Министерство образования Республики Беларусь

Учреждение образования  
БЕЛОРУССКИЙ  ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

                        Факультет      Информационных технологий и управления

                        Кафедра         Интеллектуальных информационных технологий

**ОТЧЁТ**

по лабораторной работе №6

по дисциплине “Средства и методы защиты

информации в интеллектуальных системах”

Вариант 10

Выполнила:

Демидовец Д.В. , гр. 221703

Проверила:

Крищенович В.А.

Минск, 2024

**МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ**

Теоретические сведения:

Межсетевой экран – это комплекс программно-аппаратных средств межсетевой защиты, позволяющий реализовать частную политику безопасности (набор правил), определяющую условия прохождения пакетов данных через границу из одного участка информационной сети в другой. Как правило, межсетевой экран устанавливается между локальной сетью предприятия и глобальной сетью Интернет. Межсетевой экран является также программным решением, являющимся элементом операционных систем семейства Windows, начиная с Windows NT и более поздних. В качестве другого, часто используемого названия для межсетевого экрана используют термины firewall (английский) и брандмауэр (русская транскрипция с немецкого).

Основными задачами, решаемыми межсетевыми экранами являются:

1) Ограничение доступа внешних пользователей к ресурсам защищаемой внутренней сети.

2) Разграничение доступа пользователей защищаемой сети к внешним ресурсам. Такое разграничение позволяет, например, ограничить доступ своих сотрудников к внешним ресурсам, не требуемым для выполнения своих функциональных обязанностей.

Брандмауэр — это инструмент для защиты компьютеров от несанкционированного доступа. Он фильтрует входящий и исходящий трафик на основе заданных правил. Основные возможности брандмауэра включают:

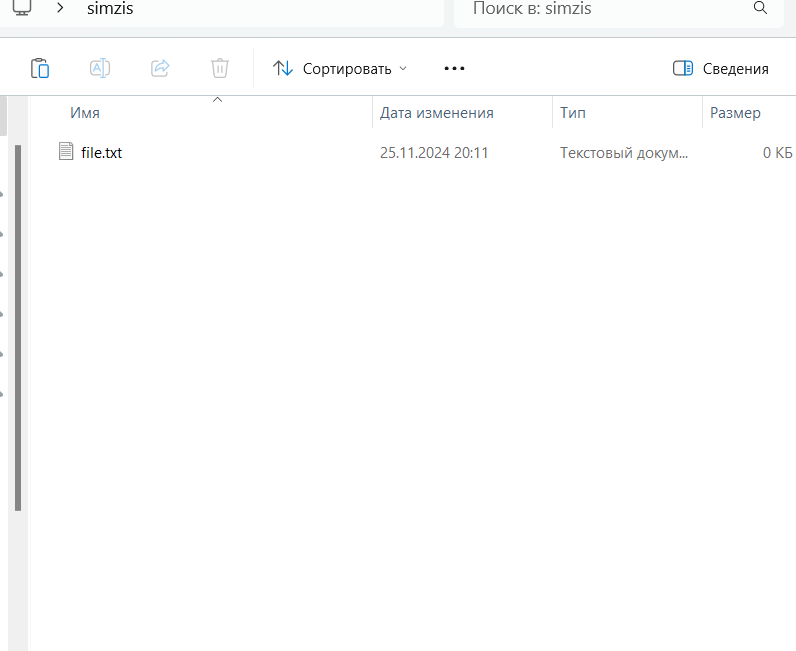
* Разрешение или блокировка доступа по IP-адресу.
* Управление доступом по портам.
* Создание правил для определенных приложений.

Основные параметры правил включают IP-адрес, который позволяет разрешать или блокировать доступ для конкретных устройств, порты, которые используются для ограничения доступа к приложениям, работающим на определенных протоколах (например, HTTP - порт 80, FTP - порт 21), и программы, для которых можно настроить разрешения или ограничения.

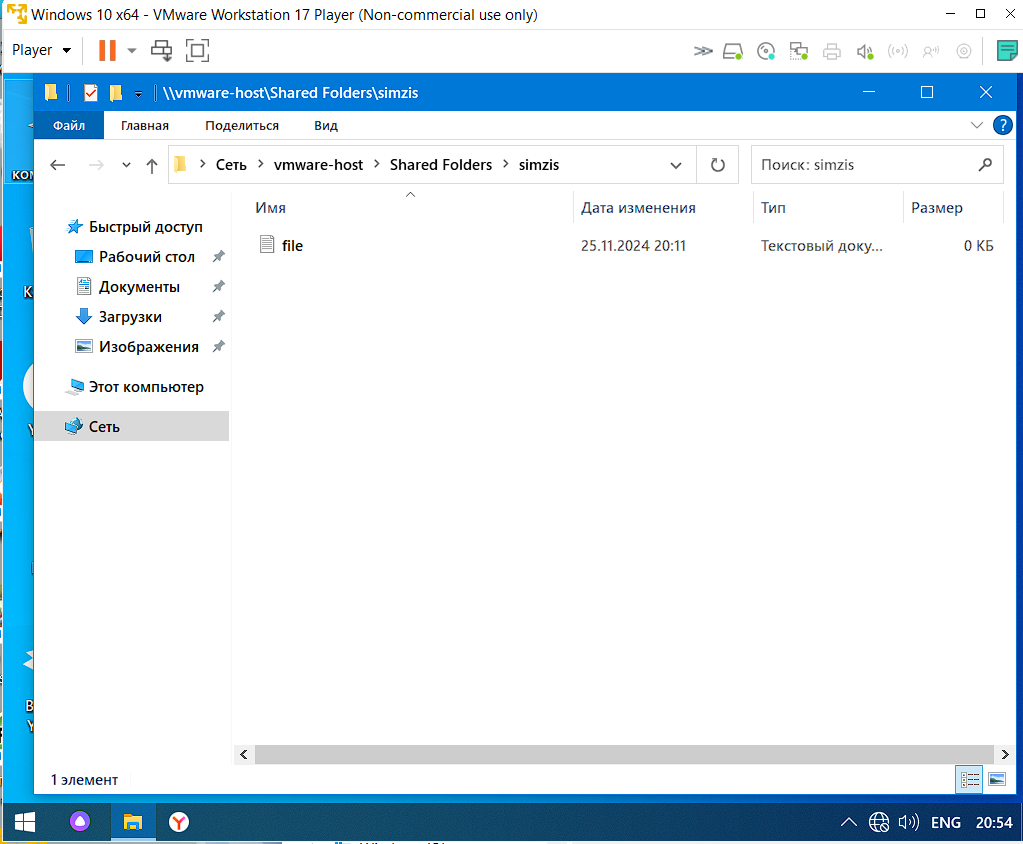
Для управления доступом в Windows используются правила входящего и исходящего трафика. Входящий трафик — это запросы, поступающие на устройство, а исходящий — запросы, отправляемые с устройства наружу.

**Задание для самостоятельного выполнения**

1) Создать папку с общим доступом на одной из виртуальных машин.



Папка на основной Windows

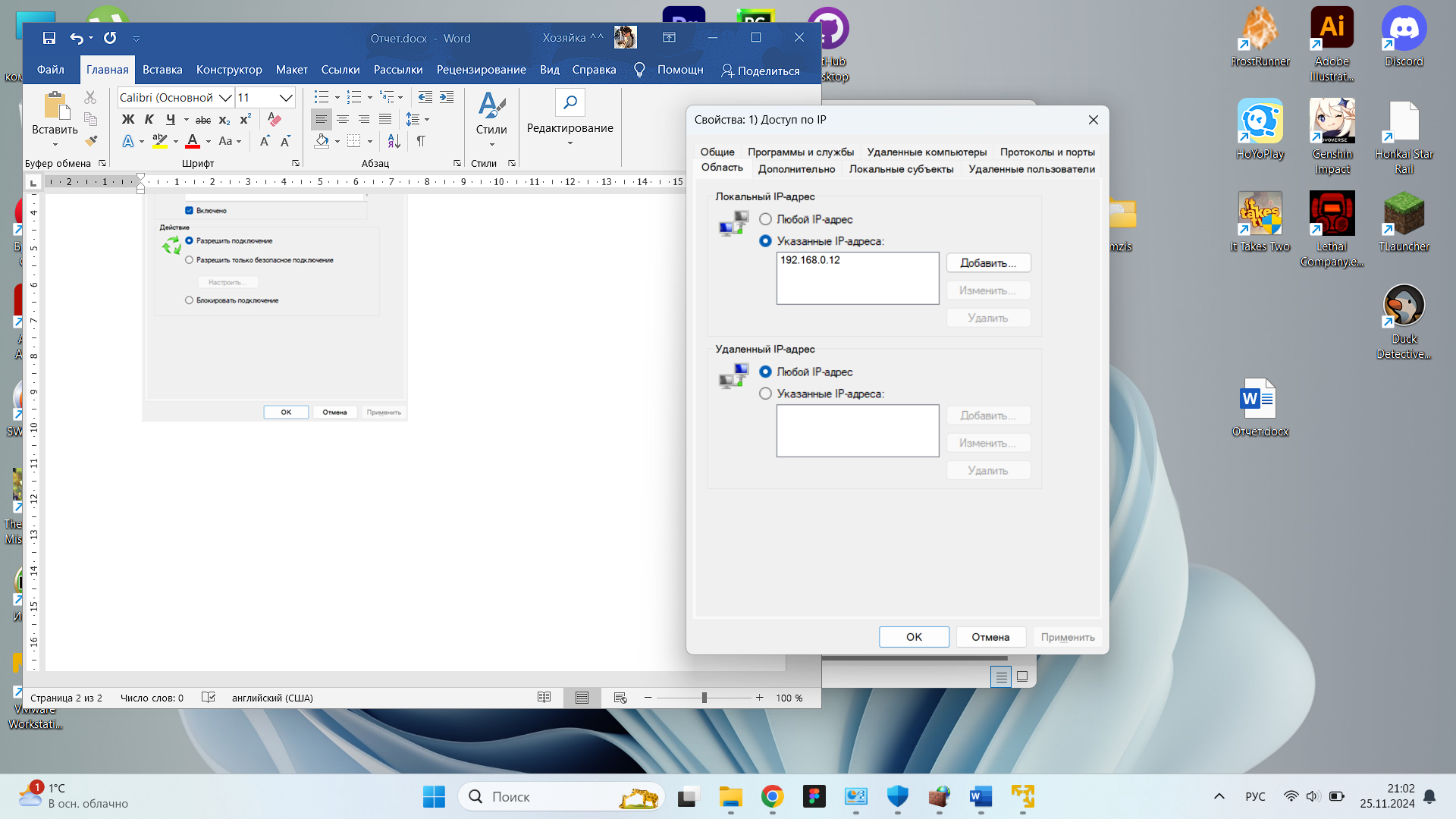


Папка на Windows 10 в WMware Workstation

2) Настроить брандмауэр, применив различные политики:

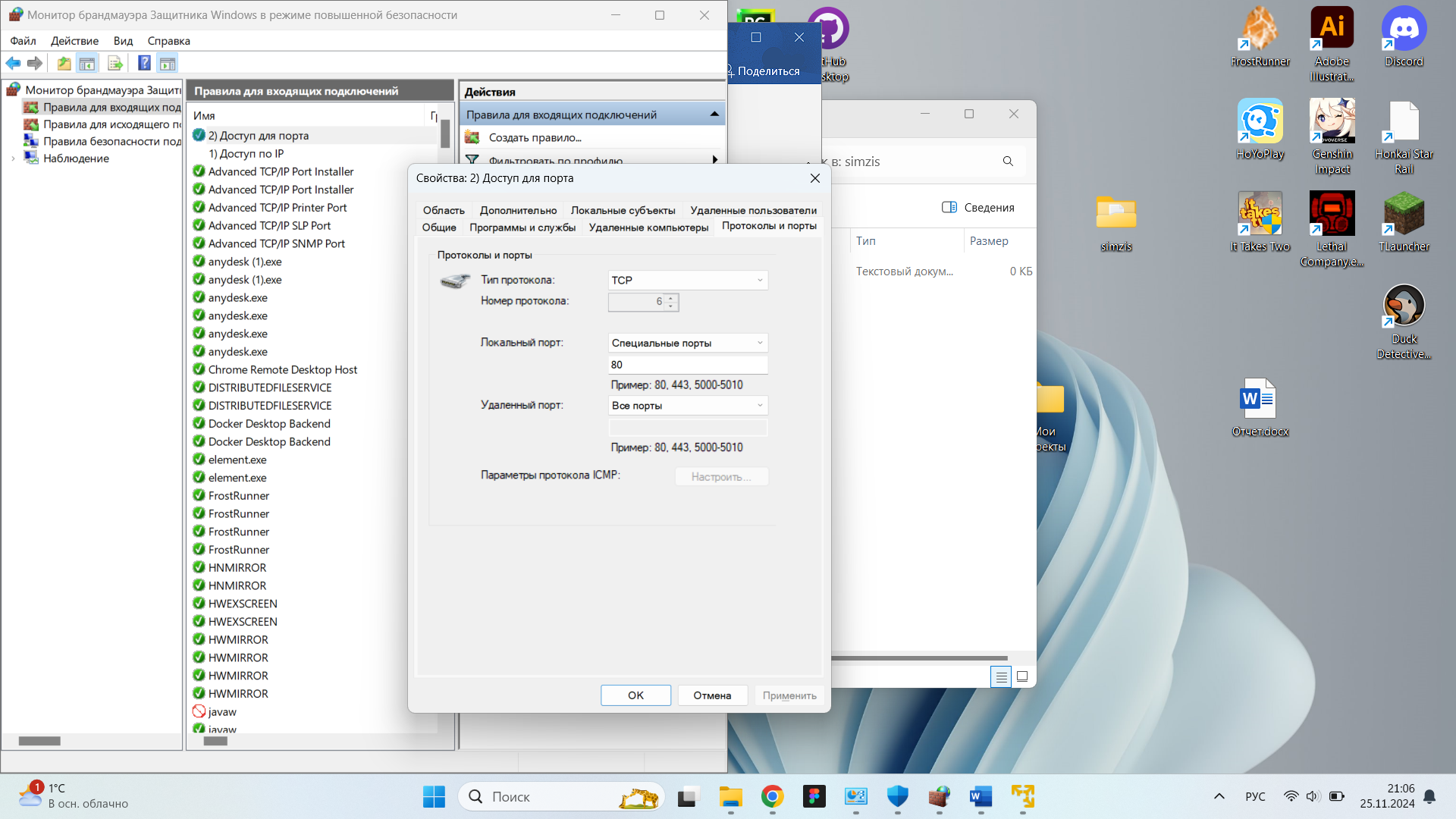
а) доступ к разделяемому ресурсу разрешен только компьютеру с данным

IP-адресом;



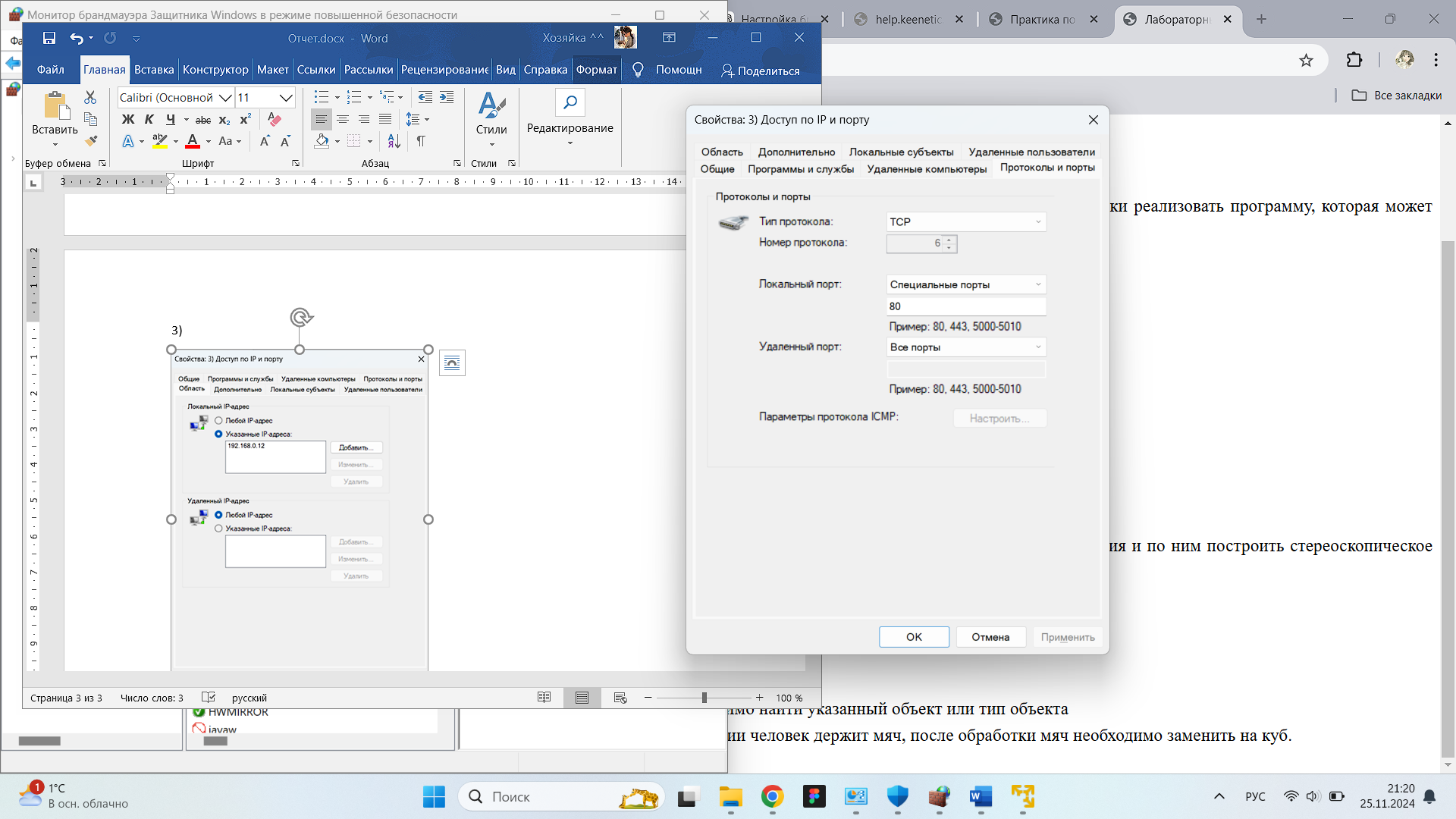
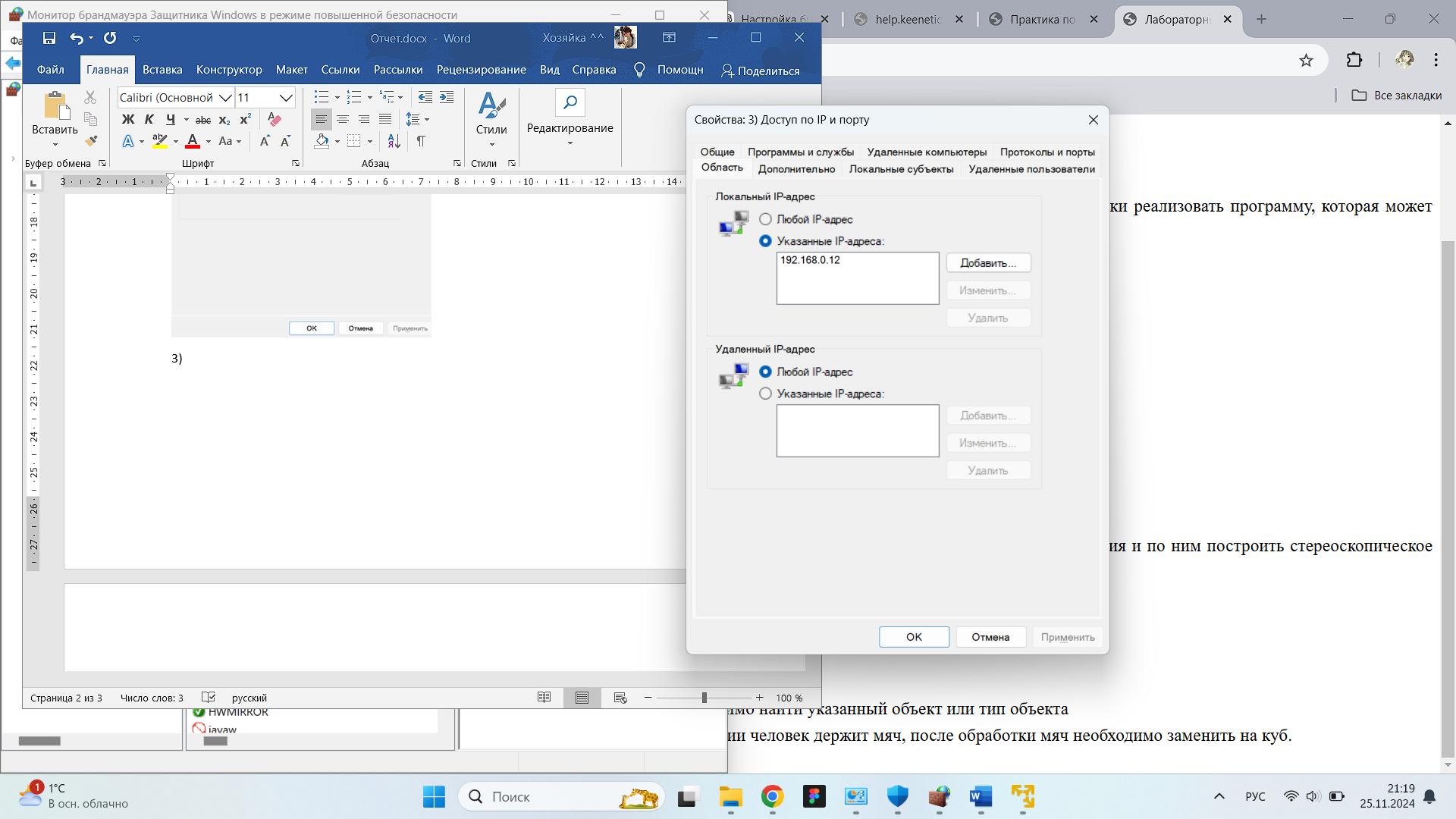
б) доступ к виртуальной машине разрешен только по заданным портам

(например, www или ftp);

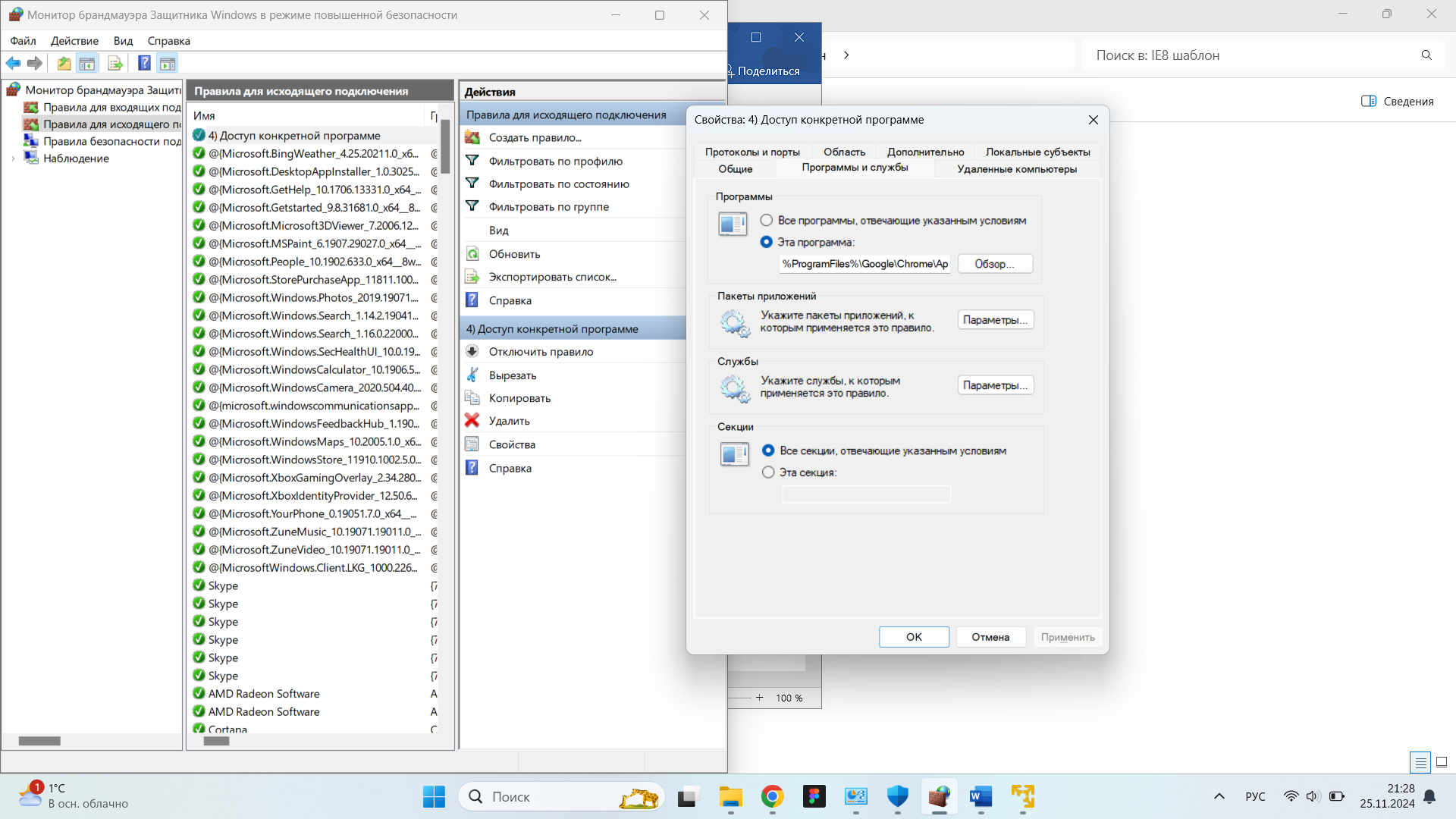


в) доступ к виртуальной машине разрешен только по заданным портам

(например, www или ftp) и только компьютерам с данным IP-адресом (адресами);

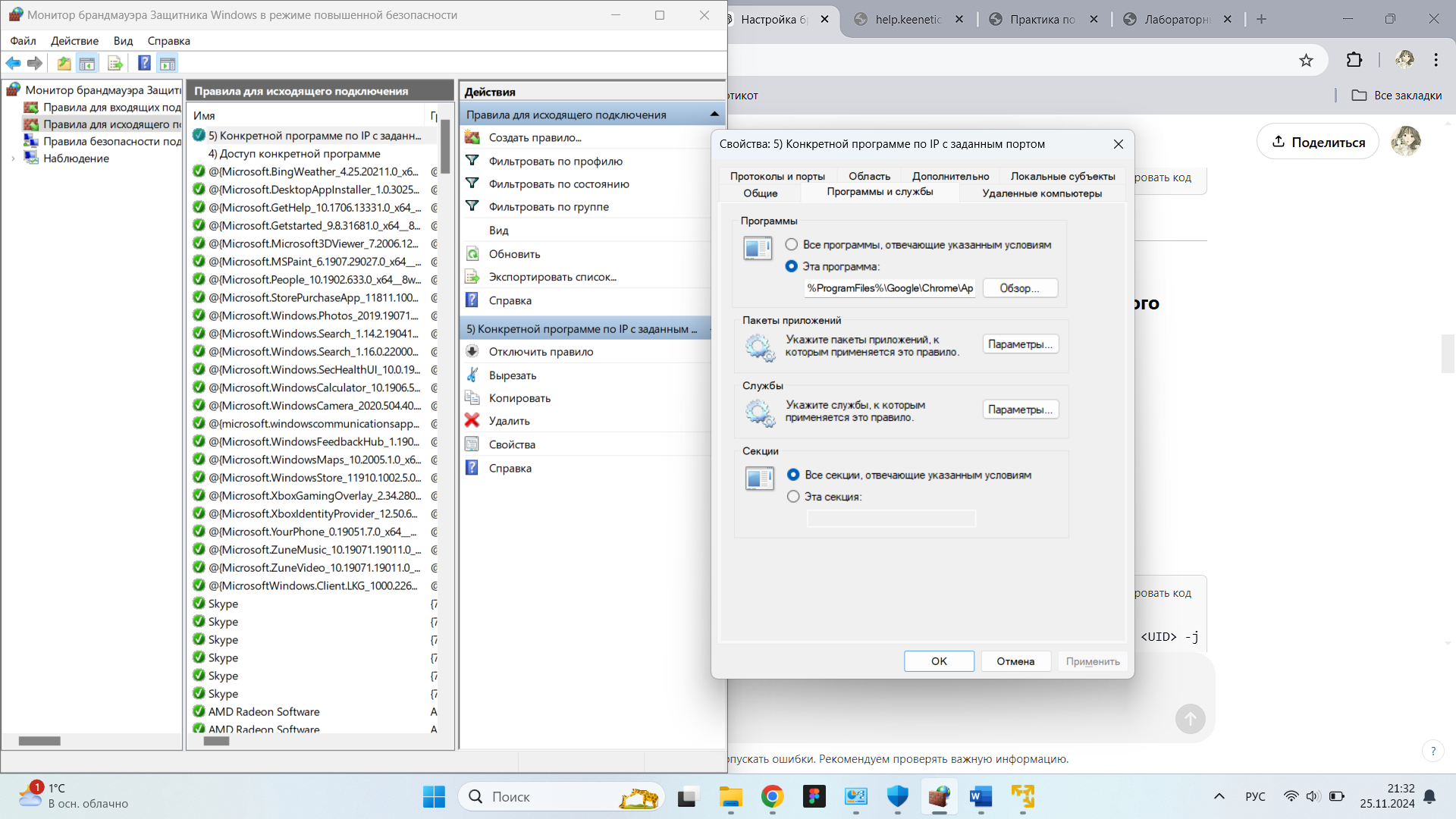
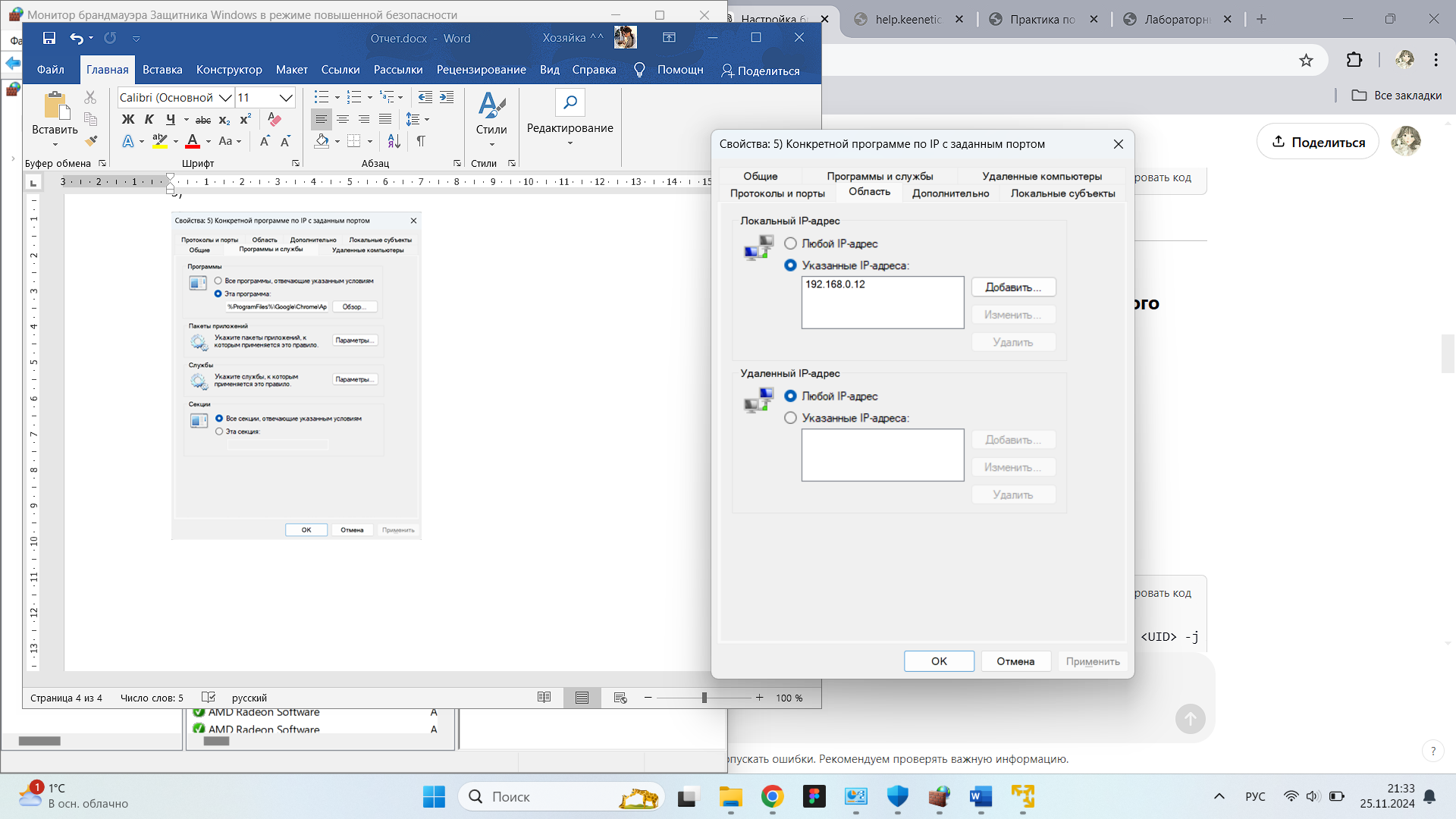


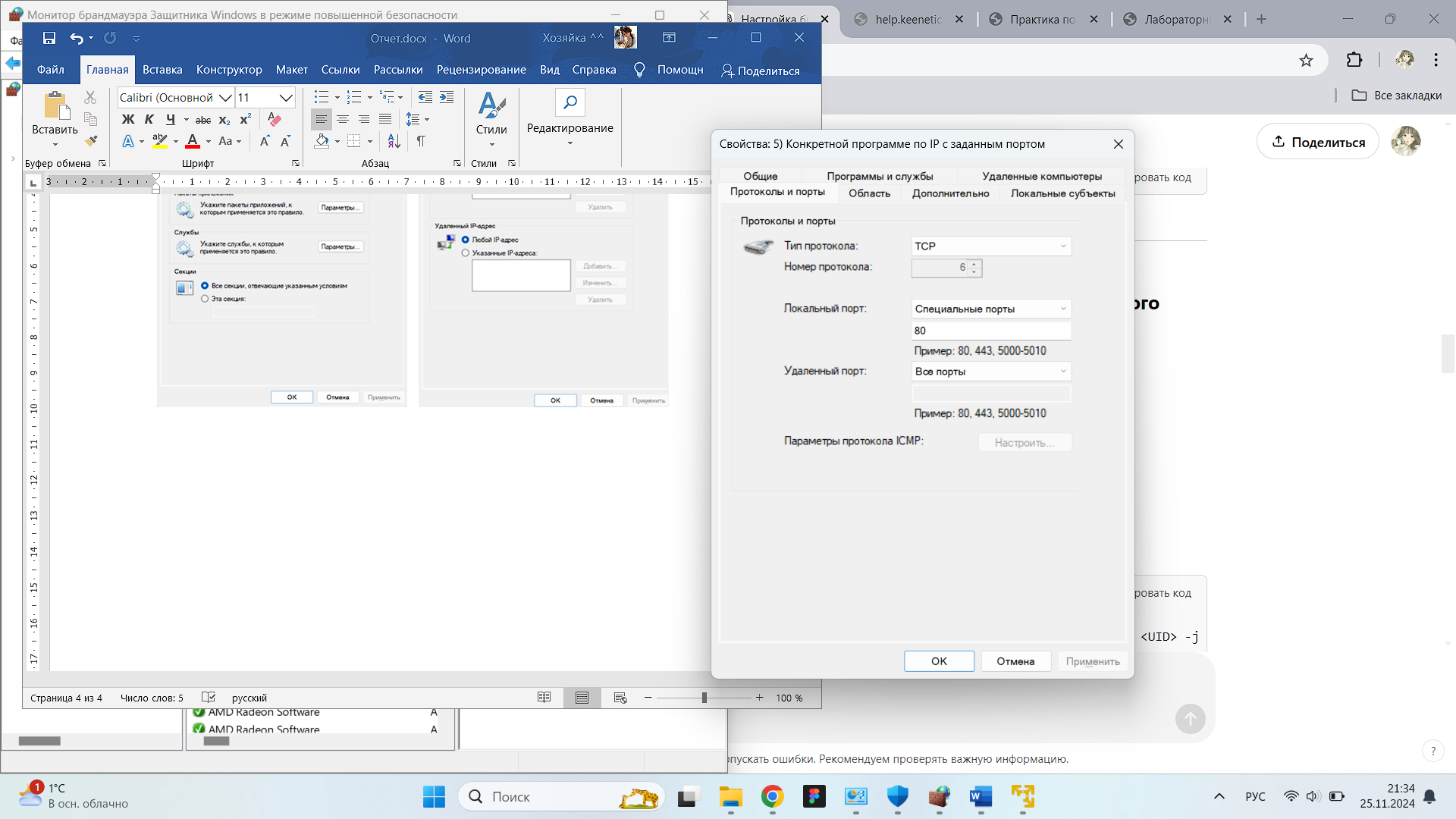
г) доступ к внешним ресурсам разрешен только конкретным программам;



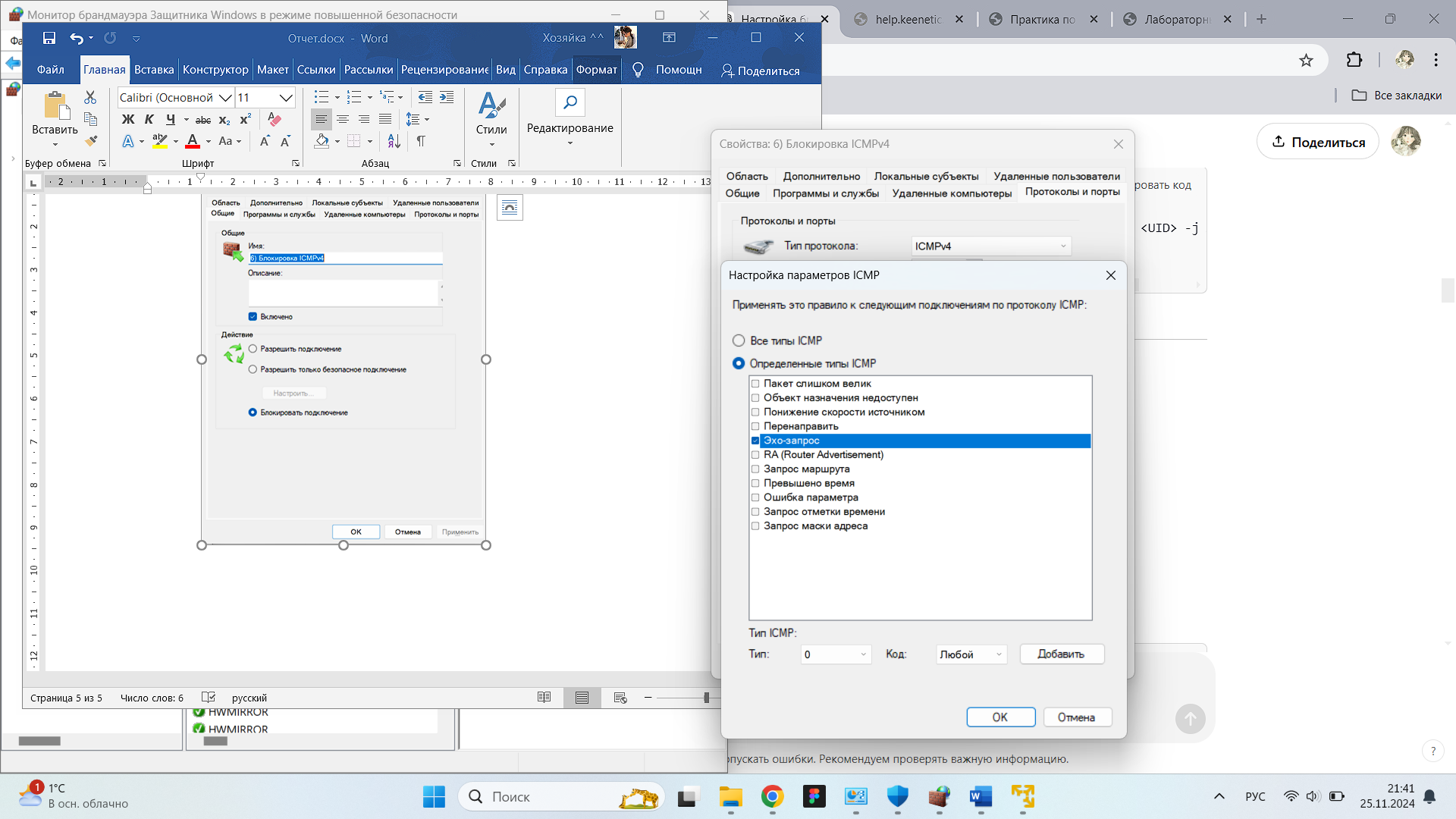
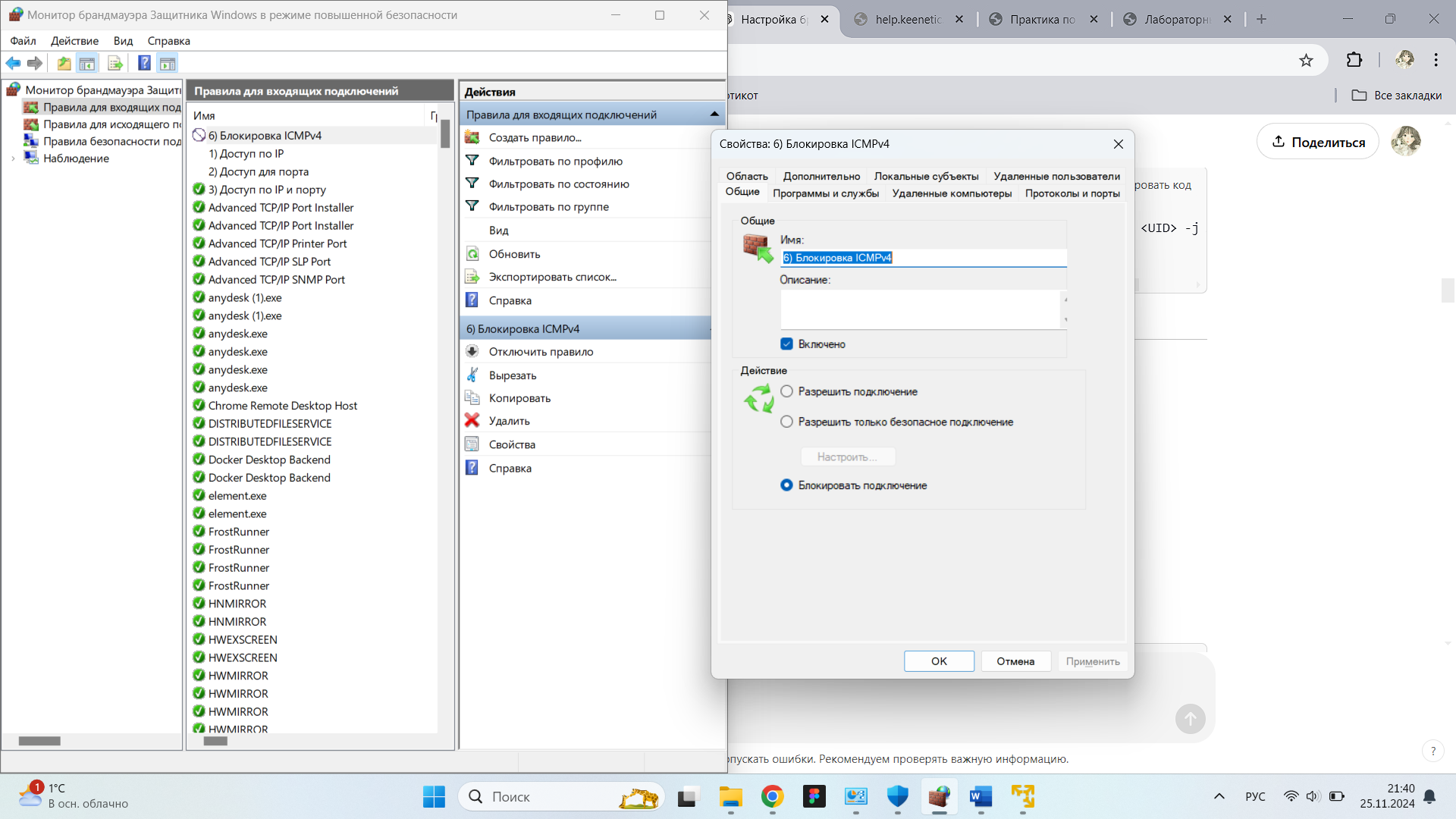
д) конкретной программе разрешен доступ к ресурсам удаленного

компьютера с данным IP-адресом по заданному порту;





е) запретить запрос входящего эха (ICMP).



**Вывод:** в результате выполнения задания были приобретены навыки работы с брандмауэром Защитника Windows, включая создание и применение правил для входящего и исходящего трафика. Кроме того, освоена настройка сетевых соединений в VMware Workstation и взаимодействие виртуальных машин. Работа позволила на практике применить принципы безопасности, создавая эффективные и детализированные политики защиты. Полученные знания и навыки могут быть использованы для защиты ресурсов и предотвращения несанкционированного доступа в реальных условиях.