НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет информационных технологий

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) Программная инженерия и компьютерные науки

Предмет: Защита информации

Лабораторная работа № 1

Тема: **Средства безопасности в Windows 7**

Выполнил, гр 20209 Княжев М.А.  
Преподаватель Перов А.А.

Новосибирск  
2023

**Цель лабораторной работы**

Цель работы – ознакомиться с функциями безопасности Windows 7, улучшениями и приложениями.

**Задание:**

1. создать двух новых пользователей;

2. создать две группы безопасности, включить каждого пользователя в свою группу;

3. создать 4 каталога со следующими правами:

каталог1: только чтение для пользователя1, чтение, создание и изменение файлов для пользователя2;

каталог2: нет доступа для пользователя1, только чтение для пользователя2;

каталог3: только чтение для группы1, только чтение для группы2;

каталог4: полный доступ для группы1, создание и изменение файлов для группы2;

4. создать шаблон безопасности системы, указав параметры:

Политики учетных записей>Политики паролей>Вести журнал паролей [1 сохраненный пароль]

Политики учетных записей>Политики паролей>Минимальная длина пароля [7 знаков]

Политики учетных записей>Политики паролей>Пароль должен отвечать требованиям сложности [Включен]

Политики учетных записей>Политики блокировки учетной записи>Пороговое значение блокировки [3 ошибок входа в систему]

Локальные политики>Политики аудита>Аудит входа в систему [Успех, Отказ]

Локальные политики>Политики аудита>Аудит доступа к объектам [Успех, Отказ]

Локальные политики>Политики аудита>Аудит событий входа в систему [Успех, Отказ]

Локальные политики>Политики аудита>Аудит управления учетными записями[Успех, Отказ]

5. провести анализ параметров безопасности системы по заданному шаблону; выявить различия между шаблоном и существующими параметрами;

6. произвести настройку параметров безопасности по заданному шаблону;

7. работа с журналом безопасности и настроенными параметрами безопасности:

назначить или изменить пароль пользователя в соответствии с требованиями сложности локальной политики безопасности; найти связанное с этим событие в журнале безопасности операционной системы;

назначить или изменить пароль пользователя с нарушениями требований сложности локальной политики безопасности; найти связанное с этим событие в журнале безопасности операционной системы; произвести вход в систему под учетной записью пользователя с ошибочными данными (неправильным паролем); найти связанное с этим событие в журнале безопасности операционной системы; произвести вход в систему под учетной записью пользователя верными данными; найти связанное с этим событие в журнале безопасности операционной системы;

8. настроить следующие правила в брандмауэре Windows:

запрет исходящего трафика для подключения к сайтам (html-страницам); запрет входящего трафика для удалённого подключения к рабочей станции по протоколу RDP (утилита mstsc); проверить доступ к сайтам до и после установки правил; проверить доступ к машине по протоколу RDP до и после установки правил;

9. настроить параметры управления учетными записями пользователей на уведомление при любом изменении параметров Windows пользователями;

параметры управления учетными записями находятся в: Панель управления > Учетные записи пользователей>Изменение параметров контроля учетных записей; проверить правильность настройки можно открыв диалог «управление компьютером» из контекстного меню «моего компьютера»;

10. с помощью инструмента «Архивация и восстановление» выполнить архивацию(резервное копирование) любого каталога с файлами;

**Выполнение лабораторной работы:**

**Пункт 1:**

Открываем пуск, выбираем панель управления, в просмотре ставим категория, после чего открываем учетные записи пользователей, открываем управление другой учетной записью и создаем двух пользователей: Пользователь1, Пользователь2. Результат представлен на рисунке 1

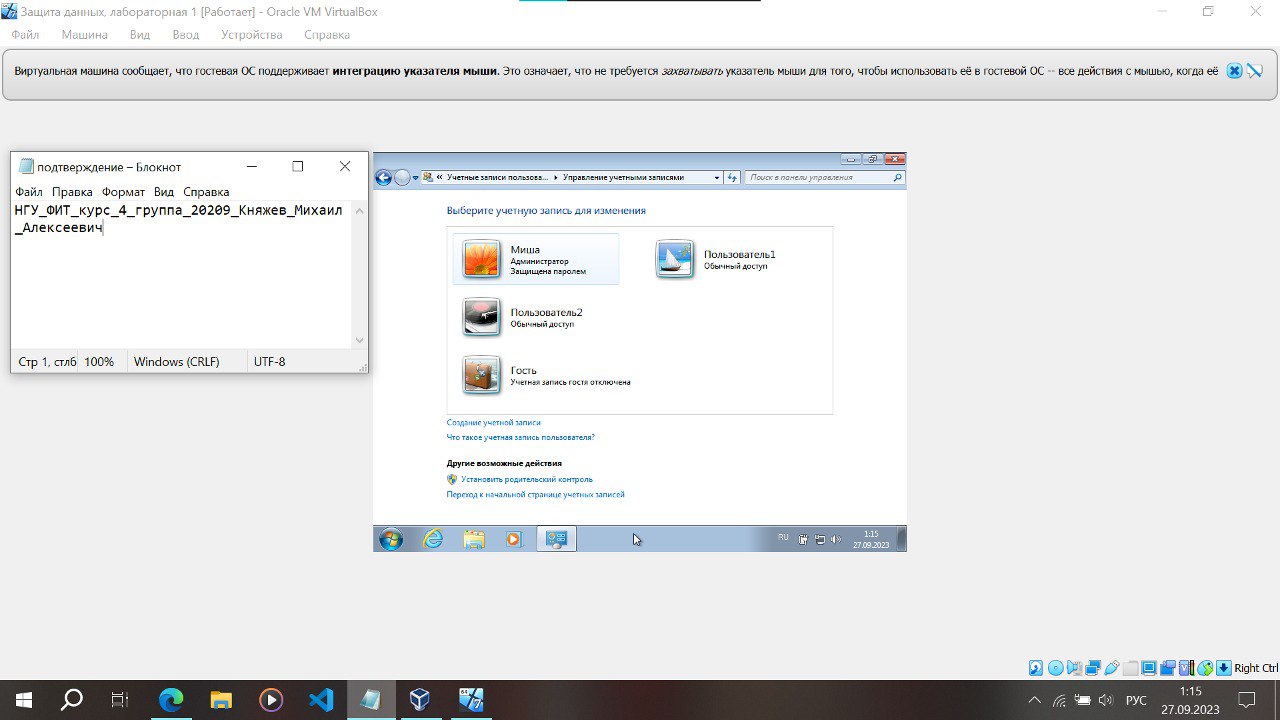


Рисунок 1

**Пункт 2:**

Открываем пуск, правой кнопкой мыши по моему компьютеру, выбираем управление, после чего переходим в локальный пользователи, там открываем вкладку группы и создаем 2 группы: Группа1, Группа2. Результат представлен на рисунке 2, 3.

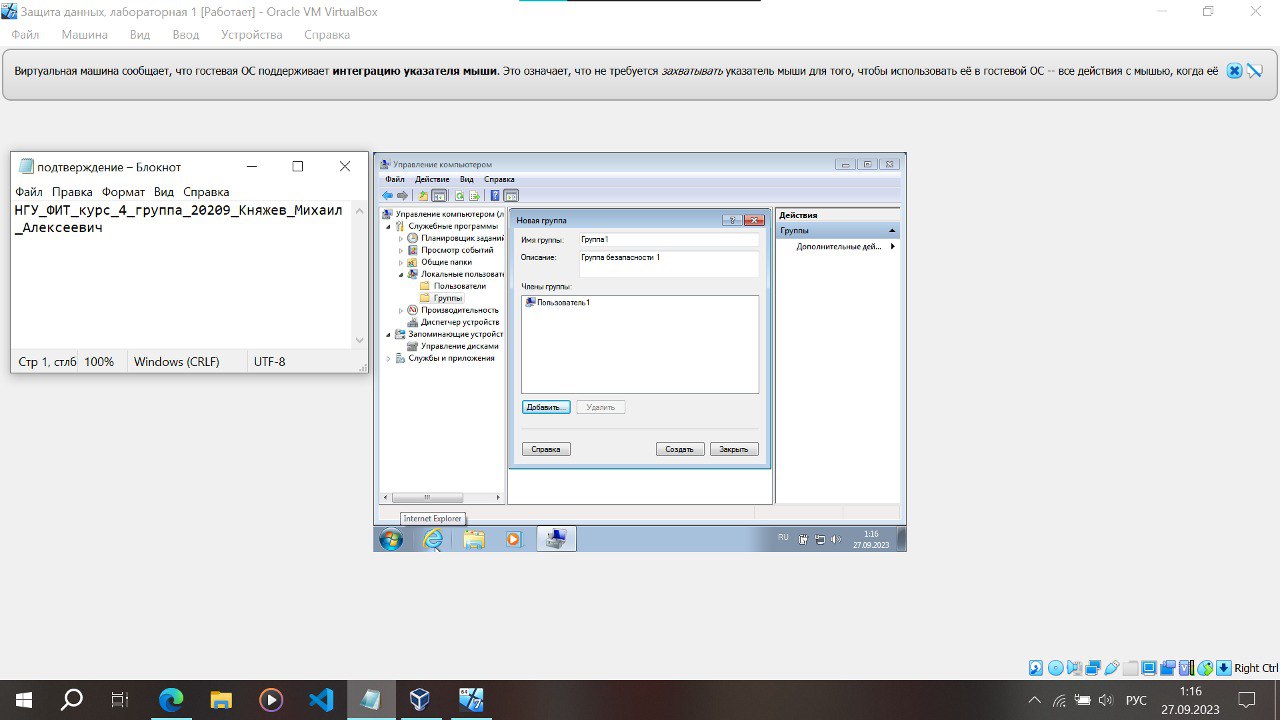


Рисунок 2

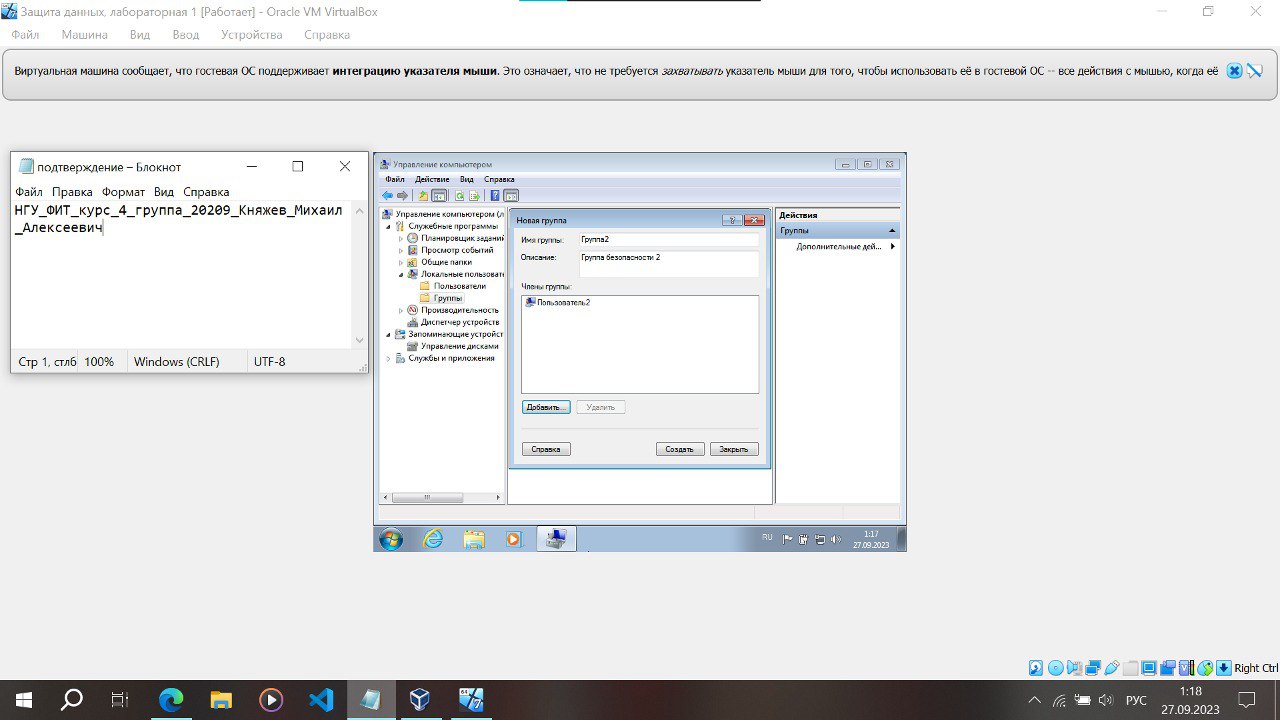


Рисунок 3

**Пункт 3:**

Создаем каталог1, правой кликаем по каталогу, открываем свойства, переходим на вкладку безопасность, выставляем нужные требования. Результат представлен на рисунке 4, 5.

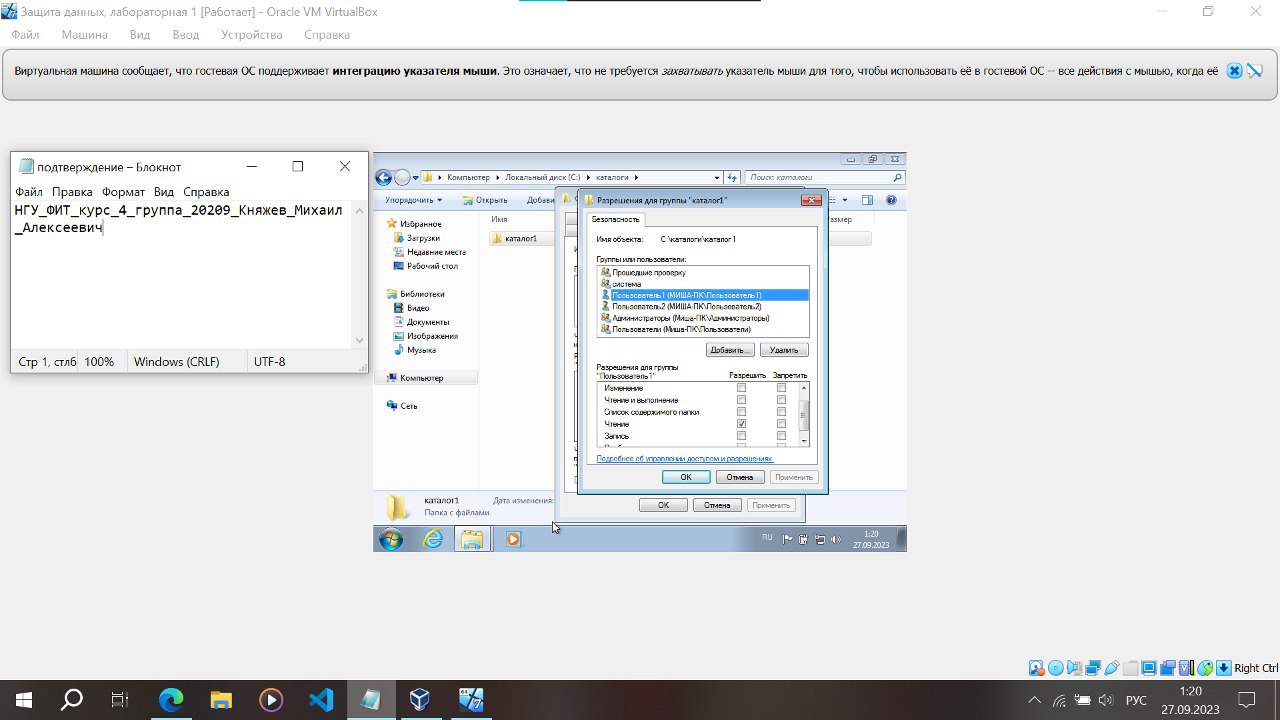


Рисунок 4

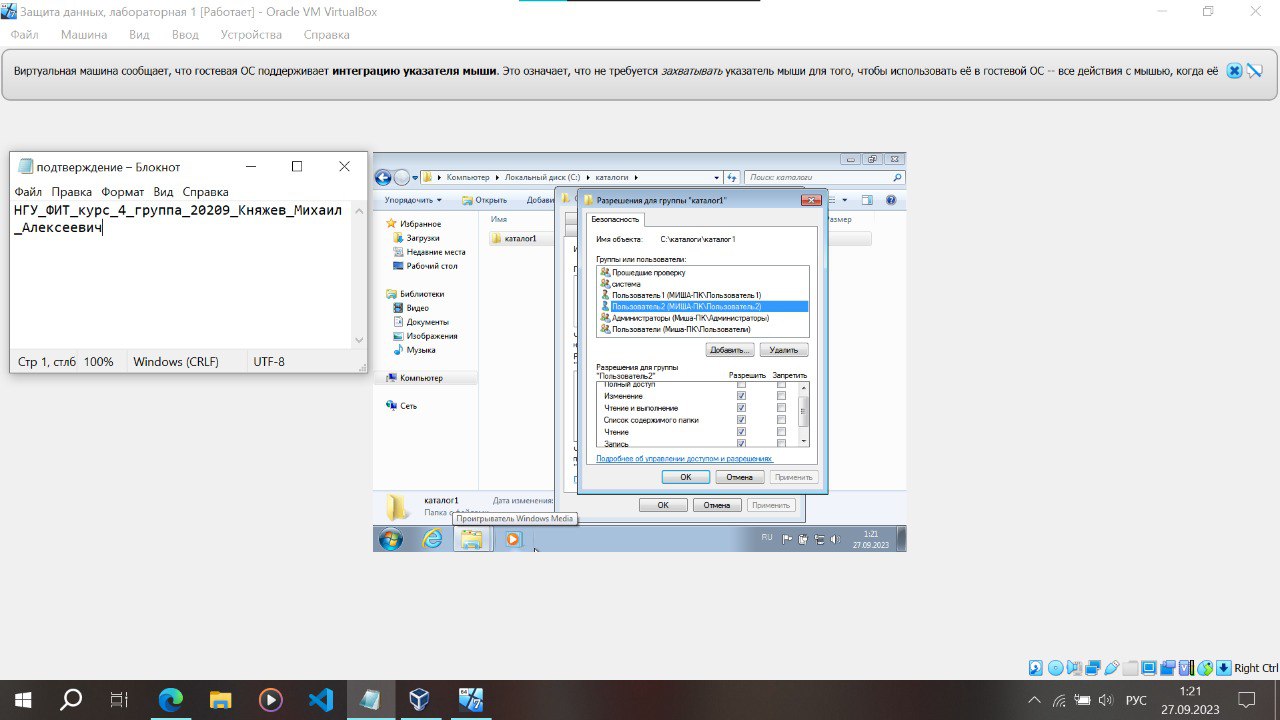


Рисунок 5

Создаем каталог2, правой кликаем по каталогу, открываем свойства, переходим на вкладку безопасность, выставляем нужные требования. Результат представлен на рисунке 6, 7.

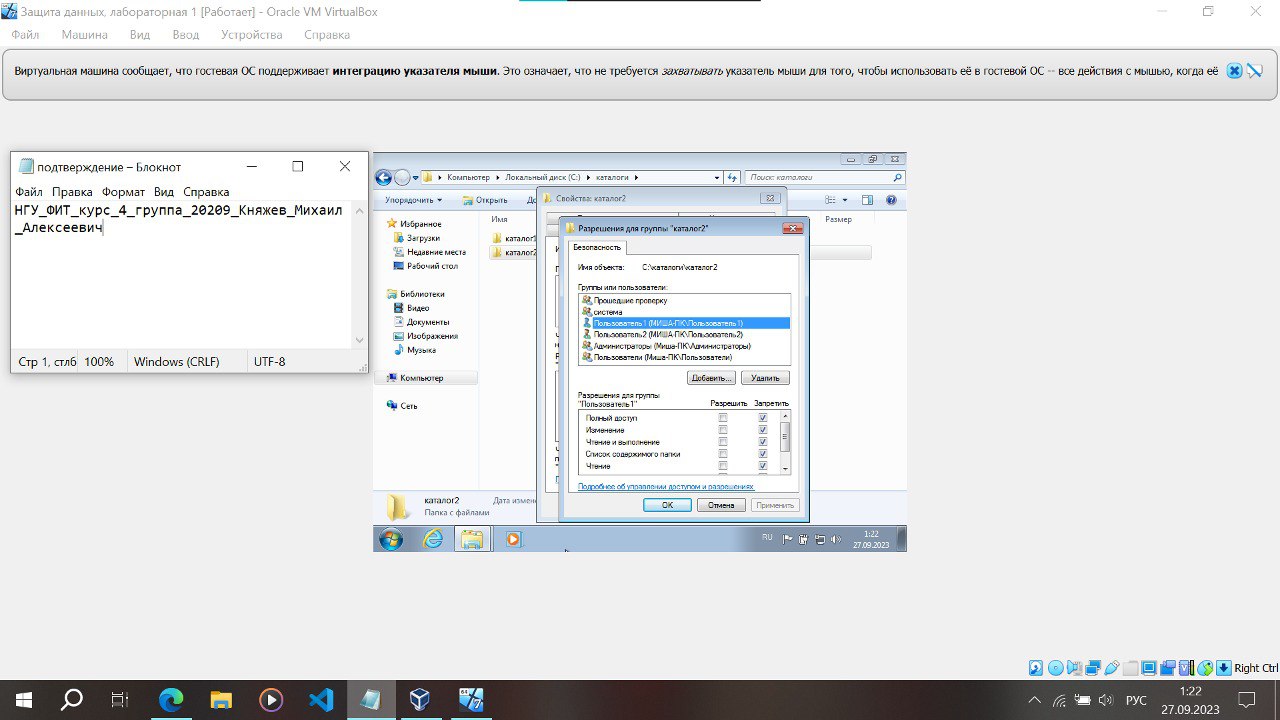


Рисунок 6

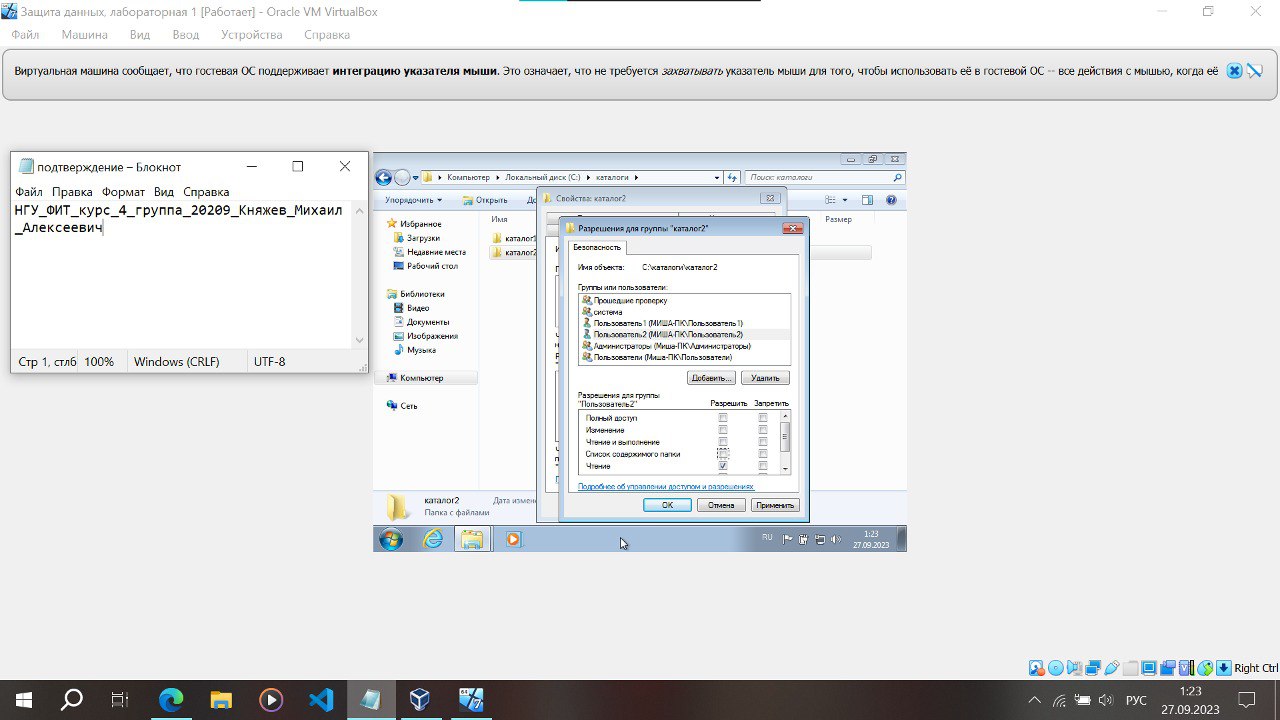


Рисунок 7

Создаем каталог3, правой кликаем по каталогу, открываем свойства, переходим на вкладку безопасность, выставляем нужные требования. Результат представлен на рисунке 8, 9.

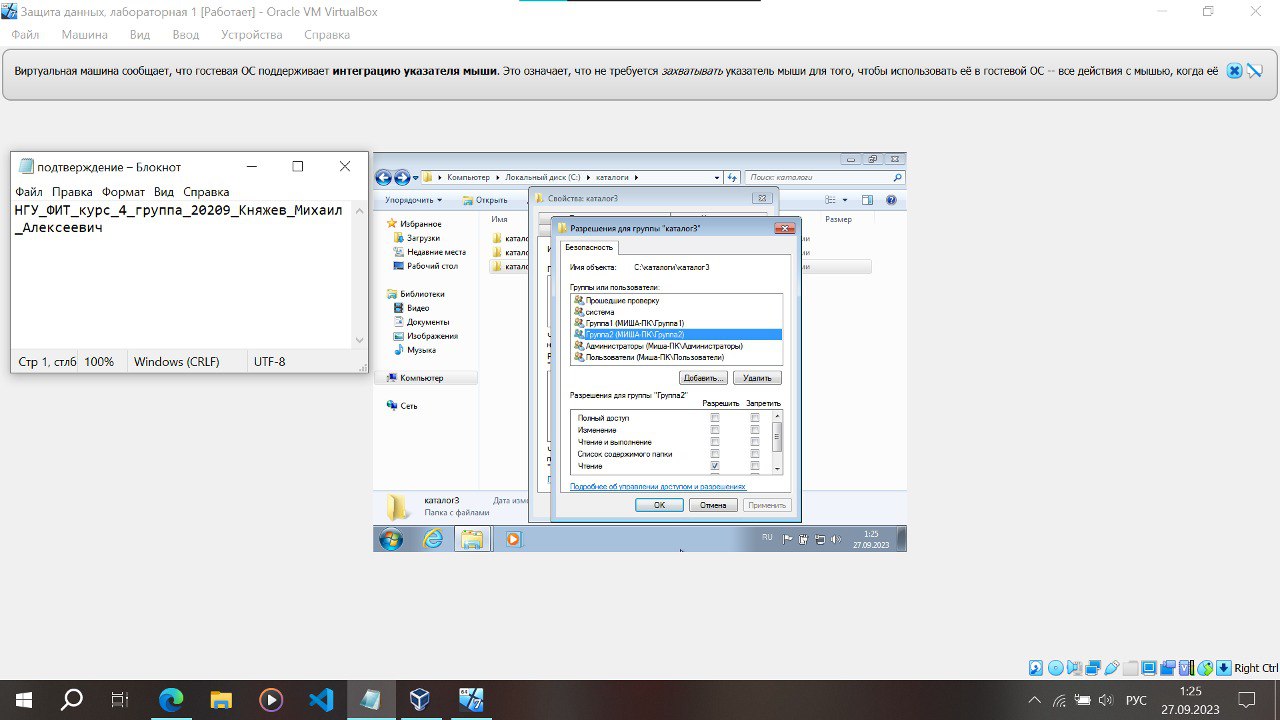


Рисунок 8

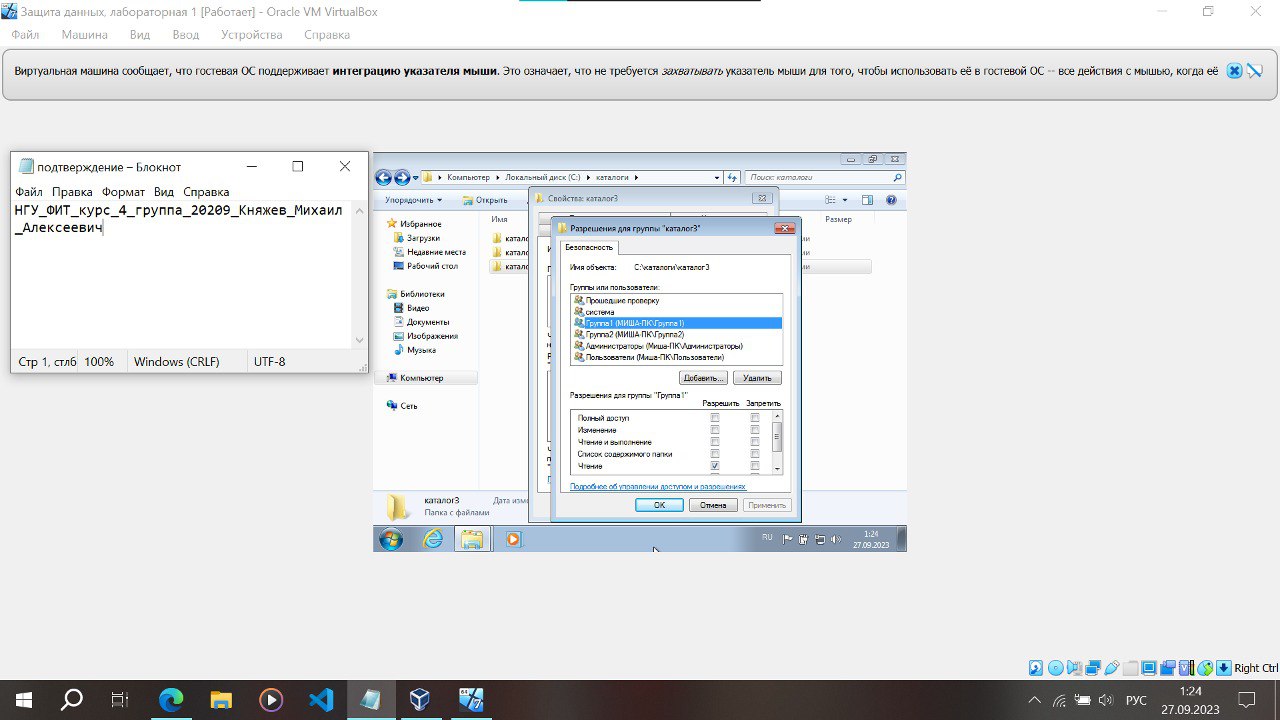


Рисунок 9

Создаем каталог4, правой кликаем по каталогу, открываем свойства, переходим на вкладку безопасность, выставляем нужные требования. Результат представлен на рисунке 10, 11.

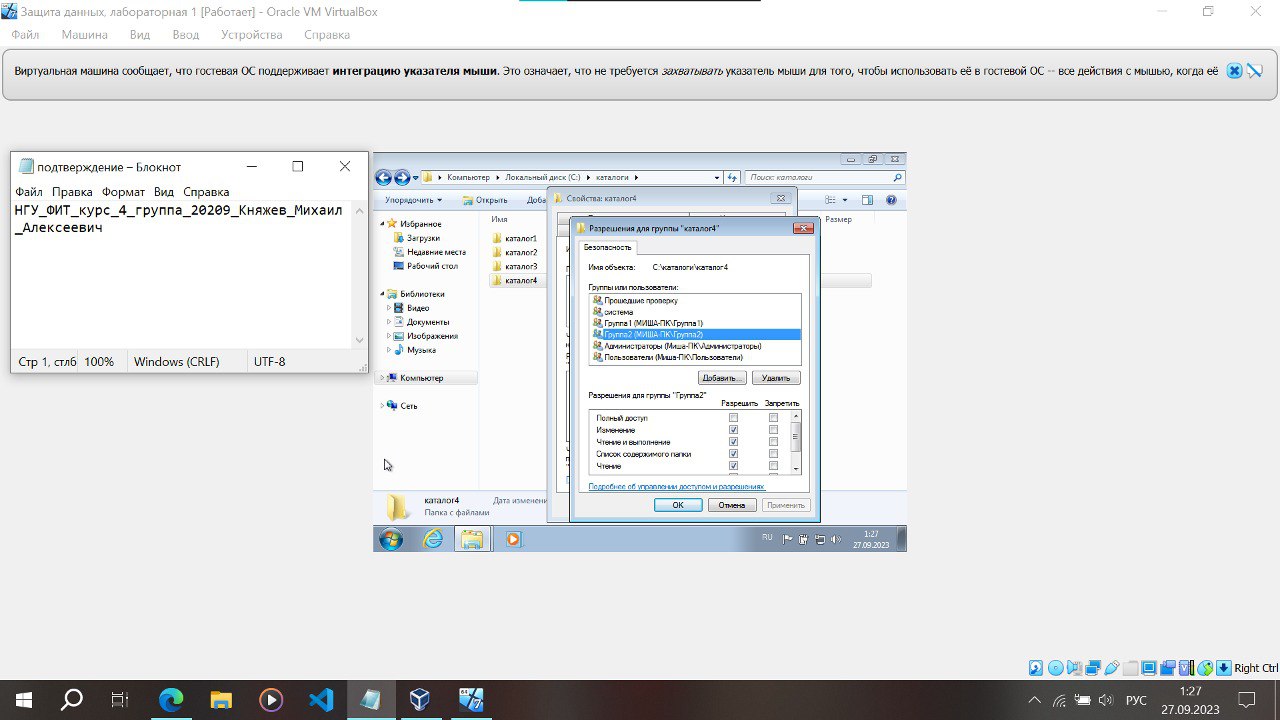


Рисунок 10

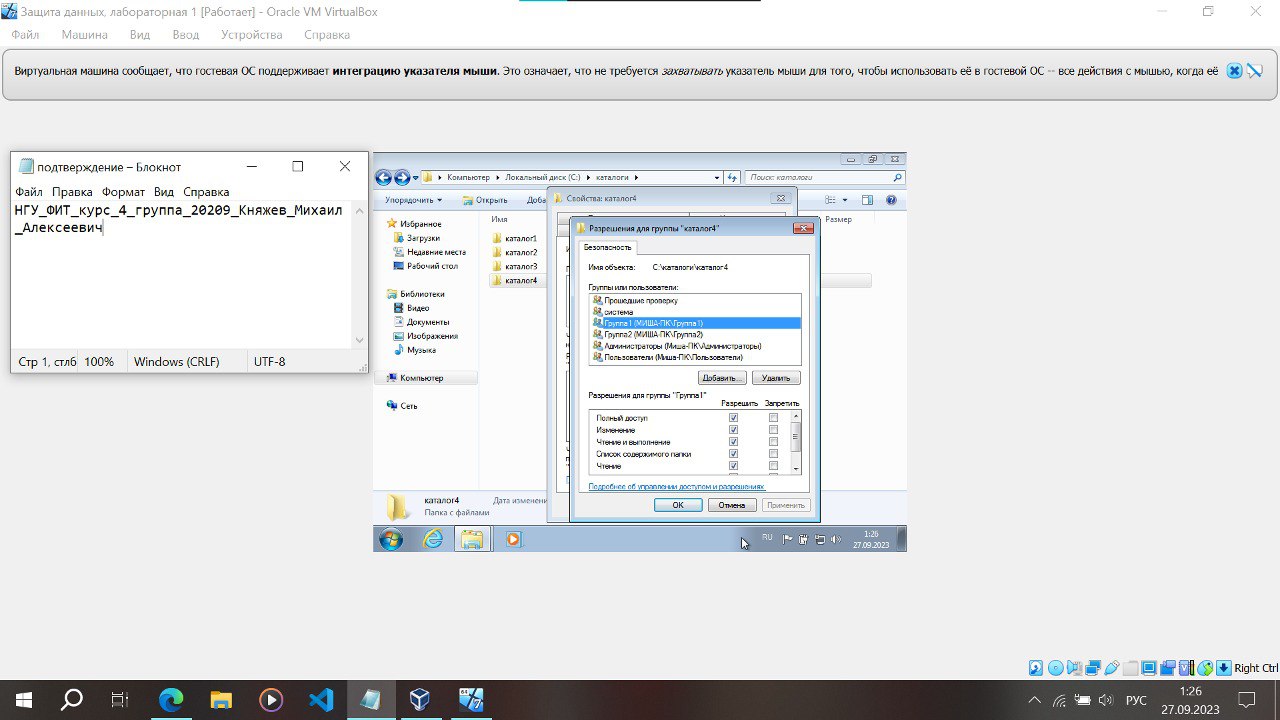


Рисунок 11

**Пункт 4:**

Открываем пуск, в поисковой строке вводим mmc, после чего нажимаем файл, выбираем добавить или удалить оснастку, в левом меню выбираем шаблон безопасности, нажимаем добавить, после чего выполняем действия, прописанные в пункте. Результат представлен в рисунках 12-19.

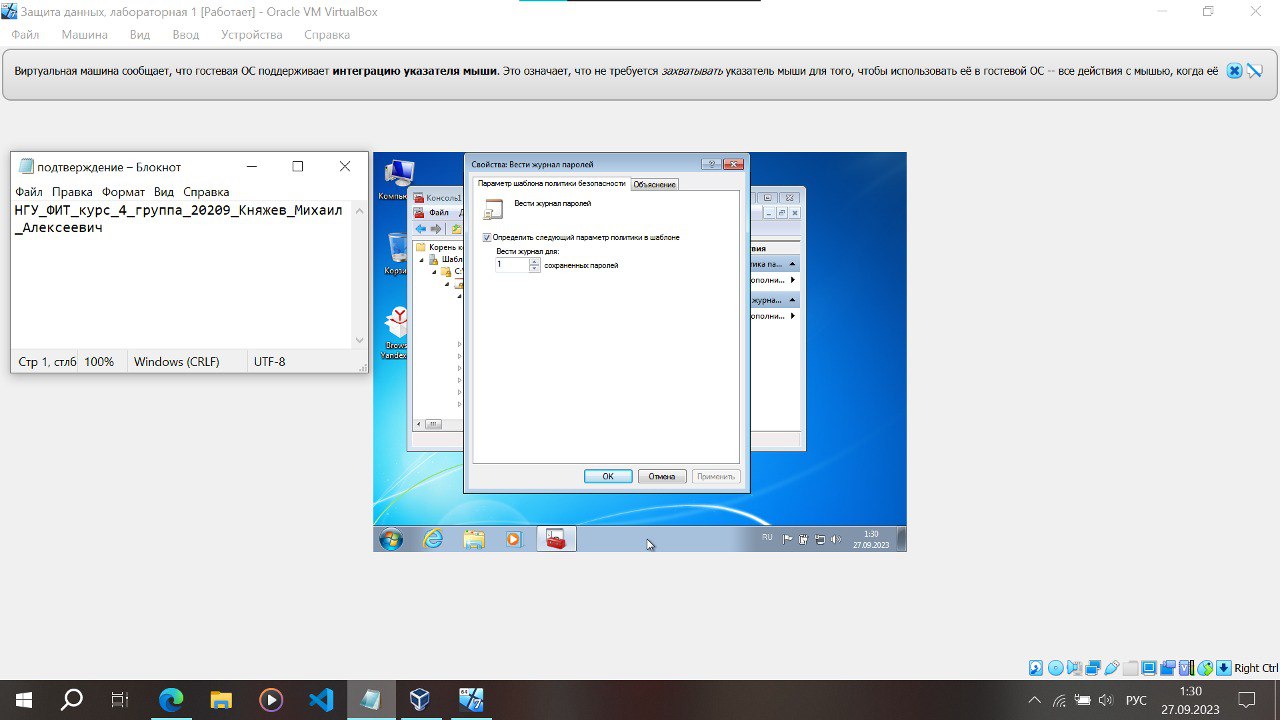


Рисунок 12

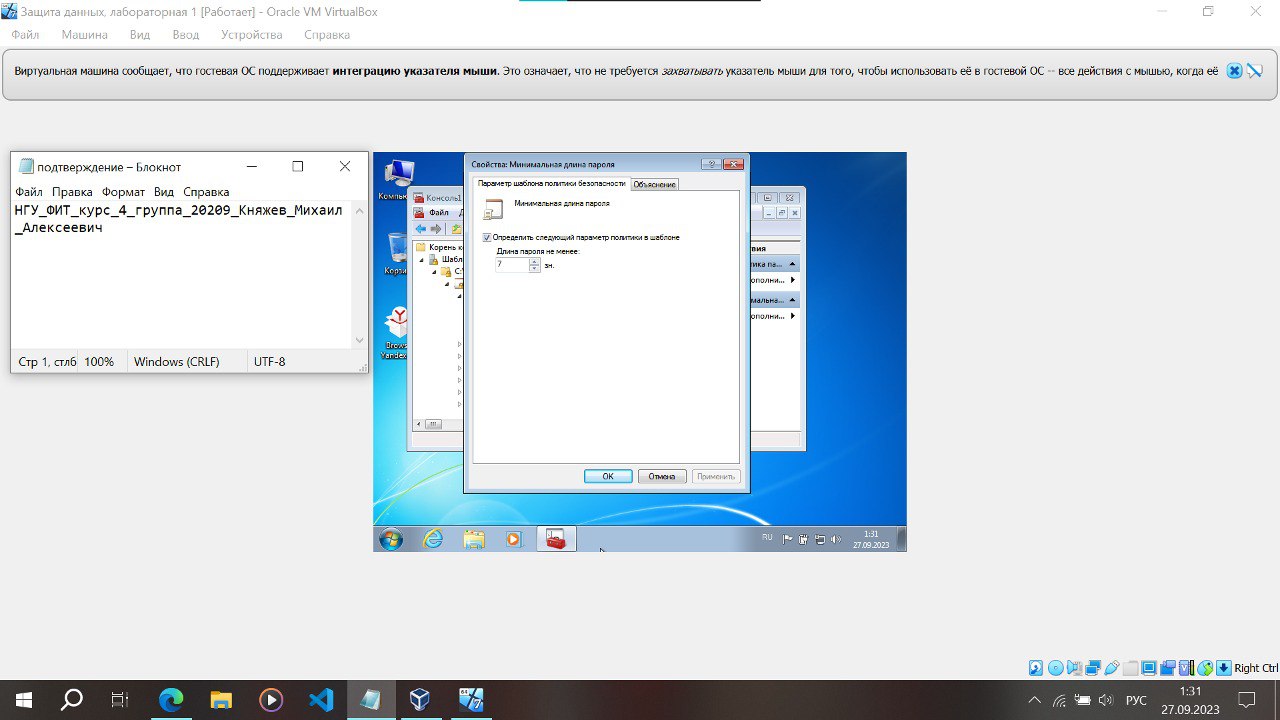


Рисунок 13

Рисунок 14

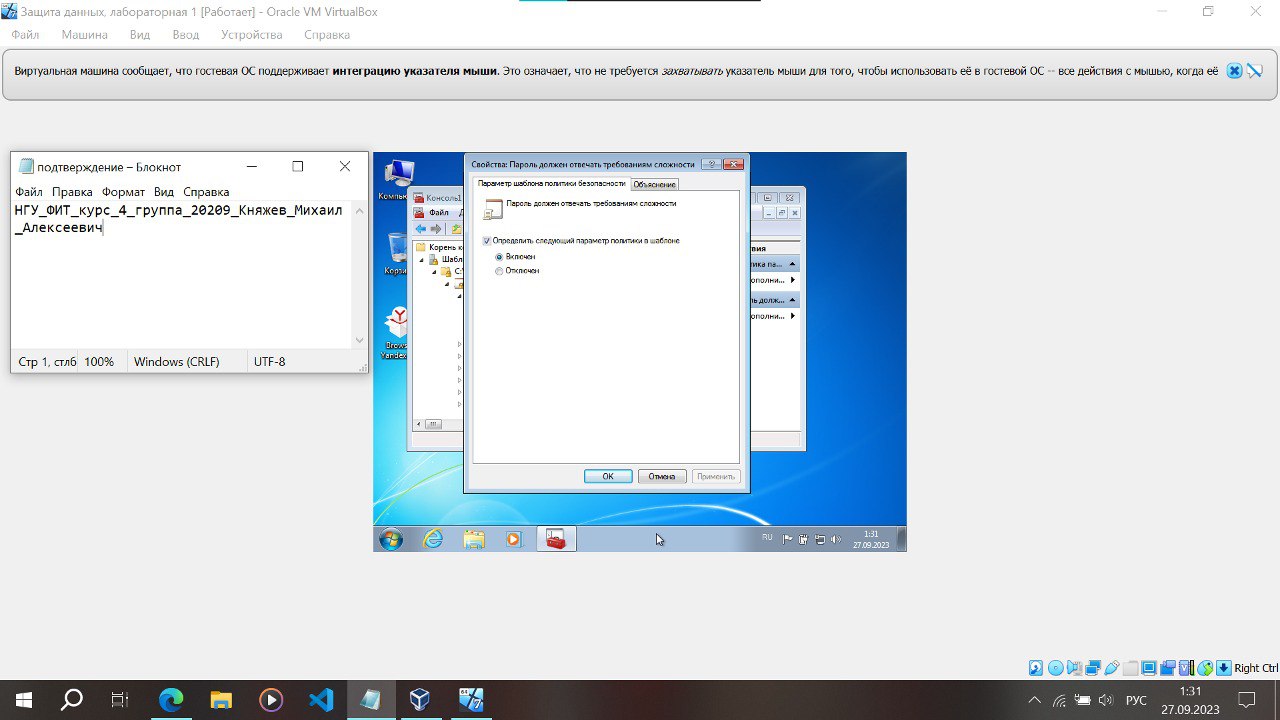
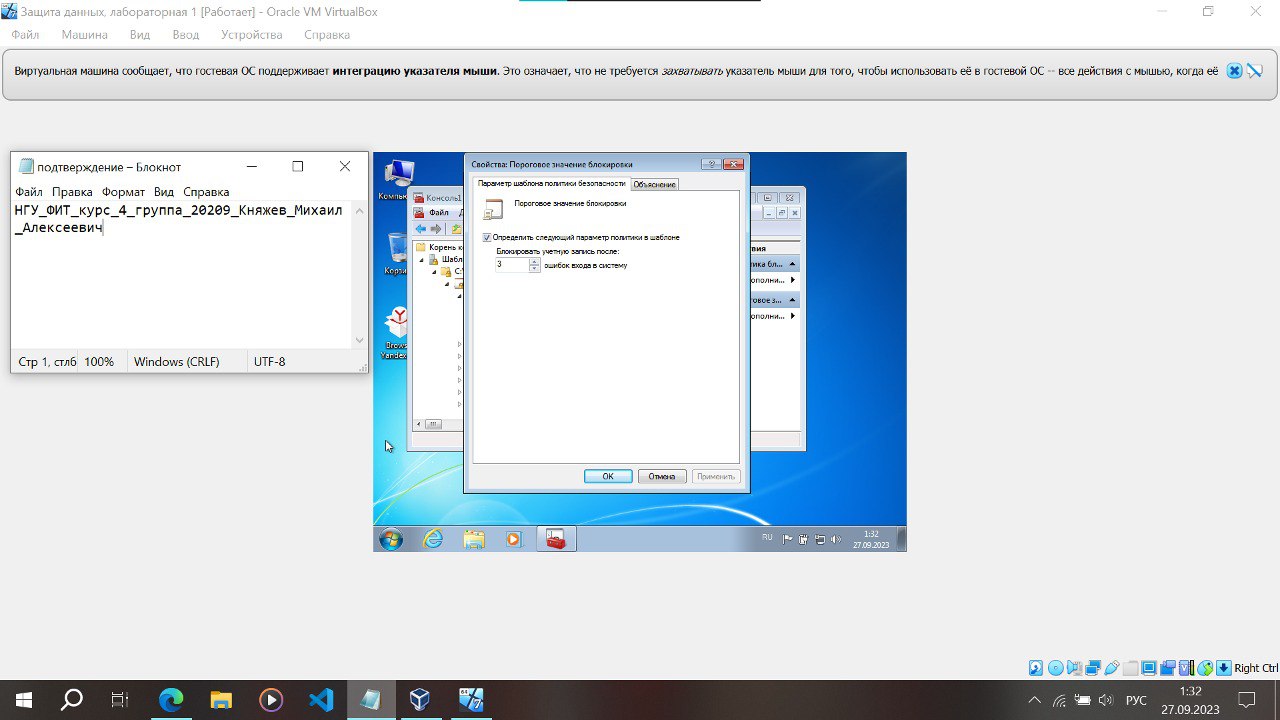


Рисунок 15

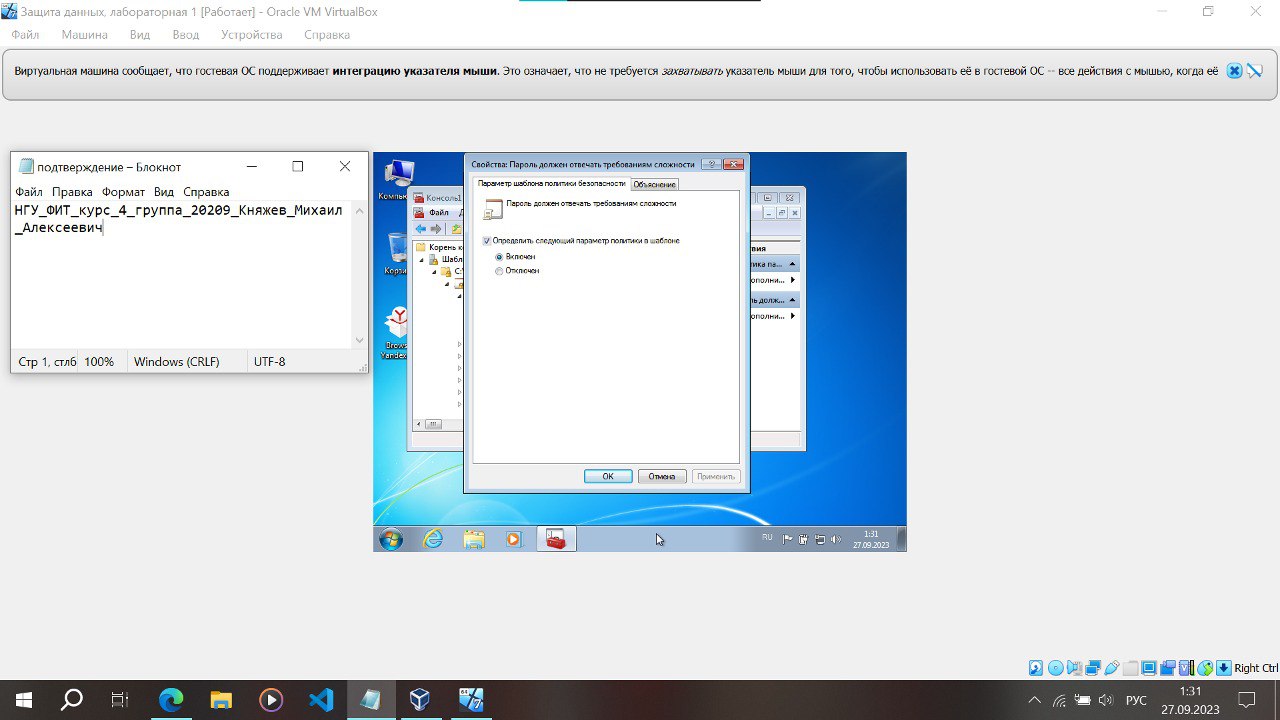


Рисунок 16

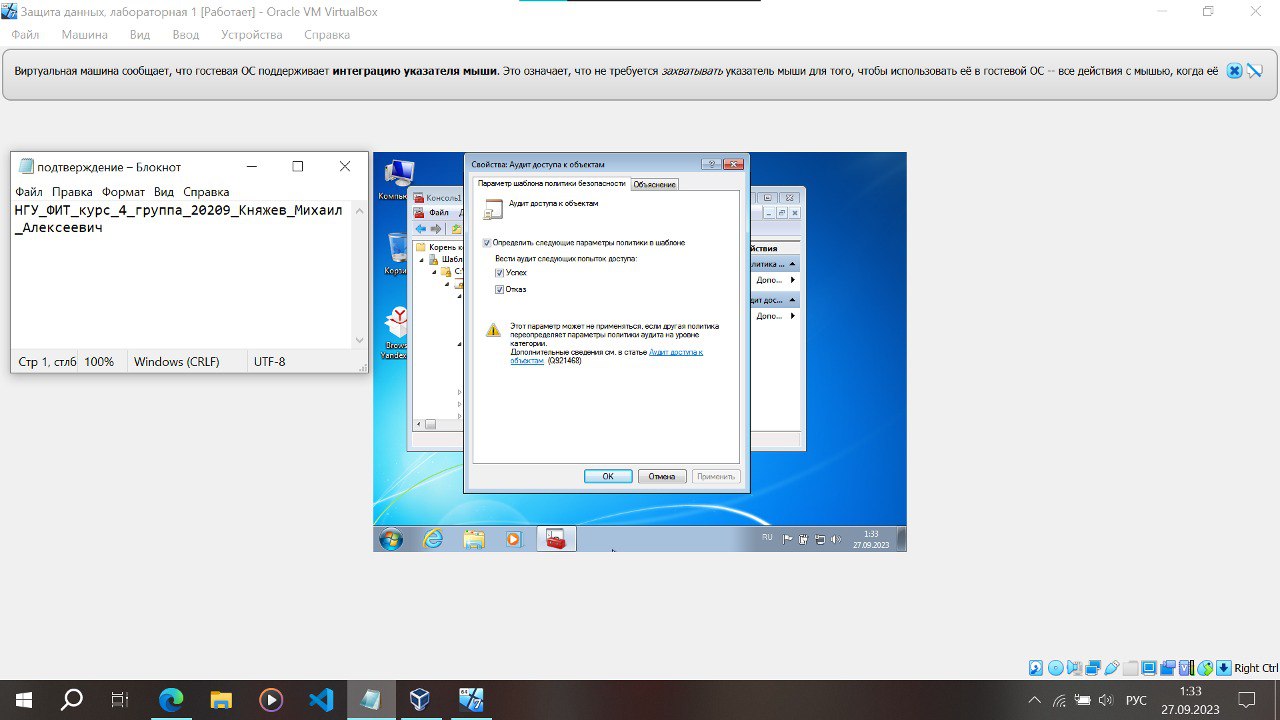


Рисунок 17

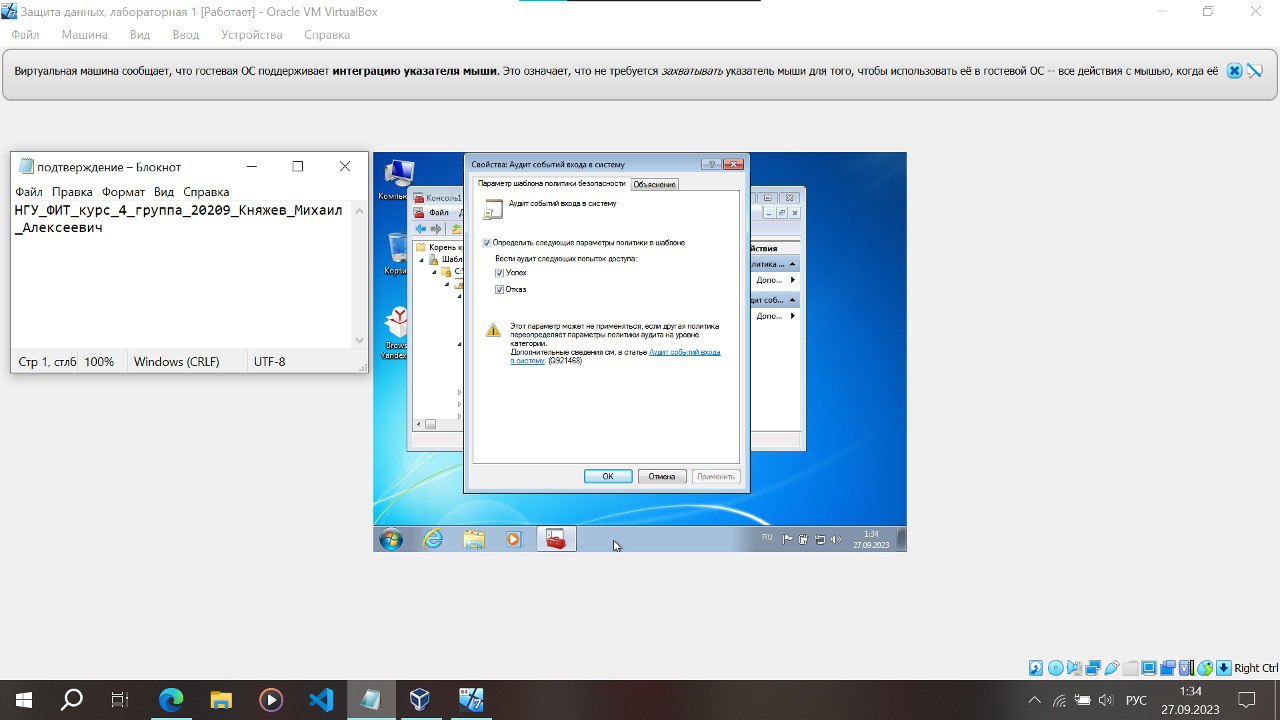


Рисунок 18

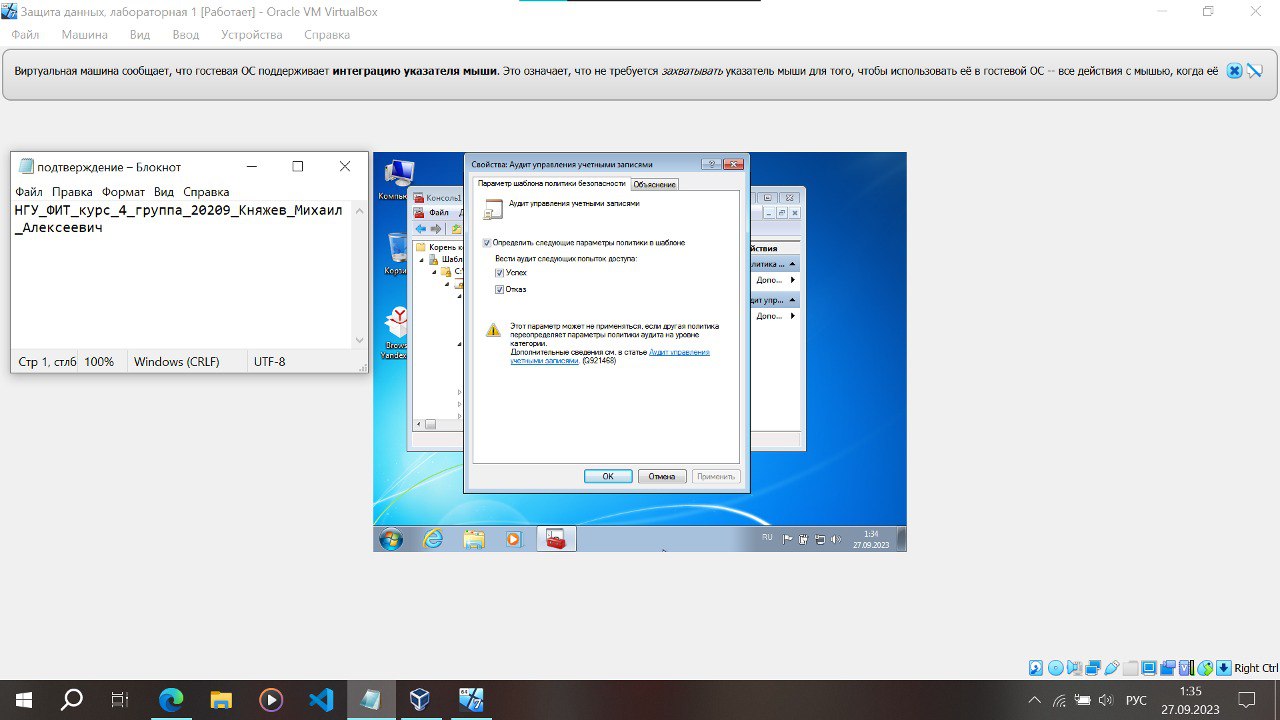


Рисунок 19

**Пункт 5:**

Открываем пуск, в поисковой строке вводим mmc, после чего нажимаем файл, выбираем добавить или удалить оснастку, в левом меню выбираем анализ и настройка безопасности, нажимаем добавить, после чего выполняем действия, которые можно прочитать в описании анализа и настройки безопасности. Результат представлен в рисунках 20-22.

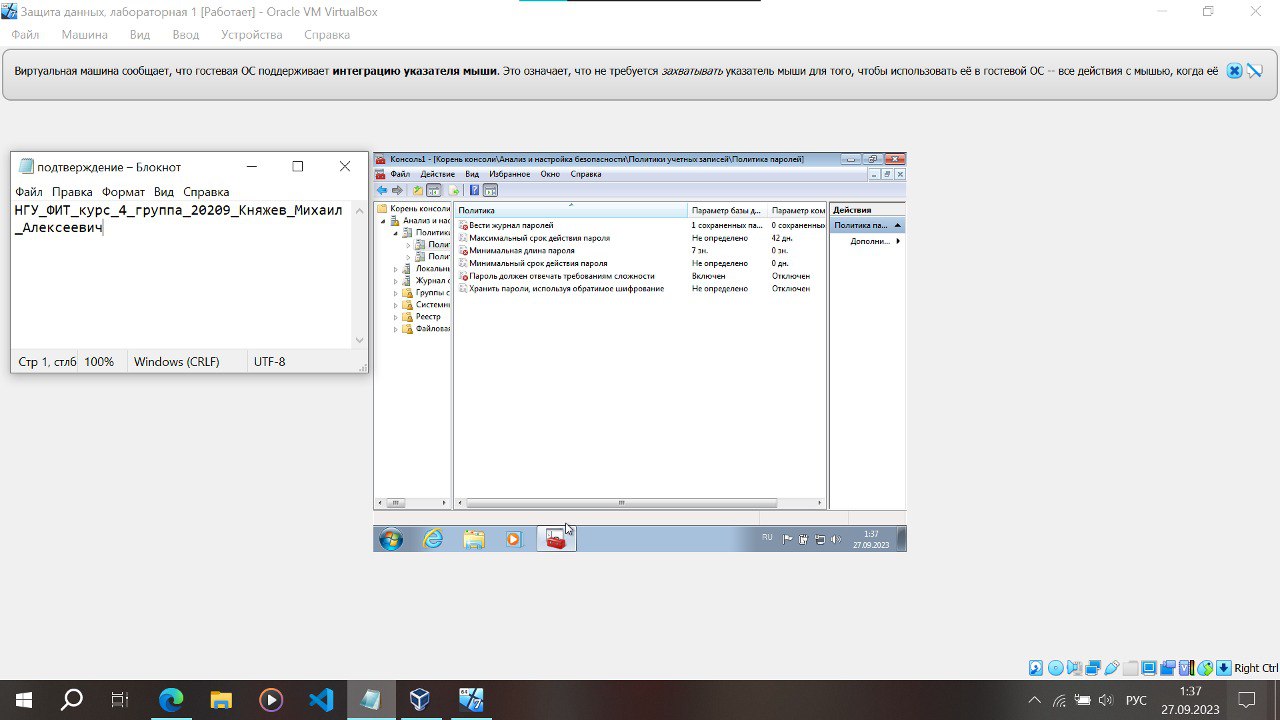


Рисунок 20

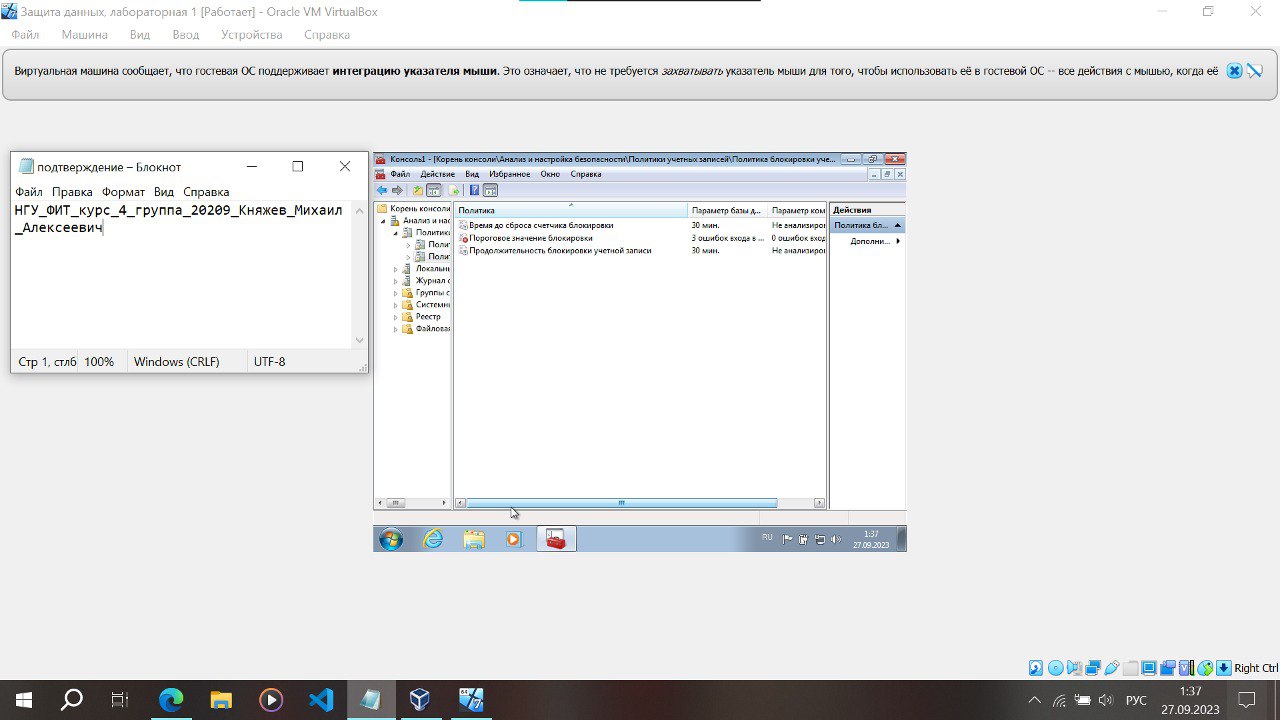


Рисунок 21

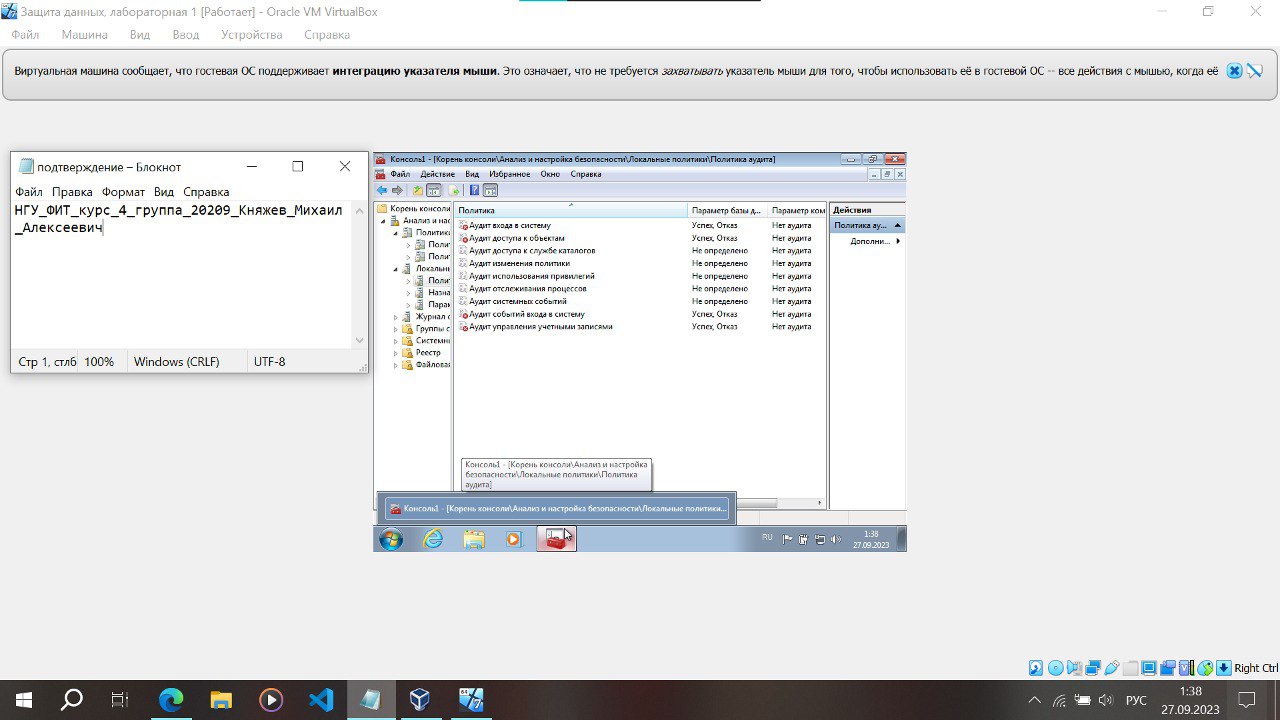


Рисунок 22

**Пункт 6:**

После выполнения пункта выполняем действия, которые можно прочитать в описании анализа и настройки безопасности. Результат представлен в рисунках 23-25.

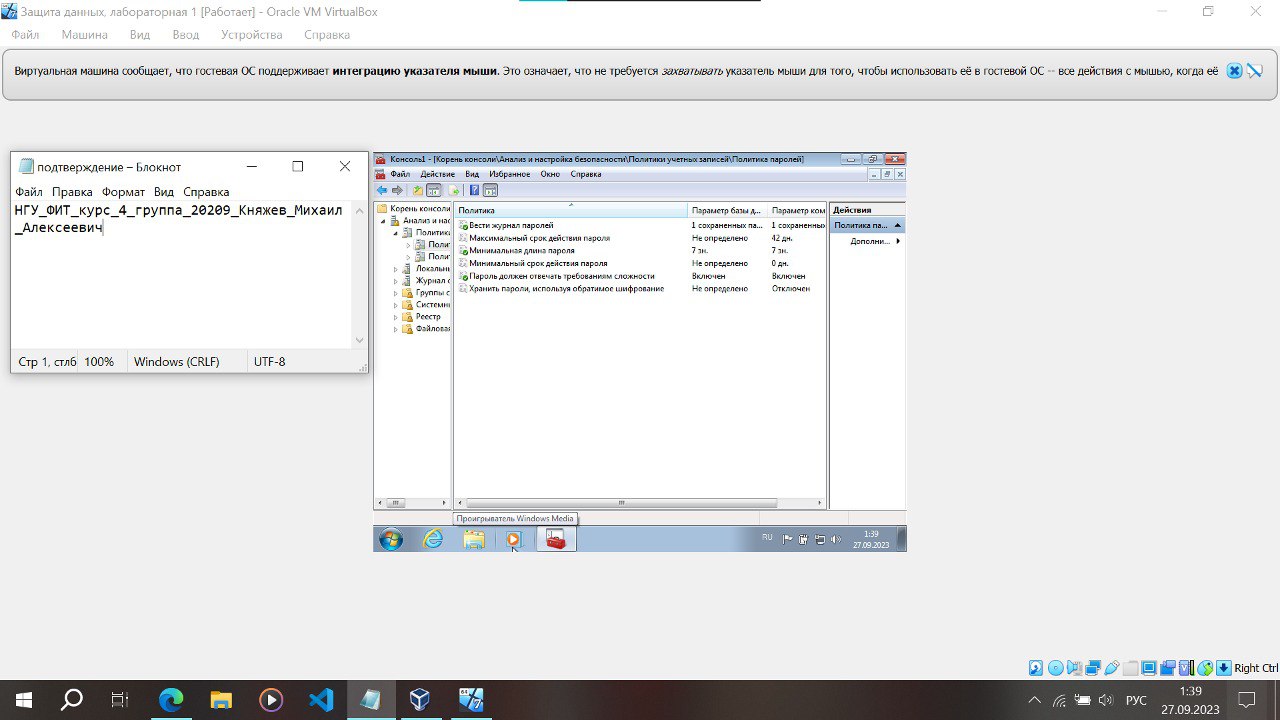


Рисунок 23

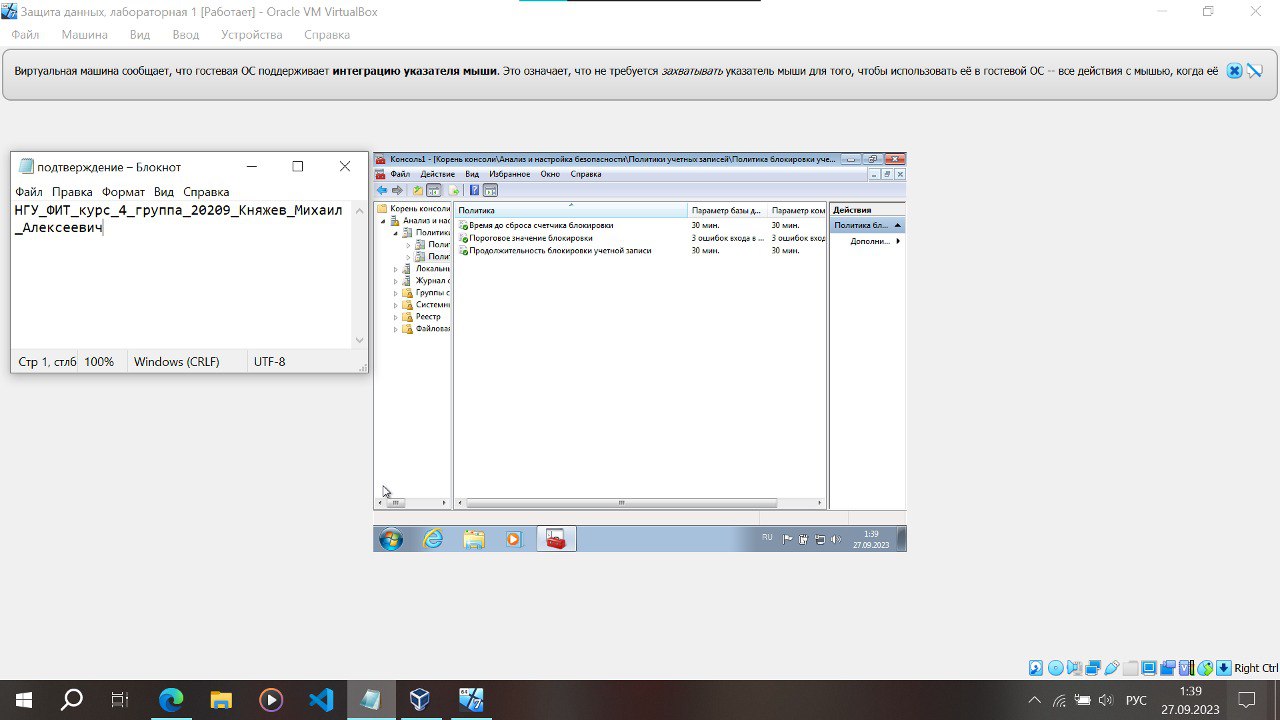


Рисунок 24

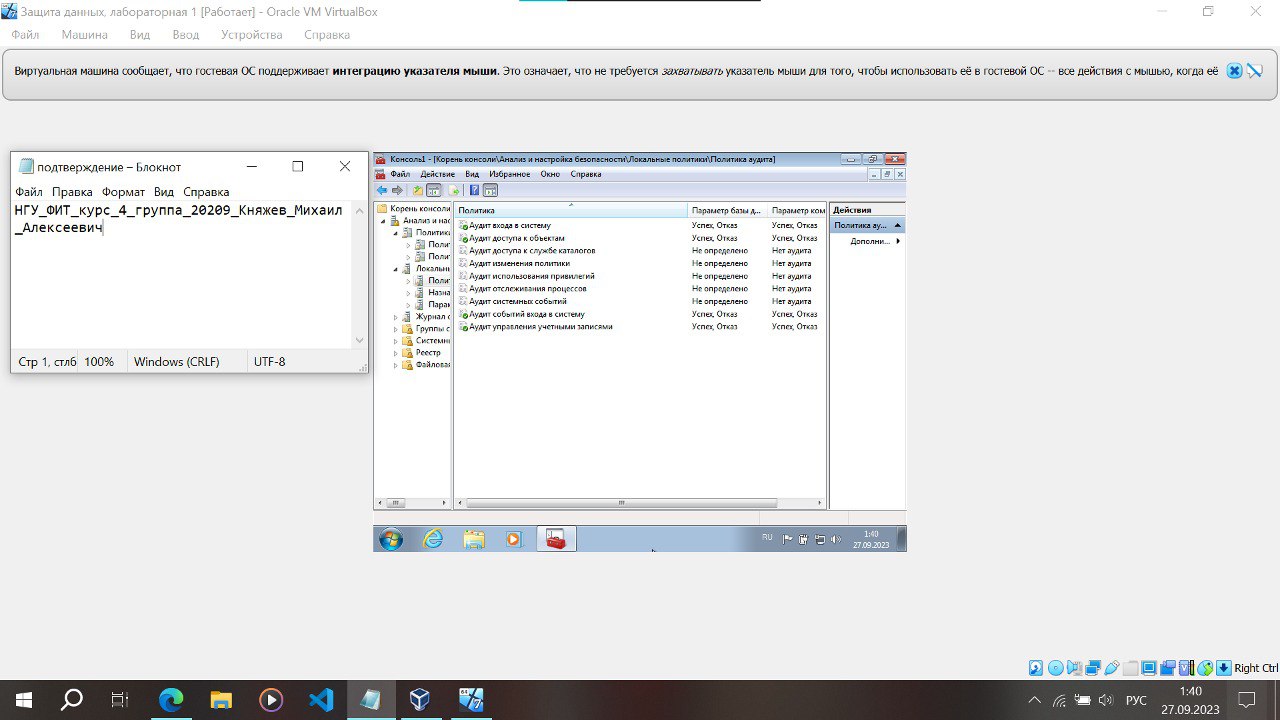


Рисунок 25

**Пункт 7:**

Выполнив действия пункта 1 без учета создания пользователей, выбираем уже созданных пользователей, меняем пароль пользователь1 учитывая шаблон безопасности, новый пароль: Йцукен1! Результат представлен в рисунке 26.

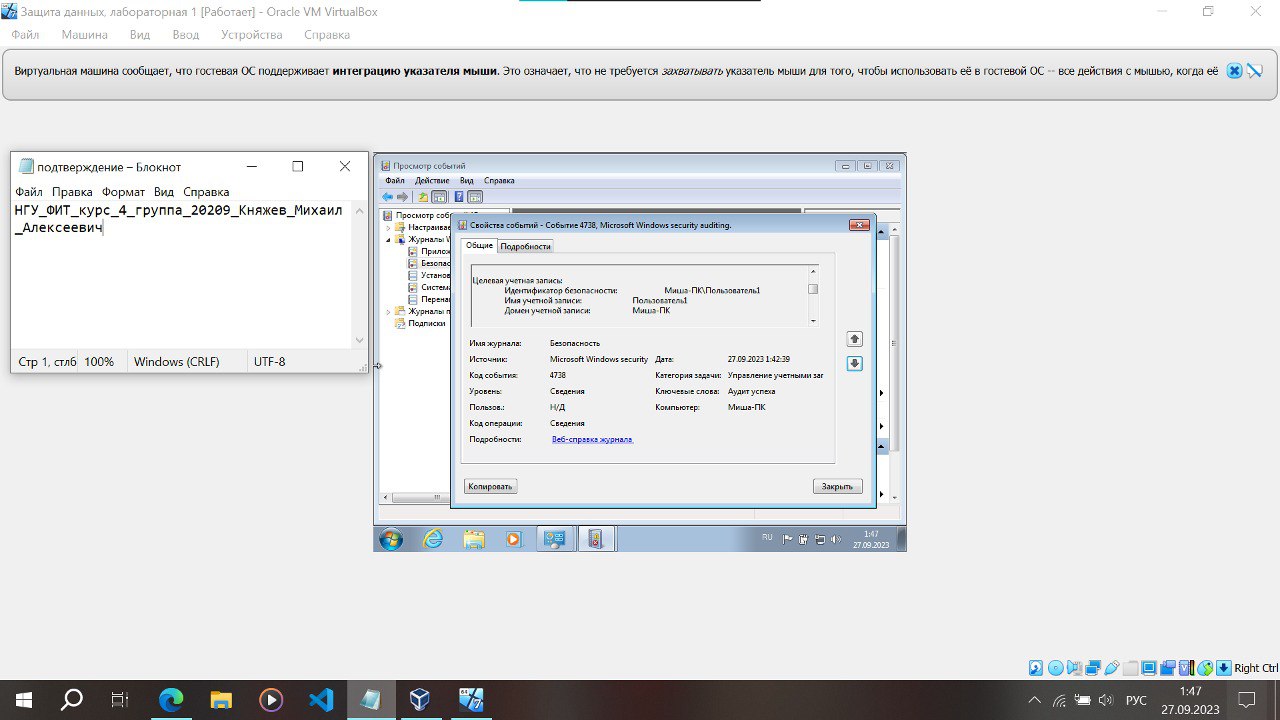


Рисунок 26

Меняем пароль пользователь1 без учета шаблона безопасности, новый пароль: 12345678. Результат представлен в рисунках 27, 28.

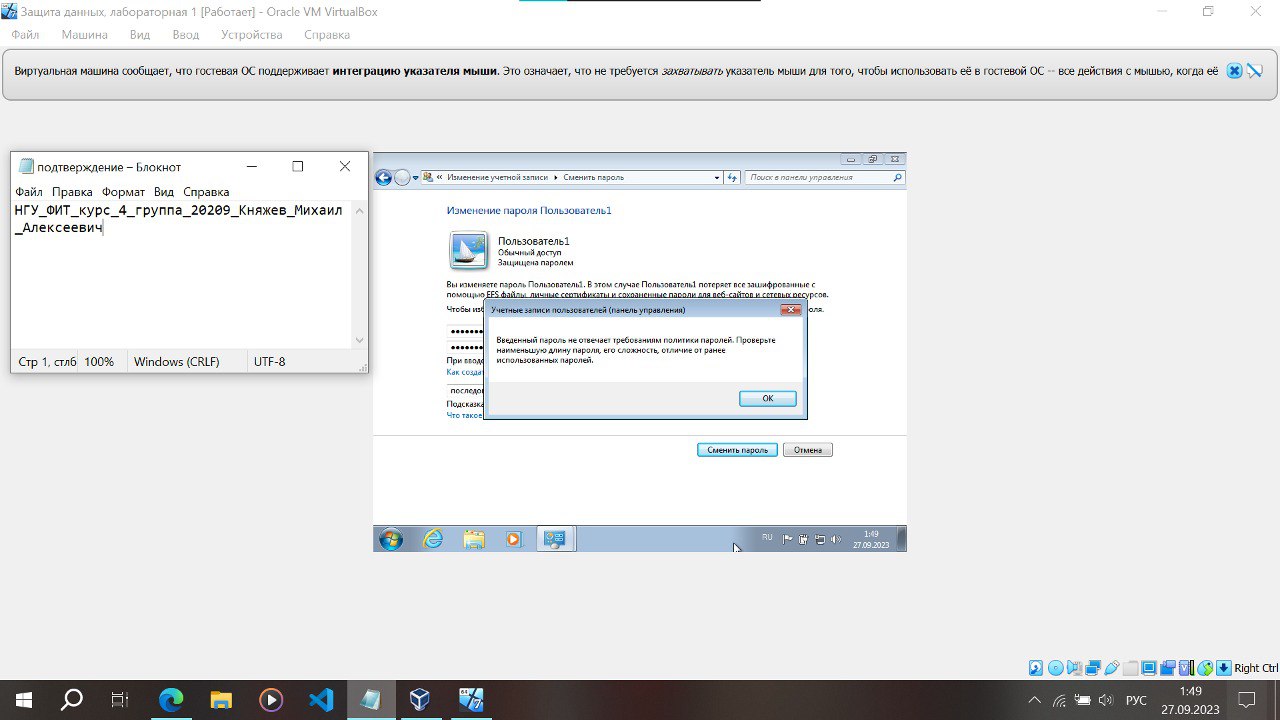


Рисунок 27

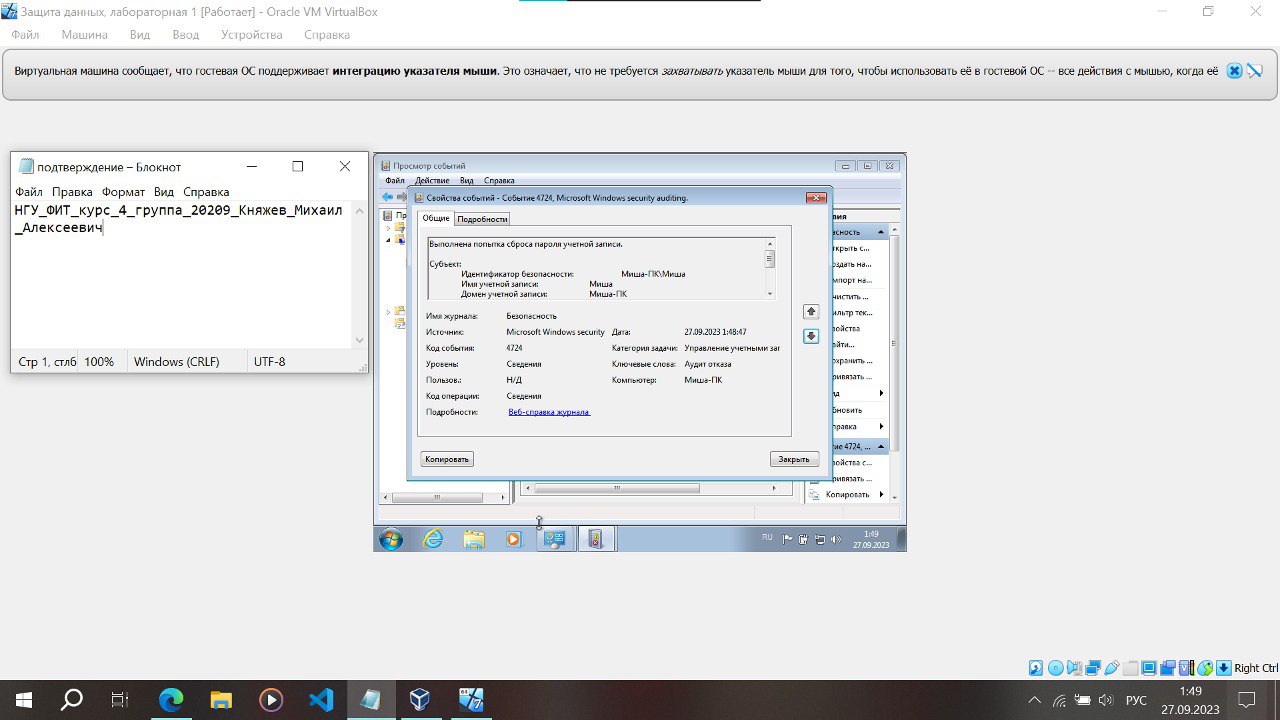


Рисунок 28

Входим в пользователь1 с неправильным паролем. Результат представлен на рисунке 29.

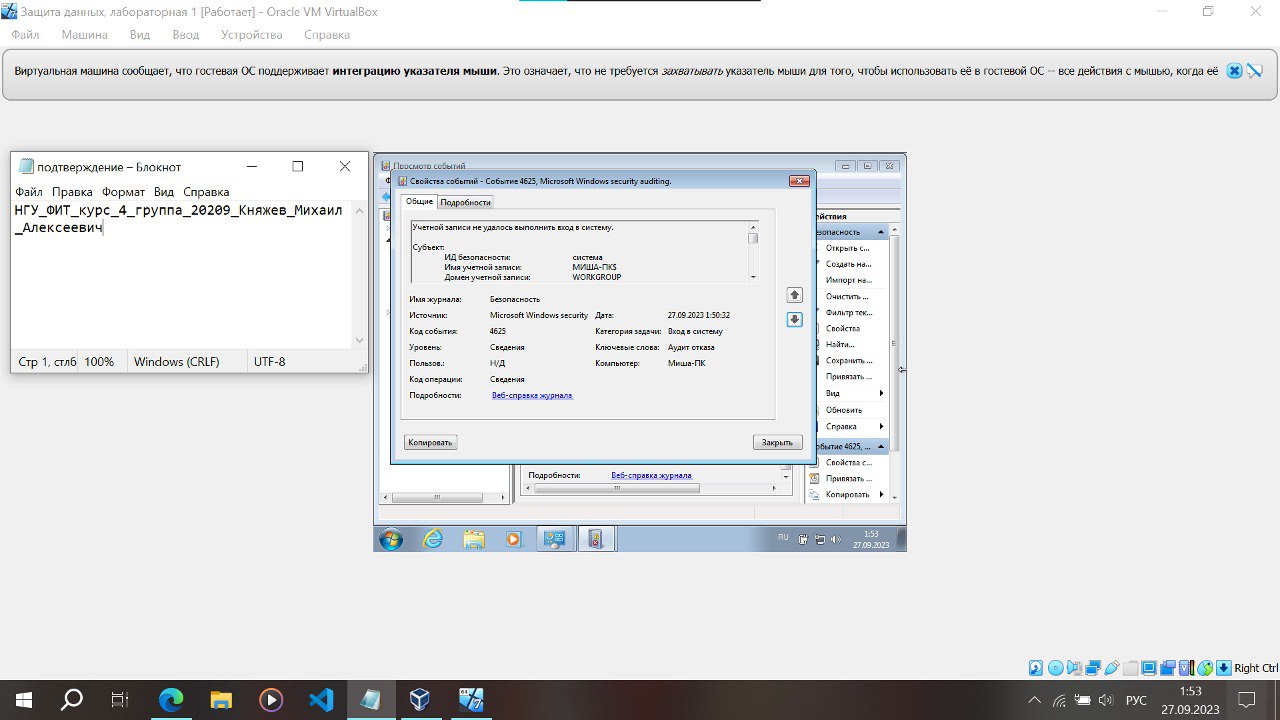


Рисунок 29

Входим в пользователь1 с правильным паролем. Результат представлен на рисунке 30.

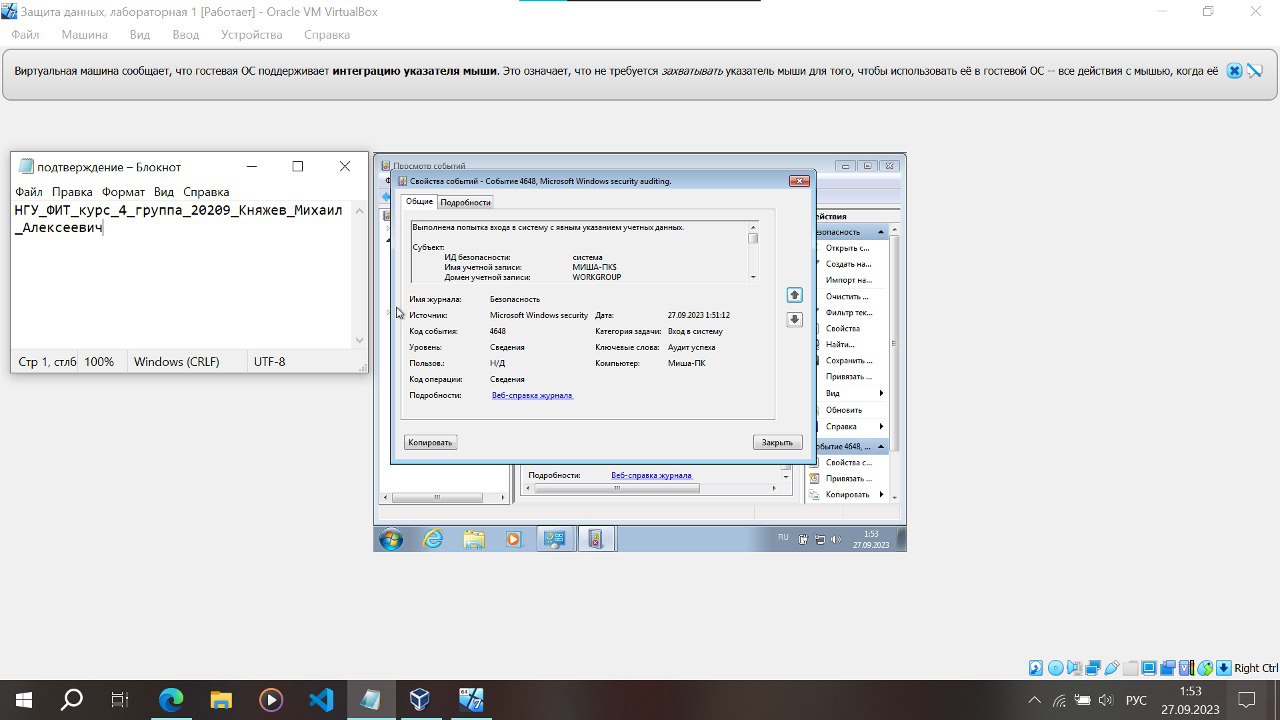


Рисунок 30

**Пункт 8:**

Проверяем что есть доступ в интернет, результат представлен на рисунке 31**.**

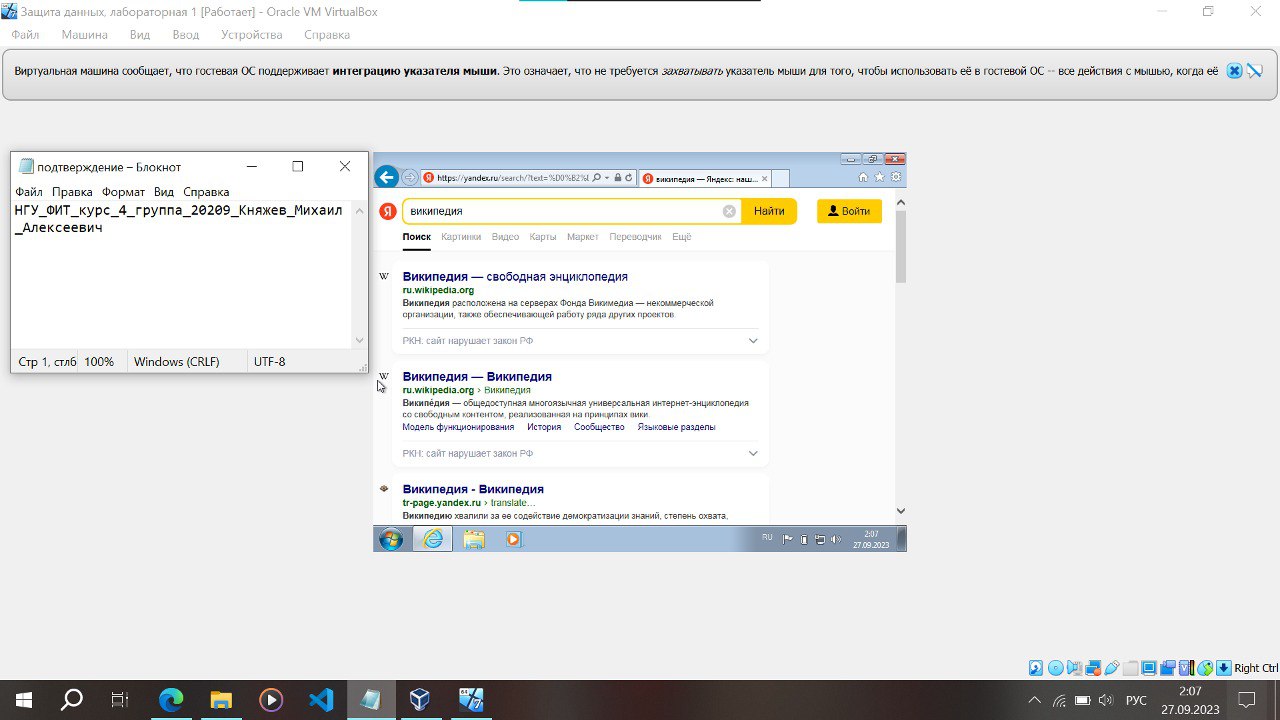


Рисунок 31

Открываем пуск, выбираем панель управления, в просмотре выбираем мелкие значки, открываем брандмауэр Windows, после чего выбираем дополнительные параметры, выбираем правила для исходящего подключения, нажимаем создать правило, оставляем для программы и нажимаем далее, выбираем все программы, после нажатия кнопки далее выбираем блокировать подключение, нажимаем далее и называем правило. Результат представлен на рисунке 32.

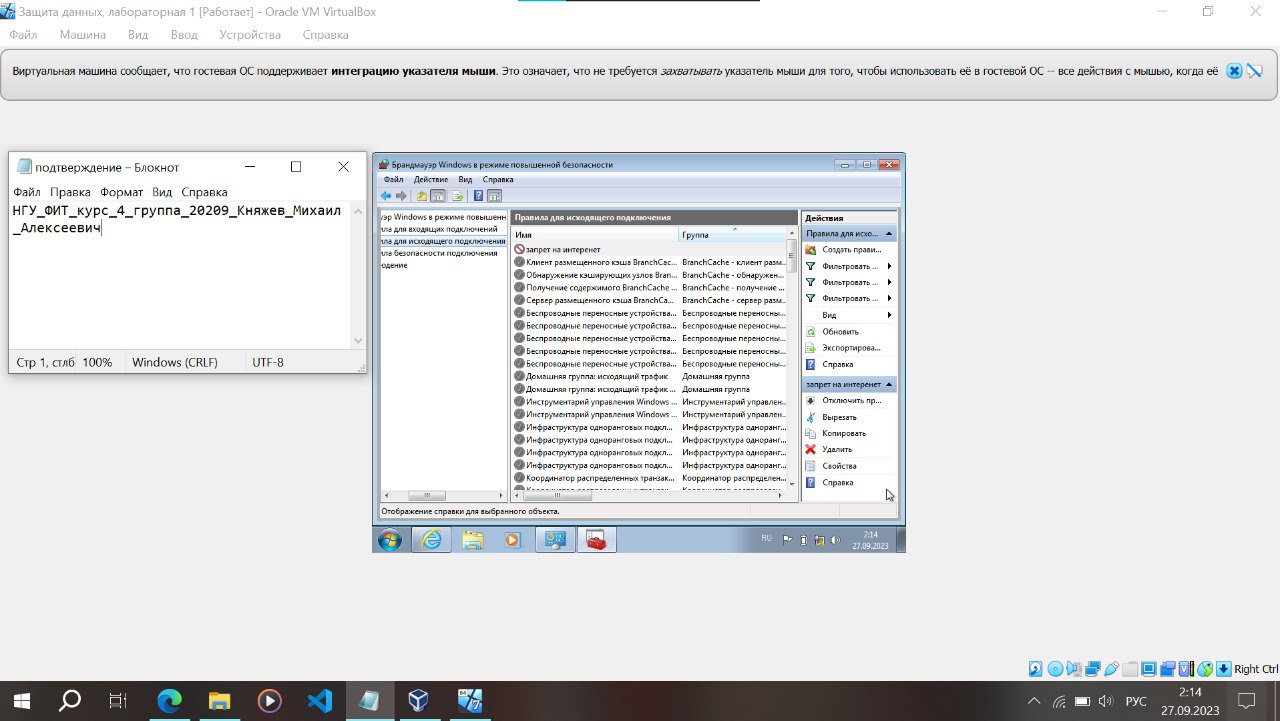


Рисунок 32

Выполняем выше описанную процедуру для правил входящего подключения, взамен шага выбрать все программы, указываем путь ../System32/mstsc. Результат показан на рисунках 33, 34.

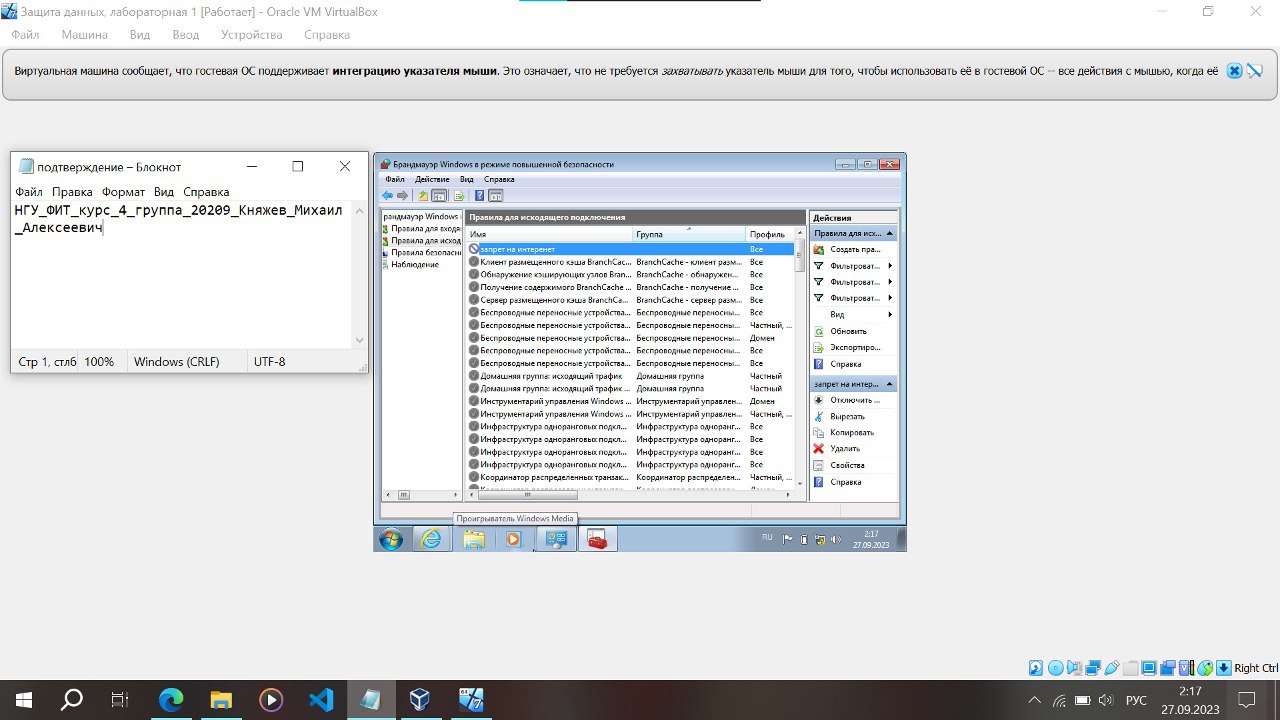


Рисунок 33

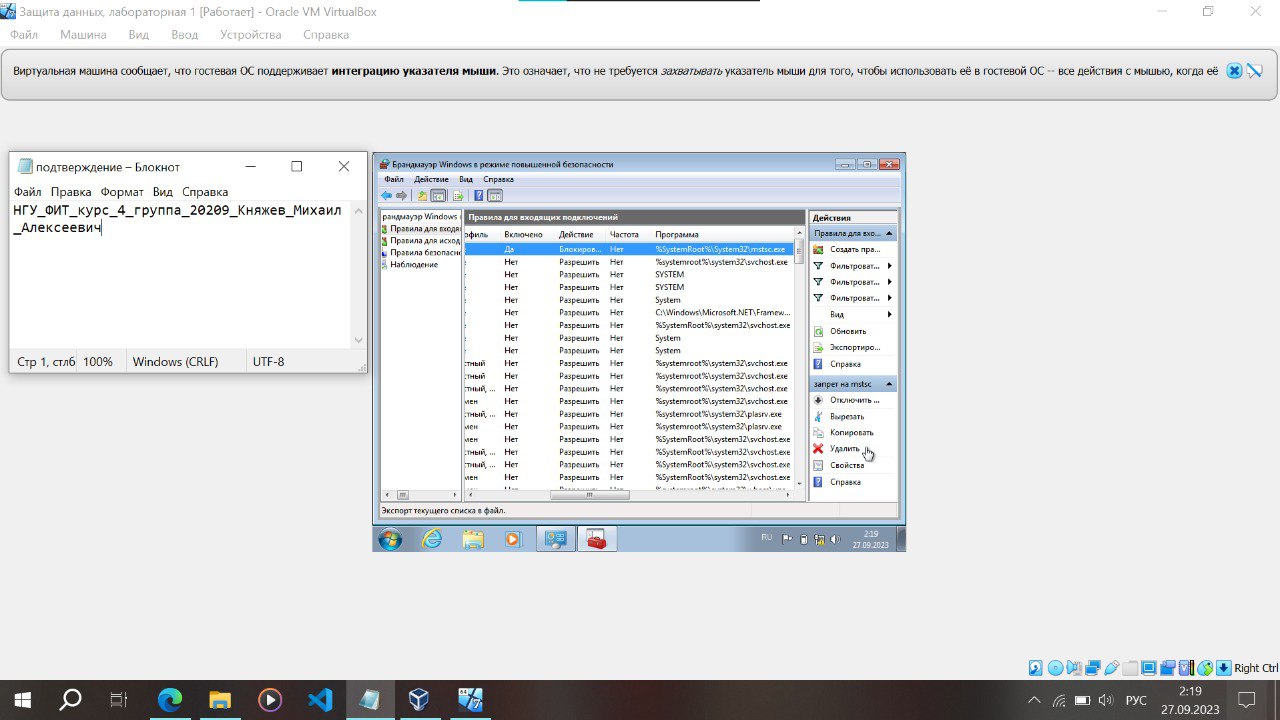


Рисунок 34

Проверяем, действительно, теперь при поисковом запросе википедия страница не отображается. Результат предоставлен в рисунке 35.

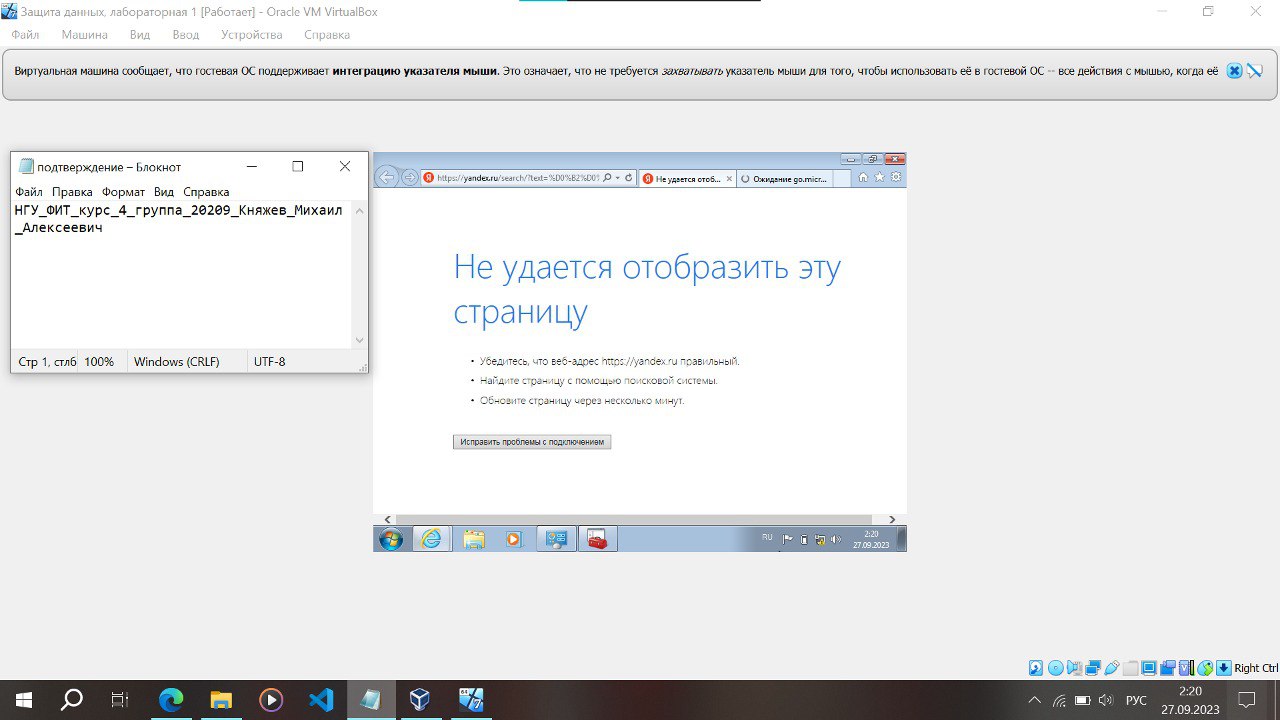


Рисунок 35

На ноутбуке (не виртуальной машине) разрешаем удаленный доступ. Открываем командную строку, вводим IPCONFIG, запоминаем свой локальный ip адрес. Открываем пуск, вводим подключение к удаленному столу, открываем его, вводим локальный адрес. Убеждаемся, что не удается подключиться к удаленному рабочему столу. Результат показан на рисунке 36.

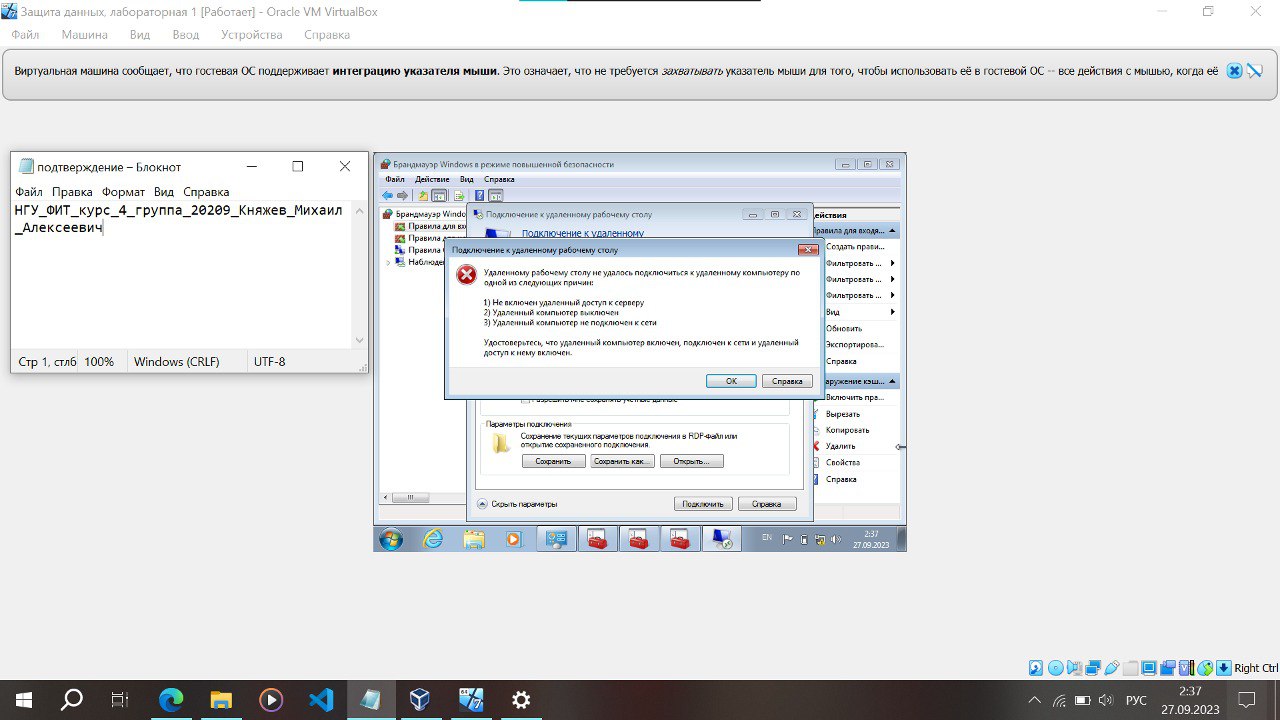


Рисунок 36

Пункт 9:

Выполняем действия, указанные в пункте. Результат представлен в рисунке 37.

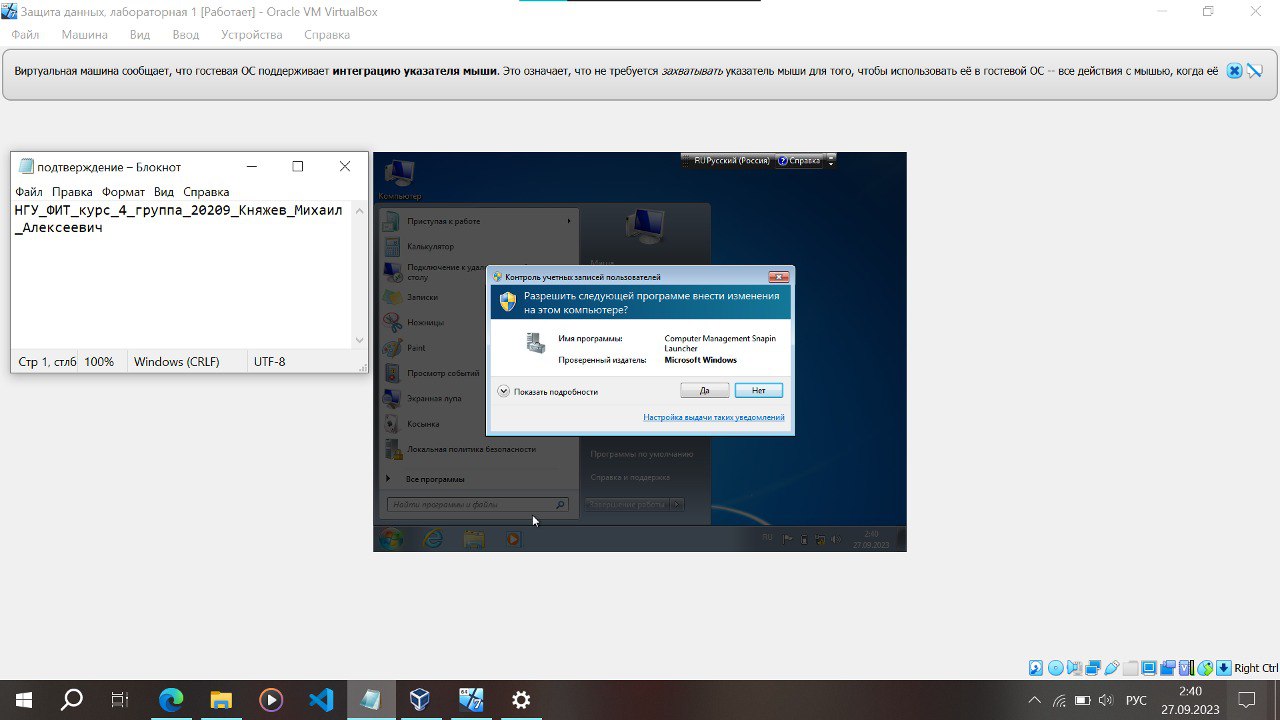


Рисунок 37

**Пункт 10:**

Открываем пуск, выбираем панель управления, в просмотре ставим мелкие значки, после чего выбираем архивация и восстановление, выполняем действия, указанные в пункте. Результат представлен на рисунке 38.

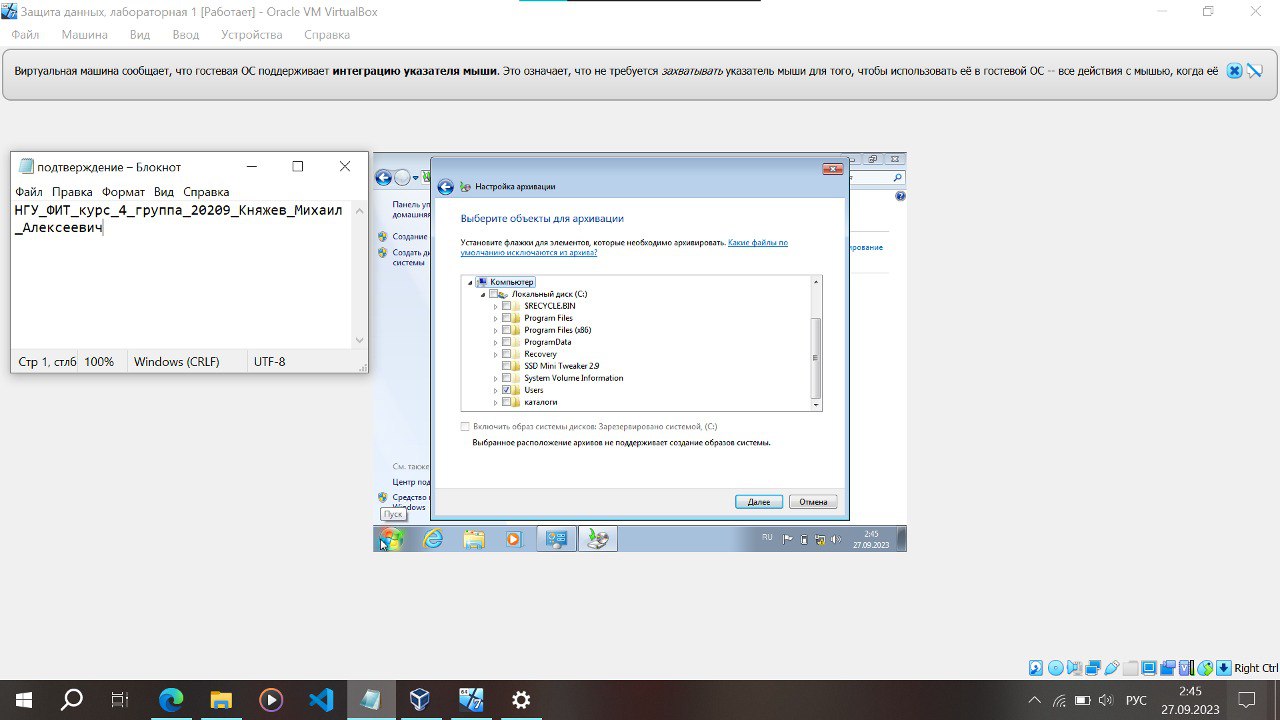


Рисунок 38