

Федеральное государственное автономное образовательное  
учреждение высшего образования

Университет ИТМО

Дисциплина: Информационная безопасность  
**Лабораторная работа Windows 2**

**Разграничение доступа к объектам файловой системы**

Вариант 13(3)

**Работу выполнил студент группы Р34131:**  
Кузнецов Максим Александрович

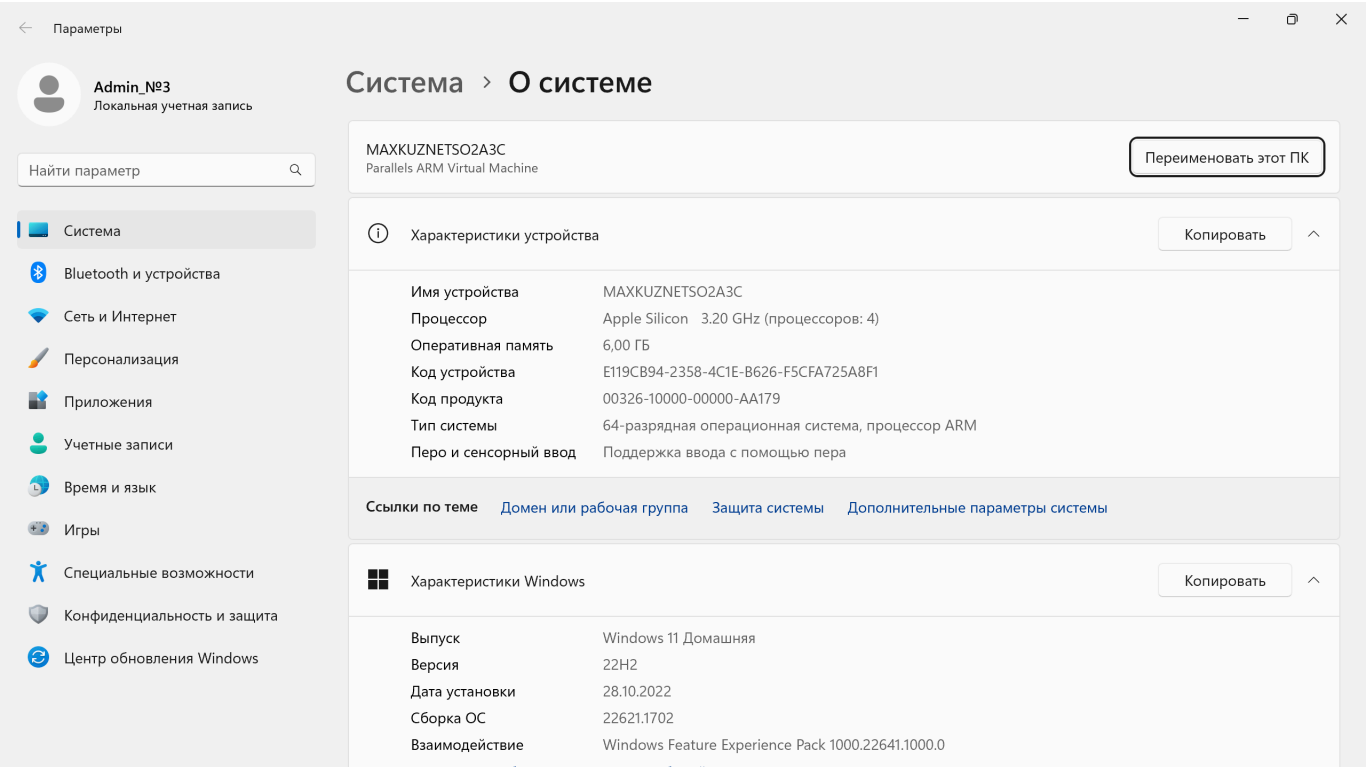
**Преподаватель:**  
Маркина Татьяна Анатольевна

2023 г.  
г. Санкт-Петербург

## 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 для выполнения лабораторной работы:  
Parallels Desktop (MacOS) Windows 11



## Основная часть

1. Укажите минимальный набор разрешений (прав доступа), необходимых для:

Загрузки операционной системы

Название объекта доступа	Администратор	Пользователь
Hvix64.exe (or 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 пользователя (User\_Новарианта) и Администратора (Admin\_Новарианта) в систему

Название объекта доступа	Администратор	Пользователь
%UserProfile%	RWX	RWX
Secur32.dll	R-X	R-X

Работы с приложениями, установленными администратором

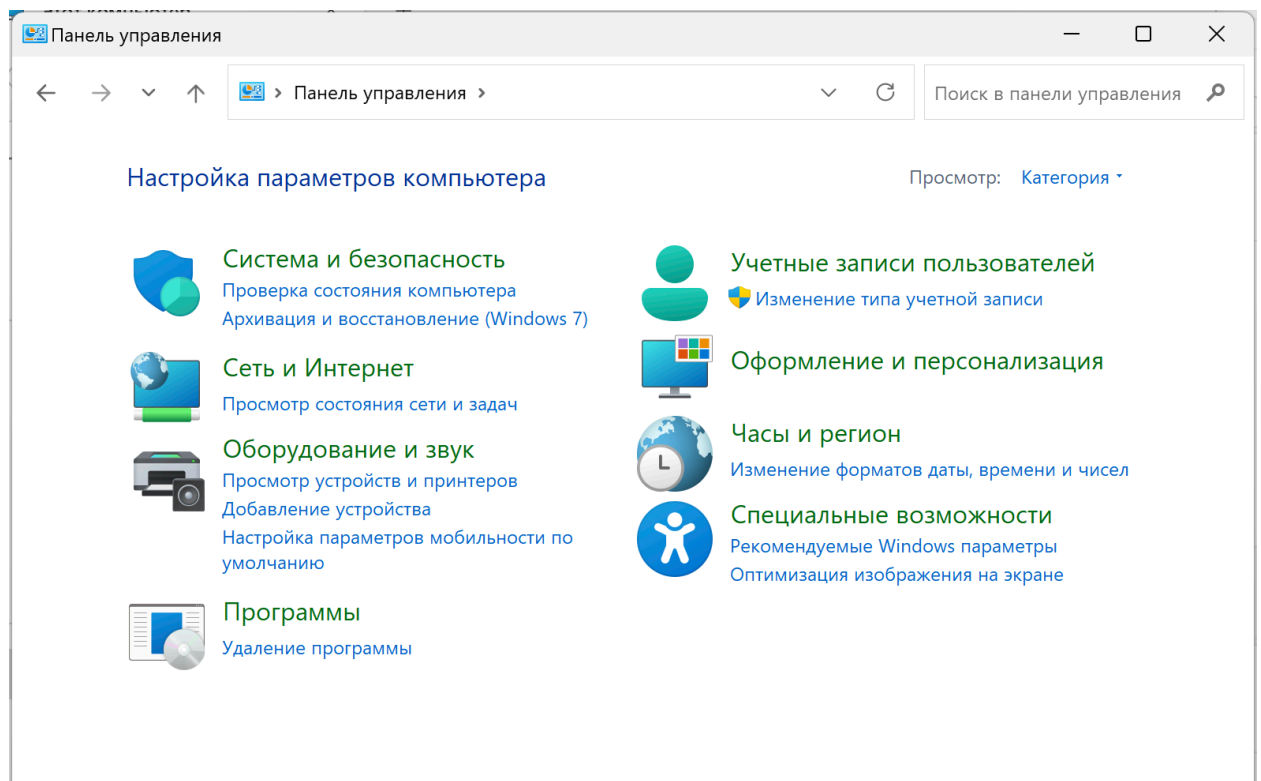
Название объекта доступа	Администратор	Пользователь
%LocalAppData%	R-X	R-X
%AppData	R-X	R-X
.dll	R-X	R-X
.exe	R-X	R-X

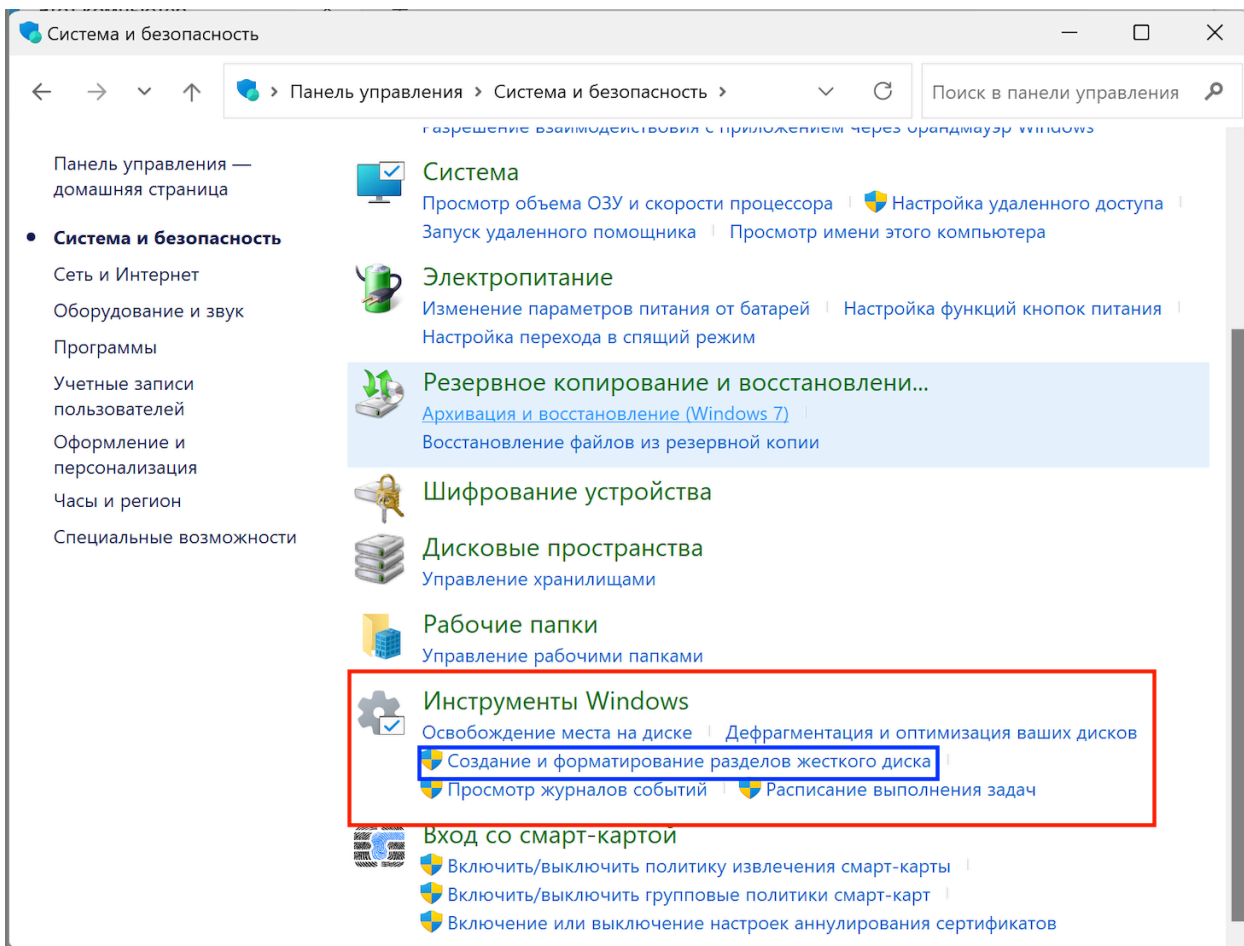
## 2. Преобразуйте файловую систему FAT (File Allocation Table) в NTFS (New Technology File System)

Опять-таки, есть несколько способов достижения желаемого результата.

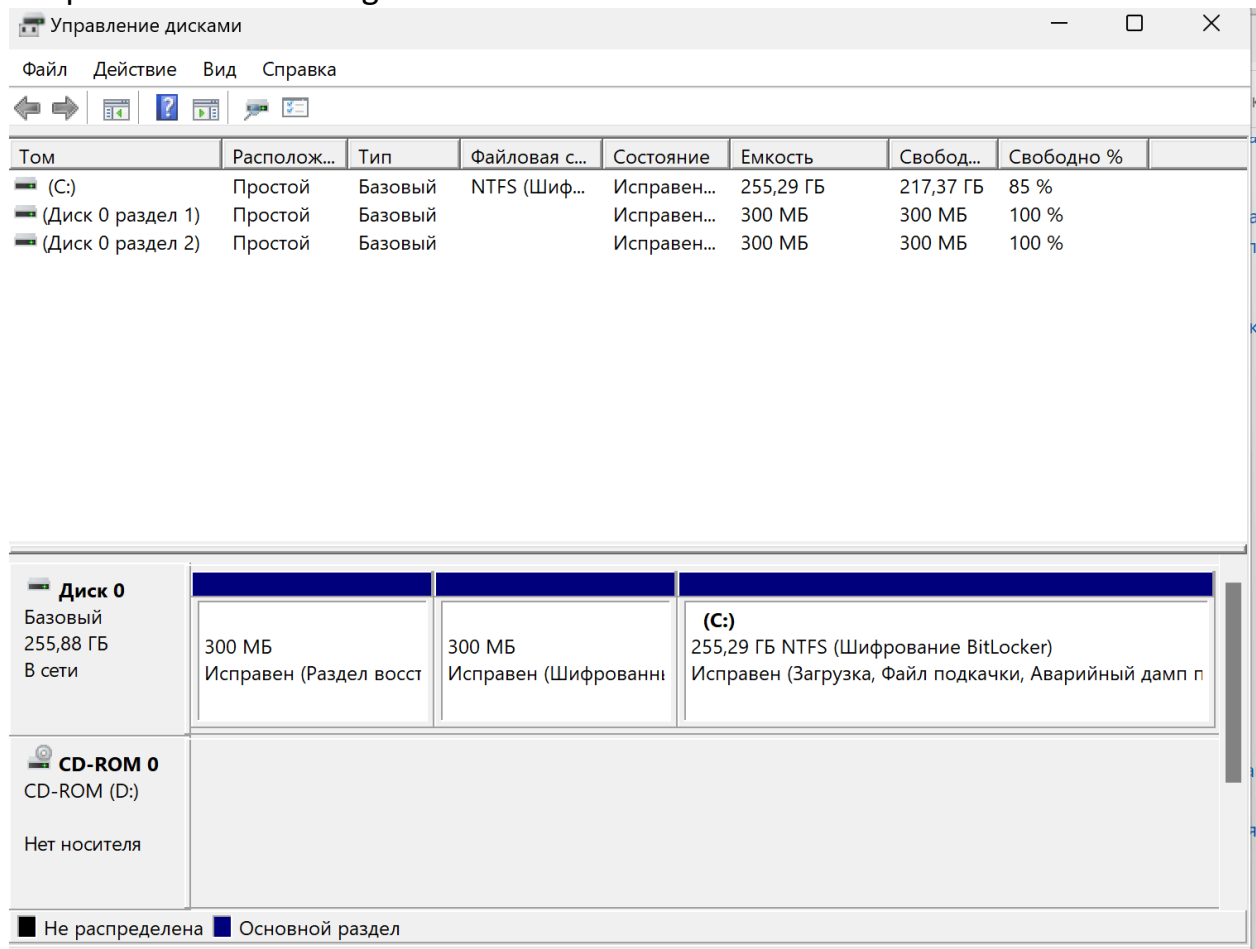
### Способ 1

Заходим в Панель Управления – Система и безопасность – Инструменты Windows – Создание и форматирование разделов жесткого диска.





## Открывает окно diskmgmt



Так как здесь есть уже NTFS, то можно подсоединить диск\устройство с FAT и проделать форматирование.

Нажимаем создать Новый Том и кликаем далее-далее-далее

## Мастер создания простого тома

Этот мастер помогает создать простой том на диске.

Простой том может располагаться только на одном диске.

Для продолжения нажмите кнопку "Далее".

< Назад

Далее >

Отмена

Мастер создания простых томов

**Форматирование раздела**  
Для сохранения данных на этом разделе его необходимо сначала отформатировать.

Укажите, хотите ли вы форматировать этот том и какие параметры форматирования при этом нужно использовать.

☐ Не форматировать данный том

☒ Форматировать этот том следующим образом:

Файловая система: NTFS

Размер кластера: По умолчанию

Метка тома: Новый том

☒ Быстрое форматирование

☐ Применять сжатие файлов и папок

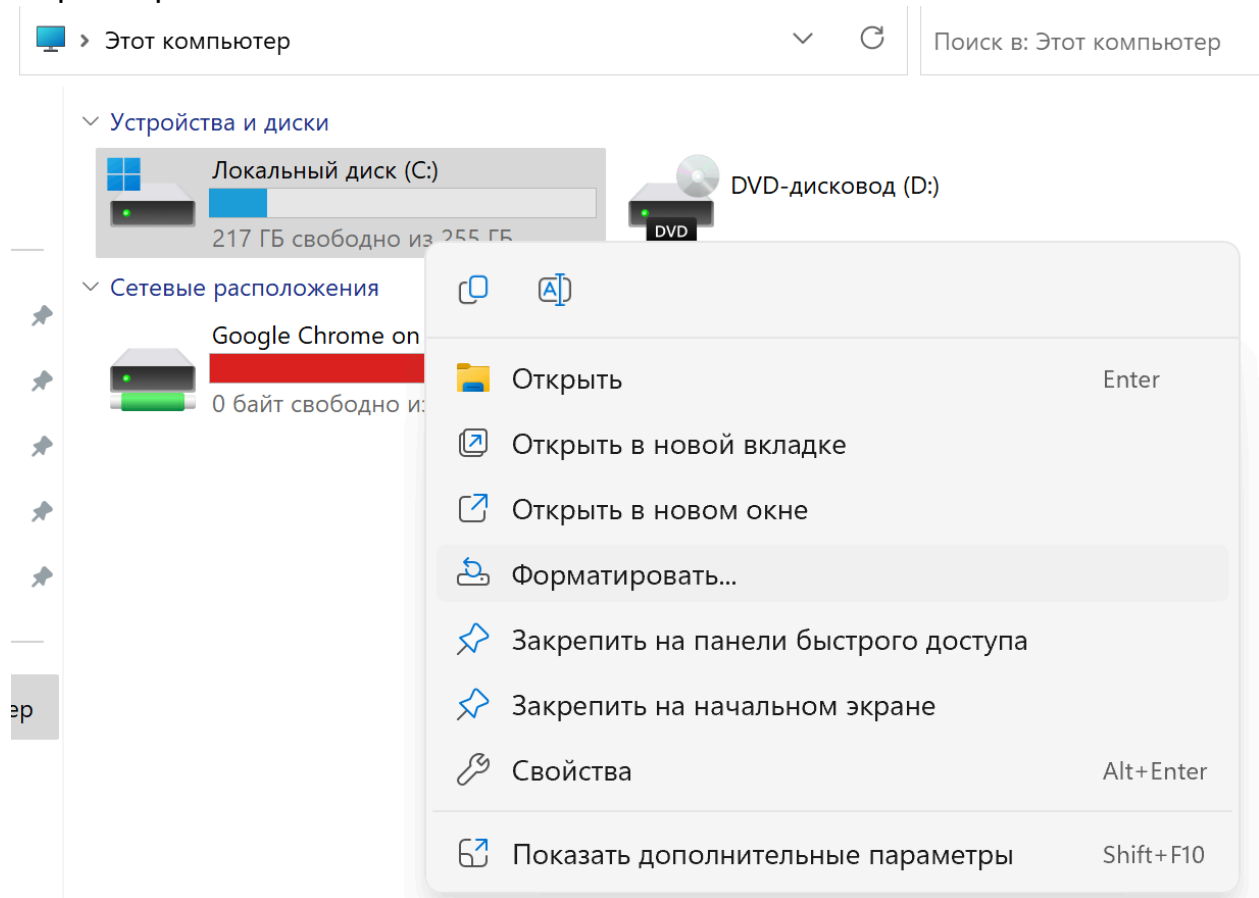
< Назад    Далее >    Отмена

Здесь из предложенных FAT/FAT32/NTFS выбираем последний.



## Способ 2

Из окна проводника на желаемом диске нажать правой кнопкой мыши на **Форматировать**



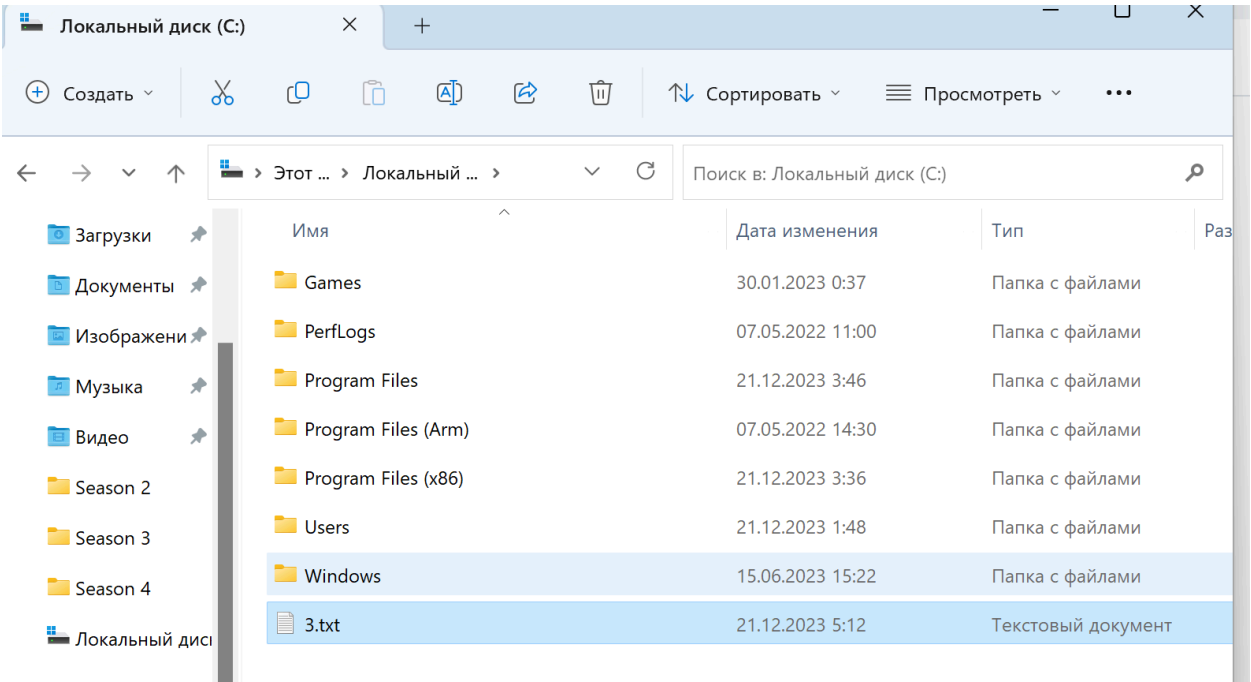
Появляется такое же окно выбора формата.

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

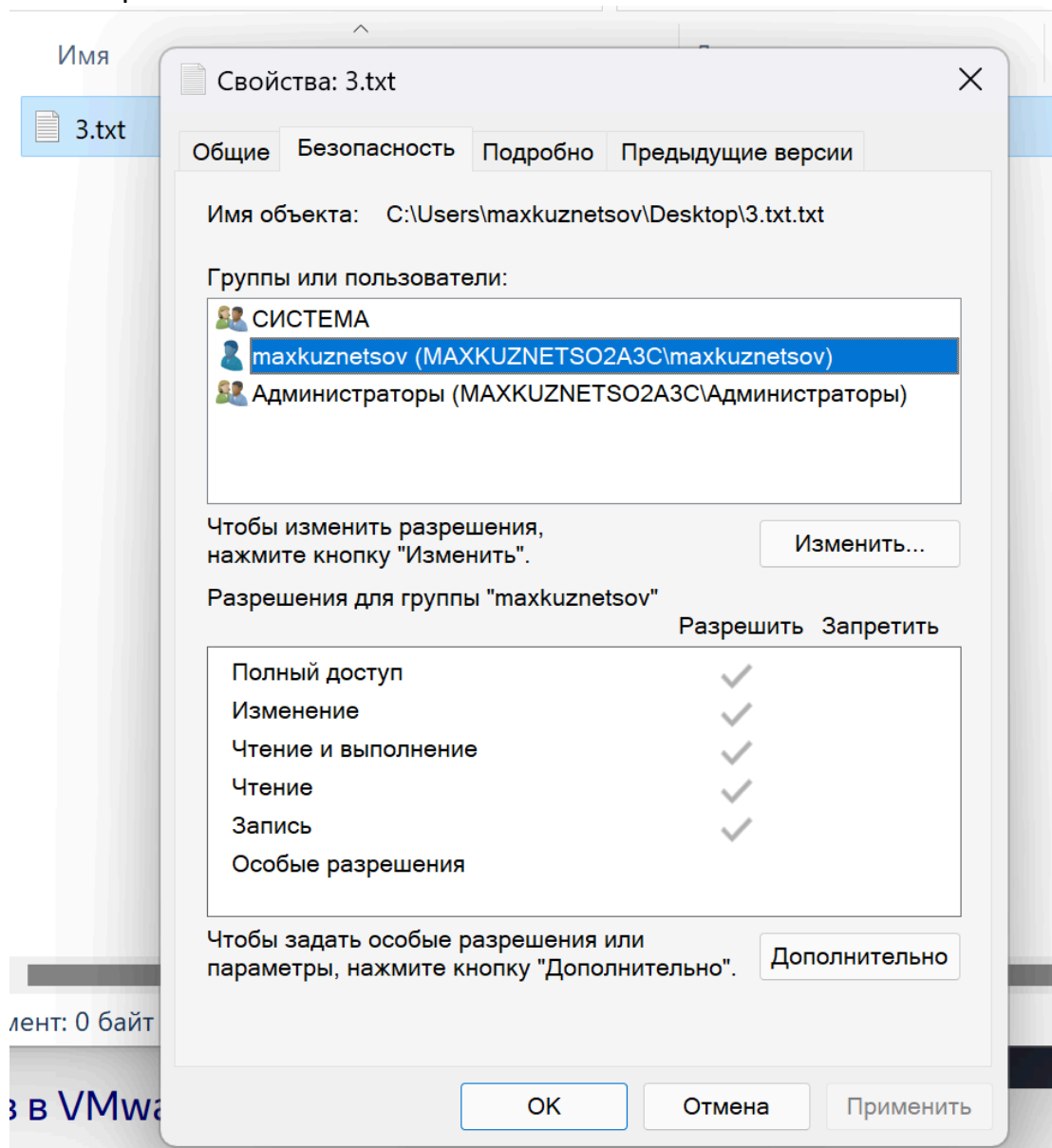
Вариант на работу – 13(3) таким образом выполняем 1.

Какие разрешения (права доступа) будут у Пользователя и у Администратора на файл «Новарианта.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»)?

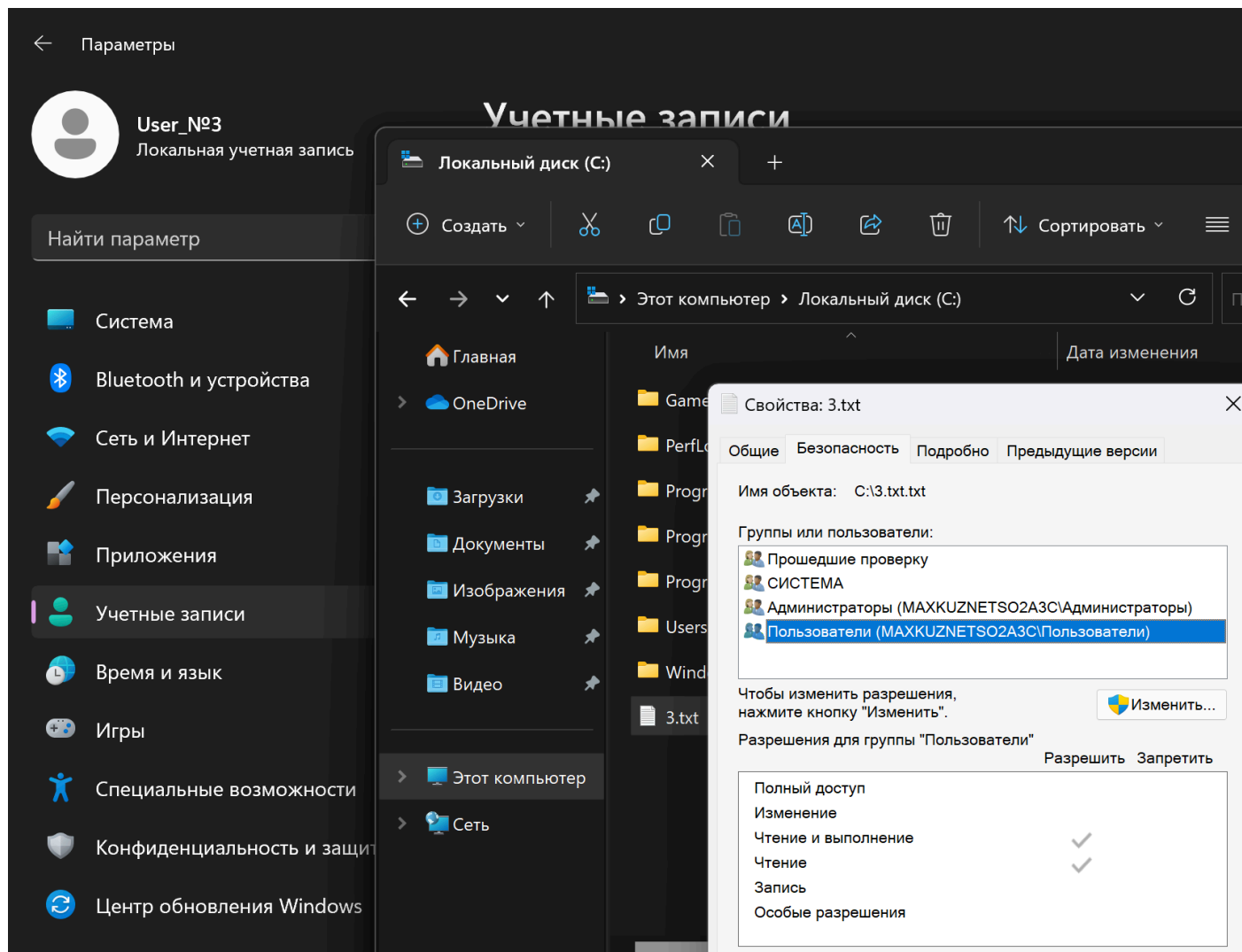
Создадим файл 3.txt



Посмотрим сначала свойства.



От директории права перешли на созданный файл, у Пользователя на файл есть доступ на чтение и выполнение, а у Администратора - полный доступ.



Вернемся в аккаунт администратора. Откроем снова свойства и изменим доступы в соответствии с заданием:

для Пользователя установлено «Запись»

для Администратора установлено «Чтение»

для группы «Все» установлено «Изменение»

Разрешения для группы прошедшие  
проверку"

Разрешить Запретить

Полный доступ

Изменение

Чтение и выполнение

Чтение

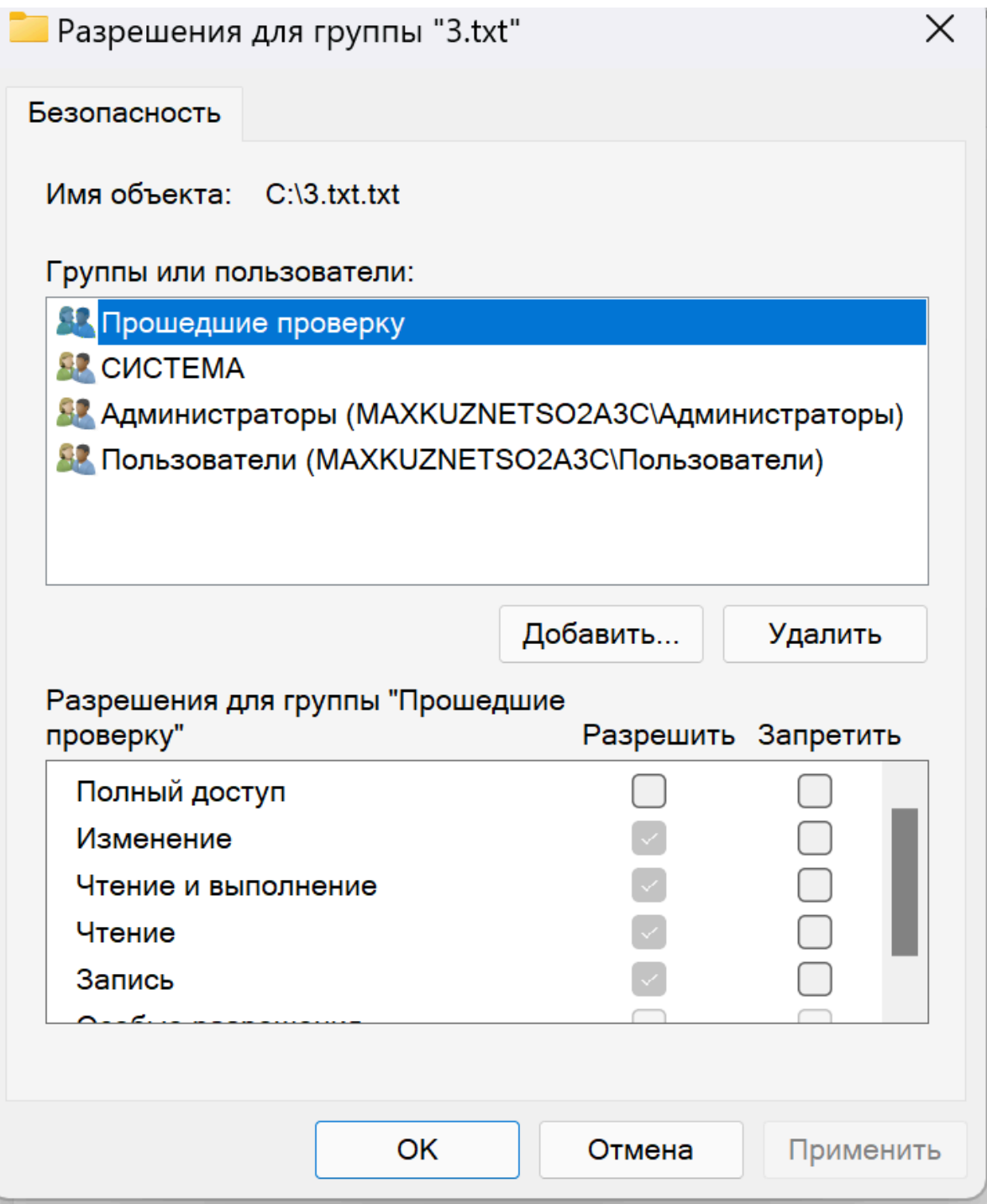
Запись

Особые разрешения



Чтобы задать особые разрешения или  
параметры, нажмите кнопку "Дополнительно".

Дополнительно









Разрешения для группы "3.txt"



Безопасность

Имя объекта: C:\3.txt.txt

Группы или пользователи:

-  Admin\_№3 (MAXKUZNETSO2A3C\Admin\_№3)
-  User\_№3 (MAXKUZNETSO2A3C\User\_№3)
-  Прошедшие проверку
-  СИСТЕМА
-  Администраторы (MAXKUZNETSO2A3C\Администраторы)
-  Пользователи (MAXKUZNETSO2A3C\Пользователи)

Добавить...

Удалить

Разрешения для группы "Admin\_№3" Разрешить Запретить

Полный доступ	<input type="checkbox"/>	<input type="checkbox"/>
Изменение	<input type="checkbox"/>	<input type="checkbox"/>
Чтение и выполнение	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Чтение	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Запись	<input type="checkbox"/>	<input type="checkbox"/>
Создание	<input type="checkbox"/>	<input type="checkbox"/>

ОК

Отмена

Применить




Разрешения для группы "3.txt"


×


Безопасность


Имя объекта: C:\3.txt.txt


Группы или пользователи:


 Admin\_№3 (MAXKUZNETSO2A3C\Admin\_№3)

 User\_№3 (MAXKUZNETSO2A3C\User\_№3)

 Прошедшие проверку

 СИСТЕМА

 Администраторы (MAXKUZNETSO2A3C\Администраторы)

 Пользователи (MAXKUZNETSO2A3C\Пользователи)

Добавить...

Удалить

Разрешения для группы "User\_№3"

Разрешить

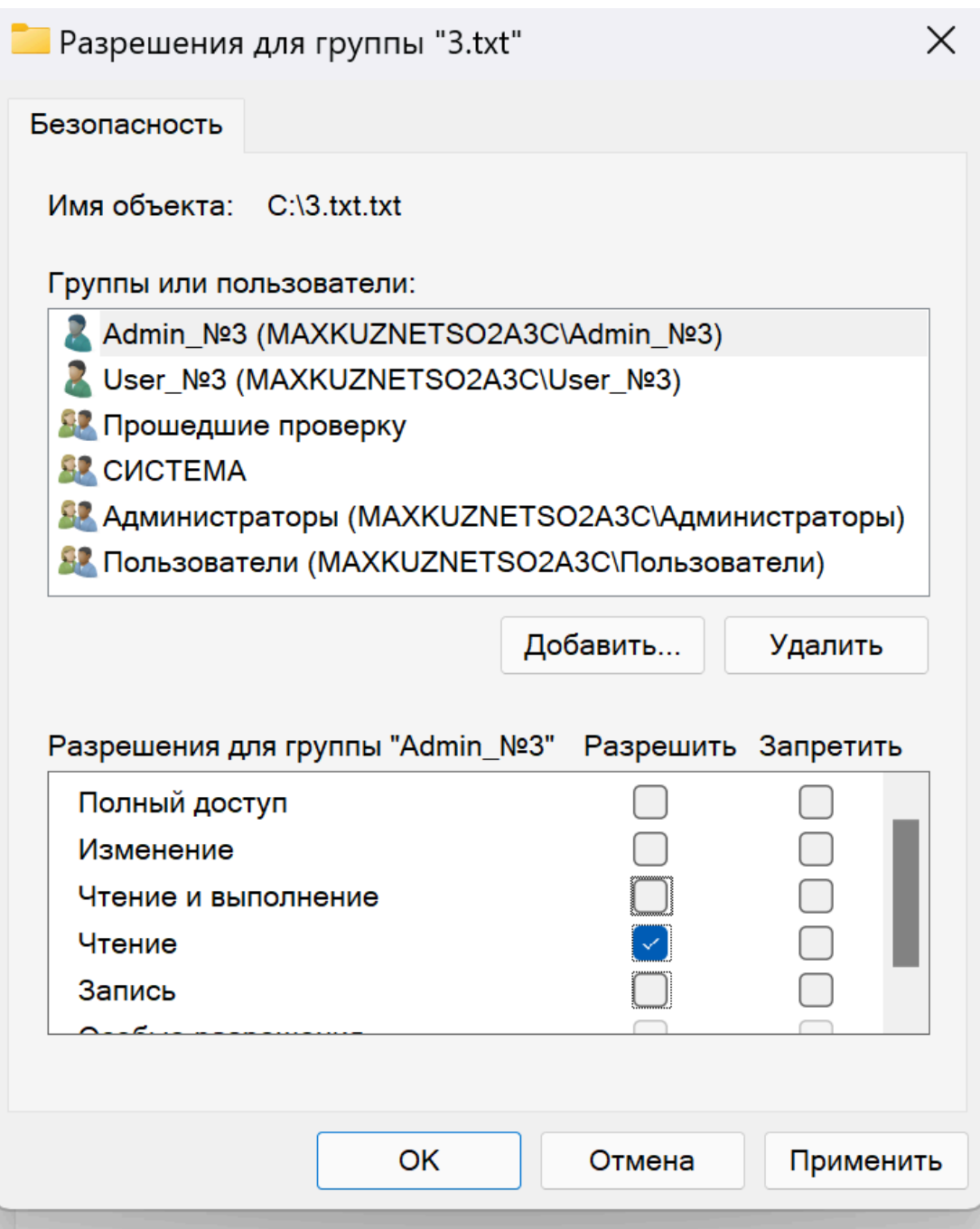
Запретить

Полный доступ	<input type="checkbox"/>	<input type="checkbox"/>
Изменение	<input type="checkbox"/>	<input type="checkbox"/>
Чтение и выполнение	<input type="checkbox"/>	<input type="checkbox"/>
Чтение	<input type="checkbox"/>	<input type="checkbox"/>
Запись	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Создание подкаталогов и файлов	<input type="checkbox"/>	<input type="checkbox"/>

ОК

Отмена

Применить



Разрешения для группы "3.txt"

Безопасность

Имя объекта: C:\3.txt.txt

Группы или пользователи:

Admin\_№3 (MAXKUZNETSO2A3C\Admin\_№3)

User\_№3 (MAXKUZNETSO2A3C\User\_№3)

Прошедшие проверку

СИСТЕМА

Администраторы (MAXKUZNETSO2A3C\Администраторы)

Пользователи (MAXKUZNETSO2A3C\Пользователи)

Добавить...

Удалить

Разрешения для группы "Пользователи"

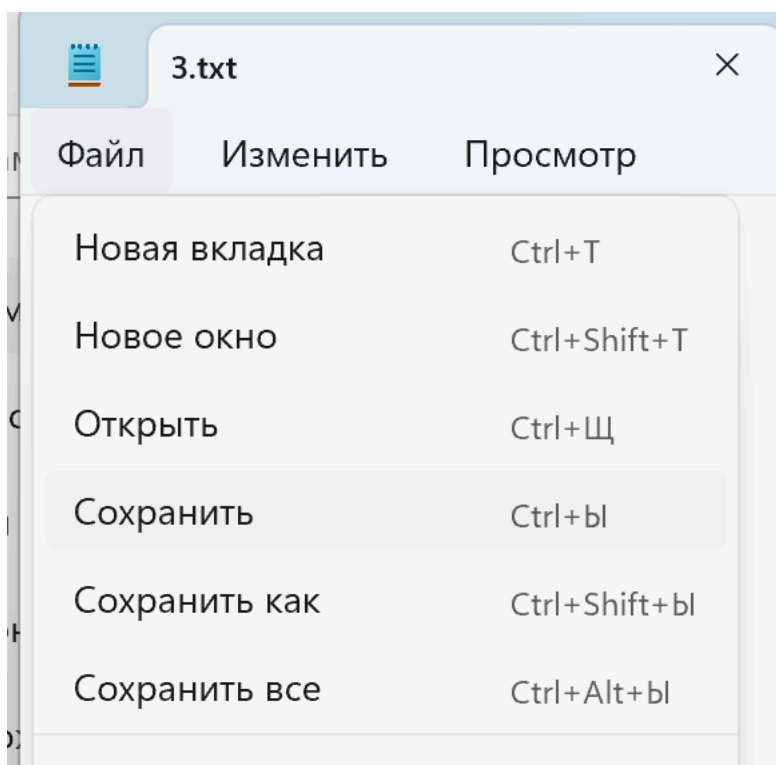
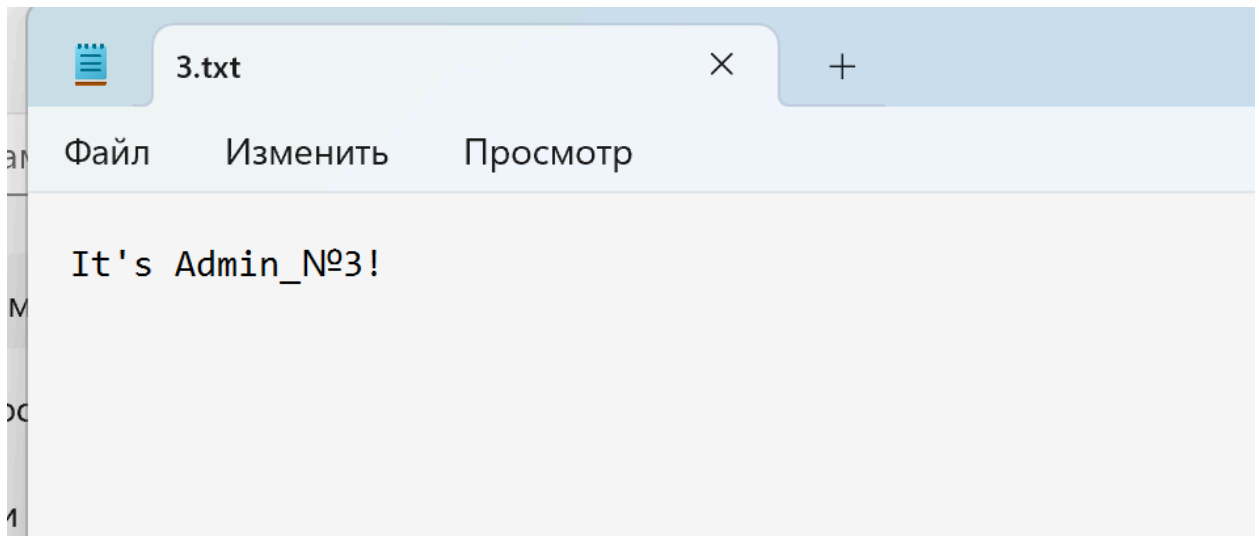
	Разрешить	Запретить
Полный доступ	<input type="checkbox"/>	<input type="checkbox"/>
Изменение	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Чтение и выполнение	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Чтение	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Запись	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Особые разрешения	<input type="checkbox"/>	<input type="checkbox"/>

OK

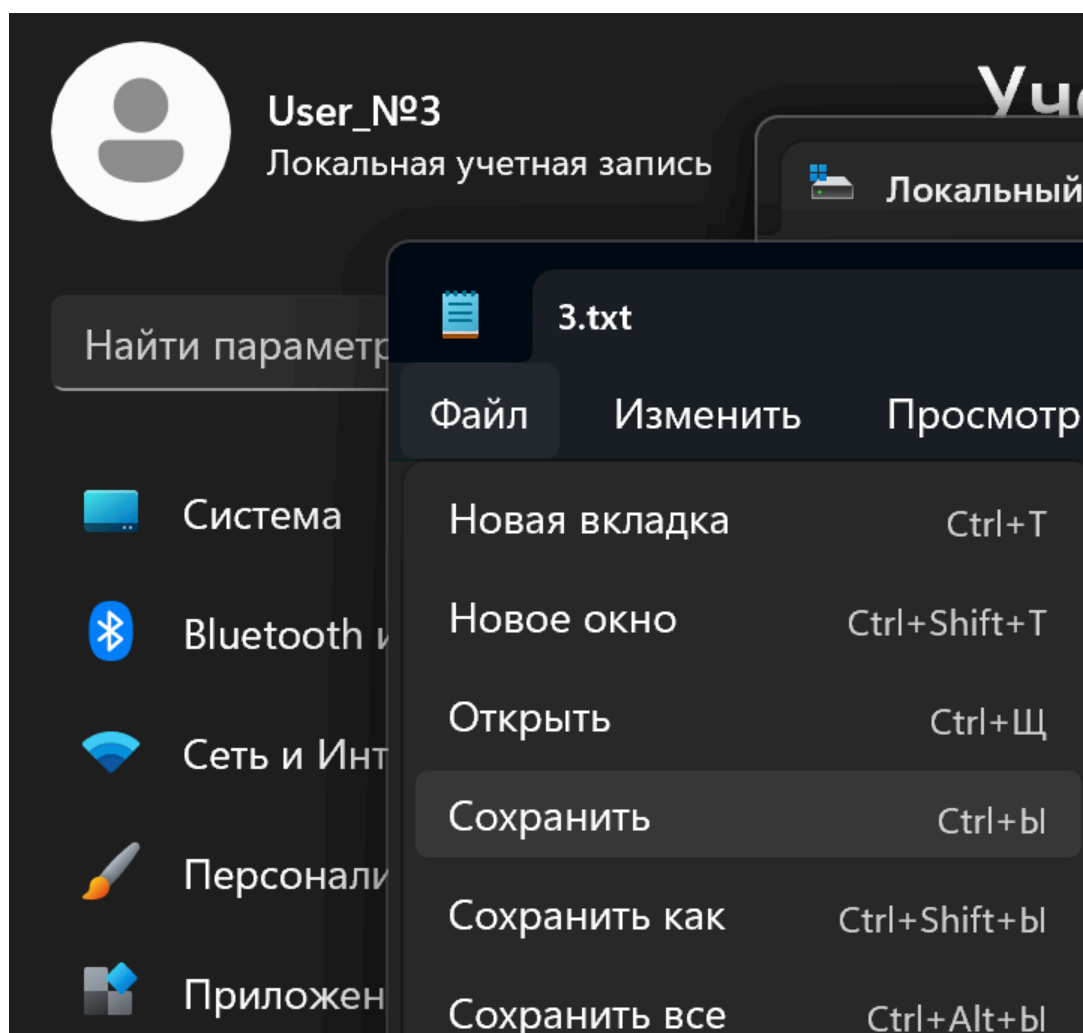
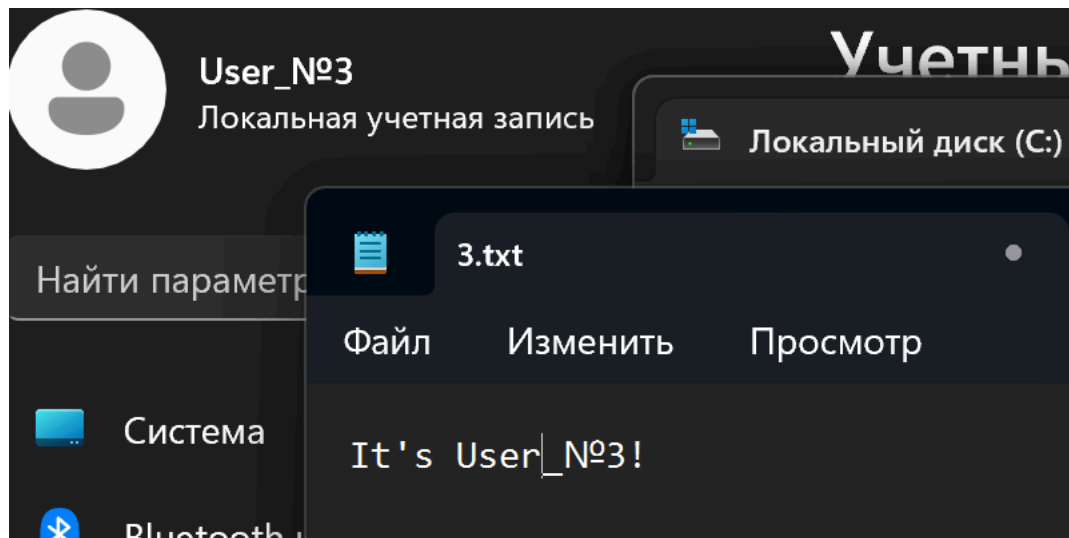
Отмена

Применить

Теперь переключимся на Admin\_3. Появилась возможность писать и сохранять файл



Теперь переключимся на User\_№3. Появилась такая же возможность писать и сохранять файл

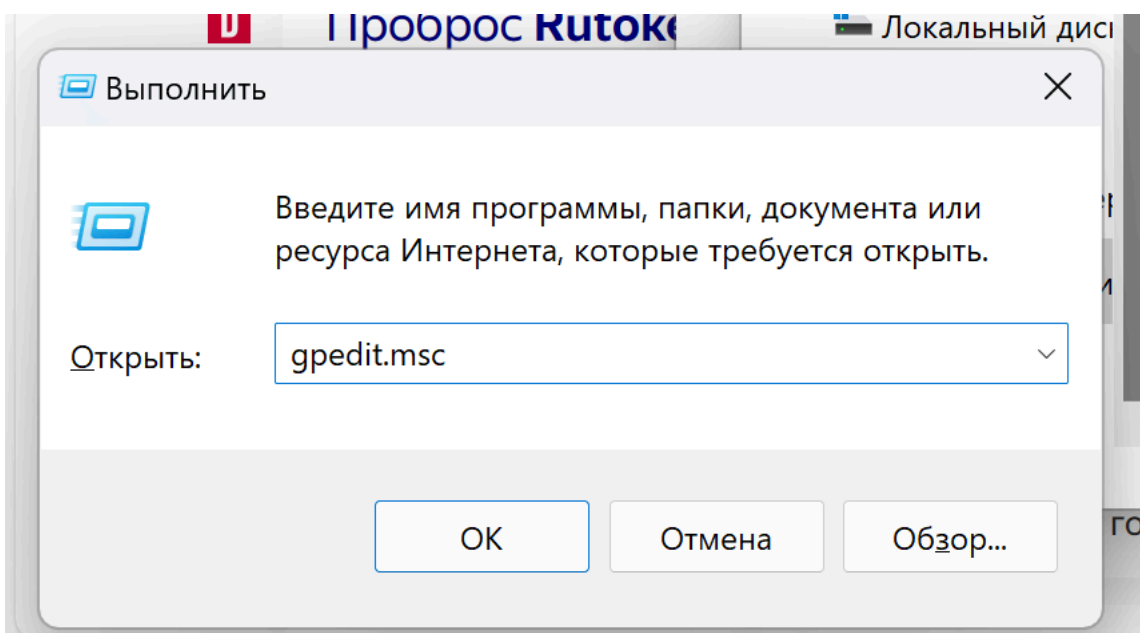


#### 4. Выполните настройки встроенных механизмов защиты ОС Windows в соответствии с заданием

Запретить встроенными средствами ОС Windows пользователю запись информации на внешние flash-накопители. Проанализировать возможность и сложность настройки.

##### Способ 1

Нажать сочетание клавиш Win+R, вводим → gpedit.msc (Однако, так как данная утилита первоначально у меня не сработала, то используется аналогичная ей Policy Plus)



Policy Plus

FileViewFindShareHelp

User or Computer

Компоненты Windows

Меню «Пуск» и панель задач

Общие папки

Панель управления

Принтеры

Рабочий стол

Сервер

Сеть

Система

App-V

Device Guard

ISCSI

Kerberos

LAPS

Аудит создания процессов

Варианты действий после нажатия CTRL+ALT+DEL

Восстановление

Восстановление системы

Вход в систему

Групповая политика

Диагностика

Дисковые квоты

Диспетчер сервера

Дисплей

Доступ к съемным запоминающим устройствам

Доступ к устройствам Enhanced Storage

Завершение работы

Защита DMA ядра

Защита файлов Windows

Инфраструктура классификации файлов

Контроль памяти

Параметры диспетчера служб

Параметры завершения работы

Параметры уменьшения рисков

Передача учетных данных

Перенаправление папок

Политики ОС

Помощь при ошибке «Отказано в доступе»

Поставщик теневых копий файлового ресурса общего назначения

Профили пользователей

Публикация ресурсов

Доступ к съемным запоминающим устройствам

This category contains 33 policies and 0 subcategories.

Name	State	Comment
Up: Система	Parent	
WPD-устройства: Запретить запись	Not Configured (U)	
WPD-устройства: Запретить запись	Not Configured (C)	
WPD-устройства: Запретить чтение	Not Configured (U)	
WPD-устройства: Запретить чтение	Not Configured (C)	
Время (в секундах) до принудительной перезагрузки	Not Configured (U)	
Время (в секундах) до принудительной перезагрузки	Not Configured (C)	
Все съемные запоминающие устройства: разрешение прямого доступа в удаленных сеансах	Not Configured (C)	
Компакт-диски и DVD-диски: Запретить выполнение	Not Configured (U)	
Компакт-диски и DVD-диски: Запретить запись	Not Configured (C)	
Компакт-диски и DVD-диски: Запретить запись	Not Configured (C)	
Компакт-диски и DVD-диски: Запретить чтение	Not Configured (U)	
Компакт-диски и DVD-диски: Запретить чтение	Not Configured (C)	
Ленточные накопители: Запретить выполнение	Not Configured (C)	
Ленточные накопители: Запретить запись	Not Configured (U)	
Ленточные накопители: Запретить запись	Not Configured (C)	
Ленточные накопители: Запретить чтение	Not Configured (U)	
Ленточные накопители: Запретить чтение	Not Configured (C)	
Накопители на гибких дисках: Запретить выполнение	Not Configured (C)	
Накопители на гибких дисках: Запретить запись	Not Configured (U)	
Накопители на гибких дисках: Запретить запись	Not Configured (C)	
Накопители на гибких дисках: Запретить чтение	Not Configured (U)	
Накопители на гибких дисках: Запретить чтение	Not Configured (C)	
Специальные классы: Запретить запись	Not Configured (U)	
Специальные классы: Запретить запись	Not Configured (C)	
Специальные классы: Запретить чтение	Not Configured (U)	
Специальные классы: Запретить чтение	Not Configured (C)	
Съемные диски: Запретить выполнение	Not Configured (C)	
Съемные диски: Запретить запись	Not Configured (U)	
Съемные диски: Запретить запись	Not Configured (C)	
Съемные диски: Запретить чтение	Not Configured (U)	
Съемные диски: Запретить чтение	Not Configured (C)	
Съемные запоминающие устройства всех классов: Запретить любой доступ	Not Configured (U)	
Съемные запоминающие устройства всех классов: Запретить любой доступ	Not Configured (C)	

Computer source: Local GPO | User source: Local GPO

3°C Cloudy

Поиск

5:51

21.12.2023

## Съемные диски: Запретить запись

Requirements:  
Не ниже Windows Vista

Этот параметр политики запрещает запись на съемные диски.

Включение этого параметра политики запрещает запись на съемные носители этого класса.

Если параметр политики отключен или не определен, запись на съемные носители этого класса разрешена.

Примечание. Чтобы пользователи могли записывать данные только на запоминающие устройства, защищенные BitLocker, включите параметр политики «Запретить запись на диски, не защищенные BitLocker», расположенный в «Конфигурация компьютера\Шаблоны администрирования\Компоненты Windows\Шифрование дисков BitLocker\Съемные диски».

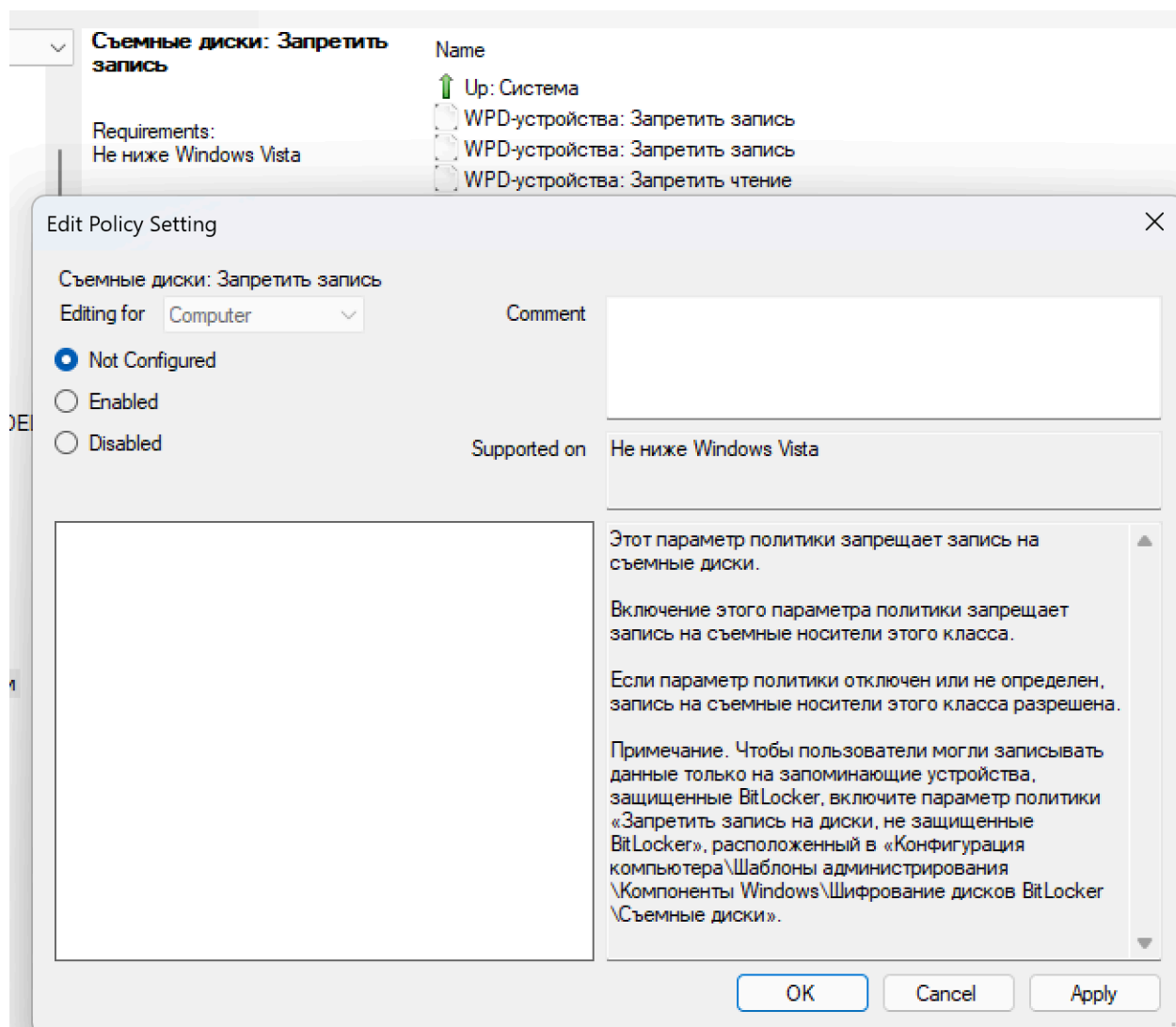
Name

- ↑ Up: Система
- WPD-устройства: Запретить запись
- WPD-устройства: Запретить запись
- WPD-устройства: Запретить чтение
- WPD-устройства: Запретить чтение
- Время (в секундах) до принудительной перезагрузки
- Время (в секундах) до принудительной перезагрузки
- Все съемные запоминающие устройства: разрешение прямого доступ
- Компакт-диски и DVD-диски: Запретить выполнение
- Компакт-диски и DVD-диски: Запретить запись
- Компакт-диски и DVD-диски: Запретить запись
- Компакт-диски и DVD-диски: Запретить чтение
- Компакт-диски и DVD-диски: Запретить чтение
- Ленточные накопители: Запретить выполнение
- Ленточные накопители: Запретить запись
- Ленточные накопители: Запретить запись
- Ленточные накопители: Запретить чтение
- Ленточные накопители: Запретить чтение
- Накопители на гибких дисках: Запретить выполнение
- Накопители на гибких дисках: Запретить запись
- Накопители на гибких дисках: Запретить запись
- Накопители на гибких дисках: Запретить чтение
- Накопители на гибких дисках: Запретить чтение
- Специальные классы: Запретить запись
- Специальные классы: Запретить запись
- Специальные классы: Запретить чтение
- Специальные классы: Запретить чтение
- Съемные диски: Запретить выполнение
- Съемные диски: Запретить запись**

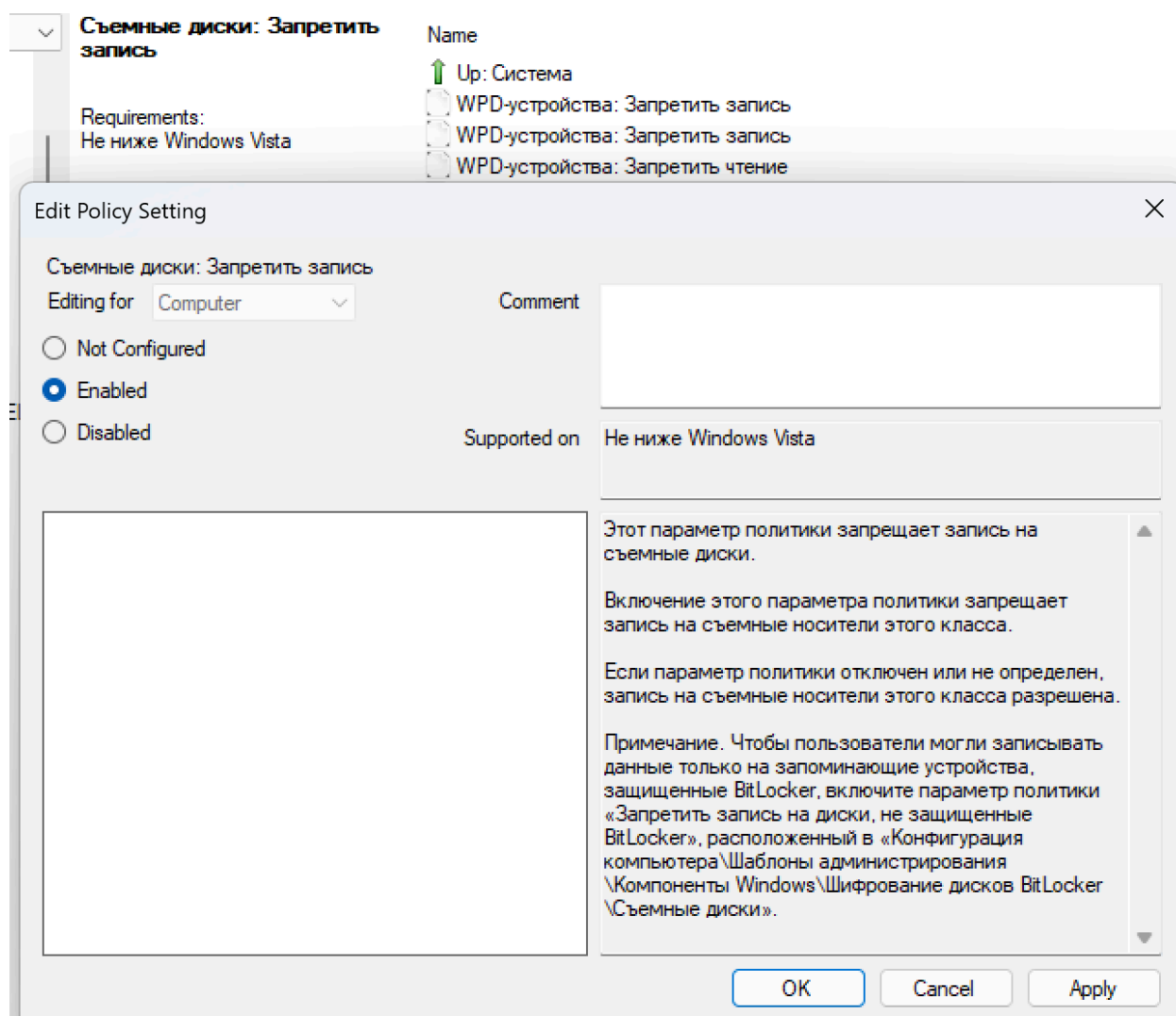
Буквы U и C отвечают соответственно за User и Computer правило

 Съемные диски: Запретить запись	Not Configured (U)
 Съемные диски: Запретить запись	Not Configured (C)





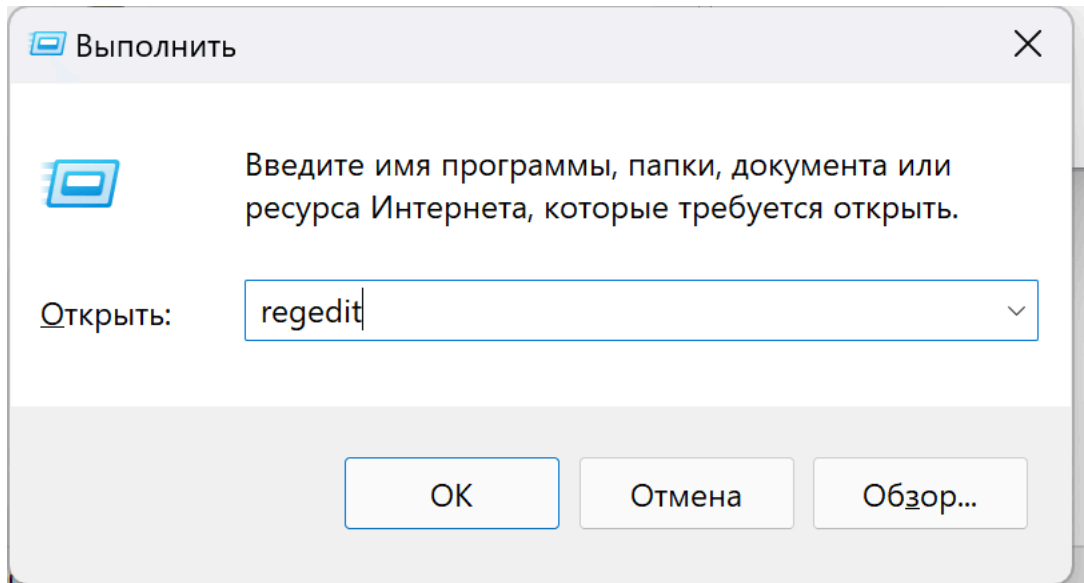
Ставим селект в Enabled → Ок → Apply



## Способ 2

Так как первый способ был немного искажен за отсутствием редактора групповой политики (gpedit), то ту же блокировку можно выполнить с помощью редактора реестра:

Жмем Win+R



В редакторе реестра переходим к одному из разделов:

1. HKEY\_LOCAL\_MACHINE — для запрета использования USB накопителей для всех пользователей.
2. HKEY\_CURRENT\_USER — только для текущего пользователя



# Редактор реестра

Файл Правка Вид Избранное Справка

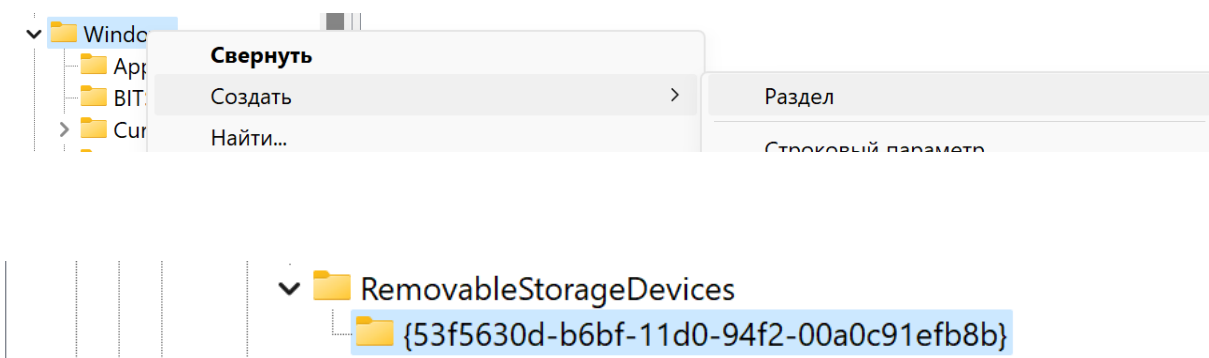
Компьютер\HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies

- > HKEY\_CURRENT\_USER
- ▼ HKEY\_LOCAL\_MACHINE
  - > BCD00000000
  - > HARDWARE
  - > SAM
  - SECURITY
  - ▼ SOFTWARE
    - > Aktiv Co.
    - > Classes
    - > Clients
    - CVSM
    - DefaultUserEnvironment
    - > Google
    - > Microsoft
    - > MySmartLogon
    - > ODBC
    - > OEM
    - > OpenSSH
    - > Parallels
    - > Partner
    - ▼ Policies
      - ▼ Microsoft
        - > Cryptography
        - > Edge
        - Peernet
        - > SystemCertificates
        - TabletPC
        - TPM
        - ▼ Windows
          - Appx
          - BITS
          - > CurrentVersion
          - DataCollection
          - EnhancedStorageDev
          - GameDVR
          - > IPsec
          - NetCache
          - Network Connection
          - NetworkConnectivity
          - NetworkProvision

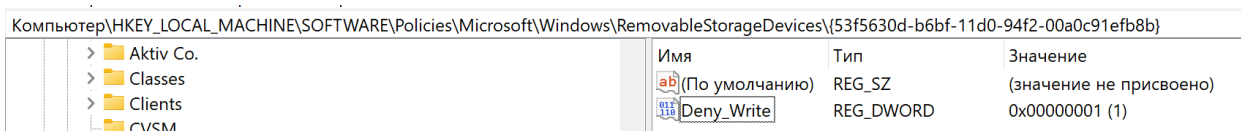
Имя

ab(П

Создаем подраздел *RemovableStorageDevices*, а в нем — подраздел с именем *{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}*



В этом подразделе создаем следующие параметры: нужные параметры DWORD32 (даже для Windows x64) — с именем *Deny\_Write* — для запрета записи на USB накопитель. И установим значение 1.



Запрет на запись на Flash накопителя вступит в силу сразу после внесения изменения (если на момент блокировки накопитель уже был подключен к компьютеру или ноутбуку, он будет доступен до отключения и повторного подключения).

P. S. Описанные способы работают для съемных USB флешек и дисков, однако не работают для устройств, подключенных по протоколу MTP и RTP (например, хранилище Android телефона продолжит быть доступным). Для отключения доступа по этим протоколам, в редакторе локальной групповой политики в том же разделе нужно использовать параметры «WPD-устройства» для запрета чтения и записи.

В редакторе реестра это будет выглядеть как подразделы:

*{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}*

*{6AC27878-A6FA-4155-BA85-F98F491D4F33}*

*{F33FDC04-D1AC-4E8E-9A30-19BBD4B108AE}*

В политиках *RemovableStorageDevices* (как описывалось выше) с параметрами *Deny\_Write*.

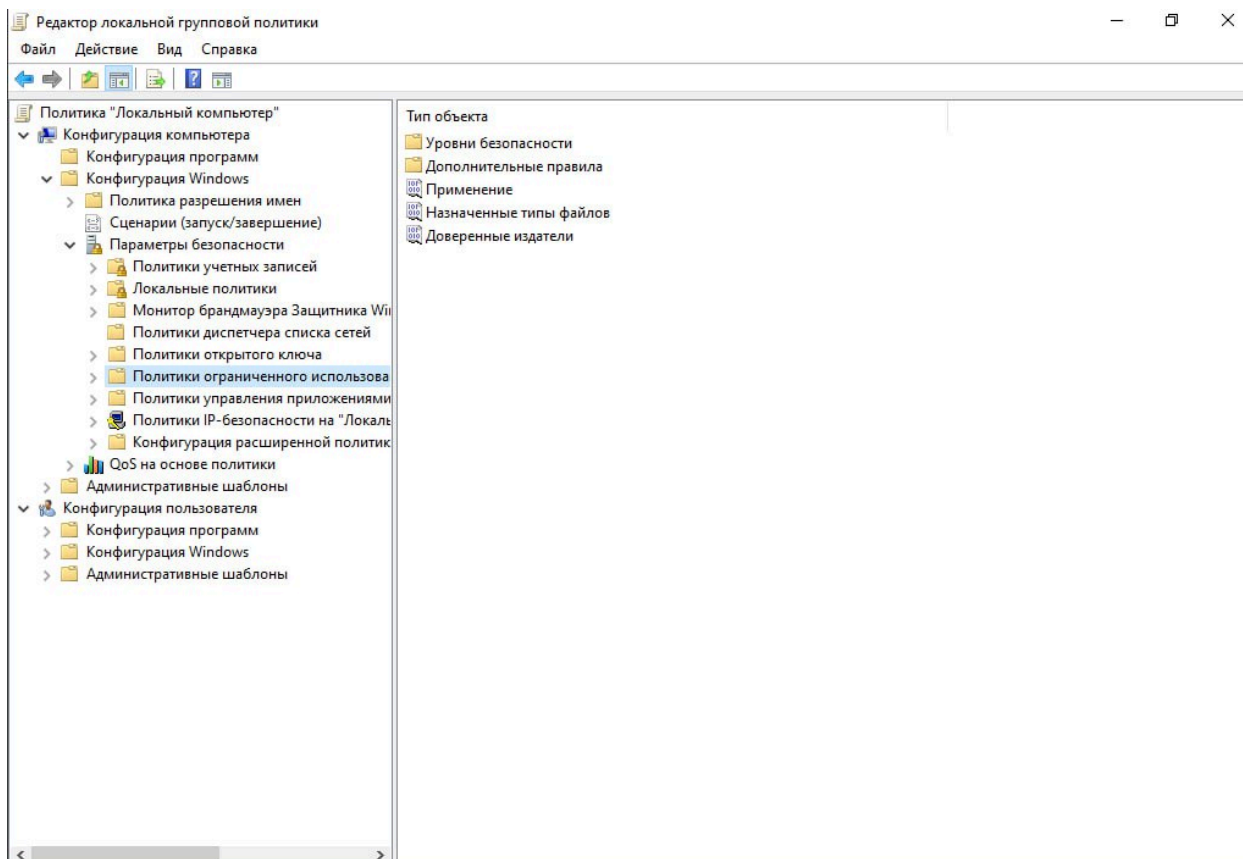
5. Разрешите средствами операционной системы выполнять системные и прикладные программы только из папок %ProgramFiles% и %SystemRoot%

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, вводим → gpedit.msc (Для версии Windows 11 Home нужно скачивать пакеты)

```
@echo off
dir /b C:\Windows\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientExtensions-Package~3*.mum >find-gpedit.txt
dir /b C:\Windows\servicing\Packages\Microsoft-Windows-GroupPolicy-ClientTools-Package~3*.mum >>find-gpedit.txt
echo Ustanovka gpedit.msc
for /f %%i in ('findstr /i . find-gpedit.txt 2^>nul') do dism /online /norestart /add-package:"C:\Windows\servicing\Packages\%%i"
echo Gpedit ustanovlen.
pause
```

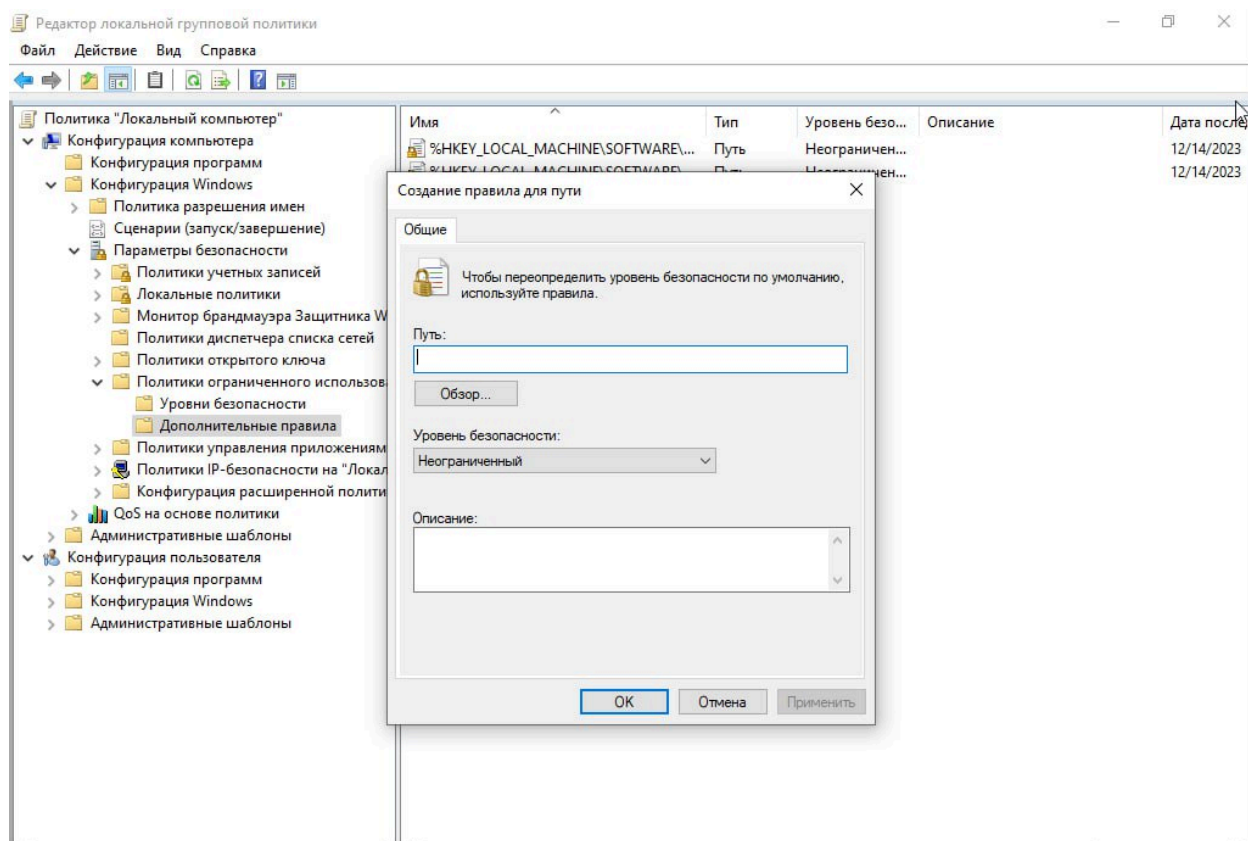
После установки пакетов заходим в gpedit.msc



Идем по пути:  
Конфигурация компьютера → Конфигурация Windows →  
Параметры безопасности → Политики ограниченного использования программ.

Затем нажимаем правую кнопку мыши → Политики ограниченного использования программ → Создать политику ограниченного использования программ





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

Редатор локальной групповой политики

ФайлДействиеВидСправка

←→📁📄🔍🔧🔗🔑🔒🔓🔔🔕🔖🔗🔑🔒🔓🔔🔕🔖

Политика "Локальный компьютер"

▼

Конфигурация компьютера

▼

Конфигурация Windows

>

Политика разрешения имен

Сценарии (запуск/завершение)

▼

Параметры безопасности

>

Политики учетных записей

>

Локальные политики

>

Монитор брандмауэра Защитника Windows

>

Политики диспетчера списка сетей

>

Политики открытого ключа

▼

Политики ограниченного использования

>

Уровни безопасности

Дополнительные правила

>

Политики управления приложениями

>

Политики IP-безопасности на "Локальный компьютер"

>

Конфигурация расширенной политики

>

QoS на основе политики

>

Административные шаблоны

▼

Конфигурация пользователя

>

Конфигурация программ

>

Конфигурация Windows

>

Административные шаблоны

Имя	Тип	Уровень безо...	Описание	Дата после...
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Путь	Неограничен...		12/14/2023
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Путь	Неограничен...		12/14/2023
%ProgramFile%	Путь	Неограничен...		12/21/2023

Редактор локальной групповой политики

ФайлДействиеВидСправка

←→🔍📄🔗🔧🔑🔒🔗🔑🔒

Политика "Локальный компьютер"

▼

Конфигурация компьютера

▼

Конфигурация Windows

>

Политика разрешения имен

📄

Сценарии (запуск/завершение)

▼

Параметры безопасности

>

Политики учетных записей

>

Локальные политики

>

Монитор брандмауэра Защитника Windows

>

Политики диспетчера списка сетей

>

Политики открытого ключа

▼

Политики ограниченного использования

>

Уровни безопасности

📄

Дополнительные правила

>

Политики управления приложениями

>

Политики IP-безопасности на "Локальный компьютер"

>

Конфигурация расширенной политики

>

QoS на основе политики

>

Административные шаблоны

▼

Конфигурация пользователя

>

Конфигурация программ

>

Конфигурация Windows

>

Административные шаблоны

Имя

%HKEY\_LOCAL\_MACHINE\SOFTWARE\...

%HKEY\_LOCAL\_MACHINE\SOFTWARE\...

%ProgramFile%

%SystemRoot%

Тип

Путь

Путь

Путь

Путь

Уровень безо...

Неограничен...

Неограничен...

Неограничен...

Неограничен...

Описание

Дата после...

12/14/2023

12/14/2023

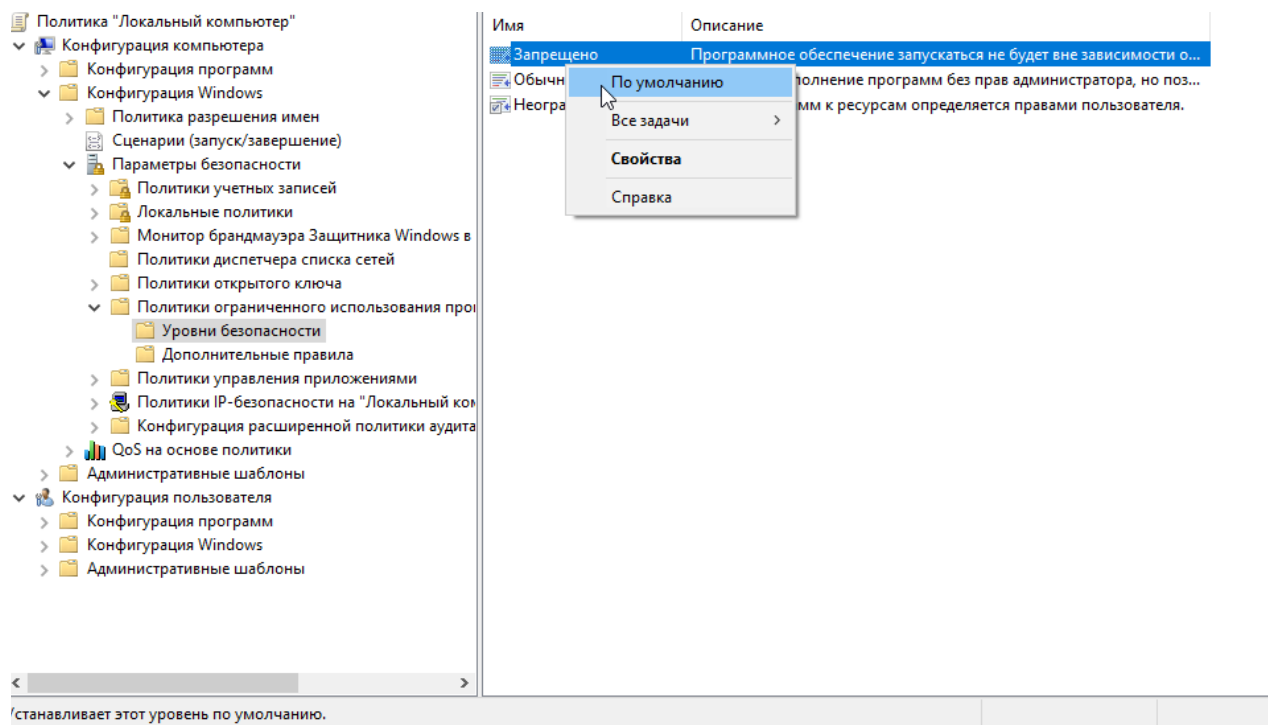
12/21/2023

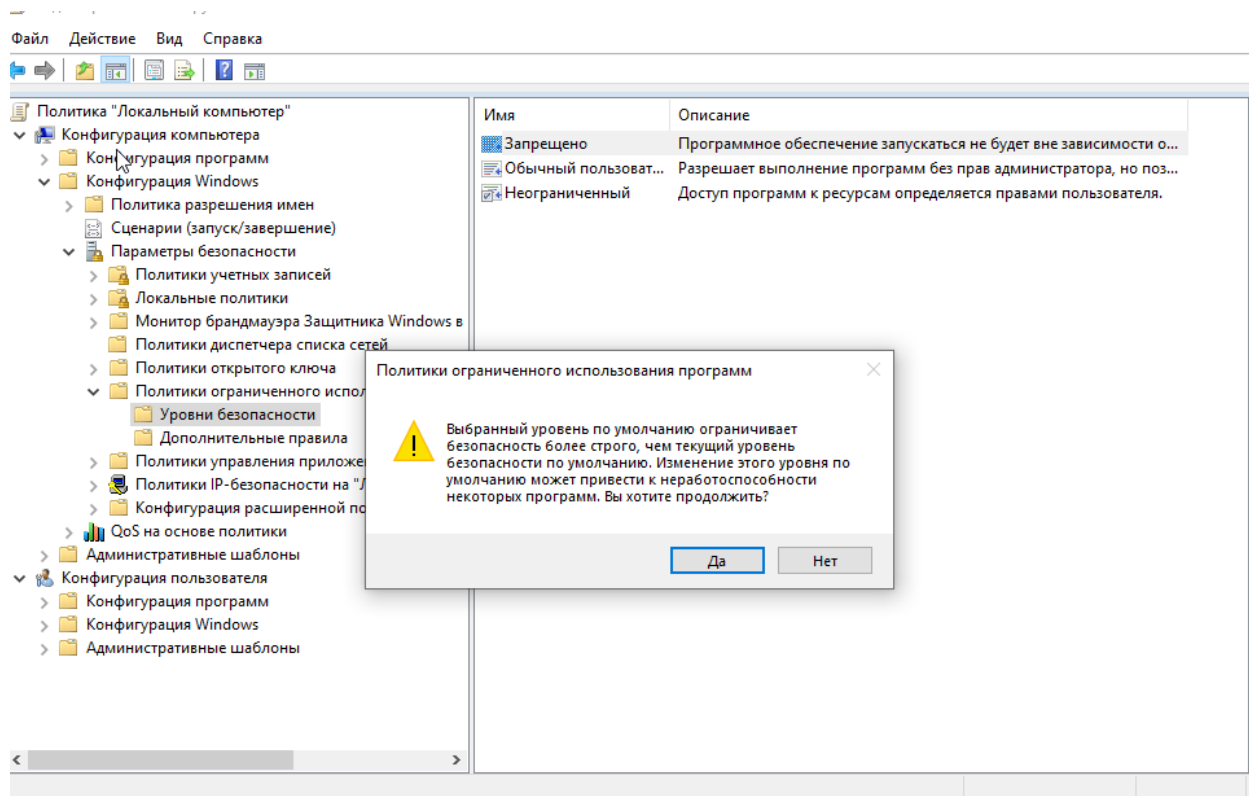
12/21/2023

Заккрыть

Переходим теперь в уровни безопасности.

**По умолчанию** установим запрет на выполнение любых программ, за исключением тех, которые находятся в %ProgramFiles% %SystemRoot%





## Вывод:

В результате выполнения данной лабораторной работы я:

- познакомился с файловыми системами FAT32 и NTFS.
- изучил работу программы с разрешениями
- научился управлять правами доступа на различные файлы.