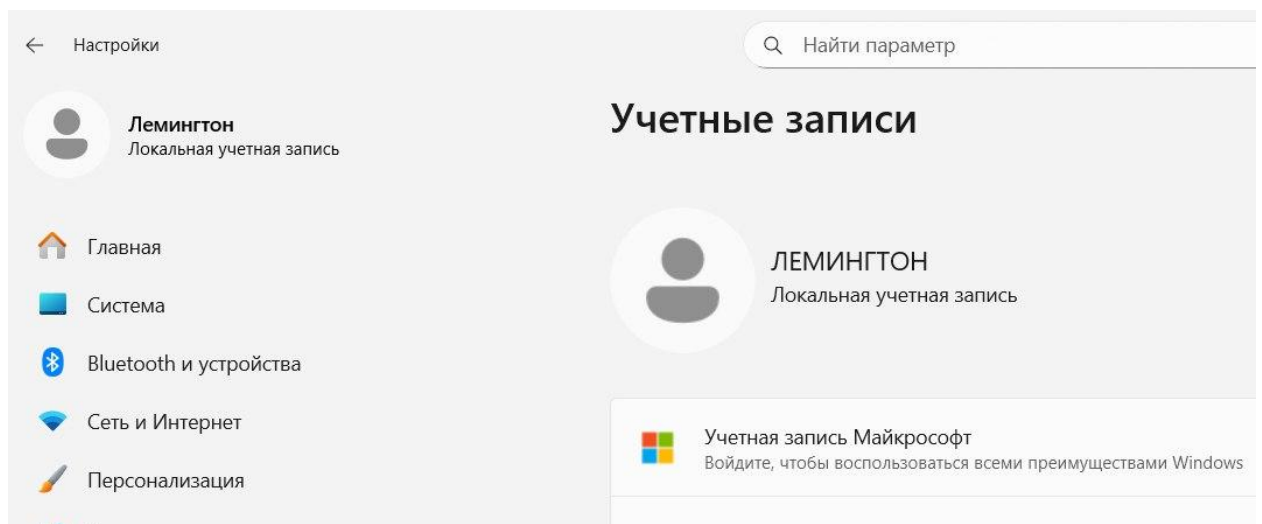
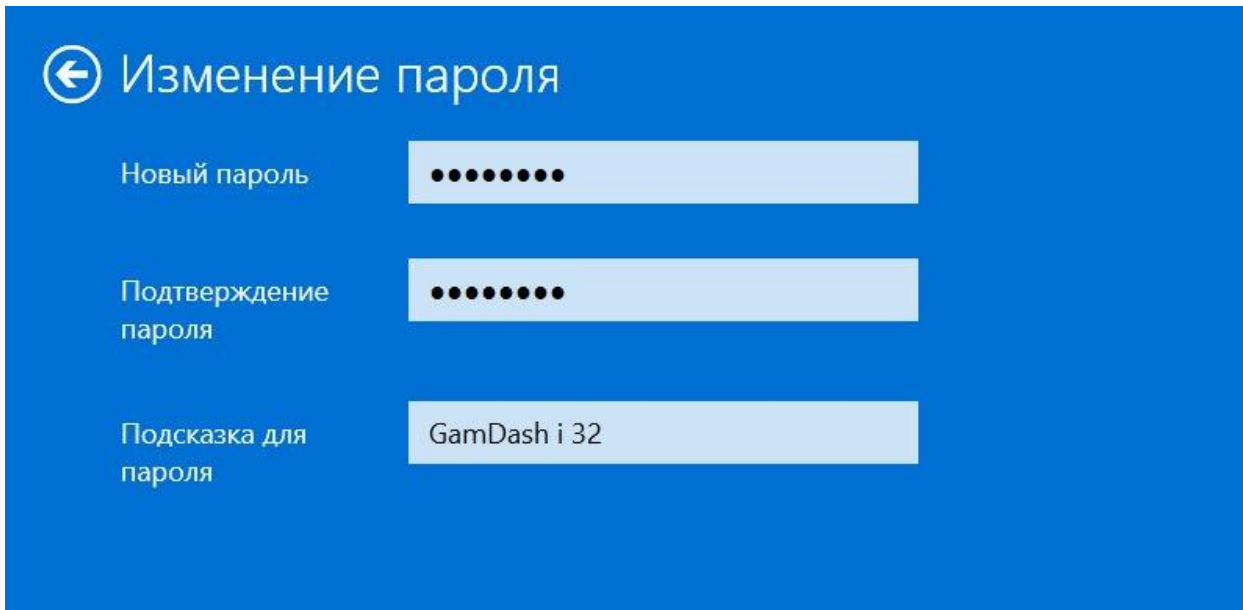


Рисунок 1.6 – Учетная запись

## 1.7 Проверим сработало ли политика



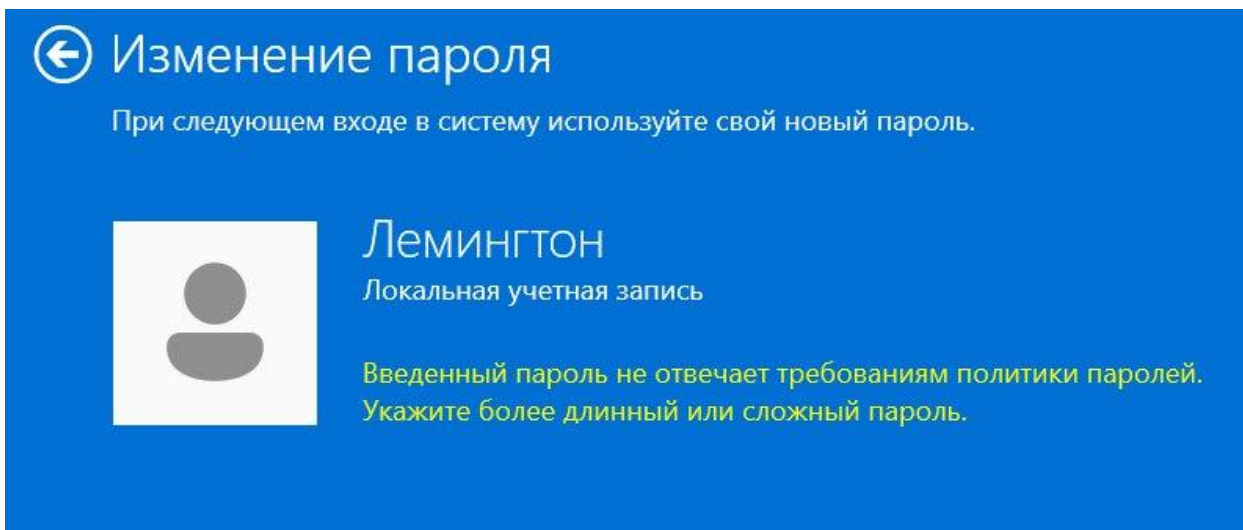
← Изменение пароля

Новый пароль

Подтверждение пароля


Подсказка для пароля GamDash i 32

Рисунок 1.7.1 – Изменение пароля



← Изменение пароля

При следующем входе в систему используйте свой новый пароль.

 Лемингтон  
Локальная учетная запись

Введенный пароль не отвечает требованиям политики паролей.  
Укажите более длинный или сложный пароль.

Рисунок 1.7.2 – Результат

## 2 Настройка Брандмауэра

Брандмауэр — это система, которая выступает в роли барьера между двумя сетями для защиты от угроз.

2.1 Открываем брандмауэр через диалоговое окно “Выполнить” вводим команду firewall.cpl

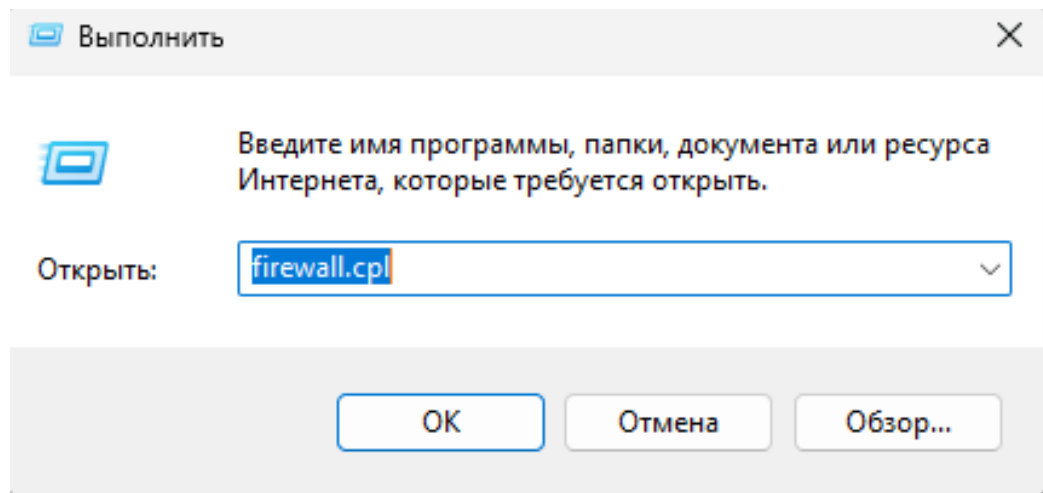


Рисунок 2.1.1 – Ввод команды “firewall.cpl”.

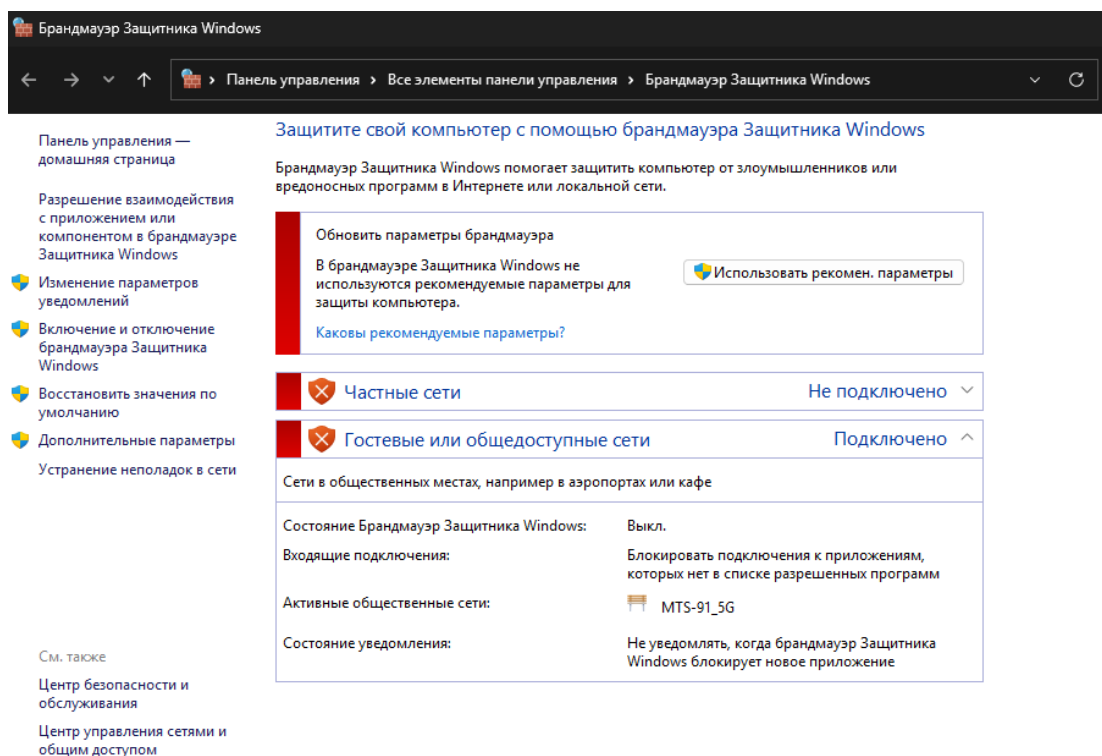




Рисунок 2.1.2 – Брандмауэр.

2.2 Перейдем в раздел “Изменение параметров уведомлений”.  
Выставляем ползунки “Включить брандмауэр Защитника Windows” для его работы.

#### Настройка параметров для каждого типа сети

Вы можете изменить параметры брандмауэра для каждого из используемых типов сетей.

##### Параметры для частной сети

-  ☒ Включить брандмауэр Защитника Windows
- ☐ Блокировать все входящие подключения, в том числе для приложений, указанных в списке разрешенных программ
- ☐ Уведомлять, когда брандмауэр Защитника Windows блокирует новое приложение
-  ☐ Отключить брандмауэр Защитника Windows (не рекомендуется)

##### Параметры для общественной сети



-  ☒ Включить брандмауэр Защитника Windows
- ☐ Блокировать все входящие подключения, в том числе для приложений, указанных в списке разрешенных программ
- ☐ Уведомлять, когда брандмауэр Защитника Windows блокирует новое приложение
-  ☐ Отключить брандмауэр Защитника Windows (не рекомендуется)

Рисунок 2.2.1 – Включение брандмауэра.

2.3 Перейдем в раздел “Дополнительные параметры”.

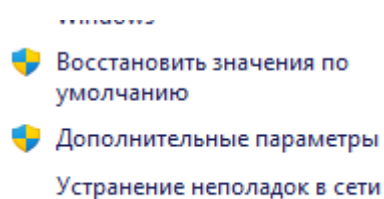


Рисунок 2.3 – Дополнительные параметры.

2.4 Выбираем пункт “Правило для исходящего подключения” и справа нажимаем на создать правило.

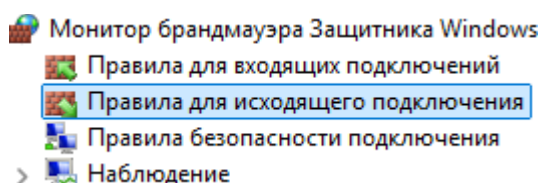


Рисунок 2.4.1 – Правило для исходящего подключения.

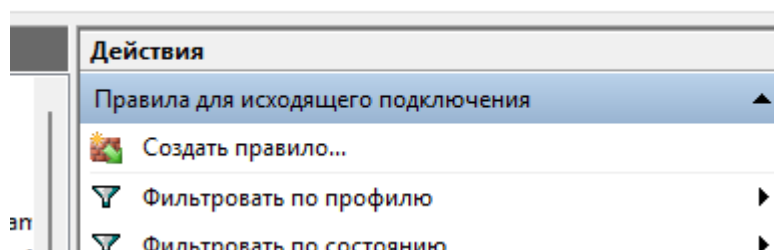


Рисунок 2.4.2 – Создать правило.

2.5 Выбираем ползунок для “для программы” и вписываем путь до приложения “Chrome” далее выбираем “Блокировать подключение”. Назовем его “Блок браузер”.

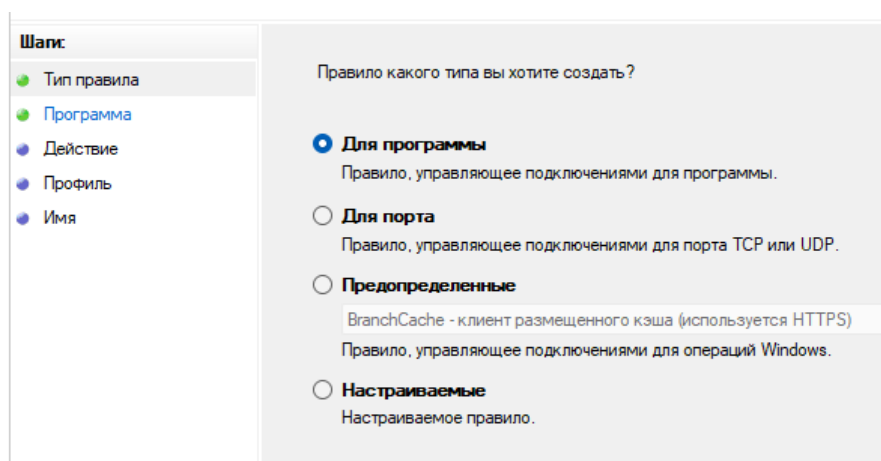


Рисунок 2.5.1 – Окно тип правил.

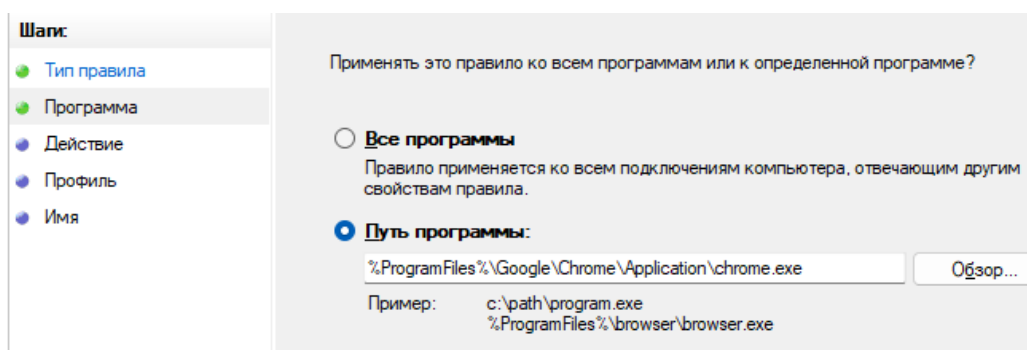


Рисунок 2.5.2 – Окно для программы.



**Шаги:**

- Тип правила
- Протокол и порты
- Действие**
- Профиль
- Имя

Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.

☐ **Разрешить подключение**  
Включая как подключения, защищенные IPSec, так и подключения без защиты.

☐ **Разрешить безопасное подключение**  
Включая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений.

☒ **Блокировать подключение**

Рисунок 2.5.3 – Окно действие.

**Имя:**

**Описание (необязательно):**

Рисунок 2.5.4 – Называем правило.

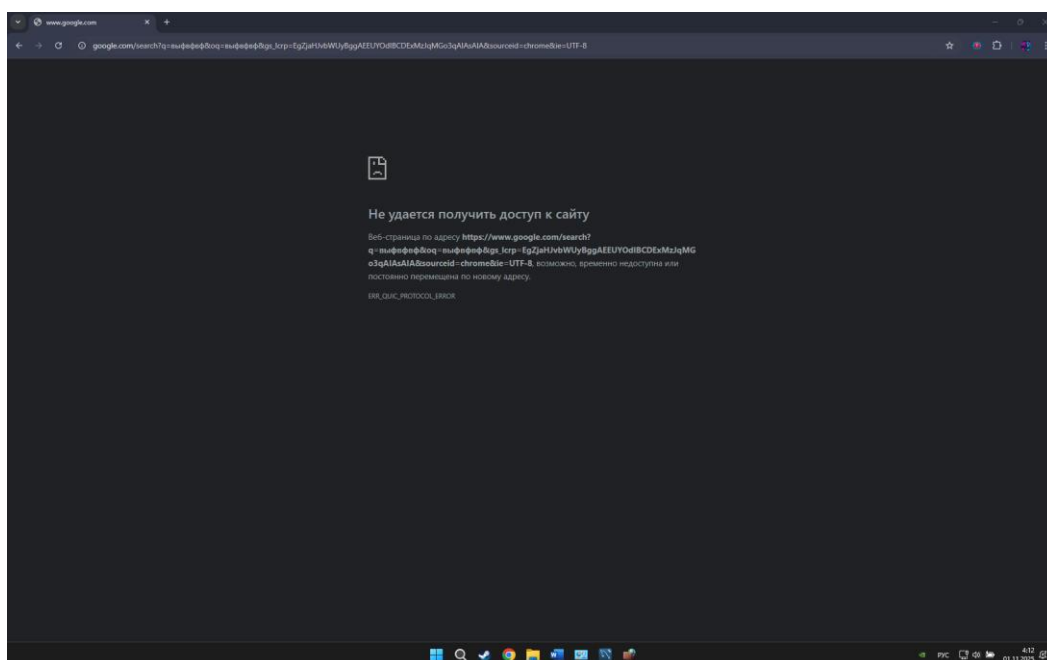


Рисунок 2.5.5 – Результат применения правила.