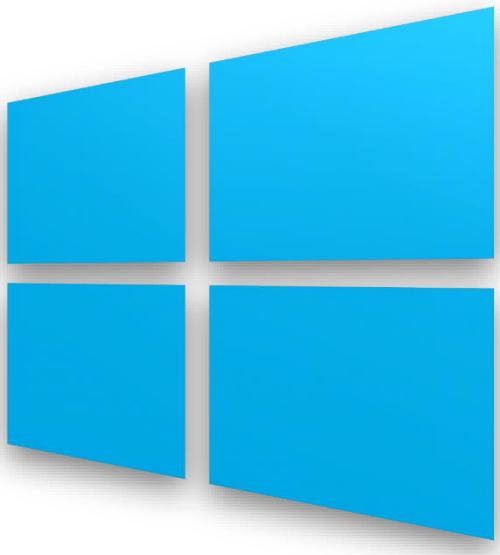
ИКОНОМИЧЕСКИ УНИВЕРСИТЕТ - ВАРНА

КАТЕДРА „ИНФОРМАТИКА”

Операционни системи

УПРАЖНЕНИЕ 6: ПРАВА ЗА ДОСТЪП НА ПОТРЕБИТЕЛСКИТЕ АКАУНТИ И ГРУПИ



Изготвил: гл. ас. д-р Радка Начева

ДАТА: 28 МАРТ 2019 Г.

УПРАЖНЕНИЕ 6: ПРАВА ЗА ДОСТЪП НА ПОТРЕБИТЕЛСКИТЕ АКАУНТИ И ГРУПИ

I. ЦЕЛ И ТЕМИ НА УПРАЖНЕНИЕТО

Целта на упражнението е да запознае студентите с правата за достъп на потребителските акаунти и групи в ОС Windows и способите за тяхното управление.

Темите[1], засегнати в упражнението, са:

1. Видове права (NTFS права за достъп)
2. Способи за тяхното управление

След изпълнение на предвидените задачи в упражнението студентите следва да придобият практически умения по управление на правата за достъп на потребителски акаунти и групи в Windows чрез инструменти на операционната система.

[1] ***Забележка**: Някои от поставените теми се разглеждат в теоретичната част на упражнението, а други – в практическата.*

II. ТЕОРЕТИЧНА ПОДГОТОВКА

1. Видове права (NTFS права за достъп) и способи за тяхното управление

NTFS правата за достъп (NTFS permissions) задават сигурност на достъпа (локален или отдалечен) за потребител или потребителска група до даден файл или директория на устройства, форматирани в NTFS.

При създаване на нова папка, тя наследява разрешенията от родителската. Когато създадете файл в папка, той наследява разрешенията, зададени за основната папка.

Правата могат да бъдат:

- **Full Control** – преглеждане съдържанието на папка, четене и отваряне на файл, създаване на нови файлове, промяна на правата за достъп, вземане на собственост на файл, т.е. пълни права за достъп;
- **Modify** – всичко гореизброено, освен промяна на права за достъп и вземане на собственост;
- **Read & Execute** – прочит на файлове и изпълняване на програми;
- **List Folder Contents (само за папки)** – преглед на съдържанието на папка;
- **Read** – прочит на файл;
- **Write** – създаване на файлове, записване на данни;
- **Special permissions** – други права.

В Таблица 1 са пояснени подробно специалните права за достъп.

Таблица 1

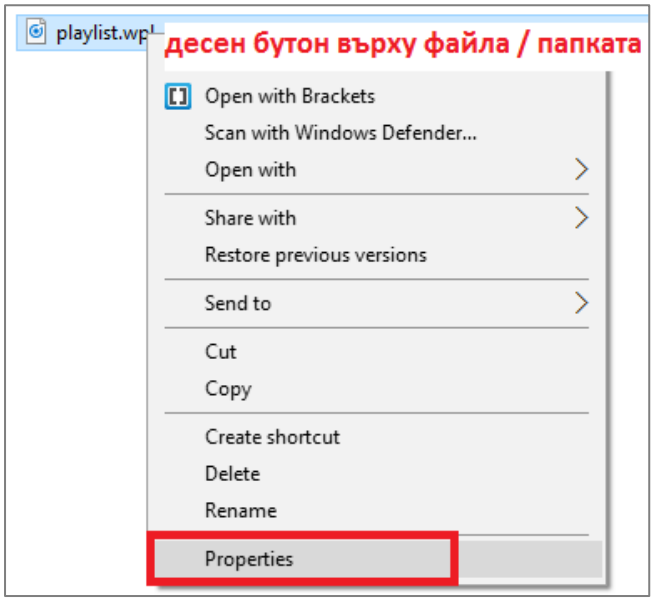
Допълнителни права за достъп в ОС Windows

Разрешение	Описание
Full Control (Пълен контрол)	Позволено е извършване на всякакви действия с файла или папката, именно – четене, записване, промяна и изтриване, включително на файловете и подпапките, съдържащи се в конкретната папка.
Traverse folder / execute file (Преглеждане на папка / изпълнение на файл)	Позволява достъп до папка, независимо от това дали достъпът до данните в папката е осигурен. Позволява изпълнение на файл.
List folder / read data (Прелистване на папка / четене на данни)	Позволява разглеждане на съдържанието на папка или файл.
Read attributes (Четене на атрибути)	Дава достъп само за четене (read-only access) до основни атрибути на файл или папка.
Read extended attributes (Четене на допълнителни атрибути)	Дава достъп само за четене (read-only access) до допълнителни атрибути на файл или папка.
Create files / write data (Създаване на файлове / Четене на данни)	Опцията за създаване на файлове позволява създаването или поставянето (чрез преместване или копиране) на файлове в дадена папка. Опцията за записване на данни позволява презаписване на данните във файла, но не и вмъкване на данни.
Create folders / append data (Създаване на папки / добавяне на данни)	Опцията за създаване на папки позволява създаване на подпапки в текущата папка. Опцията за добавяне на данни позволява данните да бъдат приложени към съществуващ файл (файл не може да бъде презаписана).
Write attributes (Записване на атрибути)	Позволява промяна на основни атрибути на файлове и папки.
Write extended attributes (Записване на допълнителни атрибути)	Позволява промяна на допълнителни атрибути на файлове и папки.
Delete subfolders and files (Изтриване на подпапки и файлове)	Осигурява разрешение за изтриване на всички файлове или папки, съдържащи се в дадена папка.

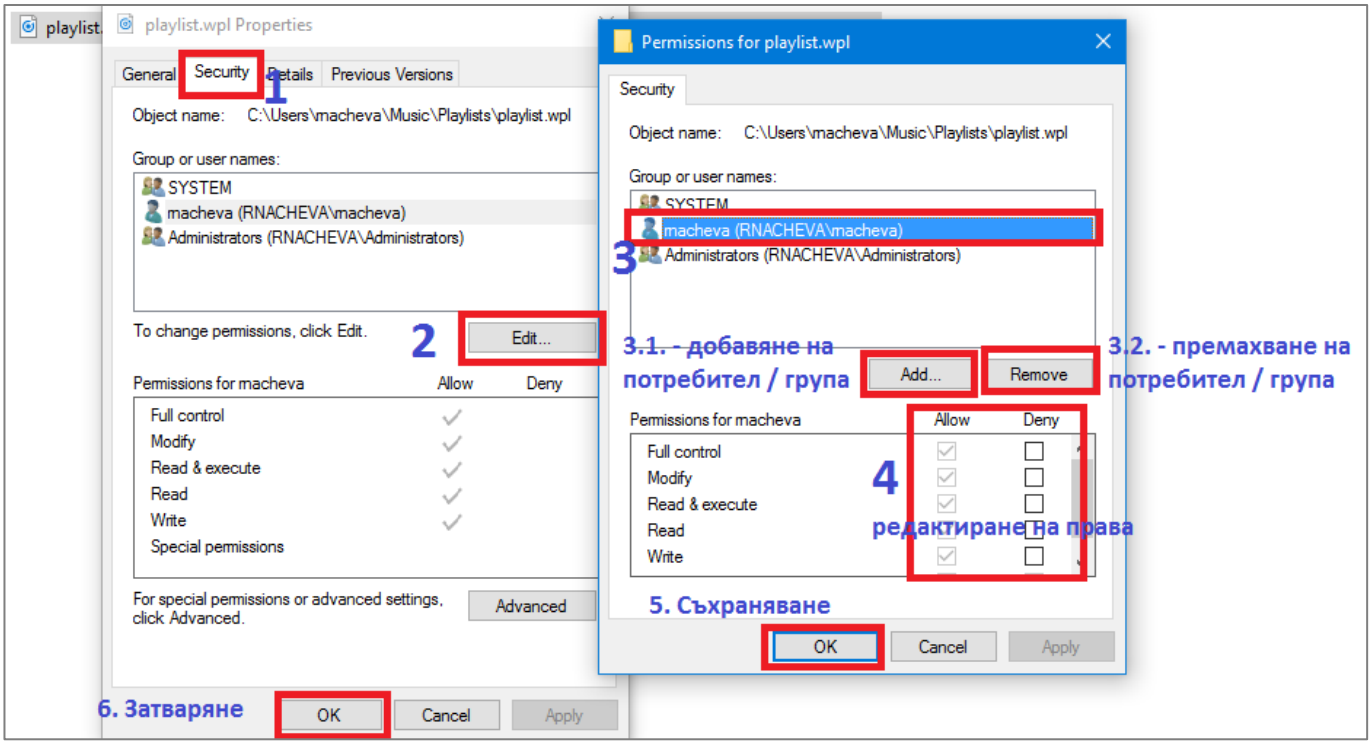
Разрешение	Описание
Delete (Изтриване)	Позволява изтриване на файл или папка. При изтриване на папка, потребителят или групата трябва да има разрешение за изтриване на папки или файлове.
Read permissions (Четене на разрешения)	Осигурява достъп за четене едновременно основни и специални разрешения на файлове и папки.
Change permissions (Промяна на разрешения)	Позволява промяна на основни и специални разрешения на даден файл или папка.
Take ownership (Назначаване на собственост)	Позволява на даден потребител да вземе собствеността на конкретен файл или папка.

2. Способи за управление на правата за достъп

За да се контролират правата за достъп, трябва да изберете от контекстното меню на файла / папката Properties->Security (вж. Фиг. 1 и Фиг. 2).

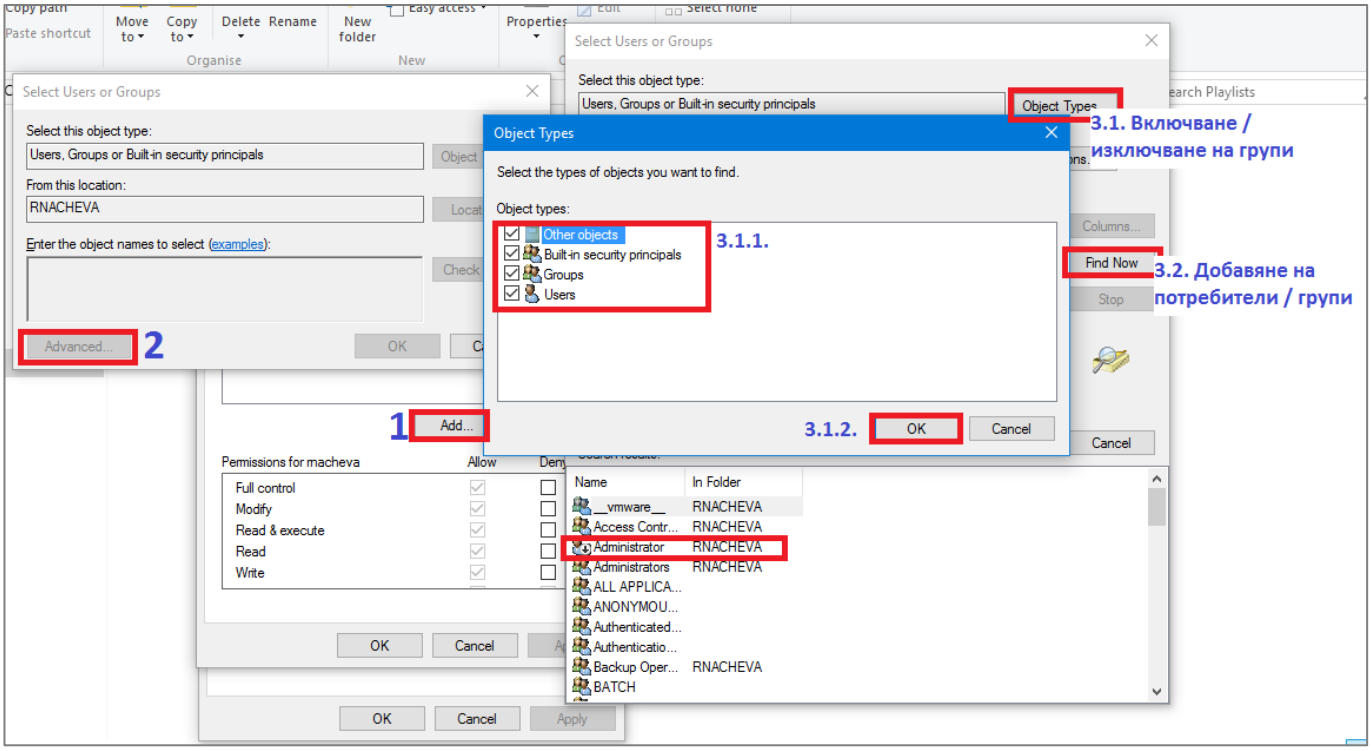


Фиг. 1. Избор на свойства на файла / папката



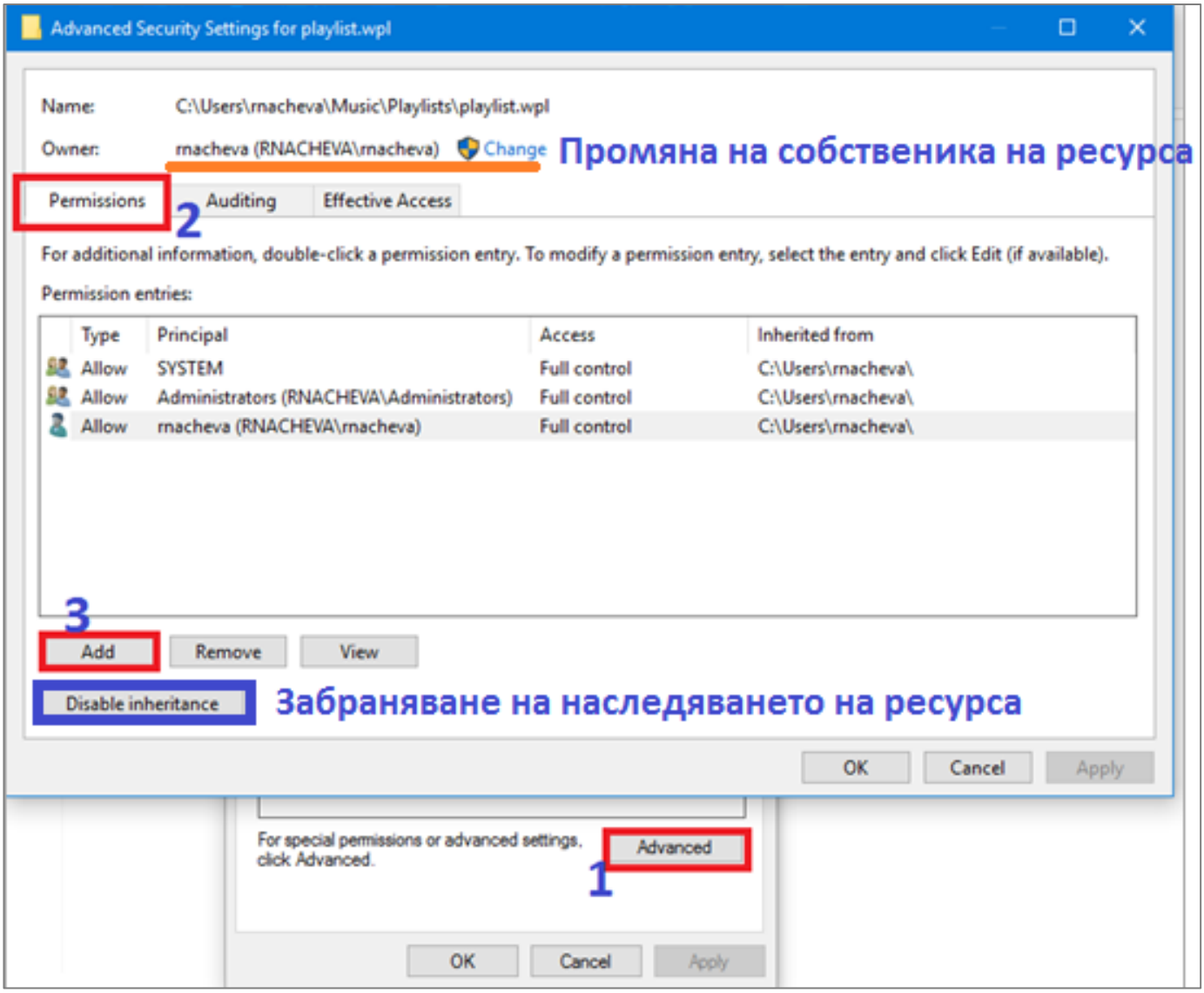
Фиг. 2. Редактиране на правата за достъп до файла / папката

Ако трябва да се добавят права за достъп на потребители или потребителски групи за работа с конкретен файл или папка, то трябва да се спазват стъпките, показани на Фиг. 3.

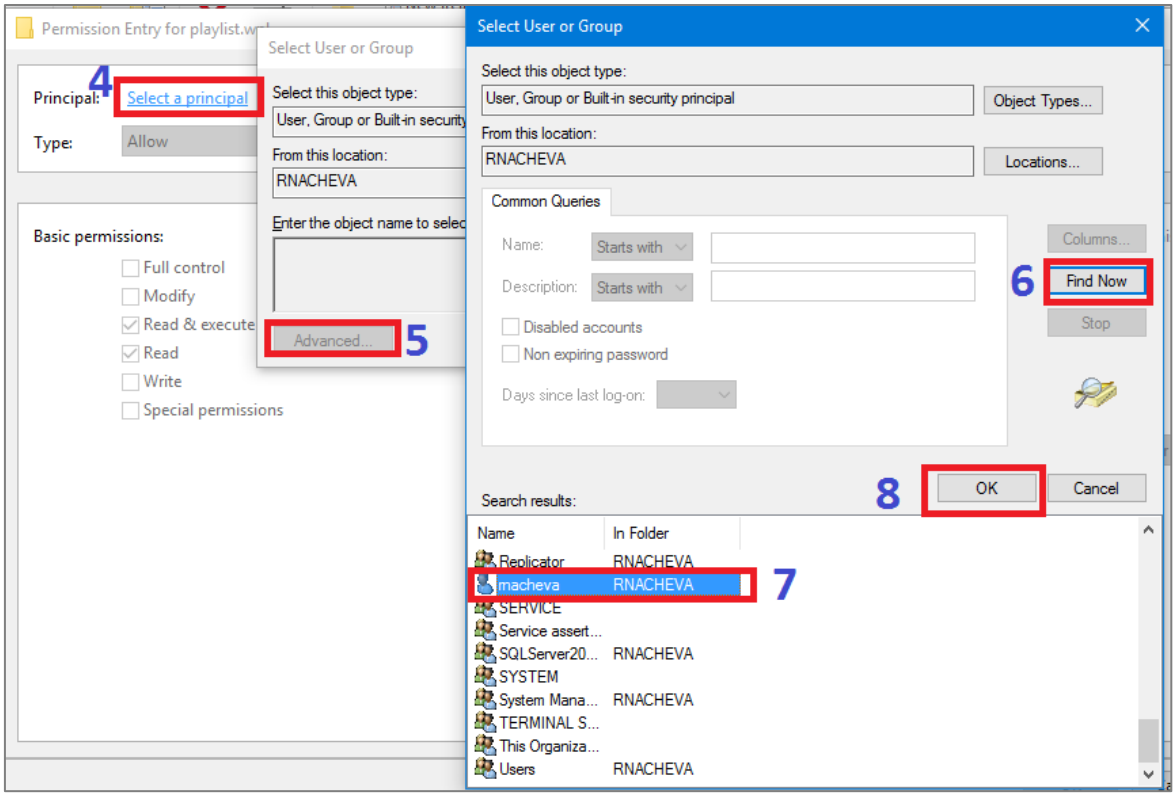


Фиг. 3. Добавяне на права за потребители / потребителски групи към файл / папка

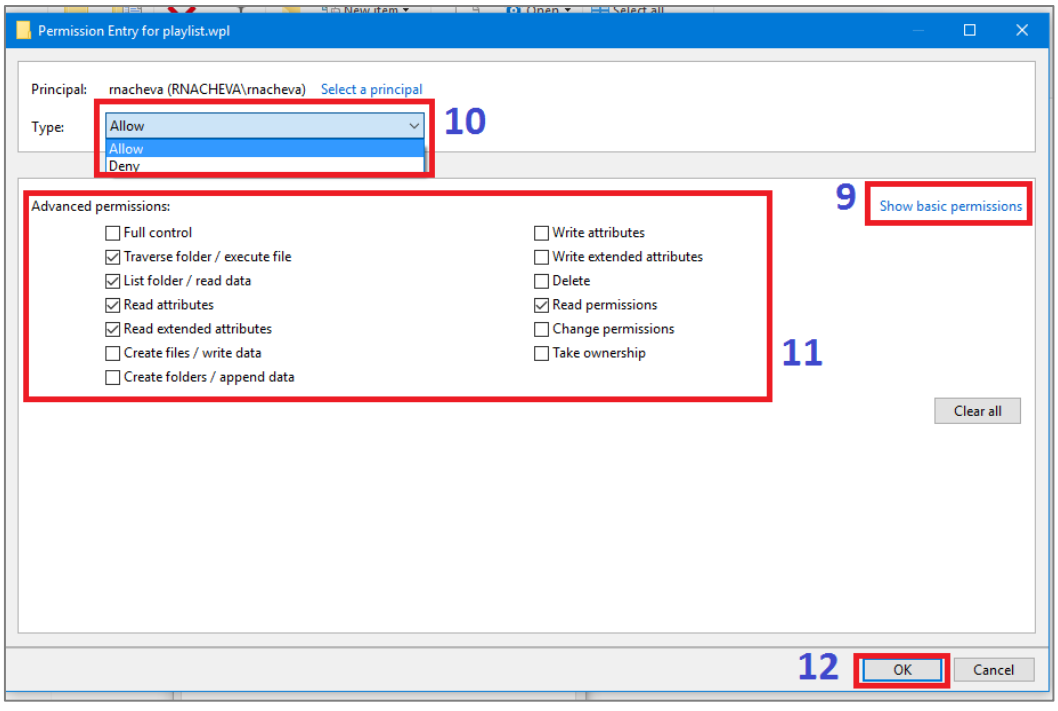
Ако има необходимост от задаване на допълнителни права за достъп (Special Permissions), като промяна на собственика на ресурса, забрана на наследяването на правата и задаване на разширени права за достъп, то трябва да се следват стъпките, показани на Фиг. 4, 5 и 6.



Фиг. 4. Задаване на допълнителни права за достъп - 1



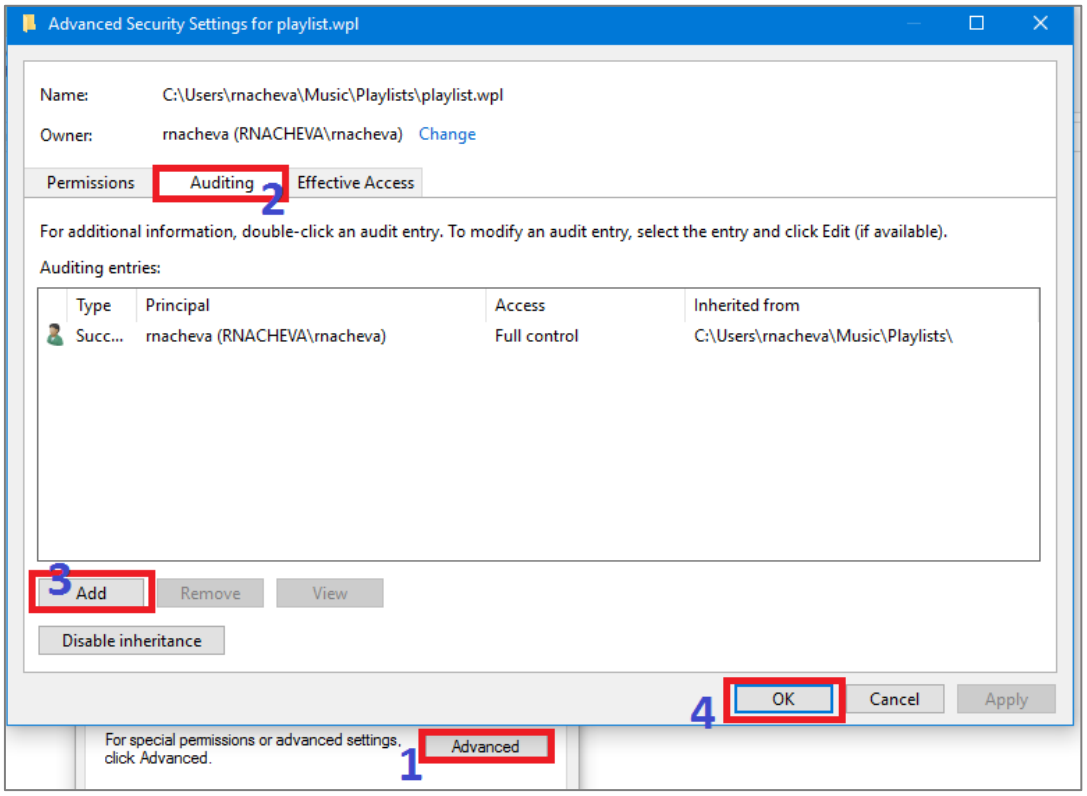
Фиг. 5. Задаване на допълнителни права за достъп - 2



Фиг. 6. Задаване на допълнителни права за достъп - 3

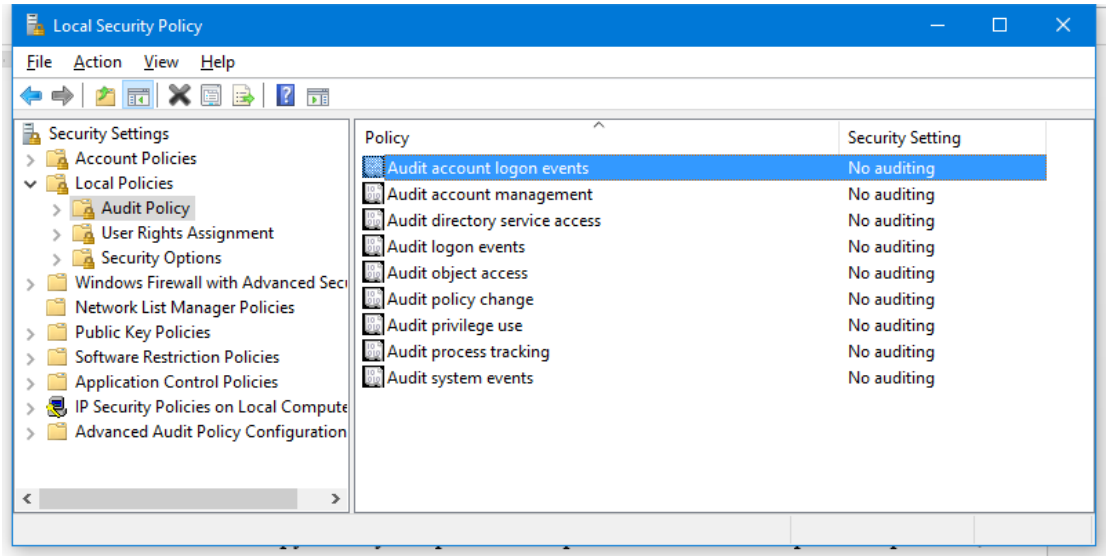
Всички описани до момента стъпки могат да бъдат прегледани и на следното видео: https://www.youtube.com/watch?v=FFZsXI9sq34 .

От свойствата на файла или папката могат да се задават допълнителни права за одит: **десен бутон -> Properties -> таб Security -> Advanced -> таб Auditing -> бутон Continue** (Фиг. 7). За активиране на опцията се изискват администраторски права. Одитът на файлове или папки позволява да се извърши тестване на наложените политики за сигурност и да се определи дали някои от потребителите се опитват да използват машината по неупълномощен начин.



Фиг. 7. Активиране на одит на файл или папка

За да се приложи опцията коректно, първо е необходимо да се активират съответните политики за одит от **Control Panel -> Administrative Tools -> Local Security Policy -> Local Policies -> Audit Policy** (Фиг. 8).

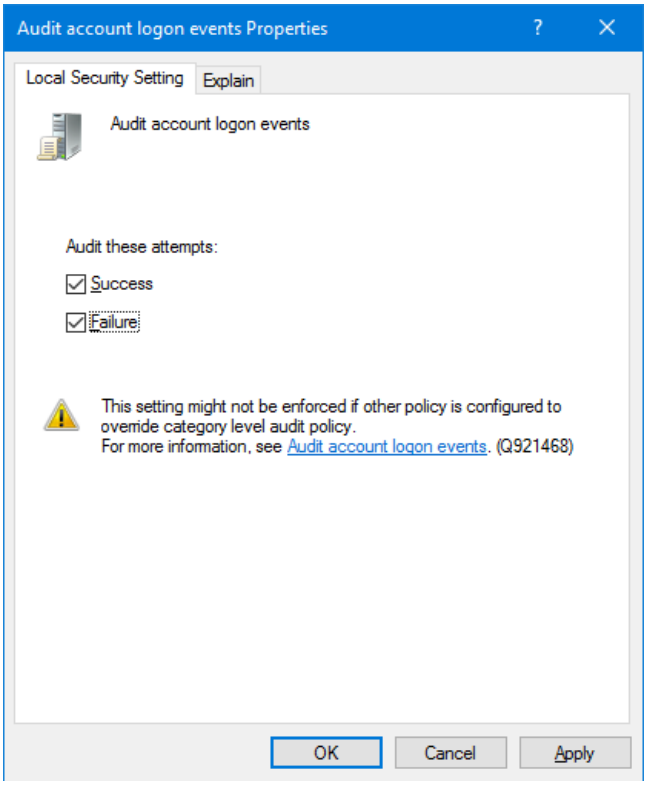


Фиг. 8. Политики за одит

Активирането на всички опции не е задължително и дори препоръчително, поради няколко причини:

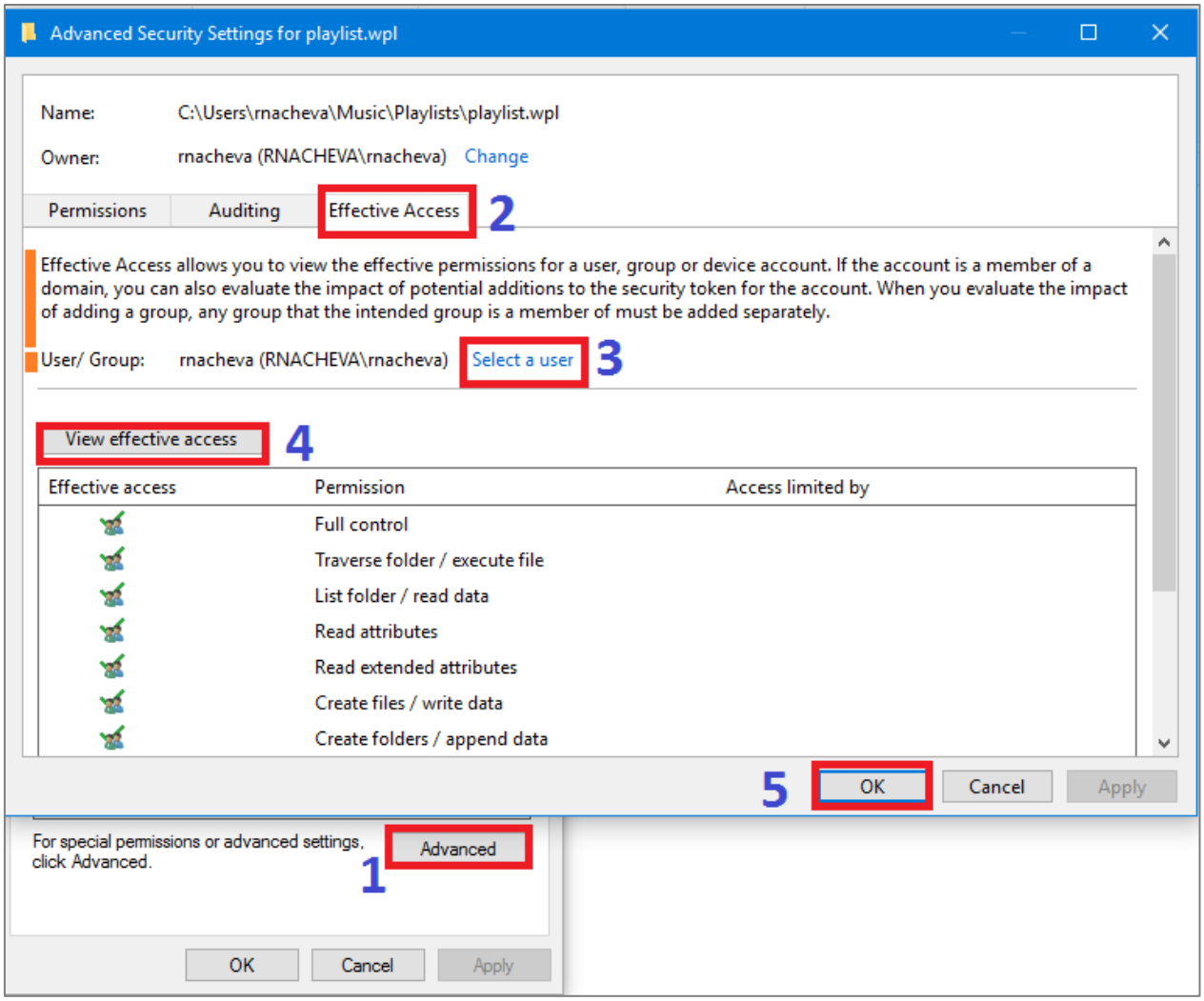
- В процеса на одит се създават лог файлове. Всяко вписване в дневника заема малко количество от свободното дисково пространство. Ако се появят твърде много одитирани събития (понякога стотици в минута), може да се изчерпи свободното дисково пространство;
- При всеки одит се консумира и малко количество процесорно време и памет, което може да се отрази негативно на производителността на системата.

За всеки един от видовете одит може да се избере (с двоен клик върху политиката) дали да се записват успешните или неуспешните изпълнения на съответните действия (Фиг. 9).



Фиг. 9. Активиране на политика за одит

Последната опция от свойствата на файла / папката, които са свързани с правата на достъп, е прегледът на достъпа – Фиг. 10.



Фиг. 10. Преглед на достъпа за даден потребител или група

III. ВЪПРОСИ ЗА САМОПРОВЕРКА

1. Какви видове права за достъп познавате в ОС Windows? Разяснете тяхното предназначение.

2. Какви способи за управление на права за достъп познавате в ОС Windows?

IV. ОБОБЩЕНИЯ И ДОПЪЛНИТЕЛНА ЛИТЕРАТУРА

Допълнителна литература:

1. User Accounts, Groups, Permissions & Their Role in Sharing
2. File and Folder Permissions
3. How IT works NTFS Permissions
4. Logon Scripts – The Basics
5. Microsoft Management Console - Overview