Национальный исследовательский университет ИТМО

Факультет Программной Инженерии и Компьютерной Техники

Вариант №4

Лабораторная работа №1.2

«Разграничение доступа к объектам файловой системы»

По дисциплине:

«Информационная безопасность»

Работу выполнила:

Студентка группы P34102

Никонова Наталья Игоревна

Преподаватель:

Рыбаков Степан Дмитриевич

Санкт-Петербург

2023

Выполнение

1. Определение набора разрешений
    a. Загрузка операционной системы

Название объекта доступа	Права администратора	Права пользователя
smss.exe	rx	
csrss.exe	rx	
lsass.exe	rx	
winlogon.exe	rx	
services.exe	rx	
C:/Windows/System32	rx	rx

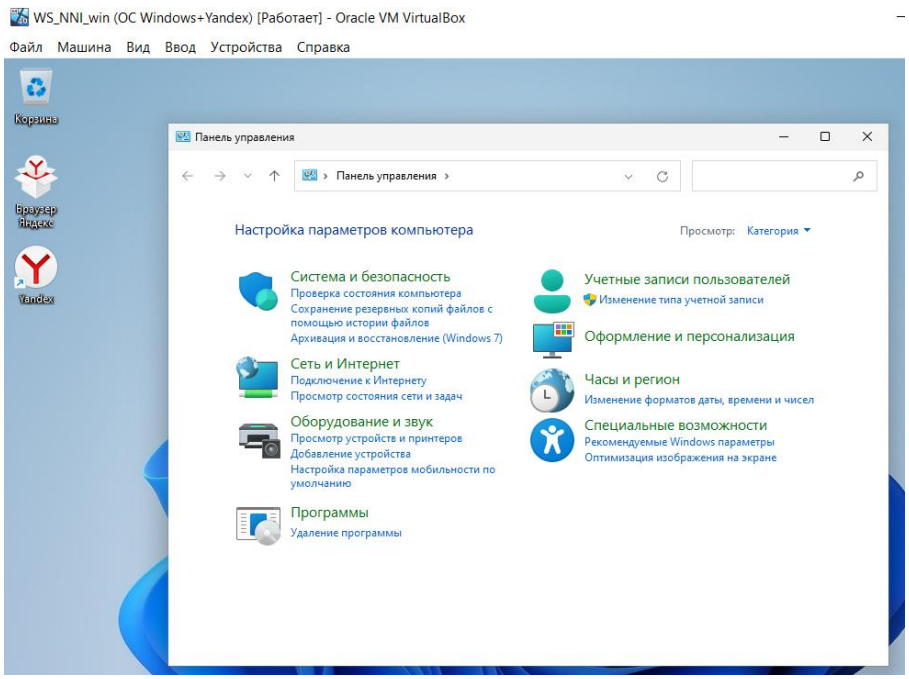
    b. Вход в систему

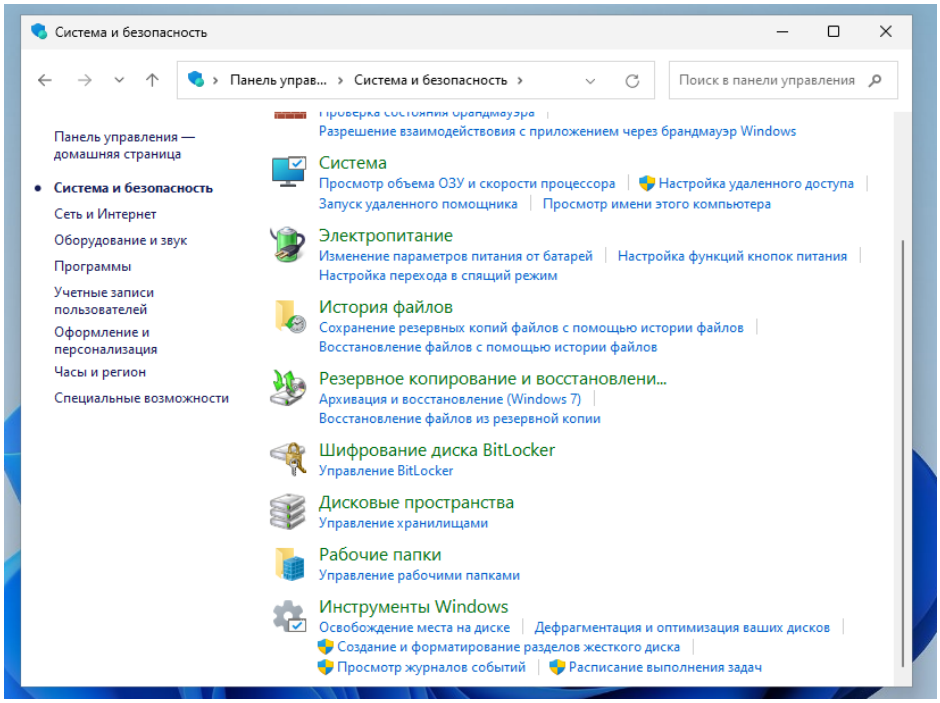
Название объекта доступа	Права администратора	Права пользователя
%UserProfile%	rwx	rwx
Secur32.dll	rx	rx

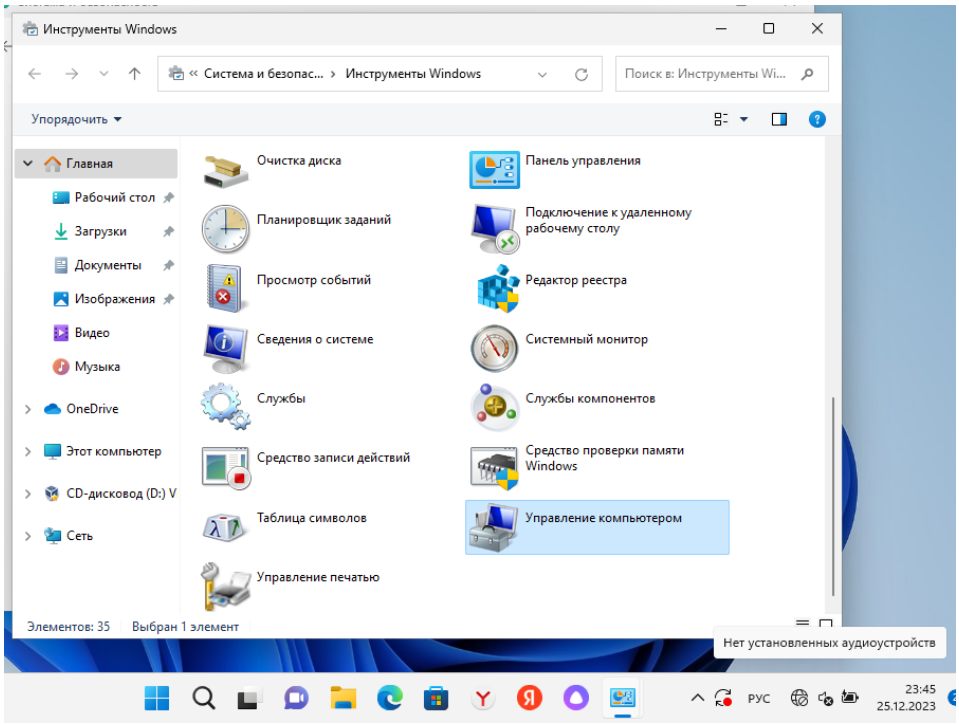
    c. Работа с установленными администратором приложениями

Название объекта доступа	Права администратора	Права пользователя
%AppData%	rx	rx
%LocalAppData%	rx	rx
*.exe	rx	rx
*dll	rx	rx

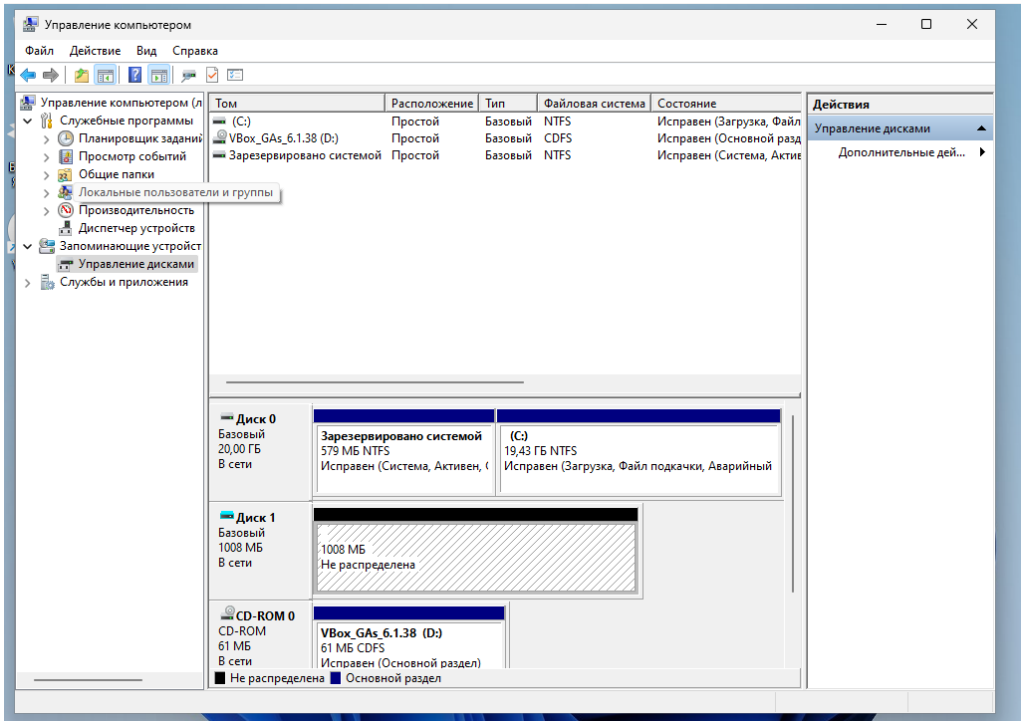
2. Преобразование файловой системы FAT в NTFS.
    a. Первый способ

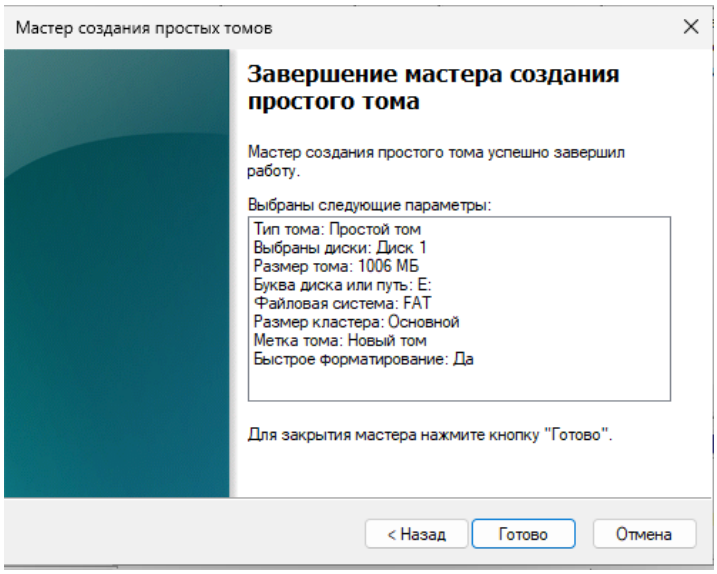




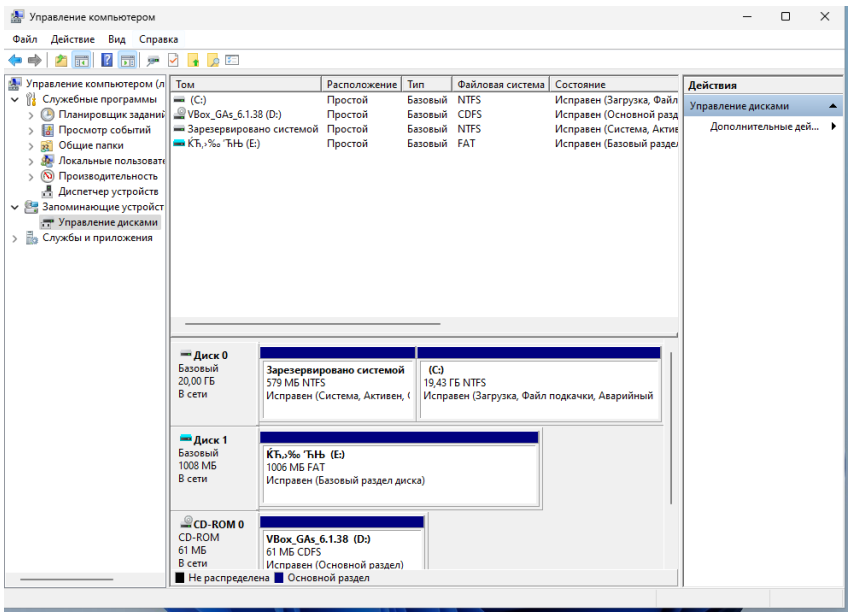


Для форматирования я создала виртуальный диск и выделила на нем том E с нужной файловой системой FAT

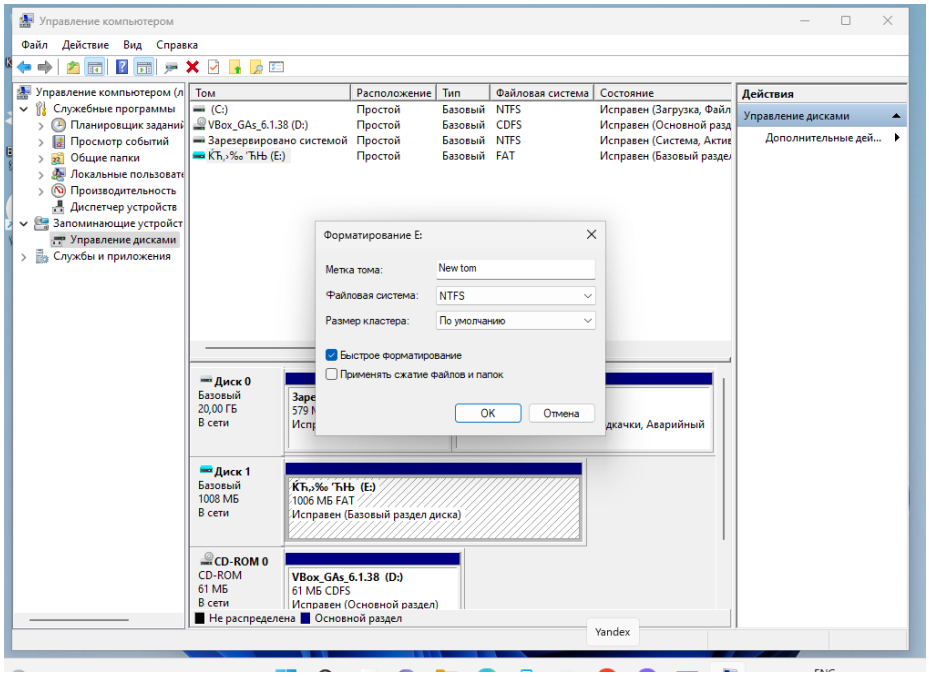


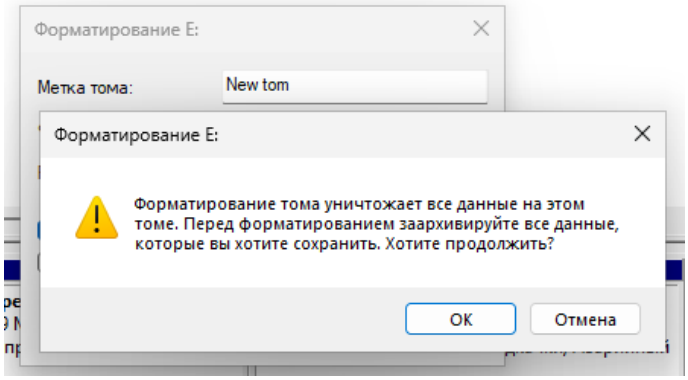


Только кодировка полетела

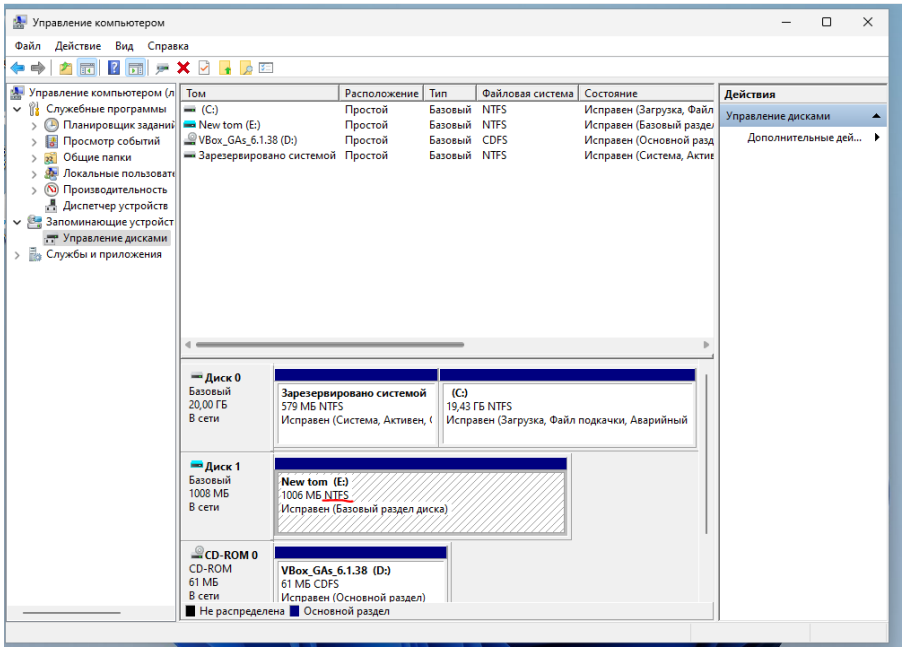


А теперь форматируем с потерей данных (и попробуем поменять метку)





Ура, есть система NTFS



b. Второй способ

```
C:\Windows\System32>chkdsk E: /f
Тип файловой системы: FAT.
Том NEW TOM создан 26.12.2023 1:15
Серийный номер тома: D8DF-A2C6
Проверка файлов и папок...
Проверка файлов и папок завершена.

Windows проверила файловую систему и не обнаружила проблем.
Дальнейшие действия не требуются.

1 054 588 928 байт всего на диске.
       16 384 байт в 1 скрытых файлах.
       32 768 байт в 2 файлах.
1 054 539 776 байт доступно на диске.

       16 384 байт в каждой единице распределения.
Всего единиц распределения на диске:        64 367.
Доступно единиц распределения на диске:        64 364.

C:\Windows\System32>LABEL E:
Том в устройстве E: имеет метку NEW TOM
Серийный номер тома: D8DF-A2C6
Метка тома (11 символов, ENTER - метка не нужна): _
```

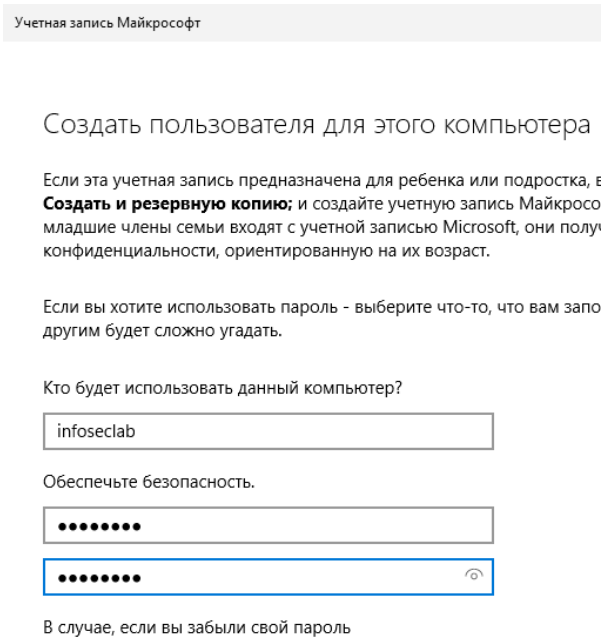
Само преобразование

```
C:\Windows\System32>convert E: /fs:ntfs
Тип файловой системы: FAT.
Введите метку тома для диска E: NEW TOM
Том NEW TOM создан 26.12.2023 17:17
Серийный номер тома: D8DF-A2C6
Проверка файлов и папок...
Проверка файлов и папок завершена.

Windows проверила файловую систему и не обнаружила проблем.
Дальнейшие действия не требуются.

1 054 588 928 байт всего на диске.
       49 152 байт в 3 скрытых файлах.
       32 768 байт в 2 файлах.
1 054 507 008 байт доступно на диске.

       16 384 байт в каждой единице распределения.
Всего единиц распределения на диске:        64 367.
Доступно единиц распределения на диске:        64 362.

Оценка места на диске, необходимого для преобразования файловой системы...
Всего на диске:                 1030144 КБ
Свободно:                       1029792 КБ
Необходимо для преобразования:     6684 КБ
Преобразование файловой системы
Преобразование завершено

C:\Windows\System32>chkdsk E: /f
Тип файловой системы: NTFS.
Метка тома: NEW TOM.

Этап 1. Проверка базовой структуры файловой системы...
  Обработано записей файлов: 41.
Проверка файлов завершена.
 Длительность фазы (Проверка записи файла): 6.23 мс.
  Обработано больших файловых записей: 0.
 Длительность фазы (Восстановление потерянной файловой записи): 0.97 мс.
  Обработано поврежденных файловых записей: 0.
 Длительность фазы (Проверка поврежденной файловой записи): 0.87 мс.

Этап 2. Проверка связей имен файлов...
  Обработано записей индекса: 65.
Проверка индексов завершена.
 Длительность фазы (Проверка индексов): 7.48 мс.
  Проверено неиндексированных файлов: 0.
 Длительность фазы (Переподключение потерянного элемента): 1.03 мс.
  Восстановлено неиндексированных файлов в утерянное и найденное: 0.
 Длительность фазы (Восстановление потерянного элемента в раздел "Потерянные и найденные"): 1.83 мс.
  Обработано записей повторного анализа: 0.
  Обработано записей повторного анализа: 0.
 Длительность фазы (Проверка точки повторного анализа и ИД объекта): 2.21 мс.

Этап 3. Проверка дескрипторов безопасности...
Проверка дескрипторов безопасности завершена.
```

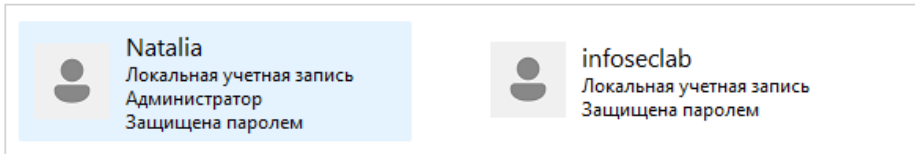
```
 Длительность фазы (Проверка дескриптора безопасности): 4.59 мс.
  Обработано файлов данных: 12.
 Длительность фазы (Проверка атрибута данных): 0.94 мс.

Windows проверила файловую систему и не обнаружила проблем.
Дальнейшие действия не требуются.

   1030143 КБ всего на диске.
      7532 КБ в 8 файлах.
        80 КБ в 14 индексах.
         0 КБ в поврежденных секторах.
      5367 КБ используется системой.
      4880 КБ занято под файл журнала.
   1017164 КБ свободно на диске.

      4096 байт в каждой единице распределения.
Всего единиц распределения на диске:     257535.
Доступно единиц распределения на диске:     254291.
Общая длительность: 27.94 мс (27 мс).
```

3. Так как четный вариант: владелец папки пользователь, у него разрешение на чтение, у Администратора – полный доступ, у группы «все» - не установлены разрешения.

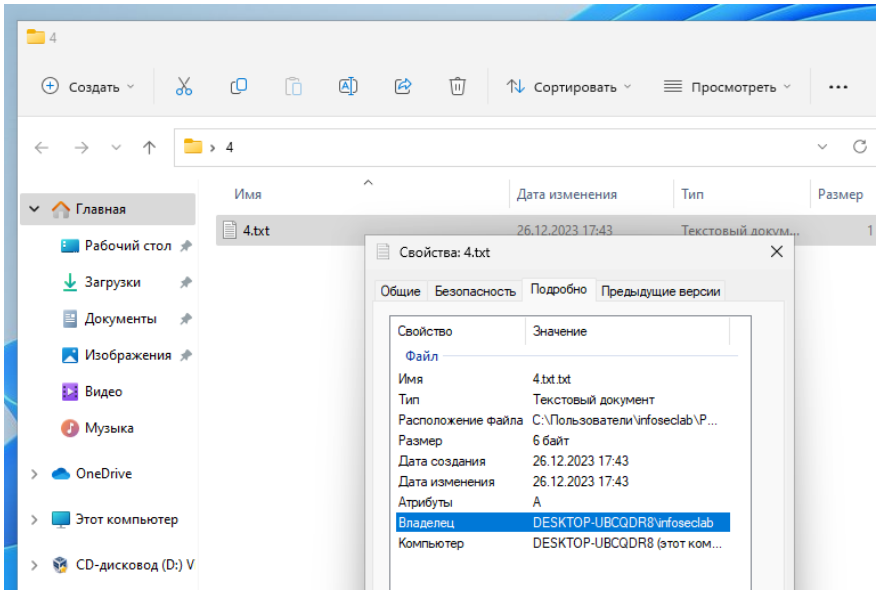
Так как мой основной пользователь – Администратор, создам ещё одного



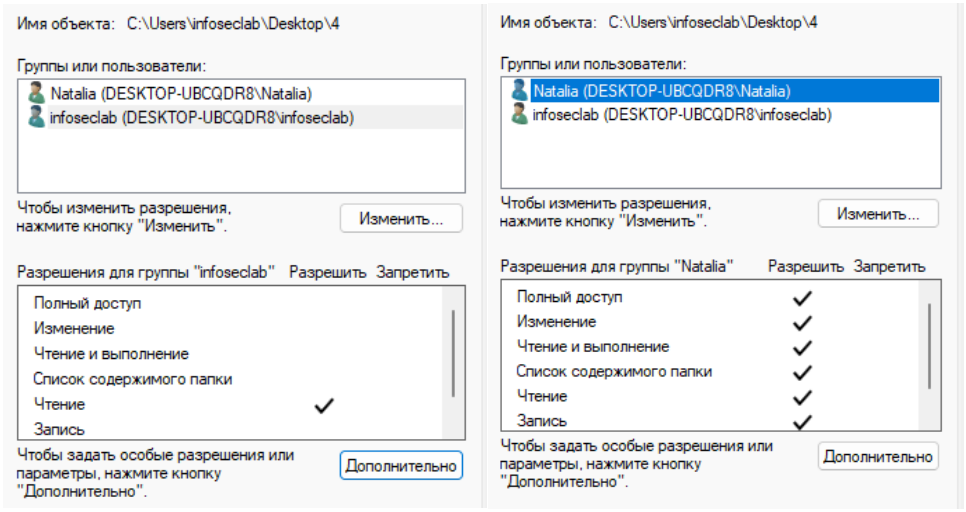
Теперь нас два

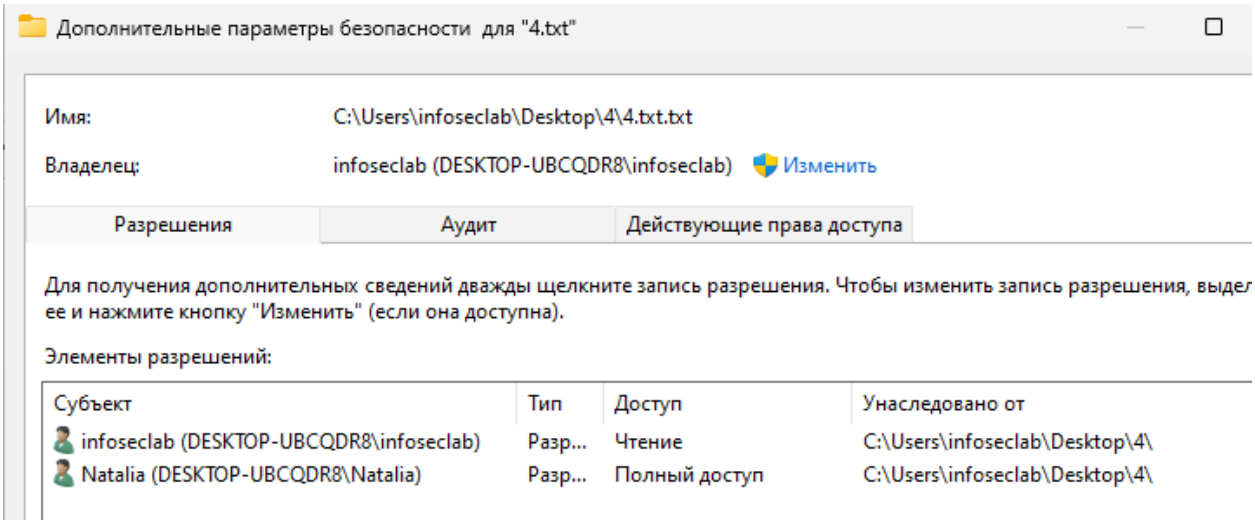


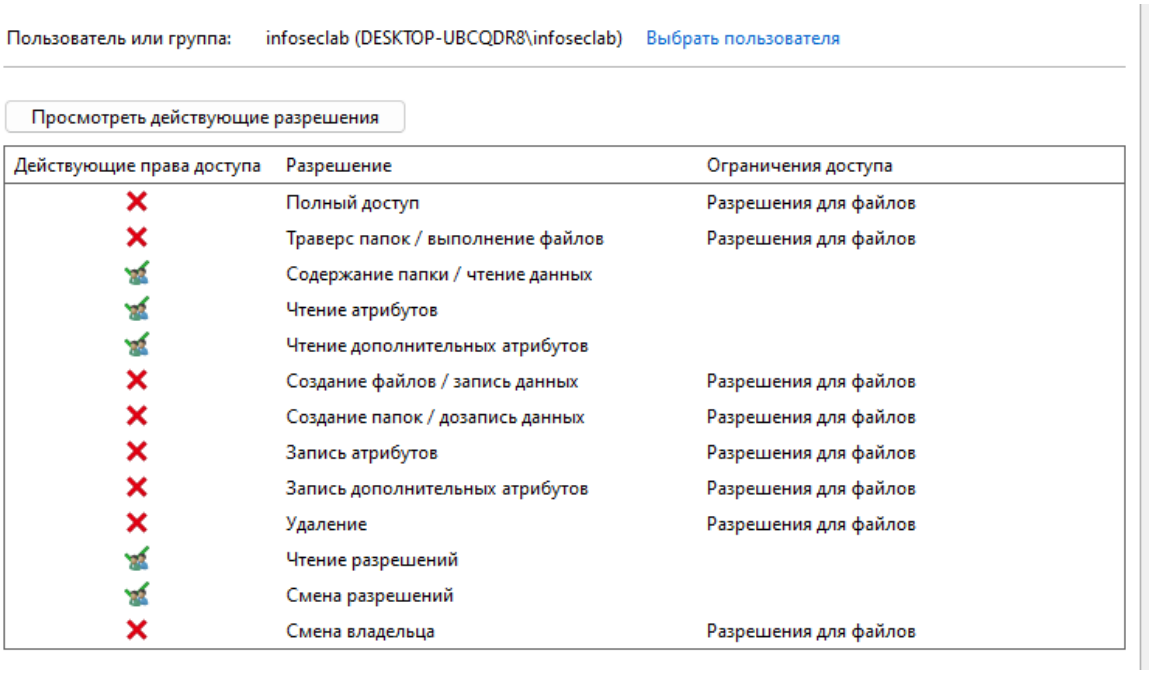
Создала в новой учетке папку и файл

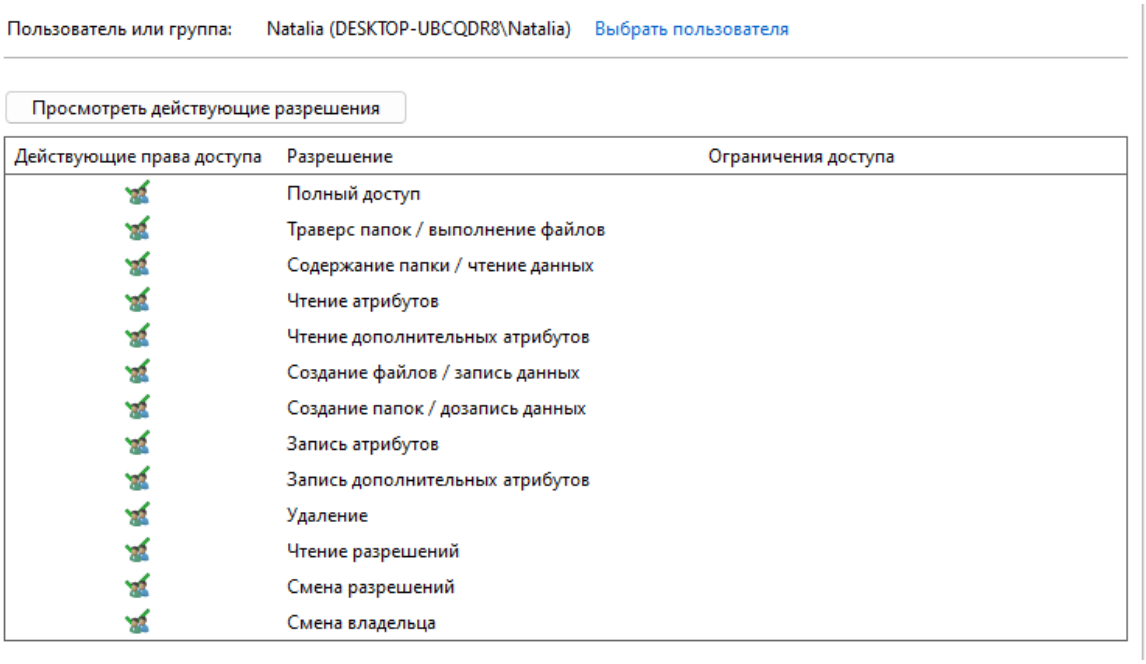


С записи администратора задала нужные права на папку (при этом пришлось удалить наследование прав для infoseclab, иначе при выборе чтения появлялось разрешение и на изменение)


Имя объекта: C:\Users\infoseclab\Desktop\4
Группы или пользователи:
Natalia (DESKTOP-UBCQDR8\Natalia)
infoseclab (DESKTOP-UBCQDR8\infoseclab)
Чтобы изменить разрешения, нажмите кнопку "Изменить".
Изменить...
Разрешения для группы "infoseclab" Разрешить Запретить
Полный доступ
Изменение
Чтение и выполнение
Список содержимого папки
Чтение
Запись
Чтобы задать особые разрешения или параметры, нажмите кнопку "Дополнительно".
Дополнительно
Имя объекта: C:\Users\infoseclab\Desktop\4
Группы или пользователи:
Natalia (DESKTOP-UBCQDR8\Natalia)
infoseclab (DESKTOP-UBCQDR8\infoseclab)
Чтобы изменить разрешения, нажмите кнопку "Изменить".
Изменить...
Разрешения для группы "Natalia" Разрешить Запретить
Полный доступ
Изменение
Чтение и выполнение
Список содержимого папки
Чтение
Запись
Чтобы задать особые разрешения или параметры, нажмите кнопку "Дополнительно".
Дополнительно


Дополнительные параметры безопасности для "4.txt"
Имя: C:\Users\infoseclab\Desktop\4\4.txt.txt
Владелец: infoseclab (DESKTOP-UBCQDR8\infoseclab) Изменить
Разрешения
Аудит
Действующие права доступа
Для получения дополнительных сведений дважды щелкните запись разрешения. Чтобы изменить запись разрешения, выдел
ее и нажмите кнопку "Изменить" (если она доступна).
Элементы разрешений:
Субъект
Тип
Доступ
Унаследовано от
infoseclab (DESKTOP-UBCQDR8\infoseclab) Разр... Чтение C:\Users\infoseclab\Desktop\4\
Natalia (DESKTOP-UBCQDR8\Natalia) Разр... Полный доступ C:\Users\infoseclab\Desktop\4\

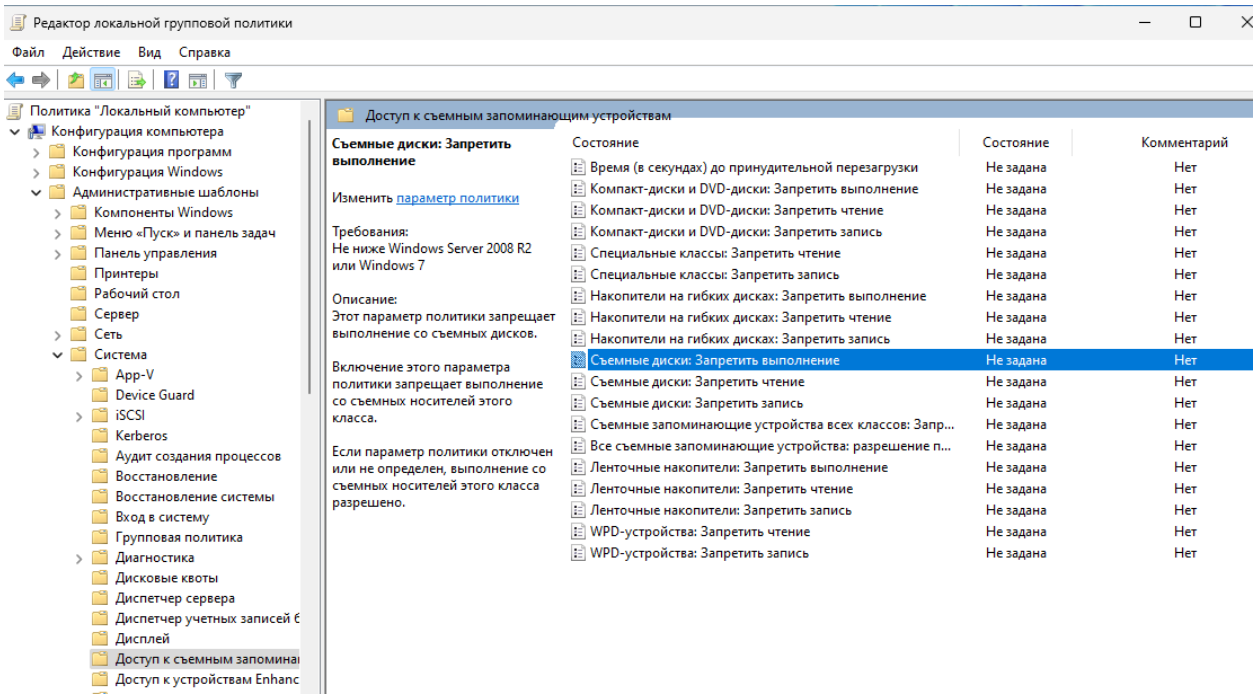

Пользователь или группа: infoseclab (DESKTOP-UBCQDR8\infoseclab) Выбрать пользователя
Просмотреть действующие разрешения
Действующие права доступа
Разрешение
Ограничения доступа
Полный доступ Разрешения для файлов
Траверс папок / выполнение файлов Разрешения для файлов
Содержание папки / чтение данных
Чтение атрибутов
Чтение дополнительных атрибутов
Создание файлов / запись данных Разрешения для файлов
Создание папок / дозапись данных Разрешения для файлов
Запись атрибутов Разрешения для файлов
Запись дополнительных атрибутов Разрешения для файлов
Удаление Разрешения для файлов
Чтение разрешений
Смена разрешений
Смена владельца Разрешения для файлов

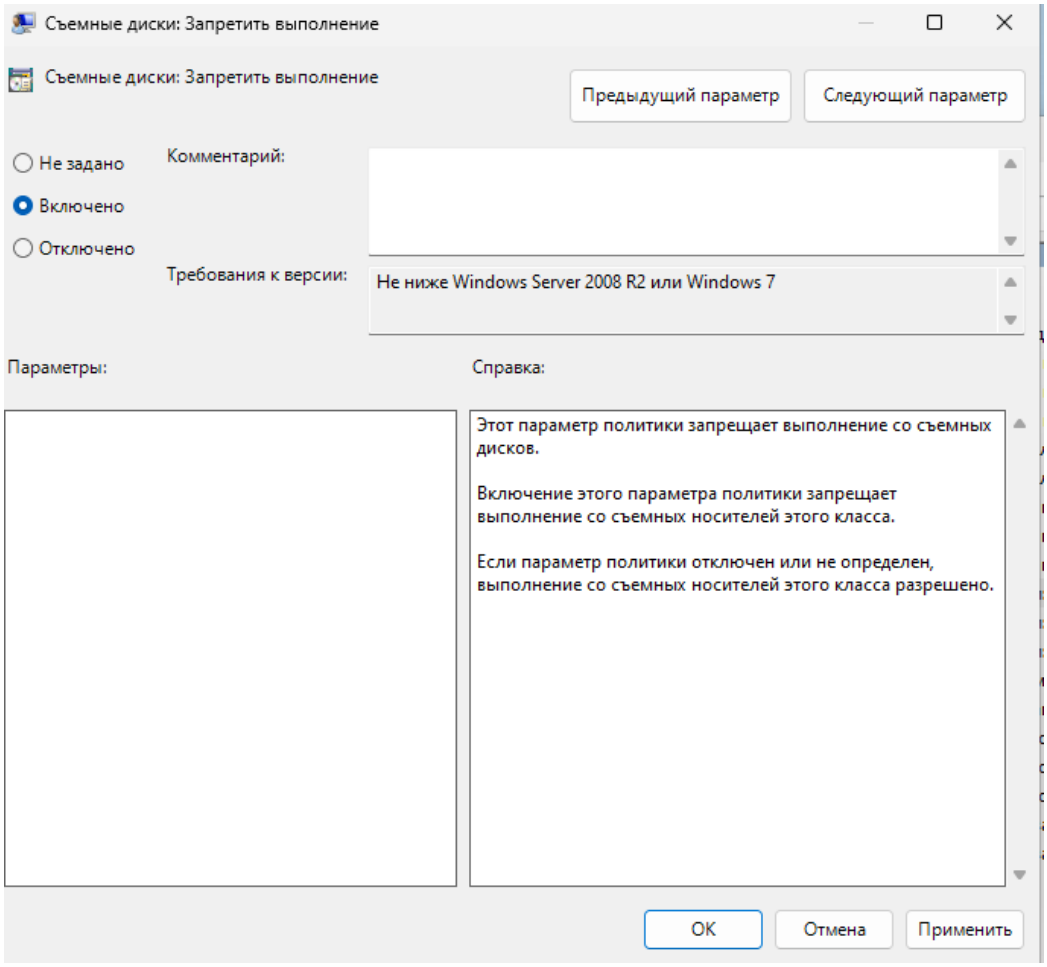


4. Запретить встроенными средствами ОС пользователю запуск программ с внешних flash-накопителей

Запускаем gpedit.msc – редактор групповых политик.

Переходим в конфигурацию компьютера – административные значения – система – доступ к съемным запоминающим устройствам. Запрещаем конкретно выполнение.



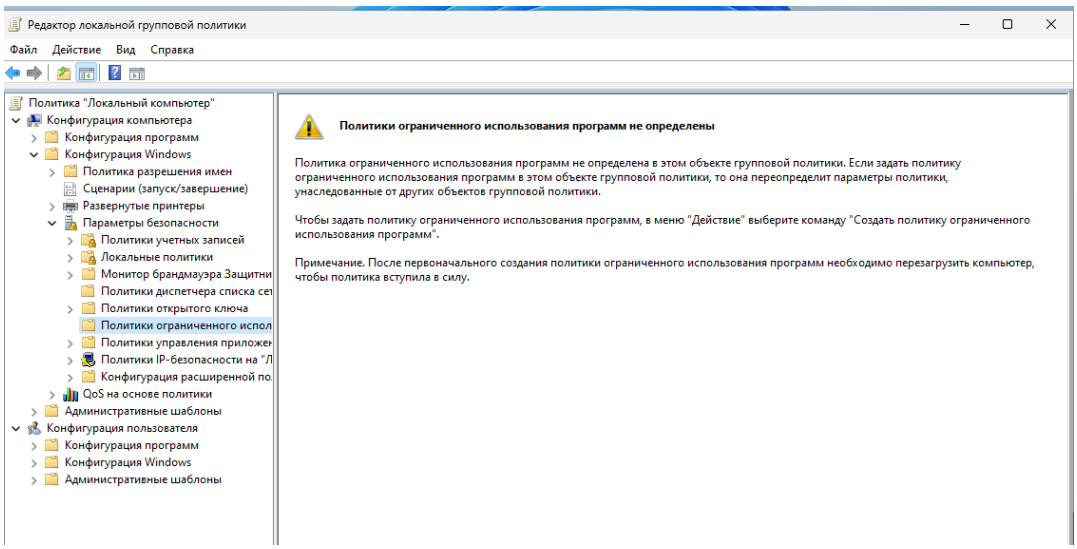


5. Разрешить выполнять системные и прикладные программы только из папок %ProgramFiles% и %SystemRoot%

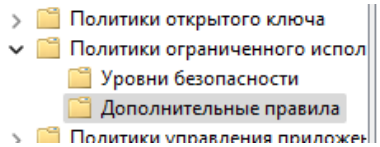
Пользуемся все тем же gpedit.mcs

Переходим в: Конфигурация компьютера -> Конфигурация Windows -> Параметры

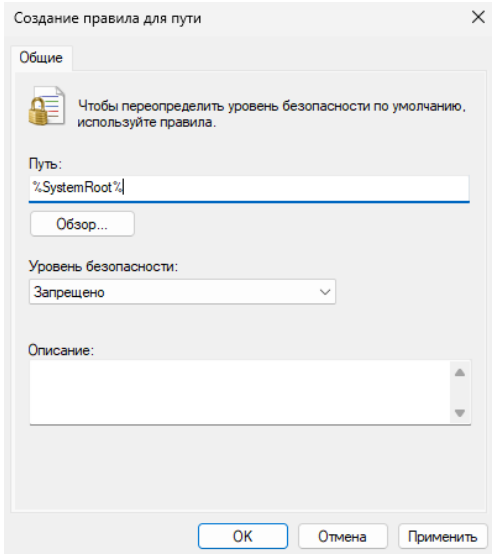
безопасности -> Политики ограниченного использования программ. Пока они не определены

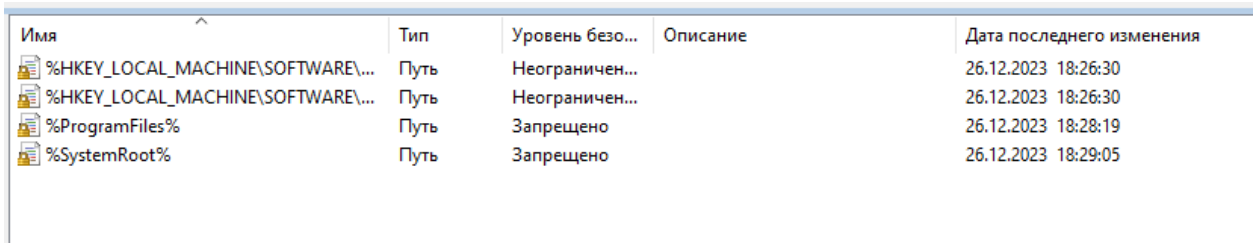


Создаем новую



Создаем новое правило по пути





Дополнительные задания

1. Сравните файловые системы FAT и NTFS

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 однотипные 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	NFTS
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

2. Опишите все возможные способы задания прав
    a. Через проводник и вкладку свойства – использовала в лабе в пункте третьем
    b. С помощью команды icacls "<путь до папки/файла>" /grant <кому>:
    Основные права:
        i. ● F (full access)
        ii. ● M (modify access)

iii. ● RX (read and execute access)
iv. ● R (read-only access)
v. ● W (write-only access)

c. Через редактор политик

Вывод

В ходе выполнения лабораторной работы я познакомилась с некоторыми встроенными средствами операционной системы, которой пользуется большинство рядовых пользователей. Больше всего мне понравилось, что можно запретить выполнение, да и чтение и запись с flash накопителей – стало понятно, почему ничего не удавалось сделать на компьютерах в центре доп. образования.