**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ  
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»  
(БГТУ им. В.Г.Шухова)**

Лабораторная работа по теме

«Обеспечение безопасности ресурсов с помощью разрешений NTFS»  
дисциплина:

Администрирование распределенных вычислительных систем

Выполнил: ст. группы ВТ-41   
Фаракшин Н. Р.  
Проверил: Федотов Е.А.

**Белгород 2020**

**Лабораторная работа № 6**

**Обеспечение безопасности ресурсов с помощью разрешений NTFS**

**Цель работы:** получить навыки обеспечения безопасности ресурсов с помощью разрешений NTFS.

**Краткие сведения**

Разрешения NTFS позволяют явно указать, какие пользователи и группы имеют доступ к файлам и папкам и какие операции с содержимым этих файлов или папок им разрешено выполнять.

Система безопасности NTFS эффективна независимо от того, обращается ли пользователь к файлу или папке, размещенных на локальном компьютере или в сети.

Разрешения, устанавливаемые для папок, отличаются от разрешений, устанавливаемых для файлов. Администраторы, владельцы файлов или папок и пользователи с разрешением Полный доступ имеют право назначать разрешения NTFS пользователям и группам для управления доступом к этим файлам и папкам.

В NTFS хранится список управления доступом (access control list, ACL) для каждого файла и папки на томе NTFS. В этом списке перечислены пользователи и группы, для которых установлены разрешения для файла или папки, а также сами назначенные разрешения. Чтобы пользователь получил доступ к ресурсу, в ACL должна быть запись, называемая элемент списка управления доступом (access control entry, АСЕ), для этого пользователя или группы, к которой он принадлежит. Эта запись назначит запрашиваемый тип доступа (например, Чтение) пользователю. Если в ACL нет соответствующей АСЕ, то пользователь не получит доступ к ресурсу.

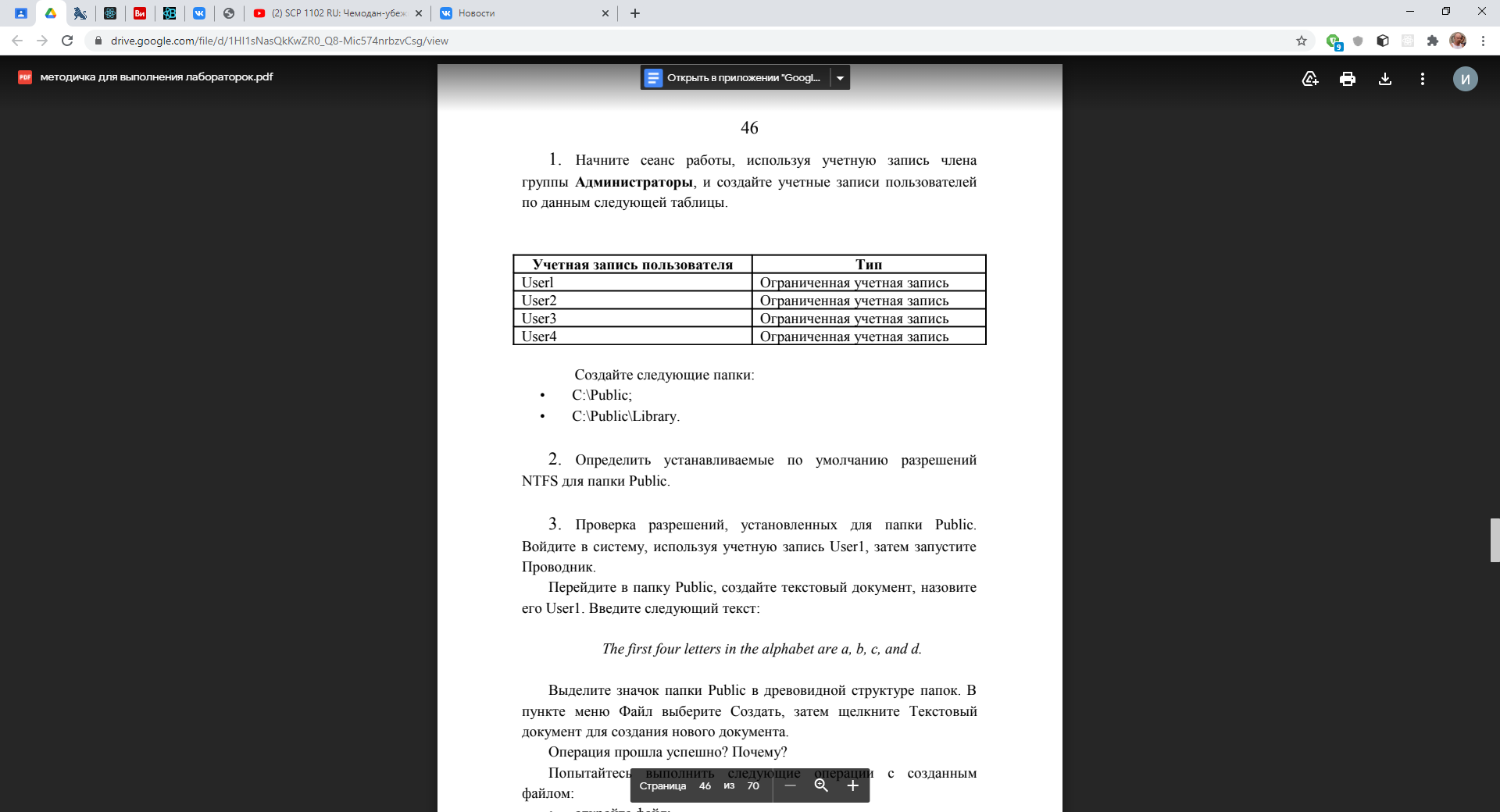
Эффективные разрешения пользователя для ресурса — это совокупность разрешений NTFS, которые вы назначаете отдельному пользователю и всем группам, к которым он принадлежит.

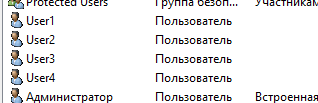
Приоритет разрешений для файлов над разрешениями для папок В NTFS разрешения для файлов имеют больший приоритет, чем разрешения для папок. Если у вас есть разрешение на доступ к файлу и право Обход перекрестной проверки, то вы сможете воспользоваться доступом к этому файлу, даже если у вас нет доступа к папке, в которой содержится файл. Вы можете получить доступ к тем файлам, для которых у вас есть разрешения, воспользовавшись UNC-именем файла или локальным путем для открытия файла из соответствующего приложения.

Можно запретить доступ к файлу пользователю или группе, хотя этот метод контроля ресурсов нельзя назвать предпочтительным. Запрет имеет больший приоритет, чем разрешение на всех уровнях, на которые он распространяется. Даже если у группы, в которую входит пользователь имеется разрешение на доступ к файлу или папке, запрет на доступ для пользователя блокирует все имеющиеся разрешения.

**Выполнение работы:**

1. Начните сеанс работы, используя учетную запись члена группы Администраторы, и создайте учетные записи пользователей по данным следующей таблицы.

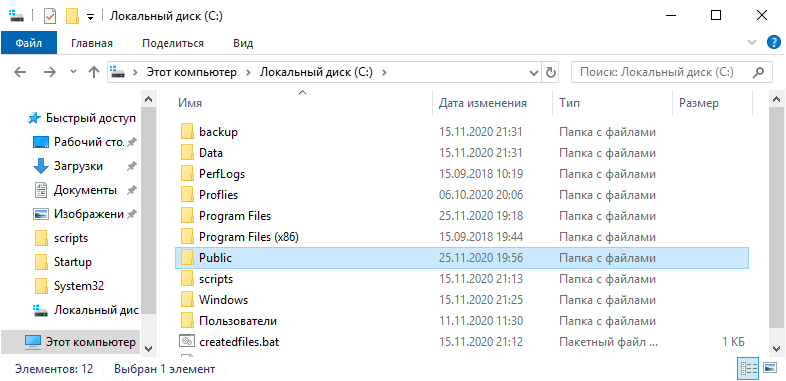


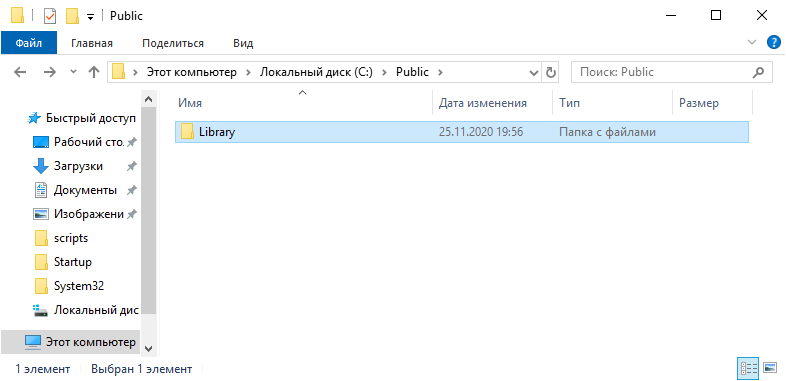


Создайте следующие папки:

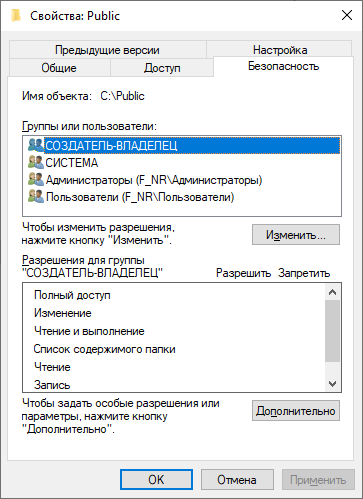
• C:\Public;

• C:\Public\Library.





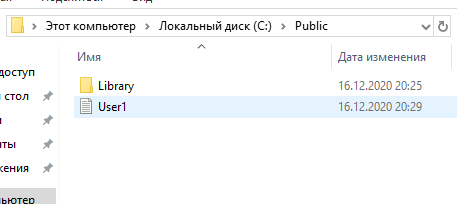
2. Определить устанавливаемые по умолчанию разрешений NTFS для папки Public.



3. Проверка разрешений, установленных для папки Public. Войдите в систему, используя учетную запись User1, затем запустите Проводник. Перейдите в папку Public, создайте текстовый документ, назовите его User1. Введите следующий текст:

The first four letters in the alphabet are a, b, c, and d.

Выделите значок папки Public в древовидной структуре папок. В пункте меню Файл выберите Создать, затем щелкните Текстовый документ для создания нового документа. Операция прошла успешно? Почему?



Операция прошла успешно, т.к. разрешения по умолчанию позволяют создание файлов другим пользователям.

В папке Public снова создайте текстовый документ User1.

Завершите сеанс.

Войдите в систему, используя учетную запись User2. Попытайтесь выполнить следующие операции с текстовым документом User1:

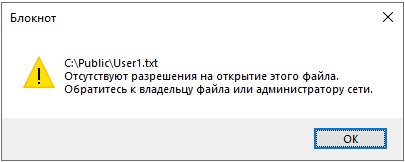
• откройте файл;

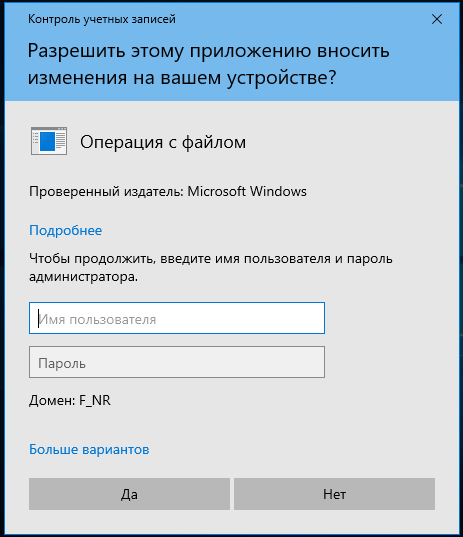
• измените файл;

• удалите файл.

Какие действия вы смогли успешно совершить и почему?

С другого аккаунта удалось только прочесть текстовый файл, остальные же действия требовали наличия необходимых прав, которые у пользователя User2 отсутствовали.





4. Установить разрешения NTFS для папки Public.

При этом необходимо соблюдать следующие правила:

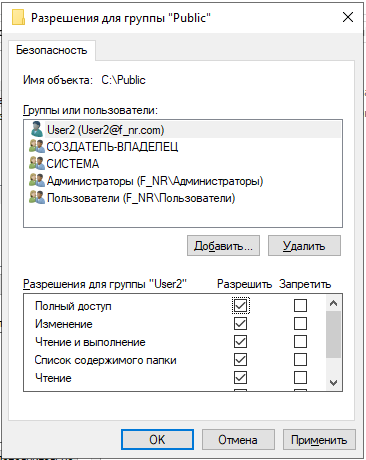
• все пользователи должны иметь возможность читать документы и файлы в папке Public;

• все пользователи должны иметь возможность создавать документы в папке Public;

• все пользователи должны иметь возможность изменять содержание, свойства и разрешения для создаваемых ими документов в папке Public;

• пользователь User2 несет ответственность за подержание папки Public и должен иметь возможность изменять и удалять все файлы в папке Public.

Основываясь на полученной в упражнении 1 информации, определите, как следует изменить разрешения для соответствия этим четырем критериям?



Для выполнения поставленной задачи необходимо установить разрешения для пользователя User2 так, как показано на скриншоте выше. У остальных же пользователей необходимо снять галочки напротив полей Полный доступ.

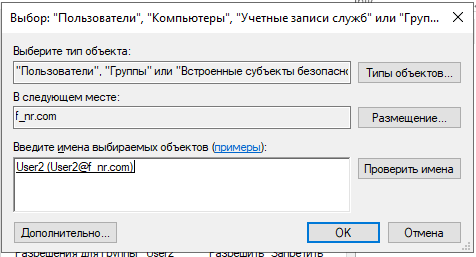
5. Установка разрешений NTFS для папки.

Войдите в систему, используя учетную запись пользователя, который является членом группы Администраторы. Затем откройте Проводник.

Выберите папку Public, затем пункт меню Свойства.

Перейдите на вкладку Безопасность диалогового окна свойств папки.

На вкладке Безопасность щелкните кнопку Добавить.



В текстовом поле Введите имена выбираемых объектов введите User2, затем щелкните кнопку Проверить имена.

В текстовом поле Введите имена выбираемых объектов должна появиться надпись “имя компьютера”\User2. Теперь пользователь User2 включен в список Группы или пользователи диалогового окна свойств папки Public.

Какие разрешения установлены для пользователя User2?

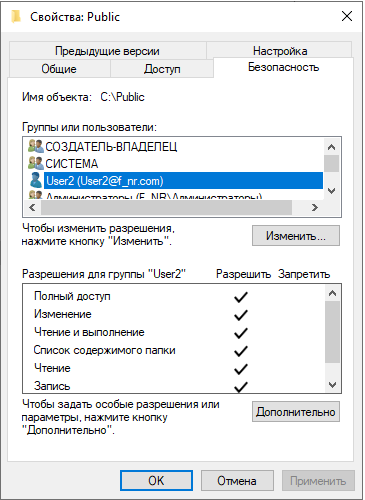
По умолчанию устанавливаются разрешения на чтение и выполнение, список содержимого папки и чтение.

Щелкните кнопку Дополнительно. Вы увидите, что пользователь User2 (“имя компьютера”\User2) включен в список Элементы разрешений.

Убедитесь, что строка User2 выделена, и щелкните кнопку Изменить. Вы увидите в текстовом поле Имя учетную запись пользователя User2 (“имя компьютера”\User2).

В колонке Разрешить щелкните Полный доступ.

Теперь в колонке Разрешить установлены все флажки.



6. Проверка разрешений NTFS для папки.

Войдите в систему, используя учетную запись User2. Запустите Проводник.

Откройте диск С:, затем откройте папку Public.

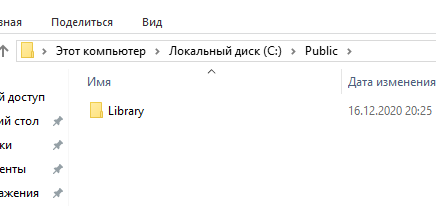
Попытайтесь совершить следующие действия с текстовым документом User1:

• измените файл;

• удалите файл.

Какие действия вы смогли совершить и почему?

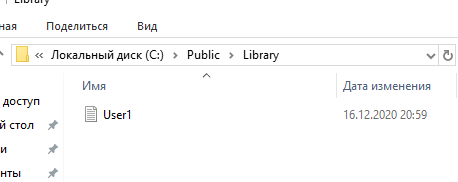
Все действия выполнить удалось, поскольку у пользователя User2 есть полный доступ к данному файлу.



7. Проверка разрешений NTFS.

Войдите в систему, используя учетную запись User1, затем запустите Проводник.

В Проводнике откройте папку Public\Library. Создайте текстовый документ User1 в папке Library.



Завершите сеанс.

8. Проверка разрешений для папки Library с использованием подключения с учетной записью User2. Зарегистрируйтесь в системе, используя учетную запись User2, затем запустите Проводник.

Откройте папку Public\Library.

Попытайтесь совершить следующие действия с текстовым документом User1

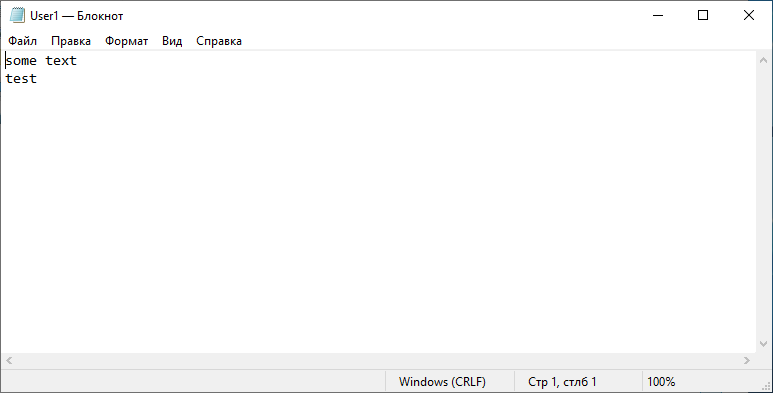
• открыть файл;

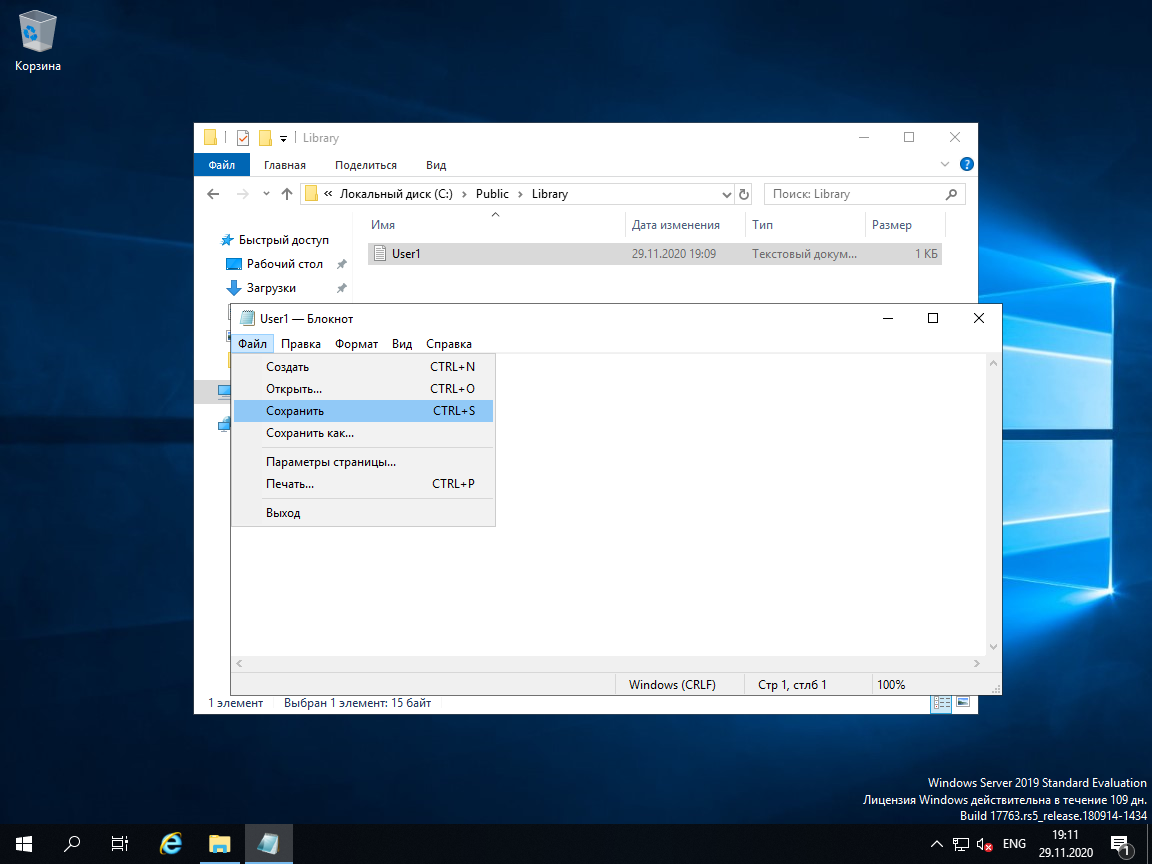
• изменить файл;

• удалить файл.

Какие действия вы смогли совершить и почему?

Все действия удалось выполнить, поскольку пользователь user2 все еще имеет полный доступ к папке Public, и соответственно ко всему ее содержимому.



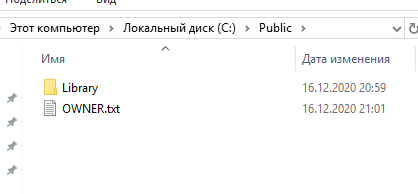


9. Смена владельца файла.

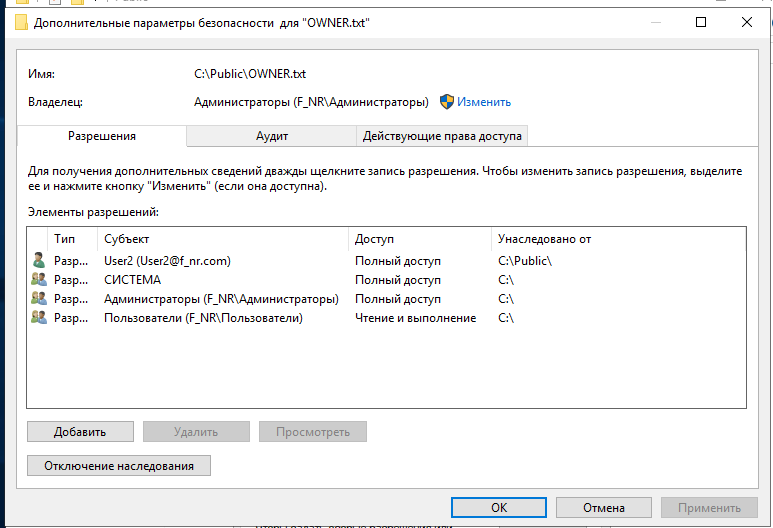
Подключитесь, используя учетную запись пользователя, который является членом группы Администраторы.

В папке Public создайте текстовый документ и назовите его OWNER.

Щелкните правой кнопкой мыши значок документа OWNER, затем выберите пункт меню Свойства.



Перейдите на вкладку Безопасность для просмотра разрешений, установленных для файла OWNER. Щелкните кнопку Дополнительно. Откроется диалоговое окно Дополнительные параметры безопасности для Owner с активной вкладкой Разрешения. Перейдите на вкладку Владелец. Кто является текущим владельцем файла OWNER?



Владельцем являются все члены группы Администраторы.

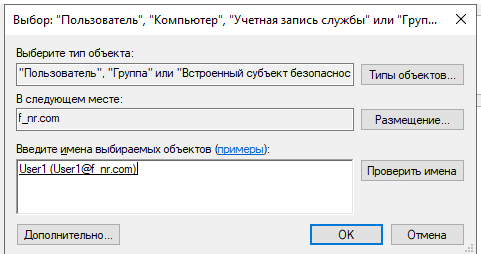
10. Установка разрешения, позволяющего пользователю сменить владельца.

В диалоговом окне Дополнительные параметры безопасности для Owner перейдите на вкладку Разрешения.

Щелкните кнопку Добавить Откроется диалоговое окно Выбор: пользователи или группы.

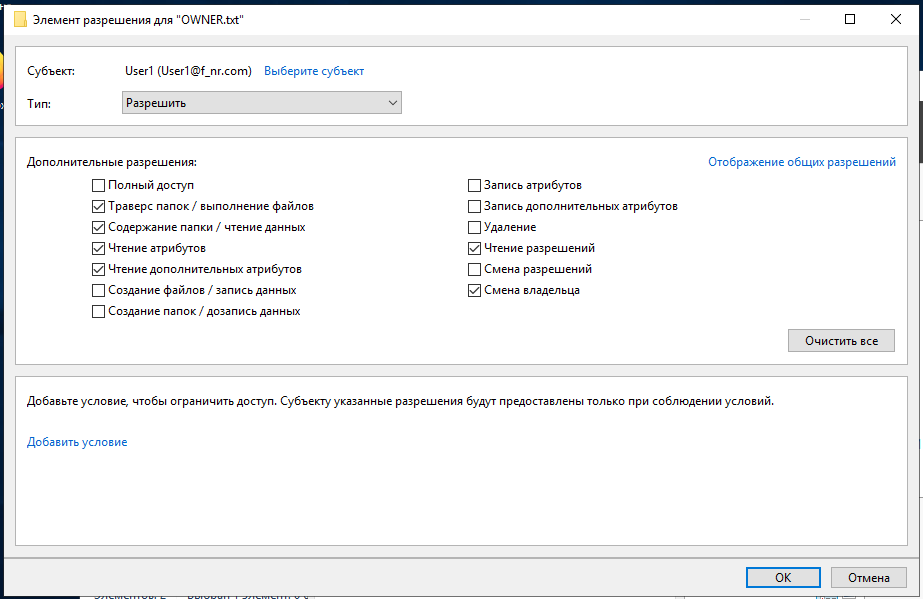
Убедитесь, что в текстовой поле Размещение, которое расположено вверху диалогового окна, выбрано имя вашего компьютера.

В текстовом поле Введите имена выбираемых введите User1, затем щелкните кнопку Проверить имена.



В списке Введите имена выбираемых объектов должна появиться запись “имя компьютера”\User1. Это означает, что учетная запись пользователя Userl найдена на компьютере с именем “имя компьютера” и является действительной учетной записью.

В колонке Разрешения установите флажок Разрешить для разрешения Сменить владельца.

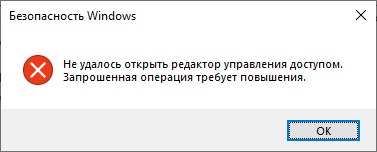


11. Смена владельца файла.

Зарегистрируйтесь в системе, используя учетную запись User1, затем запустите Проводник.

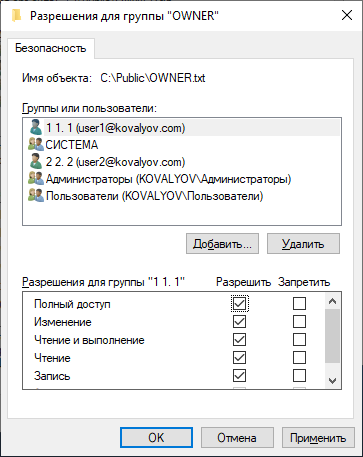
Разверните папку Public. Измените владельца на User1.  Кто теперь является владельцем файла OWNER?

Все еще пользователь Администратор, поскольку у пользователя User1 нет права на внесение изменений в папке Public.

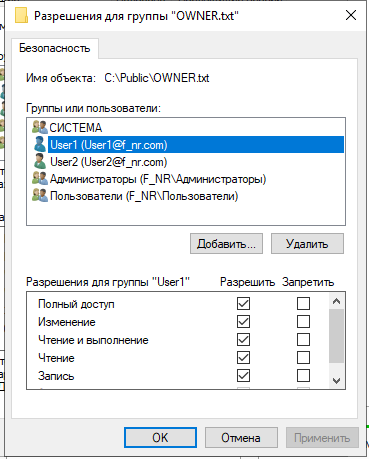
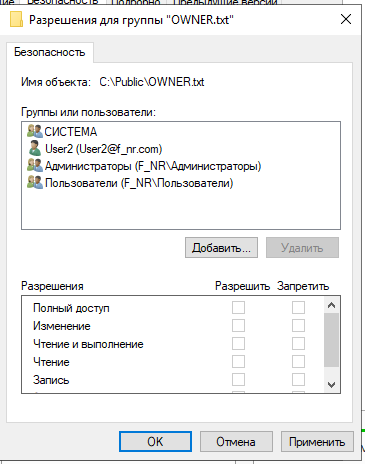


12. Проверка разрешений для файла в качестве владельца.

Установите разрешение Полный доступ пользователю User1 к текстовому документу OWNER.

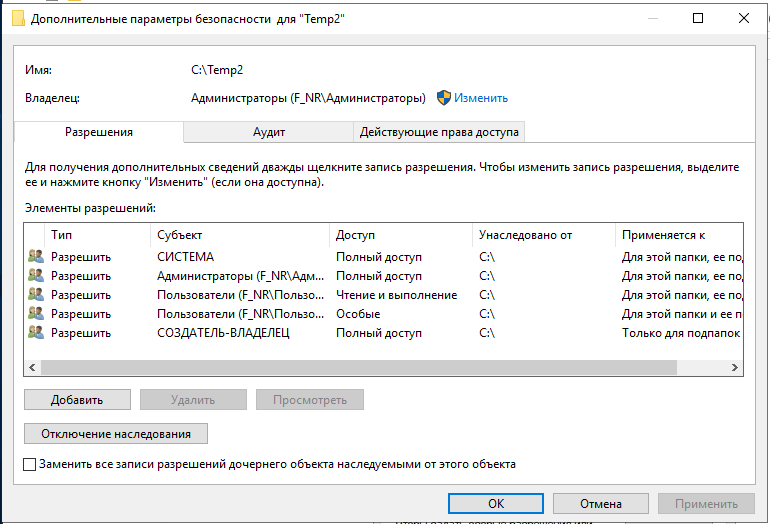


В диалоговом окне Безопасность щелкните кнопку Удалить. Удалите текстовый документ OWNER.

13. Создание папки при подключении с учетной записью пользователя.

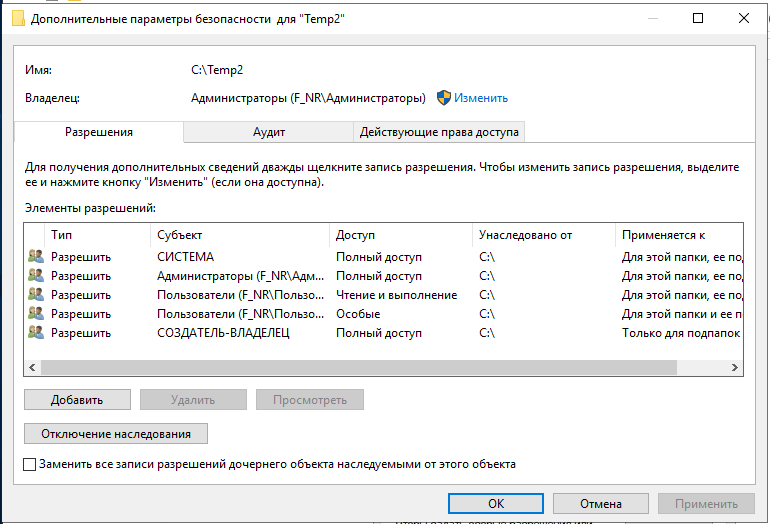
Под учетной записью User1, в Проводнике, в корневой папке диска С, создайте папку с именем Temp1.



14. Создание папки при подключении с учетной записью члена группы Администраторы.

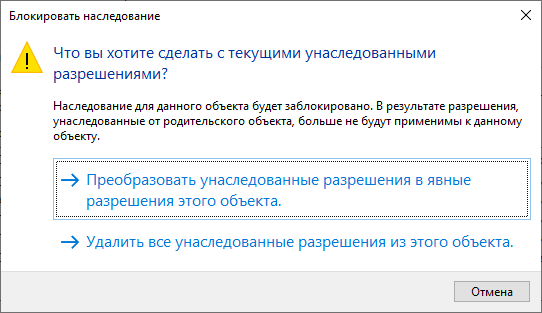
Подключитесь с учетной записью Администратор или как пользователь, который является членом группы Администраторы, и запустите Проводник.

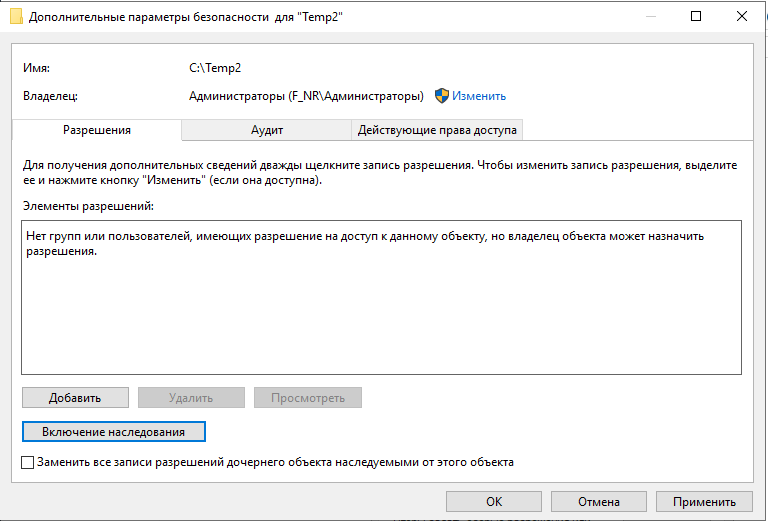
В корневой папке диска С: создайте папки Теmр2 и Теmр3. Каковы разрешения для папок Теmр2 и Теmр3, которые вы только что создали?



Владельцем папок Теmр2 и Теmр3 являются все пользователи группы Администраторы и только они.

Установите разрешения для папок Теmр2 и Теmр3. Снимите флажок Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне. В открывшемся диалоговом окне щелкните Удалить для удаления всех разрешений, кроме указанных явно.

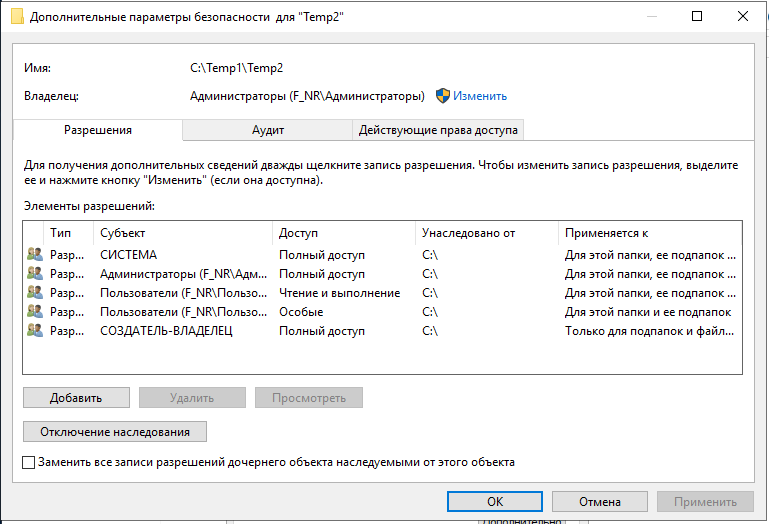




15. Копирование папки в другую папку на одном и том же томе NTFS

Под учетной записью члена группы Администраторы, в Проводнике, скопируйте папку C:\Temp2 в папку C:\Templ. Для этого выделите значок папки C:\Temp2 и, удерживая нажатой клавишу CTRL, перетащите мышью C:\Temp2 в C:\Templ.

Кто владелец папки C:\Templ\Temp2 и какие разрешения для нее установлены? Почему?



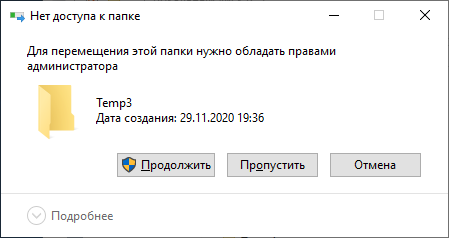
Данные разрешения были установлены таким образом, поскольку в папке Temp1 было отключено наследование прав доступа у дочерних объектов.

16. Перемещение папки на одном и том же томе.

Зарегистрируйтесь в системе как пользователь User1.

В Проводнике выделите значок папки C:\Temp3, затем переместите ее в папку C:\Templ.

Что произошло с разрешения и владельцем для папки C:\Templ\ Теmр3? Почему?



Система вывела сообщение о том, что данное действие недоступно для пользователя User1, поскольку у него нет прав на это.

Закройте все окна и завершите сеанс работы.

**Вывод:** в ходе выполнения лабораторной работы были получены навыки обеспечения безопасности ресурсов с помощью разрешений NTFS.

Для управления доступом пользователей к папкам и файлам используется детализированная и сложная система разрешений. Механизм управления доступом к объектам Windows - один из самых детализированных среди известных операционных систем. Для файлов и папок существует не менее 14 разрешений NTFS, которые могут быть включены или блокированы – и проверены. Эти разрешения можно назначать файлам или папкам и пользователям или группам. Кроме того, можно назначать порядок наследования разрешений для файлов или папок и пользователей или групп.