

федеральное государственное автономное образовательное учреждение
высшего образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

ОТЧЕТ

по лабораторной работе №2

«Разграничение доступа к объектам файловой системы»

по дисциплине **«Информационная безопасность»**

Вариант 12

Автор: Кулаков Н. В.

Факультет: ПИиКТ

Группа: Р34312

Преподаватель: Маркина Т. А.



УНИВЕРСИТЕТ ИТМО

Санкт-Петербург 2023

Содержание

[illegible]

3.2.1.4. TreeSize (Jam Software's).....	30
3.2.1.5. NTFSSecurity модуль PowerShell (by raandree).....	35
3.2.2. Сравнение FAT и NTFS.....	37
3.2.3. Описание возможных способов задания прав к файлам и папкам.....	40
3.2.3.1. Через explorer (проводник).....	40
3.2.3.2. Через powershell (Get-Acl, Set-Acl).....	40
3.2.3.3. Через icacls.....	41
3.2.3.4. Ограничение исполнения при помощи политик ограниченного использования программ или AppLocker.....	42
3.2.3.5. Через приложения сторонних разработчиков, на примере NTFS Permission Tools.....	44
4. Выводы.....	46

1. Цель работы

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

2. Программные и аппаратные средства

Hw-probe: <https://linux-hardware.org/?probe=cff5d02cde>

Вендор и модель ноутбука: HUAWEI NBLK-WAX9X 2019

Основные аппаратные средства:

- Ryzen 5 3500U with Radeon Vega Mobile Gfx
- 2x RAM HMA851S6CJR6N-VK 4GB Row Of Chips DDR4 2667MT/s
- NVMe SSD Controller SM981/PM981/PM983 512GB
- RTL8822CE 802.11ac PCIe Wireless Network Adapter

Основные программные средства:

- ОС GNU/Linux Gentoo 2.14
- Ядро 6.1.53-gentoo-r1-x86_64

Программа эмуляции:

- libvirt (libvirt) 9.4.0 + QEMU emulator version 8.0.3 (virt-manager)
- Гипервизор KVM
- UEFI

Виртуальные машины:

- Windows 10 Enterprise N LTSC 21H2 19044.1288

- MEM 4096 МБ
- 4 vCPU
- SATA 40 ГБ
- Драйвера виртуальной машины: virtio-win

Программные средства:

- NTFS Permission Tools 1.3 from MajorGeeks.com
- NTFS Permission Reporter (Free Edition)
- Permissions Reporter v.4.0 (Key Metric Software)
- TreeSize
- TreeSize File Search
- PowerShell module NTFSSecurity v.4.2.6
(<https://github.com/raandree/NTFSSecurity>)

3. Выполнение

3.1. Основная часть

3.1.1. Минимальный набор разрешений

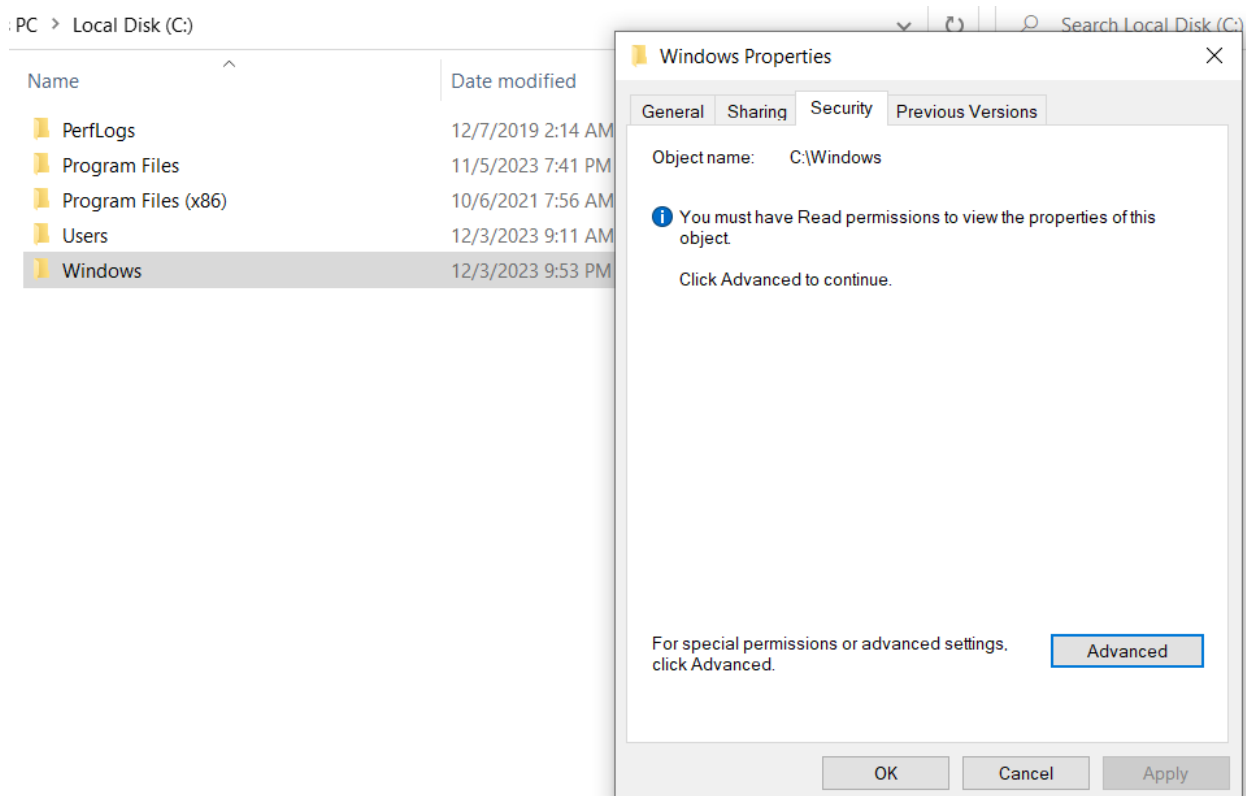
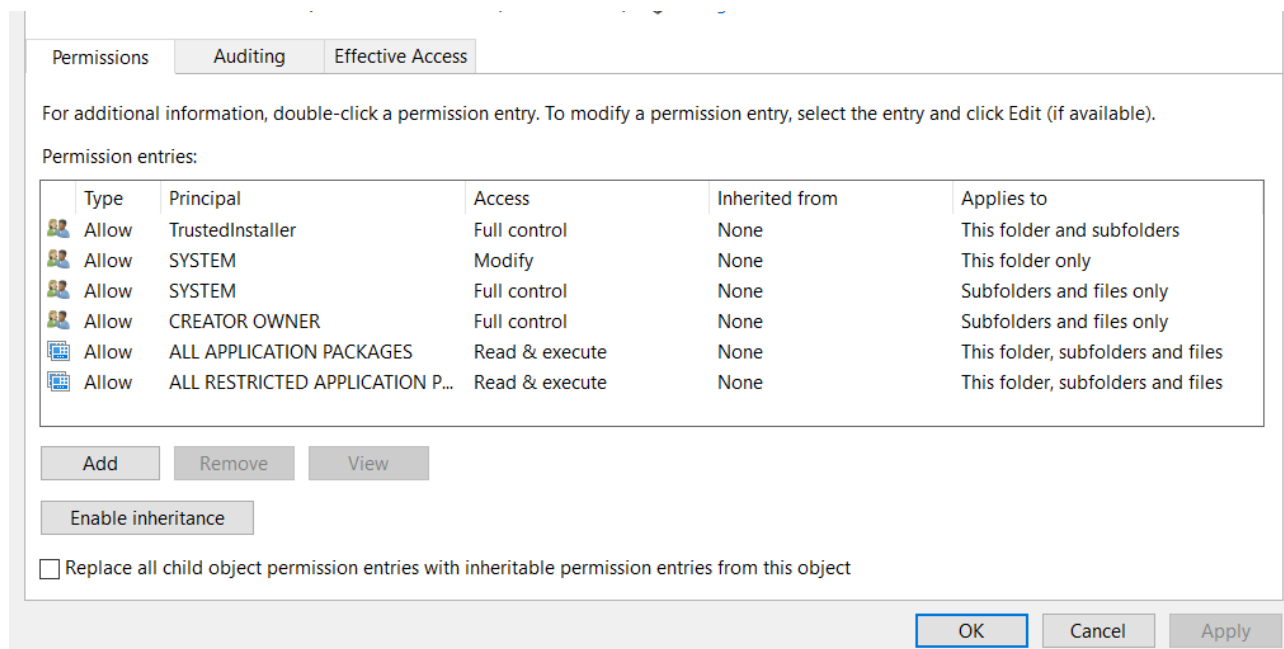
Укажите минимальный набор разрешений (прав доступа), необходимых для:

- 1. загрузки операционной системы;*
- 2. входа Пользователя (user_№варианта) и Администратора (admin_№варианта) в систему;*
- 3. работы с приложениями, установленными администратором.*

Разрешения указывать в форме R, W, X, в таблице.

Если явно в таблице не указано, что объект доступа разрешен, это значит, что он запрещен .

На рисунке ниже показано, что у пользователей (Users) и администраторов (Administrators) отображены все права.



3.1.1.1. Для загрузки ОС

Название объекта доступа	Администратор	Пользователь
-	-	-

В системе запрещены все права для пользователей, входящих в группу Users, Administrators. Все остальные права не были тронуты, например SYSTEM, который запускает страницу выбора для входа пользователей и проводит изначальную инициализацию системы.

3.1.1.2. Для входа в систему

Название объекта доступа	Администратор	Пользователь
C:\Windows*.*	RX	RX
%USERPROFILE%	RWX	RWX

В системе можно запускать системные приложения, входящие в пакет самой операционной системы, но нельзя запускать приложения, установленные администратором.

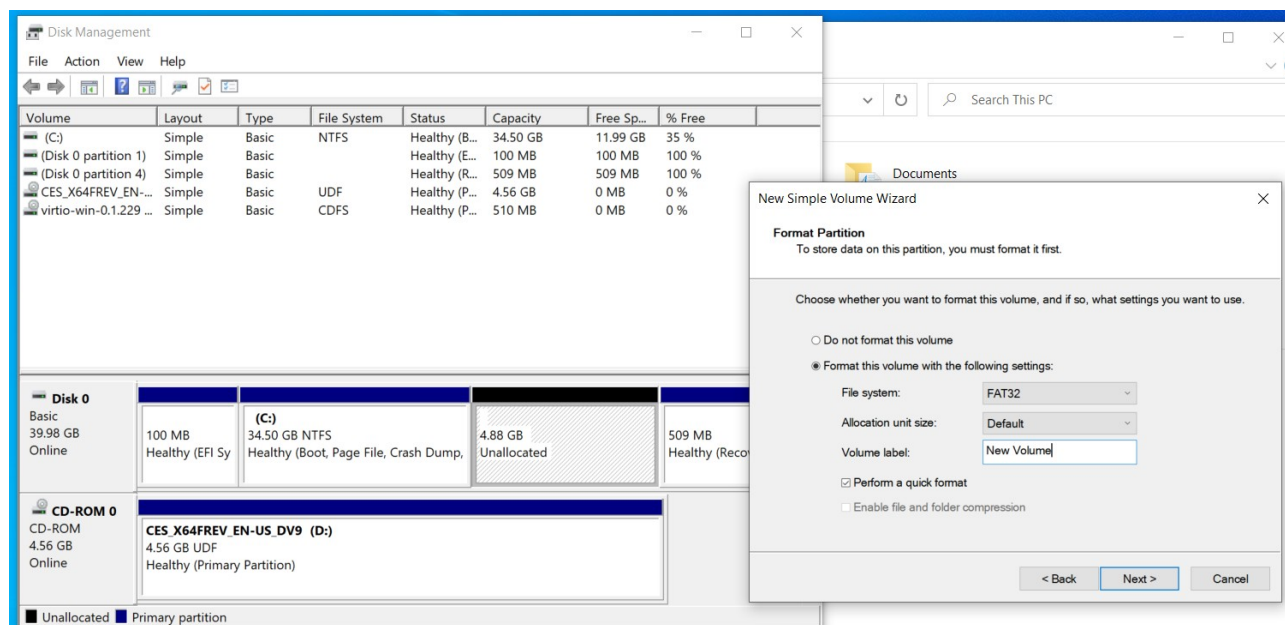
3.1.1.3. Для работы с приложениями, установленными администратором

Название объекта доступа	Администратор	Пользователь
C:\ProgramFiles	RWX	RX
C:\ProgramFiles86	RWX	RX
C:\Windows*.*	RWX	RX
%USERPROFILE%	RWX	RWX

3.1.2. Преобразование FAT в NTFS

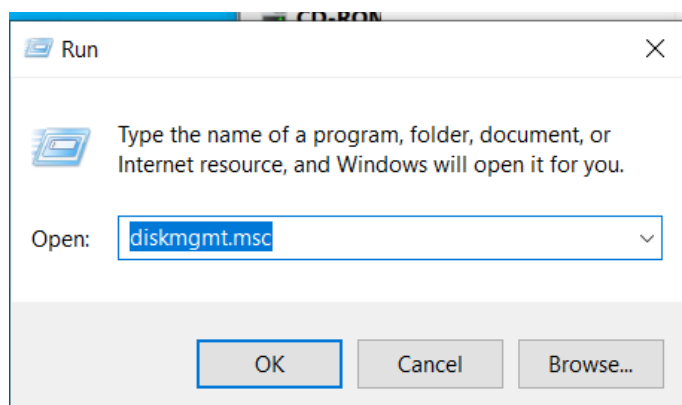
Преобразуйте файловую систему FAT (File Allocation Table) в NTFS (New Technology File System). Опишите преобразование в отчете с использованием скриншотов (минимум 2 способа).

Создаем раздел FAT32:

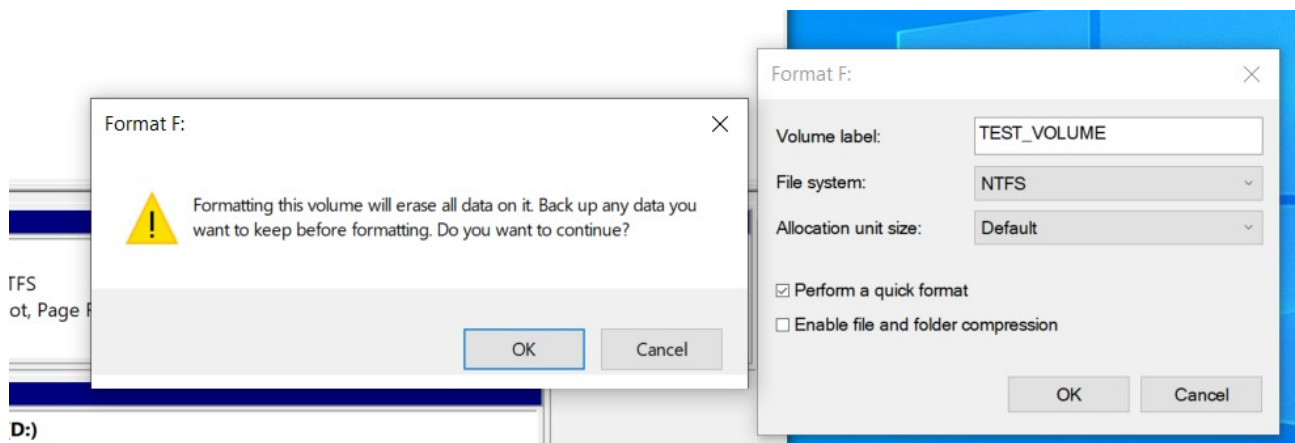


3.1.2.1. Через diskmgmt.msc с потерей данных

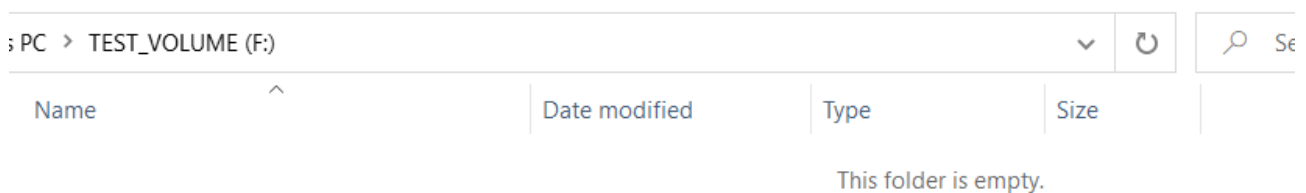
Открываем Disk Management:



Осуществляем форматирование с потерей данных:

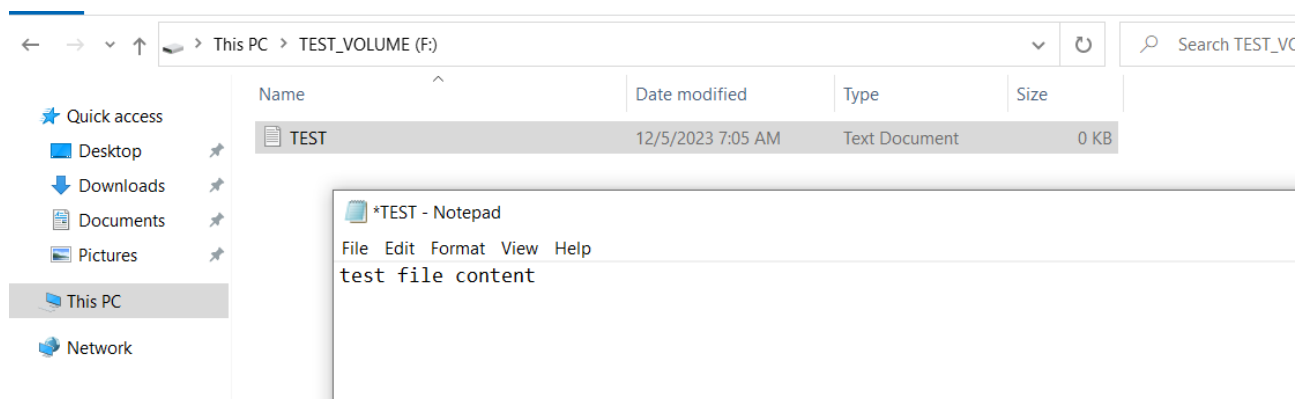


Форматирование прошло успешно, однако все данные были удалены:



3.1.2.2. Через cmd convert без потери данных

Создаем файл внутри тома формата FAT32 для дальнейшей демонстрации отсутствия потери данных:



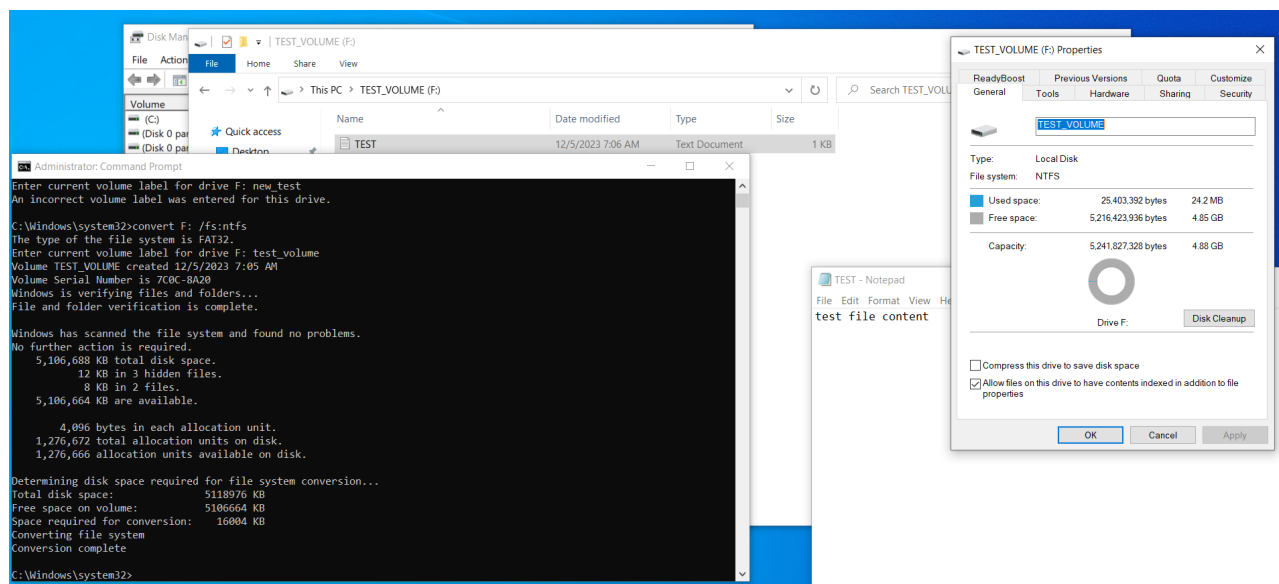
В консоли от имени администратора вводим команду для осуществления форматирования, где F: - метка тома:

```

C:\Windows\system32>convert F: /fs:ntfs
The type of the file system is FAT32.
Enter current volume label for drive F: test_volume
Volume TEST_VOLUME created 12/5/2023 7:05 AM
Volume Serial Number is 7C0C-8A20
Windows is verifying files and folders...
File and folder verification is complete.

```

Форматирование было осуществлено успешно:

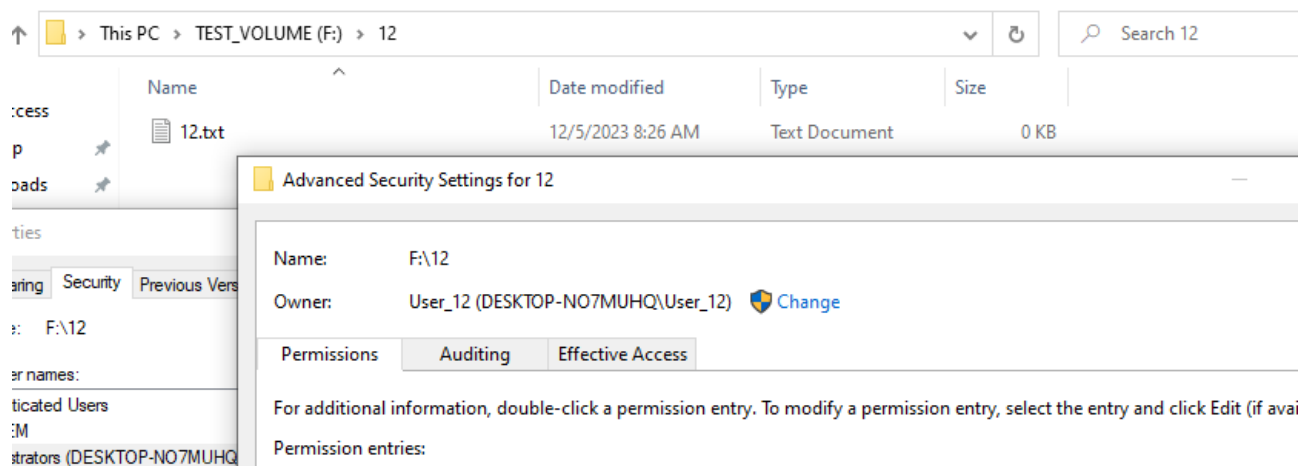


3.1.3. Разрешения на файл

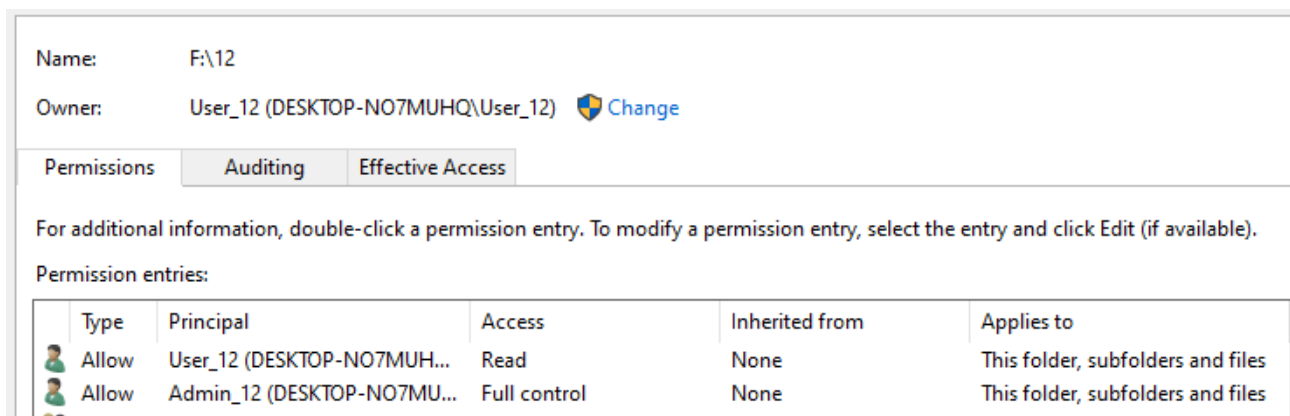
Выполните задание в соответствии с номером варианта, 1 – для нечетных вариантов, 2 – для четных вариантов. Для выполнения задания нужно создать файл с названием «№варианта.txt» и папку «№варианта», в которую поместить созданный файл.

Какие разрешения (права доступа) будут у Пользователя и у Администратора на файл «№варианта.txt», если владельцем 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»)?

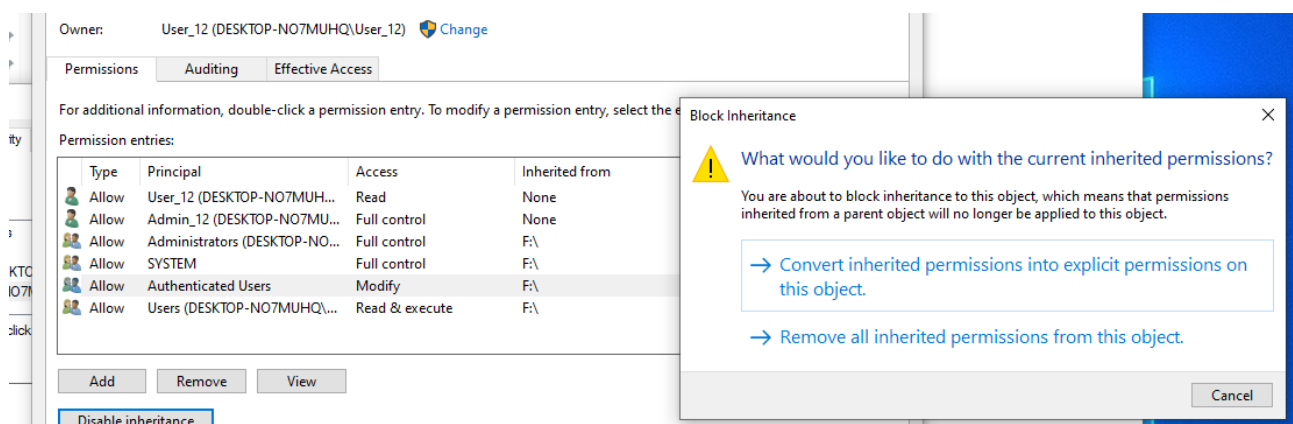
Создаю файл и папку от пользователя User_12:



Установим соответствующие разрешения (для пользователя — чтение, для администратора — полный доступ, для всех — ничего).



Отключаем явное наследование, чтобы избавиться от неявных прав, отнаследованных от вышележащих папок или корня. Нажимаем Convert.



Удаляем все неявно отнаследованные ранее права.

Name: F:\12

Owner: User_12 (DESKTOP-NO7MUHQ\User_12) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	User_12 (DESKTOP-NO7MUH...	Read	None	This folder, subfolders and files
Allow	Admin_12 (DESKTOP-NO7MU...	Full control	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files

Add Remove Edit

Enable inheritance

☐ Replace all child object permission entries with inheritable permission entries from this object

OK Cancel Apply

Таким образом, разрешения для пользователя User_12 для файла:

Advanced Security Settings for 12.txt

Name: F:\12\12.txt.txt

Owner: User_12 (DESKTOP-NO7MUHQ\User_12) [Change](#)

Permissions Auditing Effective Access

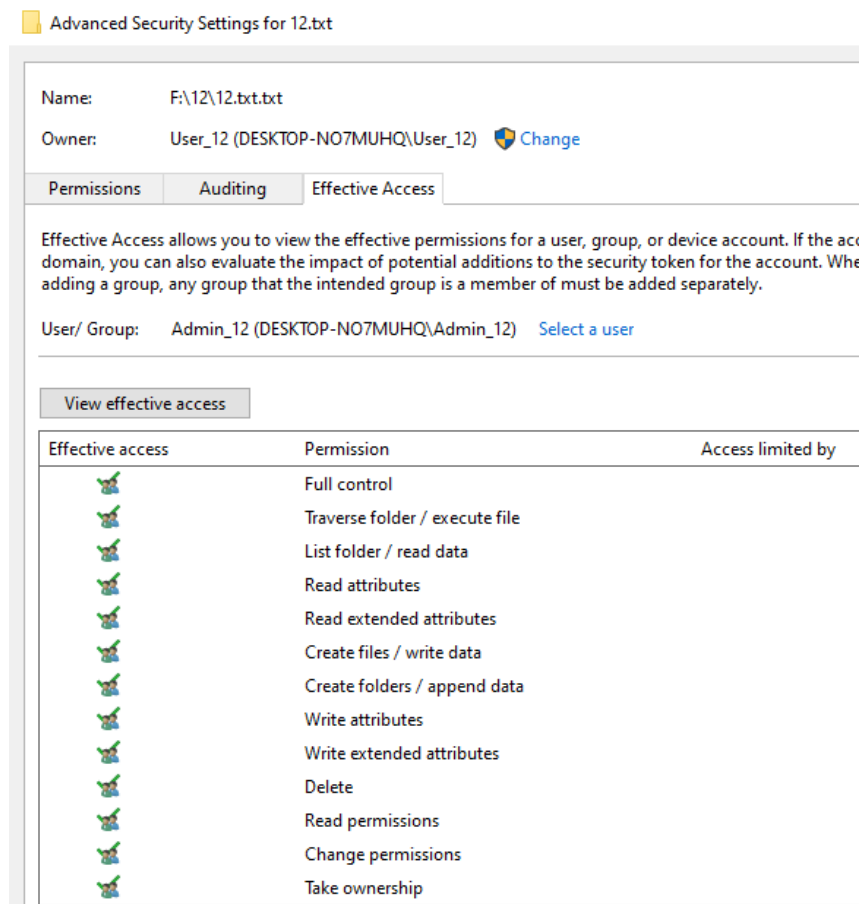
Effective Access allows you to view the effective permissions for a user, group, or device account. If the account domain, you can also evaluate the impact of potential additions to the security token for the account. When you adding a group, any group that the intended group is a member of must be added separately.

User/ Group: User_12 (DESKTOP-NO7MUHQ\User_12) [Select a user](#)

View effective access

Effective access	Permission	Access limited by
✗	Full control	File Permissions
✗	Traverse folder / execute file	File Permissions
	List folder / read data	
	Read attributes	
	Read extended attributes	
✗	Create files / write data	File Permissions
✗	Create folders / append data	File Permissions
✗	Write attributes	File Permissions
✗	Write extended attributes	File Permissions
✗	Delete	File Permissions
	Read permissions	
	Change permissions	
✗	Take ownership	File Permissions

Пользователь может читать и открывать файл, читать какие есть разрешения, однако мне может изменять или запускать файл.



Администратор Admin_12 имеет все разрешения, представоставляемые в пункте расширенных разрешений для файла 12.txt.

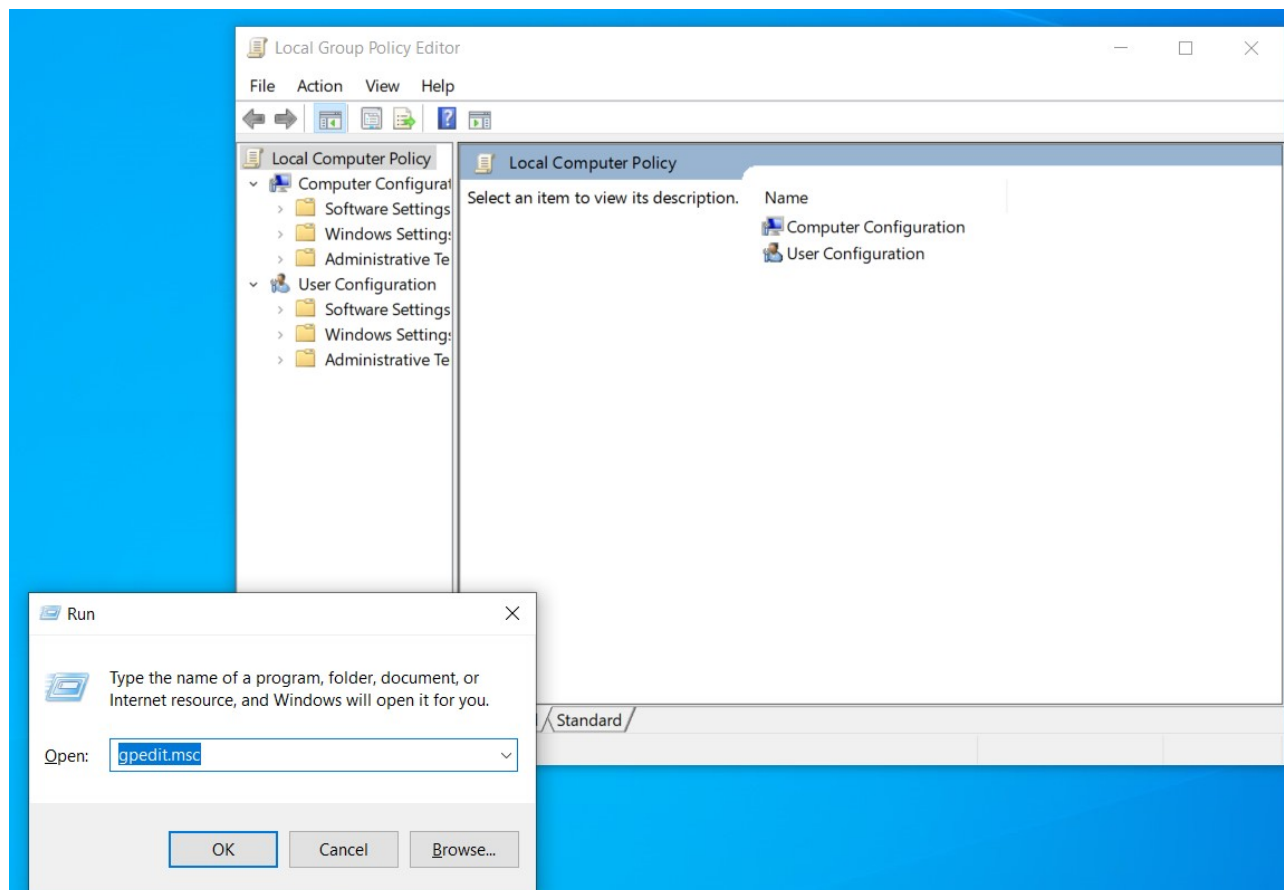
3.1.4. Настройки встроенных механизмов защиты

Выполните задание в соответствии с номером варианта, номер задания соответствует второй цифре номера варианта (например, 40 вариант – 10 задание, 34 вариант – 4 задание и т.п.). Выполните настройки встроенных механизмов защиты ОС Windows в соответствии с заданием.

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

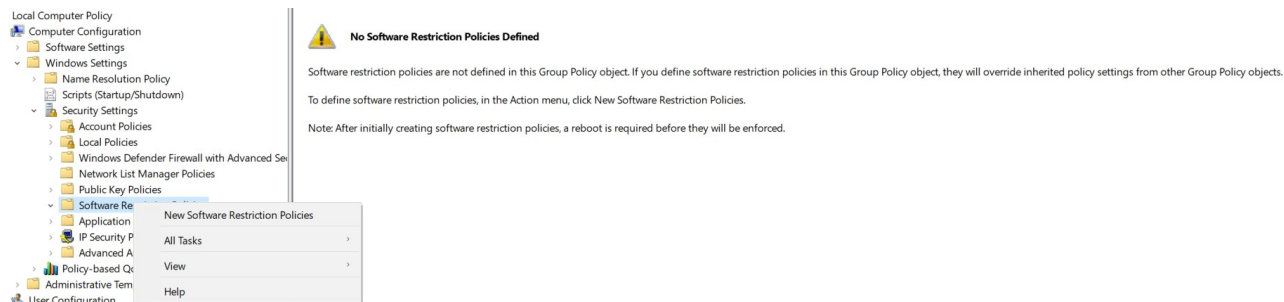
Выполнение данного задания осуществляем при помощи добавления правила в Windows Defender Exploit Guard (редактора локальных групповых политик).

Открываем gpedit.msc

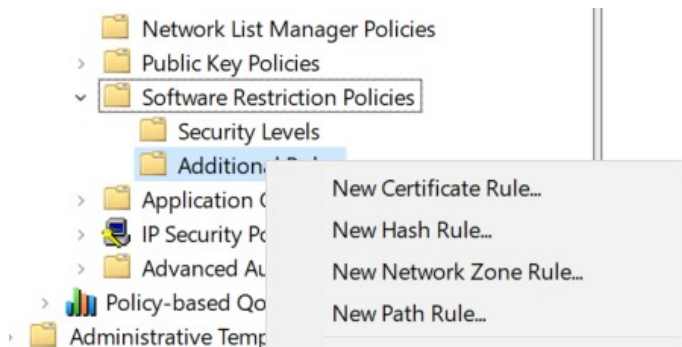


Переходим в политики ограниченного использования программ (Конфигурация компьютера → Конфигурация Windows → Параметры безопасности → Политики ограниченного использования программ).

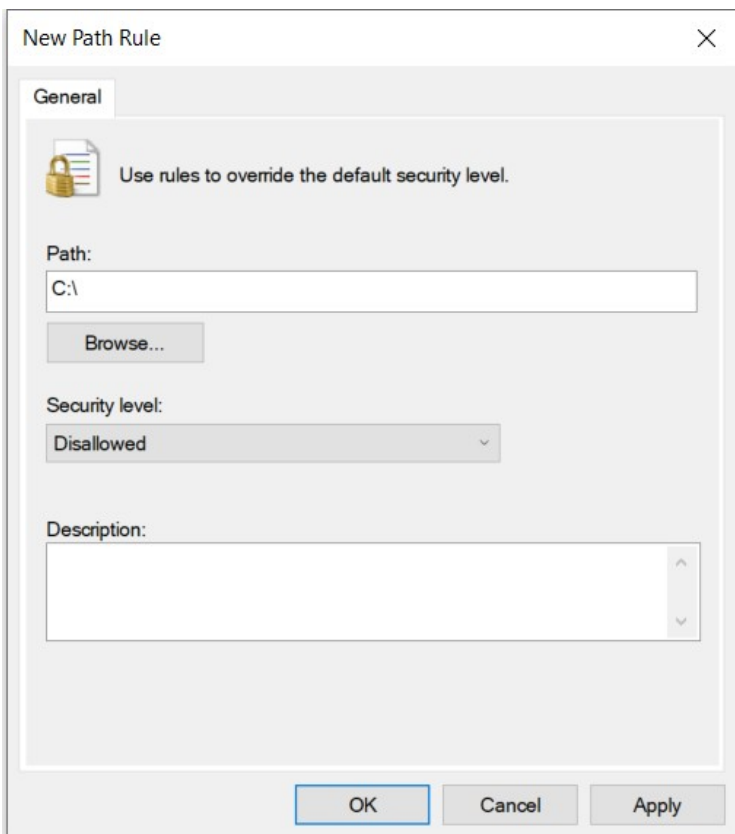
Создаем новую политику:



Создаем правило для пути:



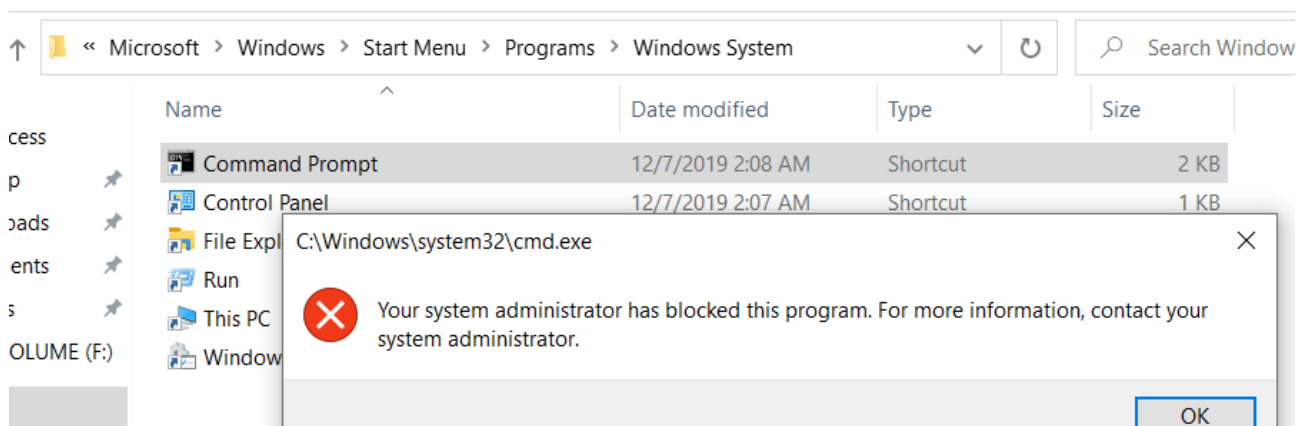
Выставляем уровень безопасности «Запрещено», в качестве системного диска указываем диск C:\. Таким образом, пользователь не сможет запустить программу, которая находится на системном диске.



Политика была добавлена:

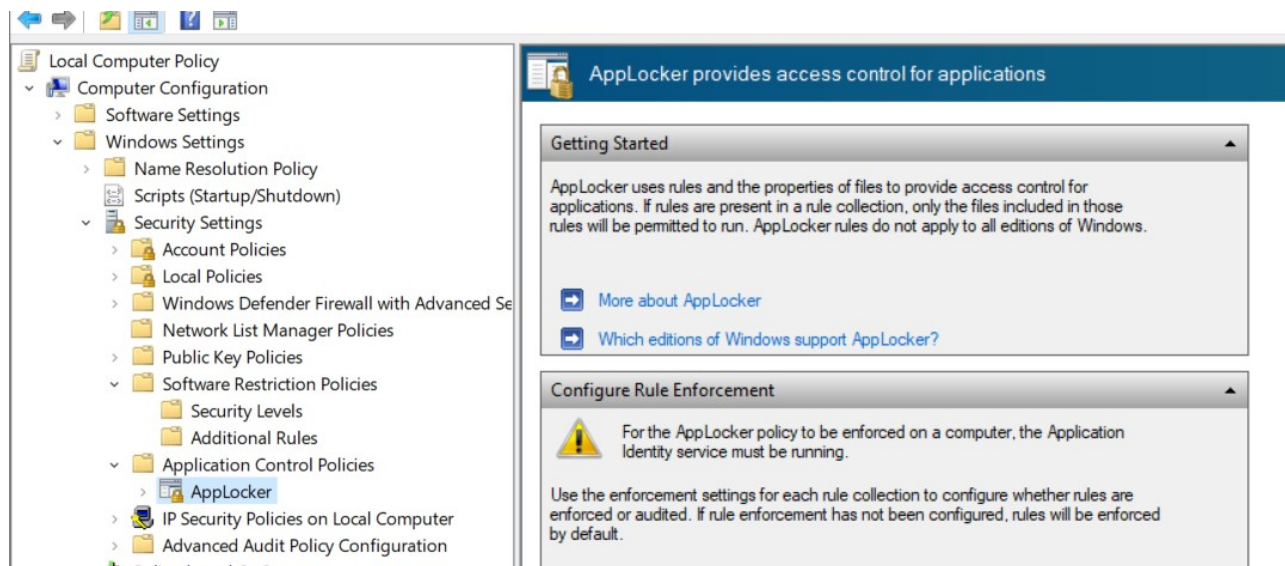
Name	Type	Security Level	Description	Last Modified Date
%HKEY_LOCAL_MACHINE\SOFTWARE\Mic...	Path	Unrestricted		12/5/2023 8:51:56 AM
%HKEY_LOCAL_MACHINE\SOFTWARE\Mic...	Path	Unrestricted		12/5/2023 8:51:56 AM
C:\	Path	Disallowed		12/5/2023 8:56:04 AM

Проверяем, что политика была применена:



Те же самые действия можно было сделать с помощью AppLocker. Он отличается от политик ограниченного использования программ тем, что содержит новые возможности и расширения: создавать правила на основе уникальных удостоверений файлов, а также выбирать пользователей или групп, которым разрешено/запрещено запускать эти приложения.

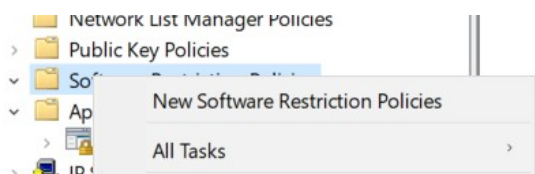
Конфигурация AppLocker находится в локальных политиках безопасности в политиках управления приложениями:



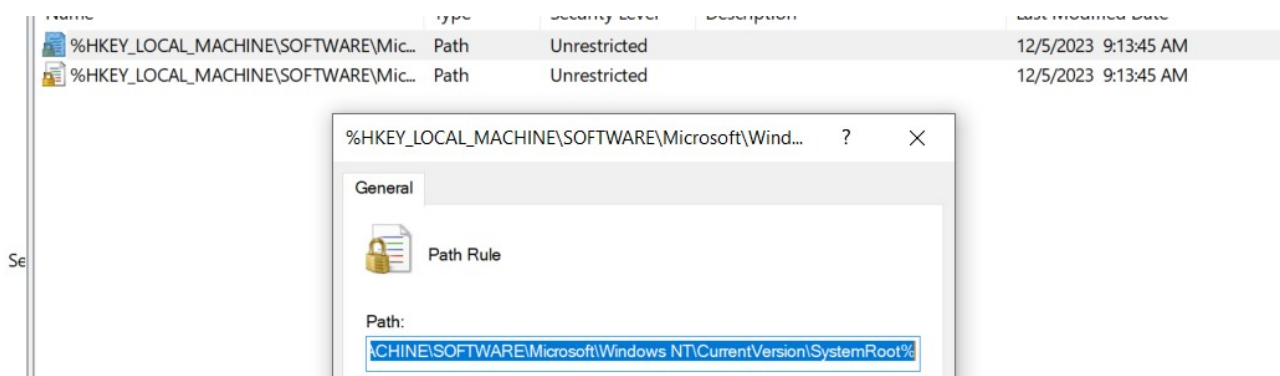
Разрешение средствам ОС на выполнение программ

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

Данные разрешения добавляются автоматически системой Windows при добавлении политик через панель контекстного меню:



После создания в дополнительных правилах появятся требуемые политики:

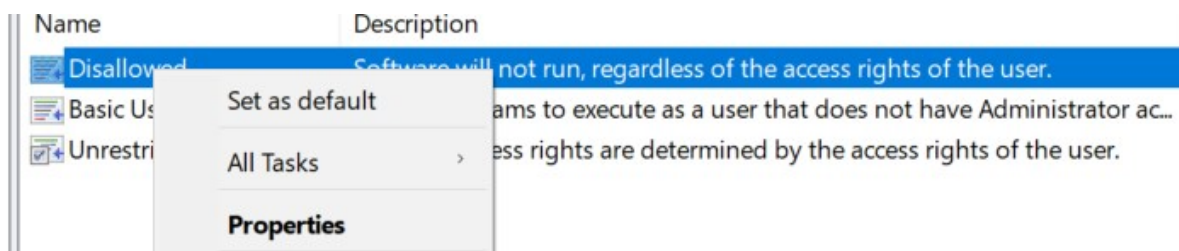


В качестве путей этих политик указано требуемое:

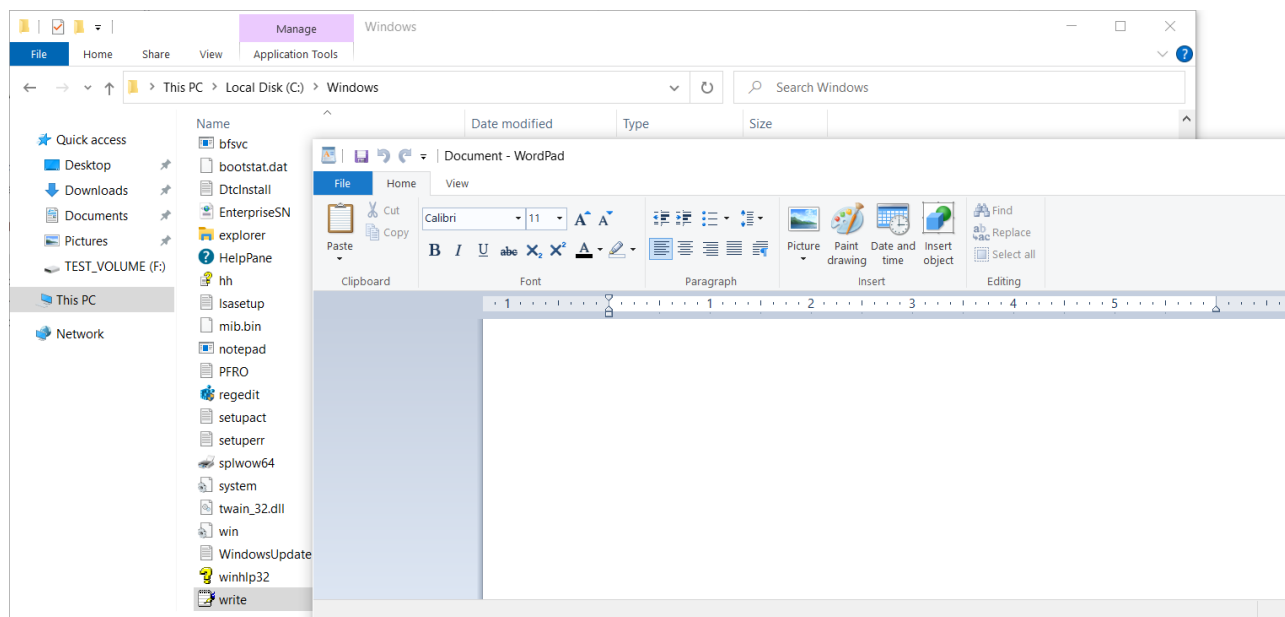
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%
Первое — соответствует C:\Windows, второе — C:\Program Files.

В уровнях безопасности (там же в «Политиках ограниченного использования») требуется указать «Запрещено по умолчанию».

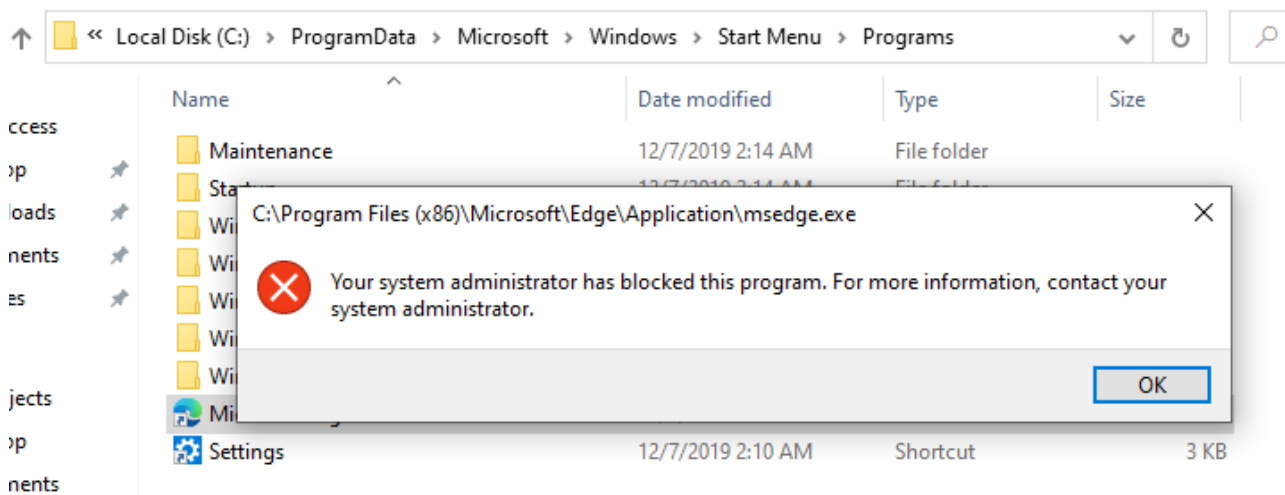
Выбираем «установить по умолчанию»:



Проверяем, что открываются приложения из папок Windows и Program Files:



Проверяем, что не открывается из других мест:



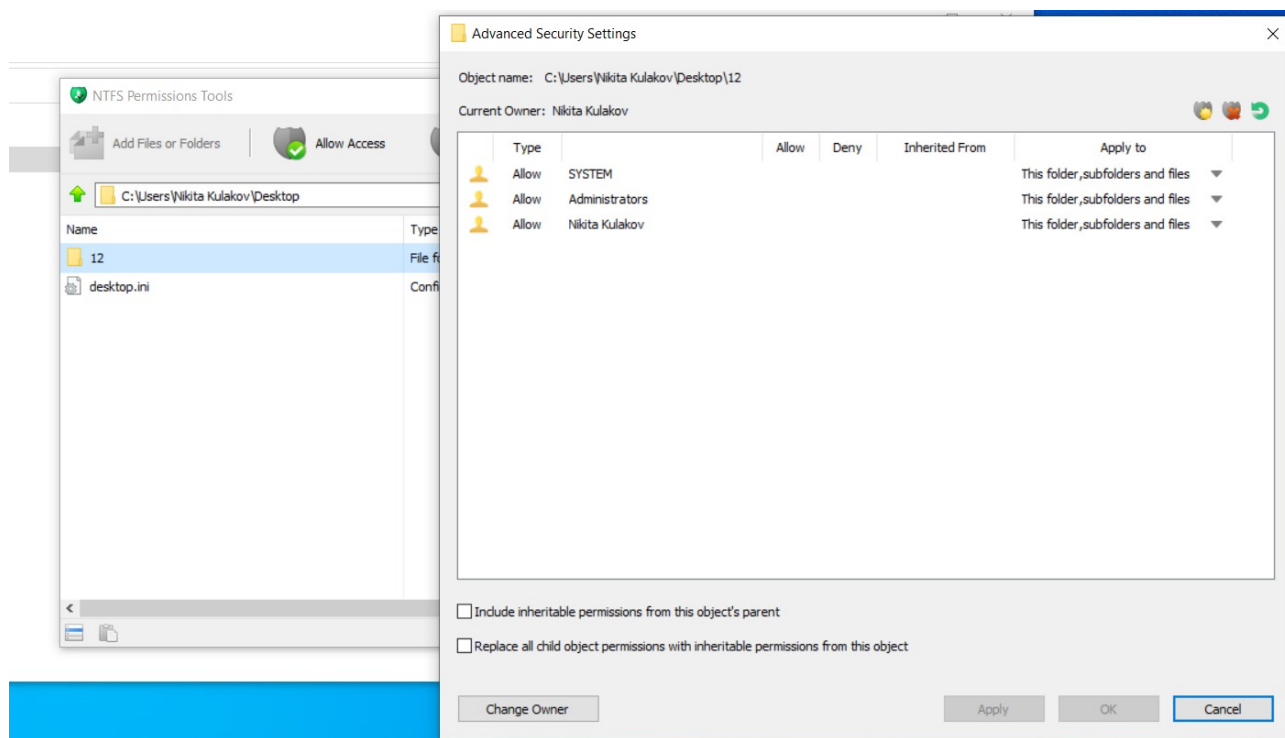
3.2. Дополнительная часть

3.2.1. Работа с разрешениями NTFS дополнительных системных программ сторонних производителей

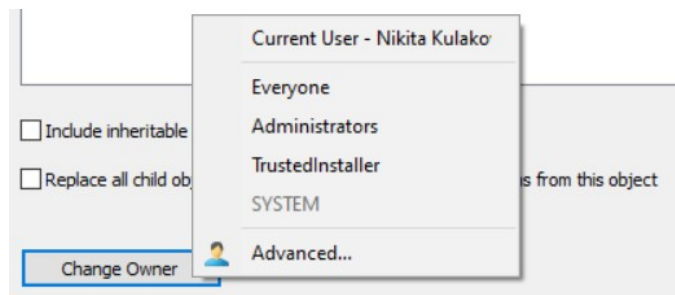
Опишите на примерах работу с разрешениями NTFS дополнительных системных программ сторонних производителей. Приведите перечень подобных программ (не менее пяти).

3.2.1.1. NTFS Permission Tools from MajorGeeks.com

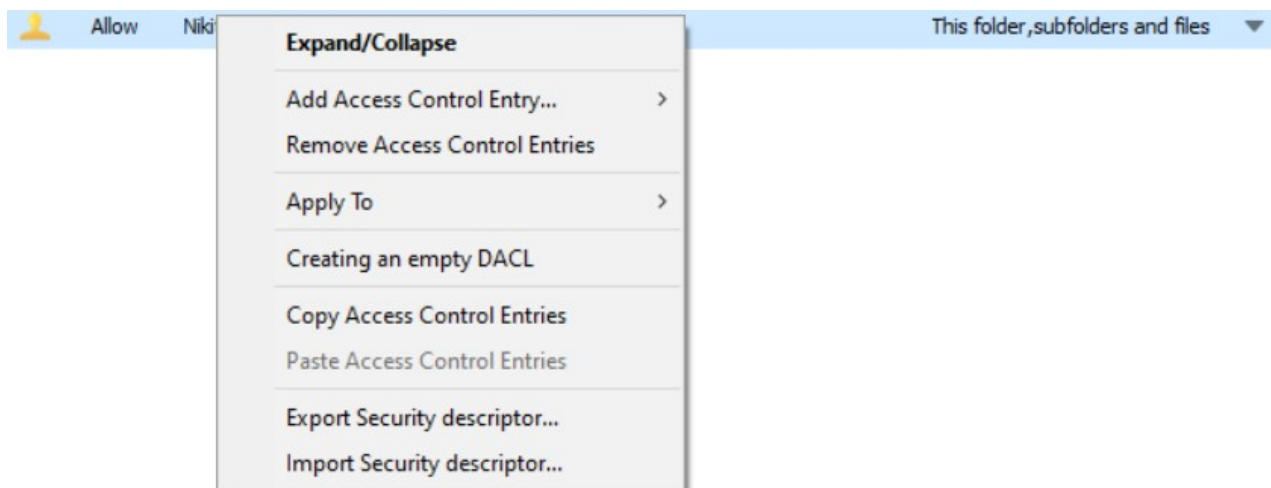
Приложение позволяет управлять правами для файловых систем NTFS. В отличие от встроенного в Windows механизма, данное приложение обладает большей функциональностью, и позволять сделать несколько действий за раз: создавать новые DACL, копировать уже существующие и применять к другим пользователям и т. п. Пример работы с данным представлен ниже.



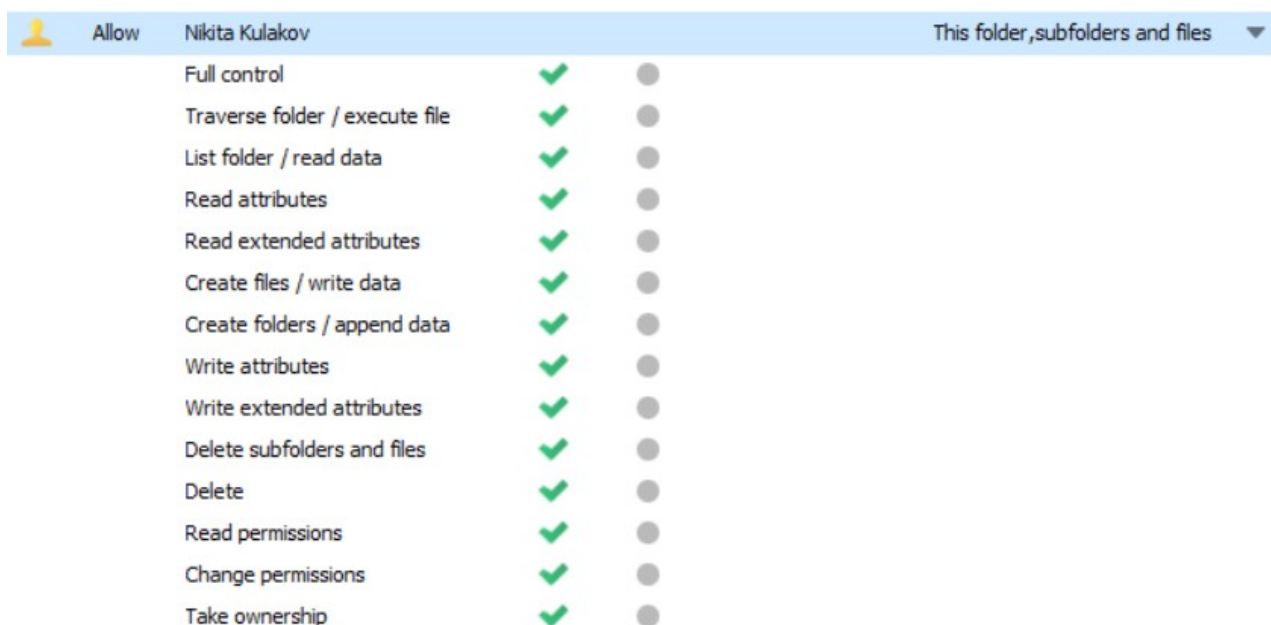
Изменение владельца выглядит следующим образом:




Также присутствует некоторое количество опций, который упрощают администрирование:



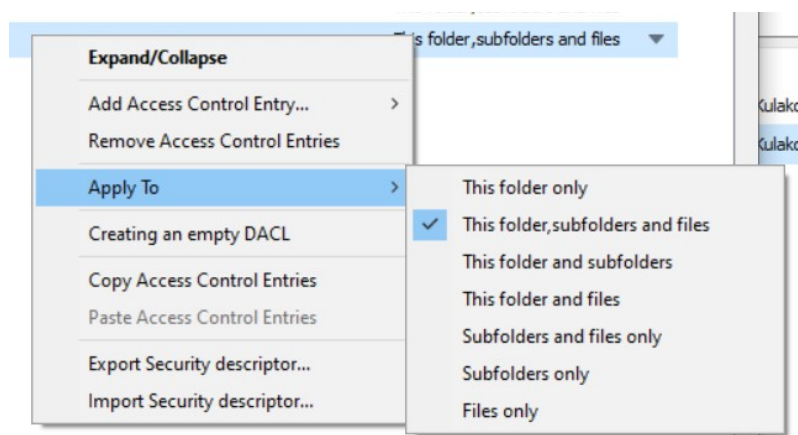
Изменение прав также можно осуществлять через выпадающее меню:



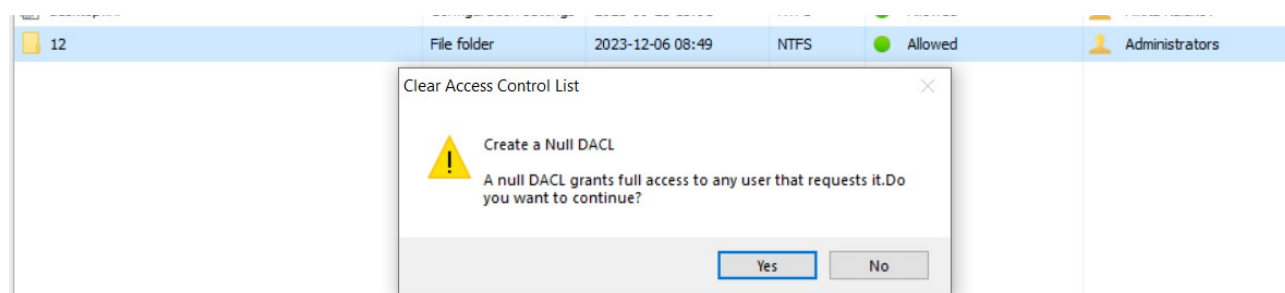
После изменения:

	Allow	Nikita Kulakov	This folder,subfolders and files ▼	
		Full control	<input type="radio"/>	<input type="radio"/>
		Traverse folder / execute file	<input checked="" type="checkbox"/>	<input type="radio"/>
		List folder / read data	<input checked="" type="checkbox"/>	<input type="radio"/>
		Read attributes	<input checked="" type="checkbox"/>	<input type="radio"/>
		Read extended attributes	<input type="radio"/>	<input type="radio"/>
		Create files / write data	<input type="radio"/>	<input type="radio"/>
		Create folders / append data	<input checked="" type="checkbox"/>	<input type="radio"/>
		Write attributes	<input checked="" type="checkbox"/>	<input type="radio"/>
		Write extended attributes	<input checked="" type="checkbox"/>	<input type="radio"/>
		Delete subfolders and files	<input checked="" type="checkbox"/>	<input type="radio"/>
		Delete	<input checked="" type="checkbox"/>	<input type="radio"/>
		Read permissions	<input checked="" type="checkbox"/>	<input type="radio"/>
		Change permissions	<input checked="" type="checkbox"/>	<input type="radio"/>
		Take ownership	<input checked="" type="checkbox"/>	<input type="radio"/>

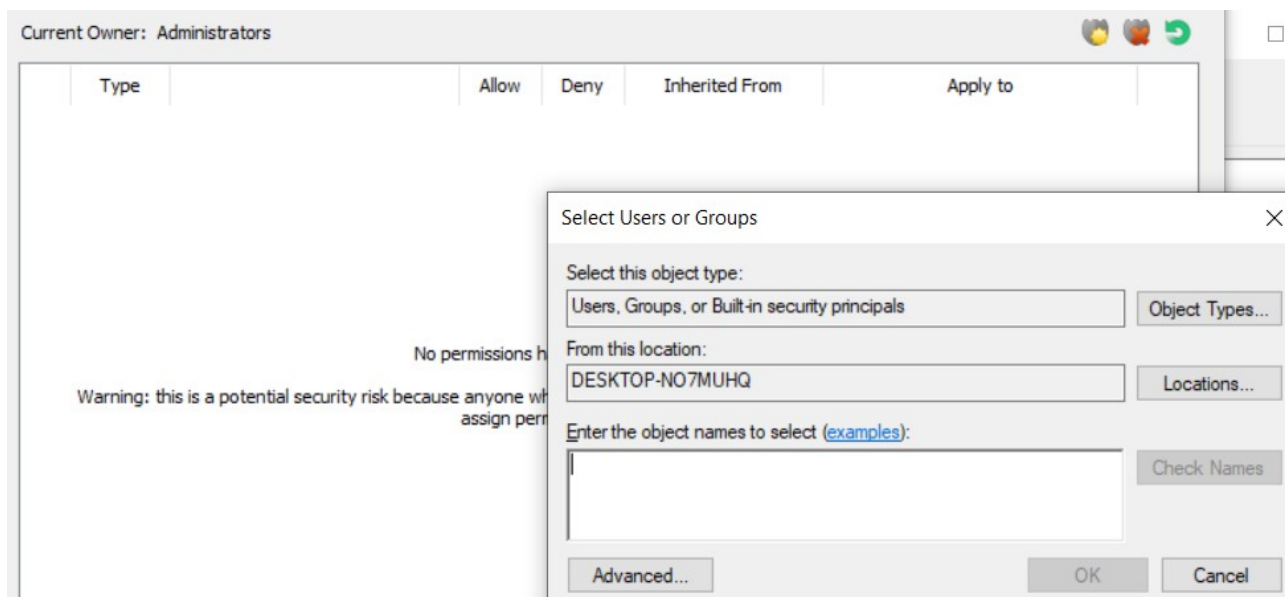
Управление уровнем применения прав для вложенных объектов:



Сброс DACL (в том же контекстном меню):



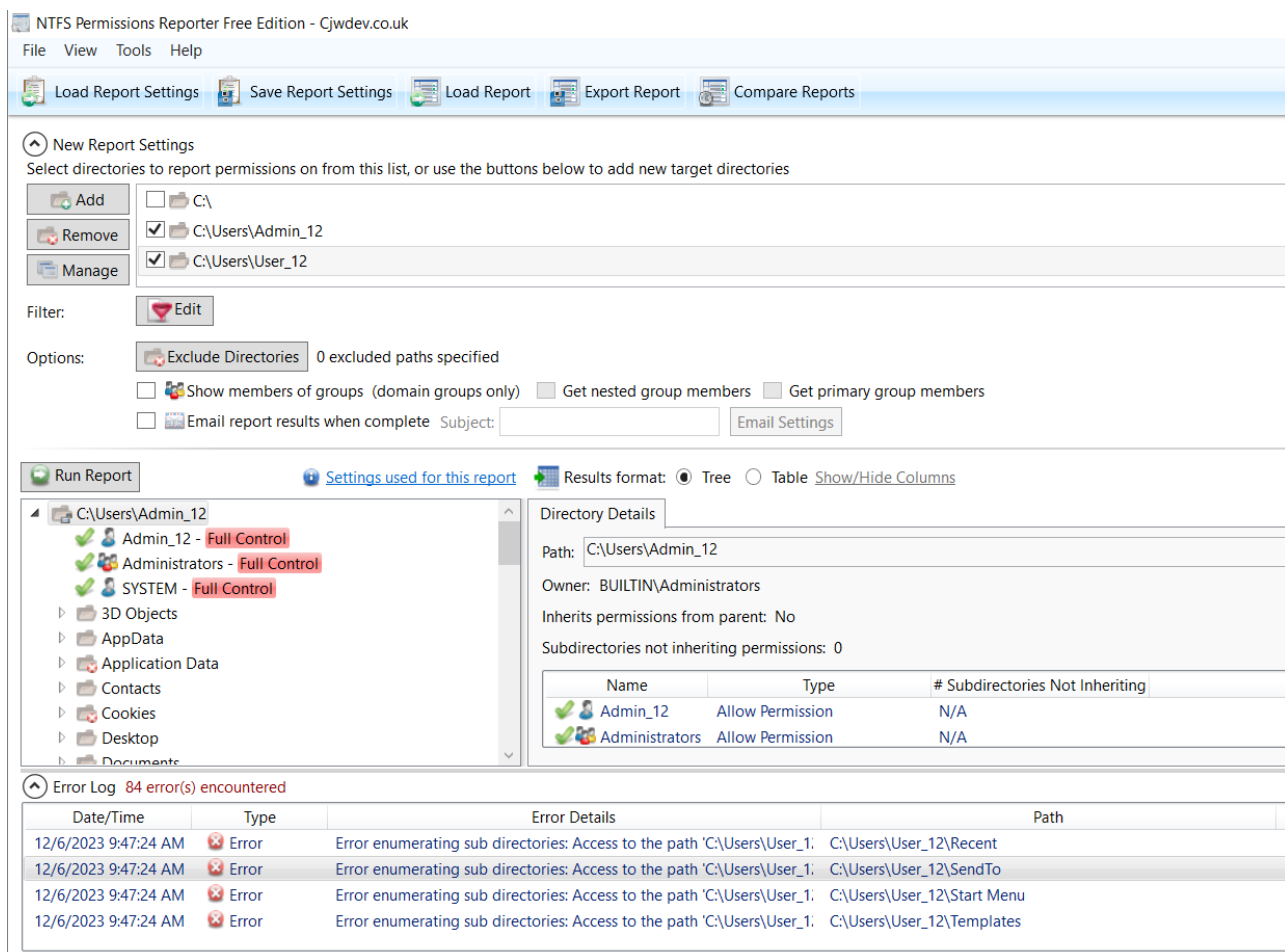
Создание записей DACL:



Также можно осуществлять копирование привилегий из одного файла на второй.

3.2.1.2. NTFS Permission Reporter (Free Edition)

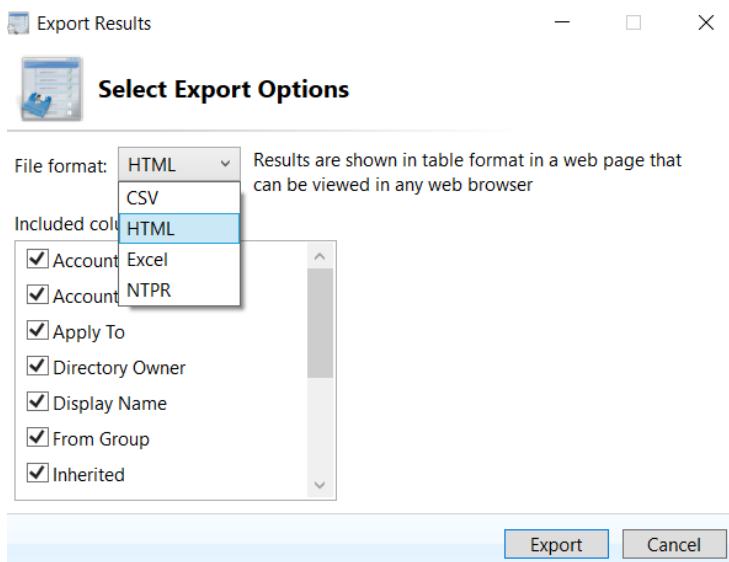
Удобное приложение, позволяющее в формате дерева быстро просматривать разрешения для выбранных папок и файлов. Выбор папок и файлов для просмотра, а также исключения осуществляется в пункте New Report Settings. Программа рекурсивно отрабатывает, и выводит отчет с визуальными дополнениями в виде привилегий для быстрого анализа разрешений в системе.



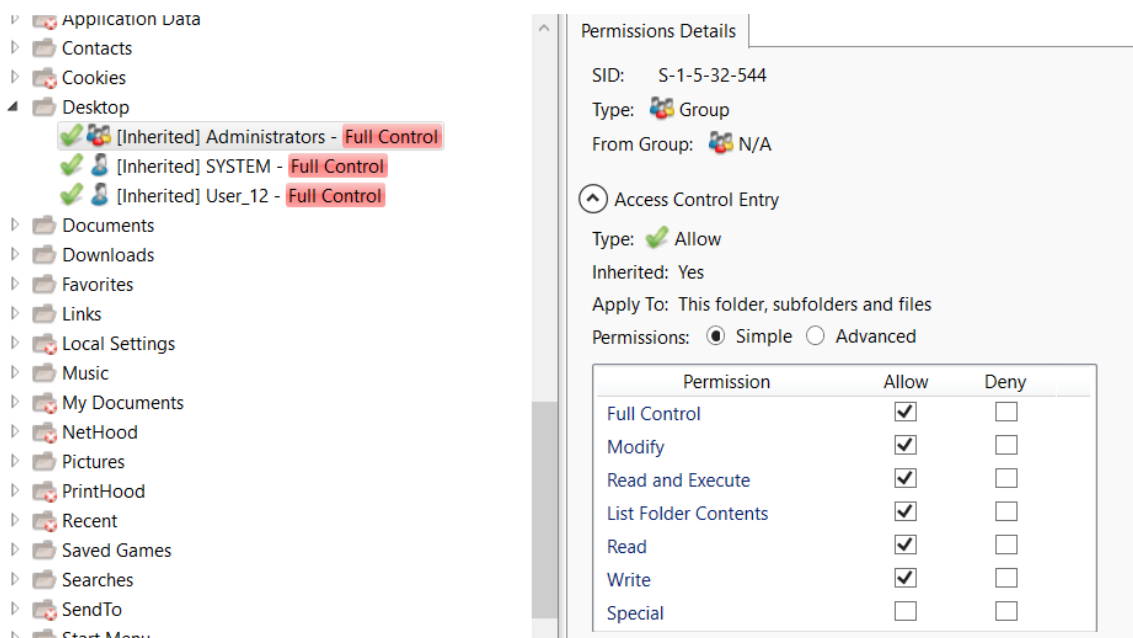
Помимо просмотра в формате дерева приложение позволяет отображать результаты в формате таблицы.

Path	Relative Path	Account Type	Account	Display Name	From Group	Type	Directory Owner	Permission (Simple)	Apply To	Inherited
C:\Users\Admin_12	\	User	NT AUTHORITY\SYSTEM	SYSTEM	N/A	Allow	BUILTIN\Administrators	Full Control	This folder, subfolders and files	No
C:\Users\Admin_12	\	Group	BUILTIN\Administrators	Administrators	N/A	Allow	BUILTIN\Administrators	Full Control	This folder, subfolders and files	No
C:\Users\Admin_12	\	User	DESKTOP-NOTMUHQ\Admin_12	Admin_12	N/A	Allow	BUILTIN\Administrators	Full Control	This folder, subfolders and files	No
C:\Users\Admin_12\3D Objects	\3D Objects	User	NT AUTHORITY\SYSTEM	SYSTEM	N/A	Allow	DESKTOP-NOTMUHQ\Admin_12	Full Control	This folder, subfolders and files	Yes
C:\Users\Admin_12\3D Objects	\3D Objects	Group	BUILTIN\Administrators	Administrators	N/A	Allow	DESKTOP-NOTMUHQ\Admin_12	Full Control	This folder, subfolders and files	Yes
C:\Users\Admin_12\3D Objects	\3D Objects	User	DESKTOP-NOTMUHQ\Admin_12	Admin_12	N/A	Allow	DESKTOP-NOTMUHQ\Admin_12	Full Control	This folder, subfolders and files	Yes
C:\Users\Admin_12\AppData	\AppData	User	NT AUTHORITY\SYSTEM	SYSTEM	N/A	Allow	DESKTOP-NOTMUHQ\Admin_12	Full Control	This folder, subfolders and files	Yes
C:\Users\Admin_12\AppData	\AppData	Group	BUILTIN\Administrators	Administrators	N/A	Allow	DESKTOP-NOTMUHQ\Admin_12	Full Control	This folder, subfolders and files	Yes

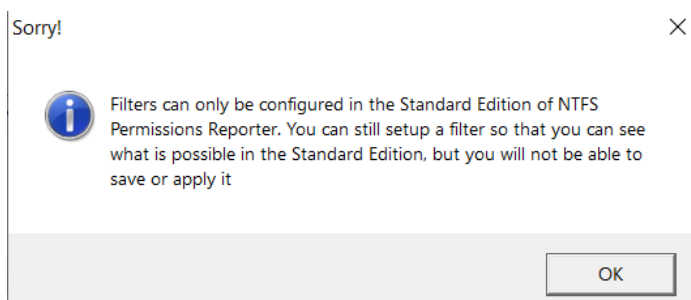
Кроме того, приложение позволяет сохранять текущую конфигурацию, а также загружать другие с помощью кнопок Save Report Settings и Load Report Settings, а также сохранять сами результаты и загружать для просмотра (Export Report и Load Report) в различных форматах:



Также программа позволяет внутри выдавать определенные разрешения:

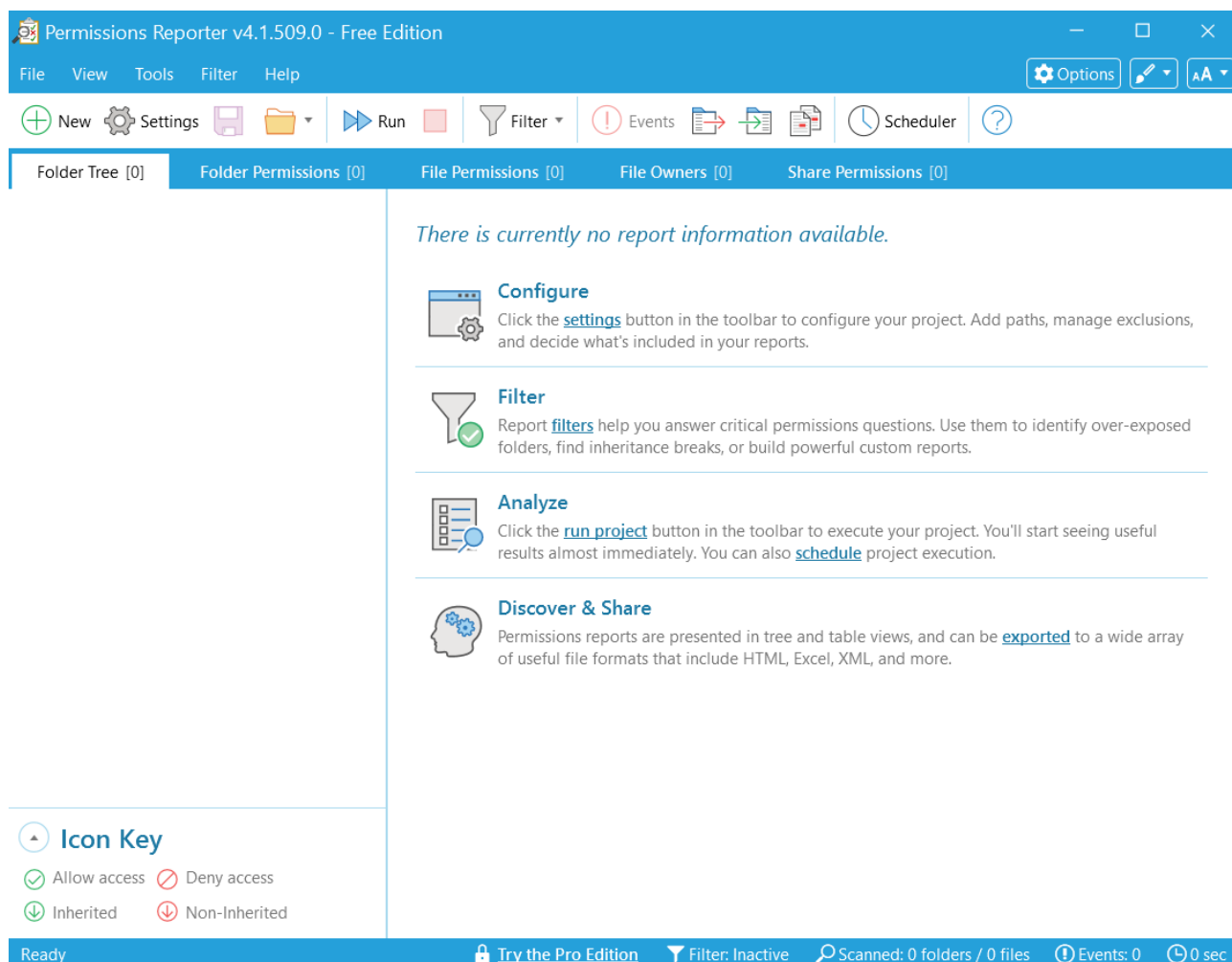


Работа с фильтрами доступна только в платной версии приложения (их невозможно применить, а только создать):

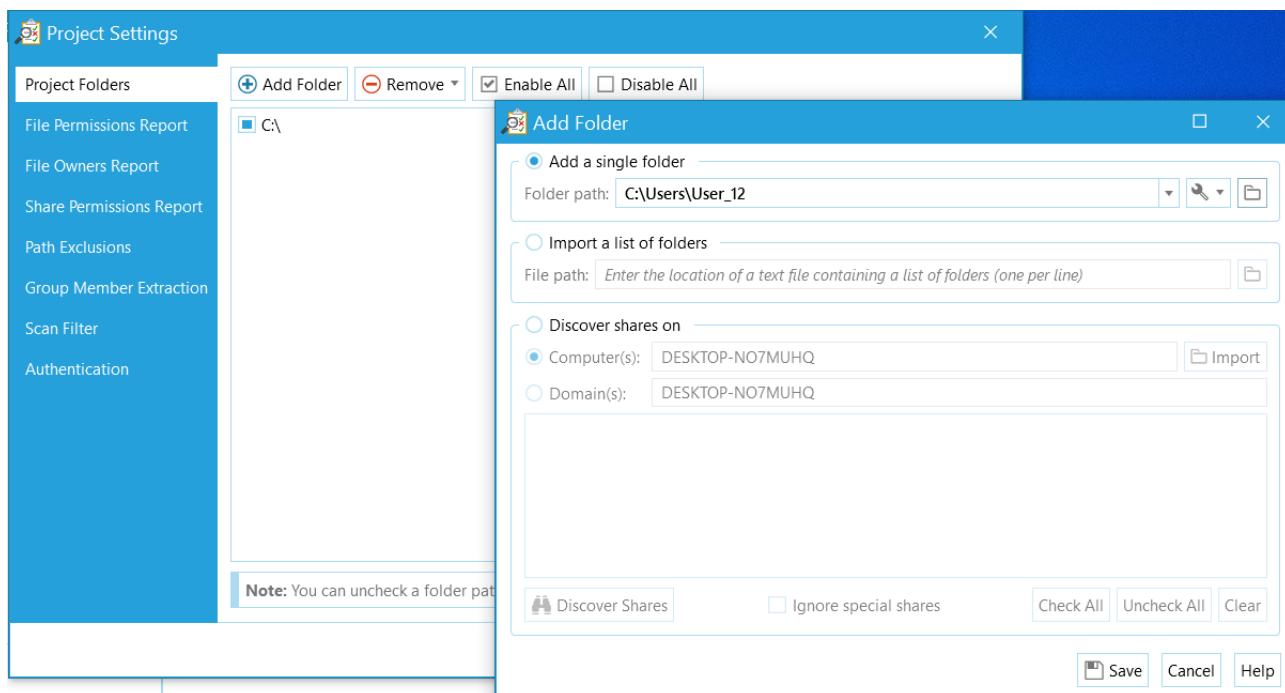


3.2.1.3. Permissions Reporter (Key Metric Software)

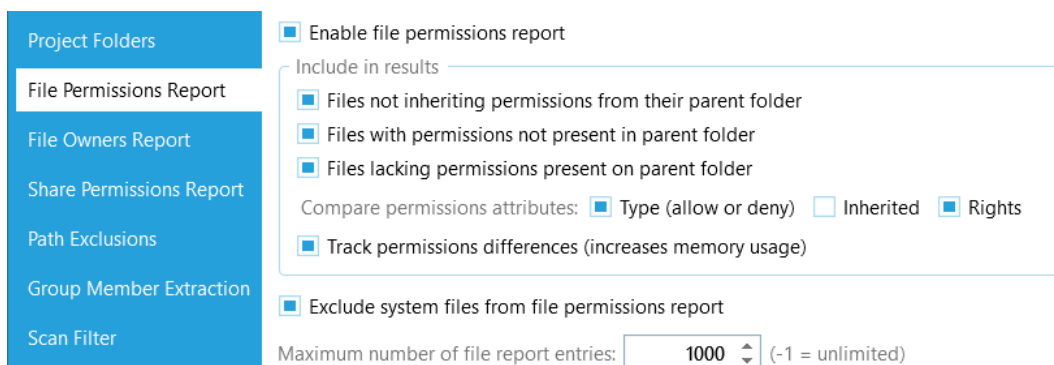
Приложение Permissions Reporter имеет схожий функционал с NTFS Permission Reporter, но обладает более приятным интерфейсом и возможностью интерактивной настройки проекта.



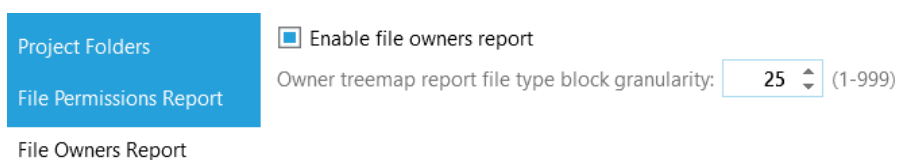
В первую очередь необходимо создать проект, добавляем проектные папки:



На вкладке File Permission Report можно настроить параметры для отчета. Ограничу размер отчета в 1000 записей. Помимо можно настроить то, какие записи будут включены в отчет: те, кто не наследует права от родительской папки, наоборот и т. п. Также можно отслеживать разрешения.



В следующей вкладке можно включить отчет по владельцам:



Настройка по общему доступу:

Project Folders
File Permissions Report
File Owners Report
Share Permissions Report
Path Exclusions
Group Member Extraction
Scan Filter
Authentication

Include in share permissions report

☐ Report no share information (share permissions report is disabled)
☒ Report all shares for each host name contained within project folders
☐ Report only on share paths explicitly contained within project folders
☐ Report on shares on these hosts:

☐ Report on shares in these domains:

Options

☐ Use WMI (Windows Management Instrumentation) to enumerate shares

Note: The permissions on administrative shares (such as "\\server\C\$") cannot change, so they are not reported by this program.

Также можно настроить, какие пути включать, а какие нет с помощью Path Exclusions:

Project Folders
File Permissions Report
File Owners Report
Share Permissions Report
Path Exclusions
Group Member Extraction
Scan Filter

+ Add Exclusion
- Remove Selected
Edit Exclusion

Edit Path Exclusion

☒ Exclude full path:
☐ Exclude folders named:

Match type: Is equal to

Save
Cancel
Help

Следующее позволяет получить по группе список членов, включу:

Project Folders
File Permissions Report
File Owners Report
Share Permissions Report
Path Exclusions
Group Member Extraction

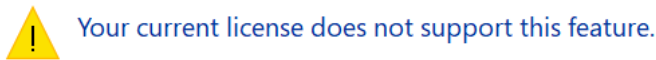
☒ Extract group members (allows groups to be expanded in folder tree)
☐ Extract nested group members

Excluded groups (members will not be extracted)

+ Add Exclusion
- Remove Selected
☒ Enable All
☐ Disable All

Следующие две вкладки доступны только для платной версии:

27



Your current license does not support this feature.

Filtering is not available in the Free edition of this program. Please upgrade your license (or start a free trial) to enable this feature.

START A FREE PRO EDITION TRIAL

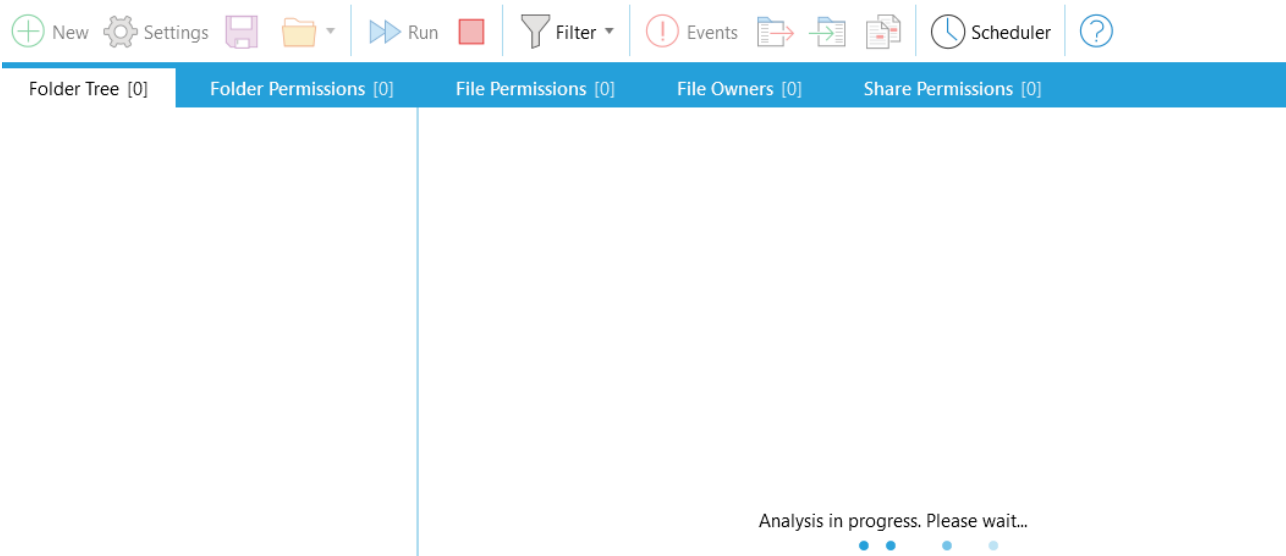
Upgrade Now

Close

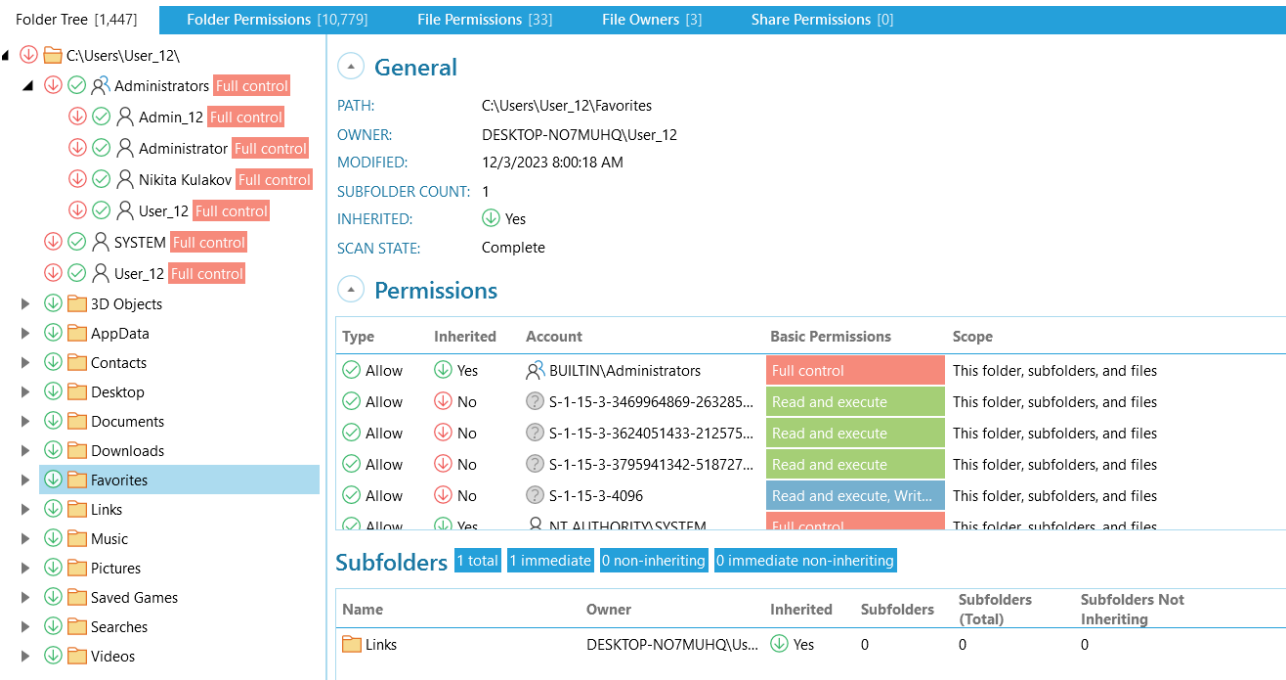


[Learn about upgrade licensing options](#)

Далее нажимаем на кнопку Run, и программа покажет сводку по проекту:



Сводка всего проекта со списком пользователей в группах:



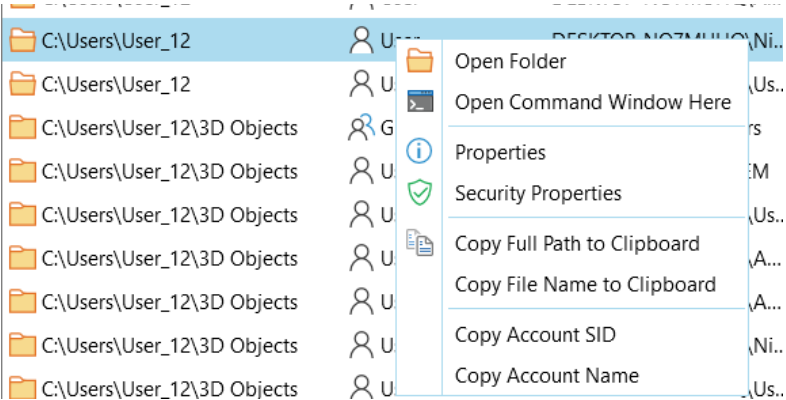
На верхней панели можно посмотреть на разрешения для папок, для файлов, и на владельцев:

Path	Account Type	Account	Type	Inherited	SID	Parent Group	Owner	Basic Permissions	Scope	Advanced Permission
C:\Users\User_12	Group	BUILTIN\Administrators	Allow	No	S-1-5-32-544	[None]	BUILTIN\Administrators	Full control	This folder, subfolders, a...	Full control, Traverse f
C:\Users\User_12	User	NT AUTHORITY\SYSTEM	Allow	No	S-1-5-18	[None]	BUILTIN\Administrators	Full control	This folder, subfolders, a...	Full control, Traverse f
C:\Users\User_12	User	DESKTOP-NO7MUHQ\Us...	Allow	No	S-1-5-21-712644886-29...	[None]	BUILTIN\Administrators	Full control	This folder, subfolders, a...	Full control, Traverse f
C:\Users\User_12	User	DESKTOP-NO7MUHQ\A...	Allow	No	S-1-5-21-712644886-29...	BUILTIN\Administrators	BUILTIN\Administrators	Full control	This folder, subfolders, a...	Full control, Traverse f
C:\Users\User_12	User	DESKTOP-NO7MUHQ\A...	Allow	No	S-1-5-21-712644886-29...	BUILTIN\Administrators	BUILTIN\Administrators	Full control	This folder, subfolders, a...	Full control, Traverse f
C:\Users\User_12	User	DESKTOP-NO7MUHQ\Ni...	Allow	No	S-1-5-21-712644886-29...	BUILTIN\Administrators	BUILTIN\Administrators	Full control	This folder, subfolders, a...	Full control, Traverse f
C:\Users\User_12	User	DESKTOP-NO7MUHQ\Us...	Allow	No	S-1-5-21-712644886-29...	BUILTIN\Administrators	BUILTIN\Administrators	Full control	This folder, subfolders, a...	Full control, Traverse f
C:\Users\User_12\3D Objects	Group	BUILTIN\Administrators	Allow	Yes	S-1-5-32-544	[None]	DESKTOP-NO7MUHQ\Us...	Full control	This folder, subfolders, a...	Full control, Traverse f
C:\Users\User_12\3D Objects	User	NT AUTHORITY\SYSTEM	Allow	Yes	S-1-5-18	[None]	DESKTOP-NO7MUHQ\Us...	Full control	This folder, subfolders, a...	Full control, Traverse f
C:\Users\User_12\3D Objects	User	DESKTOP-NO7MUHQ\Us...	Allow	Yes	S-1-5-21-712644886-29...	[None]	DESKTOP-NO7MUHQ\Us...	Full control	This folder, subfolders, a...	Full control, Traverse f
C:\Users\User_12\3D Objects	User	DESKTOP-NO7MUHQ\A...	Allow	Yes	S-1-5-21-712644886-29...	BUILTIN\Administrators	DESKTOP-NO7MUHQ\Us...	Full control	This folder, subfolders, a...	Full control, Traverse f

	Path	Inherited	Owner	Modified	Inclusion Reason
+	C:\Users\User_12\AppData\Local\Temp...	Yes	DESKTOP-NO7MUHQ\Us...	12/3/2023 8:20:03 AM	1 permissions difference(s)
+	C:\Users\User_12\AppData\Local\Temp...	Yes	DESKTOP-NO7MUHQ\Us...	12/3/2023 9:29:09 AM	1 permissions difference(s)
+	C:\Users\User_12\AppData\Local\Micro...	Yes	DESKTOP-NO7MUHQ\Us...	12/3/2023 8:20:03 AM	1 permissions difference(s)
+	C:\Users\User_12\AppData\Local\Micro...	Yes	DESKTOP-NO7MUHQ\Us...	12/3/2023 8:30:01 AM	1 permissions difference(s)
+	C:\Users\User_12\AppData\Local\Micro...	Yes	DESKTOP-NO7MUHQ\Us...	12/5/2023 3:53:16 AM	1 permissions difference(s)
+	C:\Users\User_12\AppData\Local\Micro...	Yes	DESKTOP-NO7MUHQ\Us...	12/3/2023 8:19:42 AM	1 permissions difference(s)
+	C:\Users\User_12\AppData\Local\Micro...	Yes	DESKTOP-NO7MUHQ\Us...	12/5/2023 3:53:16 AM	1 permissions difference(s)
+	C:\Users\User_12\AppData\Local\Micro...	Yes	DESKTOP-NO7MUHQ\Us...	12/5/2023 3:46:11 AM	1 permissions difference(s)
+	C:\Users\User_12\AppData\Local\Micro...	Yes	DESKTOP-NO7MUHQ\Us...	12/3/2023 8:30:01 AM	1 permissions difference(s)

NT AUTHORITY\SYSTEM	2.00 MB	4
DESKTOP-NO7MUHQ\User_12	260 MB	1,757
BUILTIN\Administrators	281 KB	7

Для каждого файла и папки существует контекстное меню:

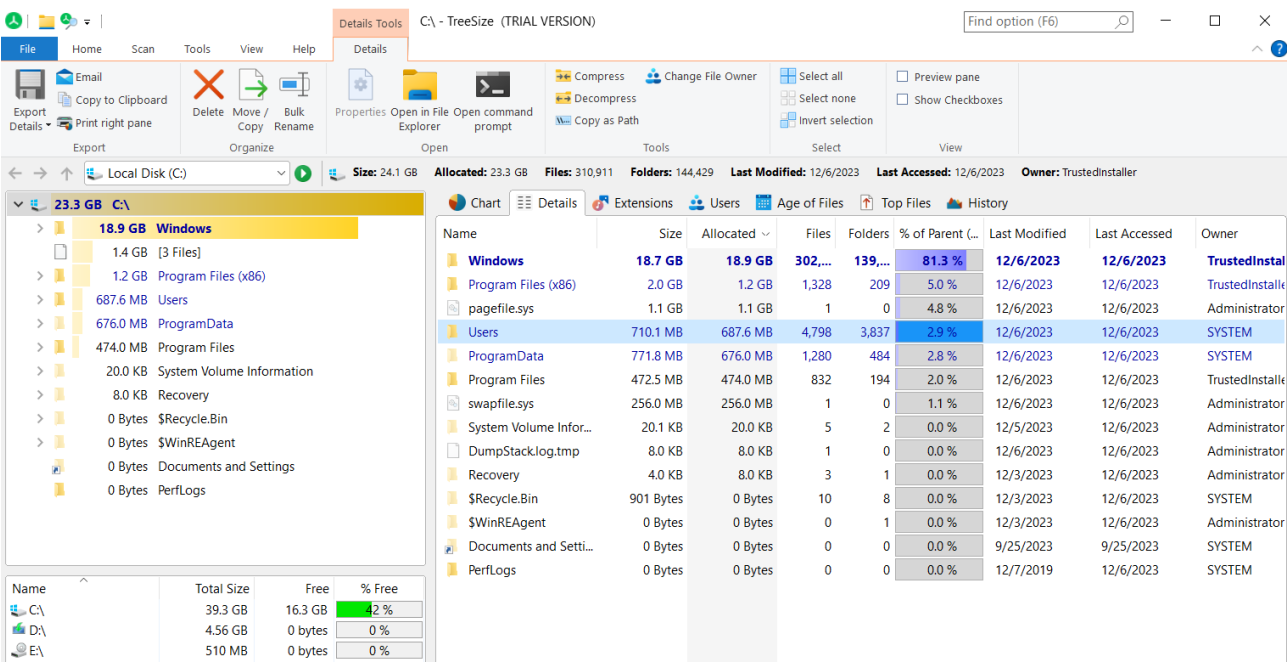


Просмотр разрешений перебрасывает на нативное окно Windows с разрешениями.

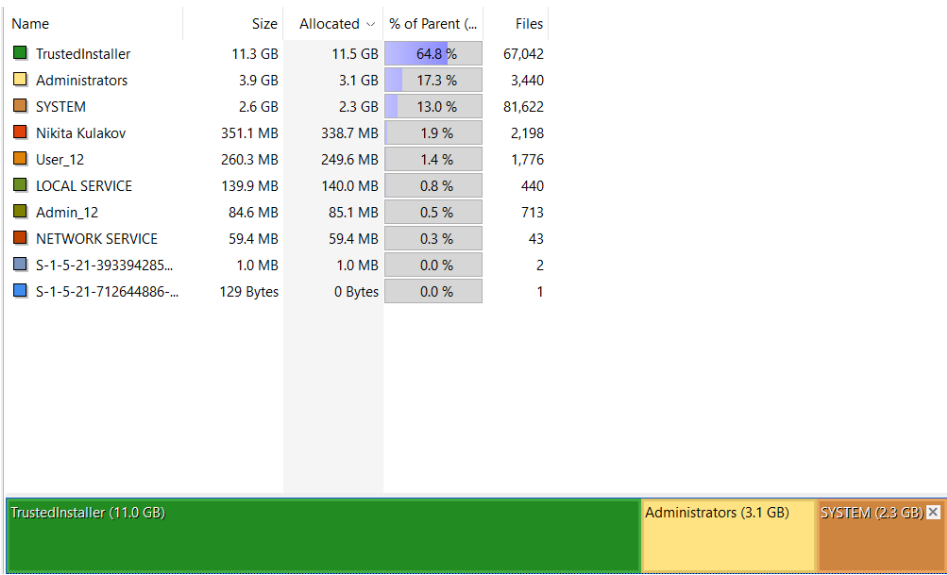
Также можно сохранить и экспортировать данные, а также загрузить (на панели File).

3.2.1.4. TreeSize (Jam Software’s)

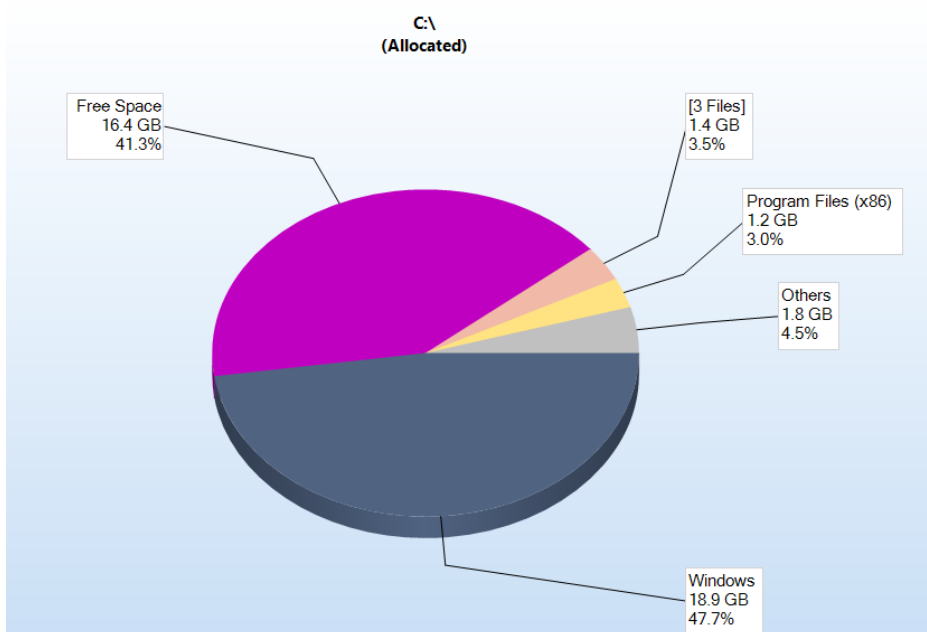
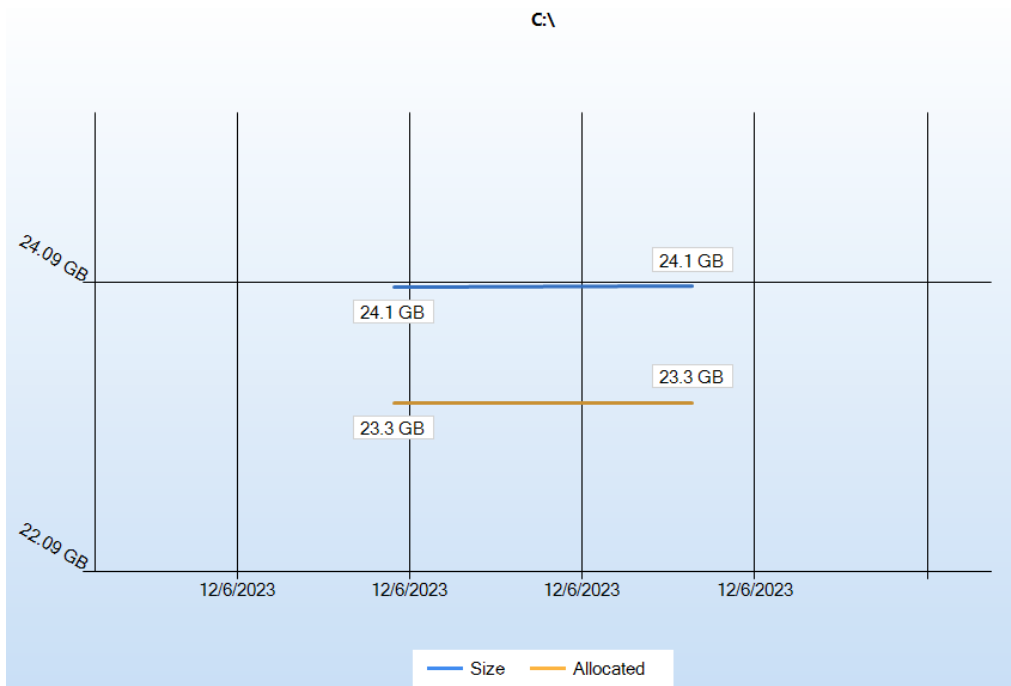
Для демонстрации использовался пробный период Professional версии данного приложения. Основным направлением данного приложения является анализ файловой системы, однако приложение позволяет проанализировать владельцев файлов, времена изменения и т. п. Программа работает достаточно быстро по сравнению с ранее использованными программами.



Также программа позволяет проанализировать, каким образом распределена память между пользователя:

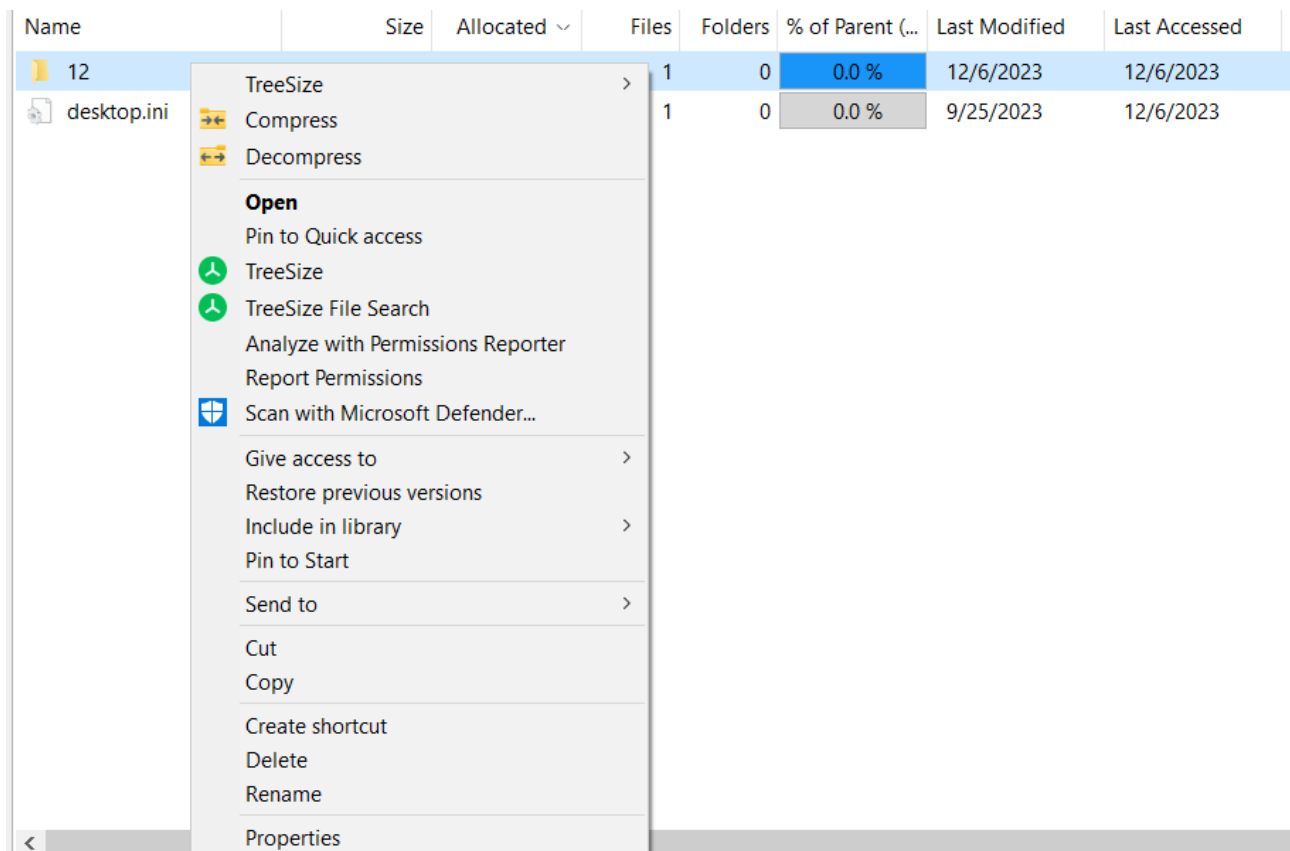


Также можно посмотреть, каким образом изменялась загрузка дисковых пространств, а также как распределено это пространство:

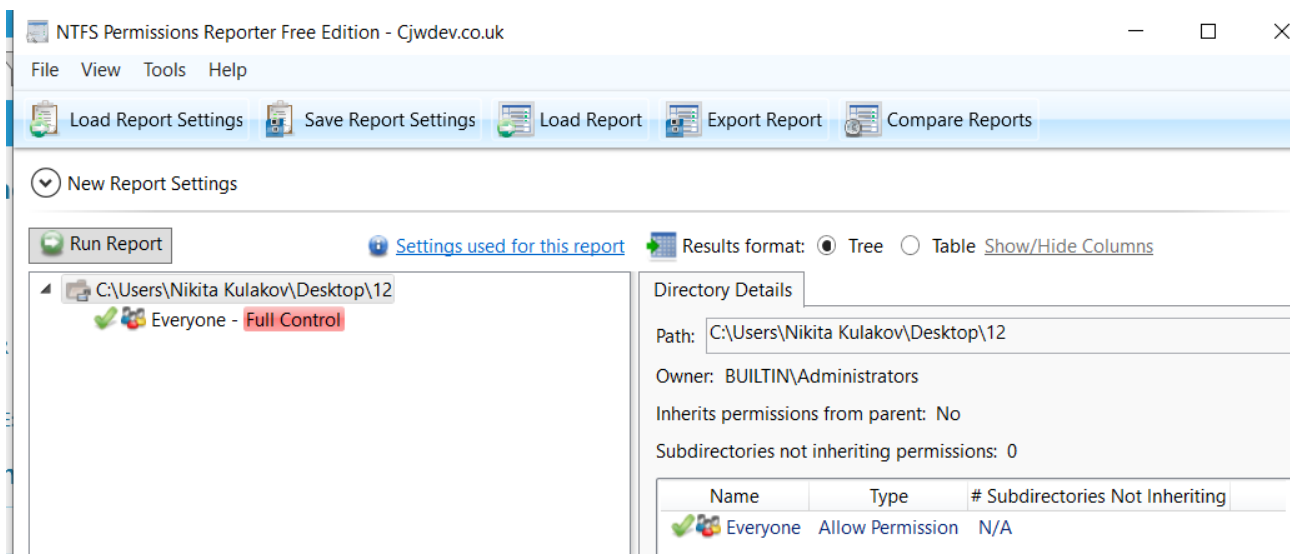


Программа интегрирована с NTFS Permissions Reporter, и позволяет использовать эти два приложения совместно. Через контекстное меню можно открыть данную папку или файл через NTFS Permissions Reporter для того,

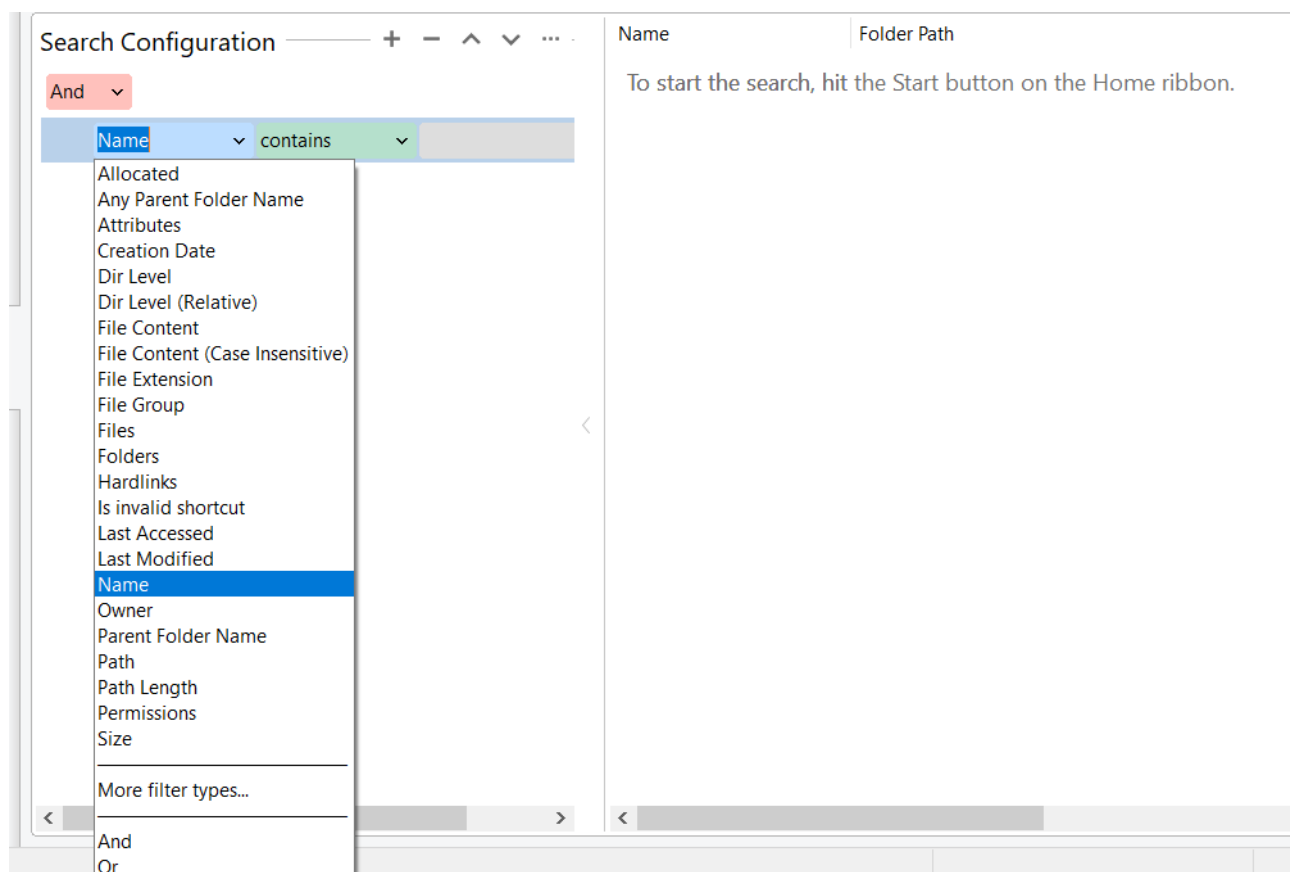
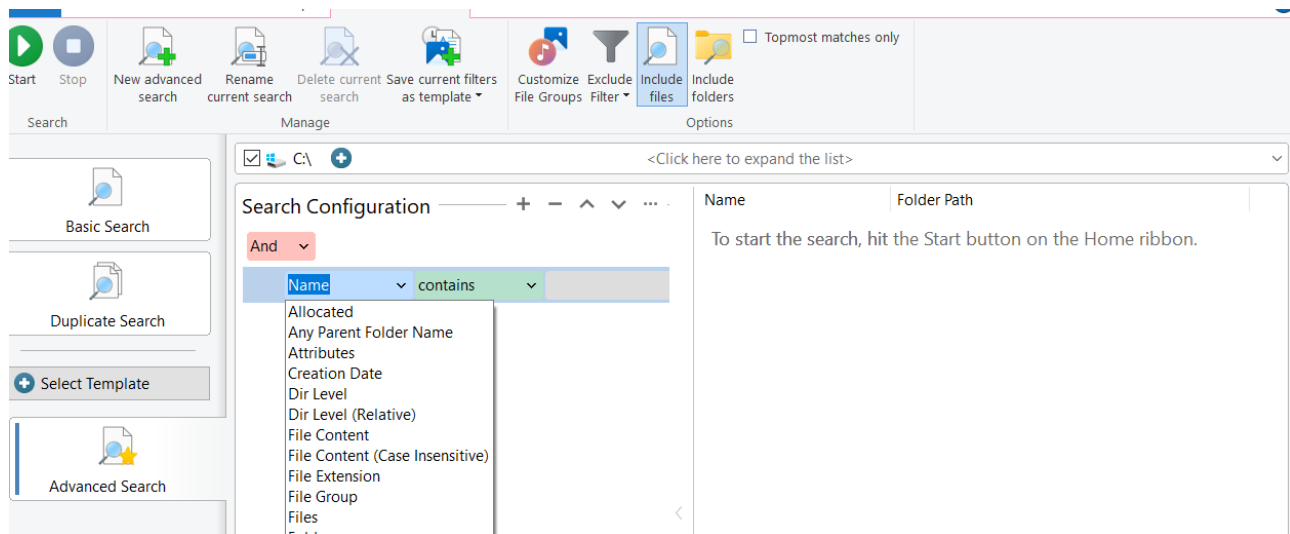
чтобы уже там выполнить необходимые действия, чтобы не дублировать функциональность.



При нажатии на **Analyze with Permissions Reporter** программа открывает соответствующее приложение:



Кроме того в комплекс данных программ входит File Search, с помощью которого можно отфильтровать файлы по многочисленным параметрам, в том числе и по разрешениям:



And ▾

Permissions ▾ Access denied ▾ User_12: []

To start the search, hit the Start button on the Home ribbon.

User name or group:

User_12 ▾

Select Permissions:

<input type="checkbox"/> Full control	<input type="checkbox"/> Read attributes
<input type="checkbox"/> List folder / read data	<input type="checkbox"/> Write attributes
<input type="checkbox"/> Create files / write data	<input type="checkbox"/> Delete
<input type="checkbox"/> Create folders / append data	<input type="checkbox"/> Read permissions
<input type="checkbox"/> Read extended attributes	<input type="checkbox"/> Change permissions
<input type="checkbox"/> Write extended attributes	<input type="checkbox"/> Take ownership
<input type="checkbox"/> Traverse folder / execute file	
<input type="checkbox"/> Delete subfolders and files	

Permission inheritance:

☒ Access permission (no restriction)

☐ Set explicitly for a file or folder

☐ Inherited by parent folder

В качестве пример был выбран фильтр просмотра папок и директорий, в которые пользователь User_12 может писать:

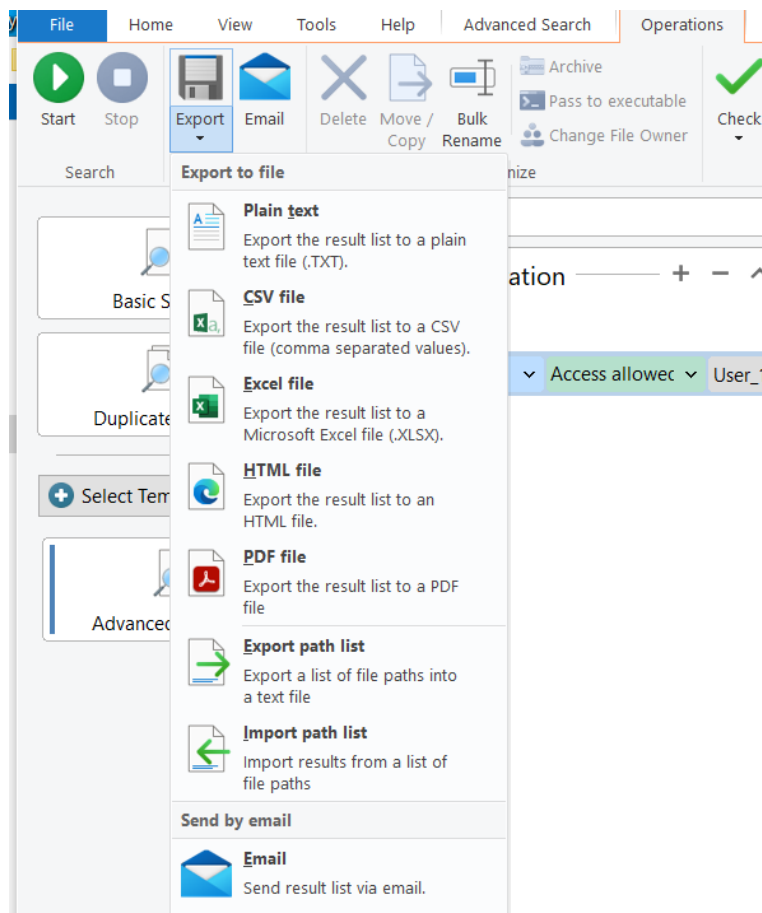
Search Configuration ▾ + - ^ ▾ ...

And ▾

Permissions ▾ Access allowed ▾ User_12: [Write at

<input type="checkbox"/> Name	Folder Path
<input type="checkbox"/> NTUSER.DAT	C:\Users\User_12\
<input type="checkbox"/> ntuser.dat.LOG1	C:\Users\User_12\
<input type="checkbox"/> ntuser.dat.LOG2	C:\Users\User_12\
<input type="checkbox"/> NTUSER.DAT(53b...	C:\Users\User_12\
<input type="checkbox"/> NTUSER.DAT(53b...	C:\Users\User_12\
<input type="checkbox"/> NTUSER.DAT(53b...	C:\Users\User_12\
<input type="checkbox"/> ntuser.ini	C:\Users\User_12\
<input type="checkbox"/> desktop.ini	C:\Users\User_12\Videos\
<input type="checkbox"/> desktop.ini	C:\Users\User_12\Searches\
<input type="checkbox"/> desktop.ini	C:\Users\User_12\Saved Games\
<input type="checkbox"/> Everywhere.searc...	C:\Users\User_12\Searches\
<input type="checkbox"/> Indexed Location...	C:\Users\User_12\Searches\
<input type="checkbox"/> winrt--(S-1-5-21-...	C:\Users\User_12\Searches\
<input type="checkbox"/> desktop.ini	C:\Users\User_12\Pictures\
<input type="checkbox"/> desktop.ini	C:\Users\User_12\Music\
<input type="checkbox"/> desktop.ini	C:\Users\User_12\Links\
<input type="checkbox"/> Bing.url	C:\Users\User_12\Favorites\
<input type="checkbox"/> Desktop.Ink	C:\Users\User_12\Links\
<input type="checkbox"/> desktop.ini	C:\Users\User_12\Downloads\
<input type="checkbox"/> Downloads.Ink	C:\Users\User_12\Links\
<input type="checkbox"/> desktop.ini	C:\Users\User_12\Favorites\

Результат можно экспортировать или отправить по почте:



3.2.1.5. NTFSSecurity модуль PowerShell (by raandree)

Для PowerShell работа с привилегиями осуществляется только через функции Get-Acl и Set-Acl. Однако данные команды используют сложный формат команд, что использование которого обычному пользователю может показаться некомфортным. Данный модуль предназначен для того, чтобы выполнять требуемые задачи по настройке разрешений более эффективно.

Требуется установить модуль в профиль PowerShell с помощью команды Install-Module:

```
PS C:\Windows\system32> Install-Module -Name NTFSSecurity

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or 'C:\Users\Nikita
Kulakov\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by running
'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install and import
the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
```

Если модуль не добавлен в профиль, то необходимо его загрузить:

```
PS C:\Users\Nikita Kulakov> Import-Module NTFSSecurity
```

После установки можно пользоваться командами из данного модуля. Модуль обладает достаточно хорошей документацией.

Просмотр прав для файла:

```
PS C:\Users\Nikita Kulakov> Get-NTFSAccess -Path 'C:\Users\Nikita Kulakov\Desktop\12\12.txt.txt'

Path: C:\Users\Nikita Kulakov\Desktop\12\12.txt.txt (Inheritance enabled)

Account      Access Rights      Applies to      Type      IsInherited      InheritedFrom
-----      -
NT AUTHORITY\SYSTEM      FullControl      ThisFolderOnly Allow      False
BUILTIN\Administrators  FullControl      ThisFolderOnly Allow      False
DESKTOP-NO7MUHQ\Nikita Kulakov FullControl      ThisFolderOnly Allow      False
```

Просмотр прав для папок и файлов через пайпы:

```
PS C:\Users\Nikita Kulakov\Desktop\12> dir | Get-NTFSAccess

Path: C:\Users\Nikita Kulakov\Desktop\12\12.txt.txt (Inheritance enabled)

Account      Access Rights      Applies to      Type      IsInherited      InheritedFrom
-----      -
NT AUTHORITY\SYSTEM      FullControl      ThisFolderOnly Allow      False
BUILTIN\Administrators  FullControl      ThisFolderOnly Allow      False
DESKTOP-NO7MUHQ\Nikita Kulakov FullControl      ThisFolderOnly Allow      False

PS C:\Users\Nikita Kulakov\Desktop\12> cd ..
PS C:\Users\Nikita Kulakov\Desktop> dir | Get-NTFSAccess

Path: C:\Users\Nikita Kulakov\Desktop\12 (Inheritance enabled)

Account      Access Rights      Applies to      Type      IsInherited      InheritedFrom
-----      -
Everyone      4294967295         ThisFolderSubfoldersAn... Allow      False
```

Добавить привилегии для файла можно следующим образом:

```
PS C:\Users\Nikita Kulakov\Desktop> Get-Item .\12\12.txt.txt | Add-NTFSAccess -Account DESKTOP-NO7MUHQ\User_12 -AccessRights FullControl
PS C:\Users\Nikita Kulakov\Desktop> Get-NTFSAccess -Path 'C:\Users\Nikita Kulakov\Desktop\12\12.txt.txt'

Path: C:\Users\Nikita Kulakov\Desktop\12\12.txt.txt (Inheritance enabled)

Account      Access Rights      Applies to      Type      IsInherited      InheritedFrom
-----      -
NT AUTHORITY\SYSTEM      FullControl      ThisFolderOnly Allow      False
BUILTIN\Administrators  FullControl      ThisFolderOnly Allow      False
DESKTOP-NO7MUHQ\Nikita Kulakov FullControl      ThisFolderOnly Allow      False
DESKTOP-NO7MUHQ\User_12 FullControl      ThisFolderOnly Allow      False
```

Уберем наследование:

```
PS C:\Users\Nikita Kulakov\Desktop> Get-Item .\12\12.txt.txt | Disable-NTFSAccessInheritance
PS C:\Users\Nikita Kulakov\Desktop> Get-NTFSAccess -Path 'C:\Users\Nikita Kulakov\Desktop\12\12.txt.txt'
```

Path: C:\Users\Nikita Kulakov\Desktop\12\12.txt.txt (Inheritance disabled)

Account	Access Rights	Applies to	Type	IsInherited	InheritedFrom
NT AUTHORITY\SYSTEM	FullControl	ThisFolderOnly	Allow	False	
BUILTIN\Administrators	FullControl	ThisFolderOnly	Allow	False	
DESKTOP-NO7MUHQ\Nikita Kulakov	FullControl	ThisFolderOnly	Allow	False	
DESKTOP-NO7MUHQ\User_12	FullControl	ThisFolderOnly	Allow	False	

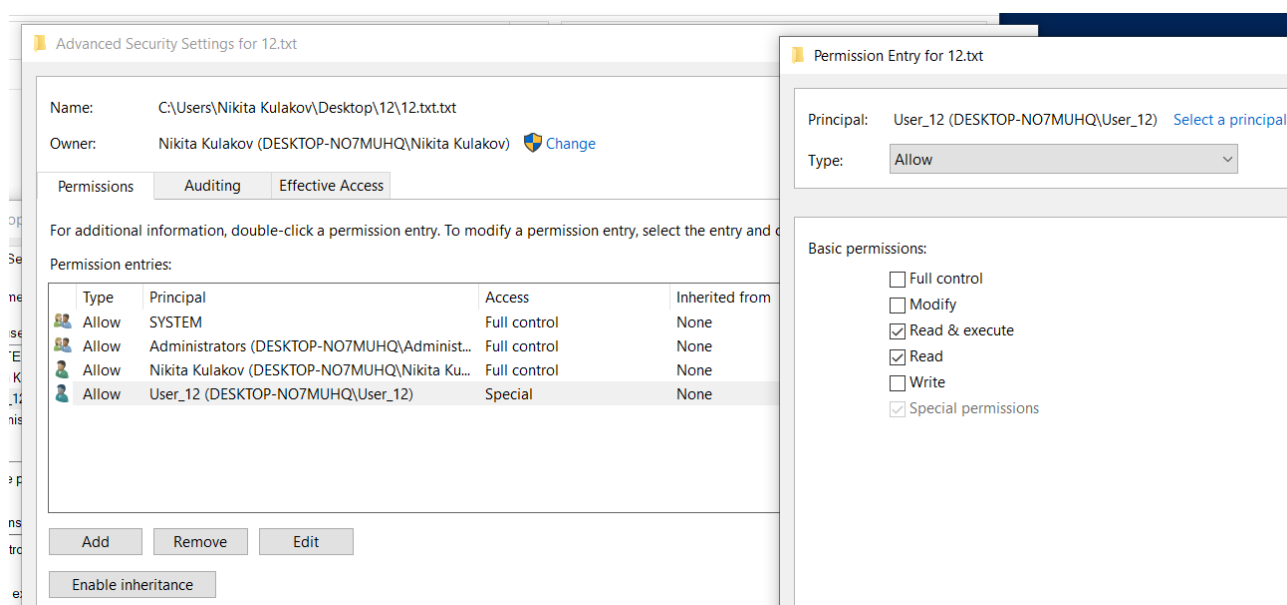
Удалим из записи DACL (ACE) Write для User_12:

```
PS C:\Users\Nikita Kulakov\Desktop> Get-Item .\12\12.txt.txt | Remove-NTFSAccess -Account: DESKTOP-NO7MUHQ\User_12 -AccessRights Write
PS C:\Users\Nikita Kulakov\Desktop> Get-NTFSAccess -Path 'C:\Users\Nikita Kulakov\Desktop\12\12.txt.txt'
```

Path: C:\Users\Nikita Kulakov\Desktop\12\12.txt.txt (Inheritance disabled)

Account	Access Rights	Applies to	Type	IsInherited	InheritedFrom
NT AUTHORITY\SYSTEM	FullControl	ThisFolderOnly	Allow	False	
BUILTIN\Administrators	FullControl	ThisFolderOnly	Allow	False	
DESKTOP-NO7MUHQ\Nikita Kulakov	FullControl	ThisFolderOnly	Allow	False	
DESKTOP-NO7MUHQ\User_12	DeleteSubdirectoriesAndFiles, Delete, Re...	ThisFolderOnly	Allow	False	

Что получилось в итоге:



3.2.2. Сравнение FAT и NTFS

Сравните файловые системы FAT и NTFS.

FAT (File Allocation Table) — относительно простая файловая система, изначально предназначенная для небольших дисков и простых структур папок. Имеет групповой метод организации, в котором таблица размещения файлов выделена в одну логическую область и находится в начале тома. В файловой

системе FAT смежные секторы диска объединяются в единицы, называемые кластерами. Количество секторов в кластере равно степени двойки.

Использовалась для твердотельных накопителей в эраз DOS и Windows 9x.

Файловая система FAT состоит из следующих секторов:

Section	Description
Сектор загрузчика	Содержит служебные структуры, которые принадлежат загрузочной записи раздела
Таблица аллокаций файлов	Определяет список (цепочку) кластеров, в которых размещаются файлы и папки тома
Корневой каталог	Содержит информацию о файлах и директориях, расположенных в корневой директории (только FAT12/FAT16)
Регион данных	Содержит сами данные

NTFS — стандартная файловая система для современных операционных систем Windows. Диск NTFS условно делится на две части. Первые 12% диска отводятся под метаинформацию. Запись каких-либо данных в эту область невозможна. Остальные 88% диска представляют собой обычное пространство для хранения файлов. NTFS поддерживает разграничение доступа к данным для различных пользователей и групп пользователей. Для повышения надежности используется журналирование. Для хранения файлов использует кластеры, по умолчанию от 512 байт до 2 МБ.

Сравнение файловых систем:

FAT (FAT32)	NTFS
-------------	------

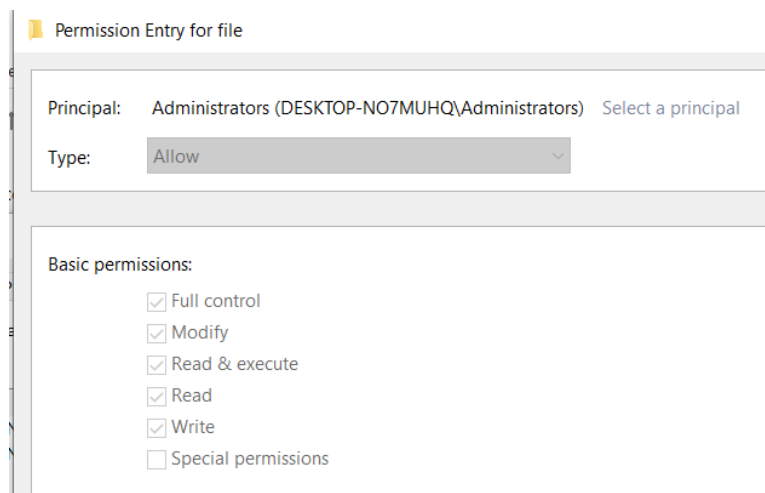
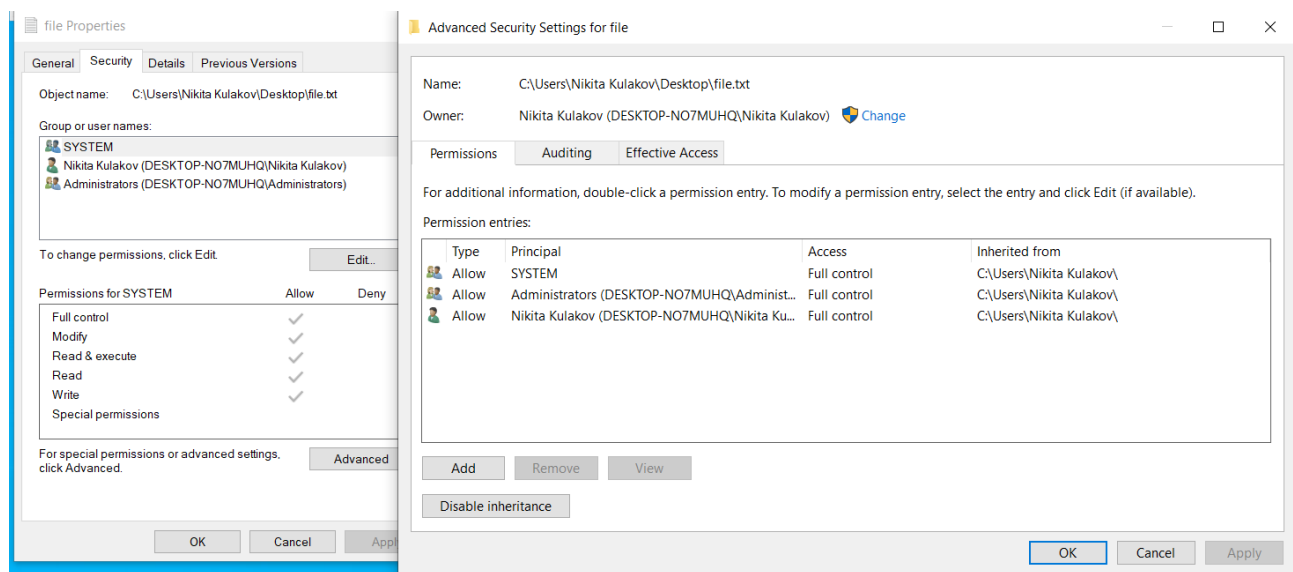
Поддержка всеми популярными ОС	Полностью поддерживается Windows, ограниченная поддержка на MacOS, Linux
Макс. Размер файла 4Гб	Макс. Размер файла 16 ЭиБ
Количество кластеров 2 ²⁸⁻¹²	Количество кластеров 2 ⁶⁴⁻¹
Длина имени 11, 255 (LFN) символов	Длина имени 255 символов
Ограниченные функции безопасности. Базовая безопасность на уровне файлов.	Поддерживает расширенные функции безопасности, такие как права доступа к файлам и папкам, шифрование и сжатие.
Шифрование не поддерживается	Шифрование поддерживается (BitLocker)
Журналирование отсутствует	Журналирование поддерживается (USN)
Отсутствует возможность восстановления поврежденных секторов	Благодаря повышенной надежности обладает способностью восстановления поврежденных секторов
Поддержка сжатия отсутствует	Поддержка сжатия присутствует
Подходит для небольших объемов; может наблюдаться снижение производительности на дисках большего размера	Как правило, более высокая производительность на больших объемах благодаря расширенным функциям.
Более высокие системные издержки из-за расширенных функций.	Более низкие накладные расходы на систему. Более простая структура.

3.2.3. Описание возможных способов задания прав к файлам и папкам

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

3.2.3.1. Через explorer (проводник)

Открываем свойства для файла или папки через контекстное меню:



3.2.3.2. Через powershell (Get-Acl, Set-Acl)

Просмотр разрешений для файлов и папок можно с помощью команды Get-Acl. Второй вариант команды выводит более подробную информацию.


```
PS C:\Users\Nikita Kulakov\Desktop> Get-Acl .\file.txt

Directory: C:\Users\Nikita Kulakov\Desktop

Path      Owner                      Access
-----
file.txt  DESKTOP-N07MUHQ\Nikita Kulakov NT AUTHORITY\SYSTEM Allow FullControl...

PS C:\Users\Nikita Kulakov\Desktop> (Get-Acl .\file.txt).Access

FileSystemRights : FullControl
AccessControlType : Allow
IdentityReference : NT AUTHORITY\SYSTEM
IsInherited       : True
InheritanceFlags  : None
PropagationFlags  : None

FileSystemRights : FullControl
AccessControlType : Allow
IdentityReference : BUILTIN\Administrators
IsInherited       : True
InheritanceFlags  : None
PropagationFlags  : None

FileSystemRights : FullControl
AccessControlType : Allow
IdentityReference : DESKTOP-N07MUHQ\Nikita Kulakov
IsInherited       : True
InheritanceFlags  : None
PropagationFlags  : None
```

Установка привилегий осуществляется с помощью команды Set-Acl:

```
PS C:\Users\Nikita Kulakov\Desktop> $ACL = Get-Acl .\file.txt
PS C:\Users\Nikita Kulakov\Desktop> $AccessRule = New-Object System.Security.AccessControl.FileSystemAccessRule("User_12", "Read", "Allow")
PS C:\Users\Nikita Kulakov\Desktop> $ACL.SetAccessRule($AccessRule)
PS C:\Users\Nikita Kulakov\Desktop> (Get-Acl .\file.txt).Access
```

```
PS C:\Users\Nikita Kulakov\Desktop> $ACL | Set-Acl .\file.txt
PS C:\Users\Nikita Kulakov\Desktop> (Get-Acl .\file.txt).Access
```

Также можно осуществлять форматирование, передавая объект Format-Table:

```
PS C:\Users\Nikita Kulakov\Desktop> (Get-Acl -Path "file.txt").Access | Format-Table IdentityReference,FileSystemRights,AccessControlType,IsInherited,InheritanceFlags -AutoSize

IdentityReference      FileSystemRights AccessControlType IsInherited InheritanceFlags
-----
DESKTOP-N07MUHQ\User_12 Read, Synchronize Allow         False       None
NT AUTHORITY\SYSTEM    FullControl     Allow         True        None
BUILTIN\Administrators FullControl     Allow         True        None
DESKTOP-N07MUHQ\Nikita Kulakov FullControl     Allow         True        None
```

3.2.3.3. Через icacls

При работе с файлами и папками:

```
PS C:\Users\Nikita Kulakov\Desktop> icacls.exe .\file.txt
.\file.txt DESKTOP-N07MUHQ\User_12:(R)
           NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           DESKTOP-N07MUHQ\Nikita Kulakov:(I)(F)

Successfully processed 1 files; Failed processing 0 files
```

```
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\Mikita Kulakov\Desktop> icacls.exe .\file.txt /grant DESKTOP-N07MUHQ\User_12:W
processed file: .\file.txt
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\Mikita Kulakov\Desktop> icacls.exe .\file.txt
.\file.txt DESKTOP-N07MUHQ\User_12:(R,W)
           NT AUTHORITY\SYSTEM:(I)(F)
           BUILTIN\Administrators:(I)(F)
           DESKTOP-N07MUHQ\Mikita Kulakov:(I)(F)
Successfully processed 1 files; Failed processing 0 files
```

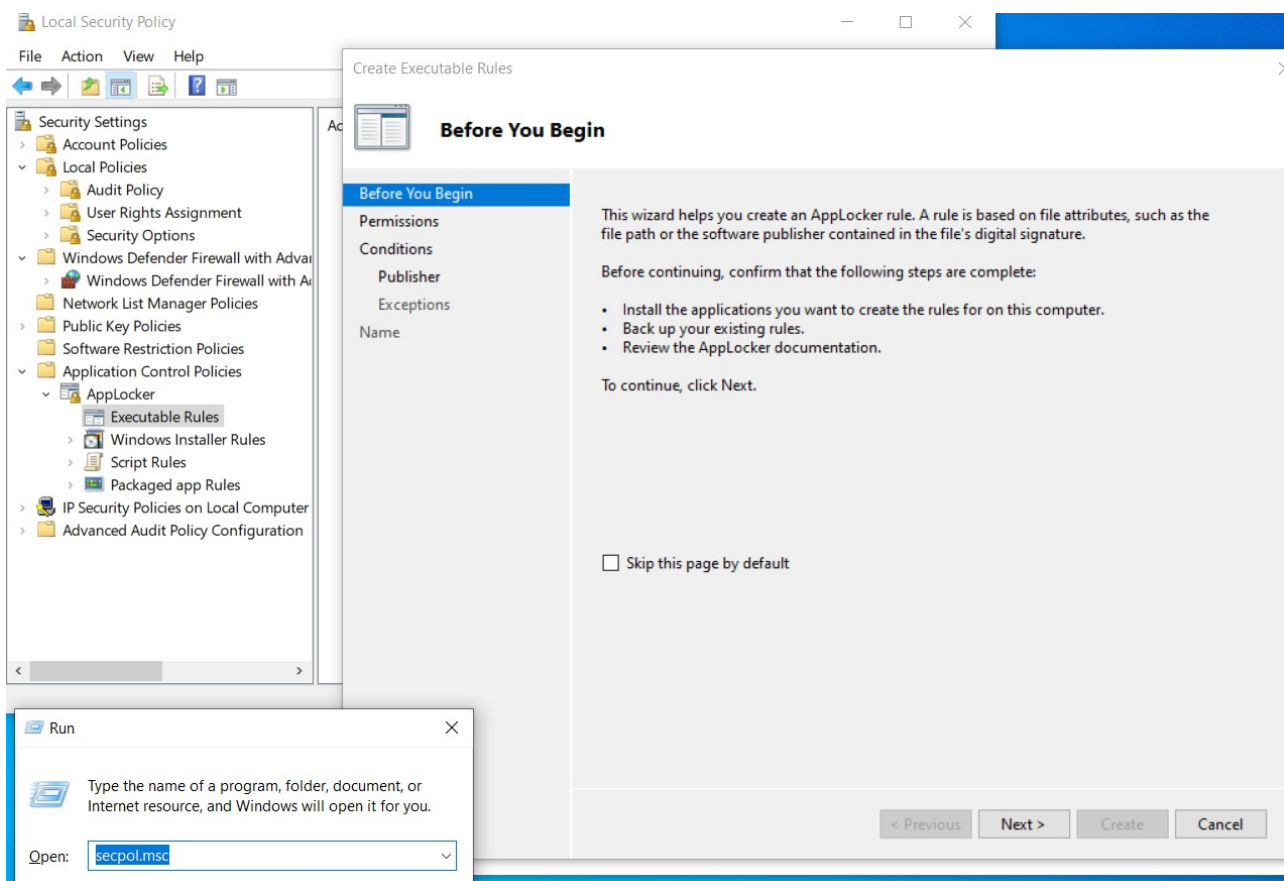
Для работы с папками могут пригодиться ключи /с (не прекращать работу при возникновении ошибки) и /t (применить права рекурсивно).

Справку по команде можно просмотреть при помощи команды icacls.exe без аргументов.

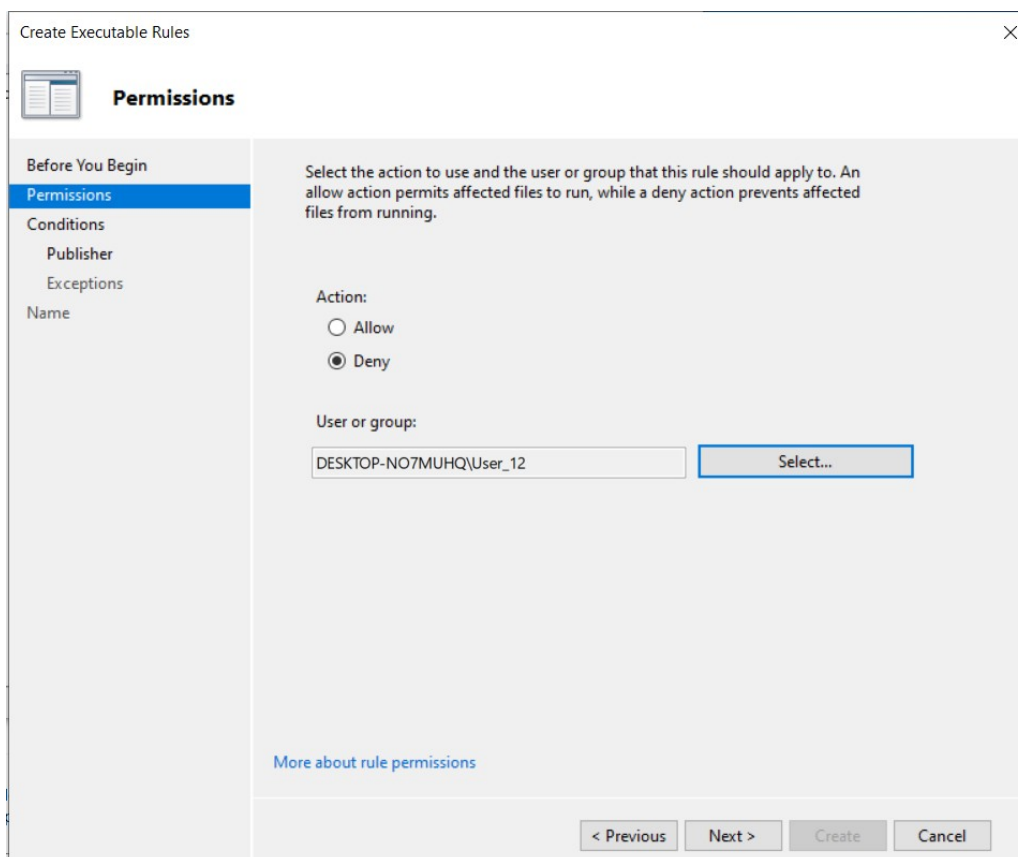
3.2.3.4. Ограничение исполнения при помощи политик ограниченного использования программ или AppLocker

С помощью политик ограниченного использования программ или AppLocker можно ограничивать разрешения на исполнение программ в Windows. Так как ранее приводились примеры с использованием политик ограниченного использования программ, то приведу здесь примеры для AppLocker.

Создадим политику на исполнение программ. Запустим Local Security Policy через secpol.msc. Перейдем в (Security Settings → Application Control Policies → AppLocker → Executable Rules).

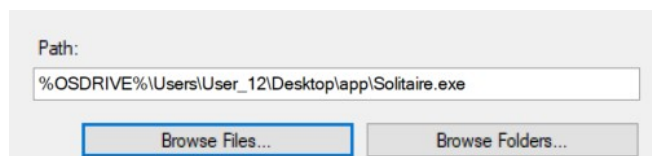


Выберем ограничивающую политику для User_12:







В качестве файла выберем Path. Также можно было выбрать хеш-сумму или Publisher, если приложение подписано, на случай если пользователь захочет переместить приложение.

Выберем в качестве пути путь до приложения. Также можно было выбрать путь до папки и задать исключения:



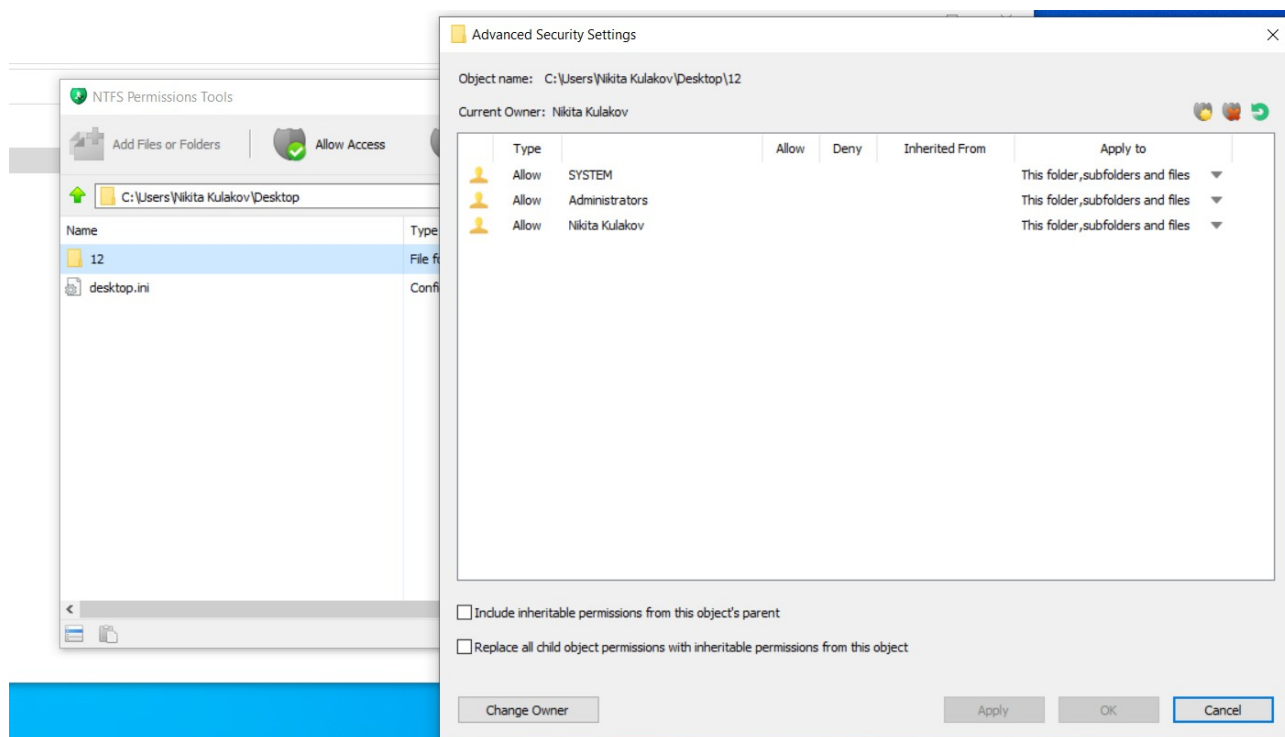
Таким образом, правила выглядят следующим образом:

Action	User	Name	Condition	Exceptions
 Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
 Allow	Everyone	(Default Rule) All files located in the Win...	Path	
 Deny	DESKTOP-NO7MUHQ\User_12	kosinka	Path	
 Allow	BUILTIN\Administrators	(Default Rule) All files	Path	

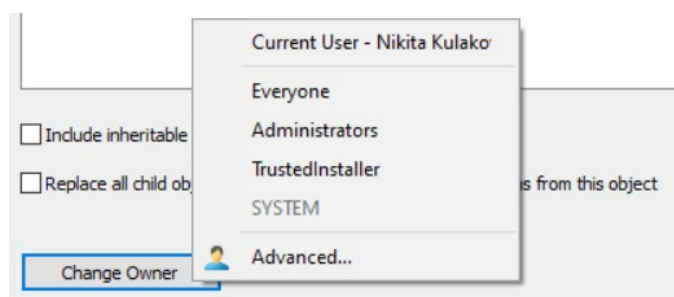
При попытке открытия приложения пользователем, ему будет высвечено, что программа заблокирована групповой политикой, также как и при использовании политик ограниченного использования программ.

3.2.3.5. Через приложения сторонних разработчиков, на примере NTFS Permission Tools

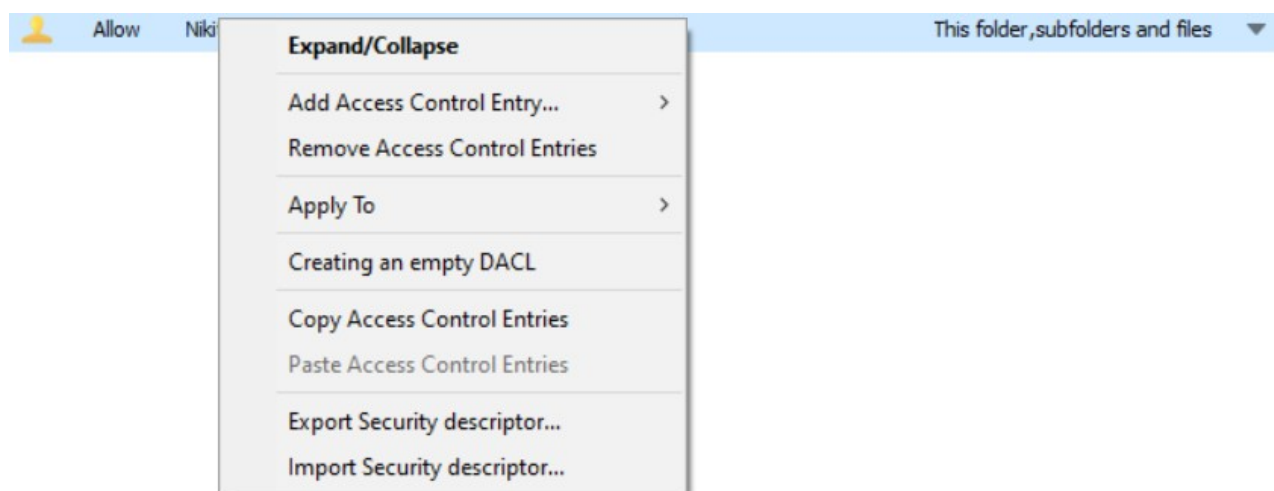
Похожим образом на проводник можно изменять разрешения и через приложение NTFS Permission Tools, продублирую пример из дополнительного задания 1:




Изменение владельца выглядит следующим образом:




Также присутствует некоторое количество опций, который упрощают администрирование:



Изменение прав также можно осуществлять через выпадающее меню:

	Allow	Nikita Kulakov	This folder, subfolders and files ▼	
		Full control	✓	●
		Traverse folder / execute file	✓	●
		List folder / read data	✓	●
		Read attributes	✓	●
		Read extended attributes	✓	●
		Create files / write data	✓	●
		Create folders / append data	✓	●
		Write attributes	✓	●
		Write extended attributes	✓	●
		Delete subfolders and files	✓	●
		Delete	✓	●
		Read permissions	✓	●
		Change permissions	✓	●
		Take ownership	✓	●

После изменения:

	Allow	Nikita Kulakov	This folder, subfolders and files ▼	
		Full control	●	●
		Traverse folder / execute file	✓	●
		List folder / read data	✓	●
		Read attributes	✓	●
		Read extended attributes	●	●
		Create files / write data	●	●
		Create folders / append data	✓	●
		Write attributes	✓	●
		Write extended attributes	✓	●
		Delete subfolders and files	✓	●
		Delete	✓	●
		Read permissions	✓	●
		Change permissions	✓	●
		Take ownership	✓	●

4. Выводы

В ходе выполнения лабораторной работы я познакомился с расширенными возможностями ОС Windows для управления разрешениями для пользователей. Редактирование разрешений осуществил при помощи проводника, функции

Get-Acl powershell и icacls.exe. Поработал с различными программами от сторонних разработчиков для редактирования и анализа разрешений. Также изменял локальные политики безопасности для задания ограничений на запуск приложений по критерию их расположения, и узнал о приложении AppLocker.