Университет ИТМО

Факультет программной инженерии и компьютерной техники

Информационная безопасность

Отчет по лабораторной работе № 7

«Разграничение доступа к объектам файловой системы»

Вариант 7

Выполнил студент группы P34302

Ким Даниил Кванхенович

Проверил преподаватель

Рыбаков Степан Дмитриевич

Санкт-Петербург 2024

Содержание отчета:

Постановка задачи и исходные данные:

Цель работы:

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

Порядок выполнения работы:

1. Укажите минимальный набор разрешений (прав доступа), необходимых для:
   a. загрузки операционной системы;
   b. входа Пользователя и Администратора в систему;
   c. работы с приложениями, установленными администратором.

2. Преобразуйте файловую систему *FAT* (*File Allocation Table*) в *NTFS* (*New Technology File System*). Опишите преобразование в отчете с использованием скриншотов (минимум 2 способа)

3. Выполните задание в соответствии с номером варианта. Для выполнения задания нужно создать файл с названием «*№варианта.txt*» и папку «*№варианта*», в которую поместить созданный файл.

   Какие разрешения (права доступа) будут у Пользователя и у Администратора на файл «*№варианта.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»)?

4. Выполните задание в соответствии с номером варианта. Выполните настройки встроенных механизмов защиты ОС *Windows* в соответствии с заданием.

   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.

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

Описание аппаратных средств:

Процессор	AMD Ryzen 7 5700U 1.80 GHz
Разрядность процессора	x64
Видеоадаптер	AMD Radeon(TM) Graphics
Основная память	INTEL SSDPEKNW512G8H
Оперативная память	2 Hynix HMA81GS6CJR8N-XN 8Гб 3200МГц
Сетевой адаптер	Realtek RTL8822CE 802.11ac

Описание программных средств:

Операционная система	Microsoft Windows 11 Home 23H2
Разрядность системы	x64

Выполнение:

Этап 1: Минимальный набор прав

Загрузка операционной системы:

Название объекта доступа	Администратор	Пользователь
Hvix64.exe hvax64.exe	R_X	___
Ntoskrnl.exe	R_X	___
Securekernel.exe	R_X	___
smss.exe	R_X	___
Wininit.exe	R_X	___
csrss.exe	R_X	___
Logonui.exe	R_X	___
lsass.exe	R_X	___
Bootim.exe	R_X	___
winlogon.exe	R_X	R_X
services.exe	R_X	___
C:/Windows/System32	R_X	R_X

Вход в систему:

Название объекта доступа	Администратор	Пользователь
%UserProfile%	RWX	RWX
Secur32.dll	R_X	R_X

Работа с приложениями, установленными администратором:

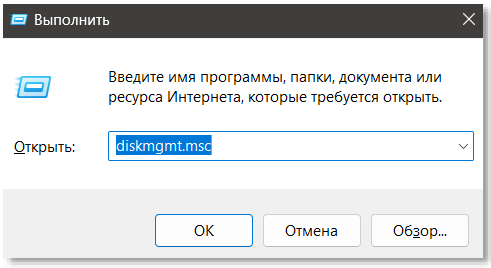
Название объекта доступа	Администратор	Пользователь
%LocalAppData%	R_X	R_X
%AppData%	R_X	R_X
.dll	R_X	R_X
.exe	R_X	R_X

Этап 2: Преобразование файловой системы *FAT* в *NTFS*

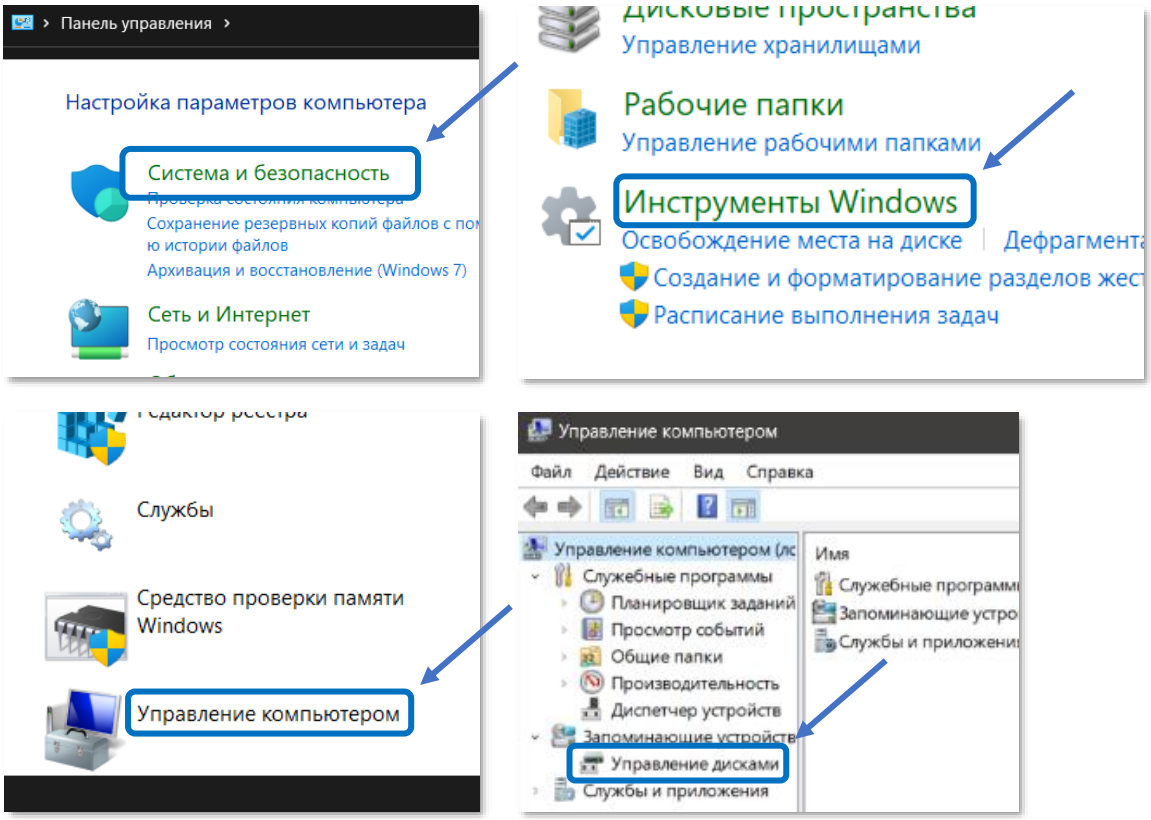
Способ 1: *diskmgmt.msc*

Любым из способов открываем средство - *Управление дисками*:

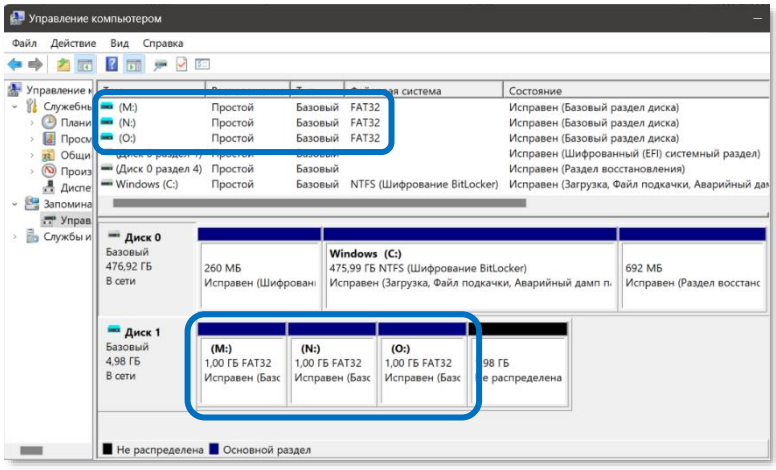
- Ввод *diskmgmt.msc* в поле *Выполнить ;*



- *Панель управления → Система и безопасность → Инструменты Windows → Управление компьютером → Управление дисками*

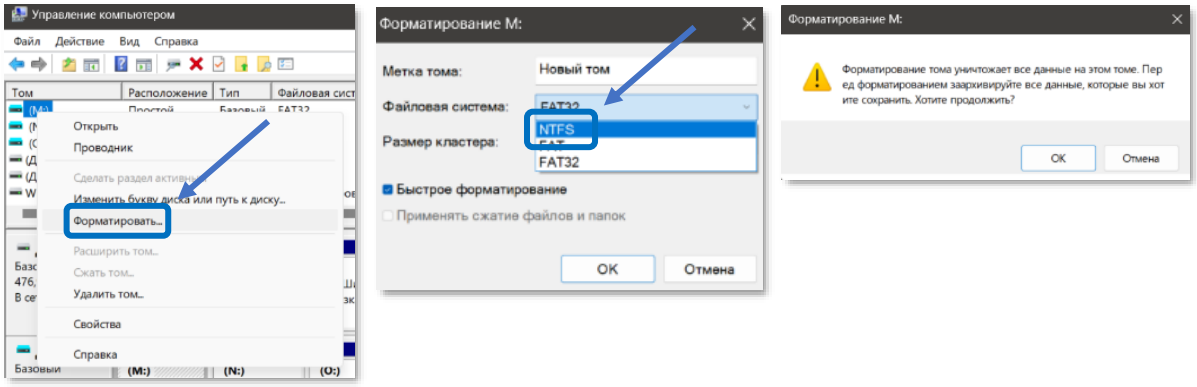


В открывшемся средстве - *Управление дисками* – наблюдаем тома (M:), (N:) и (O:).

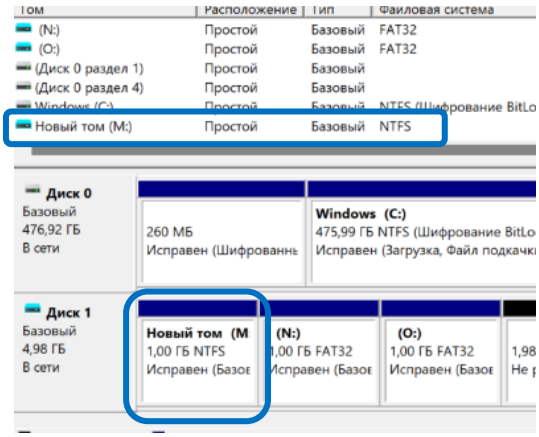


Приступаем к преобразованию файловой системы *FAT* в *NTFS*.

Форматируем один из заранее подготовленных виртуальных дисков (диск M). В качестве новой файловой системы выбираем *NTFS*. Видим предупреждение об уничтожении данных.

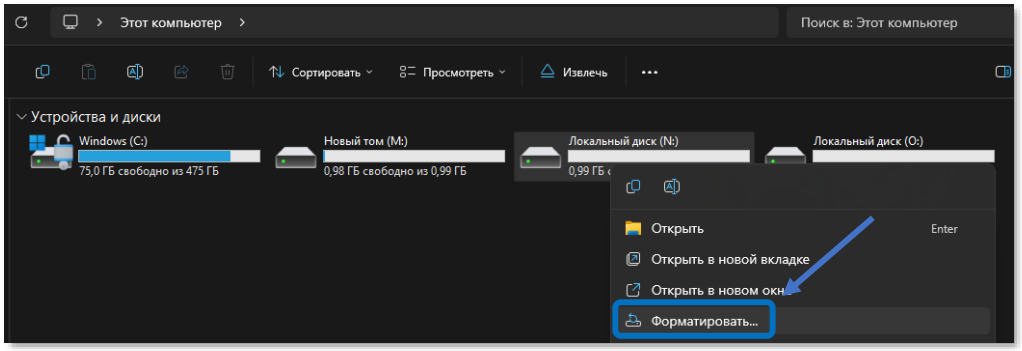


Наблюдаем желаемые изменения:

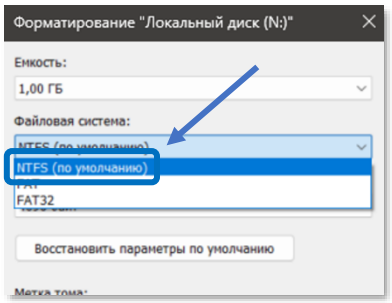


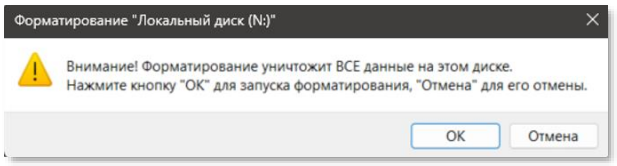
Способ 2: Проводник

В проводнике переходим к списку дисков. Выбираем один из заранее подготовленных виртуальных дисков (диск M) ПКМ и форматируем.

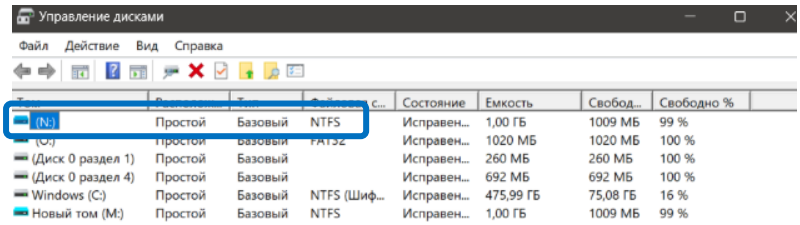


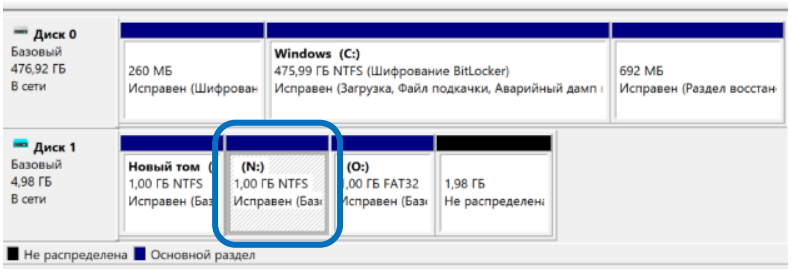
Аналогичным способом выбираем в качестве новой файловой системы NTFS и соглашаемся с угрозой об удалении данных.





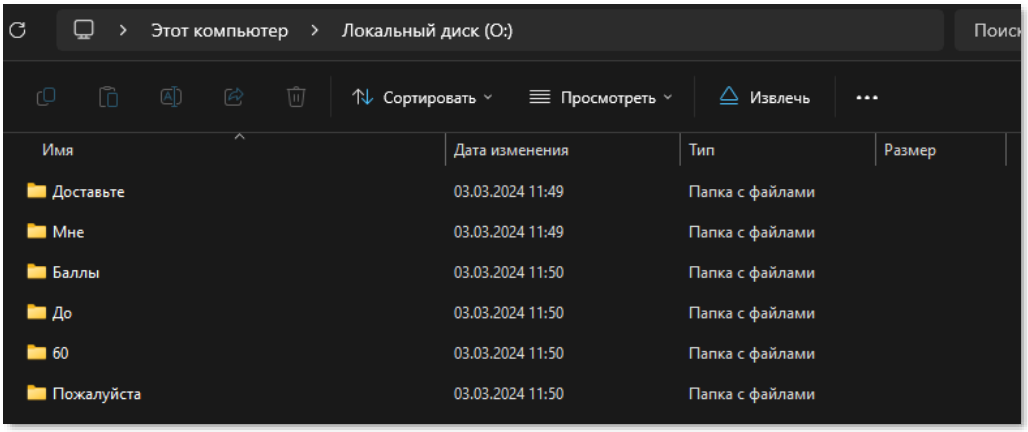
Наблюдаем желаемый результат:





Способ 3: Утилита *convert* (без уничтожения содержимого)

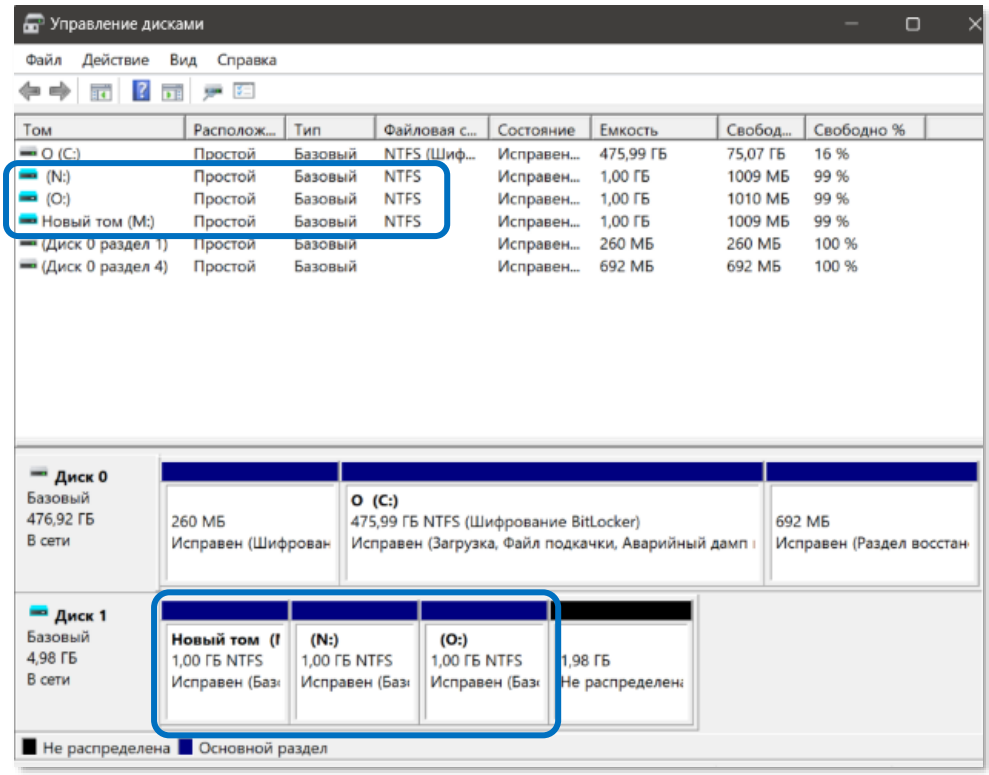
Для демонстрации сохранения данных на диске (O:) создаётся набор файлов.



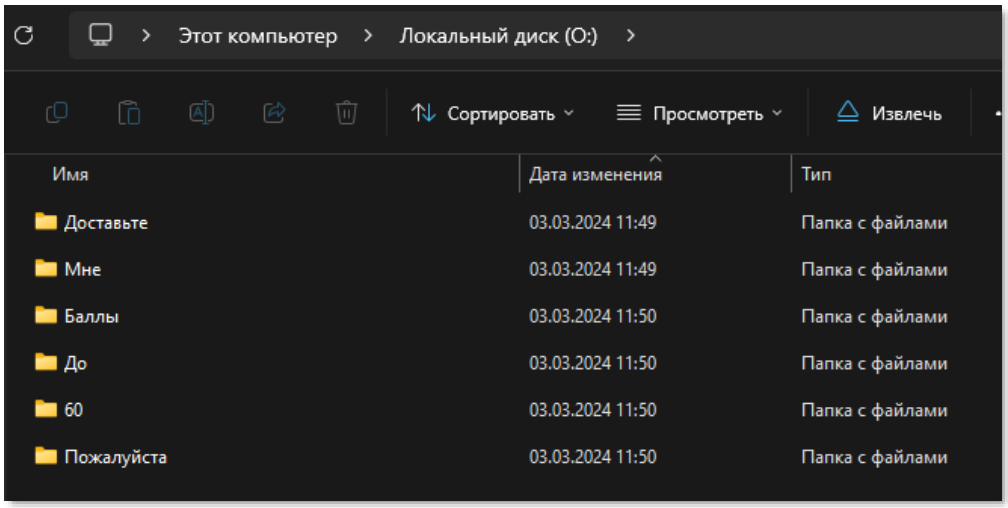
В консоли, запущенной с правами администратора, вызываем утилиту *convert* с параметрами /fs:ntfs.

```
PS C:\WINDOWS\system32> convert O: /fs:ntfs
The type of the file system is FAT32.
Volume Serial Number is 4885-E428
Windows is verifying files and folders...
File and folder verification is complete.

Windows has scanned the file system and found no problems.
No further action is required.

1 069 547 520 bytes total disk space.
       12 288 bytes in 3 hidden files.
       24 576 bytes in 6 folders.
        4 096 bytes in 1 files.
1 069 502 464 bytes available on disk.

        4 096 bytes in each allocation unit.
      261 120 total allocation units on disk.
      261 109 allocation units available on disk.

Determining disk space required for file system conversion...
Total disk space:               1048576 KB
Free space on volume:           1044436 KB
Space required for conversion:     6725 KB
Converting file system
Conversion complete
```

Наблюдаем желаемый результат:



Содержавшиеся на виртуальном диске данные не были уничтожены:

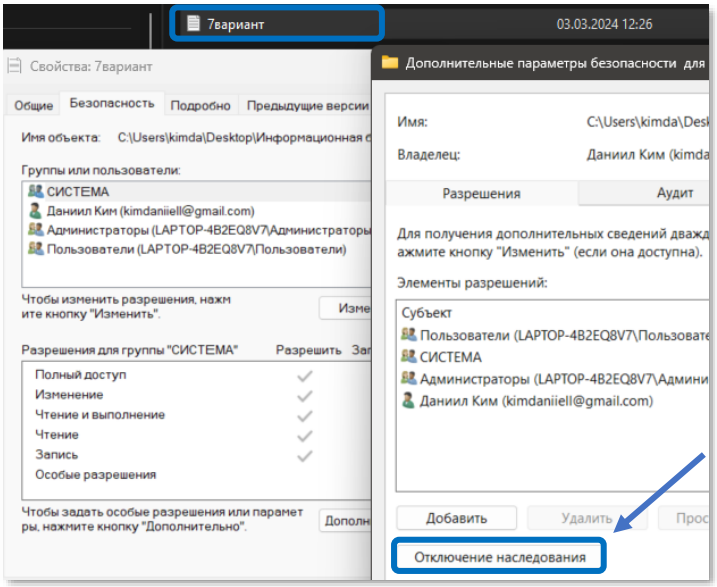


Этап 3: Разрешения

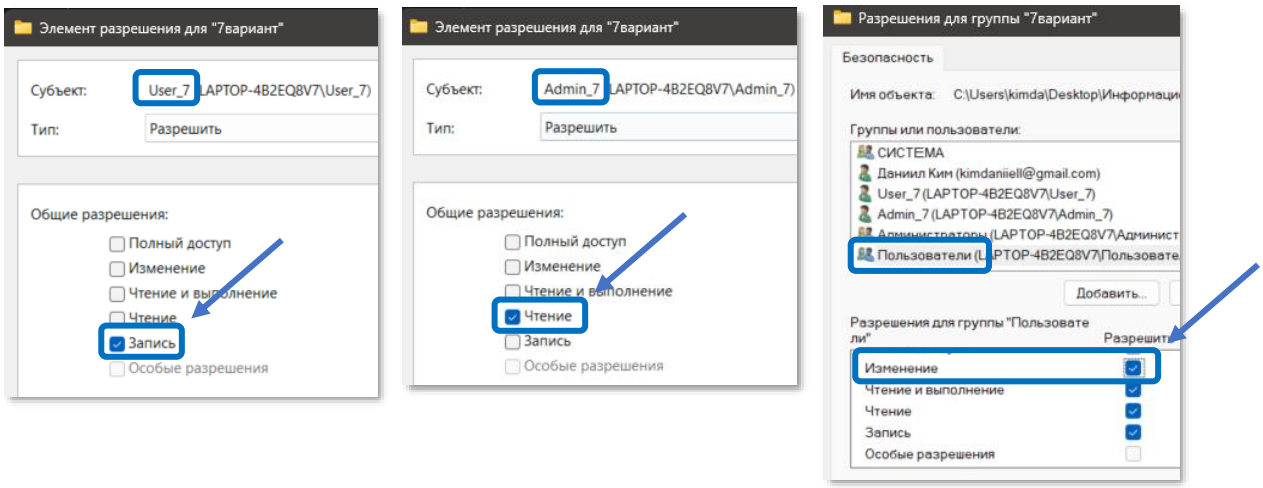
Начальные данные:

Название объекта доступа	Администратор *Admin_7*	Пользователь *User_7*	Группа «Все»
7вариант.txt	R__	_W_	CHANGE

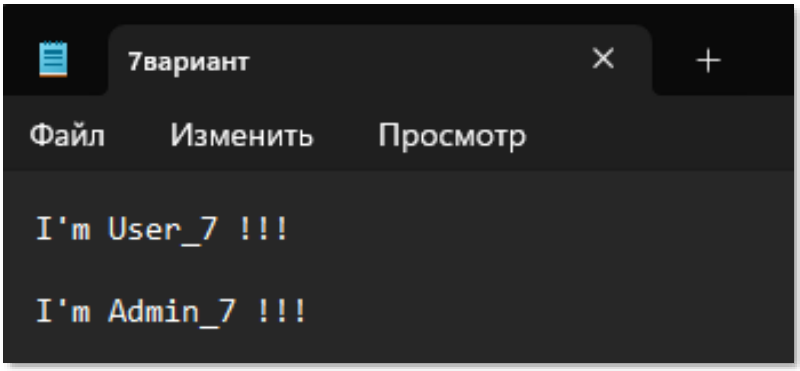
Шаг 1: *Отключение наследования*:



Шаг 2: *Установка прав согласно варианту*:



При взаимодействии с настроенным объектом безопасности (файл *7вариант.txt*) от лица *Admin_7* и *User_7* была возможность читать файл и сохранять в нем изменения.

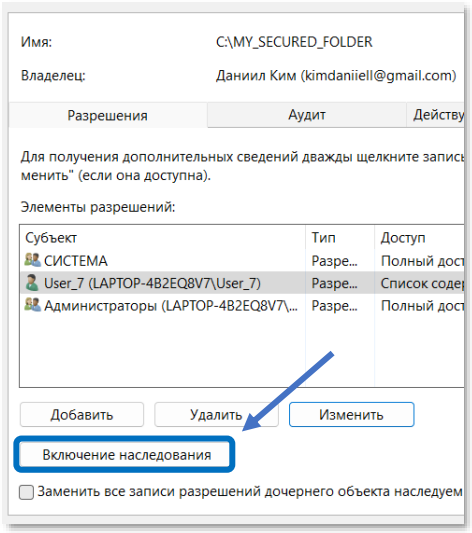


Этап 4: Настройка доступа

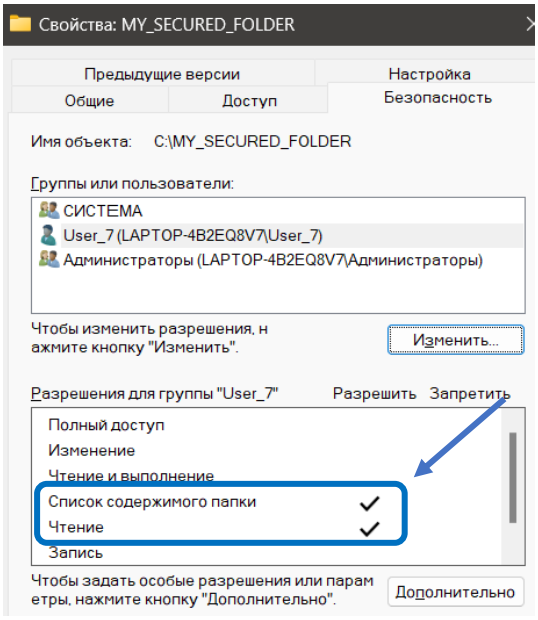
Начальные данные:

	Пользователь *User_7*	Остальные пользователи
Разрешить	Доступ к содержимому	---
Запретить	Переименовывание	Доступ к додержимому

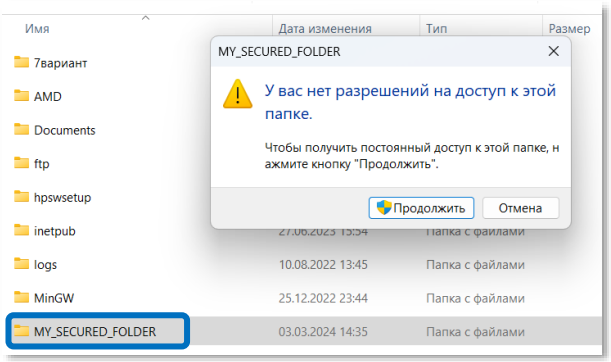
Шаг 1: *Отключение наследования*:



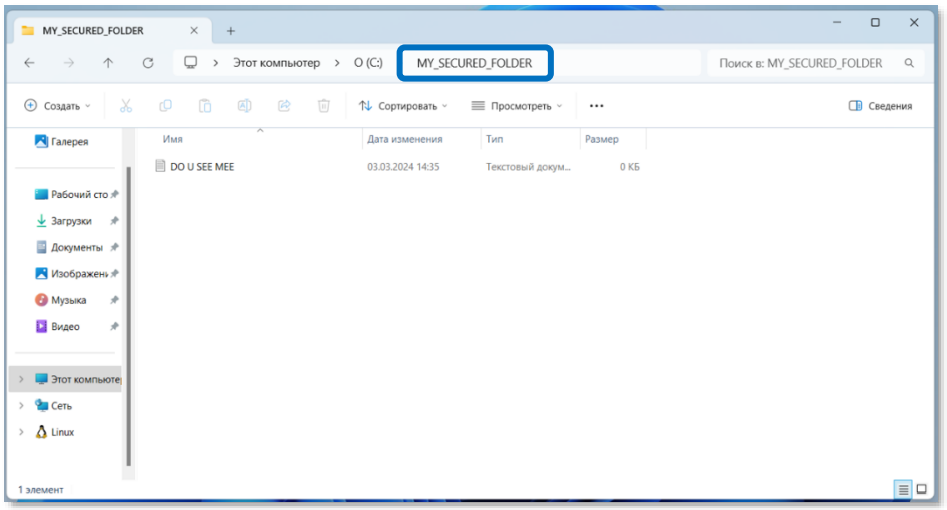
Шаг 2: *Установка прав согласно варианту*:



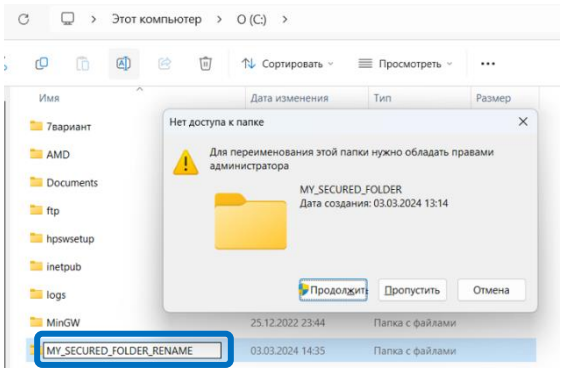
При попытке получить доступ к папке, её содержимому или чтению User_407 видит сообщение об отказе,



в то время как User_7 – нет.



Однако User_7, так же, как и остальные пользователи, не может переименовывать папку.

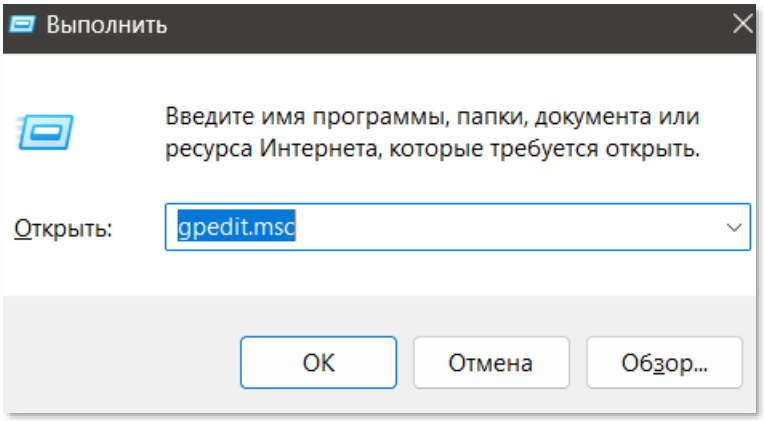


Т.к. User_7 сам принадлежит группе “Пользователи”, не

получится запретить пользователям получать доступ к целевой папке. Запреты имеют больший приоритет, чем разрешения, поэтому, для того чтобы *User_7* имел возможность работать с папкой, запрет не производится.

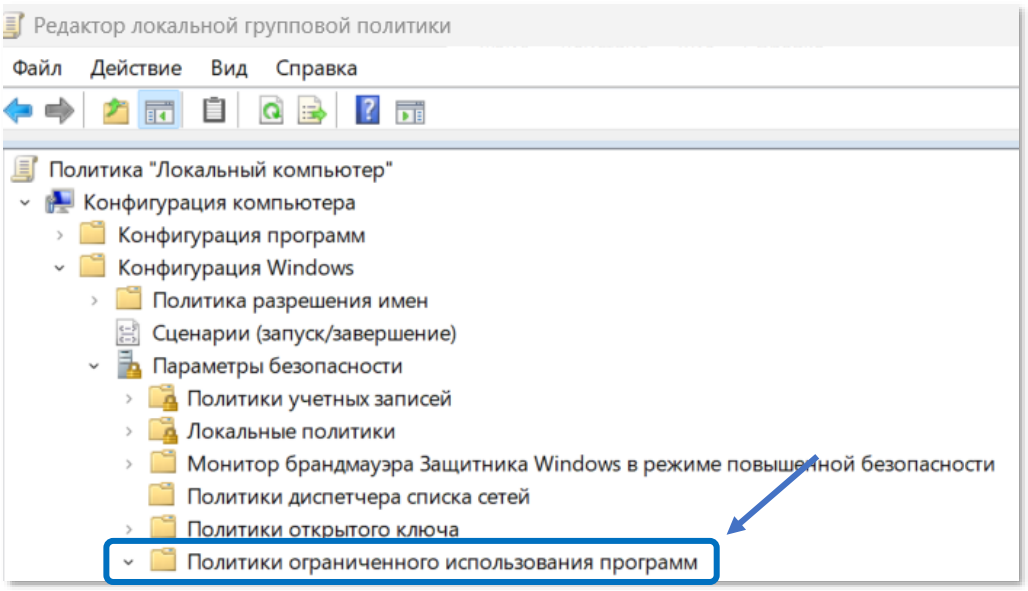
Этап 5: Разрешения для средств ОС

Для задания требуемых ограничений можно воспользоваться настройкой локальных групповых политик. Для этого в поле *Выполнить* необходимо вызвать *gpedit.msc*.

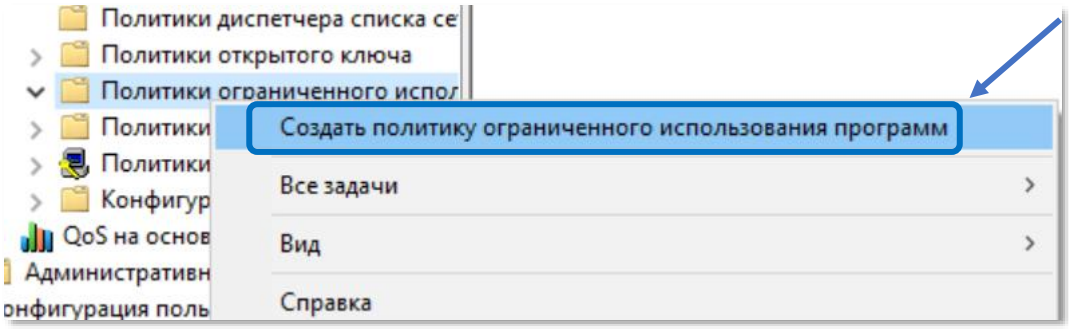


В открывшемся окне редактора локальных групповых политик нужно пройти следующий путь:

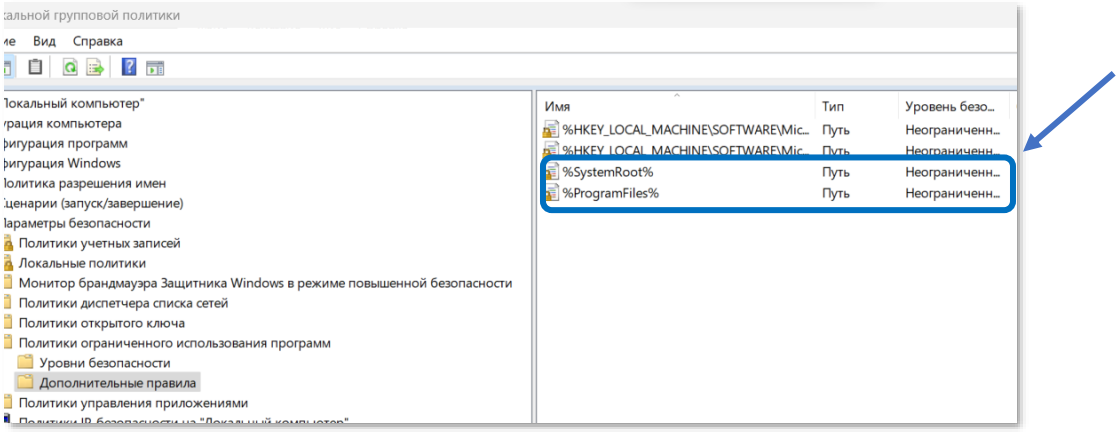
- *Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Политики ограниченного использования программ*



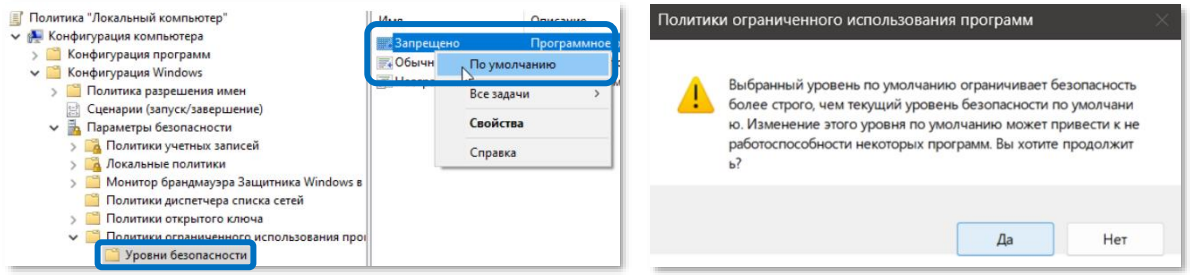
ПКМ выбираем *Политики ограниченного использования программ* и создаем новую политику.



Во вкладке *Дополнительные правила* создадим свои правила с путями %ProgramFiles% и %SystemRoot%.

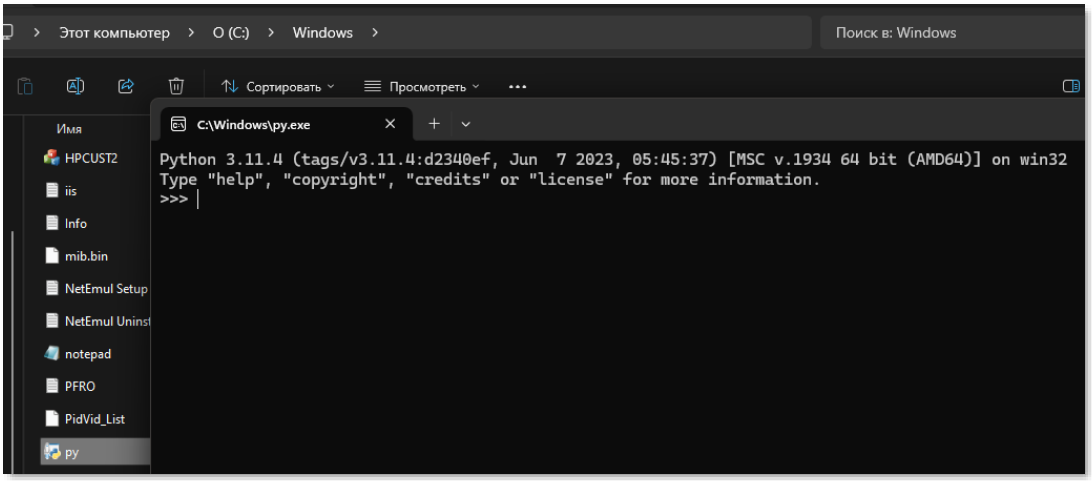


Во вкладке *Уровни безопасности* устанавливаем запрет по-умолчанию на выполнение системных и прикладных программ за исключением тех, что находятся определённых ранее путях: *%ProgramFiles %* и *%SystemRoot%*.



Проверка установленных ограничений на исполнение программ.

- Запуск программ, находящихся по заданным путям:



Вывод:

В данной работе были изучены базовые аспекты разграничения доступа к ресурсам в операционной системе *Windows 11*. В частности, был рассмотрен механизм разрешений в файловой системе NTFS, виды разрешений и способы их задания.

Во время выполнения работы был рассмотрен получен опыт работы с компонентом управления дисков - *diskmgmt.msc*, утилитой *convert*, с различными файловыми системам.

Кроме того, был закреплен материал о способах создания учетных записей и управления ими, о понятиях *ACL*, *DACL*.