ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ МОЛДОВЫ

ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАТИКИ

ДЕПАРТАМЕНТ ИНФОРМАТИКИ

**Лабораторная работа № 1**

по курсу “Securitatea Sistemelor Informatice”

**Тема**: Управление правами доступа к файлам и папкам в ОС (Windows, Linux)

Проверила: Novac L. Dr. Conf. univ.   
Выполнил:Mamaliga Artur gr I2302,

**Основные моменты теории:**

Типы учетных записей Windows:

Администраторские учетные записи предоставляют полный доступ к системе, включая установку программ, изменение ключевых настроек и управление другими учетными записями. Для снижения рисков рекомендуется минимизировать их использование.

Стандартные учетные записи имеют ограниченные возможности: пользователи могут запускать приложения и работать с файлами, но не могут вносить существенные изменения в систему, что делает их более безопасными для повседневных задач.

Детские учетные записи позволяют родителям устанавливать ограничения на использование ПК детьми, а также контролировать доступ к контенту через настройки семейной безопасности в Windows.

Политики безопасности Windows:

Локальная политика безопасности определяет доступ к системе, включая права на выполнение административных задач и доступ к ресурсам, таким как файлы и папки. Эти настройки помогают защитить компьютер от несанкционированного доступа.

Файловая система NTFS поддерживает списки контроля доступа (ACL), которые позволяют детализировать права доступа к файлам и папкам. В отличие от FAT и FAT32, NTFS предпочтительна для обеспечения безопасности на уровне файловой системы.

Идентификаторы безопасности (SID):

SID (Security Identifier) — это уникальный идентификатор, присваиваемый пользователям, группам и компьютерам. При входе в систему операционная система создает маркер доступа, содержащий SID пользователя и его групп, который используется для контроля доступа к защищаемым ресурсам.

Дескрипторы безопасности содержат информацию о правах доступа к объектам, таким как файлы и папки, включая возможности чтения, записи и выполнения.

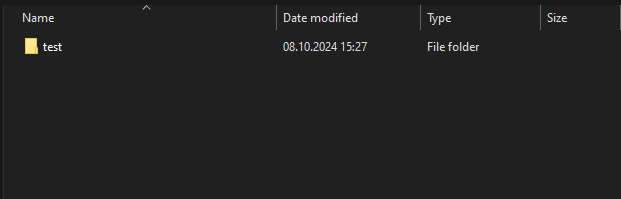
Механизм контроля доступа:

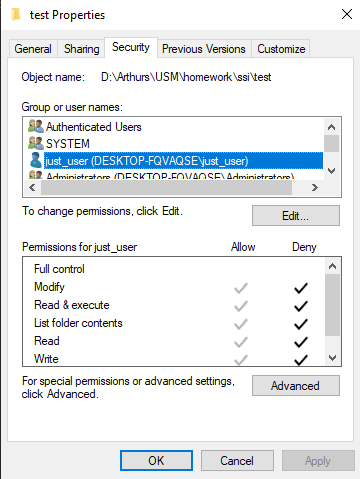
Для каждого защищаемого объекта (например, файл или папка) создается ACL (список контроля доступа), который сравнивается с маркером доступа пользователя. Если SID пользователя есть в списке и ему предоставлены необходимые права, доступ разрешается.

Приоритет разрешений: если у пользователя имеются как разрешения, так и запреты, запреты имеют приоритет. Например, если пользователю разрешено чтение файла, но группе, к которой он принадлежит, доступ запрещён, то доступ будет заблокирован.

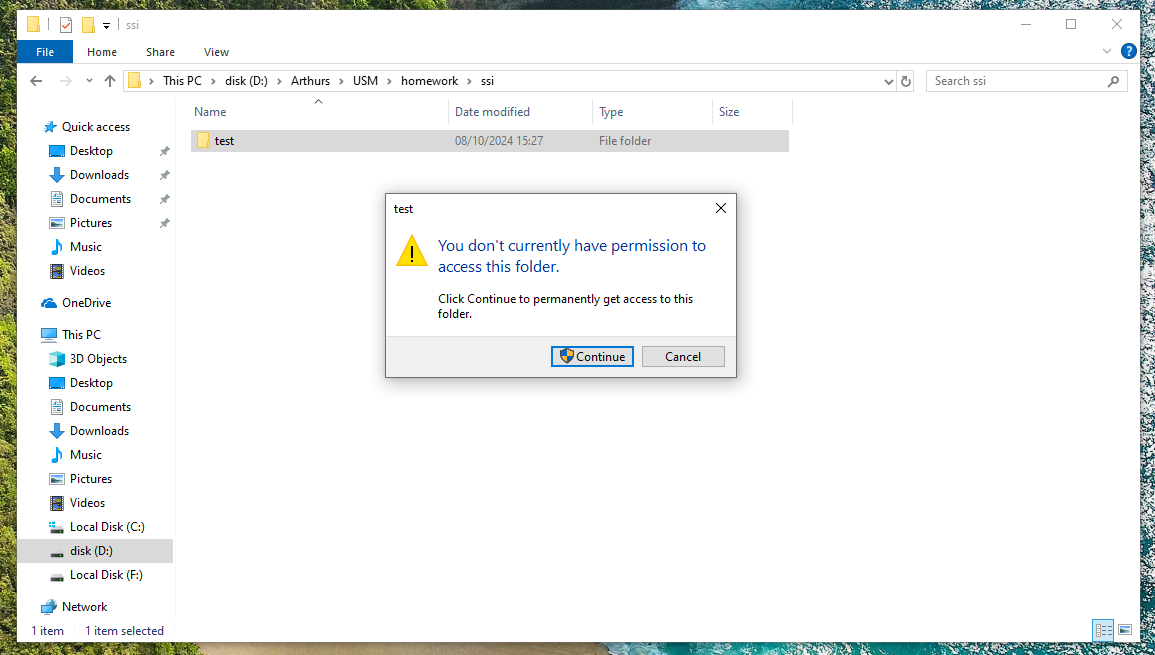
Эти принципы были использованы при выполнении первой лабораторной работы.

Создаю папку в уч. записи администратора



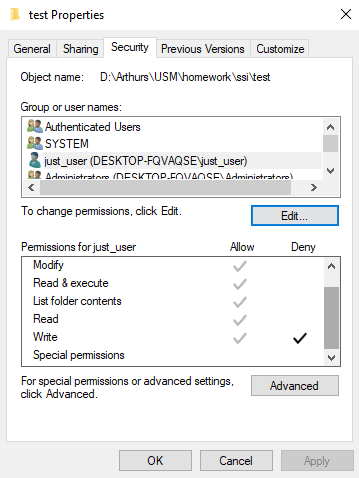


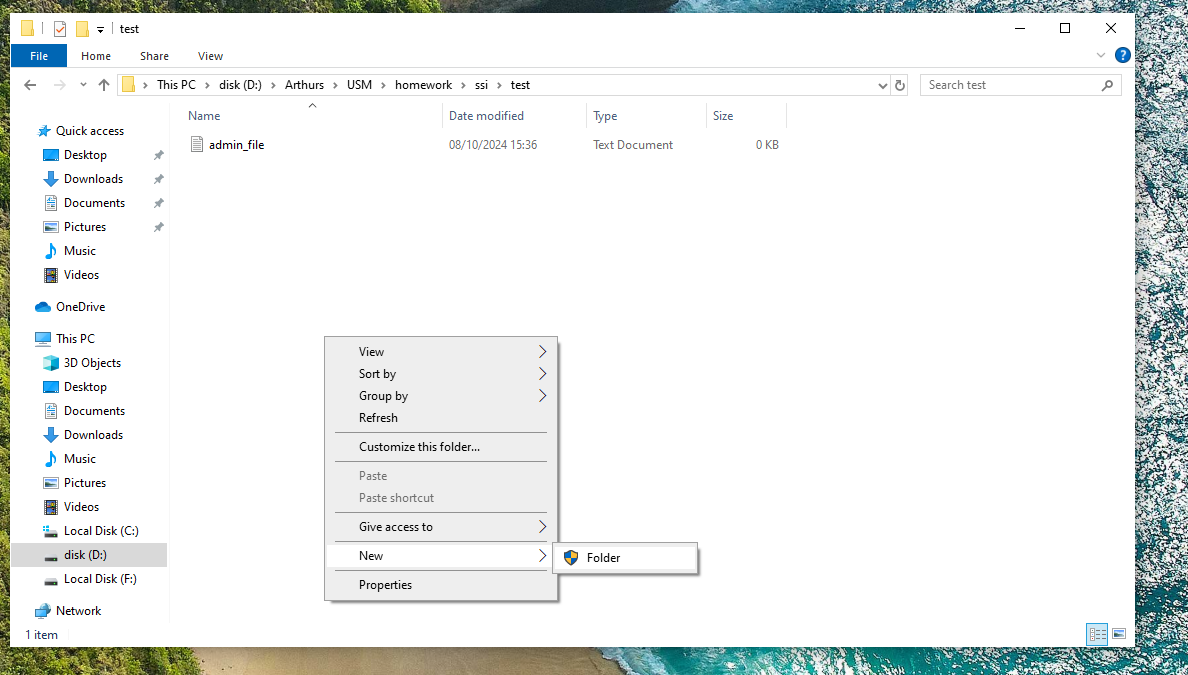
Далее заходим в св-ва данной папки и ставим галочки на полный запрет взаимодействию пользователя just\_user с папкой Test



После смены учетных записей становится видно, что обычный пользователь, после внесения изменений в настройки, не может получить доступ к этой папке и работать с ней.

Затем, используя учетную запись 1 (1 — администратор, 2 — пользователь), я предоставляю пользователю права на просмотр содержимого папки, но остальные действия для него по-прежнему запрещены. После создания текстового файла под учетной записью администратора я переключаюсь на пользователя и вижу, что могу читать файлы и просматривать содержимое папки. Однако, из-за запрета на запись, мне не удается добавлять новые файлы или изменять уже существующие.





Затем я проверил каждый пункт из списка прав доступа и составил краткое описание:

Изображение показывает список прав доступа к файлам и папкам в операционной системе Windows (особенно в файловой системе NTFS). Вот объяснение каждого права:

1. Полный доступ:

- Дает все возможные разрешения на файл или папку, включая чтение, запись, изменение, удаление, а также управление правами доступа для других пользователей. Обладатель полного доступа может совершать любые действия с объектом.

2. Изменение:

- Позволяет пользователю читать, записывать и редактировать содержимое файлов или папок, но без возможности изменения прав доступа или владения объектом. Можно изменять данные, но нельзя управлять разрешениями.

3. Чтение и выполнение:

- Дает пользователю возможность открывать и читать файлы, а также запускать программы или скрипты. Это означает, что пользователь может просматривать содержимое и запускать исполняемые файлы.

4. Список содержимого папки:

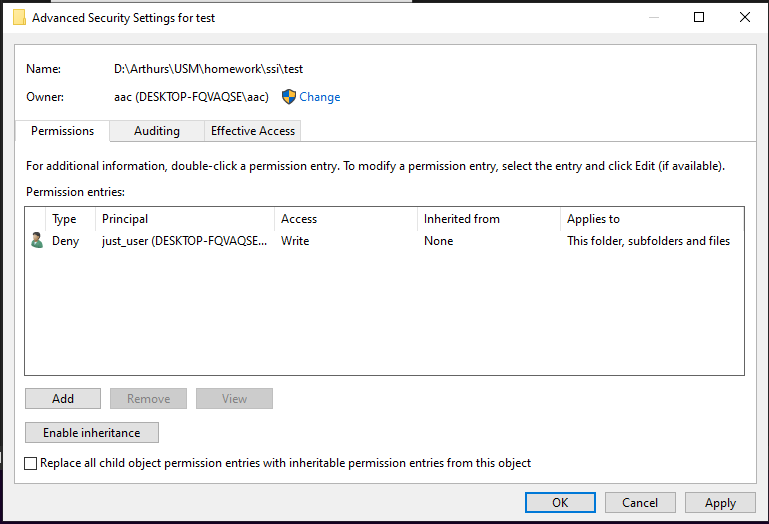
- Применимо только к папкам. Позволяет пользователю видеть список файлов и подпапок внутри директории, но без возможности открытия или изменения их содержимого.

5. Чтение:

- Предоставляет доступ к просмотру содержимого файлов и папок. Пользователь может открывать файлы для чтения, но не имеет прав на их изменение или выполнение.

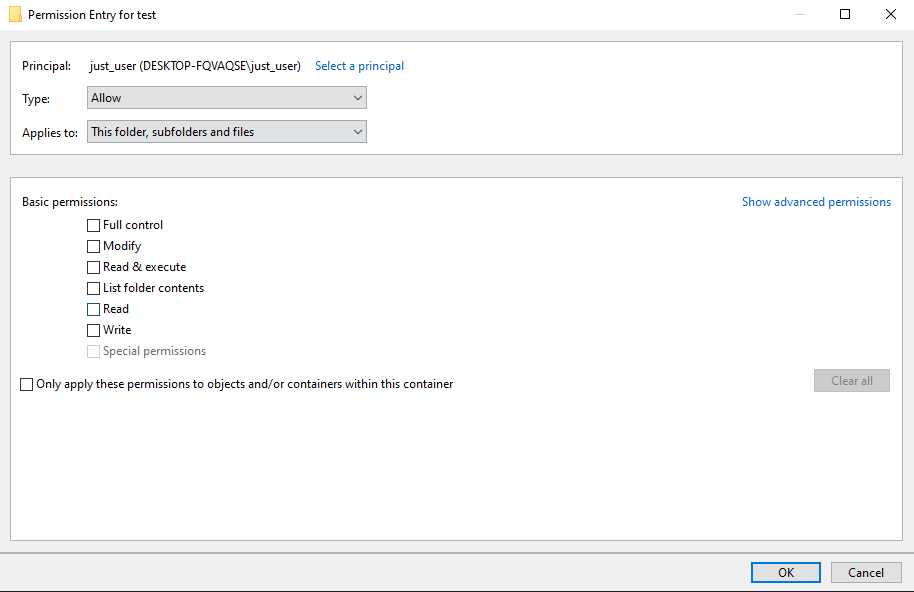
6. Запись:

- Дает пользователю возможность изменять содержимое или создавать новые файлы и папки в директории. Включает право добавлять данные, но не позволяет изменять права доступа или другие атрибуты объекта.

 Продолжая выполнять условия задачи, я отключаю все наследования.

Наследование позволяет автоматически применять одни и те же разрешения ко всем вложенным объектам (файлам и папкам) для пользователей или групп. Это означает, что если пользователь или группа имеют права на родительскую папку, они автоматически получают такие же права на дочерние объекты, когда наследование включено. Пользователи и группы, указанные в ACL родительского объекта, наследуют свои права доступа на файлы и папки внутри этой папки, что облегчает управление доступом в крупных системах.

Однако, минус наследования заключается в том, что без отключения этой функции невозможно установить уникальные права для отдельных файлов или папок. Если необходимо задать уникальные разрешения для конкретного объекта в иерархии, придется отключить наследование, что усложняет управление безопасностью. Это может привести к ситуации, когда разные объекты имеют различные права доступа, что затрудняет администрирование.



Вот описание permissions entry для папки по каждому из указанных пунктов:

1. Full control:

- Позволяет пользователю выполнять любые действия с папкой. Это включает возможность читать, записывать, изменять, удалять файлы и подпапки, а также изменять разрешения и владение самой папкой. Пользователь с этим правом может полностью управлять содержимым папки.

2. Modify:

- Позволяет пользователю читать и записывать содержимое папки, а также удалять файлы и подпапки. Однако это право не включает возможность изменять разрешения или владение папкой. Пользователь может изменять данные, но не управлять доступом к папке.

3. Read and execute:

- Позволяет пользователю открывать и читать файлы внутри папки, а также запускать исполняемые файлы. Это право не дает возможности изменять содержимое папки или добавлять новые файлы.

4. List folder contents:

- Позволяет пользователю просматривать список файлов и подпапок внутри данной папки. Это разрешение не дает права открывать или изменять содержимое этих файлов или подпапок, но дает возможность видеть, что находится внутри папки.

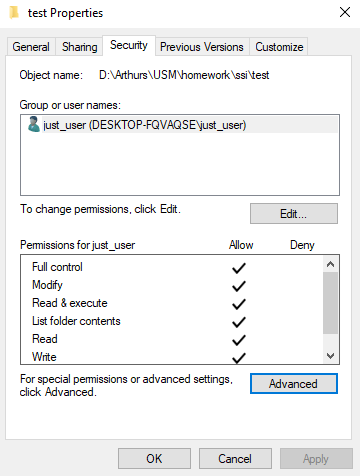
5. Read:

- Позволяет пользователю просматривать содержимое файлов и папок. Пользователь может открывать файлы для чтения, но не может их изменять или выполнять. Это право предоставляет доступ только для просмотра.

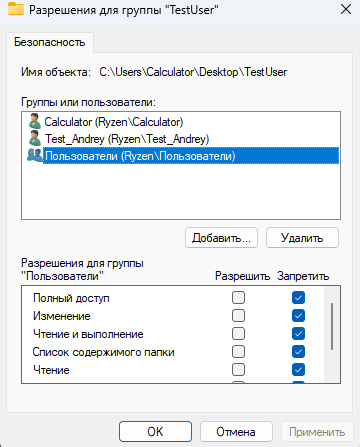
6. Write:

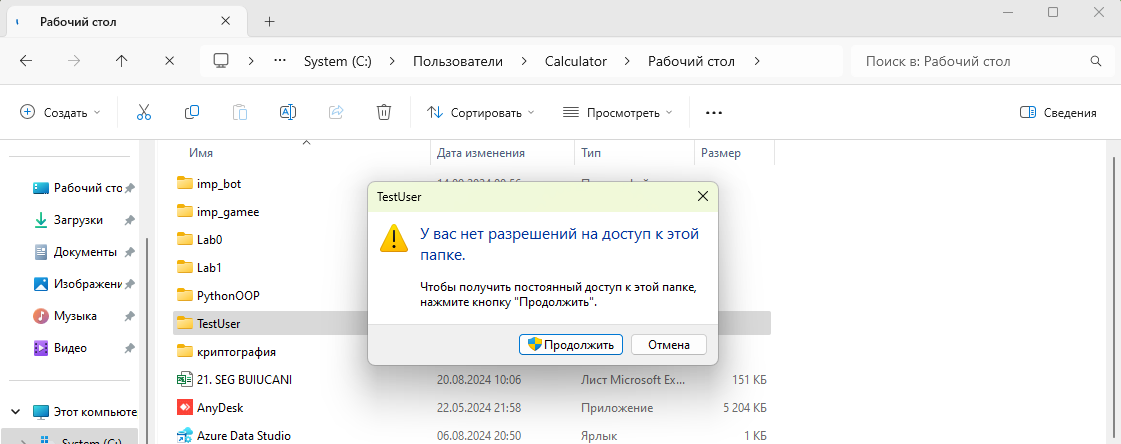
- Позволяет пользователю добавлять новые файлы или изменять содержимое существующих файлов в папке. Это разрешение дает возможность записывать данные, но не позволяет изменять другие атрибуты папки, такие как права доступа.

Даю пользователю полный доступ к папке



Далее добавляю группу пользователей и уже ей запрещаю полностью взаимодействовать с данной папкой



Как видно, несмотря на то, что пользователь 2 имеет полный доступ к взаимодействию с папкой, запрет имеет более высокий приоритет.

Тем не менее, разрешения будут суммироваться. Например, если мой пользователь имеет право читать и выполнять файлы объекта, а его группа обладает разрешением на создание файлов и запись данных, то полномочия этого пользователя объединяются.