министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

*факультет Программной инженерии и компьютерной техники*

*Дисциплина «Информационная безопасность»*

**Лабораторная работа №2**

Вариант 7

Группа: P3417

Выполнил: Ореховский А.

Проверила: Маркина Т. А.

Санкт-Петербург,

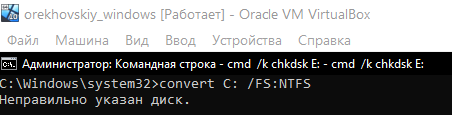
2021г

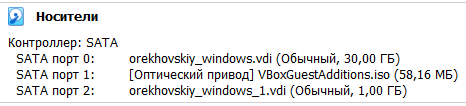
# Часть 1

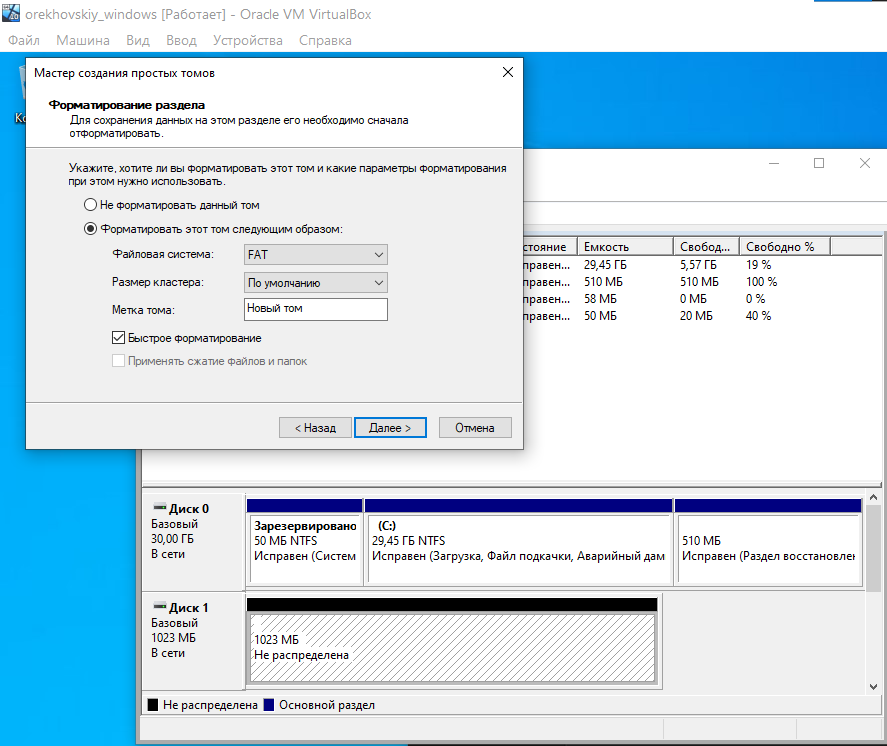
|  |  |  |
| --- | --- | --- |
| Название объекта доступа | Администратор | Пользователь |
| Загрузка системы | | |
| %SystemRoot% | RWX | RX |
| Вход в систему | | |
| lsass.exe | RX | RX |
| winlogon.exe | RX | RX |
| msgina.dll | RX | RX |
| msvl\_0.dll | RX | RX |
| userinit.exe | RX | RX |
| explorer.exe | RX | RX |
| %UserProfile% | RWX | RWX |
| Работа с приложениями, установленными администратором | | |
| Приложение | RX | RX |

# Часть 2. Преобразуйте файловую систему FAT (File Allocation Table) в NTFS (New Technology File System)

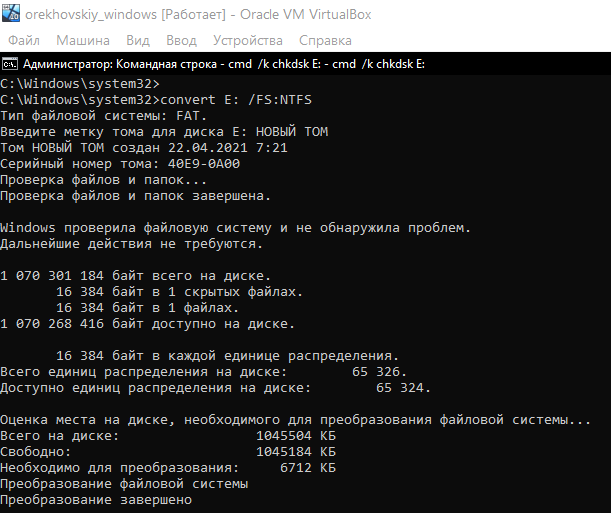
Очевидно, что преобразовать тип файловой системы у локального диска C не выйдет, поэтому добавим новый диск в ВМ и установим тип ФС в качестве FAT.

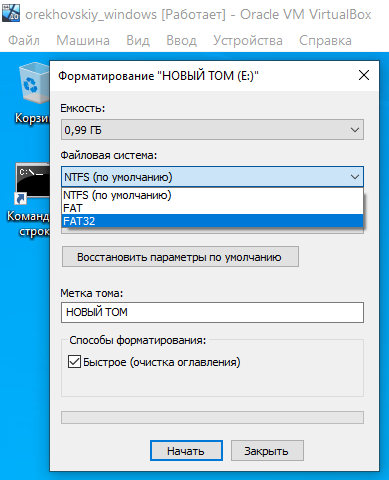






Преобразовать можно при помощи утилиты convert либо при форматировании нужного диска.



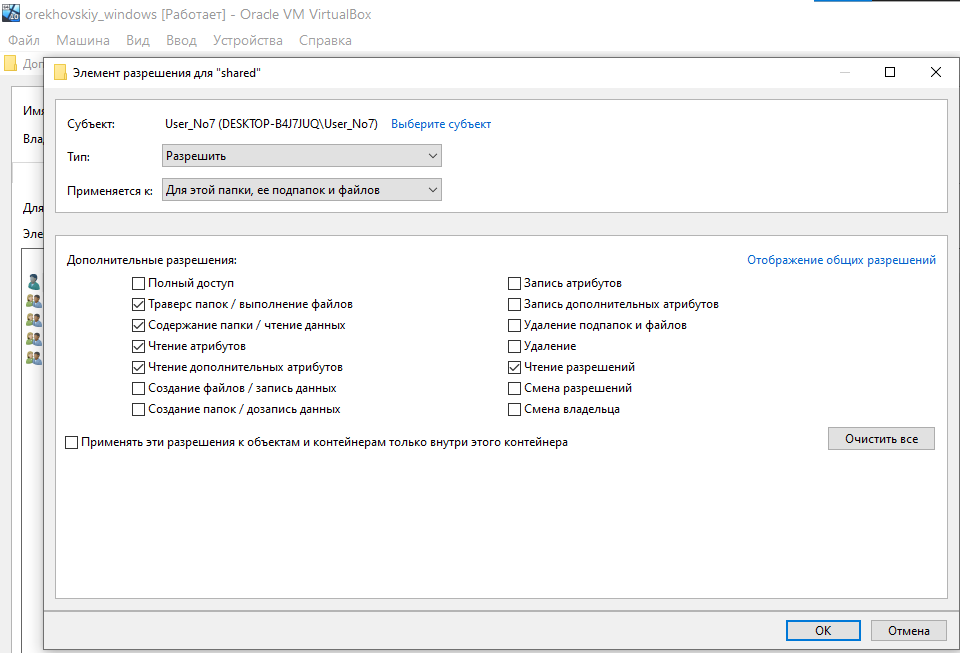


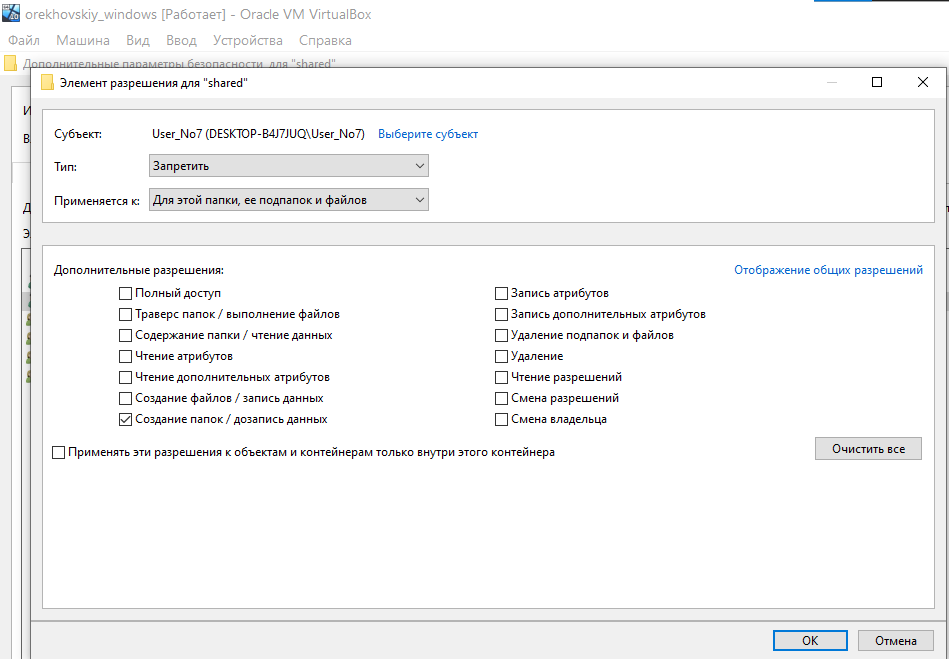
# Часть 3. Какие разрешения (права доступа) будут у Пользователя и у Администратора на файл «Noварианта.txt», если владельцем файла является Администратор, для Пользователя установлено разрешение «Запись» («Write»), для Администратора установлено разрешение «Чтение» («Read»), а для группы «Все» («Everyone») (оба пользователя входят в эту группу) -разрешение «Изменение» («Change»)?

Так как оба пользователя принадлежат группе Все и наследуют права от нее, то для обоих случаев будет доступно изменение файла.

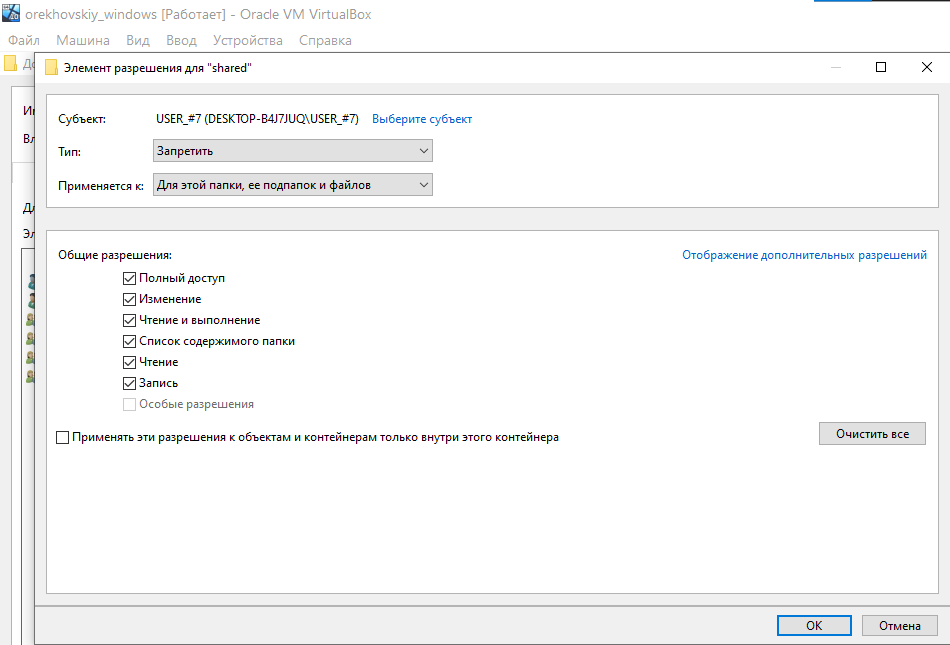
# Часть 4. Завести папку для хранения данных, разрешить встроенными средствами ОС Windows доступ пользователя к этой папке с данными, предотвратить возможность её переименования и создание новых папок для хранения данных. Остальным пользователям доступ к этой папке запретить. Проанализировать возможность и сложность настройки.

Для начала разрешим доступ к папке у конкретного пользователя, а так же запретим создание папок / дозапись данных в разных правилах.

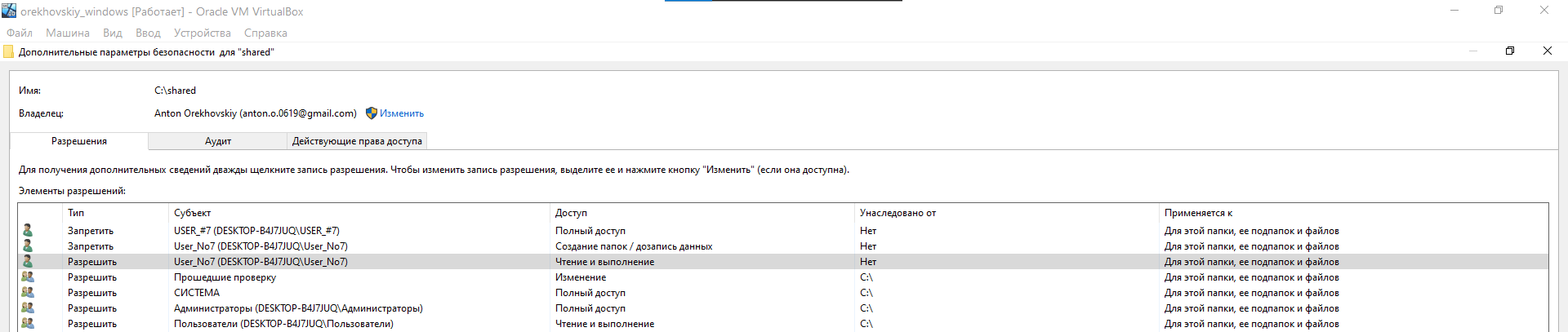




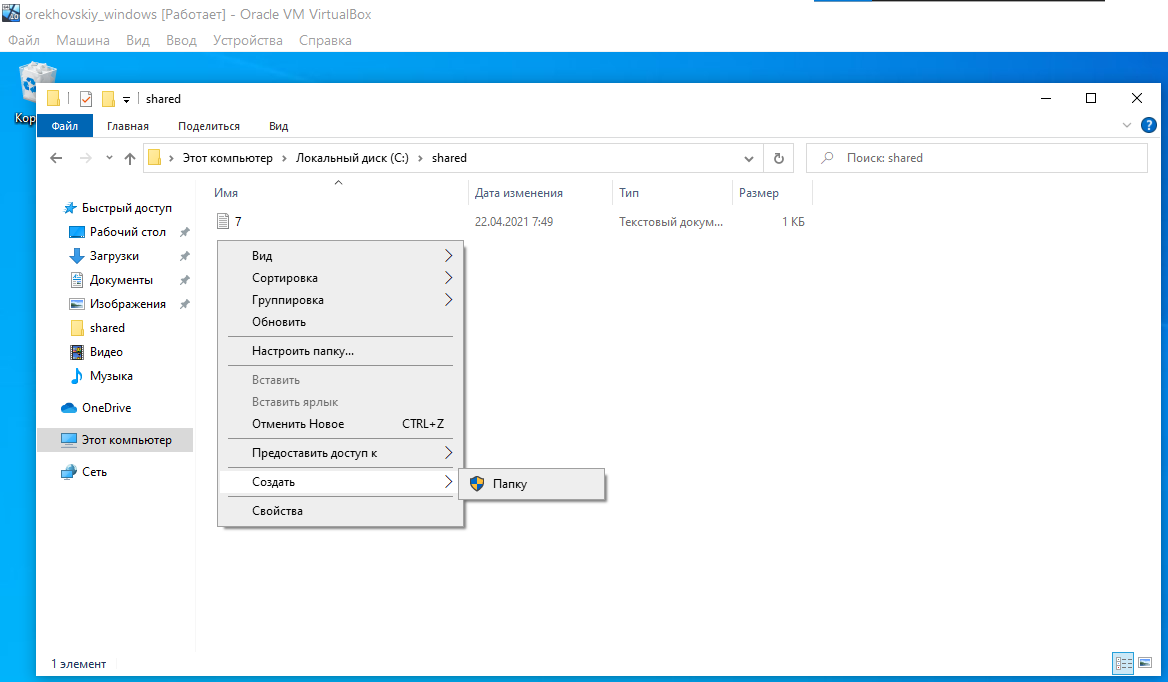
Для всех остальных пользователей нужно создать правило на полный запрет к папке.



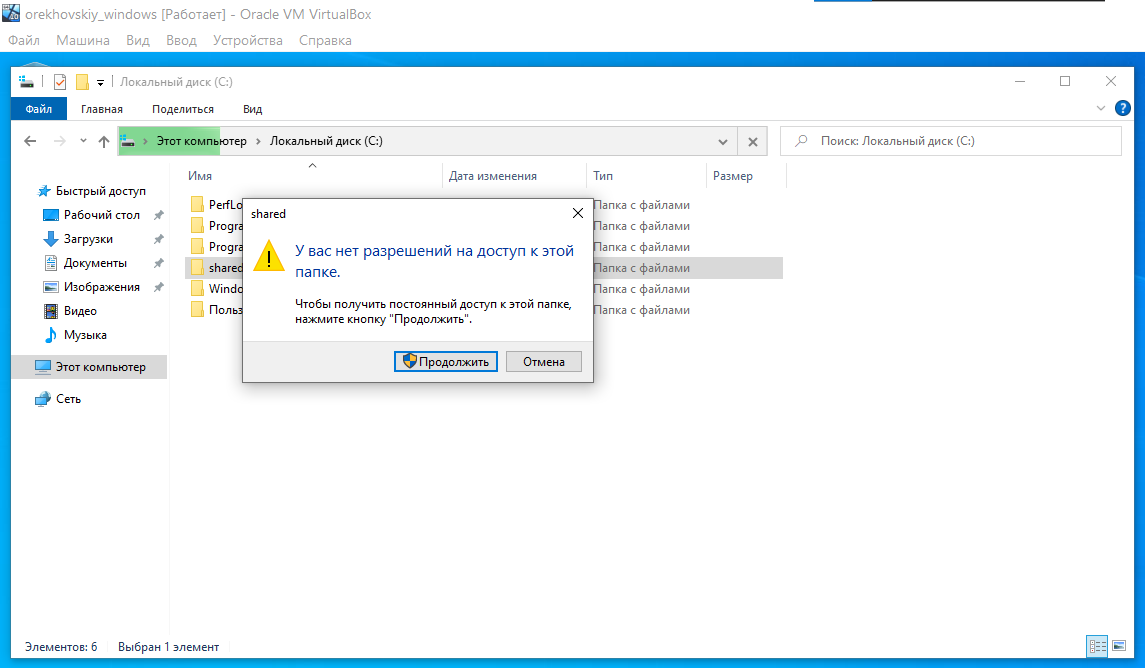
По итогам данных операций имеются следующие првила:



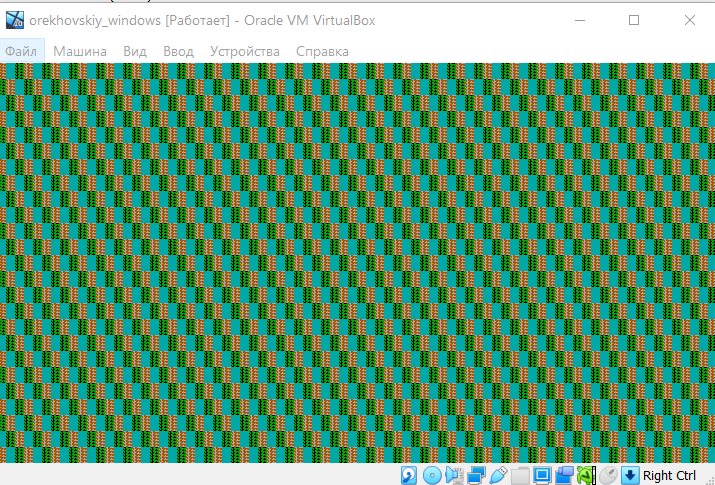
Проверим создание папки и увидим, что создавать мы не можем в данном пользователе.



Доступ к данной папке с другого пользователя, ожидаемо, запрещен.

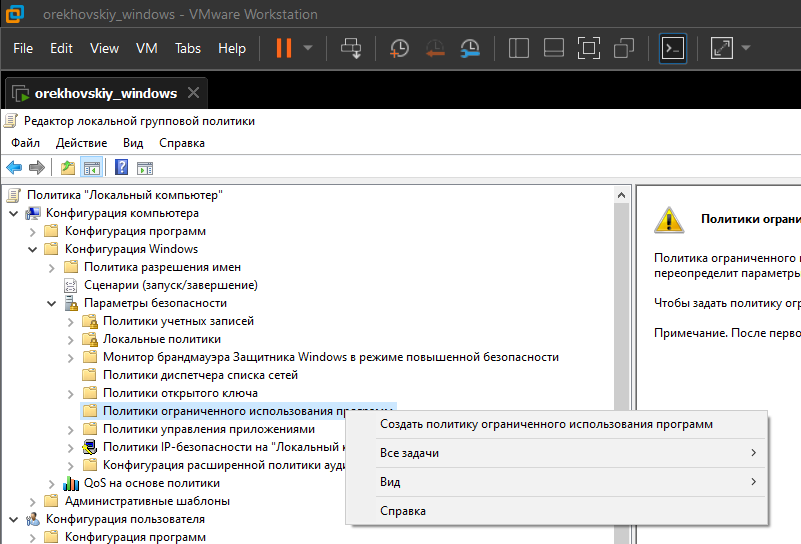


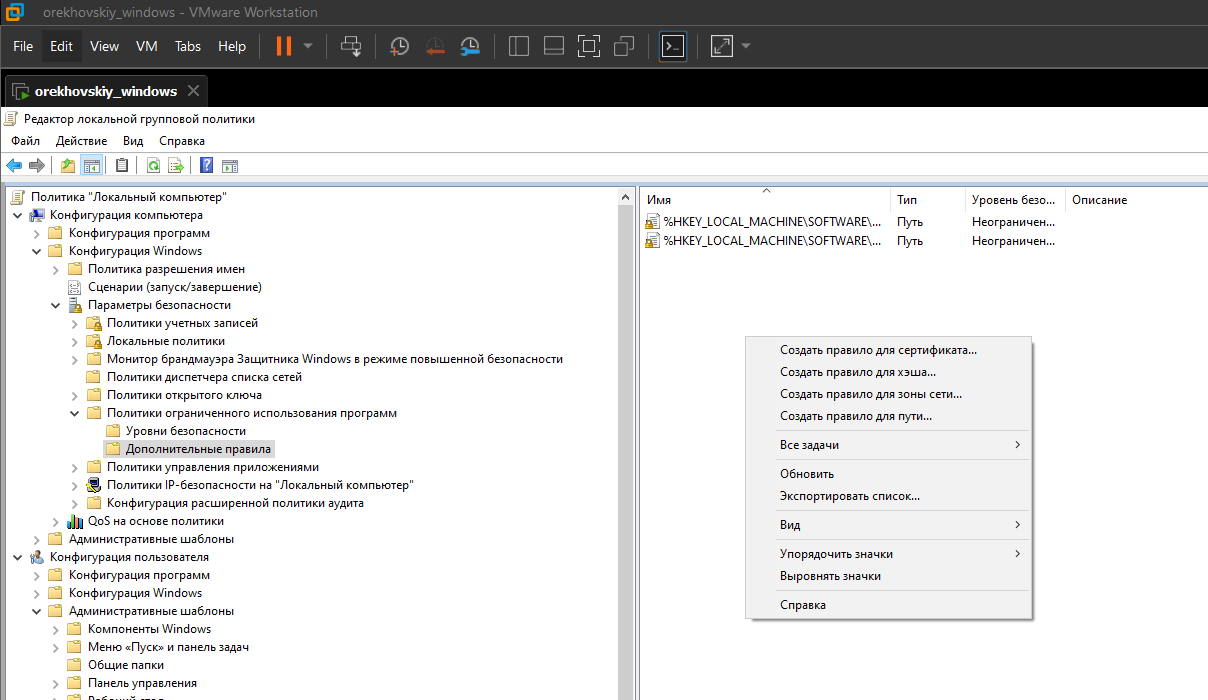
# Часть 5. Разрешите средствами операционной системы выполнять системные и прикладные программы только из папок %ProgramFiles% и %SystemRoot%



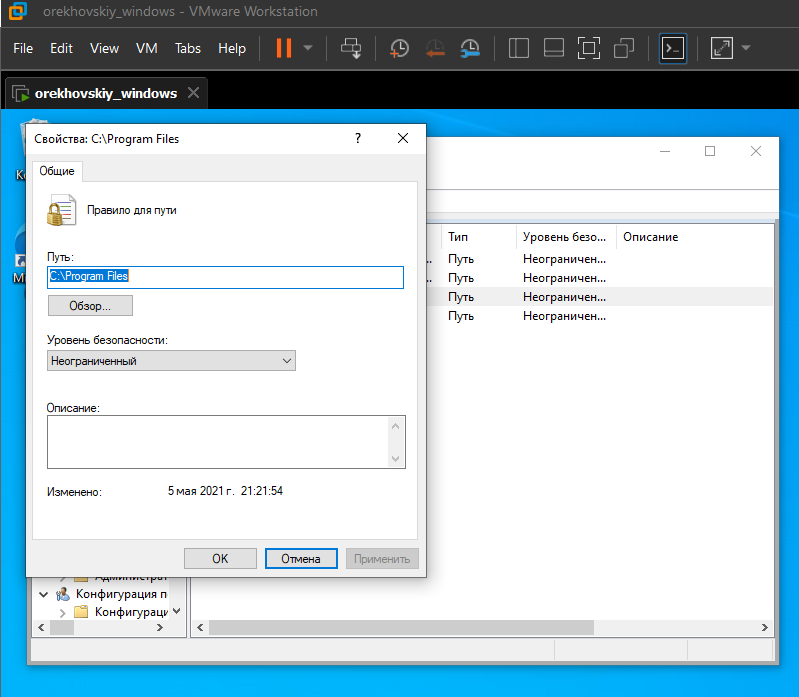
Так как VirtualBox решил сыграть в ящик, дальнейшее выполнение работы производилось в VMWare

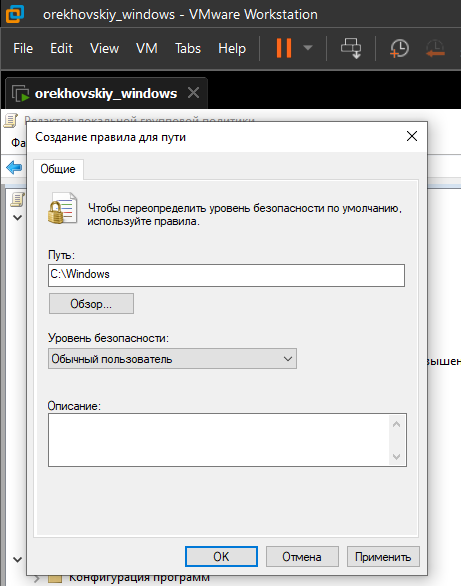
Для таких хитрых манипуляций потребуется редактор локальной групповой политики. Запустив его, необходимо перейти во вкладку Конфигурация компьютера, конфигурация Windows, параметры безопасности, политики ограниченного использования программ. Так как у меня таких политик не было по умолчанию, их необходимо создать. Далее необходимо добавить дополнительные правила, которые разрешат выполнение файлов из указанных директорий.



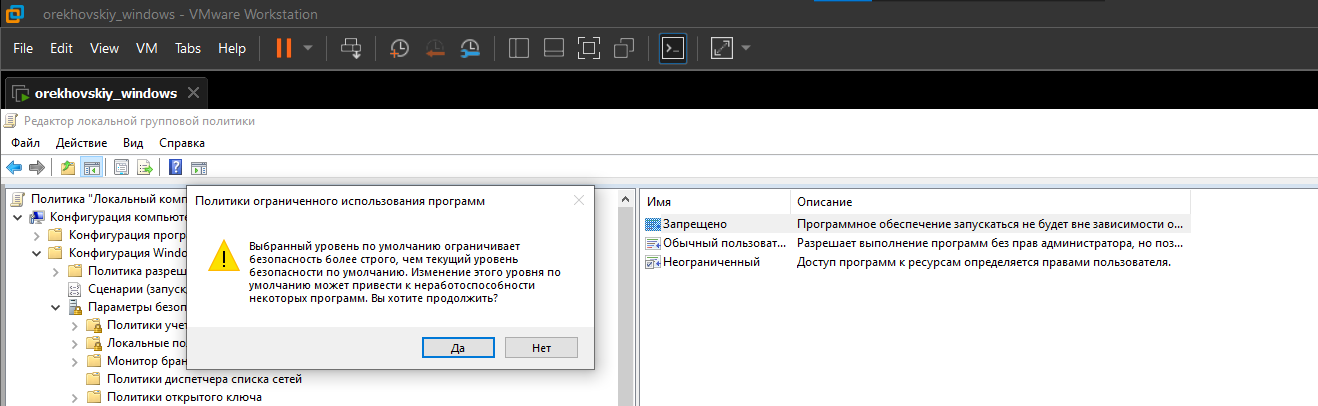


Добавляем дополнительные правила для папок “C:\Program Files” и “C:\Windows”. Уровень безопасности выбираем неограниченный, что соответствует правам пользователя.





Далее необходимо установить по умолчанию правило Запрещено.



В итоге приложения из папок не указанных ранее не запускаются.

