# 5. Защита на информацията в мрежова среда

## 5.1. Рискове, свързани с работата в мрежова среда

Компютърните мрежи са бъдещето за обмен на информация. Те непрекъснато се развиват и усъвършенстват. Този факт налага необходимостта от сигурна защита на данните от загуба или злоупотреба. Възникват два основни приоритета:

- Защита от отказ и възстановяване;
- Мрежова сигурност.

### Защита от отказ и възстановяване

Хардуерните повреди могат да бъдат сериозна причина за загуба на информация, затова е необходимо вземането на определени мерки за защита и възстановяване на данните от сривове. Могат да се предприемат някои препоръчителни действия в тази насока:

- Използване на аварийно захранване за избягване на проблеми с електрозахранването. Често срещан вариант е включването на UPS устройства, които притежават батерии, съхраняващи определено количество заряд, осигуряващо време за работа на системата след прекъсване на основното захранване.
- Архивиране на данните с помощта на програма за архивиране, в случай на повреда на твърд диск или вирусен проблем. Необходимо е осигуряване на допълнително устройства, където да се съхраняват архивираните данни.

### Мрежова сигурност

Мрежовата сигурност е основен проблем при използване на мрежова среда. Съществуват немалко случай, свързани с проникване в мрежи на правителствени и бизнес организации, както и сериозни атаки от компютърни вируси в широк мащаб. Терминът **сигурност** се обвързва с необходимите действия, които трябва да се предприемат за защита на един компютър и съдържащата се в него информация. Заплахите могат да бъдат външни и вътрешни.

### Външни заплахи

Външните заплахи могат да възникнат, когато локалната мрежа е свързана към друга мрежа, например Интернет. Използват се различни методи на проникване:

1. Неоторизирано използване на чужди потребителски имена и пароли

Всяко лице, което се нуждае от достъп до ресурсите на определена система или мрежа е необходимо да се превърне в неин **потребител** чрез придобиването на акаунт - комбинация от потребителско име (*username*) и парола (*password*), които му осигуряват определени права за достъп до файлове, програми и хардуер. **Паролата** е последователност от букви, цифри и символи и се използва за удостоверяване на правилния потребител. Процесът на получаване на права за достъп до ресурсите на системата или мрежата се нарича **оторизация**. Ако някой използва чужд акаунт без да е упълномощен за това се казва, че е налице неоторизирано използване и е налична предпоставка за нарушаване на сигурността.

2. Атаки от тип отказ на услуга (*Denial of Service, DoS*)

Тези атаки целят прекъсване на установена връзка или възпрепятстване на създаването на такава към мрежата. Те не предизвикват срив в системата, а наводняват мрежата с непотребни пакети или симулират мрежов проблем, който прекъсва комуникацията.

3. IP спуфинг

При този подход се променя IP адреса на подателя в изпращаните пакетите, така че да изглежда, че са генерирани от сигурен източник. Получателят не знае това и насочва отговорите на приетите заявки към хоста, съответстващ на заложения IP адрес.

DoS атаките често използват този подход за претоварване на мрежата и устройствата с подправени пакети.

4. Компютърни вируси и червеи

Компютърните вируси са самовъзпроизвеждащи се програми, които могат да се разпространяват от една система на друга чрез прикрепяне на кода им към различни файлове, без съгласието или знанието на потребителя. Някои от тях са безобидни и досадни (например извеждат съобщения на екрана). Други са злонамерени и се стремят към унищожаване на файлове (програми, данни).

Червеят е самовъзпроизвеждащ се вирус, който използва мрежата, за да разпраща свои копия до крайните устройства. За разлика от вируса, компютърният червей не се нуждае от прикачване към вече съществуваща програма. Разпространява се като прикрепен файл към електронната поща, като изпълними файлове, като HTML страници, съдържащи скриптове, или като документи с макроси.

5. Троянски коне

Това са злонамерени програми, представящи себе си като полезен софтуер с цел, събиране на важна информация и изпращане на атакуващия или отваряне на вратичка в сигурността на атакуваната система. Например лъжлив екран за логване в системата, кражба на поверителни данни (пароли, информация за банкови сметки и кредитни карти), контрол над системата и др.

**Вътрешни заплахи**

Вътрешните заплахи са тези, които могат да се извършат директно върху избрана система или през локалната мрежа. Мотивите за подобни пробиви в сигурността могат да бъдат свързани с корпоративен шпионаж, недоволни служители или случайни (непланирани) попадения.

**Мерки за сигурност**

Външните и вътрешните заплахи могат да бъдат избегнати при прилагане на определени мерки за сигурност, като:

1. Използване на операционни системи с висока степен на сигурност.

Съвременните операционни системи удовлетворяват това изискване. Например разновидностите на Windows или Linux очакват въвеждането на валидно потребителско име и парола, за да позволят зареждане и работа със системата. Съхранението на паролите е във вид, неудобен за осъществяване на лесен достъп до тях.

2. Автентикация и идентификация

Автентикацията е процес на удостоверяване на правилния потребител. В качеството на синоним на термина автентификация понякога се използва термина "проверка на идентичност". Идентификацията позволява на

субекта да назове себе си. За целта се използват различни идентификатори, като парола, личен идентификационен номер, криптографски ключ и др.

Например правилността на паролата за определено потребителско име гарантира, че потребителят е автентичен.

Друг често използван идентификатор за удостоверяване на самоличността на регистриран вече потребител на даден уебсайт, като част от процеса на влизане, е използването на „бисквитки“ (cookies). Те могат да спестят повторно въвеждане на потребителско име и парола при всеки следващ достъп до този сайт. Представляват текстови данни, които се съхраняват на клиентската система, обвързват се с конкретен браузър и сайт, и съдържат информация, която браузъра изпраща към сървъра при всяка негова заявка. Бисквитките имат различен период на валидност, от временни файлове, съществуващи до момента на напускане на уебсайта или деактивирате на използвания уеб браузър, до запазени за указан срок.

3. Криптиране на данните

Криптирането на данните е технология, базирана на науката криптография. Криптирането използва код или ключ за разбъркване (шифриране) и след това за подреждане (дешифриране) на данните, с цел представянето им в първоначалната им форма. Данните се криптират с помощта на алгоритъм или шифър.

4. Използване на защитна стена (Firewalls) и прокси сървър

Защитната стена филтрира входящите и изходящите пакети и определя дали да разреши преминаването на даден пакет. Тя се настройва от администратора на мрежата и обикновено се разполага на шлюза (*gateway*) на мрежата.

Прокси сървърът функционира като посредник между системите от вътрешната мрежа и тези от външната. Например една от функциите на такъв сървър е свързана с кеширане (съхраняване) на Web страници за подобряване на качеството на Web услугата.

5. Използване на антивирусен софтуер

В днешно време е задължително използването на антивирусни програми за защита на системата от вируси. Антивирусният софтуер

открива вирусни инфекции, сигнализира за тях и се опитва да предотврати евентуални техни поражения.

6. Ограничаване на физическия достъп

Тази стъпка е свързана с определяне на степента на директен физически достъп на лица до ресурсите на мрежата. При висока степен на сигурност сървърите и устройствата за връзка трябва да се поставят в зони без достъп на физически лица, освен упълномощените за това. Работните станции, които се намират в незащитени райони трябва да ограничават по софтуерен начин достъпа до важните данни в мрежата.

**Основни нормативни документи**

Съвременното общество и свързаните с него обществено-икономически реалности са пряко обвързани с компютърните технологии и тяхното динамично развитие. Този факт поражда значими юридически проблеми, свързани с правната регламентация на софтуера, базите данни и защитата им като интелектуални продукти. Филипините са първата страна в света, включила през 1972 г в авторското си право компютърните програми. През 1980 г. в САЩ също се приема закон за Авторското право върху компютърните програми. Подобни стъпки се правят във Франция и Германия. През 1991 г. Съветът на Европейските общности издава Европейската директива за правна защита на компютърните програми.

Българският Закон за авторското право и сродните му права (ЗАПСП) също разглежда компютърните програми и базите данни като обекти на авторско право и съдържа текстове, свързани със закрилата им от използване, копиране и разпространение.

Минималното ниво на технически и организационни мерки при обработване на лични данни и допустимия вид защита са определени от Комисията за защита на личните данни в Наредба № 1 от 30.01.2013 г. Тя разглежда защитата на автоматизираните информационни системи и/или мрежи като система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.

Условията и реда за предоставяне на удостоверителни услуги чрез електронни документи и електронен подпис са описани в Закона за електронния документ и електронния подпис.

## Основни принципи, гарантиращи сигурността на информацията

Представените мерки за сигурност имат за цел да запазят основните принципи, свързани с гарантиране на сигурността на информацията:

- предотвратяване на неупълномощен достъп до данните и ресурсите на системата и мрежата.
- запазване на конфиденциалността (поверителността) и целостта на информацията, което означава, че тя може да бъде използвана и променяна само от упълномощени потребители.
- осигуряване на непрекъснат достъп за упълномощените потребители.
- използване на стандартизирани решения за защита, базирани на международни стандарти и протоколи за сигурност.

## Основни начини и средства за защита на мрежата от неоторизиран достъп

Осъществяването на мерките за сигурност може да бъде постигнато по различни начини и с различни средства. Те могат да бъдат реализирани софтуерно или хардуерно, а понякога и като комбинация от двата подхода.

1. Поддържане на потребители с различни нива на достъп

Поддържането на множество потребители от една операционна или уеб система е възможност, която позволява използването на потребителски акаунти за осъществяване на достъп до системата или мрежата. Процесът на оторизация задава правомощията на всеки потребител, което води до ограничаване на действията му до позволените за него, с което определя неговото **ниво на достъп**. Например Windows 10 предлага възможност за създаването и използването на два типа акаунти, осигуряващи различни нива на достъп:

- Администраторски (*Administrator)*, позволяващ пълен контрол над компютъра и достъп до всички програми, настройки, файлове и др. Могат да се създават или премахват други потребителски акаунти, да се извършват настройки на операционната система, да се инсталират/деинсталират софтуерни и хардуерни компоненти.
- Стандартен (*Standard*), който ограничава потребителя до използване на софтуер и възможността да прави промени, които не указват

въздействие върху другите потребители или сигурността на системата.

2. Използване на сигурни пароли

Важна част от всеки план за сигурност е използването на колкото е възможно по сложна парола. Когато се налага потребител да избира парола сигурните системи налагат някои изисквания (политики), като:

- Паролите не трябва да бъдат думи или числа, които лесно да бъдат отгатнати поради тяхната връзка с потребителя (например име, фамилия, рождена дата и др.).
- Паролата трябва да бъде лесна за запомняне от потребителя, за да не се записва някъде.
- Повечето системи, поддържащи пароли, правят разлика между главна и малка буква. Използването на комбинация от тях създава по-сигурна парола (например AlExooTr).
- По-голямата дължина на паролата и включването на специални символи я прави по-сигурна (например AlEx!2#ooTr).
- В среда с висока сигурност потребителите е необходимо да се задължават да сменят паролата на определен период от време, като новата не трябва да прилича на старата.

3. Криптиране на файлове

Криптирането на файлове е операция, която шифрира съдържанието на файловете и ги запазва във вид, който не може да бъде прочетен от друг, освен от създателя им. За правилното им разчитане е необходим ключ, който притежава само собственика им. Например Windows 10 предлага такава възможност от контекстното меню на избран файл чрез последователността от стъпки *Properties/Advanced/Encrypt contents to secure data*.

4. Използване на криптиращи протоколи

Криптиращите протоколи са необходими за защита на данните при пренос по мрежата. Съществуват различни реализации на такива протоколи. Например TLS (*Transport Layer Security*) и неговият предшественик SSL (Secure Sockets Layer) са криптиращи протоколи, осигуряващи сигурност на комуникацията по Интернет. Уебсайтовете, които използват криптирана връзка със SSL или TLS имат URL с префикс "https:", вместо "http:".

5. Използване на електронен (цифров) подпис

Електронният подпис замества стандартния подпис при подписване на електронни документи. Той е електронен, криптиран печат за потвърждаване, че изпращаната цифрова информация идва от подписващия и не е изменена. Цифровият подпис не криптира данните, а помага да се гарантира:

- Автентичност – потвърждава, че подписващият е този, за когото се представя.
- Цялост - гарантира, че съдържанието не е променено или манипулирано след цифровото подписване на документа.
- Невъзможност за отричане от страна на подписалия – доказва произходът на едно подписано електронно съдържание.

6. Сигурност на електронната поща

Електронната поща може да бъде достъпна за потребителите чрез уеб приложение или пощенски клиентски софтуер, инсталиран на използваната система (например Windows Mail). Препоръчително е при изпращане или получаване на съобщение да се осигури връзка чрез криптиращи протоколи. Почти всички уеб варианти за електронна поща в момента поддържат такъв тип връзка. Може да се разпознае по URL префикса "https:". Пощенският клиентски софтуер също дава възможност за използване на криптиране, което се задава при настройка на опциите на пощенския акаунт, стига да бъде поддържано от доставчика на услугата. Допълнително и в двата варианта може да се използва електронен подпис за доказване на автентичността на съобщението.

При използване на електронна поща е препоръчително спазването на следните съвети:

- Да не се отварят електронни съобщения ако подателят липсва, не е разпознат или полето за подател съдържа данни на получателя;
- Да се игнорират съобщения, съдържащи само хипервръзки.

7. Поддържане на актуални версии на софтуерните продукти

Актуалните версии на използвания софтуер разрешават проблема с открити бъгове, които могат да се окажат предпоставка за нарушаване на

сигурността на системата. Препоръчително е да се извършва актуализация на инсталираните програми. Обновяването на антивирусния софтуер и ъпдейтите на операционната система трябва да се извършват периодично, а там където е възможно и автоматично.

8. Контролиране на достъпа до мрежата чрез защитни стени

За контролиране на достъпа до мрежата могат да се използват защитни стени, които да са подчинени на планирани правила за защита спрямо потока от данни, който трябва да бъде разрешен. Възможно е внедряването им и в локалната мрежа за създаване на безопасност при съвместна работа на различни отдели, офиси и групи от една и съща организация. Те могат да бъдат реализирани софтуерно или да комбинират хардуерни и софтуерни решения. Софтуерните защитни стени могат да бъдат инсталирани на всеки персонален компютър, за да го защитават, докато хардуерните са предназначени за защита на мрежата. Обикновено, когато една програма се опита да осъществи достъп до Интернет за първи път, софтуерните защитни стени питат дали да и разрешат достъп. Защитната стена не може да защити от вирусна атака.

**Задаване права на достъп до ресурси в локална мрежа в среда Windows 10**

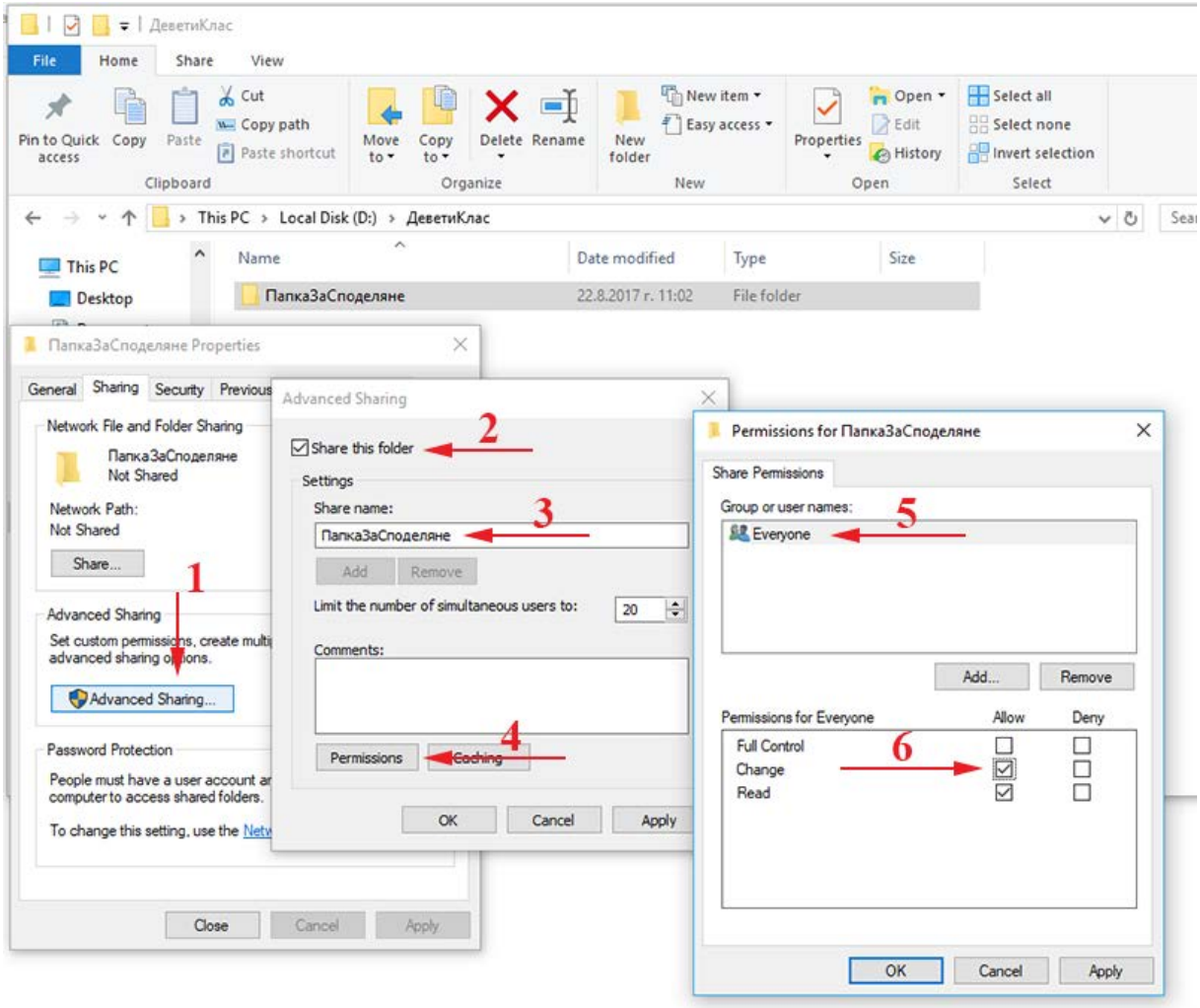
В предишния урок беше представена последователност от стъпки за споделяне на папка и принтер в средата на операционната система Windows 10. В стъпка 4 беше коментирана възможността за избор на ниво на позволение между предложените опции *Read* (само за четене, по подразбиране) и *Read/Write* (с добавяне на позволение за модифициране и изриване).

Съществува вариант за отдаване на ресурса (папката) с използването на бутона *Advanced Sharing* (фигура 1). Този бутон отваря нов прозорец, в който трябва да се сложи отметка на опцията *Share this folder* и да се посочи име, с което се отдава ресурсът (например *ПапкаЗаСподеляне*). С бутона *Permissions* се задава групата или отделен потребител, с който се споделя ресурса. В този пример това е подразбиращата се група *Everyone*, за която е поставена и отметка за модифициране на документа (*Change*) в колонката *Allow*. Възможните опции за избор са:

- *Read* – позволява да се виждат имената на отделните папки, файловете и техните атрибути, да се стартират програми, да се копират файлове.

- *Change* – включва всички привилегии от *Read* като допълва позволения за: създаване на папки, добавяне на файлове към папки, модифициране на съдържанието във файловете, изтриване на файлове или папки.

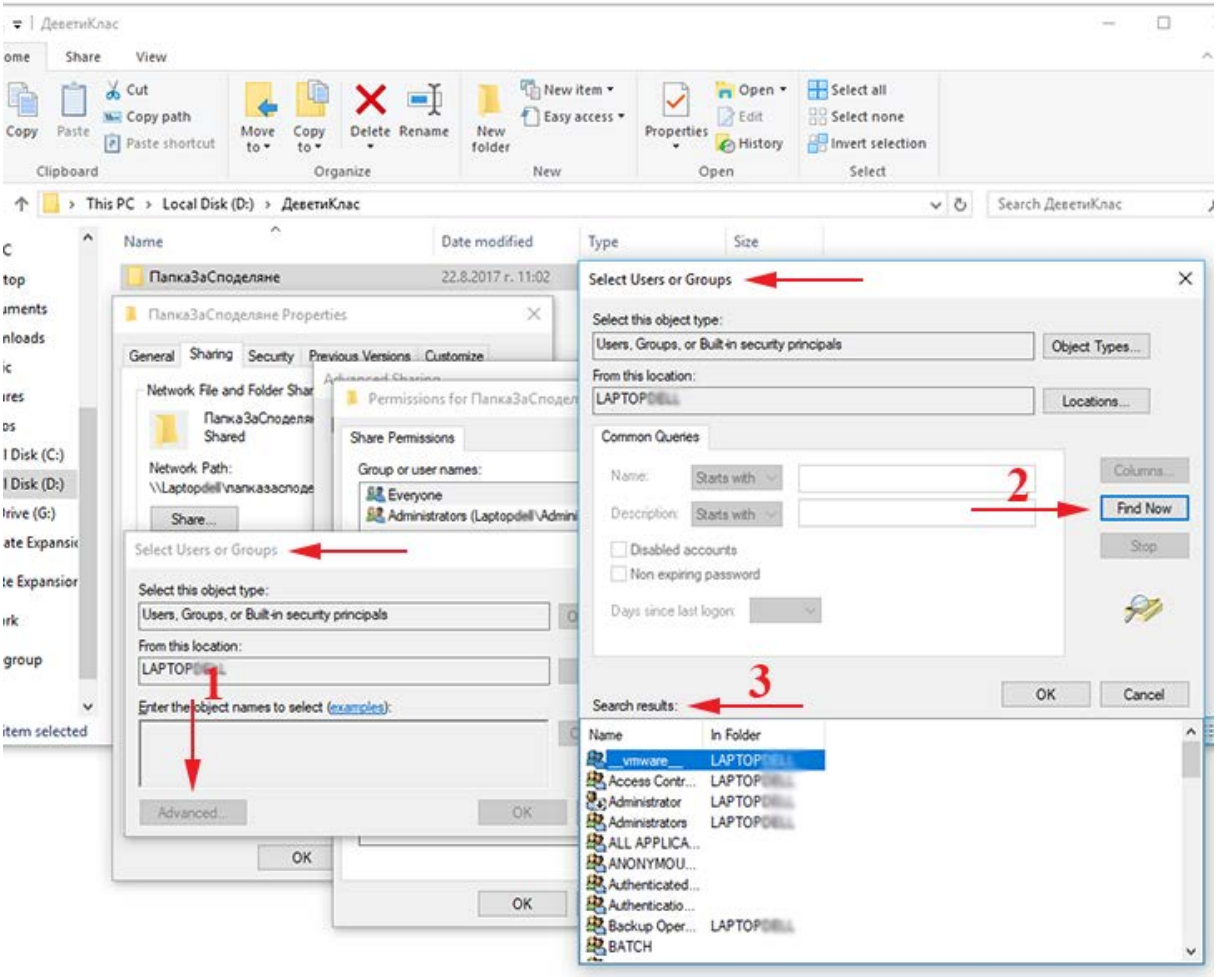
- *Full Control* – включва всички привилегии от *Change* като добавя възможности за промяна на позволения за файлове и вземане на собствеността върху тях.




**фигура 1** *Използване на* ***Advanced Sharing***

Друг потребител или група може да се добави от бутона *Add*. От серията прозорци с наименование *Select Users or Groups* (фигура 2) се избира

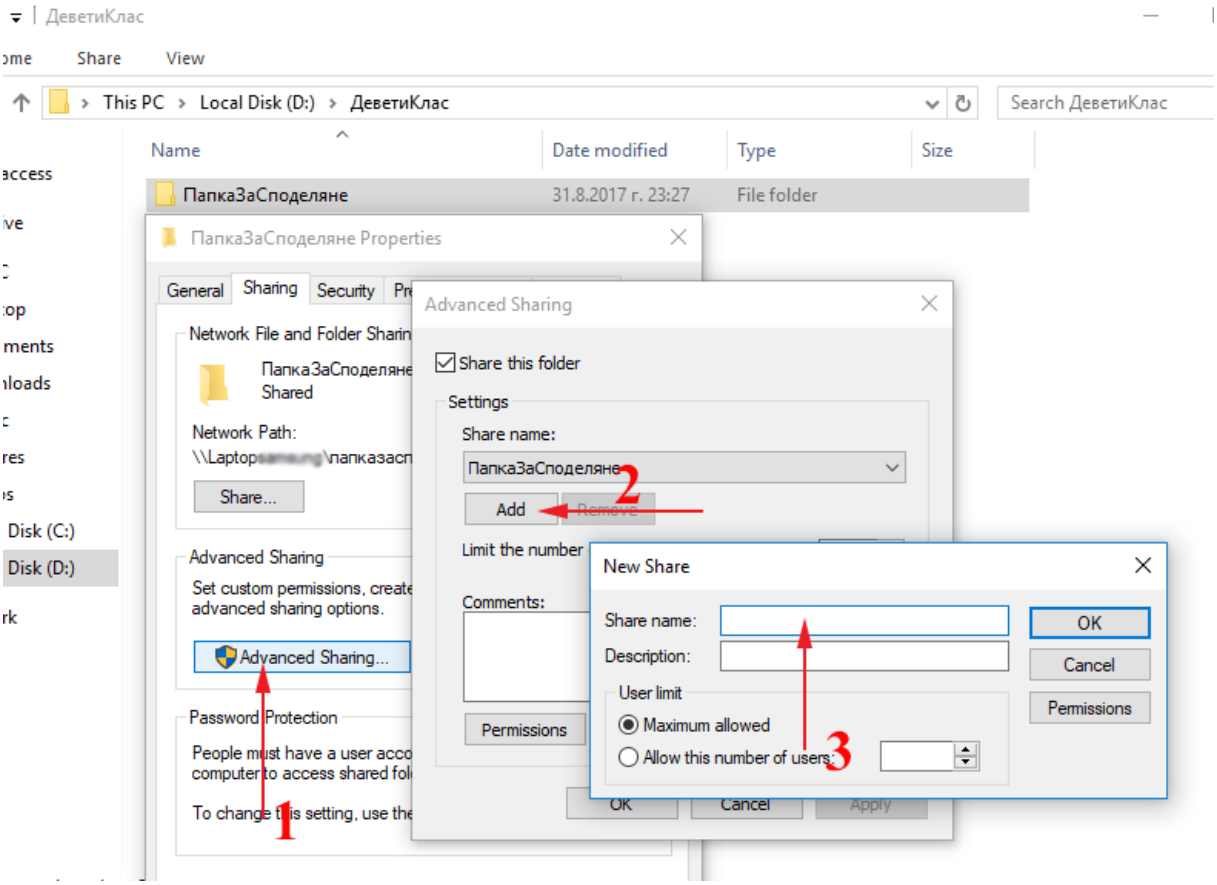
бутонът *Advanced*, след което *Find Now*. В получените резултати са предложени всички възможни варианти за избор.




**фигура 2** *Добавяне на друг потребител или група*

Използването на опцията *Advanced Sharing* не извършва модификации в секцията *Security*, свързани с целевата група или потребител, затова е необходимо те да се направят допълнително и да са съобразени с предварително зададените права.

Windows 10 позволява и възможност за отдаване на даден ресурс под различни имена с различни позволения за достъп за различните потребители и групи. За извършване на това действие е необходимо да се използва бутона *Add* от прозореца *Advanced Sharing*, показан на фигура 3.




**фигура 3** *Отдаване на ресурс под различно име*

Някои действия и съвети, свързани с управлението на споделените ресурси и задаването на позволения за тях, могат да бъдат представени по следния начин:

- Определят се потребителите, групите и техните позволения за необходимите им ресурси.
- Възможността за обединяване на потребители в групи улеснява процеса по задаване на позволения върху споделените ресурси.
- Позволенията трябва да се задават пестеливо.
- Ресурсите се организират така, че папки имащи еднакви изисквания за сигурност, да бъдат разположени в обща папка, след което само тя да бъде споделена.
- Назначените имена на споделените ресурси трябва да осигуряват лесното им разпознаване и намиране от потребителите, както и да се поддържат от всички операционни системи.