Государственное образовательное учреждение

«Белорусский государственный технологический университет»

Отчет

*по лабораторной работе №4*

ТЕМА ЗАНЯТИЯ: НАСТРОЙКА БРАНДМАУЭРА WINDOWS

|  |  |
| --- | --- |
|  | **Исполнитель:**  Студента (-ка) группы 2  Специальность\_\_\_\_ИСиТ\_\_\_  Гулевич Никита Максимович  (Ф.И.О.) |
|  | **Преподаватель**:  Ржеутская Н. В. |

Минск, 2025

**Цель**: : овладеть навыками настройки и использования брандмауэра Windows.

Ответы на контрольные вопросы:

1. Дайте определение понятию «брандмауэр».

Брандмауэр (межсетевой экран) – это аппаратный или программный комплекс, позволяющий проверять (фильтровать) входные и выходные потоки данных, проходящие через интернет или сеть. В случаи нарушения политики безопасности компьютера брандмауэр блокирует эти данные

1. Каково основное назначение брандмауэра?

Межсетевой экран является одним из основных компонентов защиты сетей наряду с интернет-протоколом межсетевого обмена (Internet Security Protocol – IPSec). Межсетевой экран осуществляет надежную аутентификацию пользователей и защиту от несанкционированного доступа. Отметим, что большая часть проблем с информационной безопасностью сетей связана с «прародительской» зависимостью коммуникационных решений от операционной системы UNIX – особенности открытой платформы и среды программирования UNIX сказались на реализации протоколов обмена данными и политики информационной безопасности. Вследствие этого ряд интернетслужб и совокупность сетевых протоколов (Transmission Control Protocol/Internet Protocol – TCP/IP) имеет «бреши» в защите.

1. Как создаются правила по ограничению доступа программ к сети?

Создание правила по ограничению доступа программ к сети. Для создания правила по ограничению доступа программ к сети необходимо открыть панель управления в меню «Пуск». В зависимости от версии операционной системы Windows может отображаться классический вид панели управления или с разделениями по категориям.

На первом этапе необходимо включить брандмауэр, в случае если он был ранее выключен. Нужно выбрать в левой панели управления вкладку «Включение и отключение брандмауэра Windows»

В появившемся окне переключаем параметры на значение «Включение брандмауэра Windows»

Вторым этапом является настройка правил для входящих и исходящих подключений. Для этого выбираем вкладку «Дополнительные параметры»

В открывшемся окне щелкаем мышью в левой панели по строке «Правила для входящих подключений», затем во вкладке меню «Действие» выбираем «Создать правило», либо нажимаем «Создать правило» в правой панели

В открывшемся мастере создания правила выбираем «Для программы», в случае если необходимо перекрыть доступ к сети конкретной программе, либо «Для порта» (например, если есть необходимость отключить часть возможностей программы)

При ограничении работы программы далее необходимо указать ее путь обязательно через папку, в которой она установлена, а не через ярлыки

Далее указывается, какое именно действие вы хотите применить. В данном случае необходимо блокировать подключение

В следующем окне указываем имя правила

В общем списке появляется созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели

При двойном нажатии на правило отображаются его свойства

1. Как можно вызвать командную строку?

1.Win+R   
2. Ввести cmd

1. Перечислите способы устранения возможных ошибок системы при включении брандмауэра.

Устранение возможных ошибок системы при включении брандмауэра. При возникновении ошибок при попытке включить брандмауэр, необходимо включить брандмауэр в соответствующих службах Windows

**Проверка настроек брандмауэра**:

* Убедитесь, что правила и политики настроены корректно.
* Проверьте, не блокируются ли необходимые порты и приложения.

**Обновление программного обеспечения**:

* Убедитесь, что операционная система и брандмауэр обновлены до последней версии.
* Установите обновления безопасности и исправления.

**Проверка конфликтов с другими программами**:

* Убедитесь, что другие средства безопасности (антивирусы, VPN и т.д.) не конфликтуют с брандмауэром.
* Отключите временно другие программы для тестирования.

**Просмотр журналов событий**:

* Изучите журналы брандмауэра и системные журналы для выявления ошибок.
* Ищите сообщения об ошибках или предупреждениях, связанных с включением.

**Тестирование конфигурации**:

* Используйте инструменты для тестирования, чтобы проверить, правильно ли функционирует брандмауэр.
* Проверьте, как система реагирует на попытки доступа.

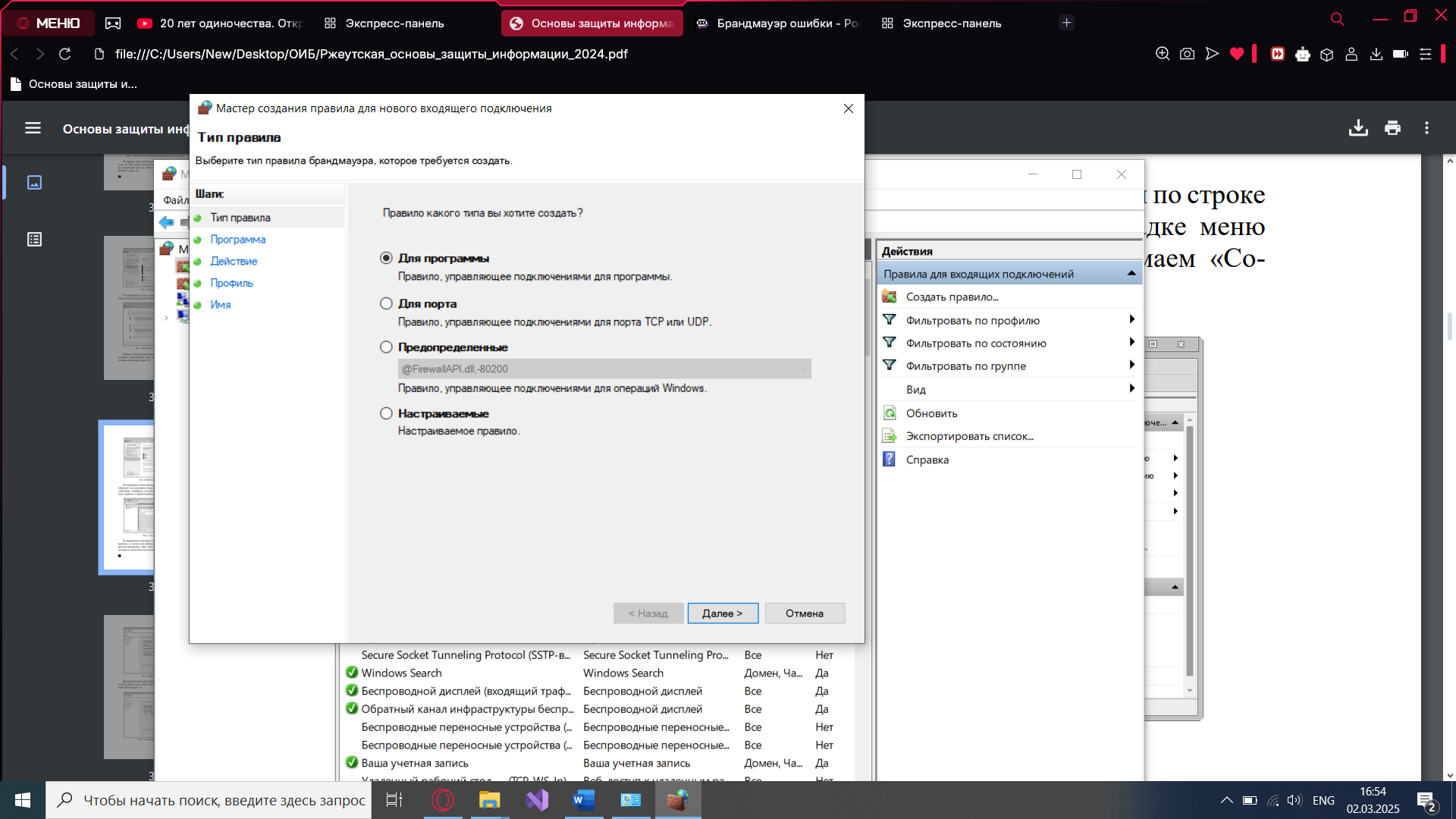
**Сброс настроек брандмауэра**:

* При серьезных проблемах можно сбросить настройки брандмауэра до заводских.
* После этого настройте его заново.

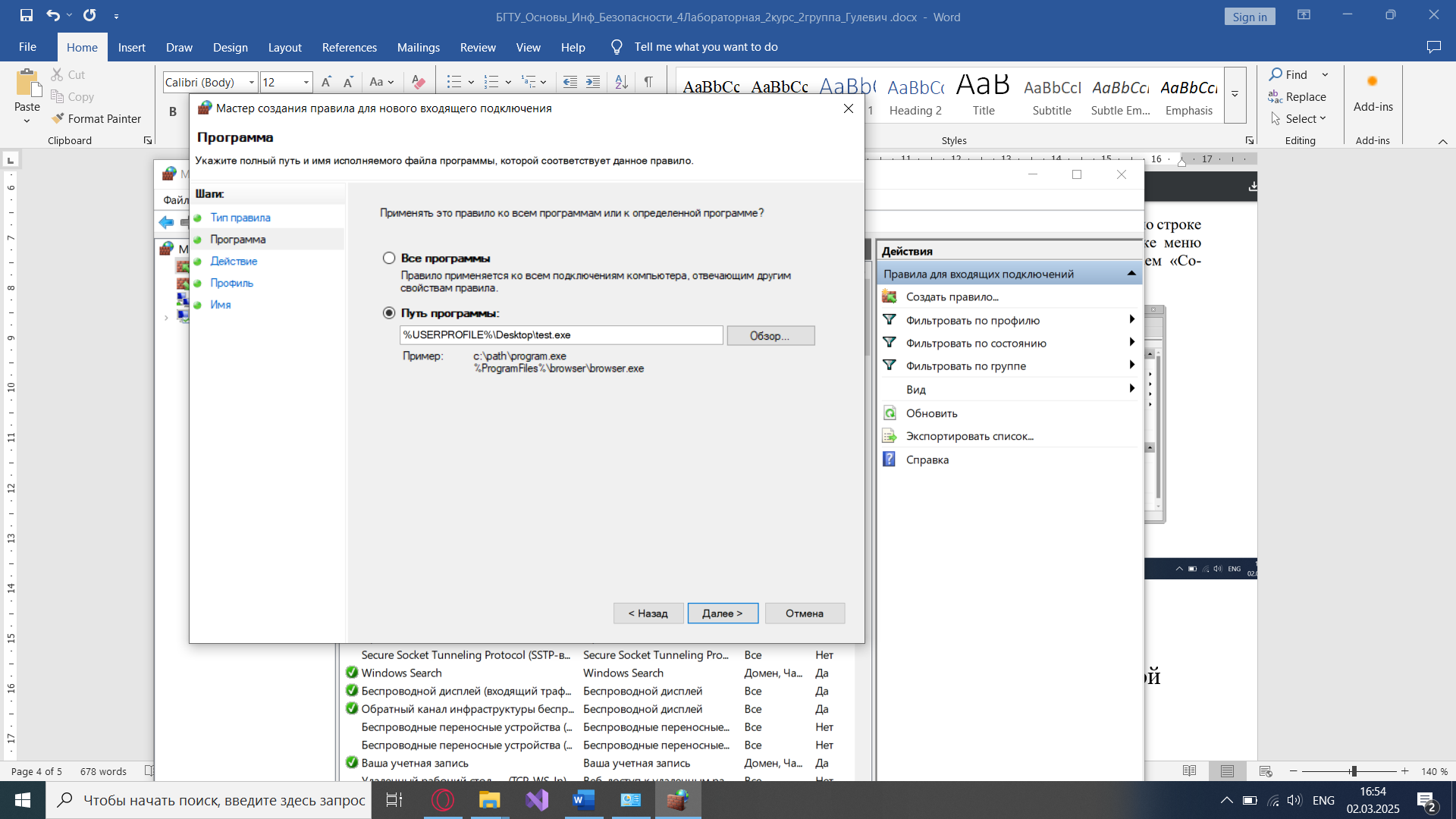
Задание для выполнения

* 1. Создайте правила для входящих подключений (с помещением в электронный конспект копий экрана с пояснениями промежуточных действий): а) для одной программы (по выбору) на блокировку подключения; б) для одной программы (по выбору) на разрешение подключения.

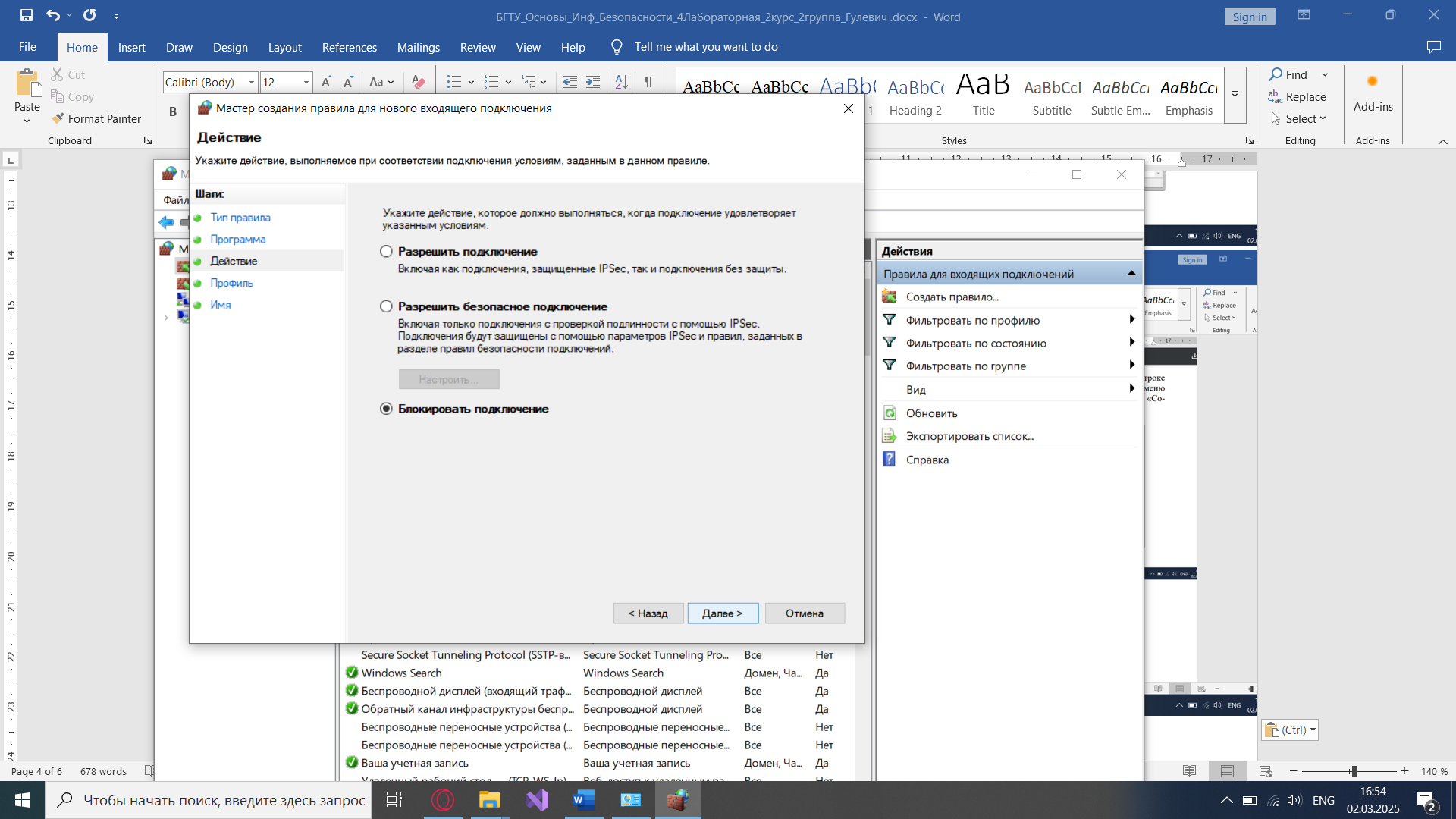
СОЗДАЕМ ПРАВИЛО ПО ПУНКТАМ ДЛЯ test.exe



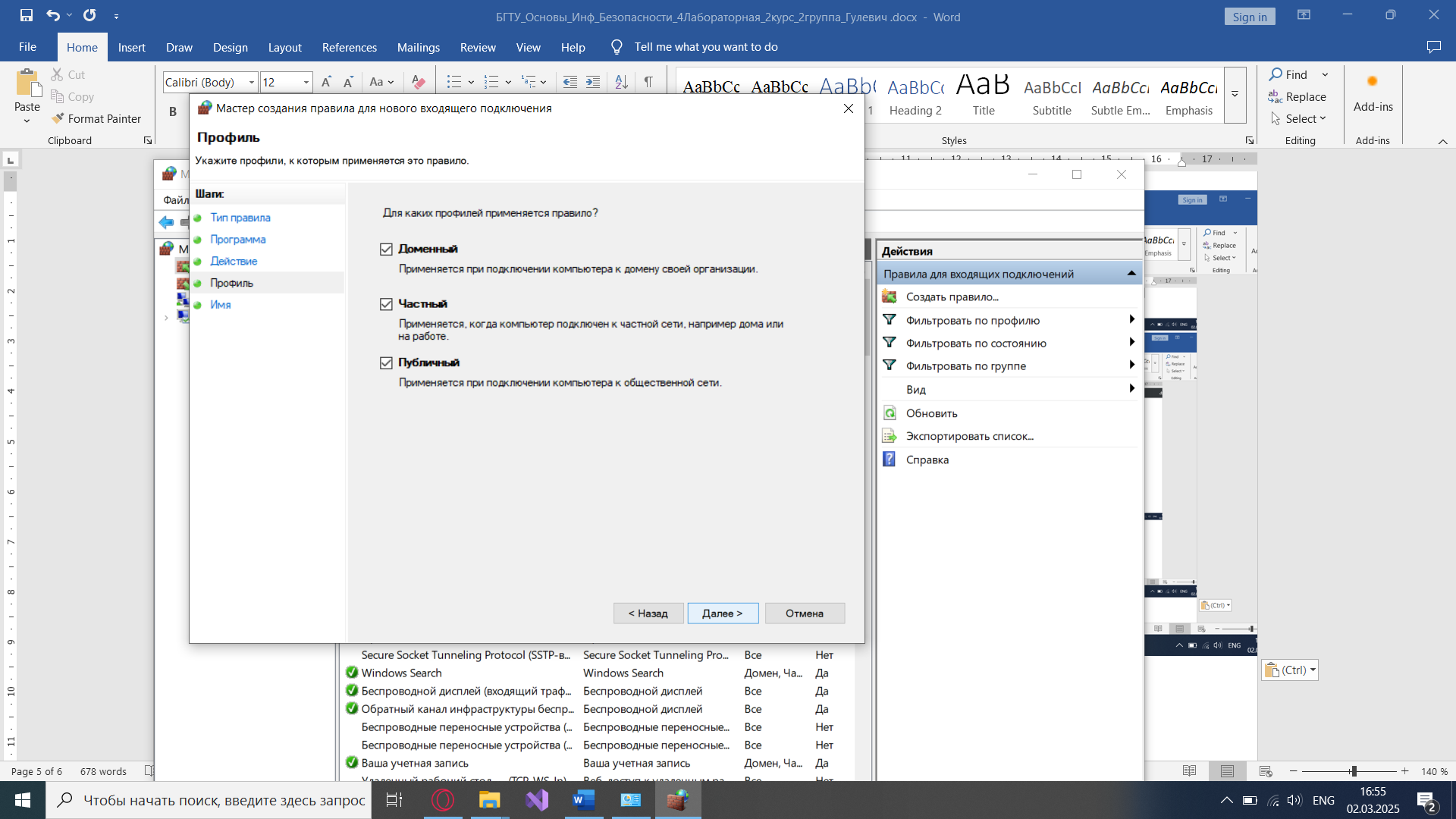
Указываем путь



Указываем тип правила

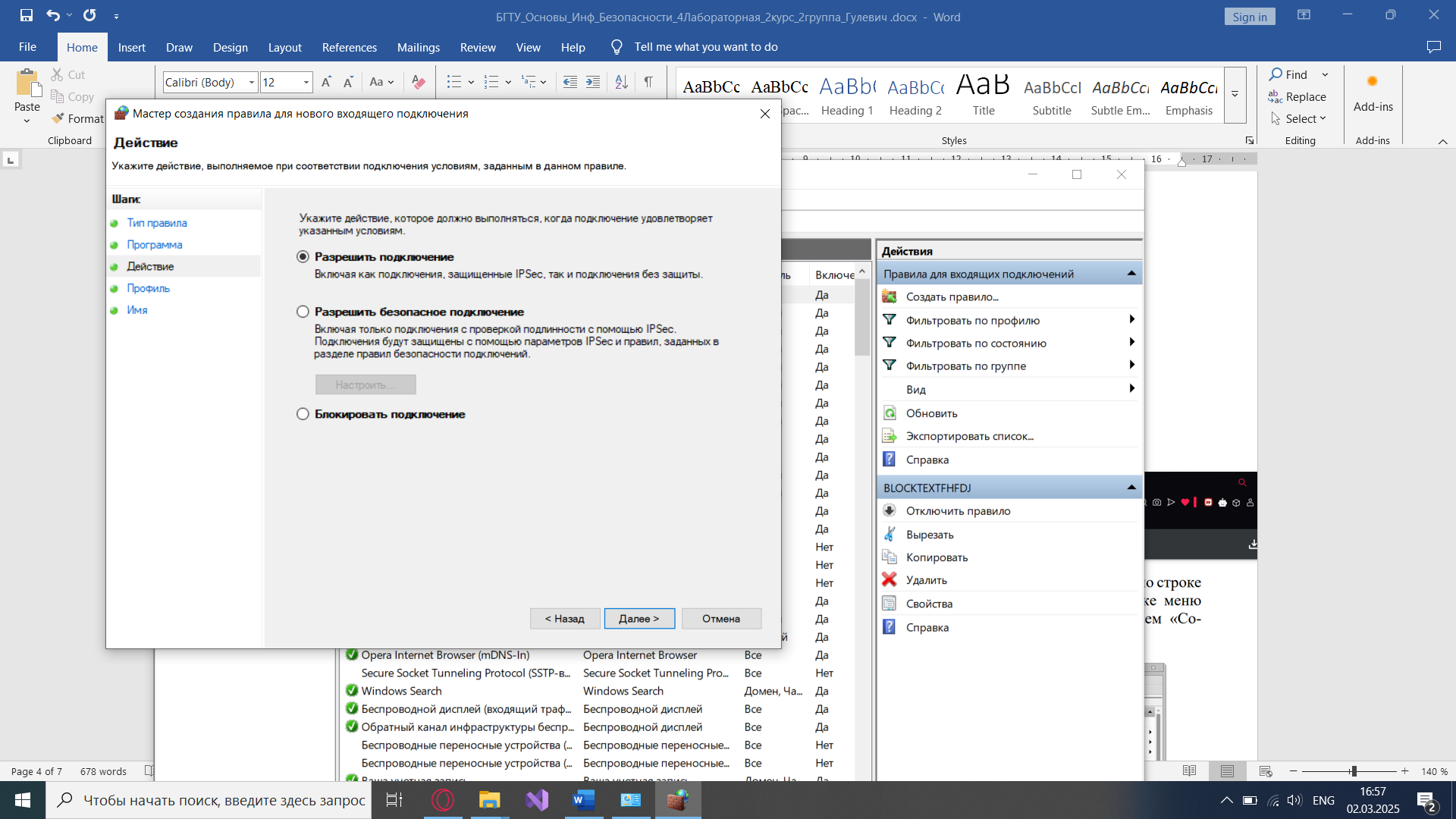


Указываем профили

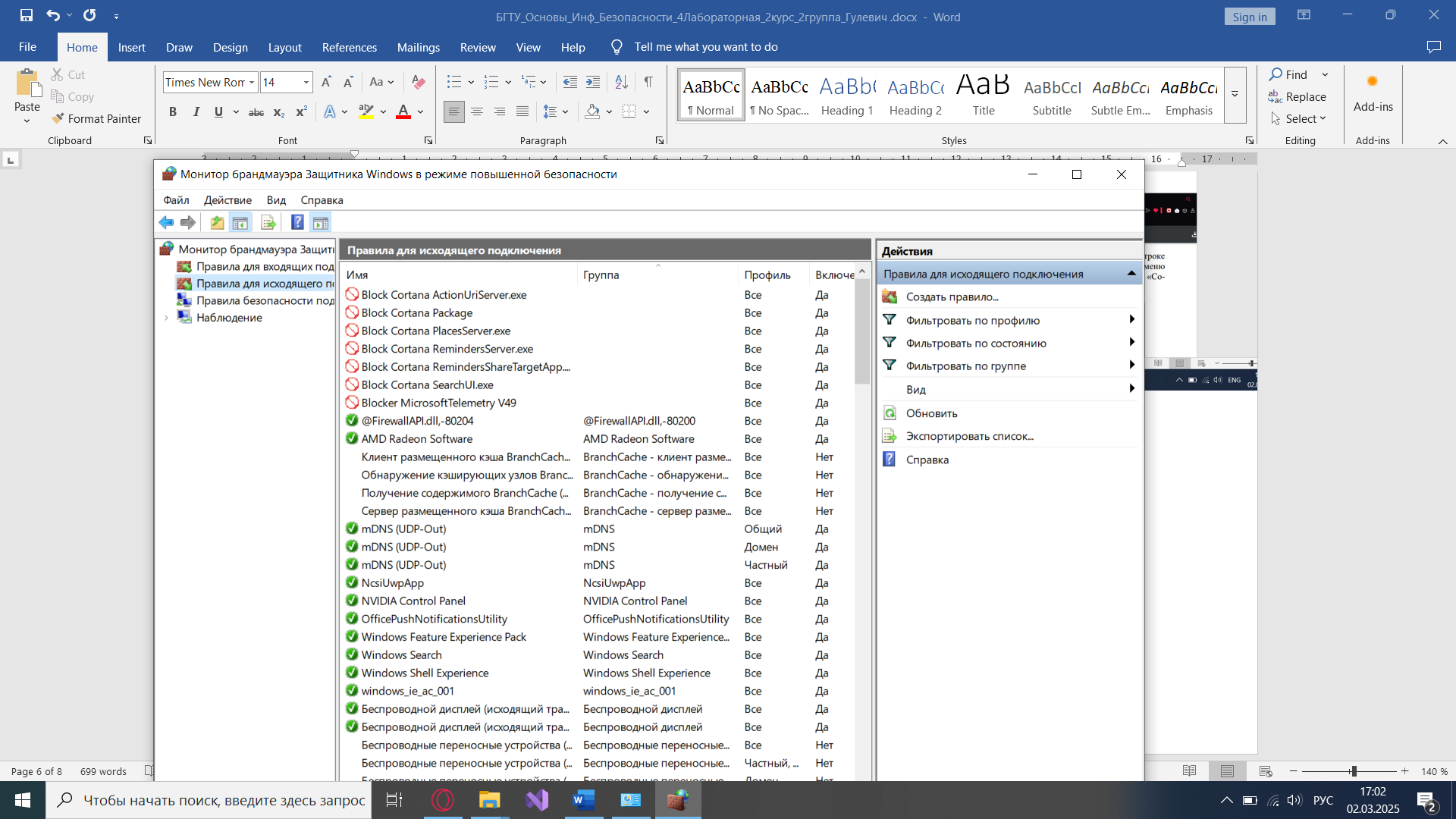




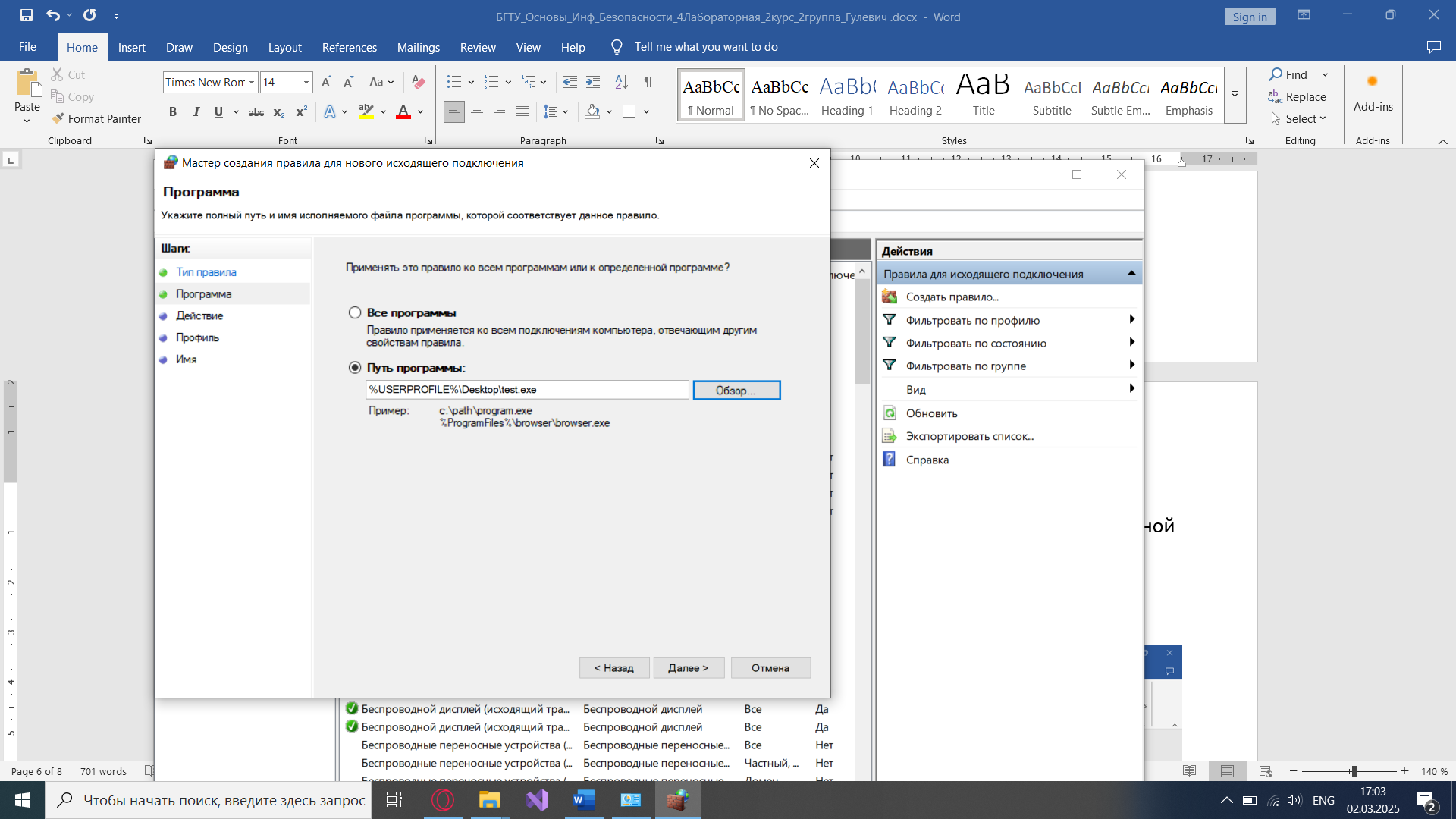
СОЗДАНИЕ РАЗРЕШАЮЩЕГО ПРАВИЛА ОТЛИЧАЕТСЯ ТОЛЬКО В 1 пункте

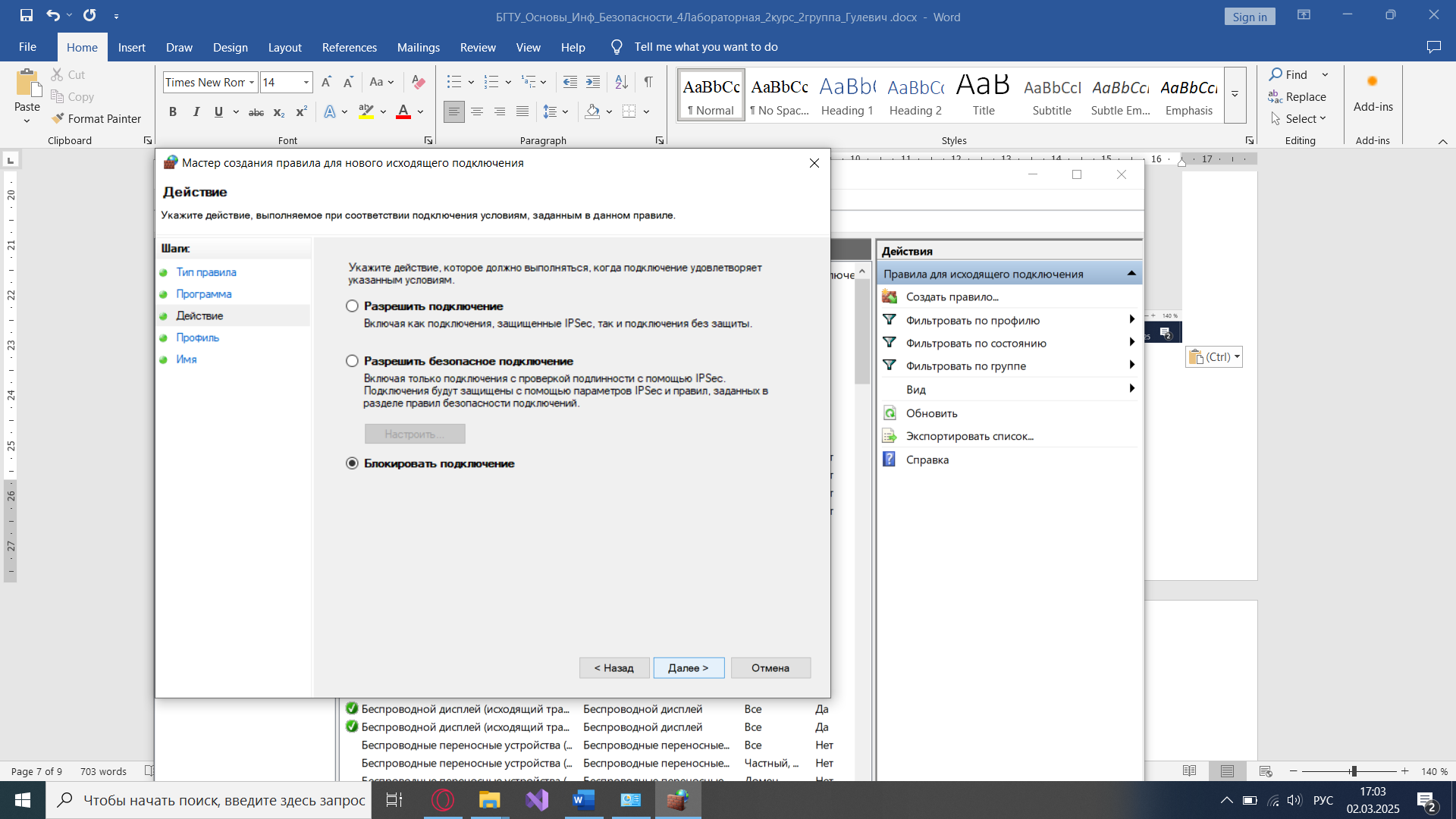


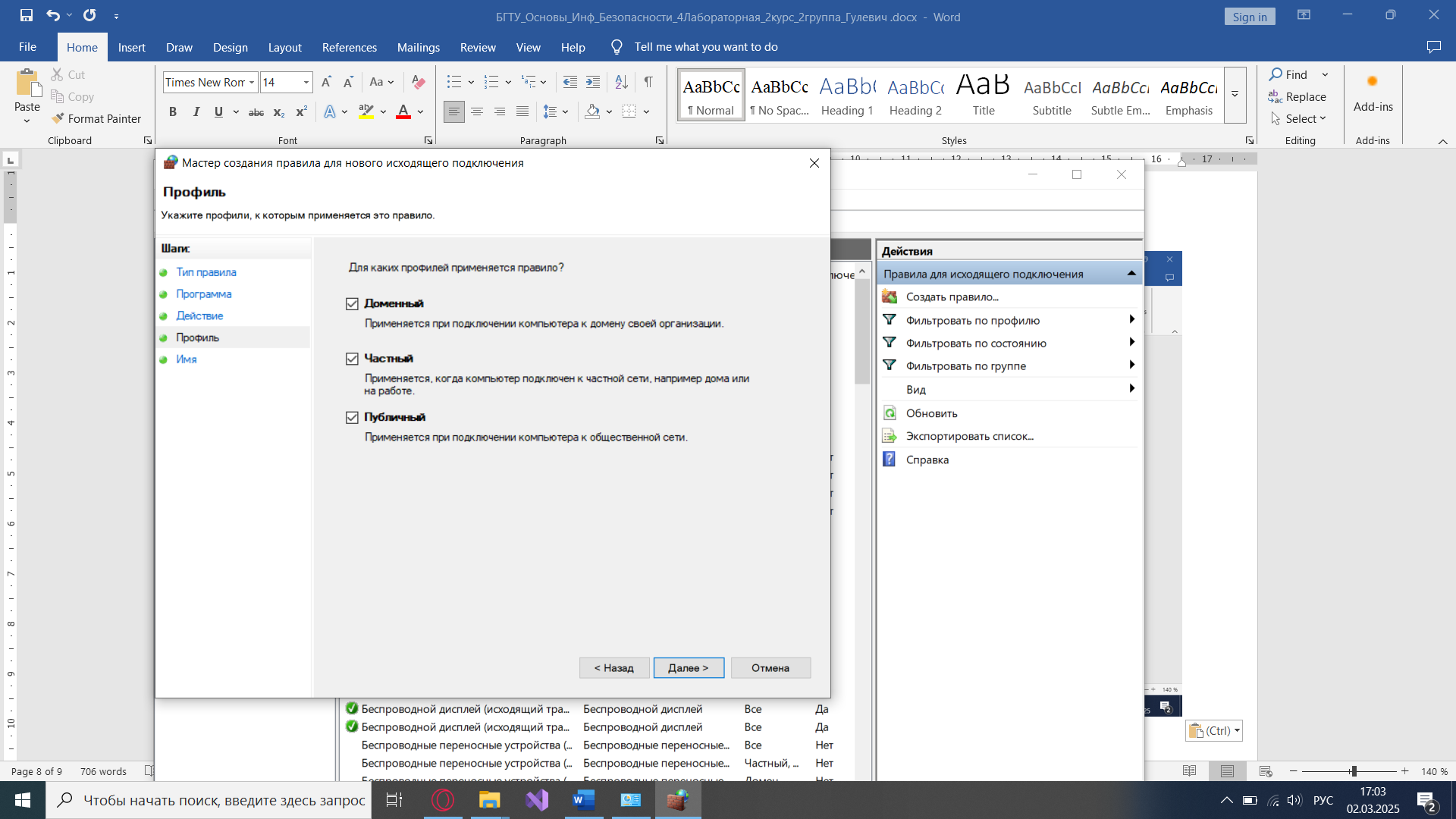
* 1. Создайте правила для исходящих подключений (с помещением в электронный конспект копий экрана с пояснениями действий): а) для одной программы (по выбору) на блокировку подключения; б) для одной программы (по выбору) на разрешение подключения.

Создаем правило

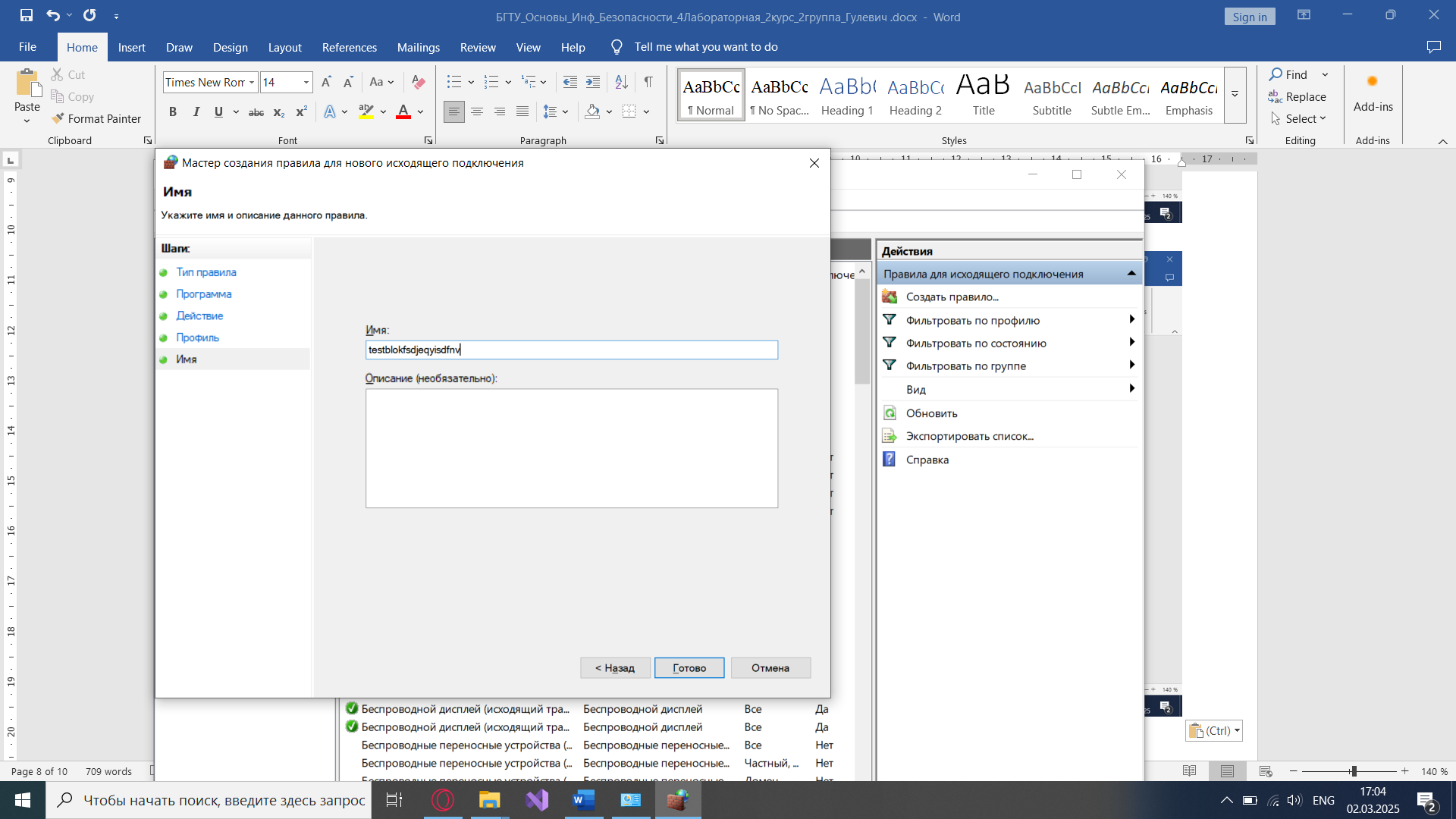
Указываем путь

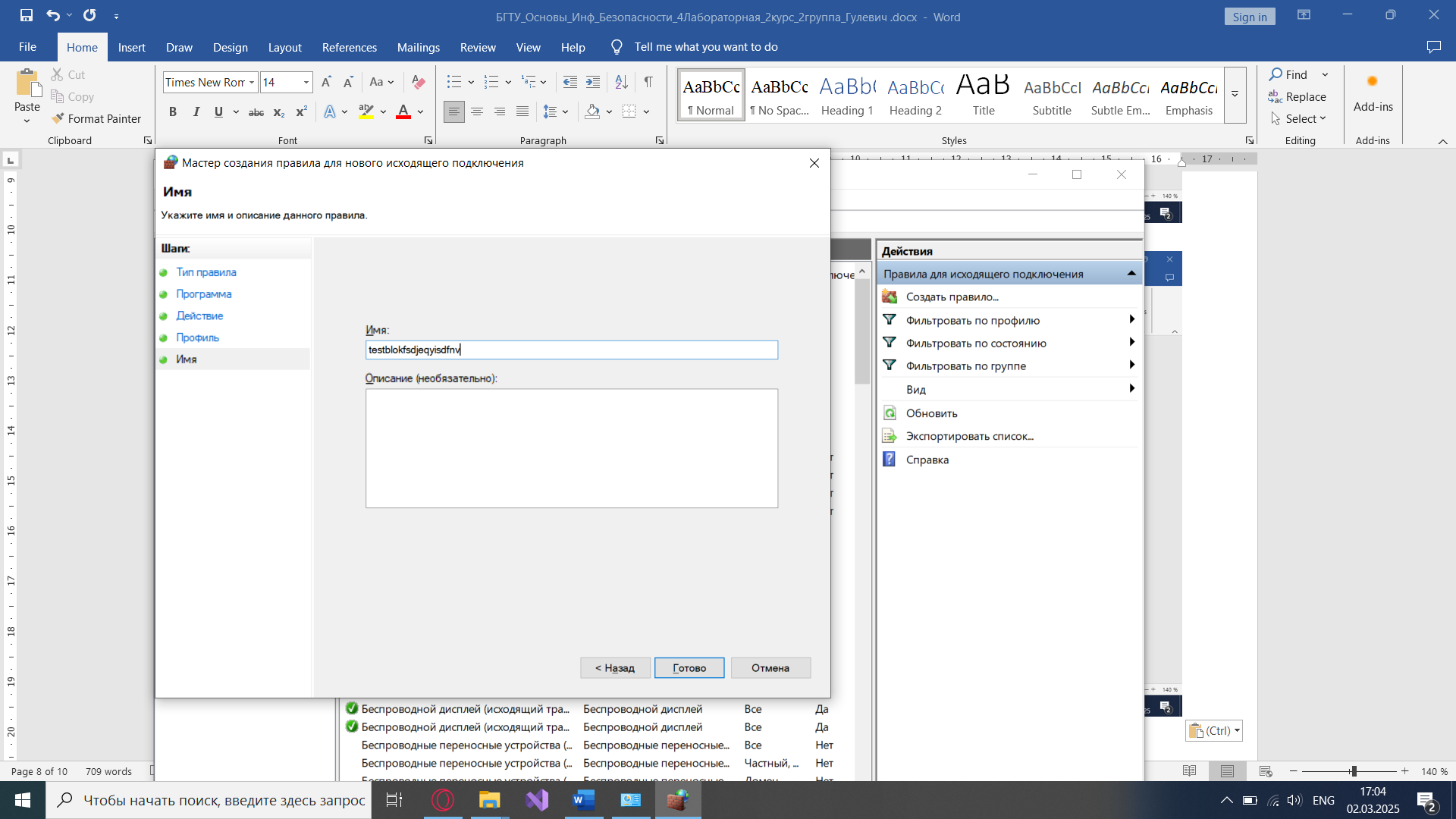


Указываем тип правила 

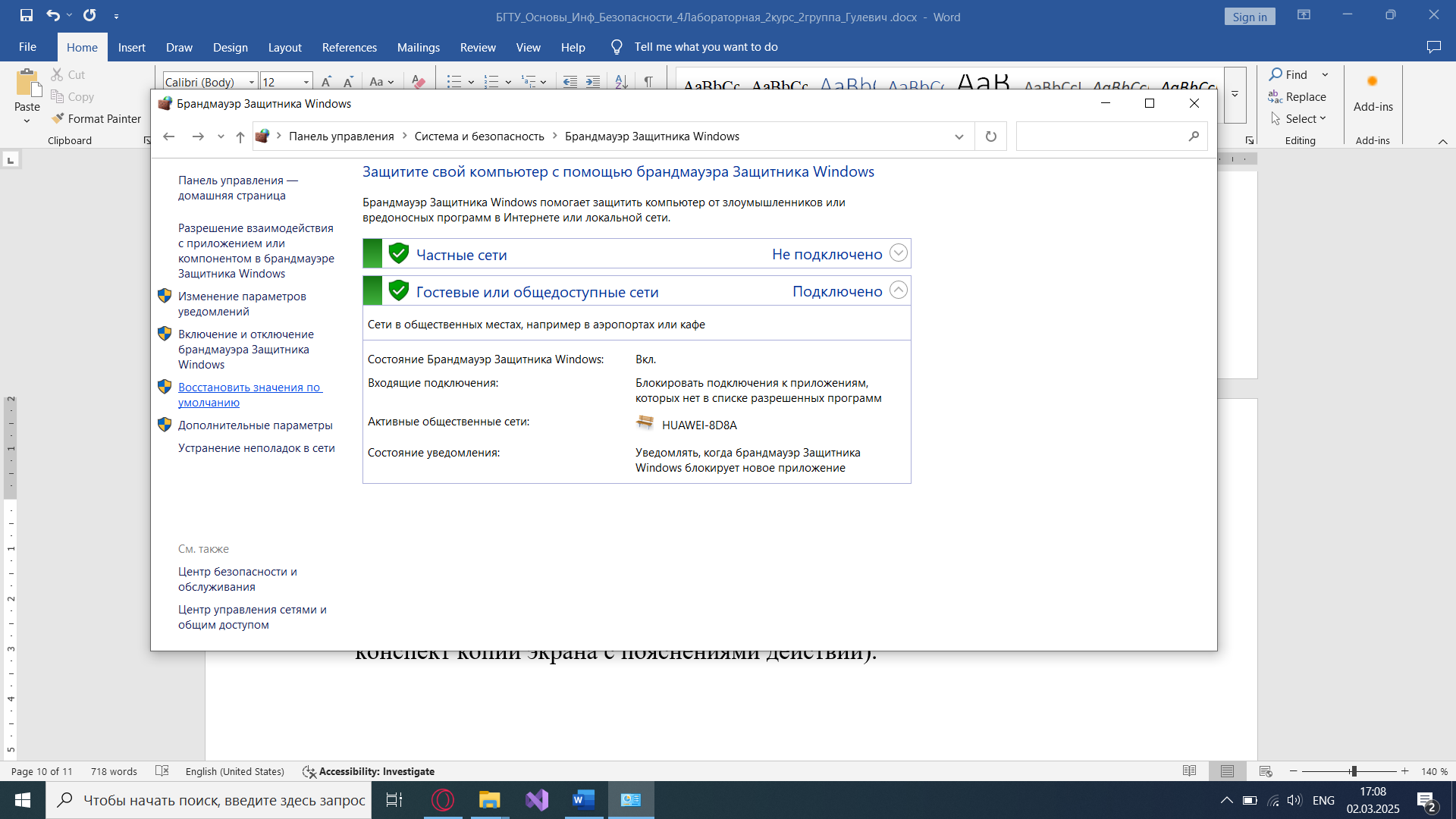
Выбираем профили применения  


Выбираем имя

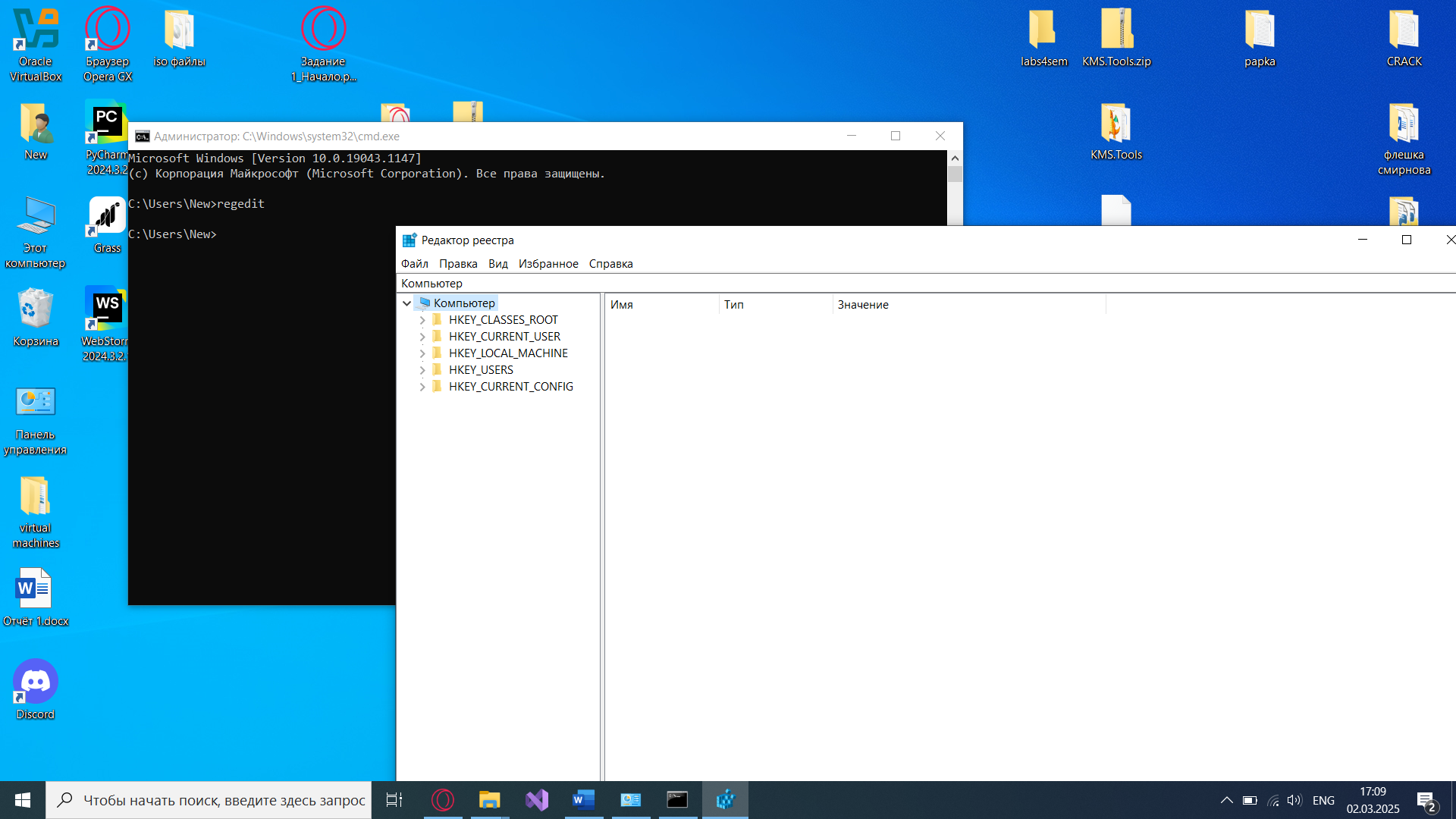


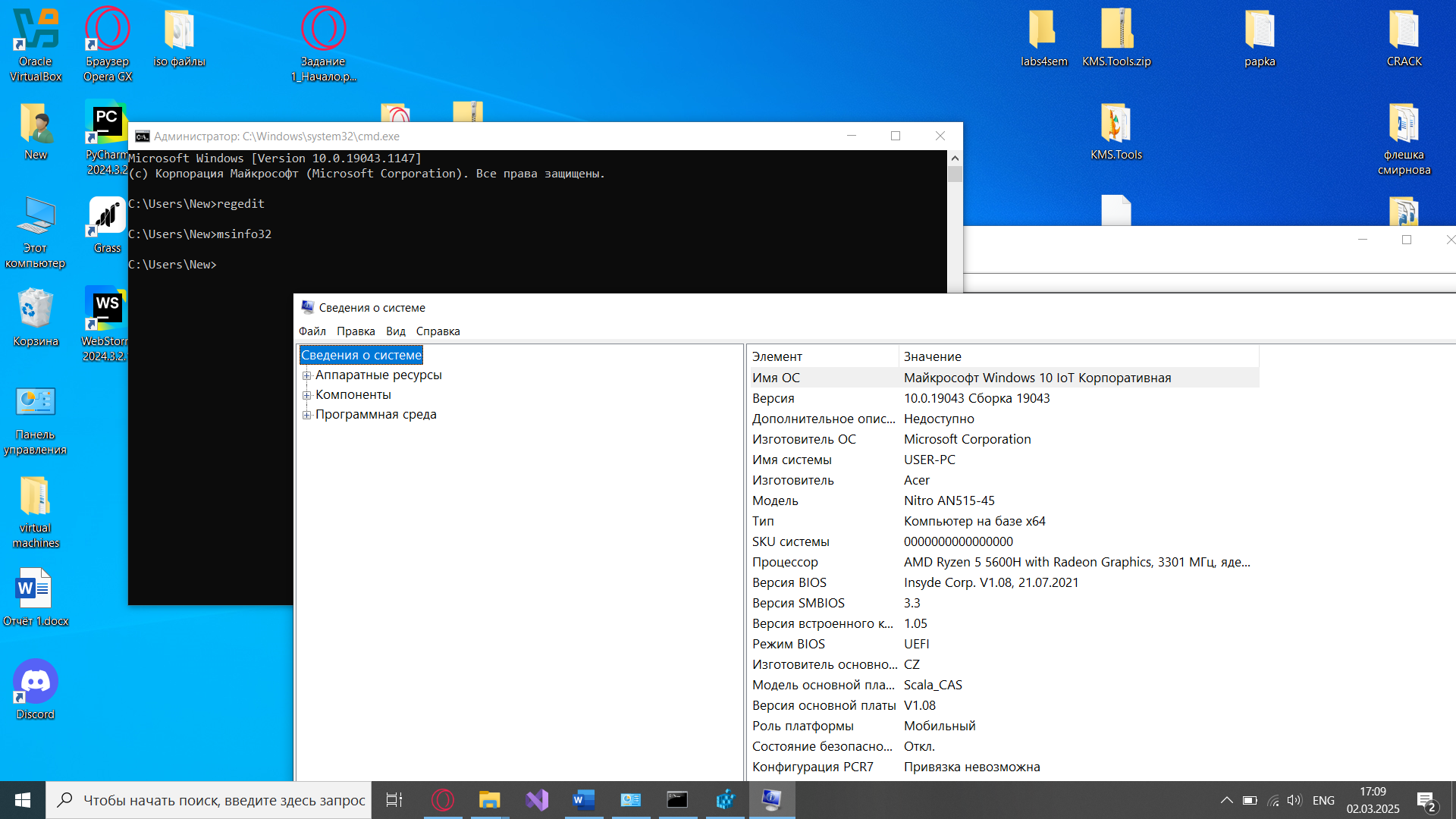
Создание разрешающего правила отличается в 1 пункте   


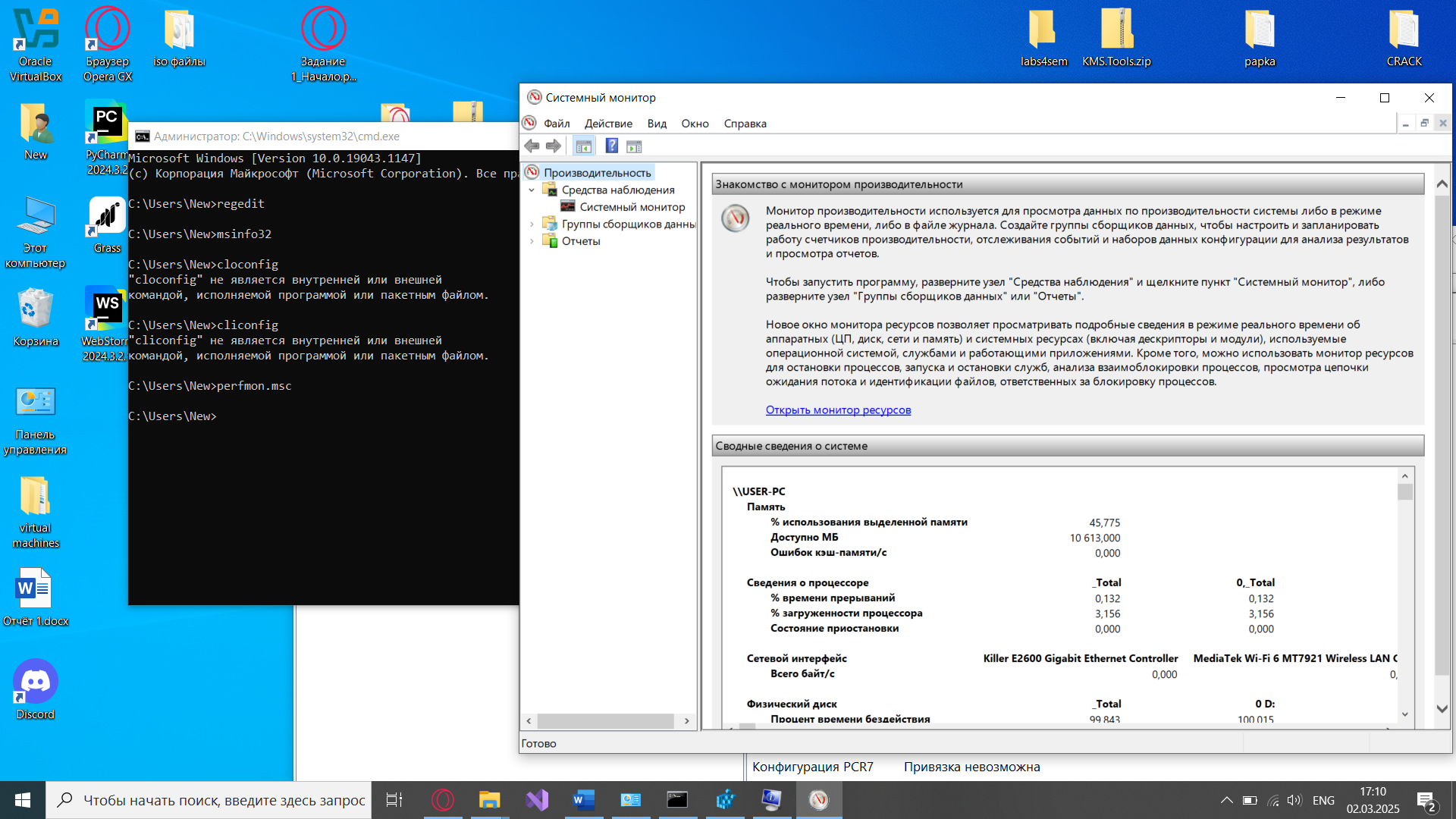
* 1. Верните настройки брандмауэра в исходное состояние до начала выполнения практического задания.



* 1. Опробуйте действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий).







**Список использованных источников**

1. Ржеутская Н. В., Нистюк О. А., Уласевич Н. И. Основы защиты информации: лабораторный практикум. Минск: Учреждение образования «Белорусский государственный технологический университет», 2024.