**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**Лабораторная работа № 2**

на тему «Технологии использования МЭ и СОВ»

|  |
| --- |
| Выполнил: студент группы ВКБ43 |
| Ковалев Данил Петрович |
| (Фамилия, имя, отчество) |
| Проверил: доцент |
| Решетникова Ирина Витальевна |
| (Фамилия, имя, отчество) |

**Цель:** изучить технологии использования средств межсетевого экранирования и систем обнаружения вторжений.

# **Ход работы:**

**Задание 1.** Настроить виртуальные машины для лабораторной работы.

Для создания виртуальных машин в данной лабораторной используется Virtual Box 7.2.0 версии. В качестве ОС используется Windows 10 Pro. Secret Net Studio был установлен с версией 8.1. Созданные виртуальные машины представлены на рисунке 1.

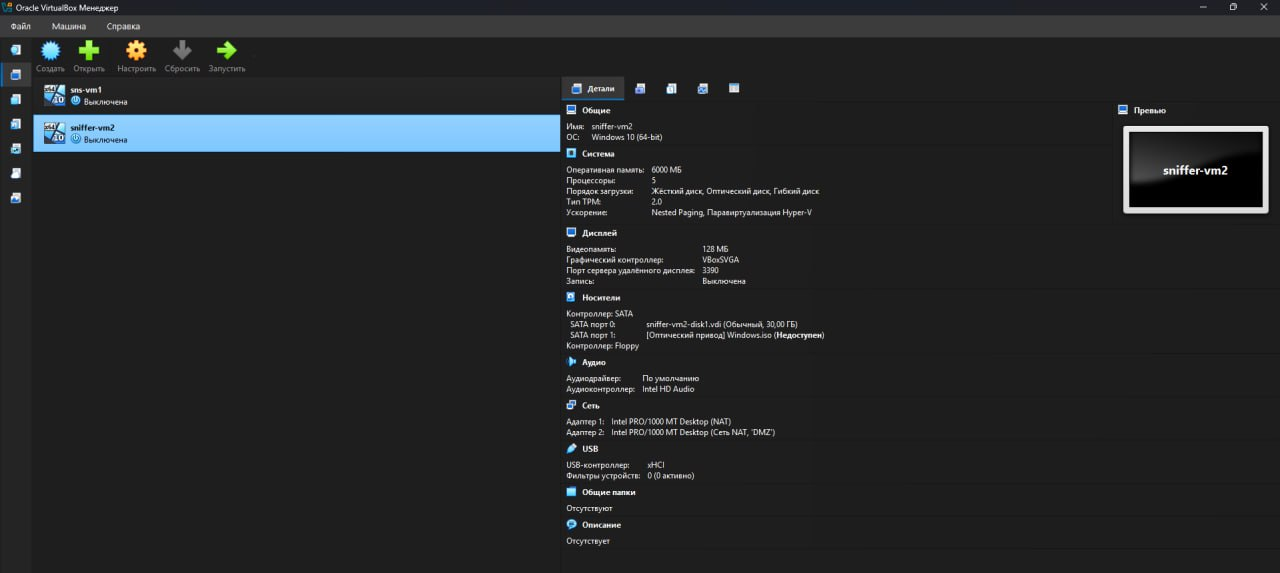


Рисунок 1 – создание виртуальных машин для лабораторной работы

Для настройки взаимодействия виртуальных машин между собой использовался протокол NAT. Присутствует такая проблема, что при стандартном NAT у виртуальных машин выдаются одинаковые адреса для взаимодействия. Чтобы решить данную проблему, нужно создать свою сеть NAT. Для решения данной проблемы была создана сеть с названием “DMZ”, которая представлена на рисунке 2.

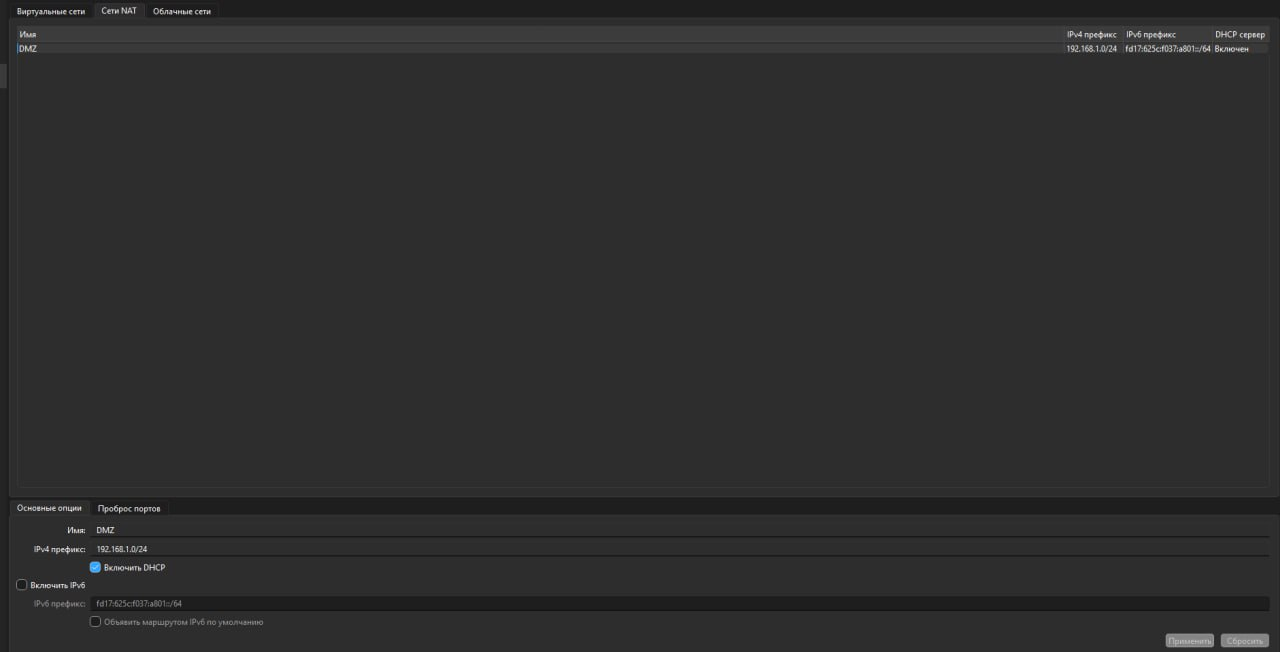


Рисунок 2 – создание сети NAT для взаимодействия виртуальных машин

При установке Secret NET Studio появилась такая надпись, которая представлена на рисунке 3.

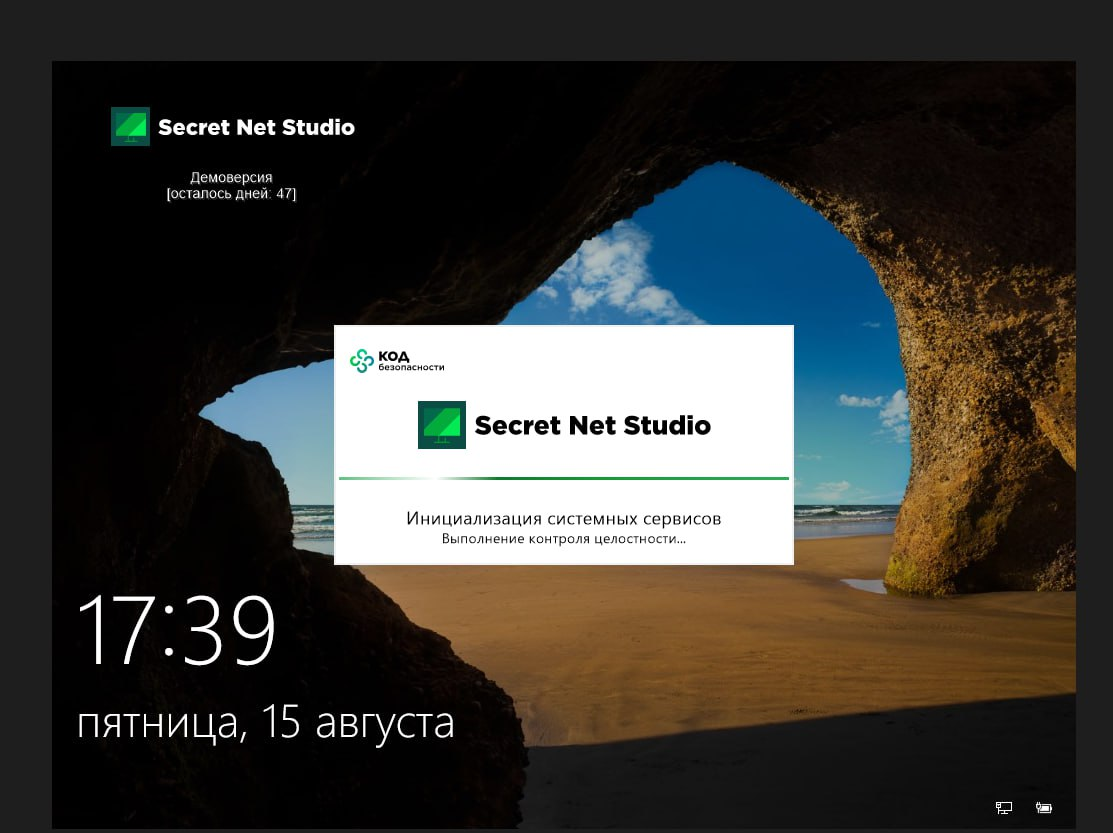


Рисунок 3 – внедрение Secret NET Studio в систему

**Задание 2.** На компьютере VM1 с установленным клиентом Secret Net Studio сделайте следующее: установите разрешение подключения к данному компьютеру через удаленный рабочий стол (RDP); Создайте на локальном диске папку с произвольным наименованием, например, “user\_files” и в ОС Windows настройте для нее общий доступ с максимальным разрешениями; с компьютера VM2 убедитесь, что подключение к компьютеру VM1 через удаленный рабочий стол и обращение к общей папке (“user\_files”) возможны.

Для выполнения задания нужно настроить соответственно операционные системы на поддержку RDP подключений. Для реализации данного пункта нужно пройти в Пуск -> Настройки -> Обновления и безопасность -> Для разработчиков -> Удаленное подключение -> Показать параметры. После проделанного пути были выбраны параметры, которые представлены на рисунке 4. Данные параметры были проставлены и на SNS-VM1, и на SNIFFER-VM2.

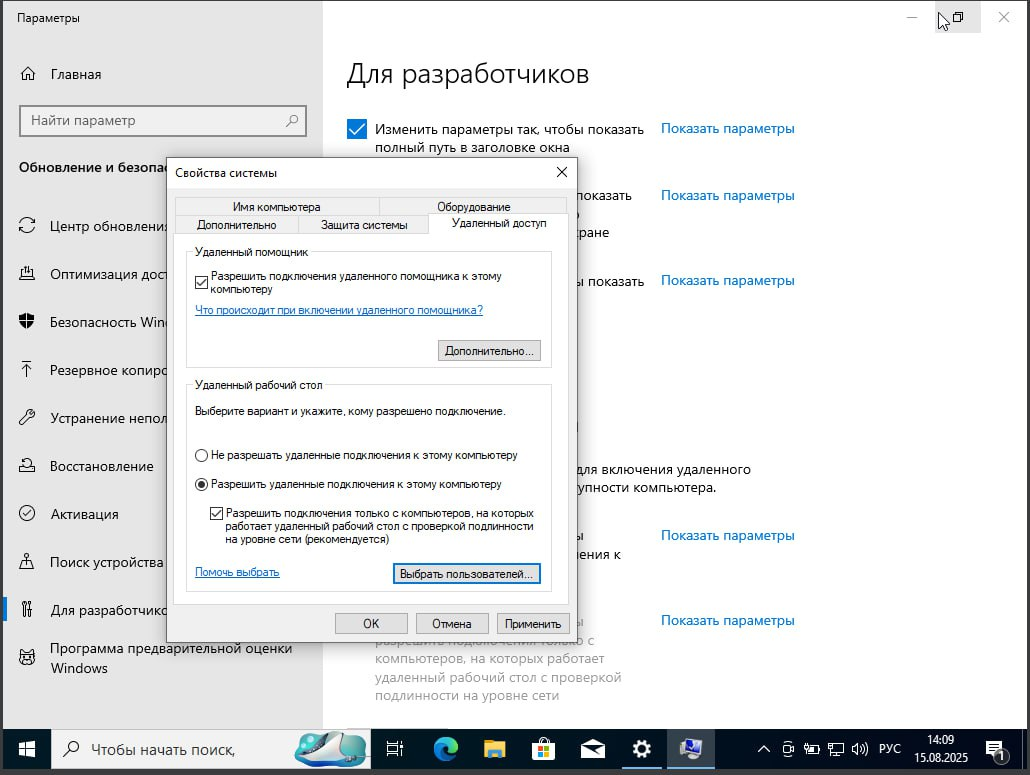


Рисунок 4 – параметры для настройки RDP в Windows 10

На рабочем столе была создана папка с названием “user\_files” (в дальнейшем для тестов была переименована в “user\_directories”), были выставлены параметры для публичного подключения для всех. Данное действие было реализовано через параметр “Свойство” и директории. Результат представлен на рисунке 5.



Рисунок 5 – директория доступна в публичном доступе

При попытке обращения через “Проводник” файл полностью виден и доступен, результат представлен на рисунке 6.

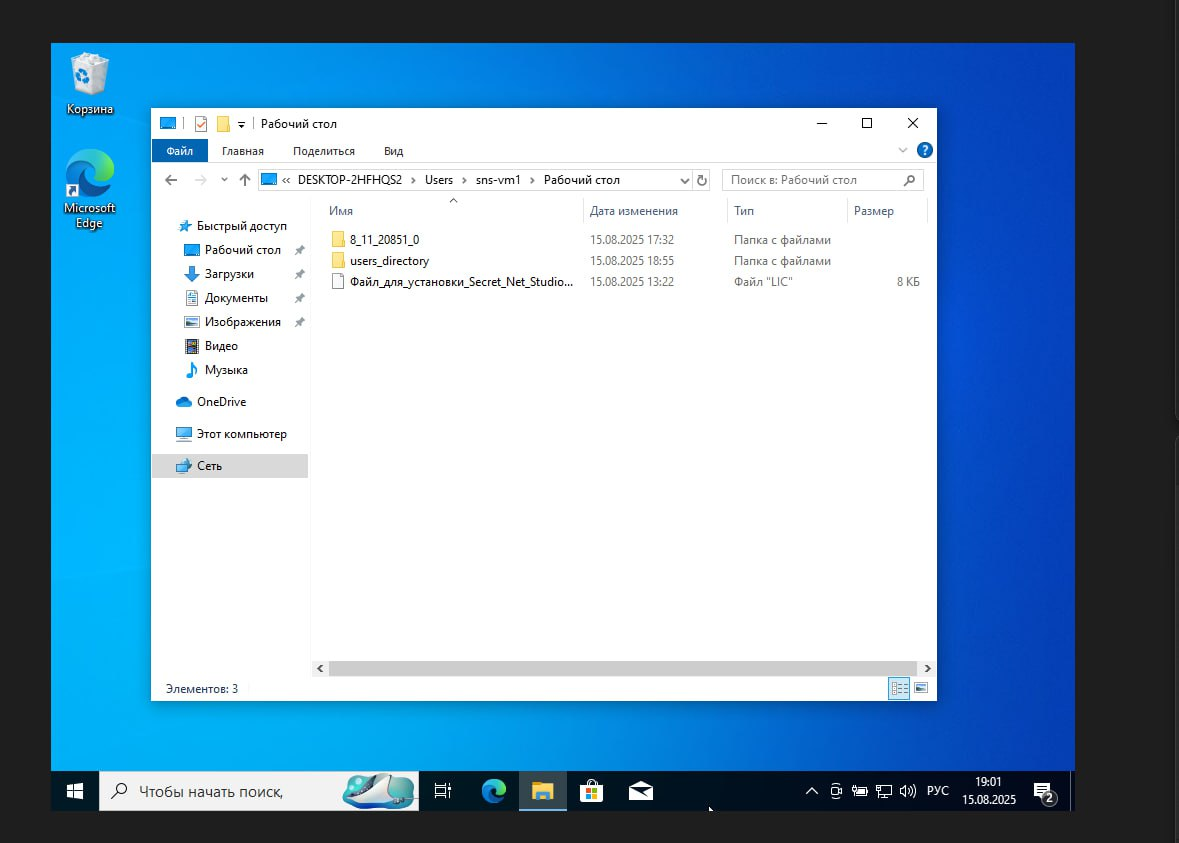


Рисунок 6 – результат проверки видимости директории с SNS-SNIFFER на SNS-VM1

**Задание 3.** Добавьте запрещающие правила: правило доступа, запрещающее доступ к VM1 (192.168.101.11) по протоколу RDP всем портам для всех пользователей и IP адресов. Активируйте механизм ICMP-защиты с настройками по умолчанию.

Для реализации данного нужно выполнить шаги, которые представлены в методичке. В параметре “Персональный межсетевой экран” нужно добавить новый фильтр. Шаги представлены на рисунках 7, 8, 9, 10.

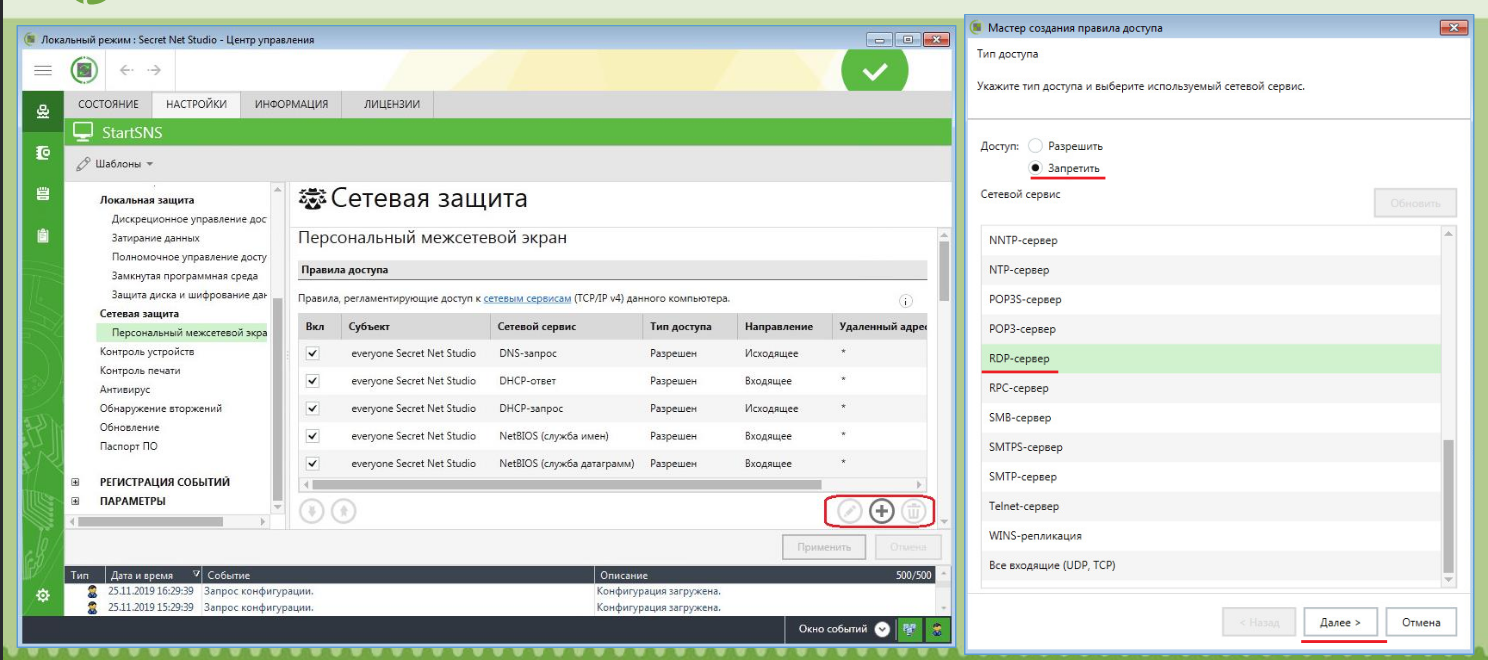


Рисунок 7 – первый шаг для создания фильтра

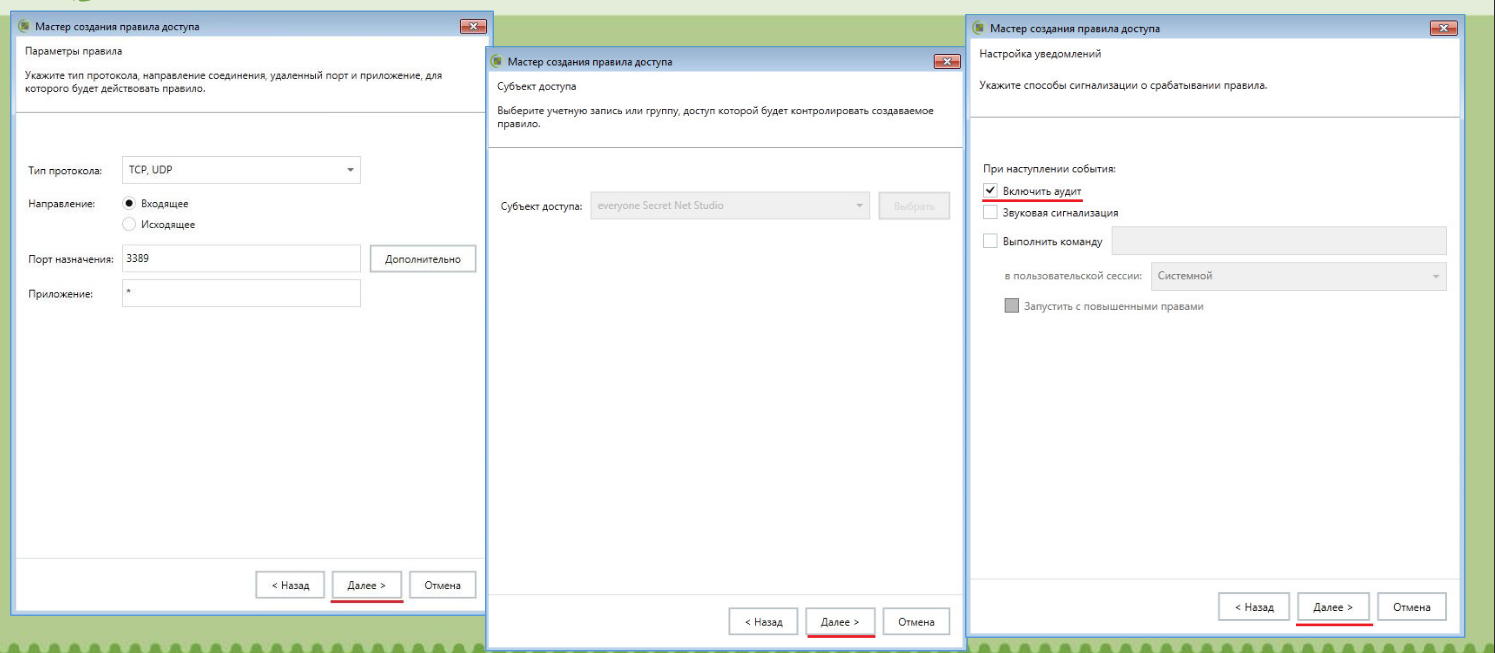


Рисунок 8 – второй шаг для создания фильтра

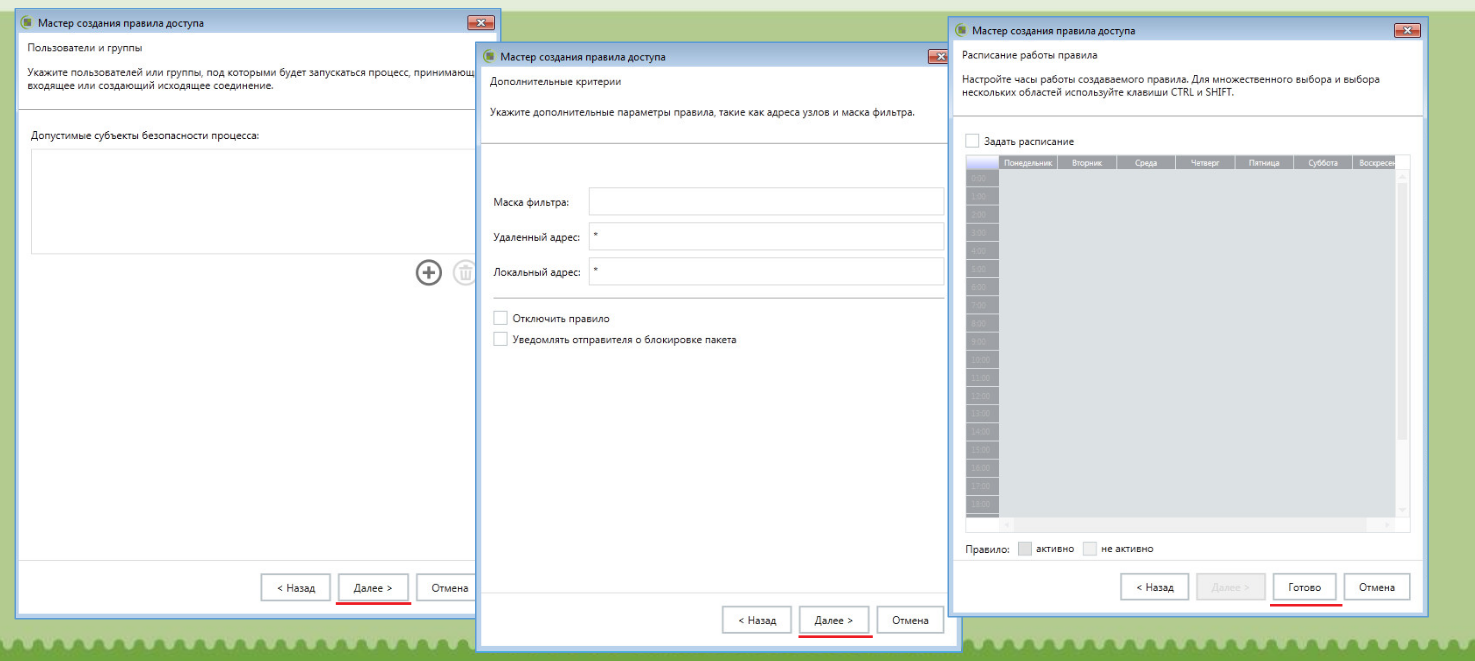


Рисунок 9 – третий шаг для создания фильтра

В результате настроек должно выйти то, что представлено на рисунке 10. Был создан новый фильтр для подключения через RDP.

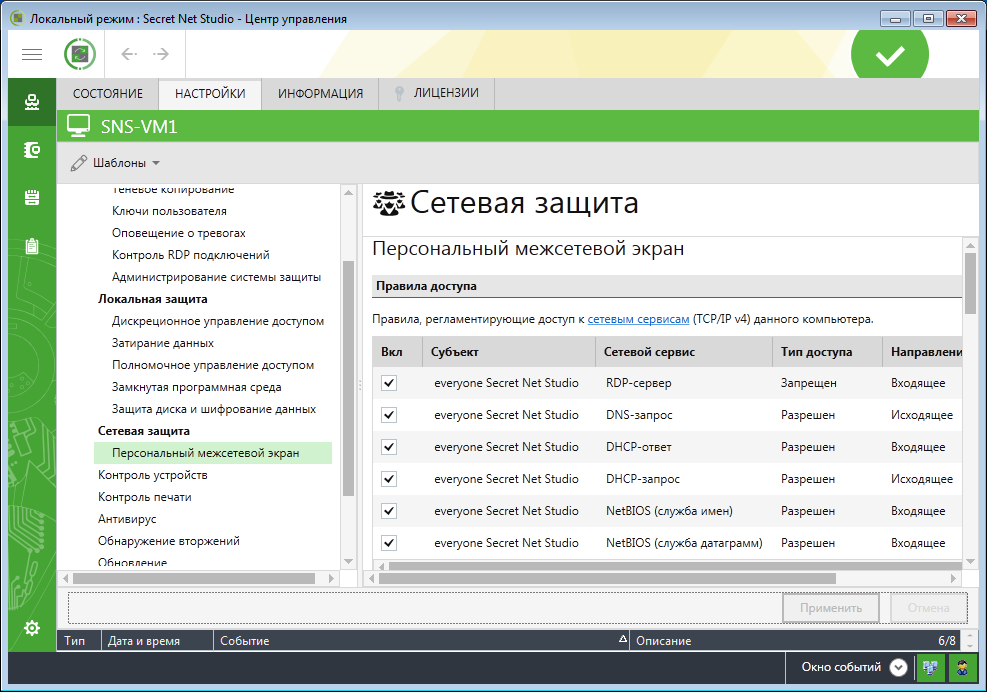


Рисунок 10 – новый фильтр для RDP-сервера

Для создания ICMP защиты был нажат просто флажок, который сам выставляет уже заготовленные значения по умолчанию, результат представлен на рисунке 11.

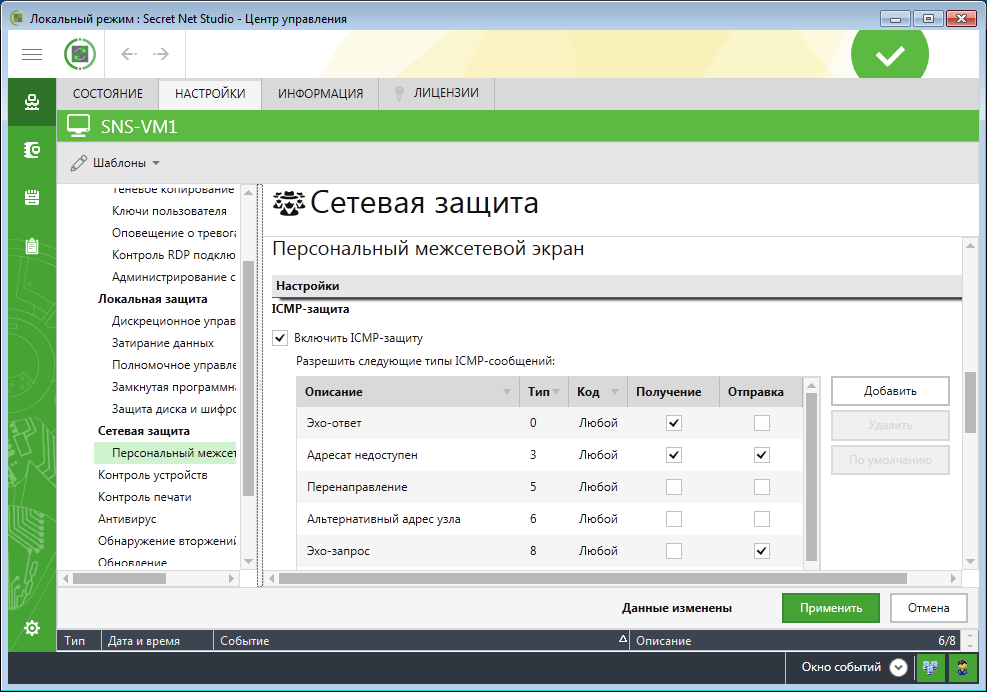


Рисунок 11- параметры для ICMP-защиты

При попытке подключения через RDP происходит ошибка, которая представлена ниже на рисунке 12, что свидетельствует о том, что защита настроена корректно и все работает.

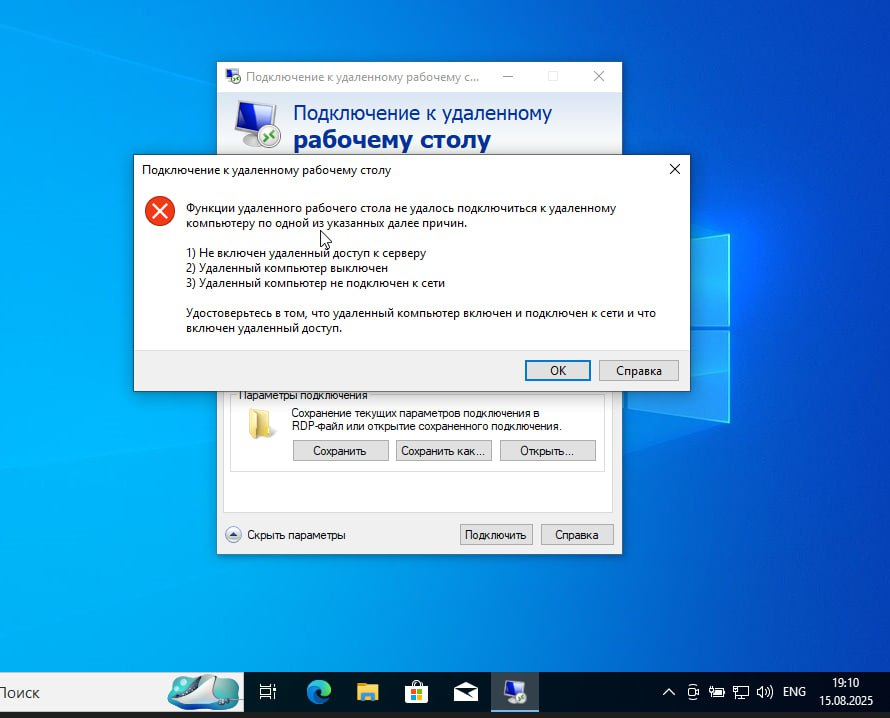


Рисунок 12 – попытка подключения к VM1, используя RDP

При попытке выполнить ping все пакеты в нашем случае не проходят, что говорит нам о корректной настройке. Результат представлен на рисунке 13.

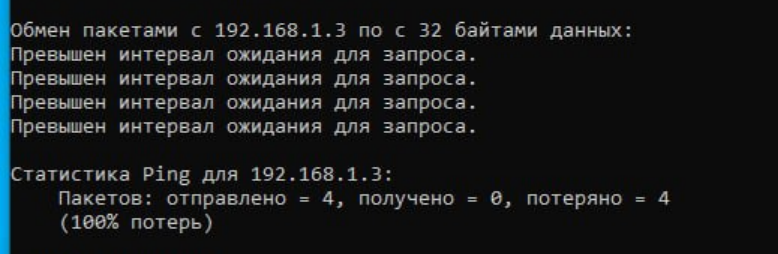


Рисунок 13 – пинг при запросе

**Задание 4.** Добавить следующие правила: системное правило, разрешающие доступ к VM1 (192.168.101.11) по протоколу ICMP для всех пользователей c IP-адреса 192.168.101.22 (с VM2); прикладное правило, запрещающее доступ к общедоступной папке "user\_files" на ВМ VM1 (192.168.101.11) с любого компьютера. При этом активируйте опцию добавления соответствующего правила доступа, разрешающего прохождение пакетов по протоколу TCP на порт 445 (и/или 139);

Зададим теперь правила, которые представлены на рисунке 14. Здесь у нас разрешается теперь получать ICMP пакеты с хоста, а также запрещается доступ к директории. Важно отметить, что данный блок не работает, если пробовать подключиться через протокол SMB. Данное поведение неизвестно почему происходит.

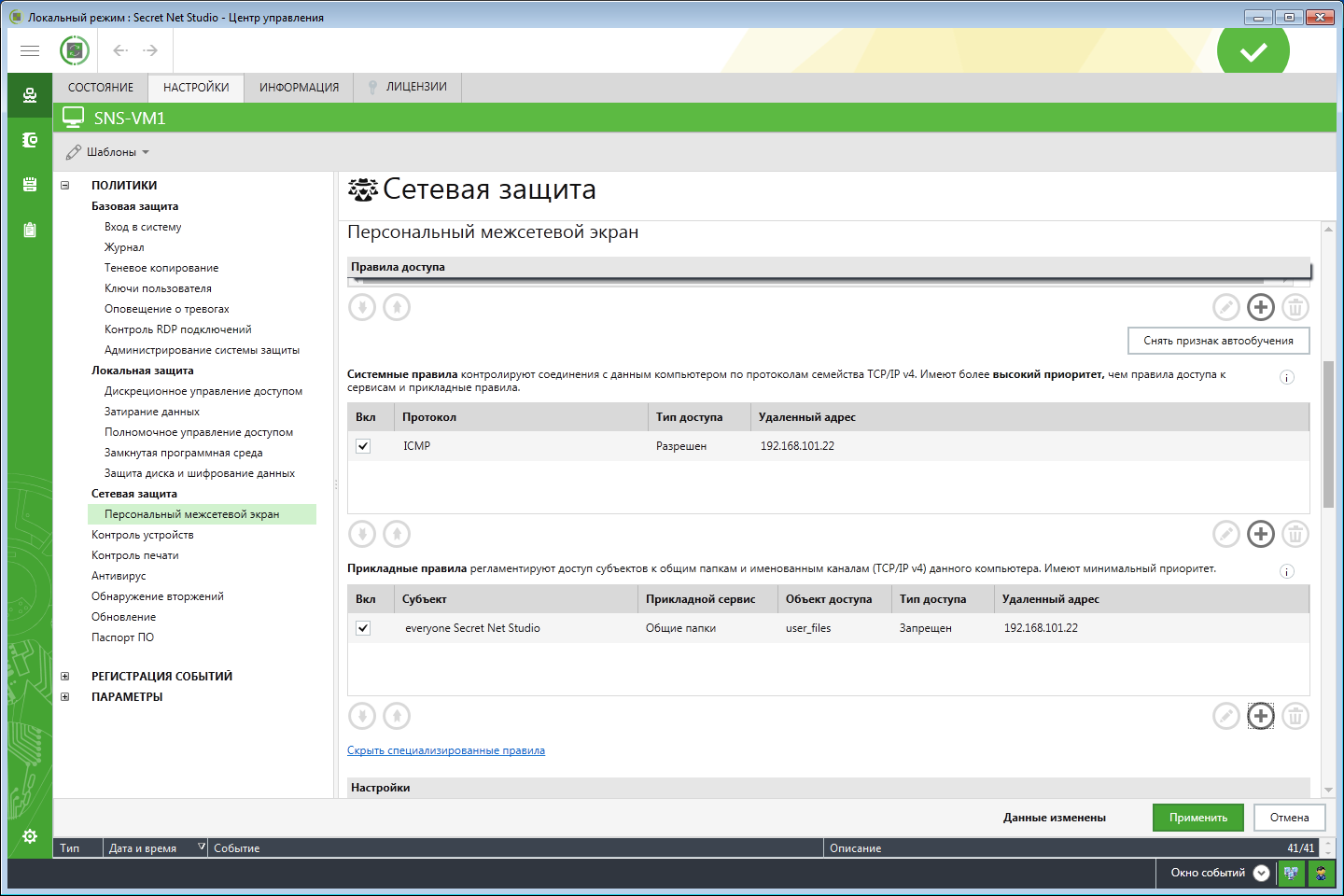


Рисунок 14 – настройки ICMP пакетов и директории

Попробуем теперь выполнить команду “ping”, после наших правил теперь все ICMP пакеты проходят. Результат представлен на рисунке 15.



Рисунок 15 – пинг, когда разрешили пакеты

Если изначально обратиться к директории через RDP протокол, то нам выдаст ошибку о том, что данные файлы не доступны, результат представлен на рисунке 16.

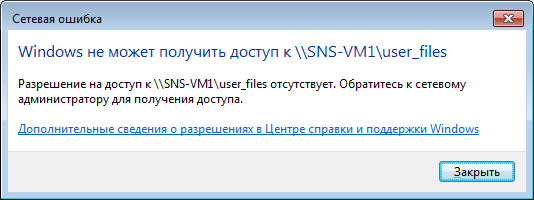


Рисунок 16 – запрет к доступу по RDP

**Задание 5.** Проведите настройку СОВ на клиенте SNS, установленном на VM1, применив следующие политики: "Включить детекторы атак" – установите флажок; "Блокировка атакующего хоста…" – оставьте отмеченным, "Время блокировки" – 1 минута; "Использовать черный список IP-адресов" – оставьте отмеченным (параметр по умолчанию активен для всех детекторов). В этом случае будут заблокированы вредоносные IP-адреса из базы опасных веб-ресурсов Kaspersky;

Проставим теперь параметры, как требуется в лабораторной работе. Для начала выберем параметр “детекторы атак” и проставим все данные, как сказано в методическом материале для лабораторной работы. Результат представлен на рисунке 17.

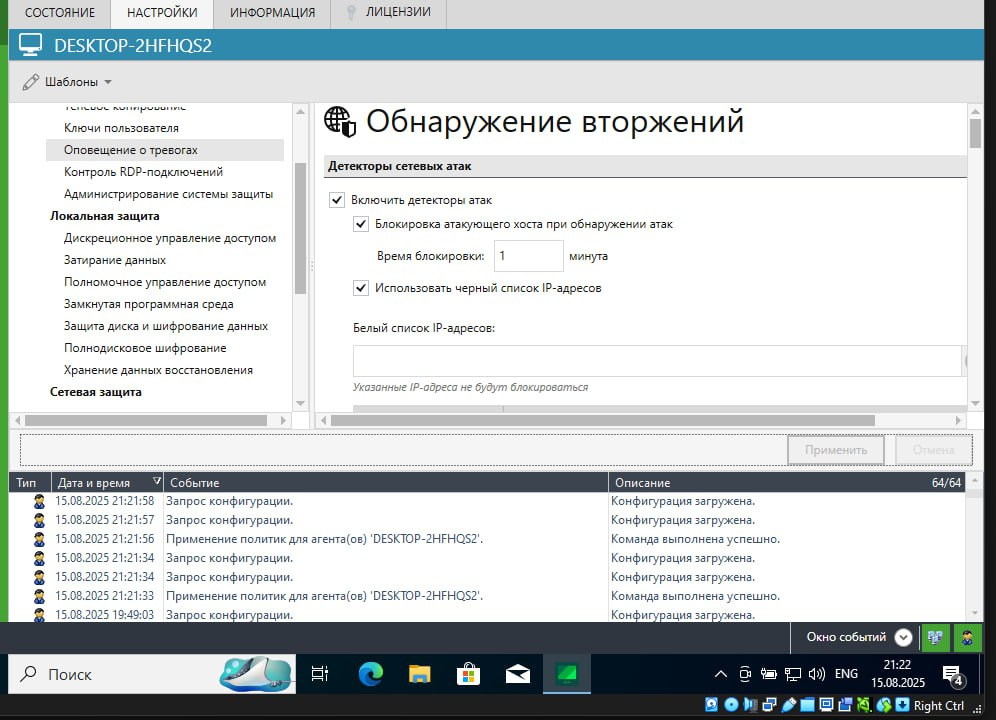


Рисунок 17 – флажок “Включить детекторы атак”

Теперь включим параметр защиты от сканирования портов, как описано в методическом материале для лабораторной работы. Результат представлен на рисунке 18.

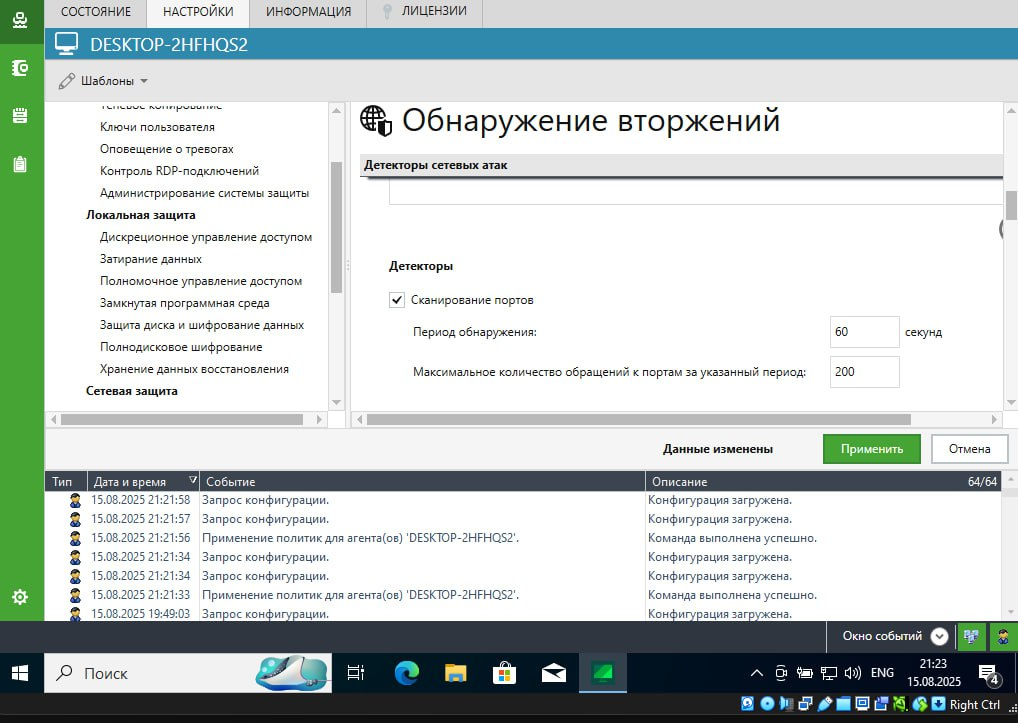


Рисунок 18 – включение параметра защиты от сканирования портов

Выставим теперь параметры для логирования происходящих инцидентов. Все параметры были выбраны, как указано в методическом материале. Результат представлен на рисунке 19.

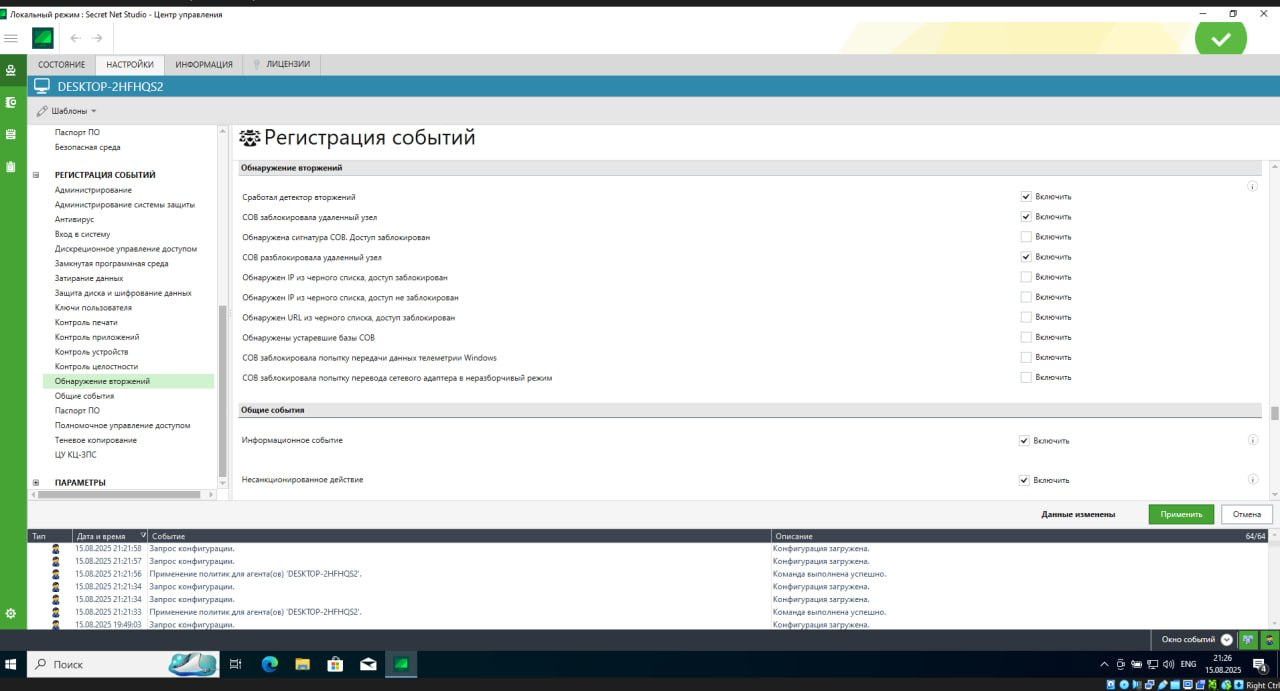


Рисунок 19 – включение логирования событий

**Задание 6.** Перейдите в консоль ВМ VM2 и проведите сканирование портов компьютера VM1 с помощью команды: nmap -T5 -PN 192.168.101.11. С помощью утилиты ping проверьте доступность компьютера VM1 (192.168.101.11) и убедитесь, что эхо-ответы не приходят.

Команда для “nmap”, представленная в методическом материале является неактуальной на данный момент. В следствии этого используется иная команда для тестирования функционала по блокировке данных. Результат представлен на рисунке 20.

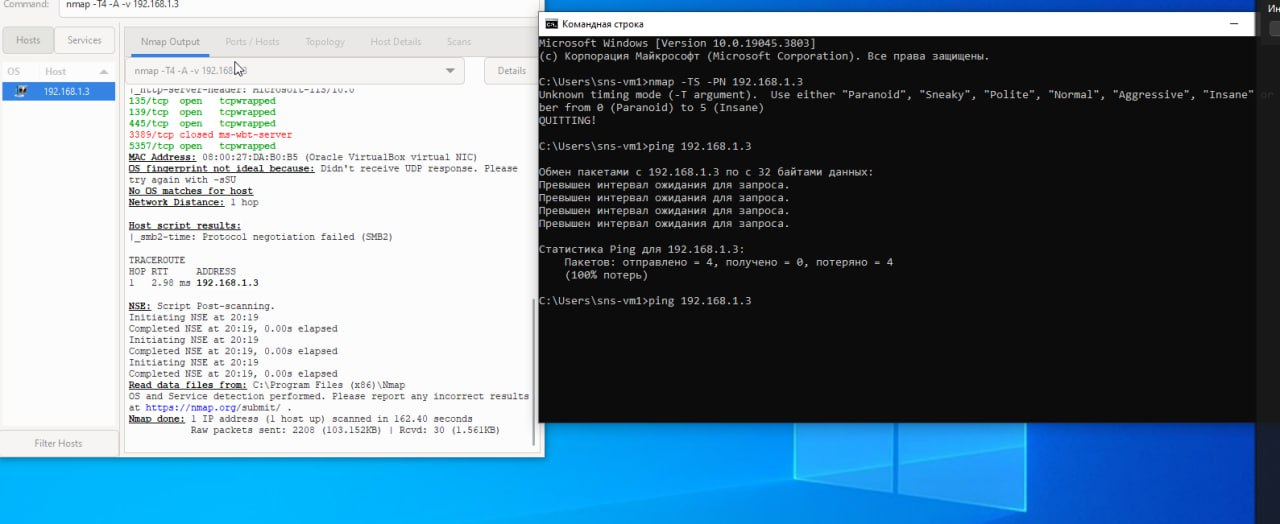


Рисунок 20 – блок машины

Теперь посмотрим какая информация у нас есть в логах. Результат представлен на рисунке 21.

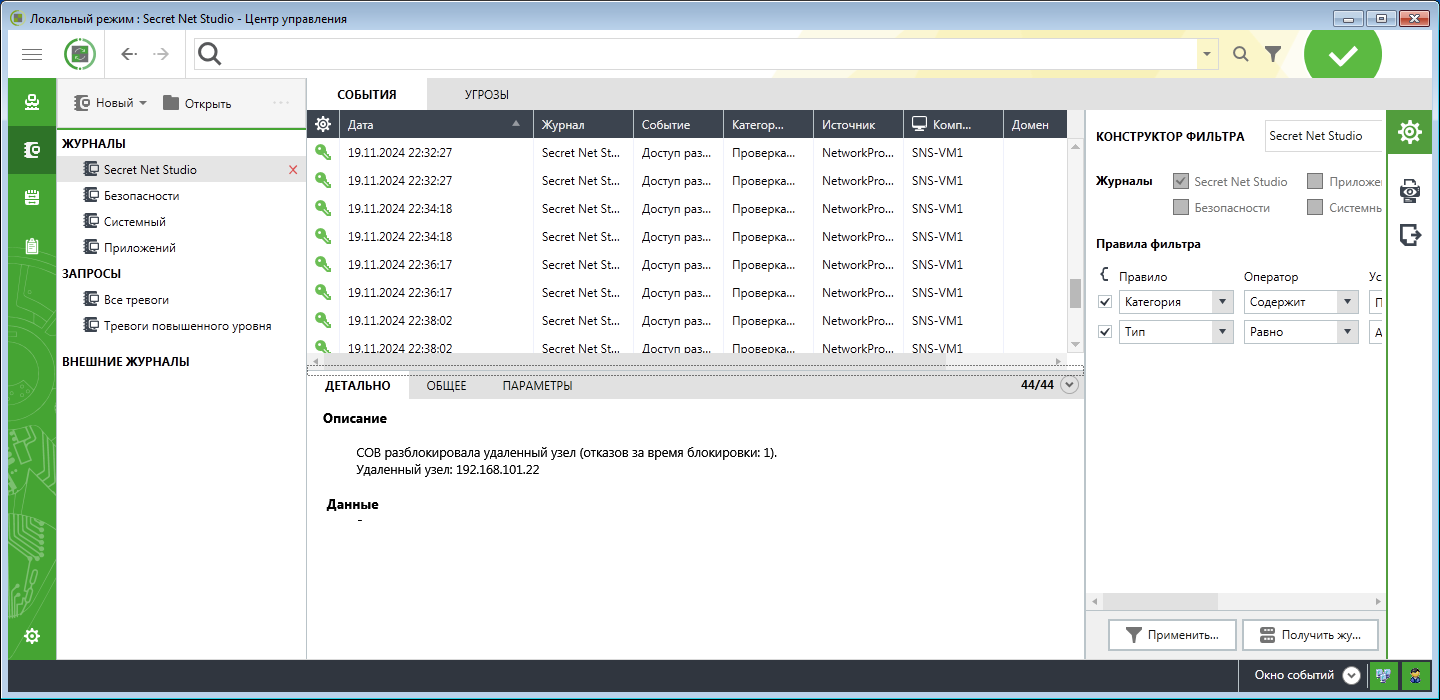


Рисунок 21 – логи от попытки доступа к машине