Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и кибербезопасности
Высшая школа программной инженерии

Лабораторная работа №4

Изучение реализации дискреционной модели доступа в ОС Windows

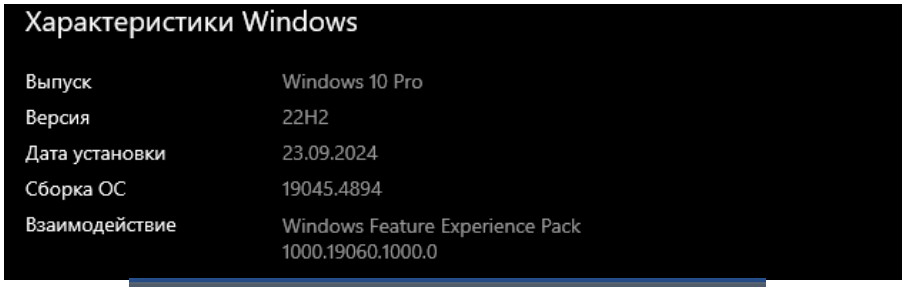
по дисциплине «Информационная безопасность»

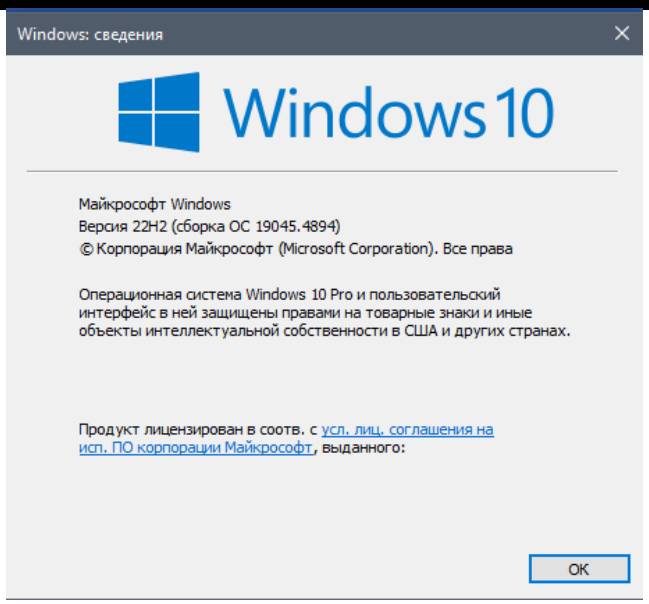
Выполнил
студент гр. 5130903/10302 А.А. Лихачева
<подпись>

Руководитель
доцент, к.т.н. А.В. Сергеев
<подпись>
«___» _____ 2024 г.

Санкт-Петербург
2024

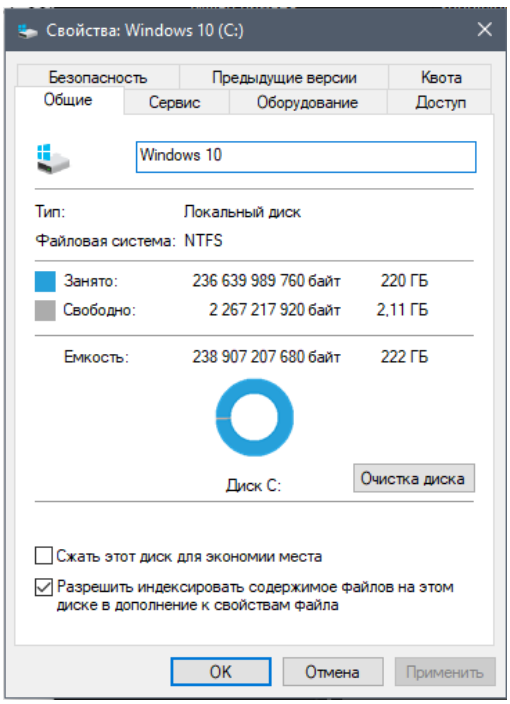
1. Определите какое издание Windows используется на компьютере. Запишите ответ в отчёт.

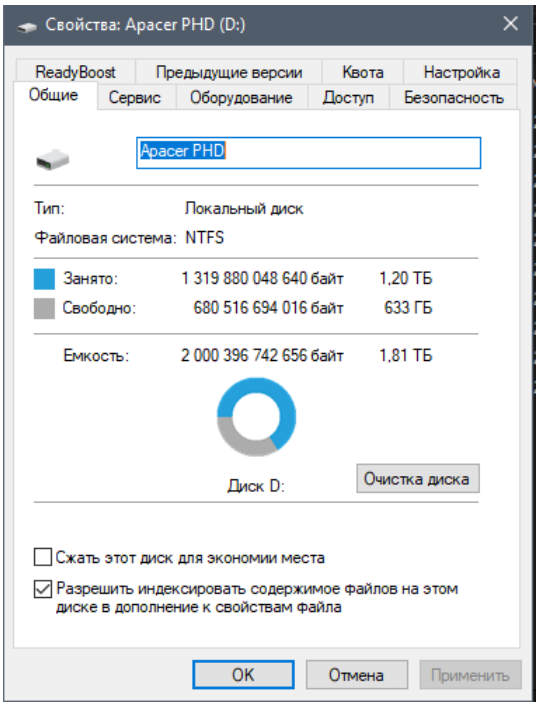




Чтобы узнать издание Windows через системную утилиту (win+R), необходимо ввести команду winrer: текущая версия – Windows 10 Pro, версия 22H2 (сборка 19045,4894).

2. Определите, какая файловая система используется на логических дисках компьютера. Запишите ответ в отчёт.





Локальный диск C: NTFS, внешний жёсткий диск D: NTFS.

NTFS (New Technology File System) — это файловая система Windows, обеспечивающая высокую безопасность данных за счёт разграничения прав доступа, шифрования, сжатия и журналирования операций. Она поддерживает большие объёмы данных и предоставляет возможность использования дисковых квот для управления ресурсами.

3. Пользователи могут быть членами разных групп. Членство в группах определяет права пользователей на доступ к разным папкам, файлам, а также возможность выполнять некоторые действия на компьютере. При установке операционной системы некоторые группы создаются автоматически для упрощения администрирования компьютера.

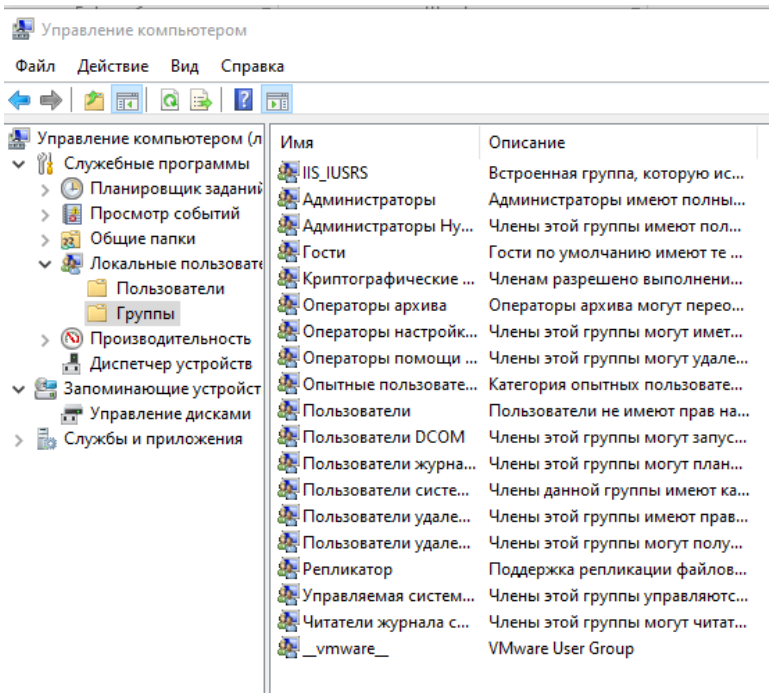
Определите, какие группы присутствуют на компьютере. Для этого сделайте следующее.

3.1. Нажмите правой кнопкой мыши на значок «Компьютер» и выберите «Управление».

3.2. Откроется окно «Управление компьютером». В левой части окна выберите «Локальные пользователи». В правой части окна будут показаны две папки: одна содержит список пользователей, другая список встроенных групп.

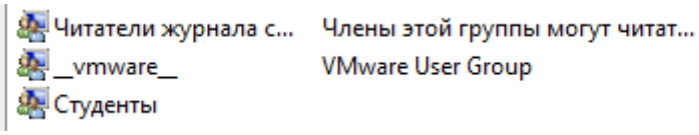
3.3. Выберите папку «Группы». Внесите в отчёт список групп присутствующих на компьютере.

Группы:



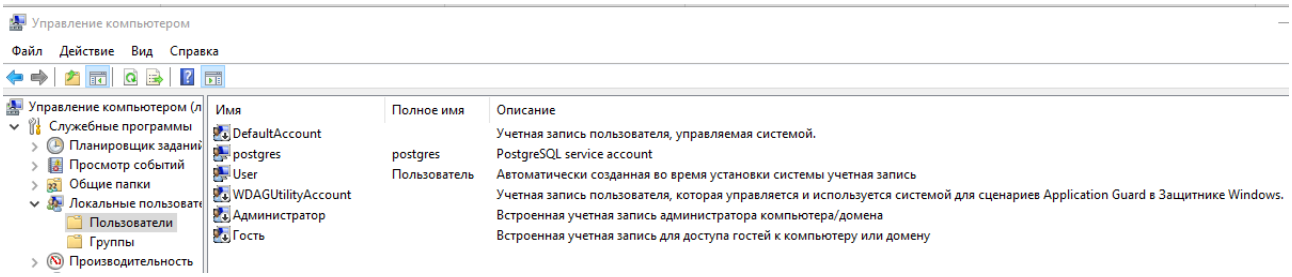
- __vmware__
- IIS_IUSRS
- Администраторы
- Администраторы Hyper-V
- Гости
- Криптографические операторы
- Операторы архива
- Операторы настройки сети
- Операторы помощи по контролю учетных записей
- Опытные пользователи
- Пользователи
- Пользователи DCOM
- Пользователи журналов производительности
- Пользователи системного монитора
- Пользователи удаленного рабочего стола
- Пользователи удаленного управления
- Репликатор
- Управляемая системой группа учетных записей
- Читатели журнала событий

4. Создайте группу с именем «Студенты».



Группа пользователей — это совокупность учетных записей пользователей, объединенных для удобства управления правами доступа и разрешениями. Вместо назначения прав каждому пользователю отдельно, администратор может задать определённые права группе, и все пользователи, входящие в неё, автоматически получают эти права.

5. Посмотрите, какие пользователи зарегистрированы на компьютере.



Пользователи:

- DefaultAccount – стандартная системная учетная запись Windows. Обычно она не используется пользователями и служит для системных задач.
- postgres – относится к суперпользователю (пользователь, который обладает полными правами и привилегиями для выполнения любых операций) по умолчанию в системе управления базами данных PostgreSQL. Эта учетная запись для администрирования базы данных, когда устанавливается PostgreSQL
- User – текущая пользовательская учетная запись.
- WDAGUtilityAccount – учетная запись, используемая для Windows Defender Application Guard (системы защиты от вредоносного ПО). Она автоматически создается Windows и не требует вмешательства пользователя. DAG изолирует потенциально опасные процессы и приложения, создавая безопасную среду , что защищает основную систему от вредоносных программ и угроз.
- Администратор – встроенная учетная запись администратора. Она может быть включена или отключена.
- Гость – встроенная учетная запись для гостевого доступа. Обычно она отключена, но ее можно включить, чтобы предоставлять ограниченный доступ другим пользователям.

6. Создайте двух новых пользователей: student1 и student2.

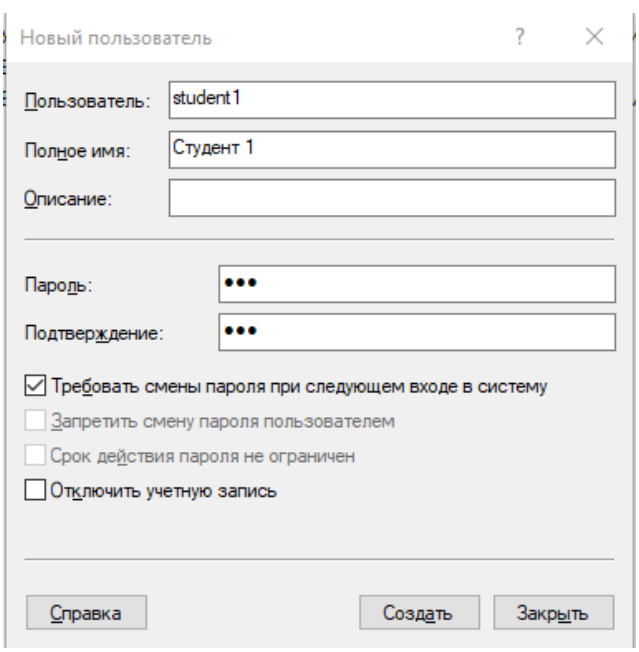
6.1. В окне новый пользователь введите следующие значения.

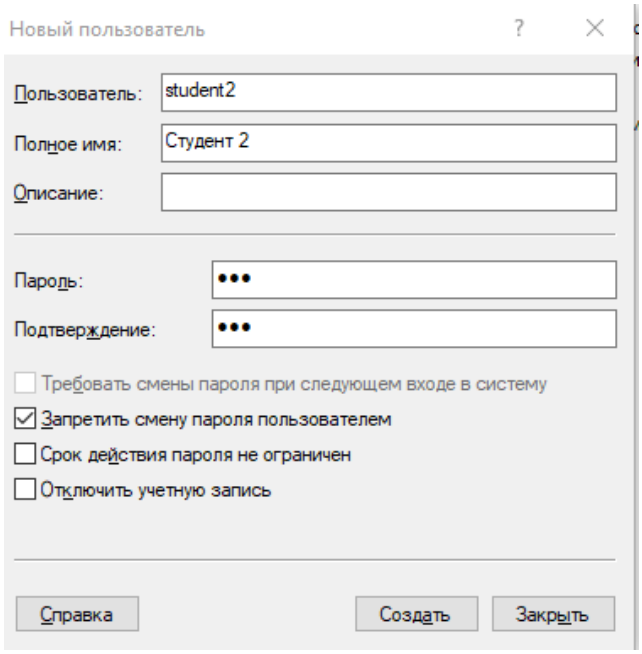
Пользователь: student1
Полное имя : Студент 1
Пароль: 111

6.2. Оставьте галочку у пункта «Требовать смену пароля при следующем входе в систему».

6.3. Нажмите кнопку «Создать».

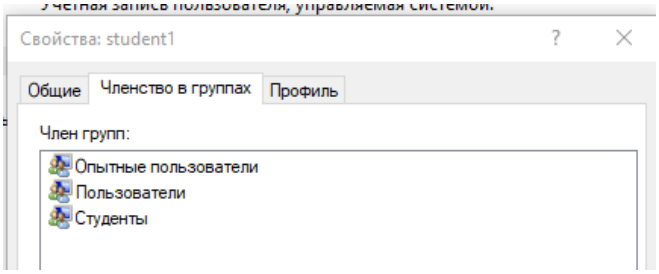
6.4. Пользователя student2 создайте аналогично и задайте пароль 222. Для student2 поставьте галочку напротив пункта «Запретить смену пароля пользователем».

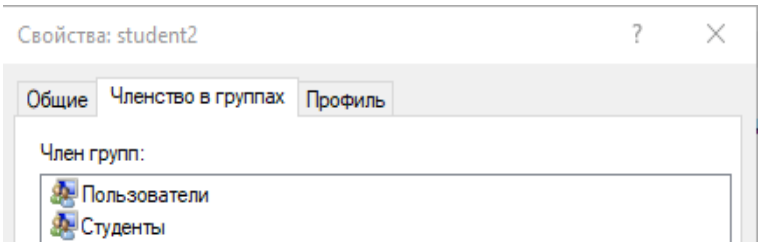




6.5. Добавьте пользователей student1 и student2 в группу «Студенты».

6.6. Пользователя student1 добавьте в группу «Опытные пользователи».

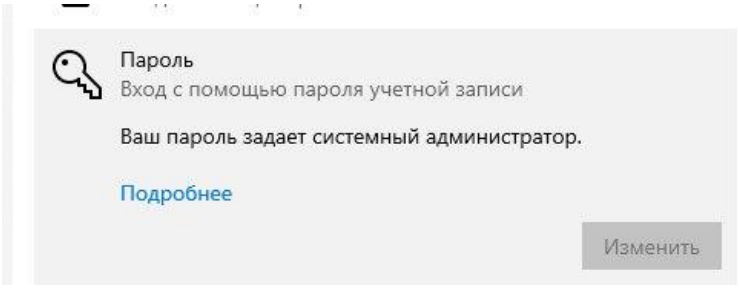




6.7. Опишите, в какие группы входят пользователи student1 и student2.
Оба пользователя входят в группы Пользователи и Студенты, student 1 входит в группу Опытных пользователей.

7. Зайдите под именем student1 и установите постоянный пароль.
При входе в учетную запись был установлен новый пароль для пользователя student1 – 12345.

8. Зайдите под именем student2 и убедитесь, что сменить пароль невозможно.
Для изменения пароля учетной записи student2 требуется пароль администратора:



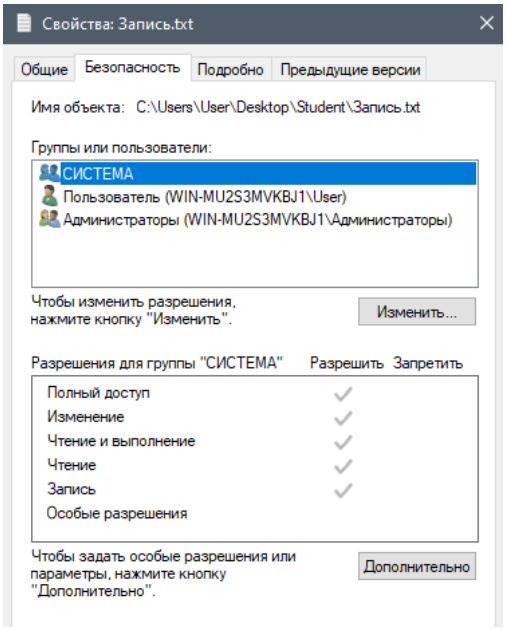
9. Предоставление разных прав доступа.

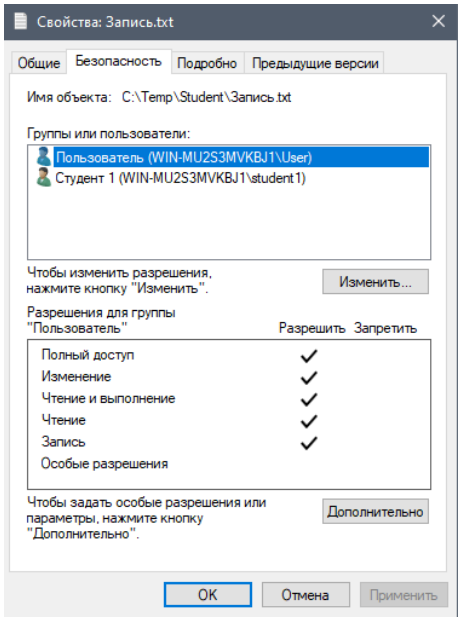
9.1. Создайте папку с именем «Student». В этой папке создайте файл с именем «Запись.txt». Внесите в файл какой-нибудь текст. Укажите, какие и у кого присутствуют по умолчанию права на доступ к созданному файлу.

У владельца, а также групп пользователей «Администраторы» и «Система» имеются полные права;

9.2. Удалите все разрешения на доступ к файлу «Запись.txt». Задайте полный доступ для пользователя, под именем которого Вы работаете. Для пользователя Student1 задайте только право «Запись».

Право на запись – изменение содержимого файла, изменение его атрибутов, а также просмотр владельца файла и разрешений. Содержимое файла нельзя прочитать, но можно записать в файл данные, переименовать и удалить файл

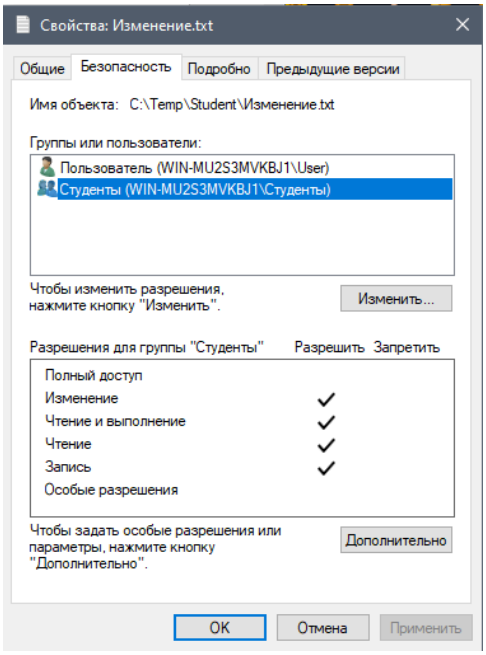




9.3. Создайте файл «Изменение.txt» и внесите в файл какой-нибудь текст. Удалите все разрешения на доступ к файлу. Задайте полный доступ для пользователя, под именем которого Вы работаете. Для группы «Студенты» задайте право «Изменение».

Право на изменение – изменение содержимого файла и удаление файла плюс то, что предусмотрено разрешениями «Запись» и «Чтение и выполнение».

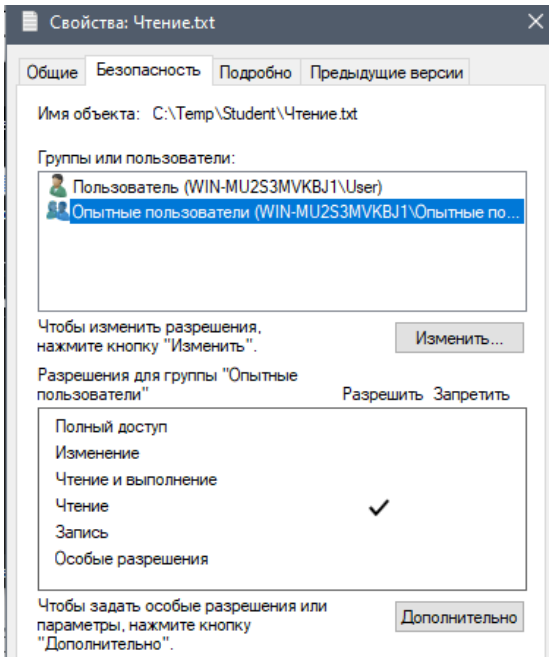
Право на выполнение (чтение и выполнение) – То же что и «Право на чтение» плюс возможность запуска приложения, если файл исполняемый.

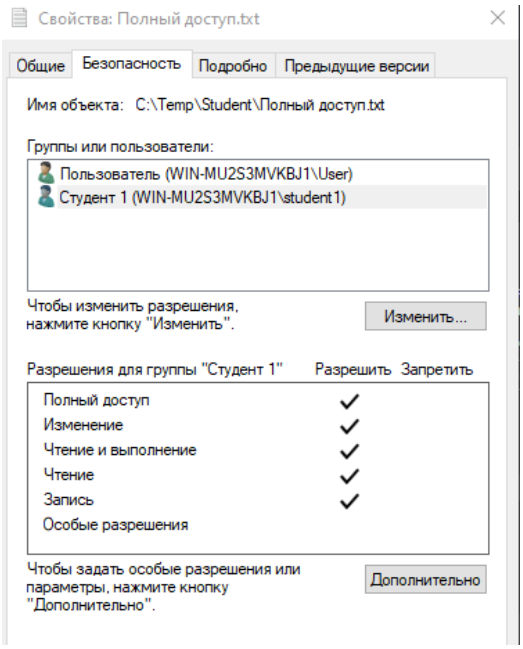


9.4. Создайте файл «Чтение.txt» и внесите в файл какой-нибудь текст. Удалите все разрешения на доступ к файлу. Задайте полный доступ для пользователя, под именем которого Вы работаете. Для группы «Опытные пользователи» задайте право «Чтение».

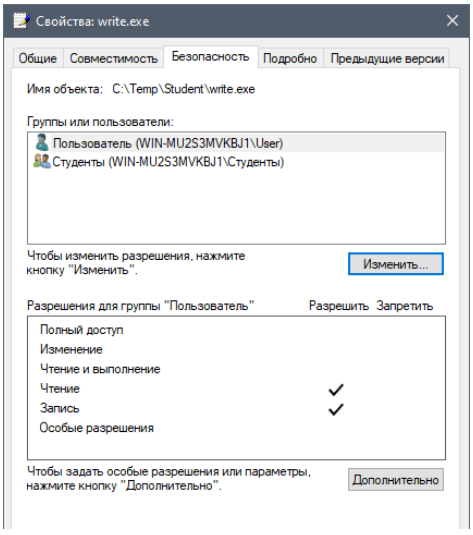
Право на чтение – чтение файла и просмотр его свойств: имя владельца, разрешений и атрибутов. Содержимое файла можно читать, но нельзя изменять. Файл можно переименовывать и удалять.

9.5. Создайте файл «Полный доступ.txt» и внесите в файл какой-нибудь текст. Удалите все разрешения на доступ к файлу. Задайте полный доступ для пользователя, под именем которого Вы работаете и для пользователя Student1.

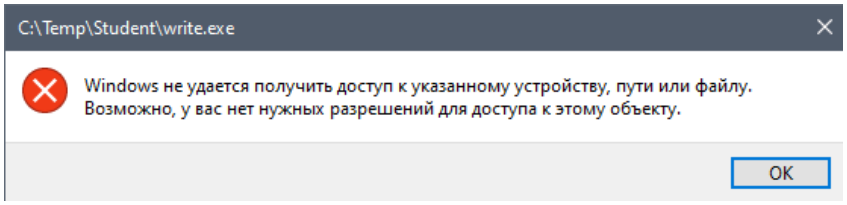


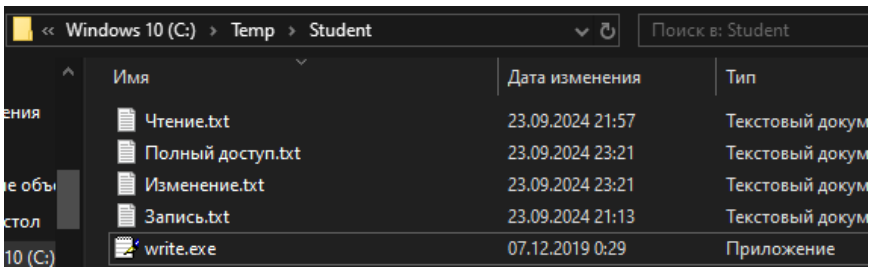


9.6. Из папки Windows скопируйте программу поиска справки winhlp32.exe в папку Student. Убедитесь, что файл запускается на выполнение из папки Student. Запретите выполнение данного файла, не запрещая чтение файла. Убедитесь, что программа winhlp32.exe перестала выполняться.



Поскольку программа для поиска справки winhlp32.exe не поддерживается в текущей версии Window, она была заменена исполняемым файлом WordPad – write.exe.





10. Зайдите под пользователем Student2. Зайдите в папку Student. Укажите, какие права на доступ к файлам имеет пользователь Student2. Результаты определения прав пользователя запишите в следующую таблицу

Имя файла	Чтение	Запись	Объяснение
Запись.txt	-	-	Student2 не имеет прав на чтение или запись данного файла. (Имеют право пользователи User и Student1)
Изменение.txt	+	+	Student2 состоит в группе «Студенты», пользователи которой имеют право на «Изменение» - в т.ч. на чтение и запись.
Чтение.txt	-	-	Student2 не имеет прав на чтение или запись файла, т.к. не относится к группе «Опытные пользователи» и не является пользователем User.
Полный доступ.txt	-	-	Student2 не имеет прав на файл, так как не является User или Student1.
Write.exe	+	+	Права на запись и чтение имеют все пользователи (ограничено лишь выполнение и изменение файла).

11. Зайдите под пользователем Student1.

11.1. Зайдите в папку Student. Укажите, какие права на доступ к файлам имеет пользователь Student1. Результаты определения прав пользователя запишите в таблицу 1. Объясните получившиеся результаты.

Имя файла	Чтение	Запись	Объяснение
Запись.txt	-	+	Пользователи User и Student1 имеют право на запись данного файла. (Но не на чтение)
Изменение.txt	+	+	Student1 состоит в группе «Студенты», пользователи которой имеют право на «Изменение» - в т.ч. на чтение и

			запись.
Чтение.txt	+	-	Student1 имеет права на чтение файла, т.к. относится к группе «Опытные пользователи». Право на запись имеет только User.
Полный доступ.txt	+	+	User и Student1 имеют полные права на файл.
Write.exe	+	+	Права на запись и чтение имеют все пользователи (ограничено лишь выполнение и изменение файла).

11.2. Пользователь Student1 имеет право на запись в файл «Запись.txt», но не имеет право на чтение. Каким образом можно записать информацию в этот файл?

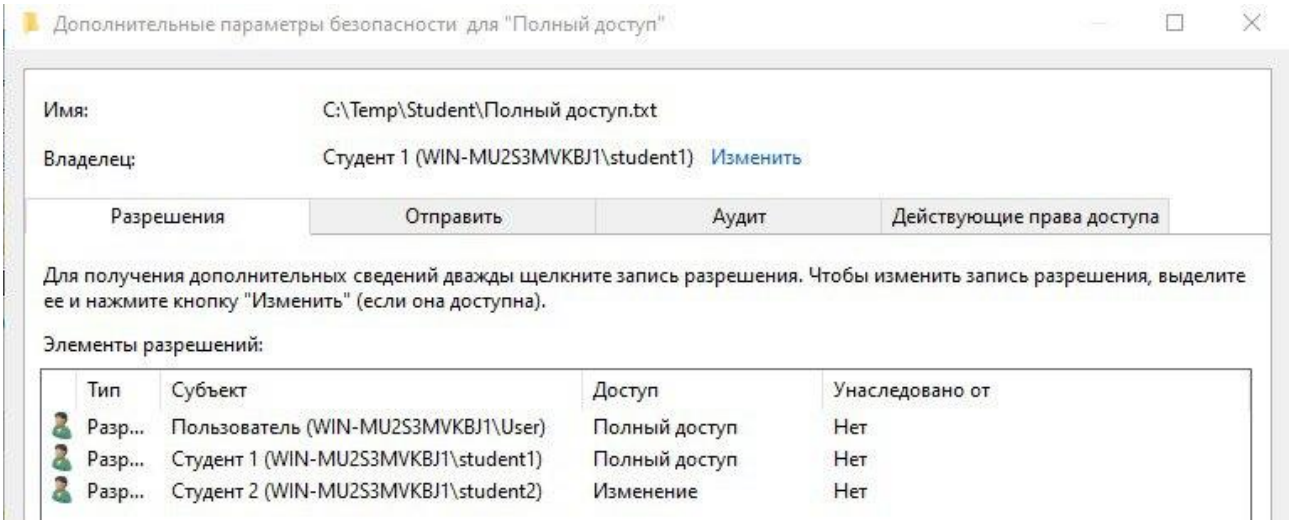
Несмотря на отсутствие прав на чтение файла, мы можем записать в него информацию с помощью специальных программных средств и команд, которые работают напрямую с записью данных. Например, в C# используются два основных класса: StreamReader для чтения файлов и StreamWriter для записи. При наличии прав на запись можно легко добавлять текст в уже существующий файл с помощью класса StreamWriter:

```
static void Main()
    {
        string FileName = "C:\\Temp\\Student\\Запись.txt";

        try
        {
            StreamWriter sw = new StreamWriter(FileName, true,
                System.Text.Encoding.Default);
            sw.WriteLine("Текст для вставки\n");
            sw.Close();
        }
        catch (Exception ex)
        {
            Console.WriteLine("Ошибка при записи в файл: " + ex.Message);
        }
    }
```

11.3. Используя право полного доступа к файлу «Полный доступ.txt» у Student1, выдайте пользователю Student2 право на изменение этого файла. Сделайте пользователя Student1 владельцем файла «Полный доступ.txt».

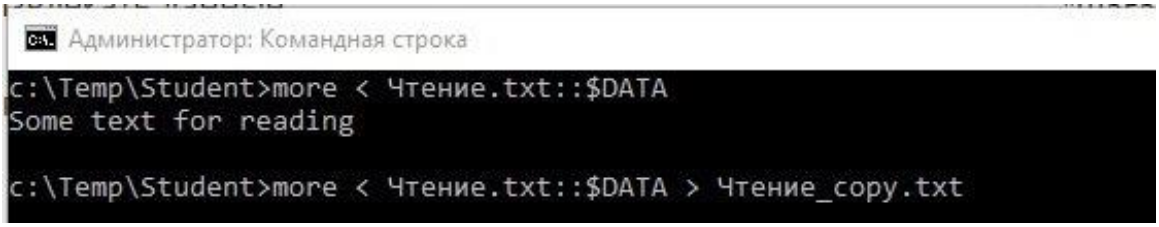
Теперь student1 стал владельцем файла «Полный доступ.txt», а student2 получил право на изменение.



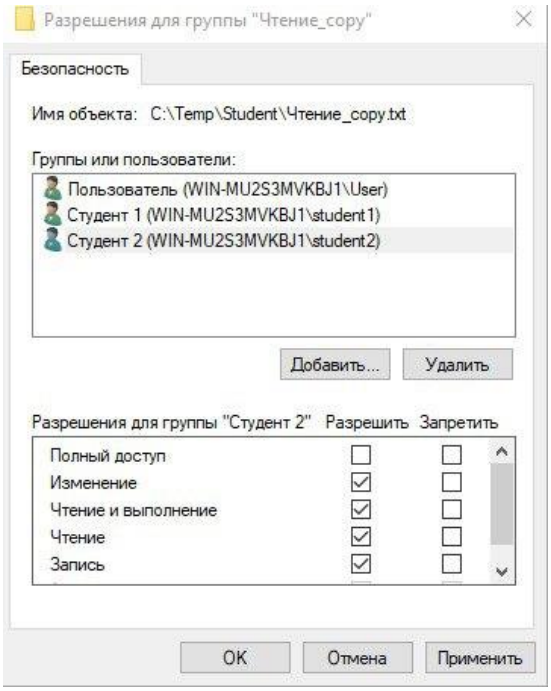
11.4. Каким образом Student1 может предоставить Student2 доступ к содержимому файла «Чтение.txt»? Проделайте эту операцию.

Поскольку Student1 имеет только права на чтение файла «Чтение.txt», он не сможет напрямую изменить права доступа к файлу. Однако, он сможет, например, прочитать содержимое файла и, скопировав его, вставить это содержимое в новый созданный файл.

Например, Student1 может открыть файл «Чтение.txt» и скопировать его содержимое в файл Чтение_copy.txt через командную строку:

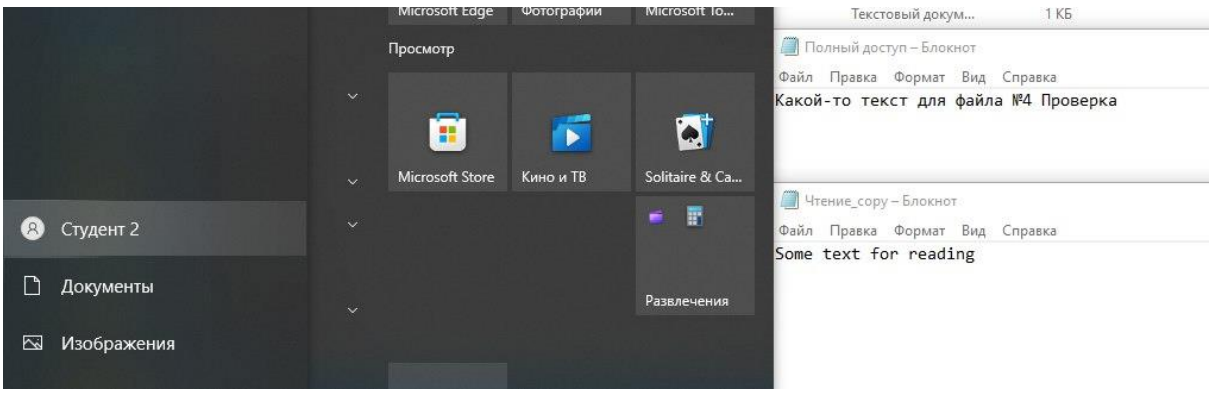


Затем Student1 сохраняет новый файл в директории, где Student2 имеет доступ, и настраивает необходимые для работы с данными права:



11.5. Зайдите под именем Student2 и проверьте, что Student2 имеет доступ к содержимому файлов «Чтение.txt» и «Полный доступ.txt»

Доступ к содержимым файлов имеется:



12. В соответствии с моделью дискреционного доступа регулировать права доступа можно не только к файлам, но и к папкам. В Windows права доступа к папкам несколько отличаются от прав доступа к файлам.

12.1. Запишите, какие в Windows используются права доступа к папкам и что они означают.

• *Список содержимого папки* – возможность посмотреть список содержимого текущего каталога. При этом пользователь не может запустить файлы или открыть подкаталоги;

• *Право на чтение* – возможность просматривать содержимое файлов и папок внутри данной папки. При этом запрещен запуск исполняемых файлов.

• *Право на чтение и выполнение* дает те же права, что и предыдущий пункт, а также возможность запускать исполняемые файлы.

• *Право на запись* - возможность создавать файлы и папки внутри данной папки.

• *Право на изменение* - предоставляет возможность открывать и создавать (изменять) файлы в папке.

• *Полный доступ* – включает в себя все перечисленные права.

• *Особые разрешения* − задается набор специальных разрешений, отличающийся от стандартных (чтение атрибутов, удаление и т.д.)

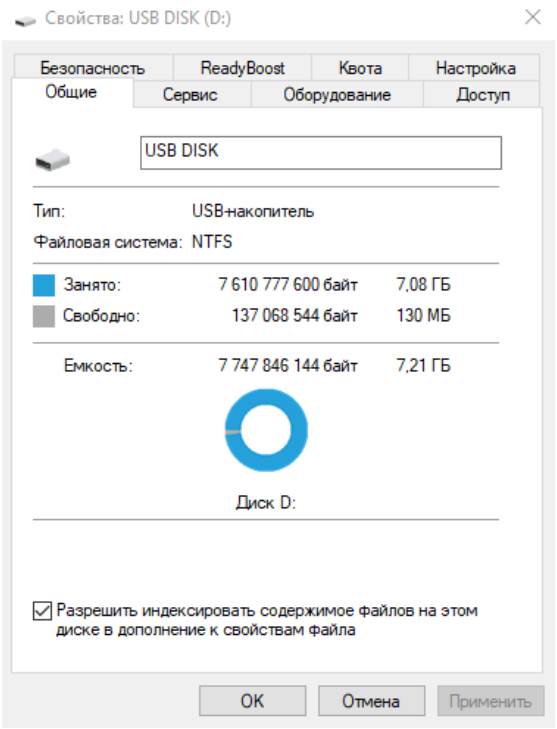
12.2. Определите, чем отличаются друг от друга следующие права доступа к папке:

1) отсутствие доступа к папке;
2) чтение и выполнение;
3) только чтение;
4) только запись.

По результатам исследований заполните таблицу 2. Перед проверкой прав доступа обязательно надо установить полный доступ к файлам, находящимся в исследуемой папке. Дело в том, что при изменении прав доступа к папке автоматически меняются права доступа к файлам.

Права	**Отсутствие доступа к папке**	**Чтение и выполнение**	**Только чтение**	**Только запись**
Просмотр содержимого папки	-	+	+	-
Изменение содержимого файла	-	+	+	+
Создание файла	-	-	-	+
Переименование файла	-	-	-	+
Удаление файла	-	+	+	-
Создание папки	-	-	-	+
Удаление папки	-	+	+	-

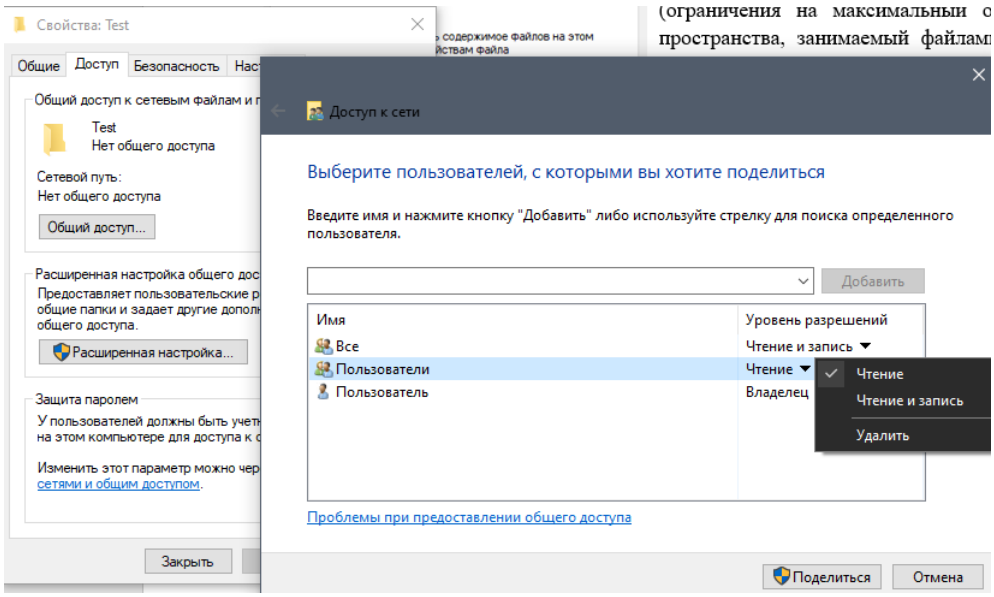
13. Подключите к компьютеру флеш-память. Какая файловая система используется на подключенной флешке?



Файловая система флеш-памяти: NTFS. Она обеспечивает разграничение прав доступа согласно дискреционной модели, а также обладает ещё рядом свойств:

- Поддерживает хранение метаданных;
- Поддерживает разграничение доступа к данным для различных пользователей и групп пользователей;
- Позволяет назначать дисковые квоты (ограничения на максимальный объём дискового пространства, занимаемый файлами тех или иных пользователей);

14. Создайте на флешке папку Test и попробуйте ограничить доступ к этой папке для группы «Пользователи». Удалось ли выполнить ограничение доступа? Почему удалось или не удалось?



Так как флешка использует файловую систему NTFS, поддерживающую разграничение доступа к данным для различных пользователей и групп пользователей, ограничения применены успешно. Это произошло благодаря поддержке системе контроля доступа (ACL — Access Control List), которая позволяет настраивать права пользователей и групп на чтение, запись или выполнение файлов и папок.

Если бы флешка использовала файловую систему FAT32 или exFAT, то ограничение доступа папки было бы невозможно, так как эти файловые системы не поддерживают расширенные механизмы управления правами доступа (ACL).