**Липецкий государственный технический университет**

Университетский колледж

Кафедра автоматизированных систем управления

Лабораторная работа №7

по «Защита информации»

Настройка сетевого экрана

Студент Щеглов Д.A

Группа T-ИС-20

Руководитель Седых Ю.И

Липецк 2022г.

Оглавление

[Цель работы 3](#_Toc98706477)

[Задание 4](#_Toc98706478)

# **Цель работы**

Изучение понятия сетевого экрана. Получение практических навыков по включению и настройке системного сетевого экрана

# **Задание**

1. Откройте Брандмаузер Windows в Панели управления и выберите Дополнительные параметры.

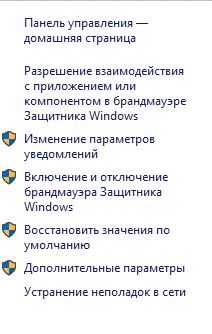


Рис 1.

1. Выберите пункт Свойства на панели справа.

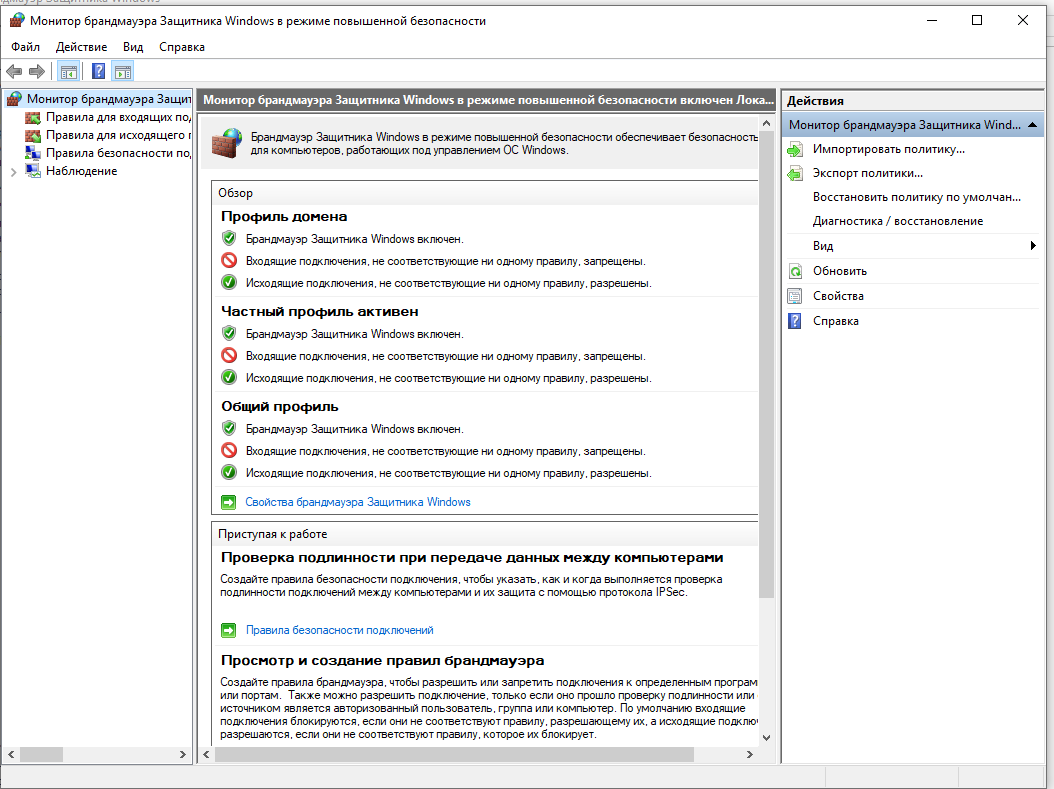


Рис 2.

1. Выберите пункт Настроить в разделе Ведение журнала (возможно настроить для различных профилей).

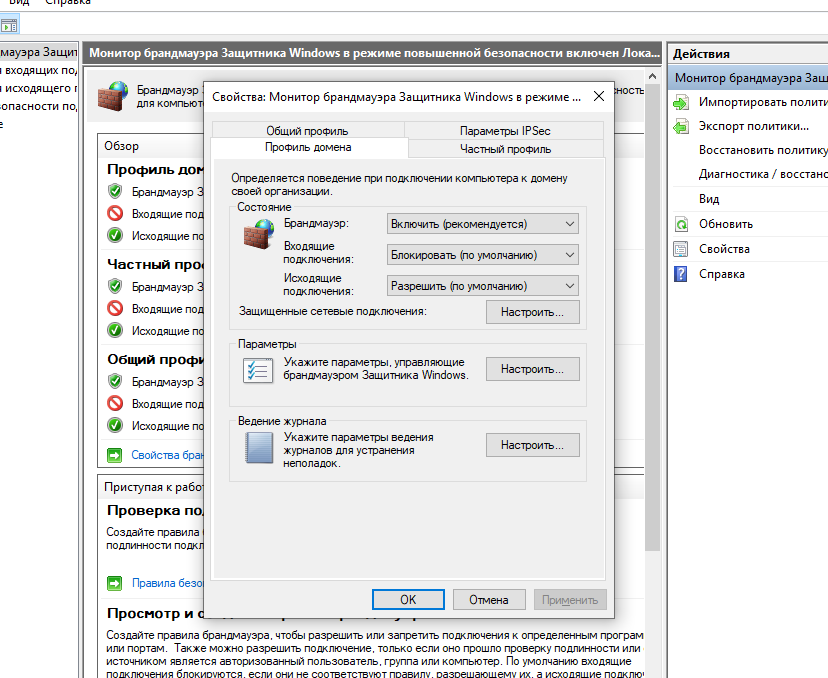


Рис.3

1. Выберите необходимые параметры, а так же ознакомьтесь со справкой, щелкнув Дополнительные сведения о ведении журналов.

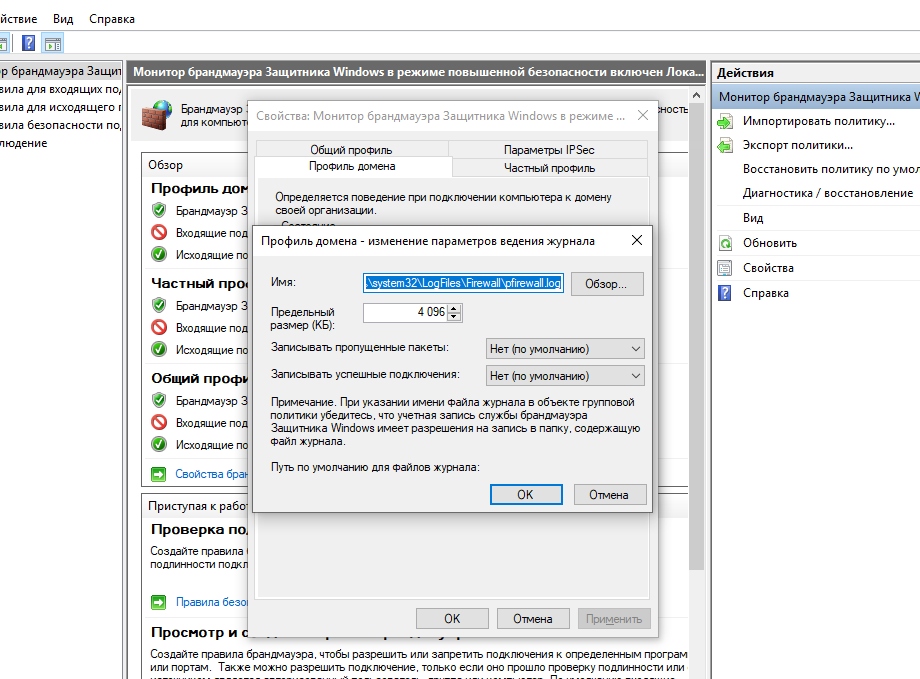


Рис. 4

1. Просмотр журнала событий

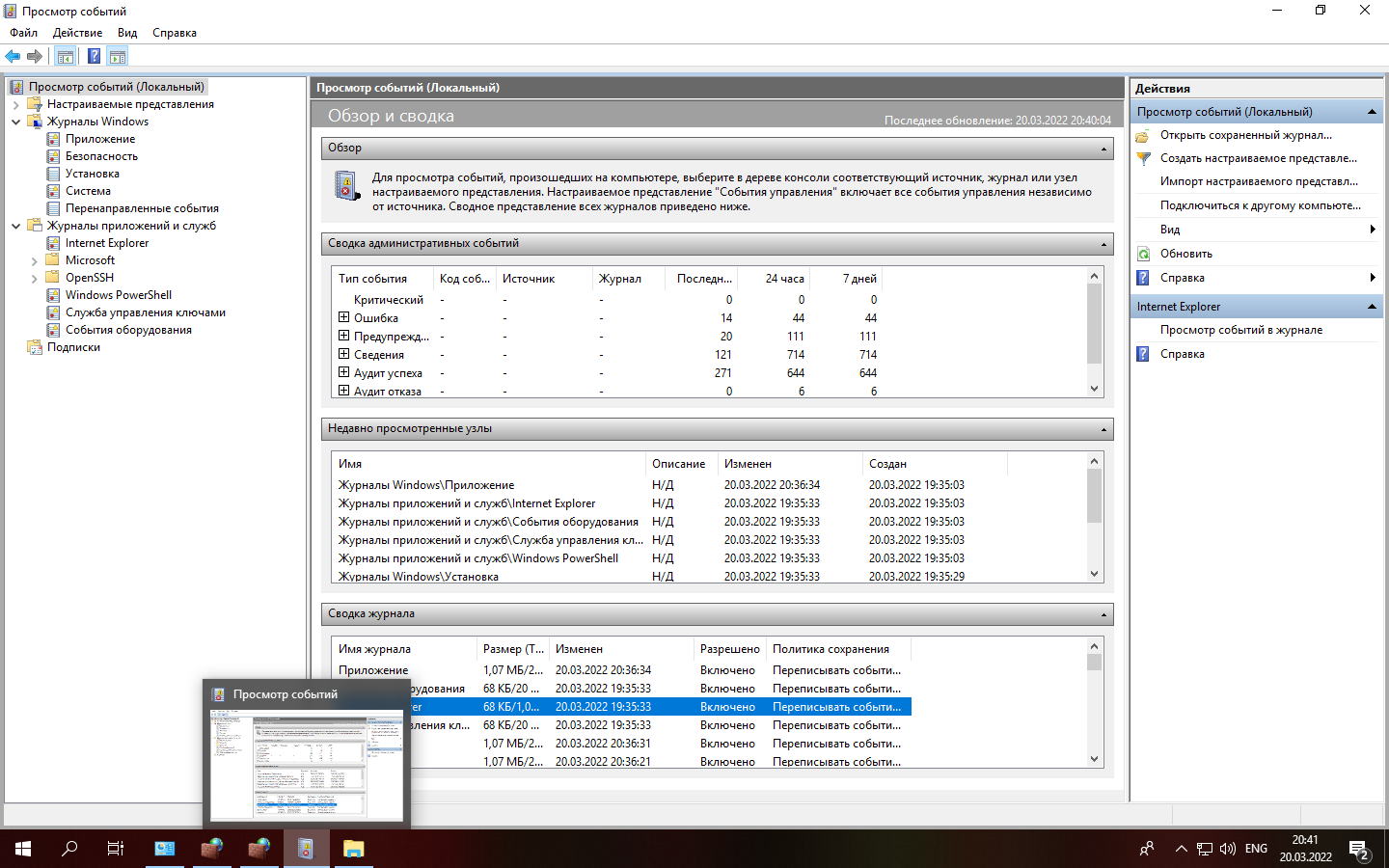


Рис. 5

Включение службы Telnet

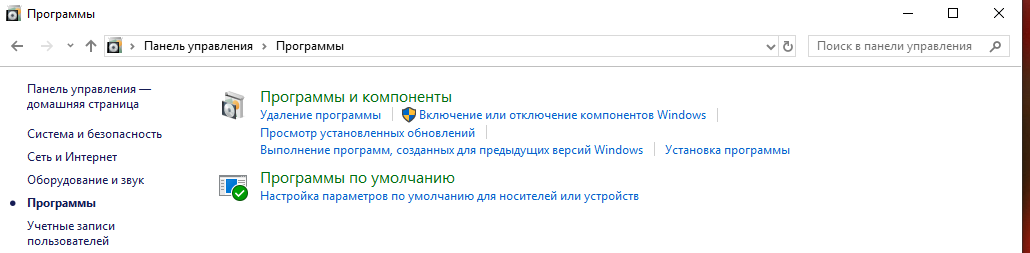


Рис 6.

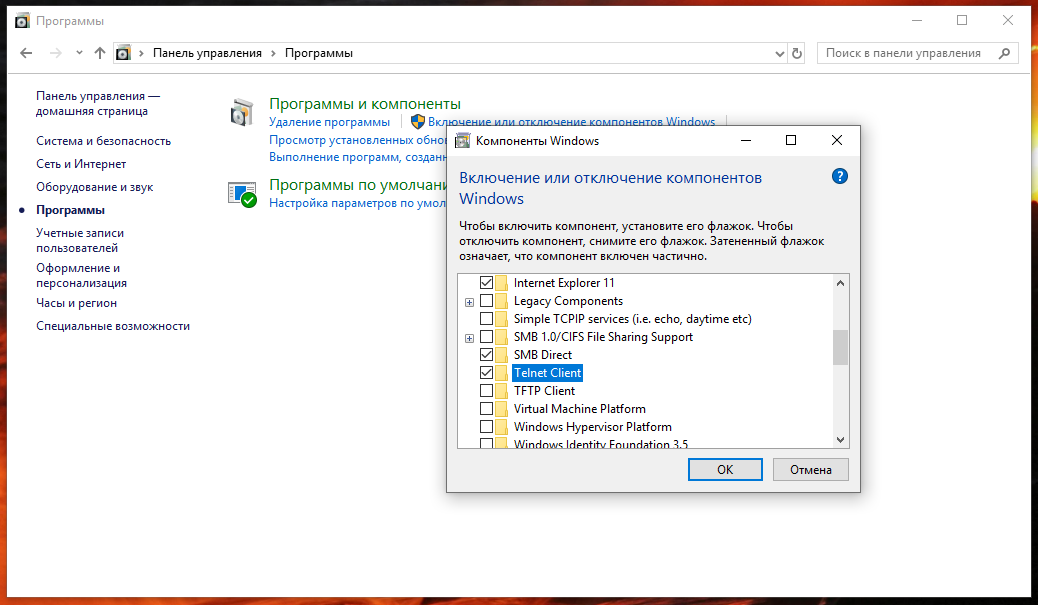


Рис 7.

Выключение брандмауэра на компьютере 2

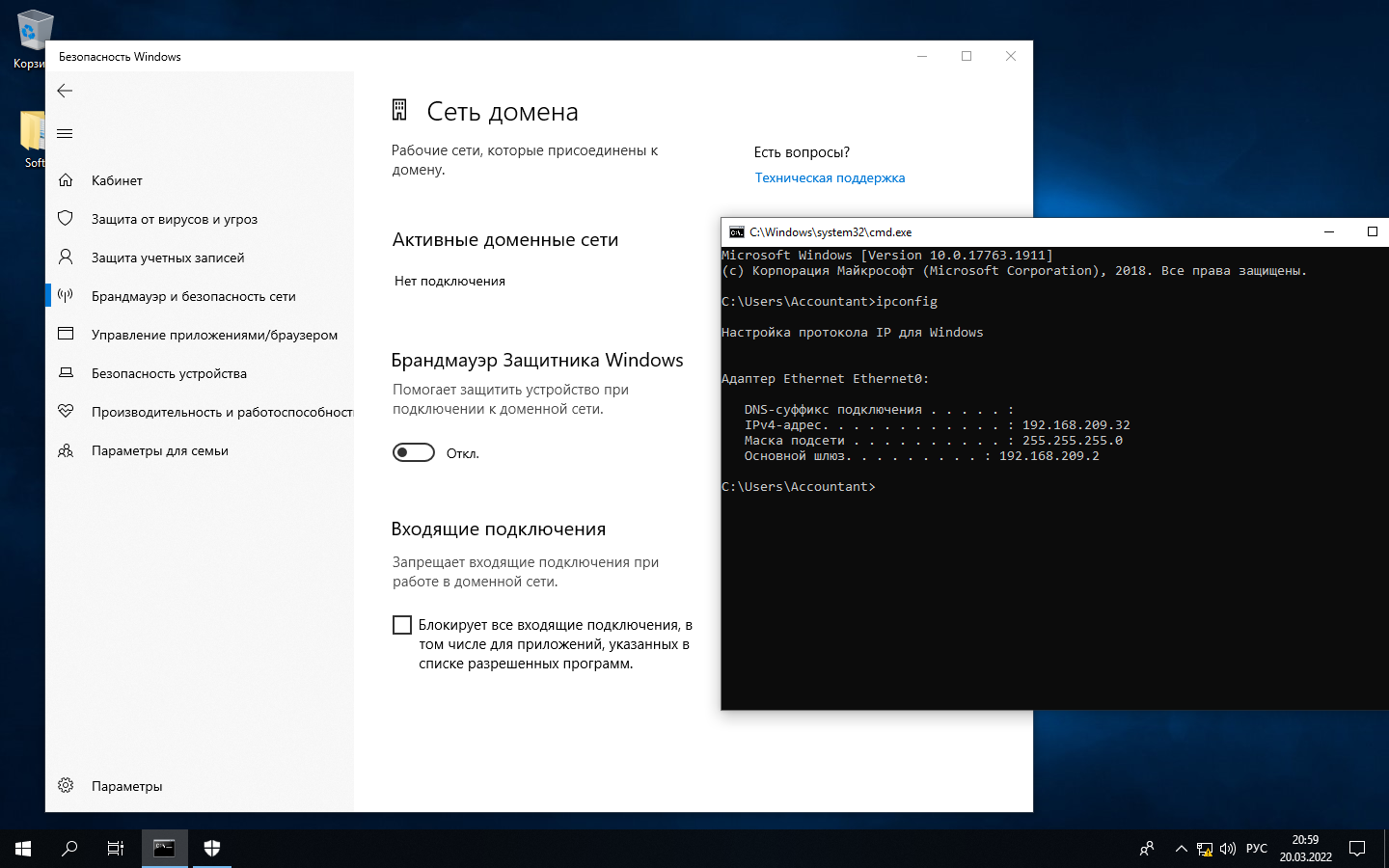


Рис. 7

Включение параметра "Брандмауэр Windows: Задать исключения для портов”

1. Оказавшись в окне монитора Защитника Windows, смещаемся к левому краю и нажимаем на кнопку «Создать правило».
2. Тип правила — В первом пункте отмечаем «Для порта».

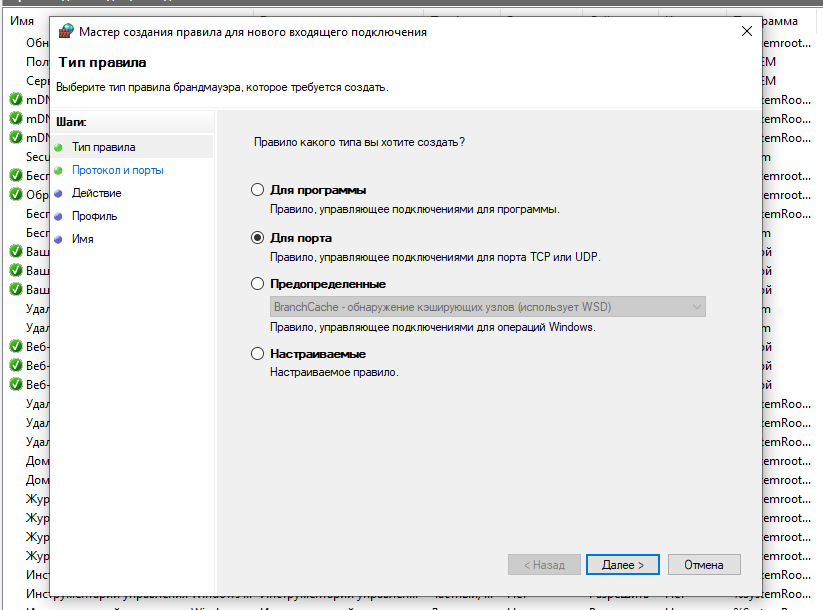


Рис 8.

1. Протокол и порты — Отметив «Протокол TCP», чуть ниже указываем необходимый порт или порты, через запятую или указав определенный диапазон через дефис (Пример: 30583-31700).Обычно, для игр или программ работающих в сети достаточно именно этого протокола, но в некоторых случаях может понадобиться открыть те же порты по протоколу UDP.В таком случае Вам придется создать ещё одно, такое же правило выбрав в этот раз именно UDP. Но, как показывает практика, если пользователь задался вопросом по добавлению портов в исключение брандмауэра, то скорей всего вся необходимая информация по портам и в каких протоколах они используются, уже известна.

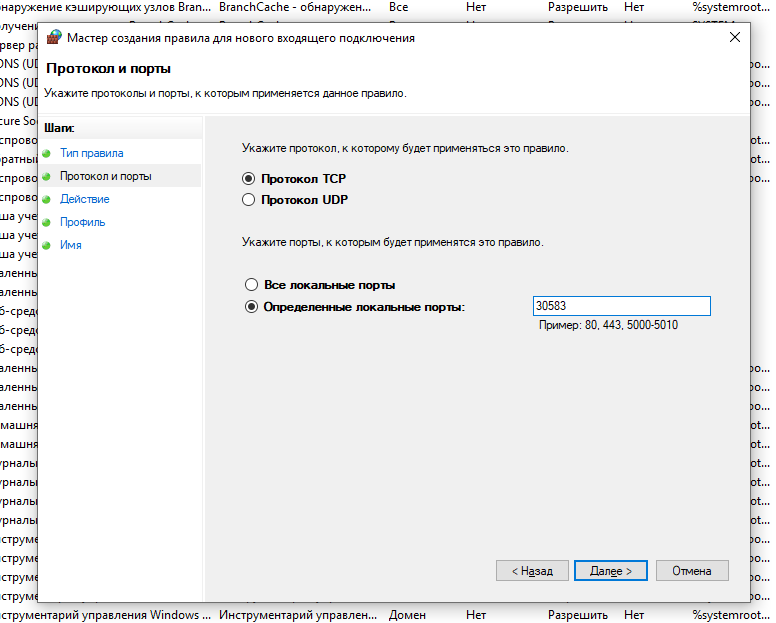


Рис 9.

1. Действие — В следующем шаге отмечаем пункт «Разрешить подключение».

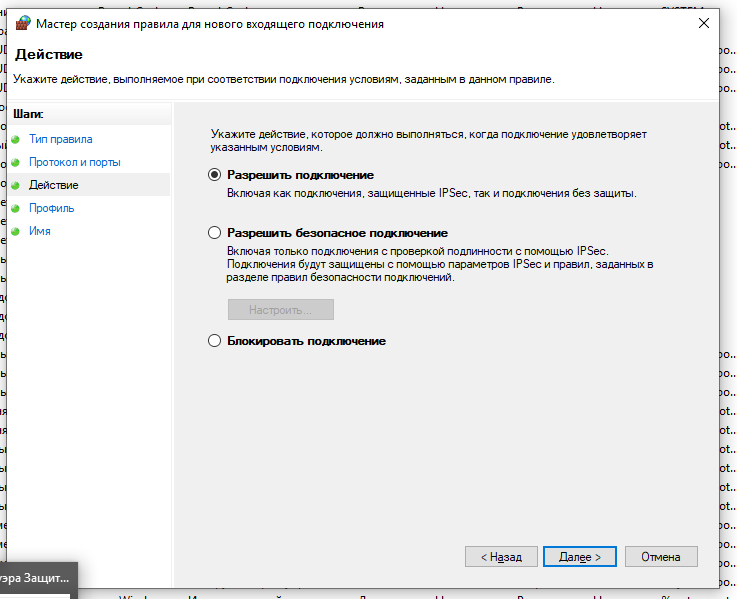


Рис 10.

1. Профиль — Применяем правило ко всем сетевым профилям.

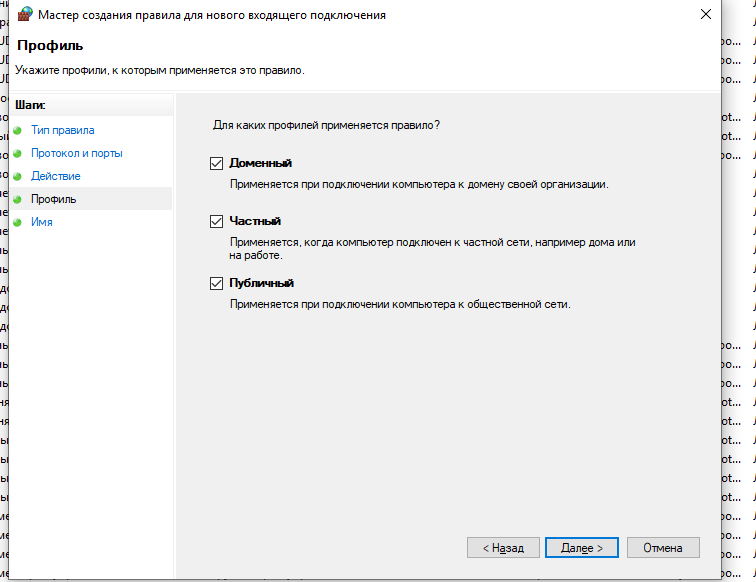


Рис 11.

1. Имя — Вводим отображаемое имя созданного правила. Для ясности, что это за порт и зачем его открыли, можно добавить описание.

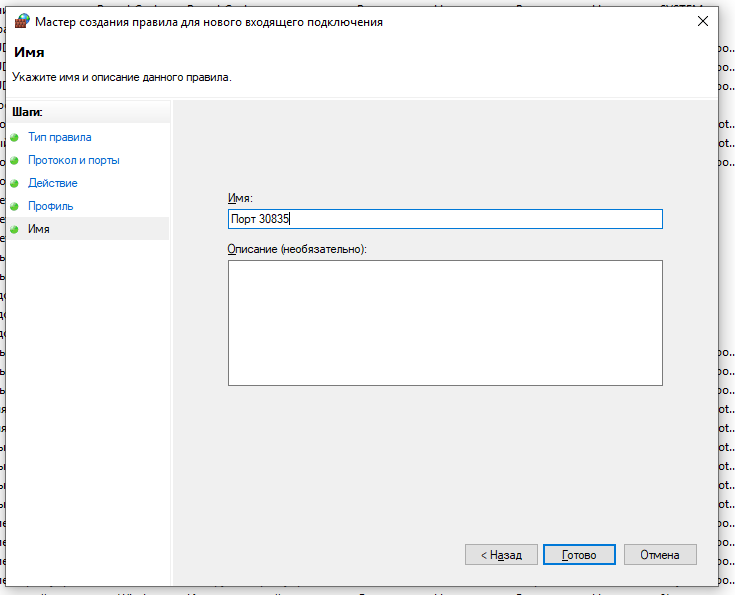


Рис 12.

1. Нажатие кнопки «Готово» – это завершающий этап открытия порта в брандмауэре.

Подключение к другому компьютеру по telnet на порту 30583. Для подключения используем команду **telnet 192.168.209 27 30583**

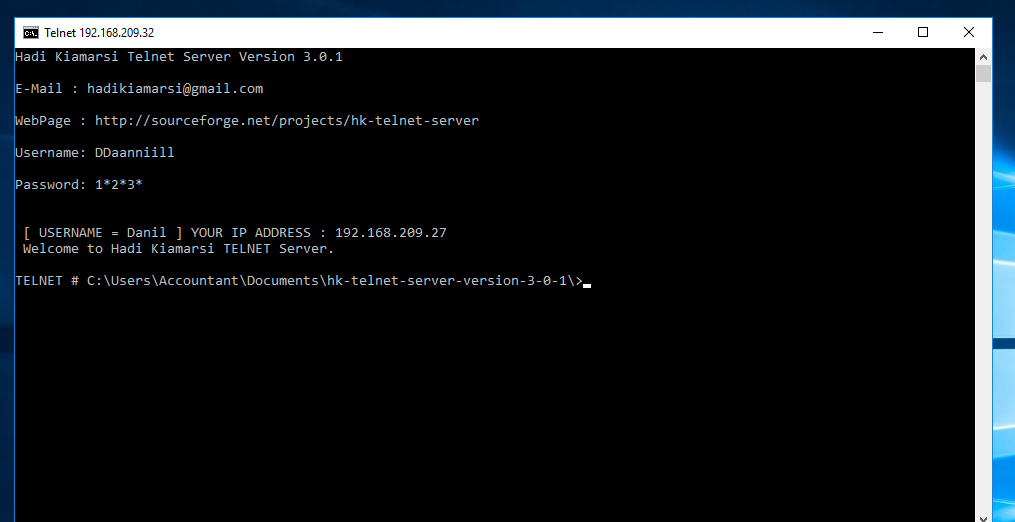


Рис 13 – Windows Server 2016

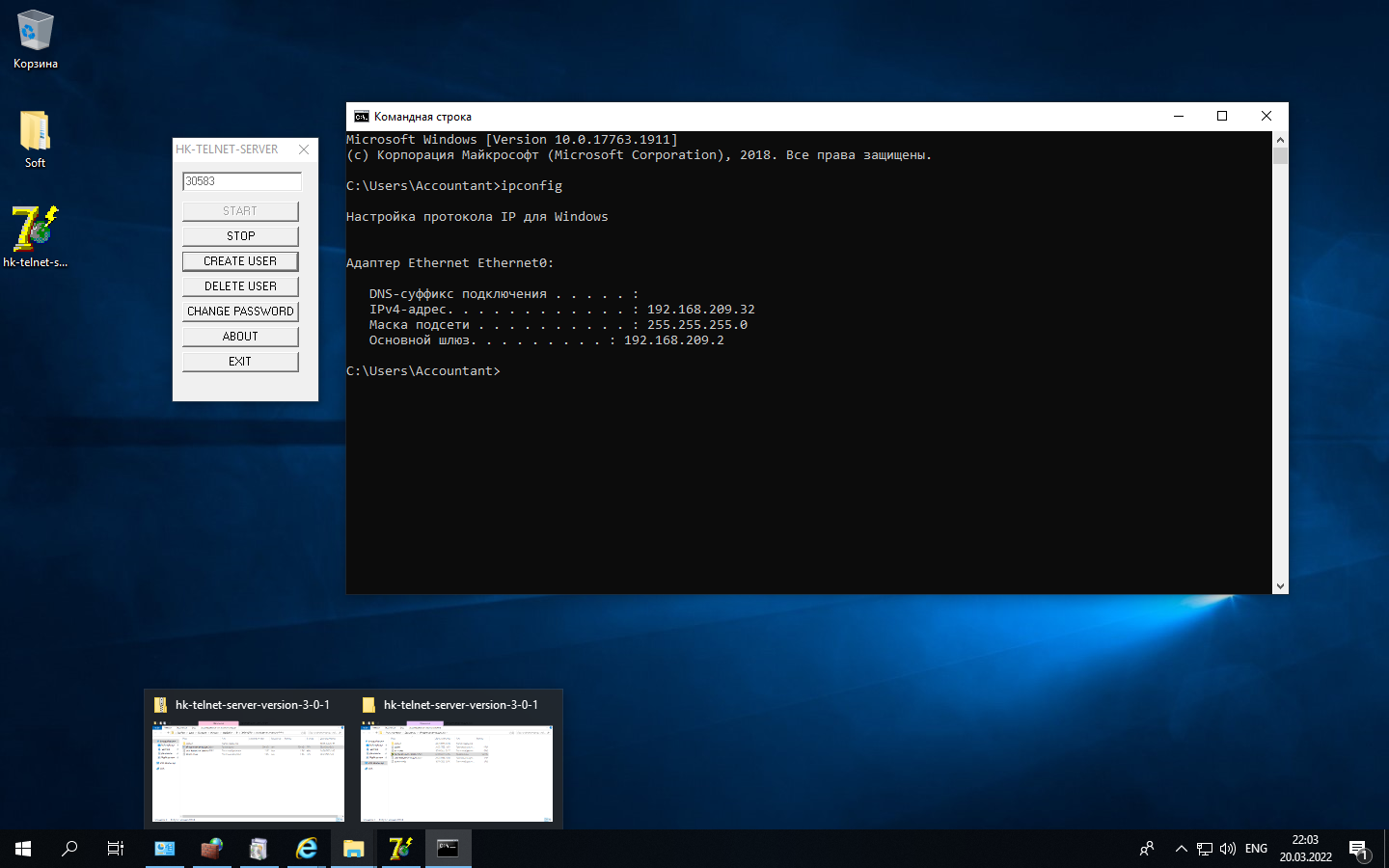


Рис 14. Windows 10 - Клиент