

Федеральное государственное автономное образовательное
учреждение высшего образования

Университет ИТМО

Дисциплина: Информационная безопасность

Лабораторная работа Windows 2

Разграничение доступа к объектам файловой системы

Вариант 12 -> 2

Работу выполнил студент группы Р34111:
Кривоносов Егор Дмитриевич

Преподаватель:
Маркина Татьяна Анатольевна

2022 г.

г. Санкт-Петербург

Содержание

Цель работы	3
Программные и аппаратные средства, используемые при выполнении работы:	3
Основная часть	4
1. Минимальный набор разрешений (прав доступа)	4
2. Преобразуйте файловую систему FAT (File Allocation Table) в NTFS (New Technology File System)	5
Способ 1 (форматирование с потерей данных)	5
Способ 2 (форматирование через командную строку без потери данных)	11
3. Выполните задание в соответствии с номером варианта, 1 – для нечетных вариантов, 2 – для четных вариантов	13
4. Выполните задание в соответствии с номером варианта.	17
5. Разрешите средствами операционной системы выполнять системные и прикладные программы только из папок %ProgramFiles% и %SystemRoot%	21
Дополнительная часть	27
Задание 2	27
Выполнение	27
Задание 3	28
Выполнение	28
Способ 1 - через проводник	28
Способ 2 - через команду icacls	30
Способ 3 - при помощи команд в PowerShell	30
Вывод	31

Цель работы

Изучить объекты файловой системы, ознакомиться с основными принципами управления доступом к файловым системам. Изучить основные способы настройки доступа к объектам файловой системы.

Программные и аппаратные средства, используемые при выполнении работы:

Для выполнения работы было использовано ПО Oracle VM VirtualBox.
Характеристики созданной виртуальной машины:

Характеристики устройства

Имя устройства	DESKTOP-DC30ER7
Процессор	AMD Ryzen 5 4600H with Radeon Graphics 2.99 GHz
Оперативная память	4,00 ГБ
Код устройства	08343D81-55F0-4E98-8B53-80834E7D1A69
Код продукта	00330-80000-00000-AA178
Тип системы	64-разрядная операционная система, процессор x64
Перо и сенсорный ввод	Для этого монитора недоступен ввод с помощью пера и сенсорный ввод

Основная часть

1. Минимальный набор разрешений (прав доступа)

а) Загрузки операционной системы

Название объекта доступа	Администратор	Пользователь
smss.exe	rx	
csrss.exe	rx	
lsass.exe	rx	
winlogon.exe	rx	
services.exe	rx	
C:/Windows/System32	rx	rx

б) Вход пользователя (User_№варианта) и Администратора (Admin_№варианта) в систему

Название объекта доступа	Администратор	Пользователь
%UserProfile%	rwX	rwX
Secur32.dll	rx	rx

в) Работы с приложениями, установленными администратором

Название объекта доступа	Администратор	Пользователь
%AppData%	rx	rx
%LocalAppData%	rx	rx
*.exe	rx	rx
*.dll	rx	rx

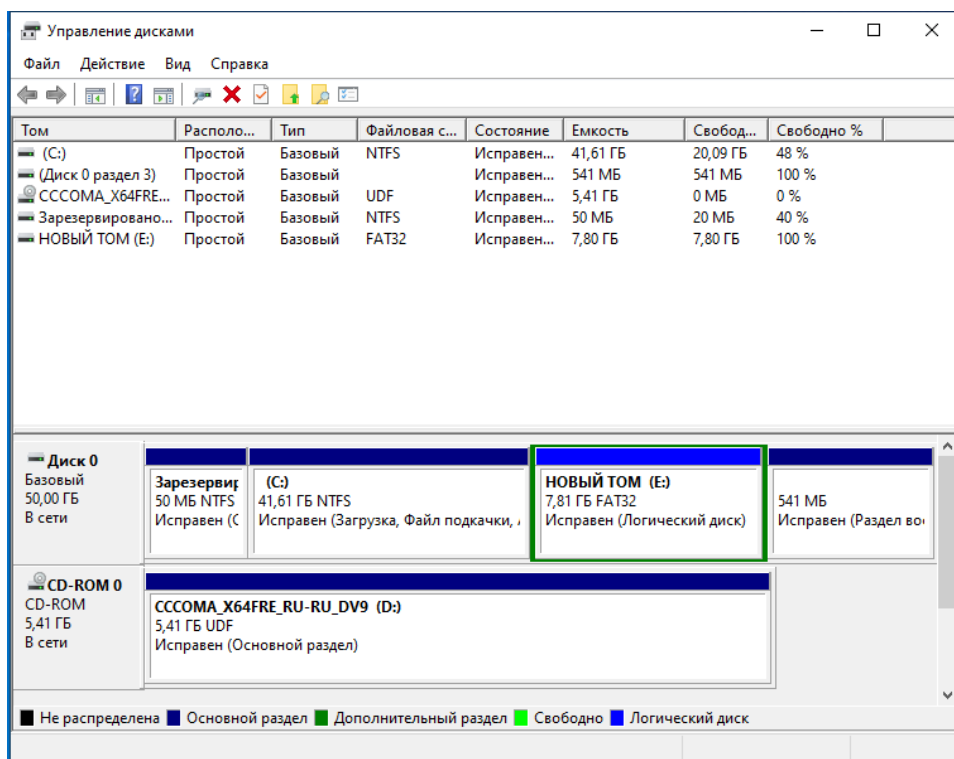
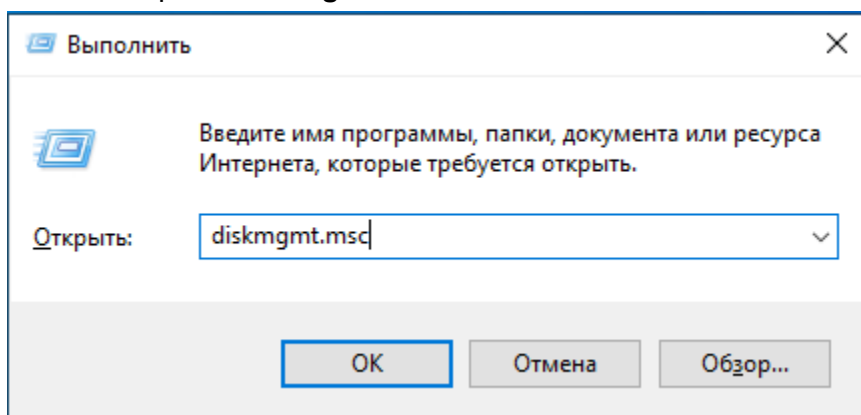
2. Преобразуйте файловую систему FAT (File Allocation Table) в NTFS (New Technology File System)

Способ 1 (форматирование с потерей данных)

Нам нужно открыть раздел: **Управление дисками**. Существует 2 способа.

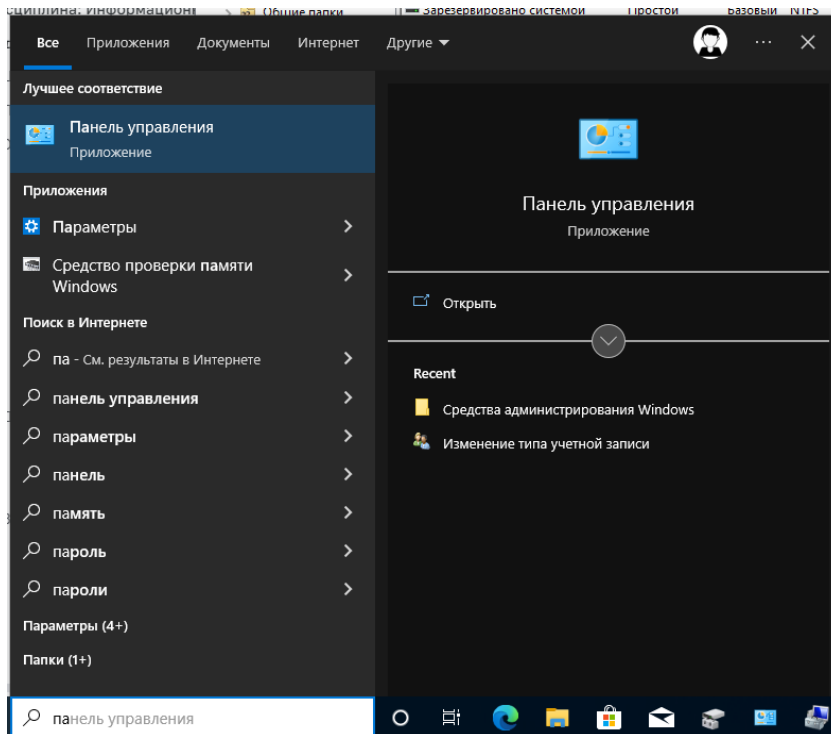
Первый:

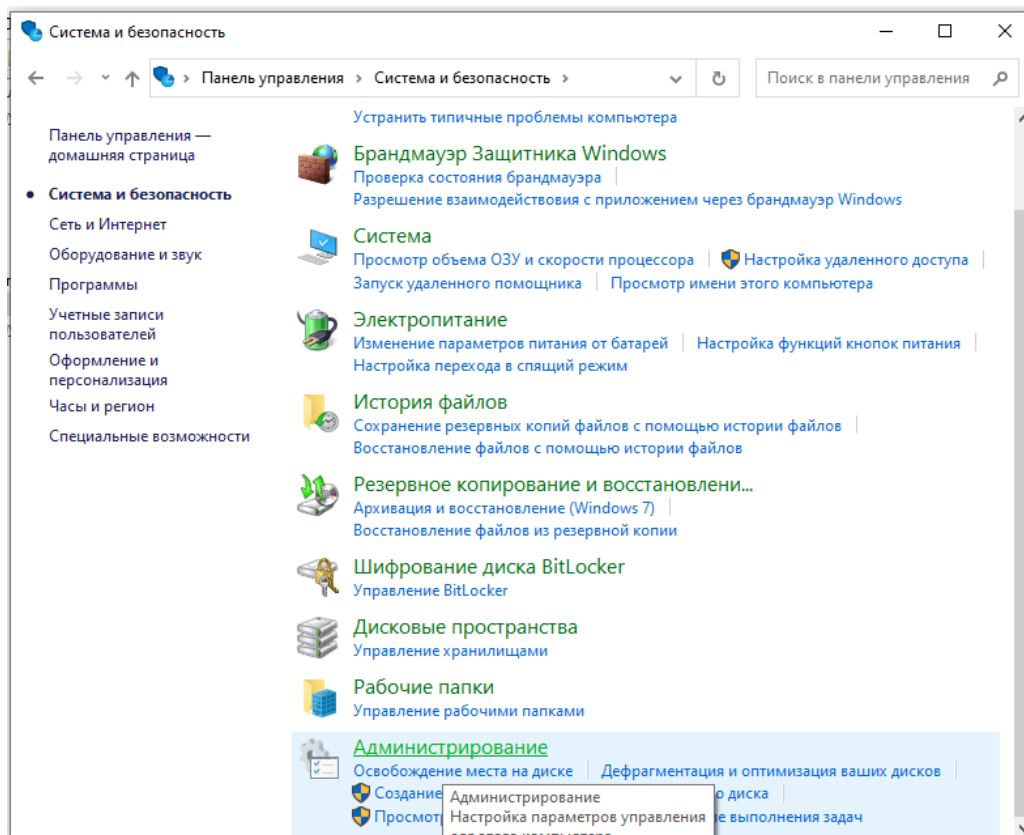
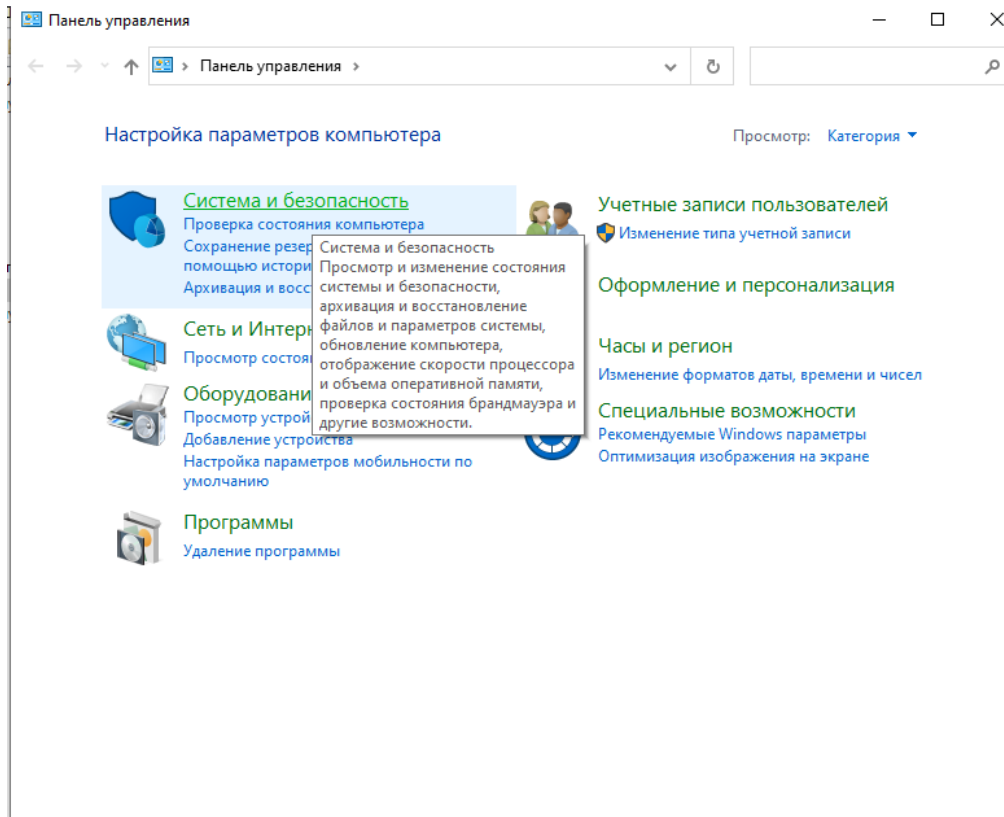
1. Нажать сочетание клавиш **Win + R**
2. Ввести в строке: **diskmgmt.msc**

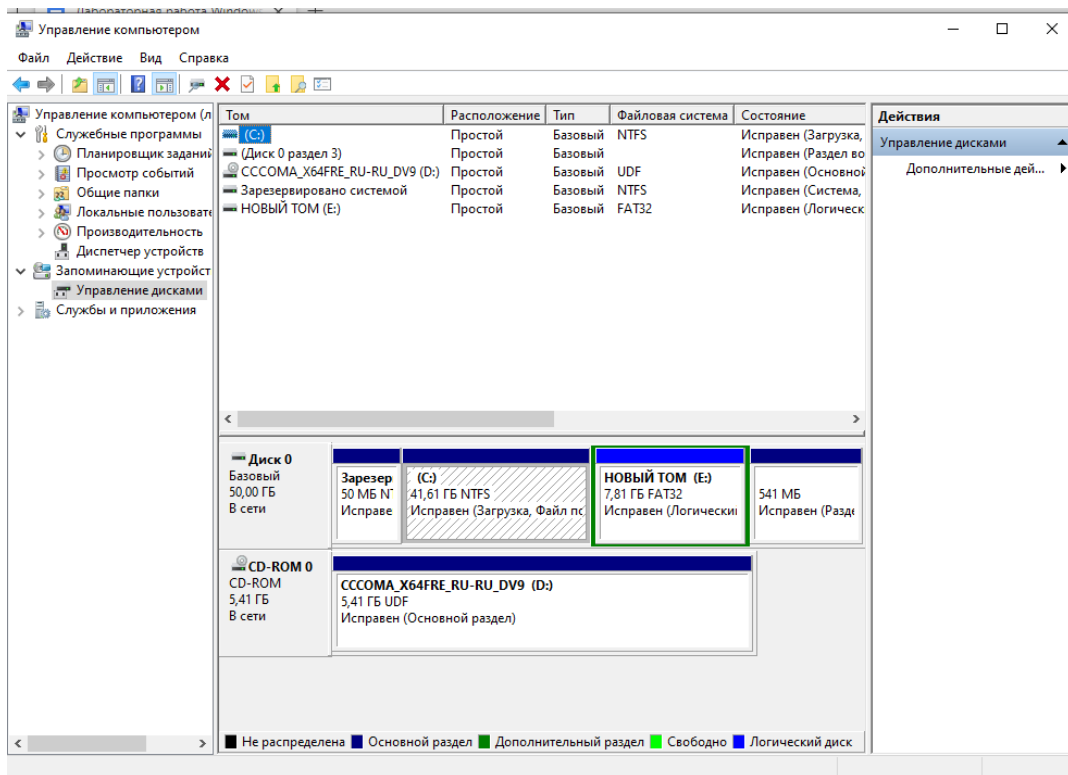
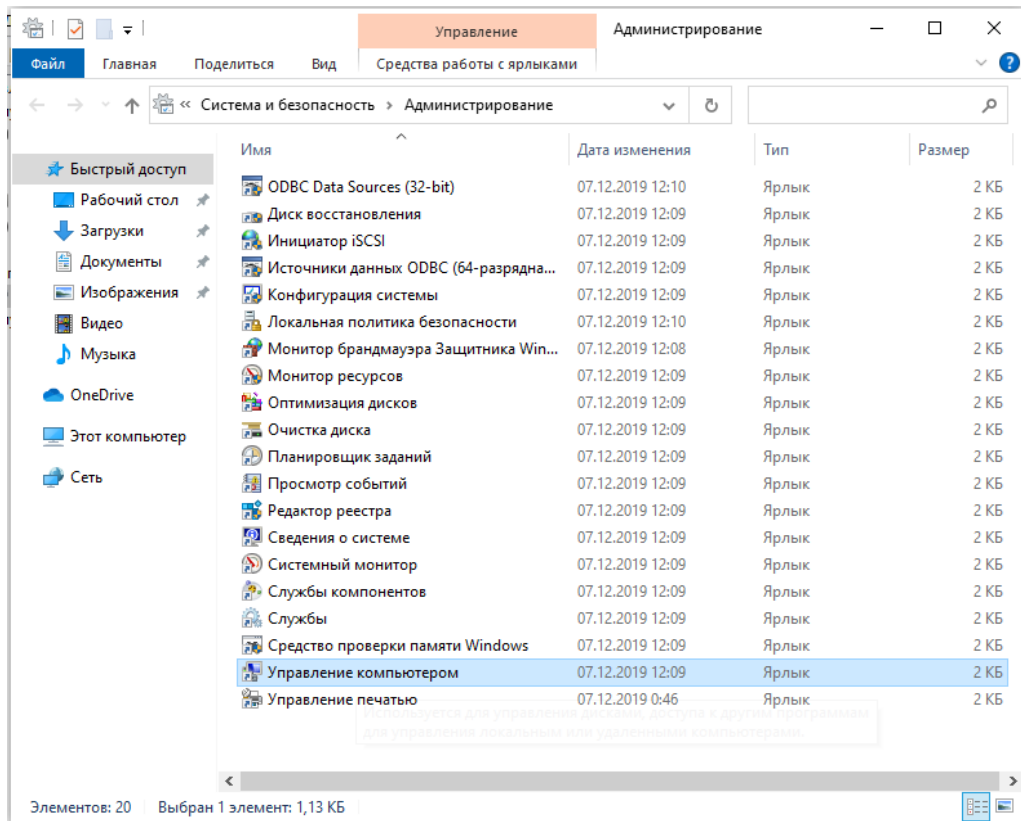


Второй:

1. Открыть: **Панель управления** -> **Система и безопасность** -> **Администрирование**
2. Затем дважды нажать на **Управление компьютером**
3. На расположенной слева панели в разделе **Запоминающие устройства** выбрать **Управление дисками**

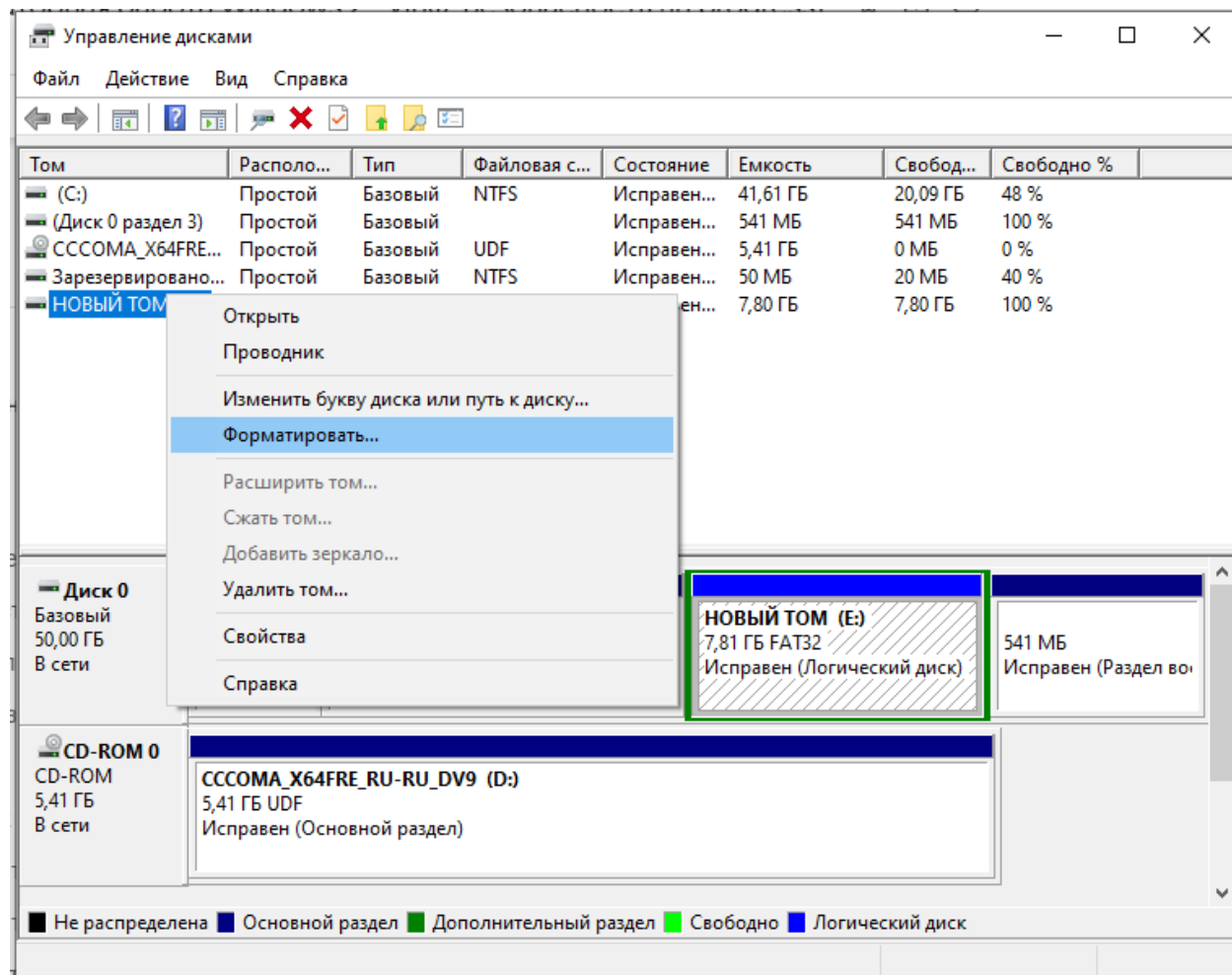




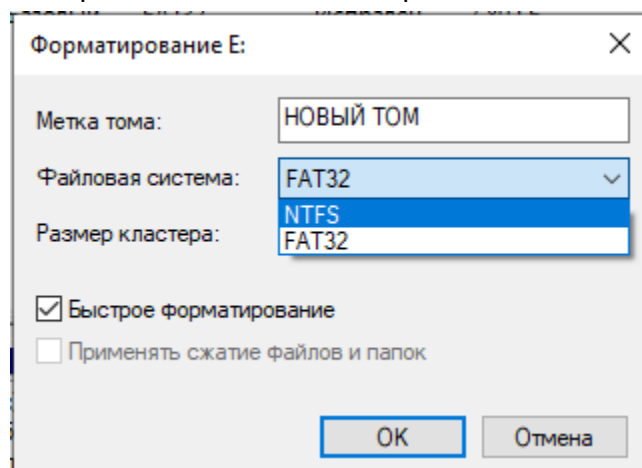


Теперь приступим к преобразованию файловой системы из FAT32 в NTFS

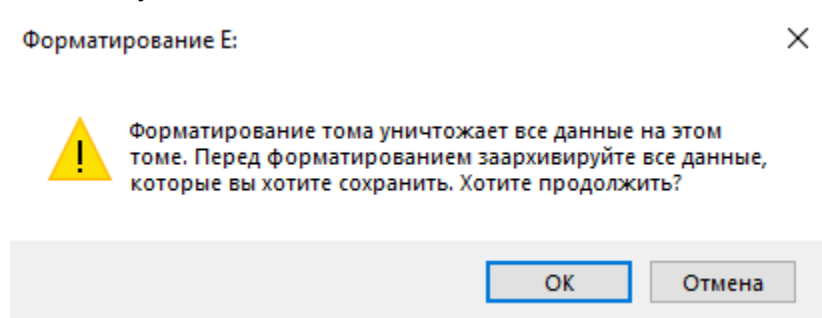
Нажимаем правой кнопкой мыши по Тому (в данном случае это **Том E:**) ->
Форматировать



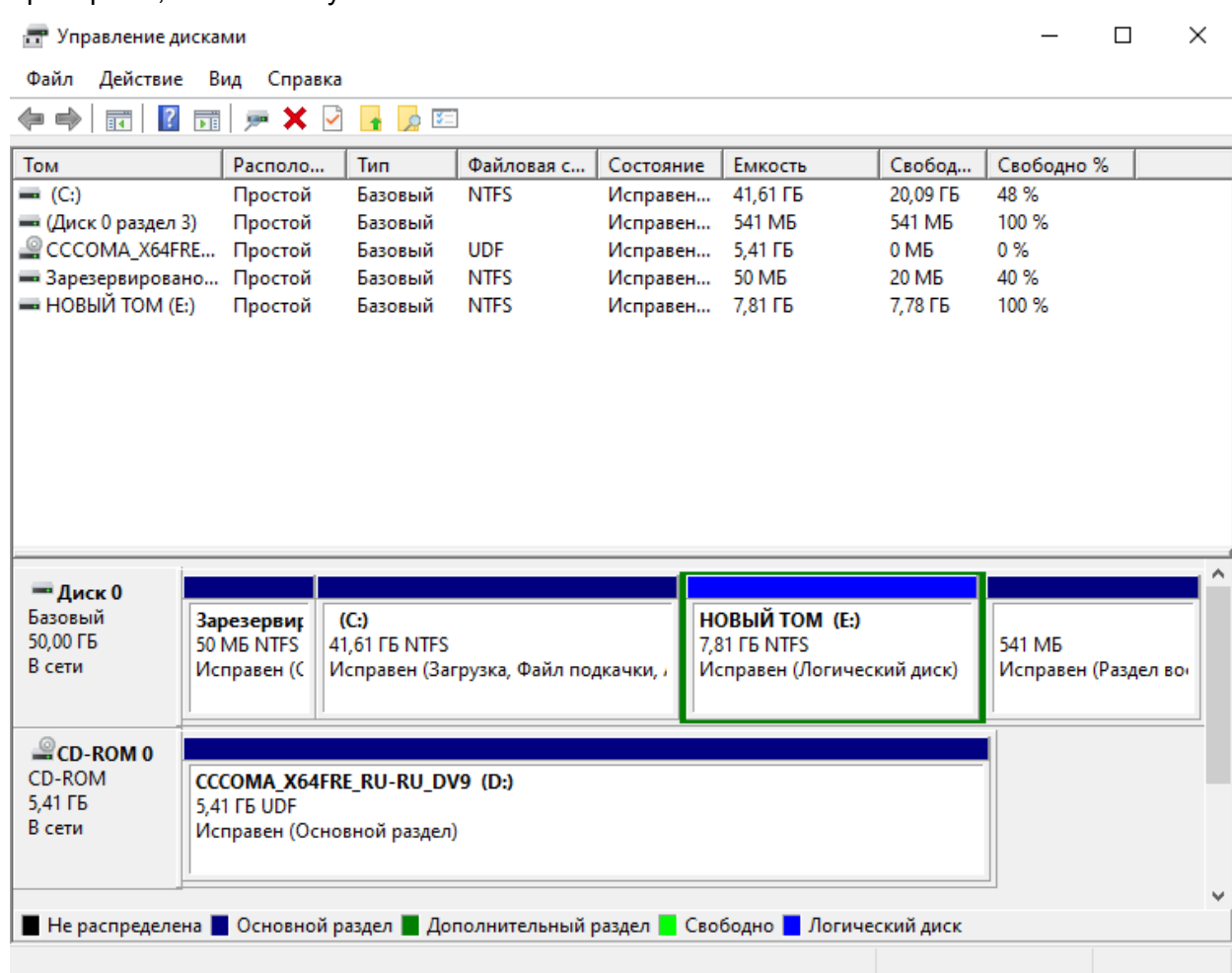
Выбираем **NTFS** в качестве файловой системы и нажимаем **“OK”**



Нас предупреждают, что данные будут уничтожены. А мы просто нажимаем “ОК” т.к. На всякий случай я сделал снимок VM.

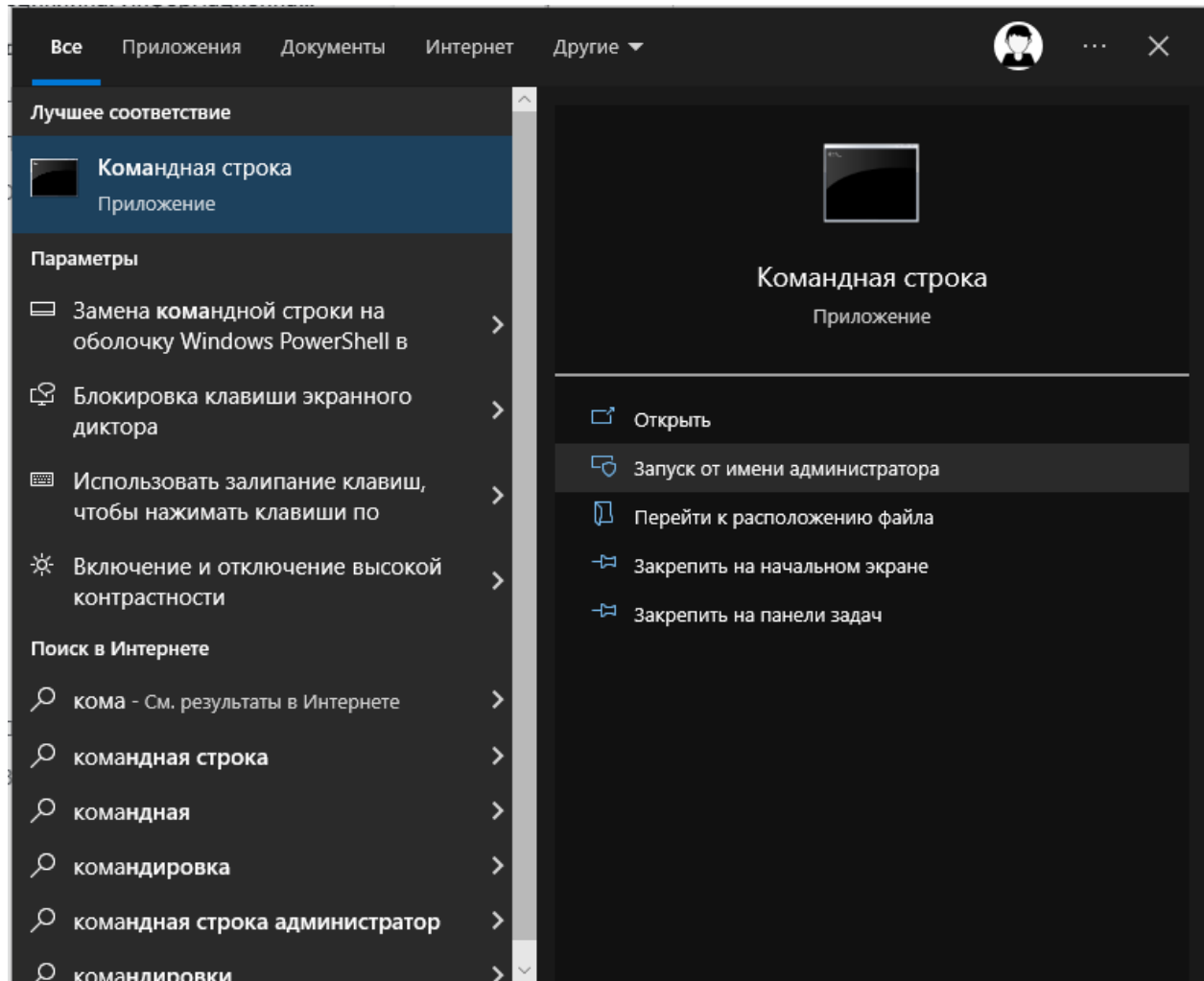


Проверяем, что все получилось



Способ 2 (форматирование через командную строку без потери данных)

Запускаем “Командная строка” от имени администратора.



Выбираем необходимый том с помощью команды: **LABEL E:**

Далее вводим метку тома: **E**

```
C:\Windows\system32>LABEL E:
Том в устройстве E: имеет метку НОВЫЙ ТОМ
Серийный номер тома: A478-53D2
Метка тома (11 символов, ENTER - метка не нужна): E

C:\Windows\system32>
```

Для преобразования файловой системы вводим команду: **convert E: /fs:ntfs**
Далее вводим метку тома: **E**

```
C:\Windows\system32>convert E: /fs:ntfs
Тип файловой системы: FAT32.
Введите метку тома для диска E: E
Том E создан 06.11.2022 17:14
Серийный номер тома: A478-53D2
Проверка файлов и папок...
Проверка файлов и папок завершена.

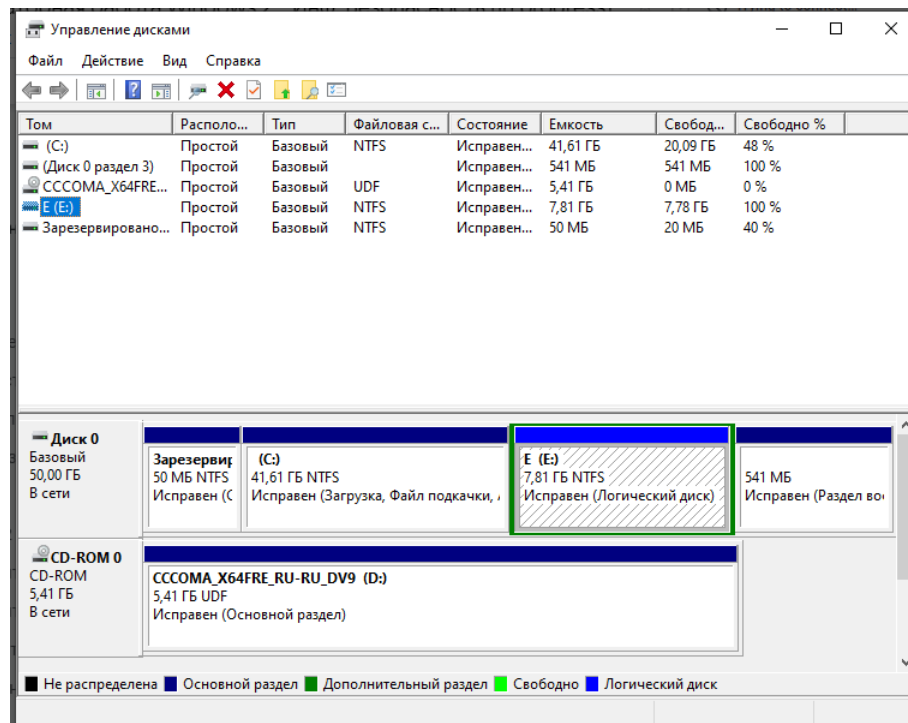
Windows проверила файловую систему и не обнаружила проблем.
Дальнейшие действия не требуются.
  8 174 592 КБ всего на диске.
    4 КБ в 1 скрытых файлах.
    8 КБ в 2 файлах.
  8 174 576 КБ доступно.

    4 096 байт в каждой единице распределения.
Всего единиц распределения на диске:    2 043 648.
Доступно единиц распределения на диске:    2 043 644.

Оценка места на диске, необходимого для преобразования файловой системы...
Всего на диске:    8190976 КБ
Свободно:    8174576 КБ
Необходимо для преобразования:    23006 КБ
Преобразование файловой системы
Преобразование завершено

C:\Windows\system32>
```

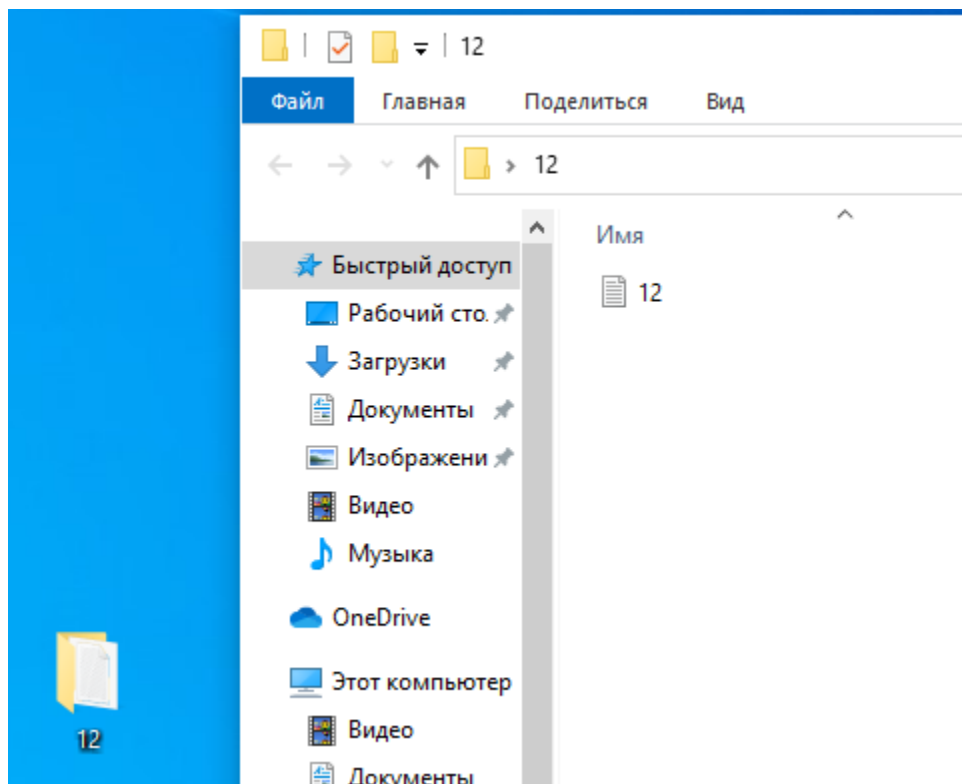
Проверяем, что все получилось



3. Выполните задание в соответствии с номером варианта, 1 – для нечетных вариантов, 2 – для четных вариантов

Какие разрешения (права доступа) будут у Пользователя и у Администратора на файл «№варианта.txt», если владельцем папки «№варианта» является Пользователь, для пользователя установлено разрешение «Чтение» («Read»), для Администратора установлено разрешение «Полный доступ» («Full control»), а для группы «Все» («Everyone») (оба пользователя входят в группу) – не установлены разрешения (установлено «No Access»)?

Создадим папку с названием **12** и в ней создадим файл с названием **12.txt**
Для пользователя установим разрешение только Чтение.

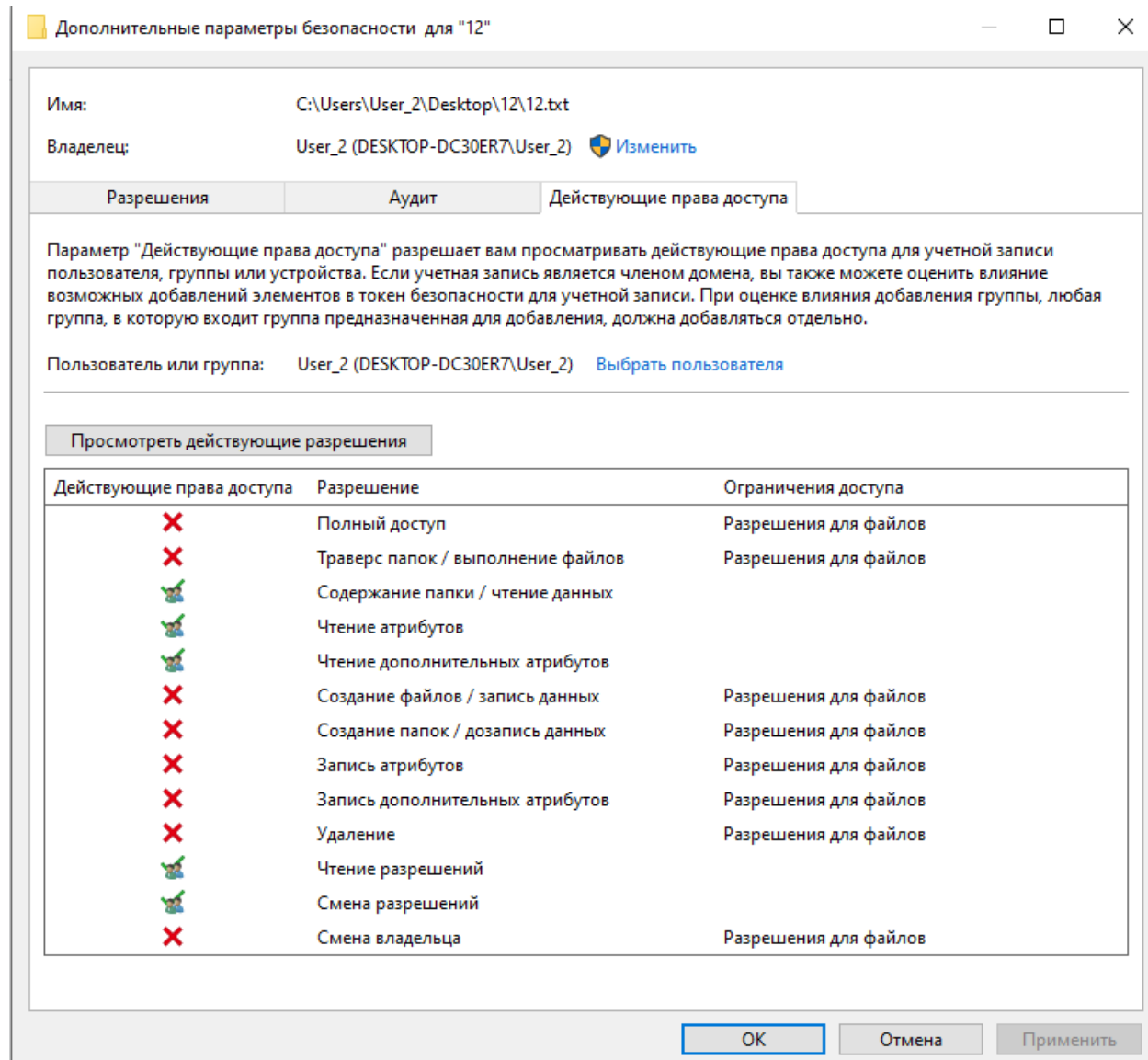


Права на файл наследуются от прав на директорию, поэтому у **Пользователя** на файл есть только доступ на чтение, а у **Администратора** - полный доступ.

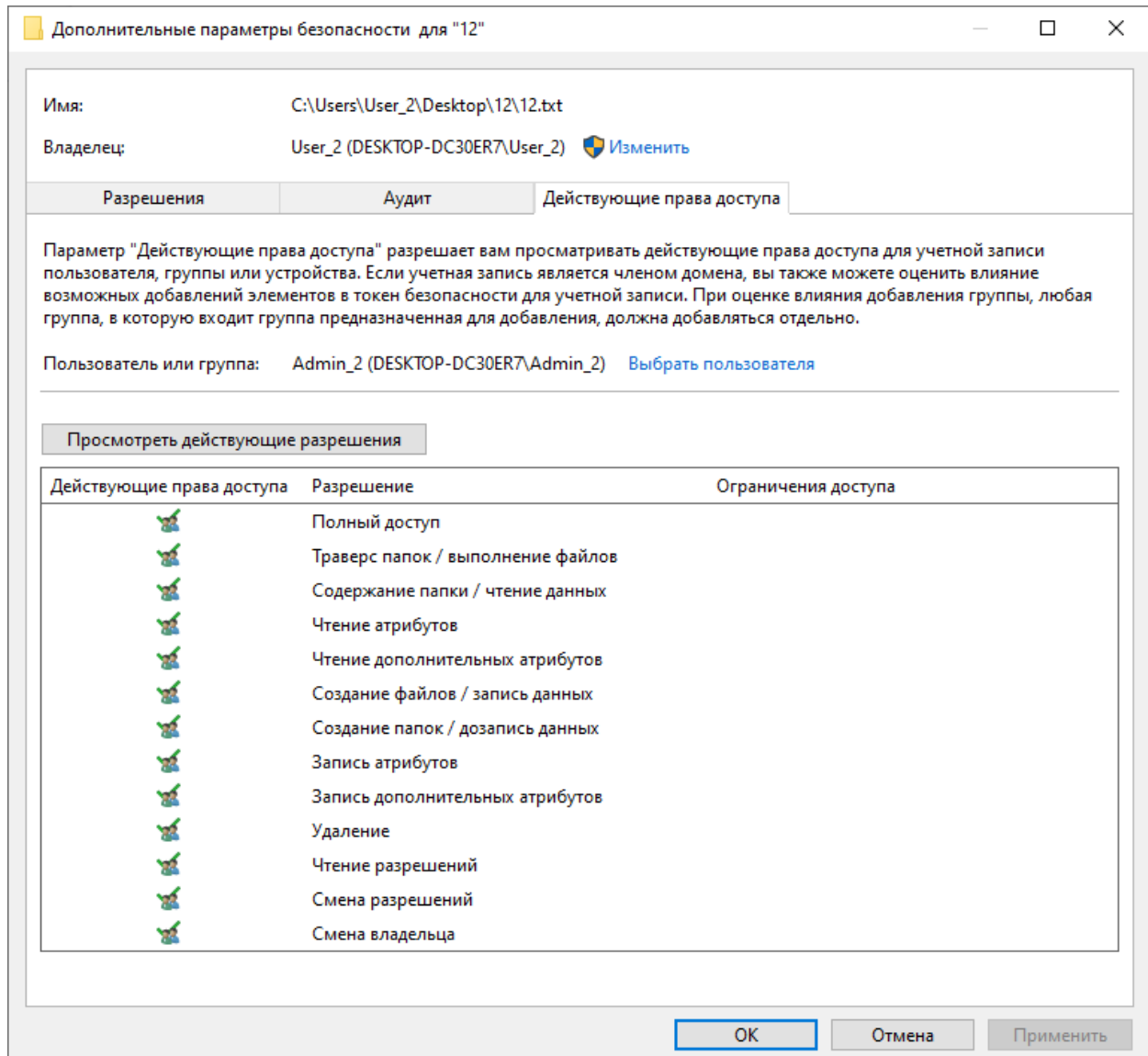
Ниже показаны права доступа на папке. Изначально у Пользователей был доступ “Чтение и выполнение”, который возможно было отключить только при отключении наследования.

Разр...	Администраторы (DESKTOP-DC30ER7\Ад...	Полный доступ	Нет
Разр...	User_2 (DESKTOP-DC30ER7\User_2)	Чтение	Нет

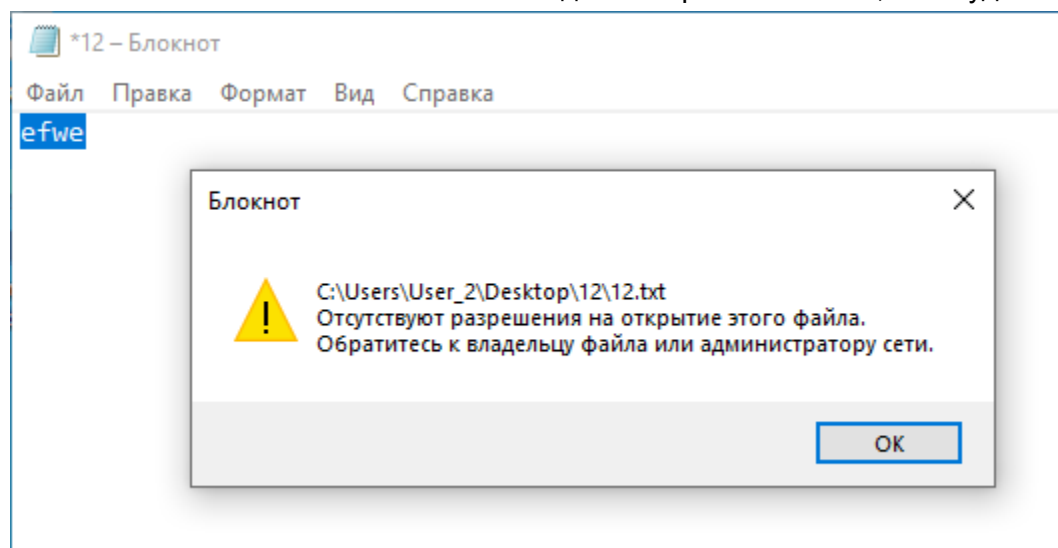
Дополнительные разрешения для Пользователей. Как видно, пользователям доступно только чтение файла и его свойства.



Дополнительные разрешения для Администратора. Ему предоставлен полный доступ, поэтому он может читать, выполнять, изменять (смена атрибутов и владельца) и удалять файл.



Соответственно изменить пользователь данный файл не может, как и удалять.



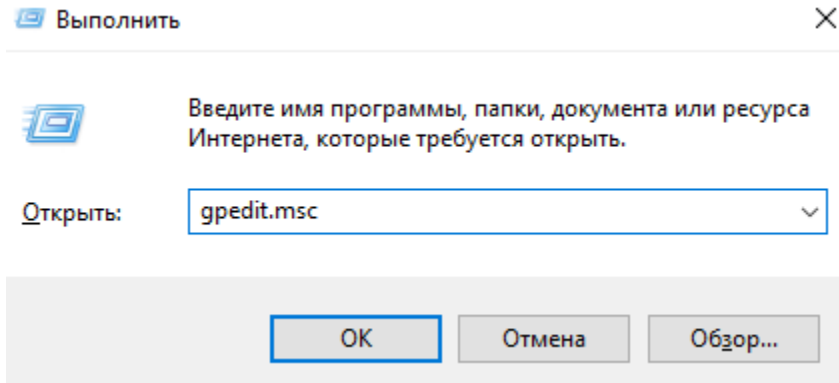
4. Выполните задание в соответствии с номером варианта.

Разрешить встроенными средствами ОС Windows только пользователю System запуск процессов из системного диска. Предотвратить возможность его модификации.

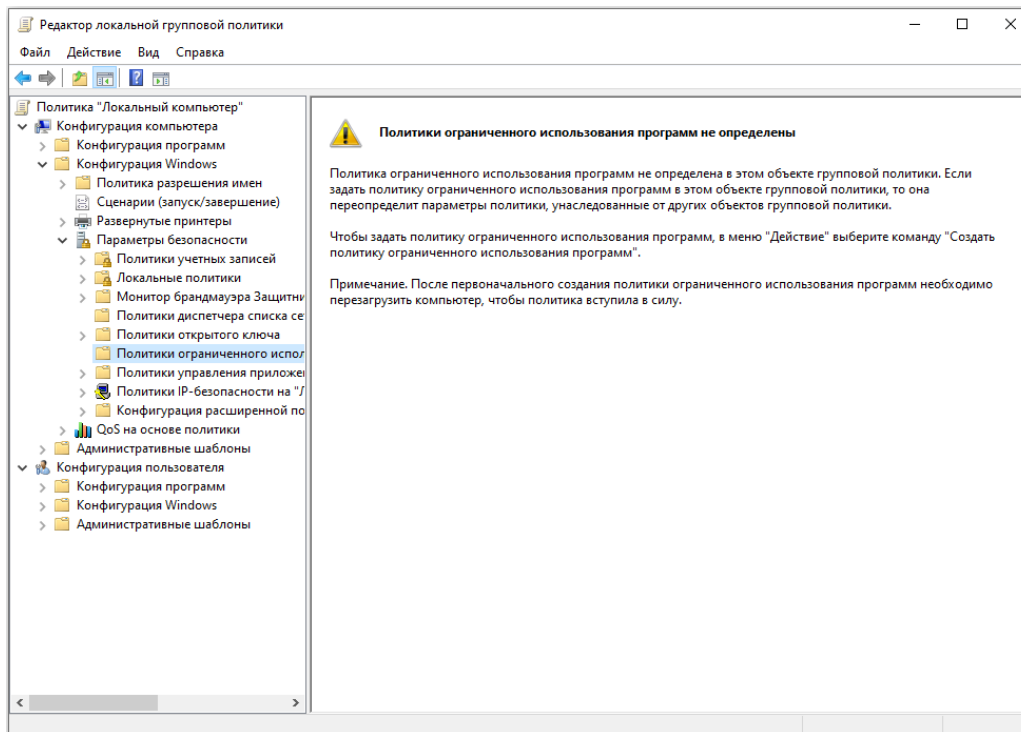
Проанализировать возможность и сложность настройки.

Нажать сочетание клавиш **Win + R**

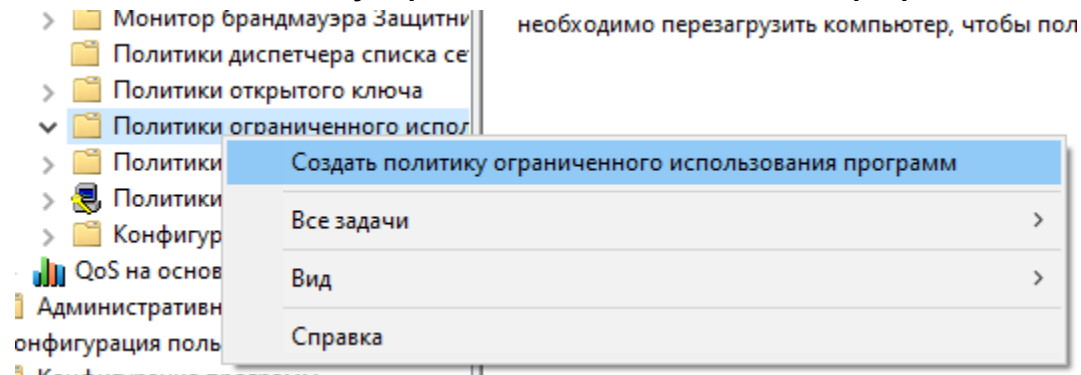
Ввести в строке: **gpedit.msc**



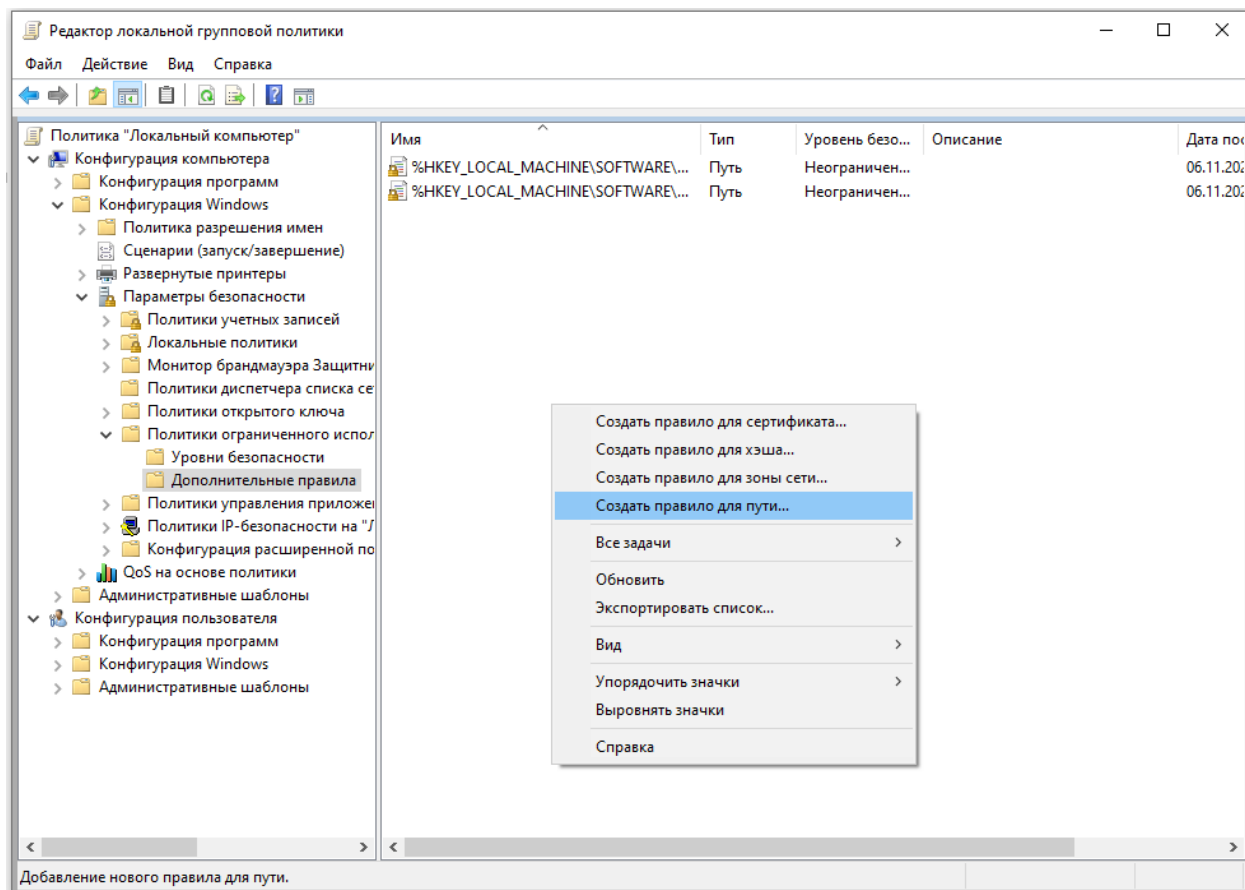
Переходим в: **Конфигурация компьютера -> Конфигурация Windows -> Параметры безопасности -> Политики ограниченного использования программ**



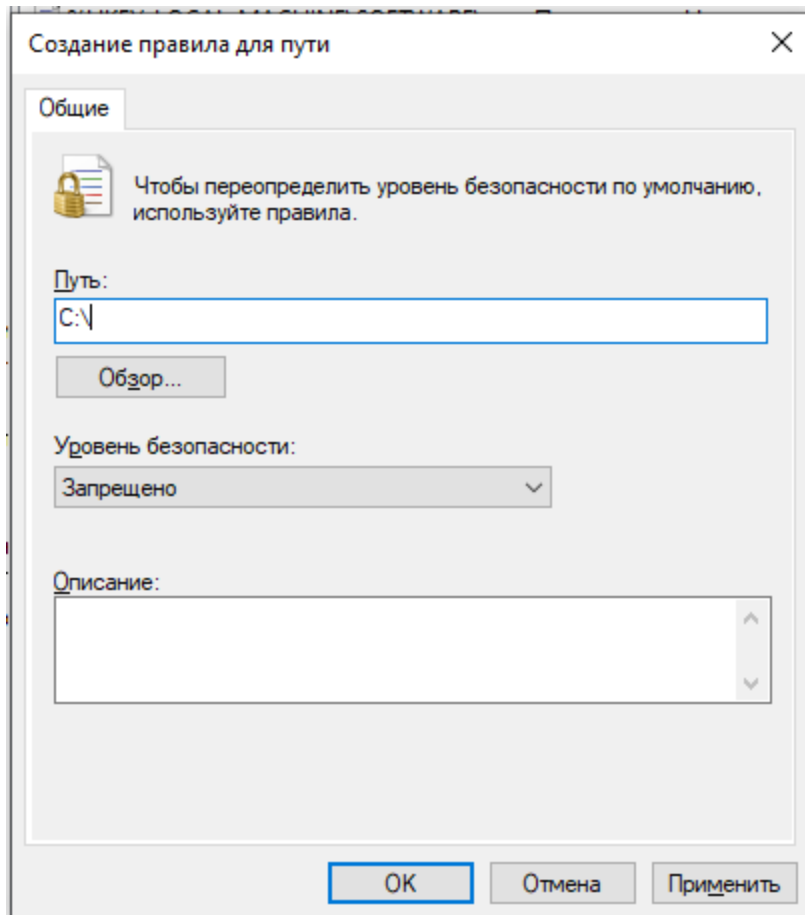
Кликаем правой кнопкой мыши по **Политики ограниченного использования программ** и затем: **Создать политику ограниченного использования программ**



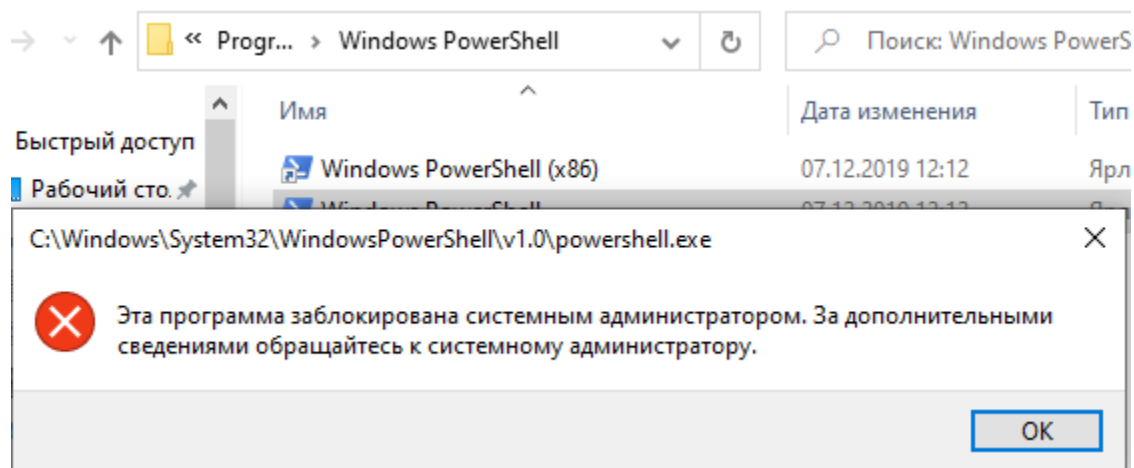
Создаем новое правило по пути...



В пути нужно прописать «C:\», в уровне защиты – **Запрещено**. При таком уровне пользователям нельзя запустить любой процесс, расположенный по этому пути (с учетом вложенных папок).



Проверим:



C:\Program Files\Internet Explorer\iexplore.exe



Эта программа заблокирована системным администратором. За дополнительными сведениями обращайтесь к системному администратору.

OK

C:\Windows\system32\gpedit.msc



Эта программа заблокирована системным администратором. За дополнительными сведениями обращайтесь к системному администратору.

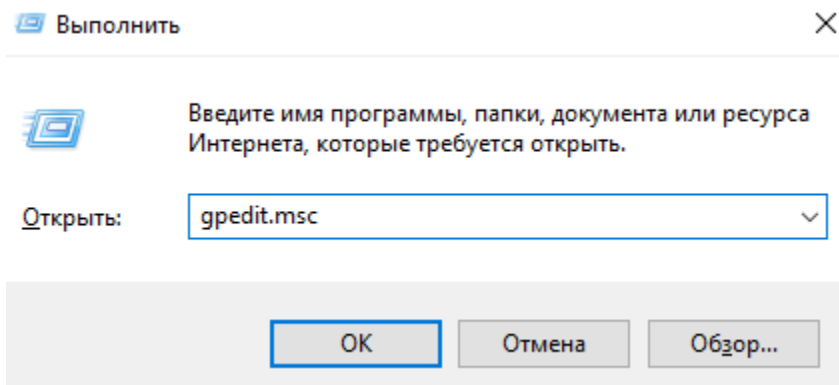
OK

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

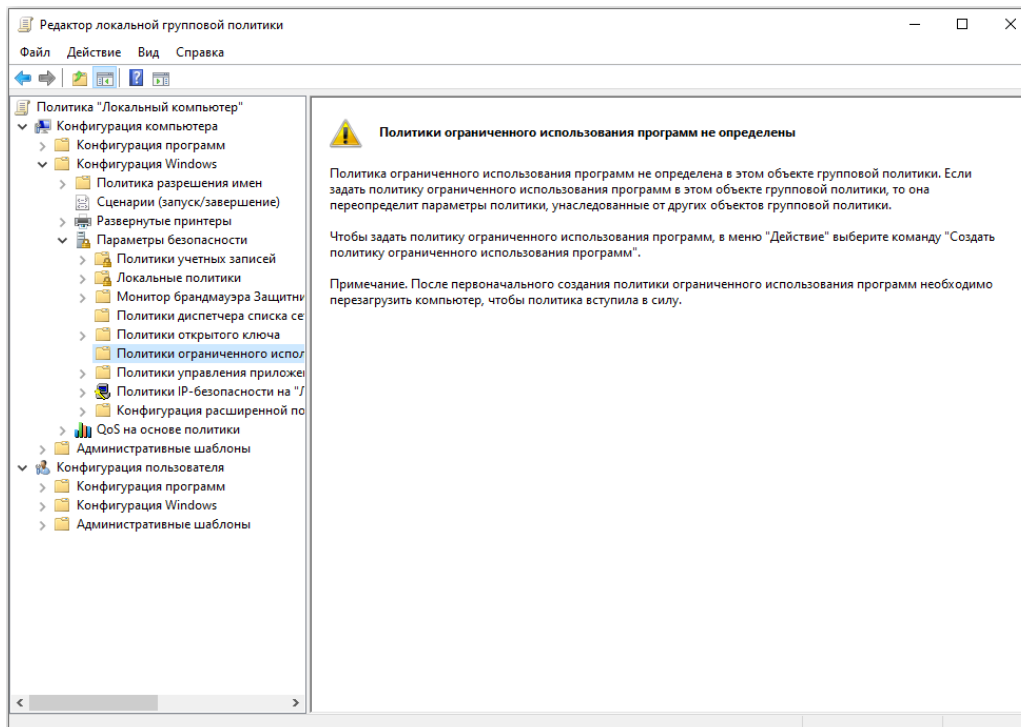
Для выполнения задания потребуются групповые политики. Надо добавить политику ограниченного использования программ. В ней добавить правила для путей, как показано на скриншоте.

Нажать сочетание клавиш **Win + R**

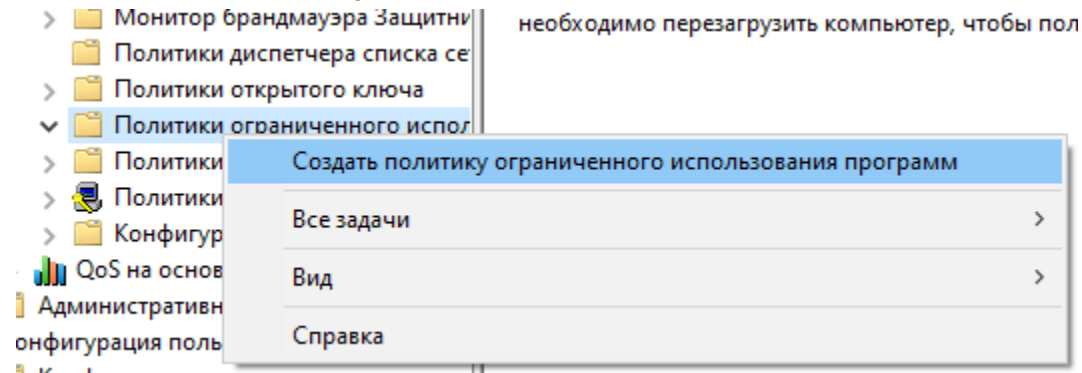
Ввести в строке: **gpedit.msc**



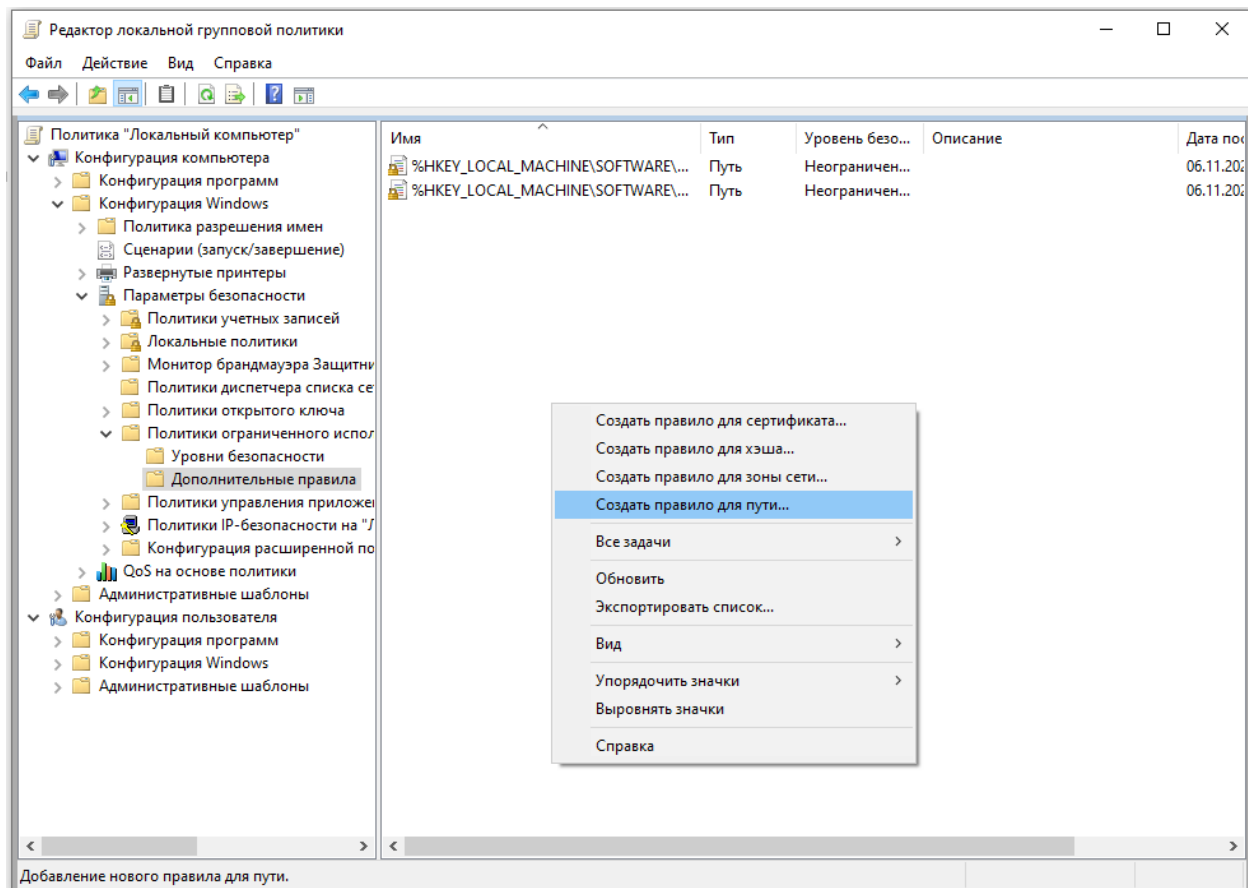
Переходим в: **Конфигурация компьютера -> Конфигурация Windows -> Параметры безопасности -> Политики ограниченного использования программ**



Кликаем правой кнопкой мыши по **Политики ограниченного использования программ** и затем: **Создать политику ограниченного использования программ**




Создаем новое правило по пути...



Свойства: %ProgramFiles%

Общие

 Правило для пути

Путь:
%ProgramFiles%

Обзор...

Уровень безопасности:
Неограниченный


Описание:

Изменено: 6 ноября 2022 г. 18:17:20

OK Отмена Применить

Свойства: %SystemRoot%

Общие

 Правило для пути

Путь:
%SystemRoot%



Обзор...

Уровень безопасности:
Неограниченный

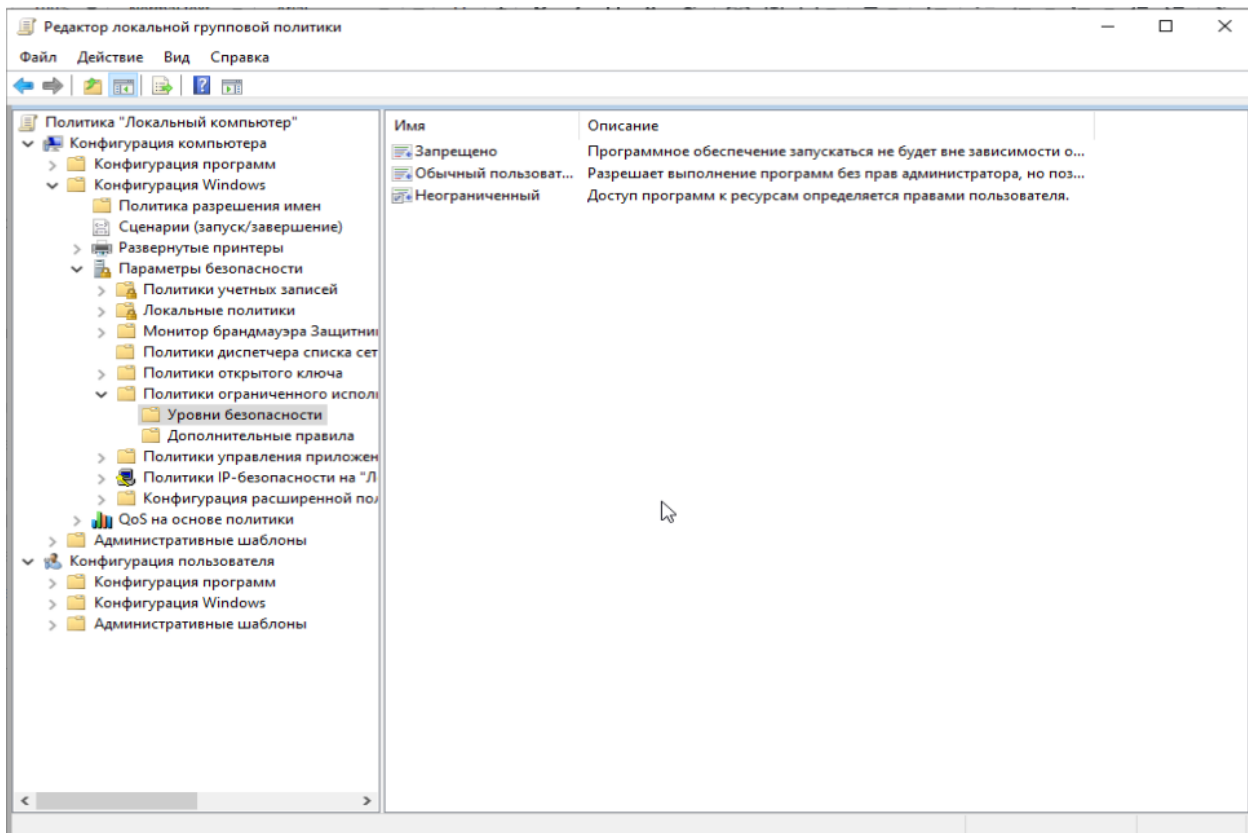
Описание:

Изменено: 6 ноября 2022 г. 18:17:40

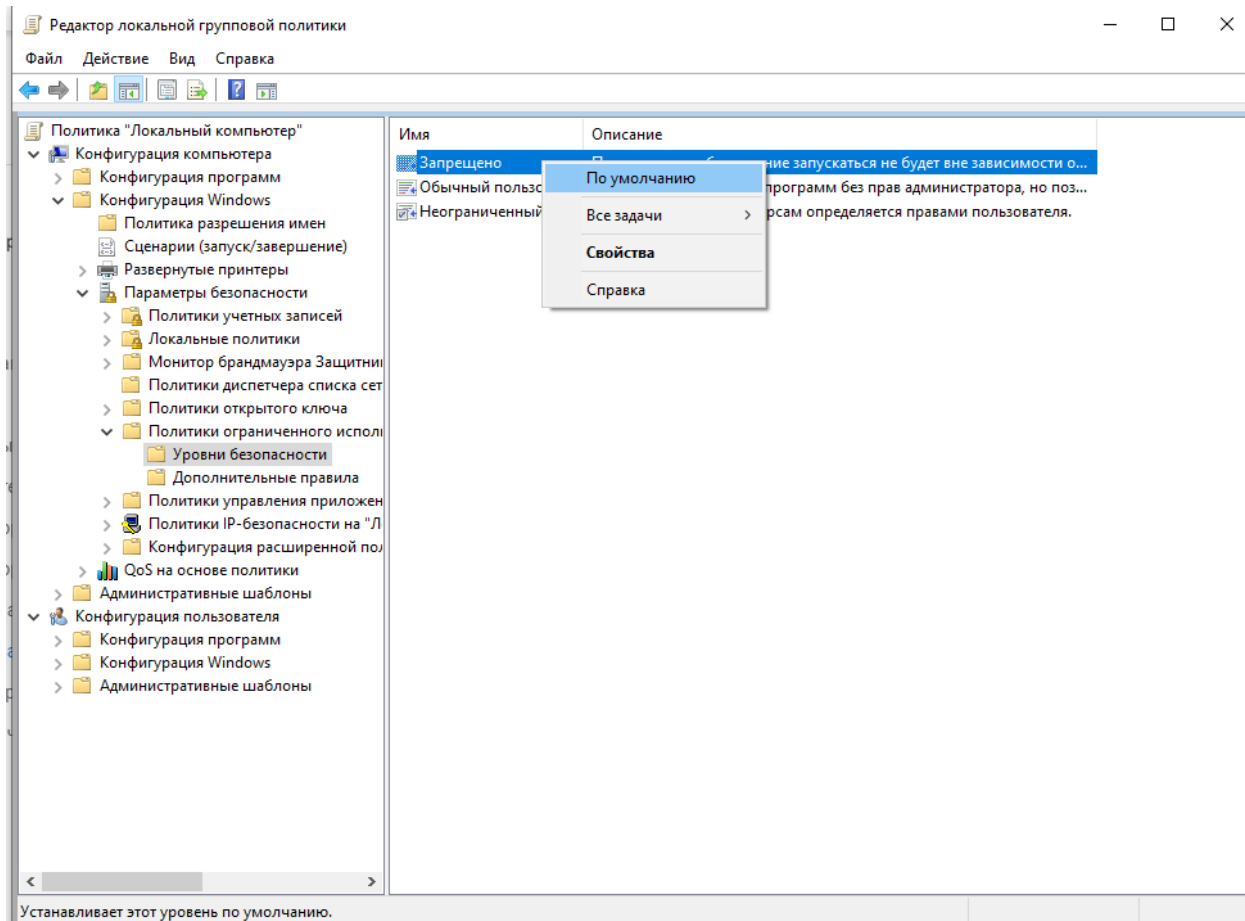
OK Отмена Применить

	C:\	Путь	Запрещено
	%ProgramFiles%	Путь	Неограничен...
	%SystemRoot%	Путь	Неограничен...

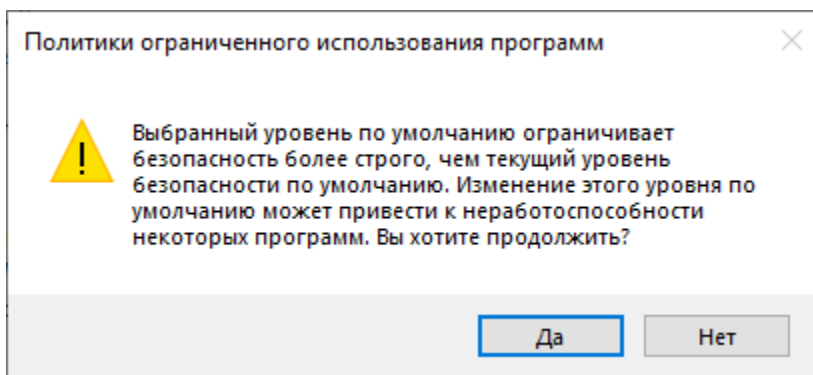
Переходим в: **Конфигурация компьютера -> Конфигурация Windows -> Параметры безопасности -> Политики ограниченного использования программ -> Уровни безопасности**



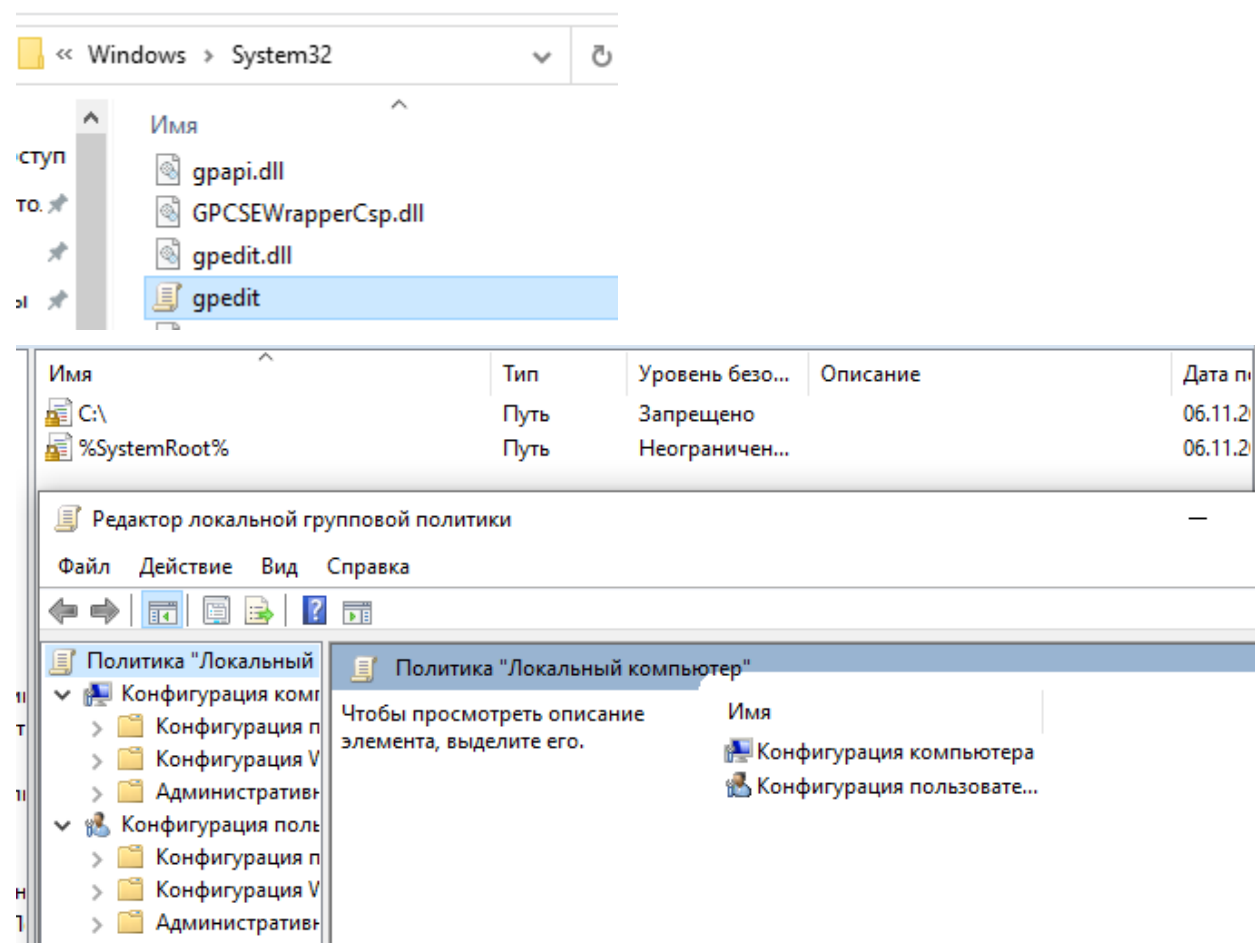
Устанавливаем Запрещено по умолчанию. Это необходимо для того, чтобы запретить выполнение всех программ кроме тех, которые находятся в директориях. Которые мы указали ранее.



Соглашаемся



Теперь проверяем:



То что не работало можно посмотреть в пункте [4. Выполните задание в соответствии с номером варианта.](#)

Дополнительная часть

Задание 2

Сравните файловые системы FAT и NTFS

Выполнение

Таблица размещения файлов FAT — это файловая система, в основе которой лежит электронная таблица данных. Существуют две наиболее популярные разновидности данной системы: FAT16 и FAT32. По сути, это одностолбчатые таблицы размещения информации с одной лишь разницей: использование 16-ти или 32-х разрядных адресаций кластеров.

NTFS – файловая система, в основе которой лежит использование сводной таблицы с информацией о файлах в начале раздела диска, а уже потом размещаются сами файлы. Данная файловая система использует специализированные структуры данных, что позволяет обеспечить высокую надежность и эффективность использования места на жестком диске.

	FAT	NTFS
Совместимость	Windows, Mac, Linux, игровые консоли	Windows, Linux, Xbox One и только чтение в Mac
Плюсы	1. кроссплатформенность 2. легкость 3. значительная скорость доступа к файлам средних и малых размеров 4. низкая требовательность к оперативному запоминающему устройству 5. меньший износ жесткого диска	1. журналируемая 2. большие лимиты на размер раздела и файла 3. шифрование 4. автоматическое восстановление 5. рациональное использование места на носителе 6. высокая производительность при работе с большими файлами 7. значительная надежность 8. поддержка сжатия 9. восстановление системы при сбоях.

Минусы	1. максимальный размер файла 4 ГБ и раздела 16 ГБ 2. не журналируемая 3. уязвимость и возможности сбоя системы 4. медленные запросы при работе с большими каталогами файлов 5. отсутствие поддержки малых кластеров 6. необходимость фрагментации пространства на диске	1. ограниченная кроссплатформенность 2. высокая требовательность к объему оперативной памяти 3. отсутствие доступа NTFS-томов в MS-DOS 4. снижение производительности при работе с малыми объемами томов
Использование	Внешние носители	Для установки Windows

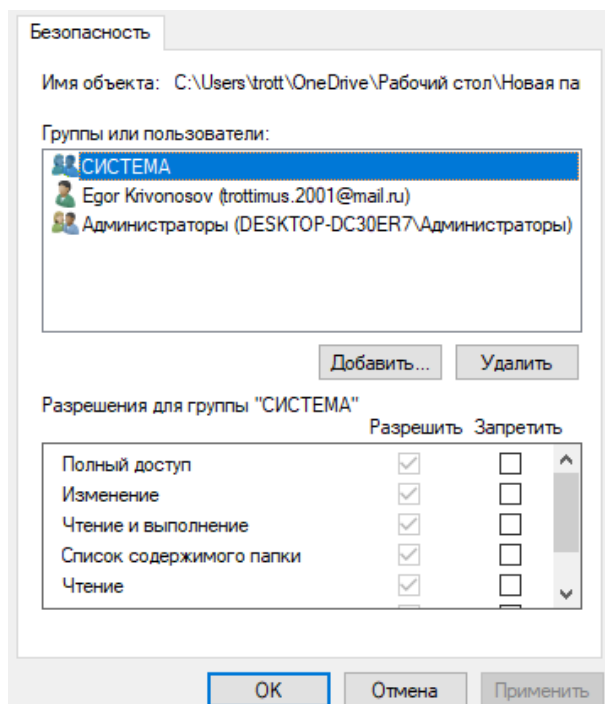
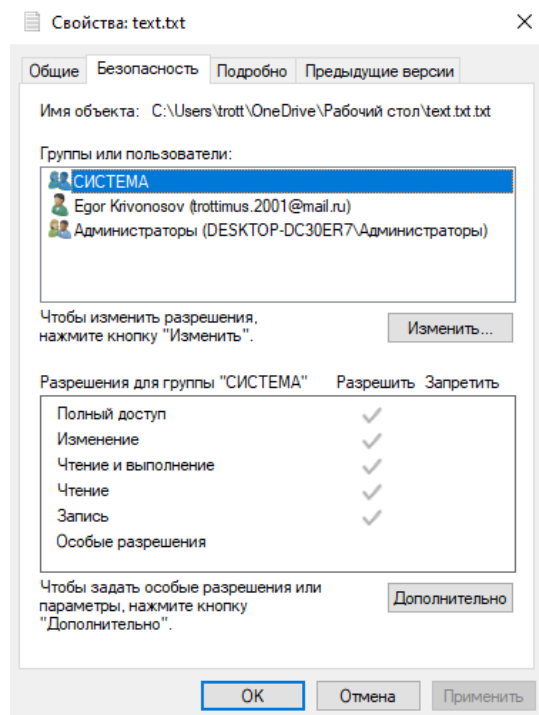
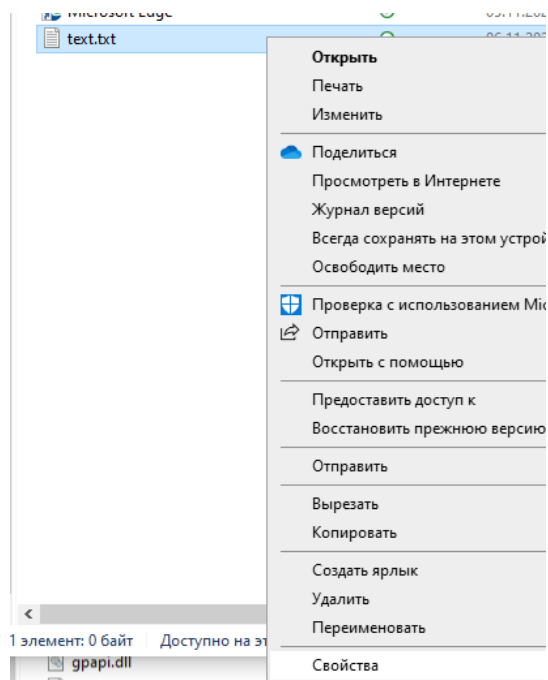
Задание 3

Опишите все возможные способы задания разрешений (прав доступа) к файлам и папкам

Выполнение

Способ 1 - через проводник

1. В **Проводнике** выбрать файл или папку для просмотра параметров безопасности и щелкнуть правой кнопкой мыши.
2. В контекстном меню выбрать команду **Свойства** и перейти на вкладку **Безопасность** диалогового окна.
3. В списке **Имя** выбрать пользователя, контакт, компьютер или группу разрешения которых нужно изменить



Способ 2 - через команду icacls

Используя команду: **icacls "<путь до папки/файла>" /grant <кому>:**

Основные права:

- F (full access)
- M (modify access)
- RX (read and execute access)
- R (read-only access)
- W (write-only access)

```
C:\Users\trott\Downloads>icacls test
test NT AUTHORITY\СИСТЕМА:(OI)(CI)(F)
      BUILTIN\Администраторы:(OI)(CI)(F)
      DESKTOP-DC30ER7\trott:(OI)(CI)(F)

Успешно обработано 1 файлов; не удалось обработать 0 файлов

C:\Users\trott\Downloads>icacls test /grant trott:(RX)
обработанный файл: test
Успешно обработано 1 файлов; не удалось обработать 0 файлов

C:\Users\trott\Downloads>icacls test
test DESKTOP-DC30ER7\trott:(RX)
      NT AUTHORITY\СИСТЕМА:(OI)(CI)(F)
      BUILTIN\Администраторы:(OI)(CI)(F)
      DESKTOP-DC30ER7\trott:(OI)(CI)(F)
```

Способ 3 - при помощи команд в PowerShell

- Посмотреть существующие правила ACL
- Создать новое правило (FileSystemAccessRule, конструктор: Identity String, FileSystemRights, AccessControlType)
- Добавить новое правило в список существующих правил
- Применить новое правило к существующим файлу или папке используя команду Set-ACL

```
PS C:\Users\trott\Downloads> $ACL = Get-ACL -Path "test.txt"
PS C:\Users\trott\Downloads> $AccessRule = New-Object System.Security.AccessControl.FileSystemAccessRule("Admin_2", "Read", "Allow")
PS C:\Users\trott\Downloads> $ACL.SetAccessRule($AccessRule)
PS C:\Users\trott\Downloads> $ACL | Set-Acl -Path "test.txt"
PS C:\Users\trott\Downloads> (Get-ACL -Path "test.txt").Access | Format-Table IdentityReference,FileSystemRights,AccessControlType,IsInherited,InheritanceFlags -AutoSize

IdentityReference      FileSystemRights AccessControlType IsInherited InheritanceFlags
-----
DESKTOP-DC30ER7\Admin_2 Read, Synchronize Allow      False      None
NT AUTHORITY\СИСТЕМА   FullControl      Allow      True       None
BUILTIN\Администраторы FullControl      Allow      True       None
DESKTOP-DC30ER7\trott FullControl      Allow      True       None

PS C:\Users\trott\Downloads>
```

Вывод

В результате выполнения данной лабораторной работы я познакомился с файловыми системами FAT32 и NTFS. Кроме того, я узнал об работе программы с разрешениями и научился задавать права доступа на различные файлы.