



**ИКОНОМИЧЕСКИ УНИВЕРСИТЕТ - ВАРНА**

**КАТЕДРА „ИНФОРМАТИКА”**

---

# ОС UNIX

**УПРАЖНЕНИЕ 4: МОНТИРАНЕ И УПРАВЛЕНИЕ НА ФАЙЛОВИ  
СИСТЕМИ. ПОТРЕБИТЕЛСКИ АКАУНТИ И ГРУПИ**



**Изготвил: гл. ас. д-р Радка Начева**

**ДАТА: 16 СЕПТЕМВРИ 2019 Г.**



## УПРАЖНЕНИЕ 4: ПОТРЕБИТЕЛСКИ АКАУНТИ И ГРУПИ

### I. ЦЕЛ И ТЕМИ НА УПРАЖНЕНИЕТО

**Целта** на упражнението е да въведе студентите в използваните инструменти за управление на потребителски акаунти и групи под Mint, както и на особеностите на правата за достъп под Linux.

**Темите**<sup>1</sup>, засегнати в упражнението, са:

1. Въведение в управлението на потребителски акаунти и групи в Mint;
2. Инструментариум за управление на акаунти и групи.

Като краен резултат от изпълнение на упражнението се очаква студентите да придобият знания и умения относно: създаване на акаунти и групи, редактиране на права за достъп на акаунти и групи до файлове, директории, дялове и дискове; назначаване на група за конкретен акаунт и др.

---

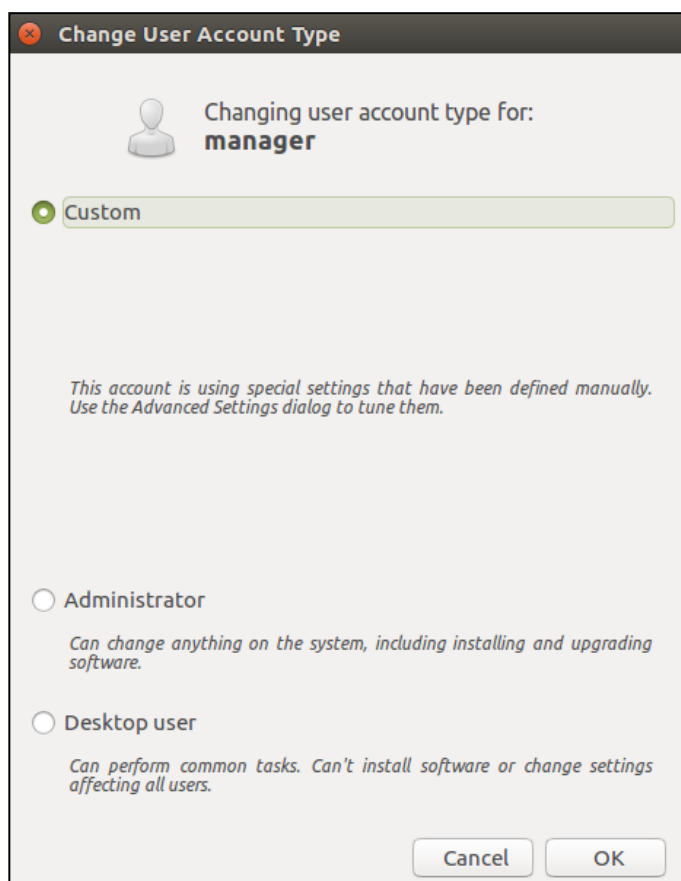
<sup>1</sup> **Забележка:** Някои от поставените теми могат да се разглеждат в теоретичната част на упражнението, а други – в практическата.

## II. ТЕОРЕТИЧНА ПОДГОТОВКА

### 1. Въведение в управлението на потребителски акаунти и групи в Mint

#### Типове акаунти

Типовете акаунти могат да са администраторски, десктоп потребител и с акаунт с настройки по избор (Фиг. 1).



Фиг. 1. Типове акаунти

В Mint може да се създава и гост акаунт. Той има право за преглед на файлове, но не и за работа с административни инструменти на системата и изпълнение на административни задачи в команден режим, като цяло. Няма парола по подразбиране.



## Дисциплина „Операционни системи UNIX“

### Права за достъп

Правата за достъп до конкретен ресурс в Linux зависят от това дали потребителят е собственик или е част от конкретна група.

**Собственик на ресурс:** Притежава папка или файл. По подразбиране, това е потребителят, който създава папката или файла.

**Групи:** Всички потребители, които са част от една и съща потребителска група, както и потребителят, създал конкретен файл или папка, имат еднакви права за достъп до файла или папката. Задаването на права за група е подходящо в случай, че много потребители трябва да имат достъп до файлове в конкретна директория.

**Други потребители:** Това са потребители, които не са собственици на файл или папка и не принадлежат на групата, която има достъп до конкретния ресурс.

**Потребителите има три вида права:** Четене (Read), Запис (Write) и Изпълнение (Execute).

**Read (r):** отваряне на файл / папка и преглед на съдържанието.

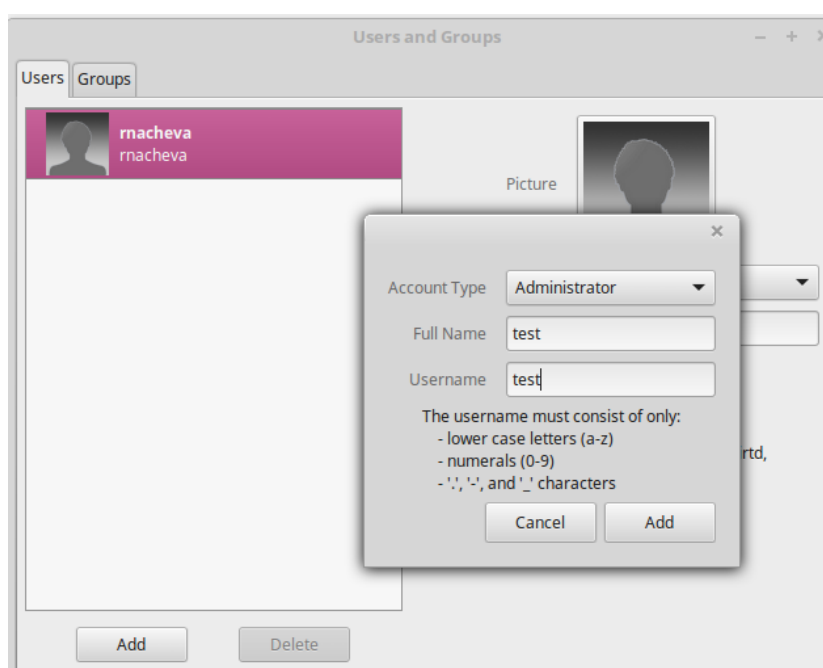
**Write (w):** права за презаписване, добавяне на съдържание или изтриване на файл или папка.

**Execute (x):** право за стартиране на файл (например, скрипт, програма).

В зависимост от типа на акаунта, потребителят има различни привилегии за достъп до ресурсите на системата. Те могат да бъдат прегледани на <https://wiki.ubuntu.com/Security/Privileges>.

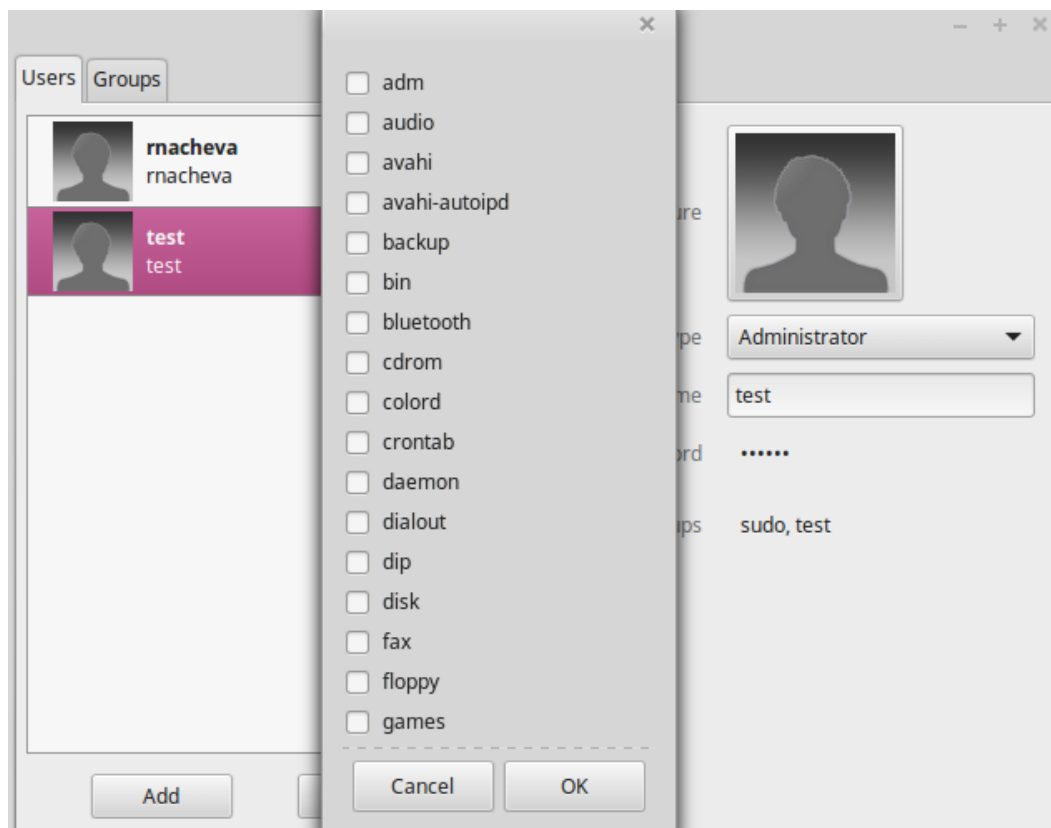
**Дисциплина „Операционни системи UNIX“****2. Инструментариум за управление на акаунти и групи****Потребителски акаунти**

Основни операции по управление на **потребителски акаунти** (създаване, редактиране на основни данни и изтриване) в Mint става от **Preferences -> Users and Groups**. Достъп получавате след въвеждане на парола за автентикация. Нов потребител се добавя от Add. Изтриване на потребител – от Delete. Вж. Фиг. 2.

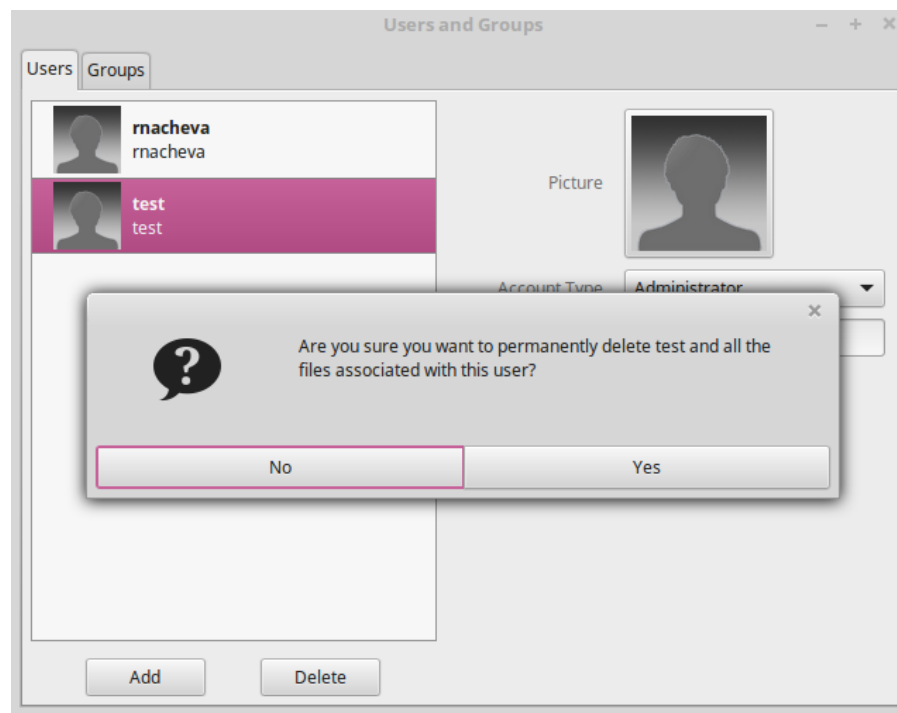


**Фиг. 2. User Accounts - 1**

При добавяне на нов акаунт (Фиг. 2) се въвеждат тип (стандартен или администратор), пълно име и потребителско име. Ако не сте задали групи и парола на акаунта, можете да го направите допълнително – вж. Фиг. 3.

**Дисциплина „Операционни системи UNIX“****Фиг. 3. User Accounts - 2**

При изтриването на акаунти се предлагат възможности за запазване на файловете на потребителите или изтриването им. Вж. Фиг. 4.

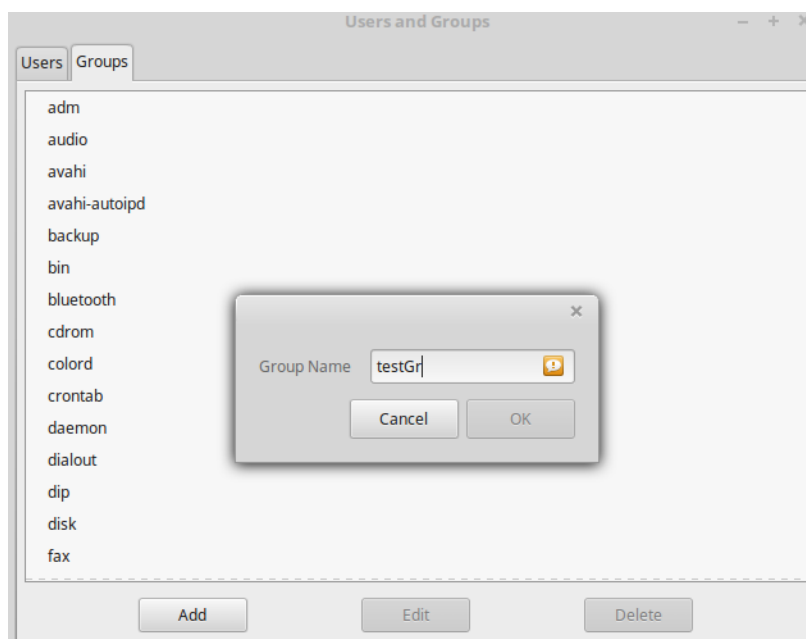
**Дисциплина „Операционни системи UNIX“****Фиг. 4. User Accounts - 3**

Още информация за управлението на потребителски акаунти е публикувана на <https://www.youtube.com/watch?v=waehiTIuOFI>.

**Потребителски групи**

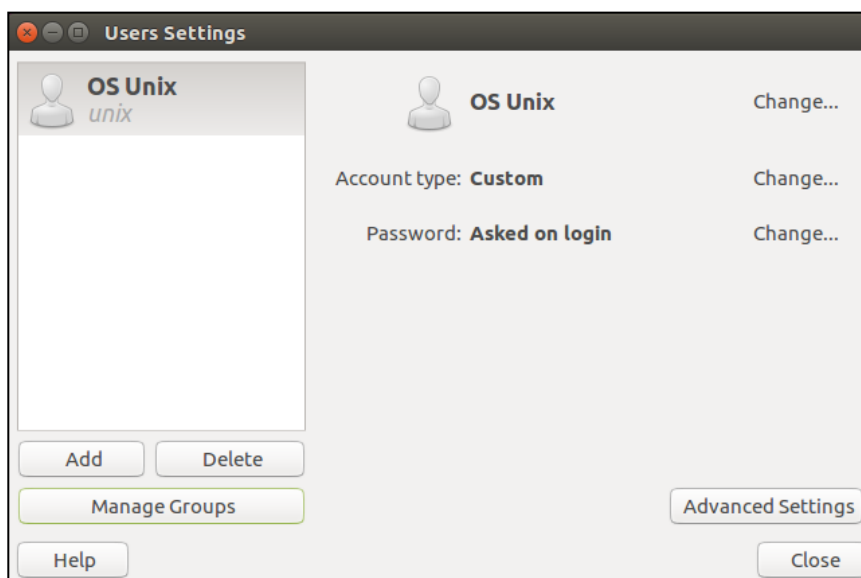
Основните операции по управление на **потребителски групи** (създаване, редактиране, изтриване, добавяне и премахване на потребители) се извършват от стандартното приложение на Mint – Users and Groups (Фиг. 5).

## Дисциплина „Операционни системи UNIX“



Фиг. 5. Основен екран на Users and Groups

Аналогичен инструмент може да се инсталира с команда **sudo apt-get install gnome-system-tools** – вж. Фиг. 6 При проблем с инсталацията, изпълнете първо команда **sudo apt-get update** и след това отново командата за инсталиране на аналогичния Users and Groups.

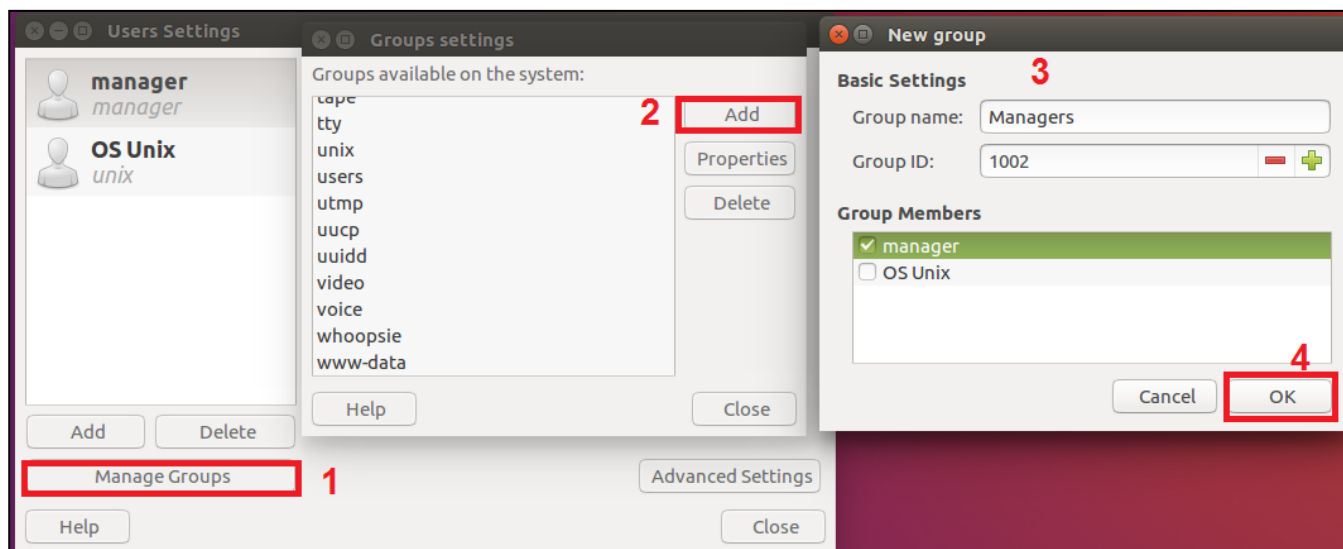


Фиг. 5. Основен екран на Users and Groups(gnome-system-tools)



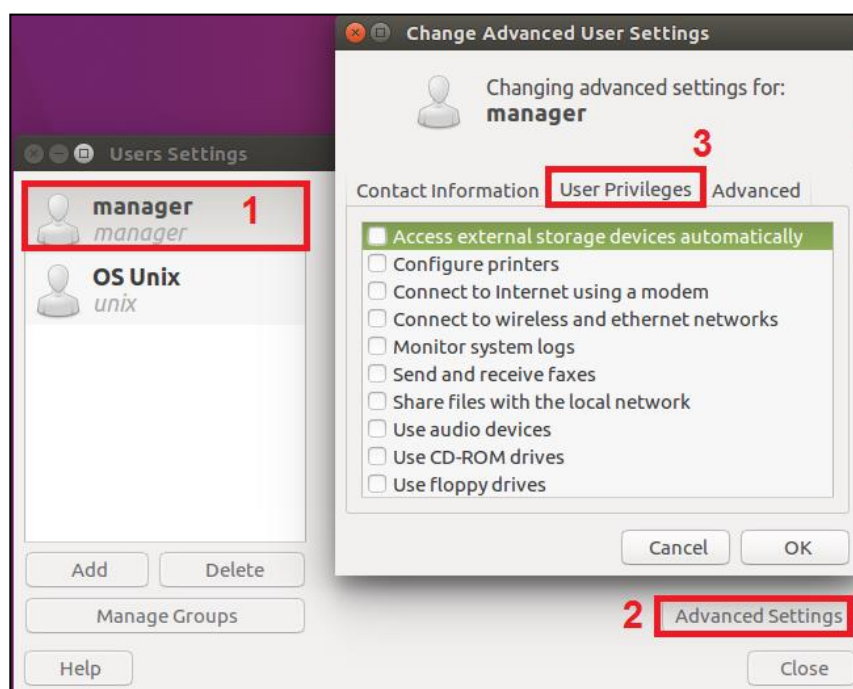
**Дисциплина „Операционни системи UNIX“**

Добавянето на група е показано на Фиг. 7. Може да се осъществи след въвеждане на администраторската парола.



Фиг. 7. Добавяне на група от Users and Groups (gnome-system-tools)

На Фиг. 8 са показани стъпките на задаване на привилегии за конкретен потребител.



Фиг. 8. Редактиране на привилегии на потребител от Users and Groups (gnome-system-tools)



## Дисциплина „Операционни системи UNIX“

Повече за управлението на потребителски акаунти и групи може да прегледате на <https://www.youtube.com/watch?v=ZNeWntArcOg>.

### III. ПРАКТИЧЕСКА ЧАСТ

1. Като системни администратори имате за задача да изпълните следните условия:

- a. Добавете нов виртуален диск 3GB с наименование “MyDisk”.
- b. Дискът трябва да е разделен на два дяла (2GB:1GB), всеки от които трябва да е форматиран в различна файлова система. Поне едната файлова система трябва да позволява пълно възстановяване на информационната структура на дяла в случай на проблеми, като внезапно спиране на хранването.
- c. Монтирайте дяловете.
- d. На всеки от дяловете създайте по една папка, в която трябва да има записан поне по един файл (текстов, изображение или друг по Ваш избор). Извършете компресиране на папките във формат \*.zip, като назначите парола за достъп.
- e. Променете приложението по подразбиране, с което се управляват архивите.
- f. Трябва да ограничите правата за достъп до по-големия дял на диска или ако предпочитате, до целия диск. Вж. [File Permissions](#).
- g. Потърсете инструмент/и, с който трябва да извършите криптиране на произволен дял от новия диск и съответно на целия диск. Например, [TrueCrypt](#). Изпълняват се последователно командите:



## Дисциплина „Операционни системи UNIX“

- *sudo add-apt-repository ppa:stefansundin/truecrypt*
- *sudo apt-get update*
- *sudo apt-get install truecrypt*

2. Направете следните потребителски групи: Managers и Assistants.

3. Трябва да създадете следните потребители, като всеки от тях има парола по Ваш избор:

- Администратор (admin) – част от групата на администраторите,
- Управител на фирма (manager) – част от група Managers, стандартен потребител;
- Офис сътрудник (assistant1) – част от група Assistants, стандартен потребител;
- Стажант (assistant2) – част от група Assistants, стандартен потребител.

3. Криптирайте /home директорията на администраторския акаунт admin:

- в терминала изпълнявате команда *sudo apt-get install ecryptfs-utils cryptsetup*;
- изпълнявате в терминала команда *sudo ecryptfs-migrate-home -u admin*;
- направете *Log out* и влезте в системата като администратор (с потребител *unix*).

4. Променете наименованието на някой от виртуалните дискове, създадени по време на предходни упражнения, на Managers.

5. Нека администраторският акаунт *unix* да бъде част от групата root.

6. Нека новият администраторски акаунт *admin* да бъде от група *sudo*.

7. На диска Managers направете папка с име *manager*. Като използвате следните команди променете собственика и групата, които да имат достъп до папката:

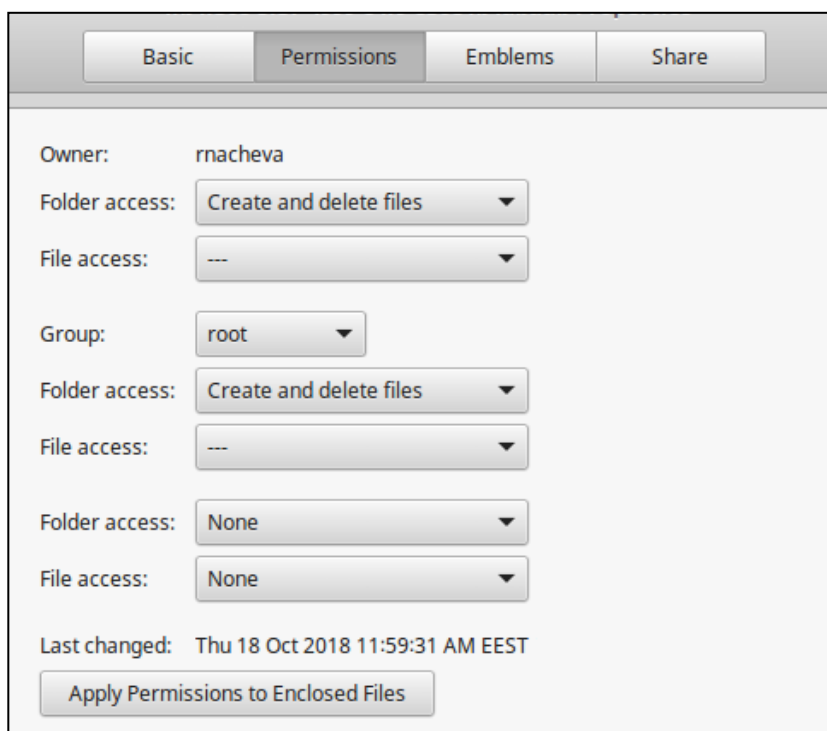
**Дисциплина „Операционни системи UNIX“**

*sudo chown manager /пълен път до папката/*

*sudo chgrp managers /пълен път до папката/*

*/пълен път до папката/* - замества се с абсолютния адрес на директорията, който можете да проверите от свойствата ѝ.

8. Ограничете достъпа на представителите на всички останали потребители до диска Managers (десен бутон върху диска -> Properties -> Permissions: Фиг. 9). Влезте с някой от създадените по-рано акаунти, за да тествате дали сте задали коректно ограничението. Трябва да работите с административен акаунт, който е група root.



**Фиг. 9. Редактиране на права за достъп до конкретен ресурс**

9. Инсталирайте Users and Groups: **sudo apt-get install gnome-system-tools**.

10. Нека групата assistant1 няма право да използва аудио и видео устройства (използва се Users and Groups от зад. 8).

11. Нека assistant2 да няма право на достъп до безжична мрежа (използва се Users and Groups от зад. 8).



## Дисциплина „Операционни системи UNIX“

12. Нека на `assistant2` да бъде наложено ограничение за използване на системата по дни. Можете да използвате инструмента [Timekpr](#) или аналогичен, по Ваш избор.

### IV. ЗАДАЧИ ЗА САМОСТОЯТЕЛНА РАБОТА

1. Потърсете допълнителен инструментариум, с който можете да управлявате файловата система на Mint.
2. Потърсете начин (чрез потребителския интерфейс или в команден режим) да забраните Guest акаунта.

### V. УКАЗАНИЯ ЗА РЕШАВАНЕ НА ПОСТАВЕНИТЕ ЗАДАЧИ ЗА САМОСТОЯТЕЛНА РАБОТА

1. За изпълнение на задача 2 можете да следвате предложените стъпки в урока <https://goo.gl/aFiAhq>.

### VI. ВЪПРОСИ ЗА САМОПРОВЕРКА

1. Какви типове потребители можете да създавате в Mint?
2. Какви права за достъп по подразбиране до конкретен ресурс има неговият собственик?

### VII. ОБОБЩЕНИЯ И ДОПЪЛНИТЕЛНА ЛИТЕРАТУРА

Допълнителна литература:

1. [Файлова структура на Linux](#)
2. [User accounts](#)