ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Информационная безопасность

Отчет по лабораторной работе №2  
«Разграничение доступа к объектам файловой системы»

Выполнил:  
Студент группы №P34101

*Патутин В.М.*Преподаватель:  
*Маркина Т. А.*

Санкт-Петербург

2022

Оглавление

[**Цель работы** 3](#_Toc120581194)

[**Вариант:** 3](#_Toc120581195)

[**Программные и аппаратные средства, используемые при выполнении работы:** 3](#_Toc120581196)

[**Основная часть** 5](#_Toc120581197)

[**1.** **Укажите минимальный набор разрешений (прав доступа), необходимых для: a. загрузки операционной системы; b. входа Пользователя (user\_№варианта) и Администратора (admin\_№варианта) в систему; c. работы с приложениями, установленными администратором. Разрешения указывать в форме R, W, X, в таблице:** 5](#_Toc120581198)

[**2.** **Преобразуйте файловую систему FAT (File Allocation Table) в NTFS (New Technology File System). Опишите преобразование в отчете с использованием скриншотов (минимум 2 способа) (в отчете: подробное описание выполнения задания со скриншотами).** 6](#_Toc120581199)

[**Способ 1:** 6](#_Toc120581200)

[**Способ 2:** 11](#_Toc120581201)

[**3.** **Выполните задание в соответствии с номером варианта, 1 – для нечетных вариантов, 2 – для четных вариантов. Для выполнения задания нужно создать файл с названием «№варианта.txt» и папку «№варианта», в которую поместить созданный файл (в отчете: расписать права доступа, продемонстрировав на скриншотах).** 13](#_Toc120581202)

[**Вариант:** 13](#_Toc120581203)

[**Решение:** 13](#_Toc120581204)

[**4.** **Выполните задание в соответствии с номером варианта, номер задания соответствует второй цифре номера варианта (например, 40 вариант – 10 задание, 34 вариант – 4 задание и т.п.). Выполните настройки встроенных механизмов защиты ОС Windows в соответствии с заданием (в отчете: подробное описание настроек встроенных механизмов защиты и выполненных действий со скриншотами).** 16](#_Toc120581205)

[**Вариант:** 16](#_Toc120581206)

[**Решение:** 16](#_Toc120581207)

[**5.** **Разрешите средствами операционной системы выполнять системные и прикладные программы только из папок %ProgramFiles% и %SystemRoot% (в отчете: подробное описание выполнения задания со скриншотами).** 20](#_Toc120581208)

[**Дополнительная часть** 25](#_Toc120581209)

[**1.** **Опишите на примерах работу с разрешениями NTFS дополнительных системных программ сторонних производителей (в отчете: описание работы всех программ со скриншотами). Приведите перечень подобных программ (не менее пяти).** 25](#_Toc120581210)

[**Программа 1:** 25](#_Toc120581211)

[**Программа 2:** 28](#_Toc120581212)

[**Программа 3:** 29](#_Toc120581213)

[**Программа 4:** 30](#_Toc120581214)

[**Программа 5:** 31](#_Toc120581215)

[**Программа 6:** 32](#_Toc120581216)

[**Программа 7:** 32](#_Toc120581217)

[**2.** **Сравните файловые системы FAT и NTFS (в отчете: сравнение выполнить в виде таблицы).** 34](#_Toc120581218)

[**3.** **Опишите все возможные способы задания разрешений (прав доступа) к файлам и папкам (в отчете: подробное описание выполнения задания со скриншотами).** 35](#_Toc120581219)

[**Способ 1:** 35](#_Toc120581220)

[**Способ 2:** 36](#_Toc120581221)

[**Вывод** 37](#_Toc120581222)

**Цель работы**  
Изучить объекты файловой системы, ознакомиться с основными принципами управления доступом к файловым системам. Изучить основные способы настройки доступа к объектам файловой системы.

# **Вариант:**

Номер варианта 22

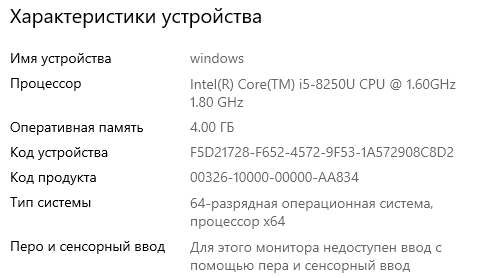
# **Программные и аппаратные средства, используемые при выполнении работы:**

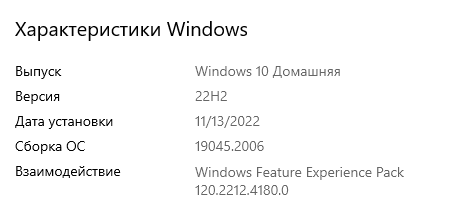
При выполнении работы было использовано ПО Oracle VM VirtualBox (ver.7.0.2).

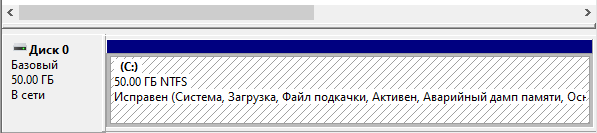


Характеристики созданной виртуальной машины:

* Операционная система Windows 10 Home (64-бит).
  + 4GB оперативной памяти
  + 50GB жесткого диска
  + Процессор: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz







# 

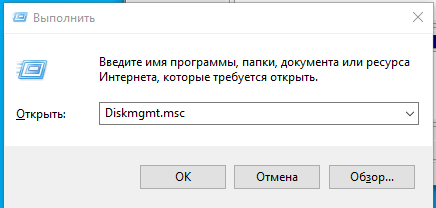
# **Основная часть**

## **Укажите минимальный набор разрешений (прав доступа), необходимых для: a. загрузки операционной системы; b. входа Пользователя (user\_№варианта) и Администратора (admin\_№варианта) в систему; c. работы с приложениями, установленными администратором. Разрешения указывать в форме R, W, X, в таблице:**

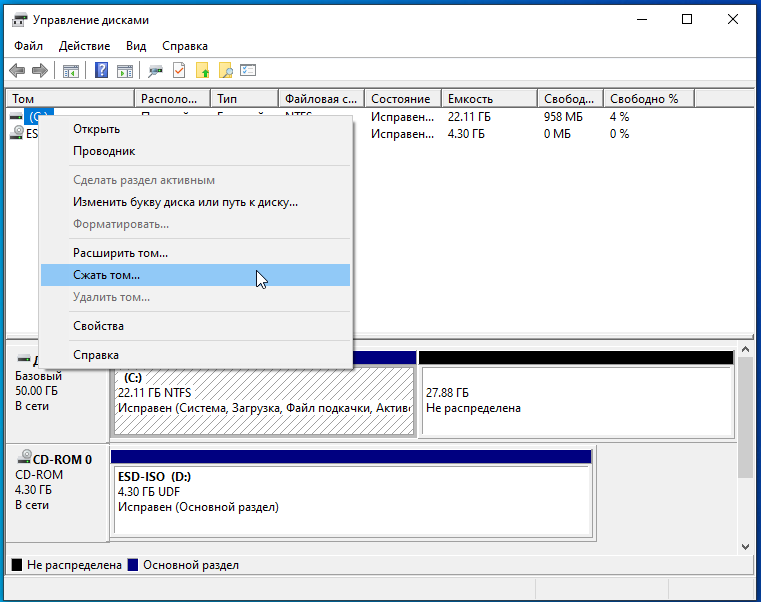
## **Преобразуйте файловую систему FAT (File Allocation Table) в NTFS (New Technology File System). Опишите преобразование в отчете с использованием скриншотов (минимум 2 способа) (в отчете: подробное описание выполнения задания со скриншотами).**

### **Способ 1:**

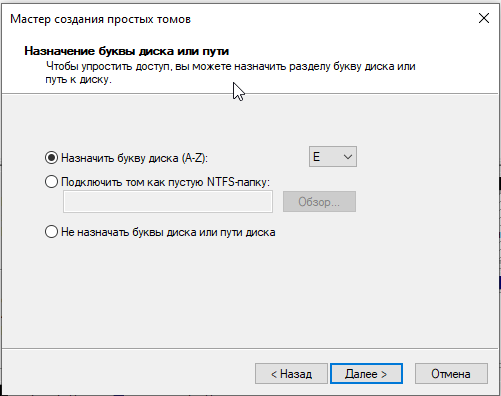
С помощью win+R открываем окно “Выполнить” и пишем:

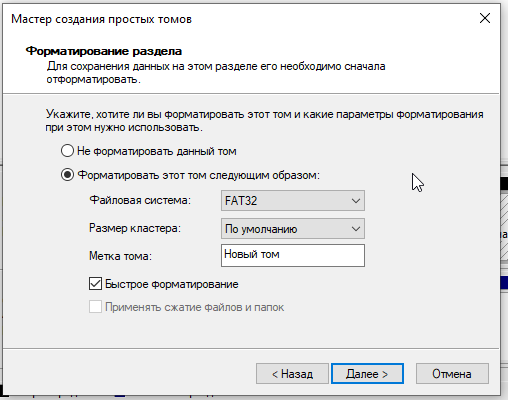


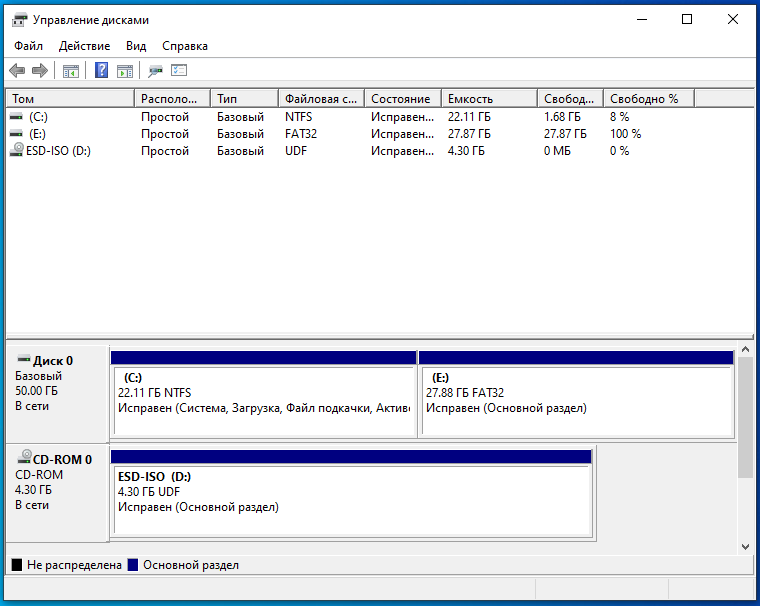
Сожмем том, чтобы получить свободное пространство для создания нового тома:



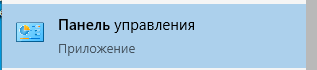
Создадим новый простой том с помощью , которого будем преобразовывать файловую систему



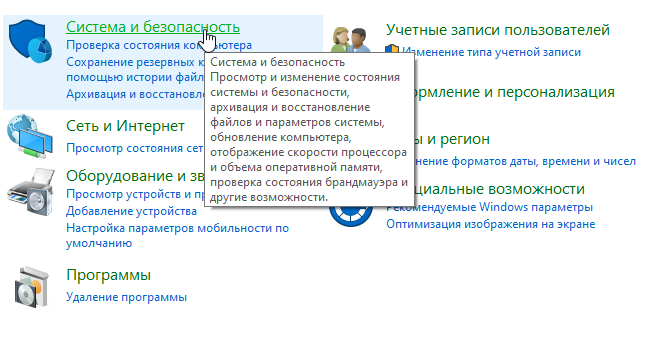




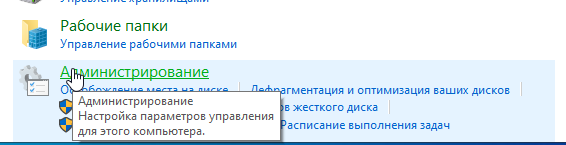
Открываем «Панель управления»



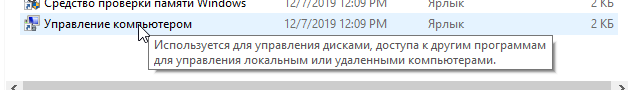
Заходим в «Система и безопасность»



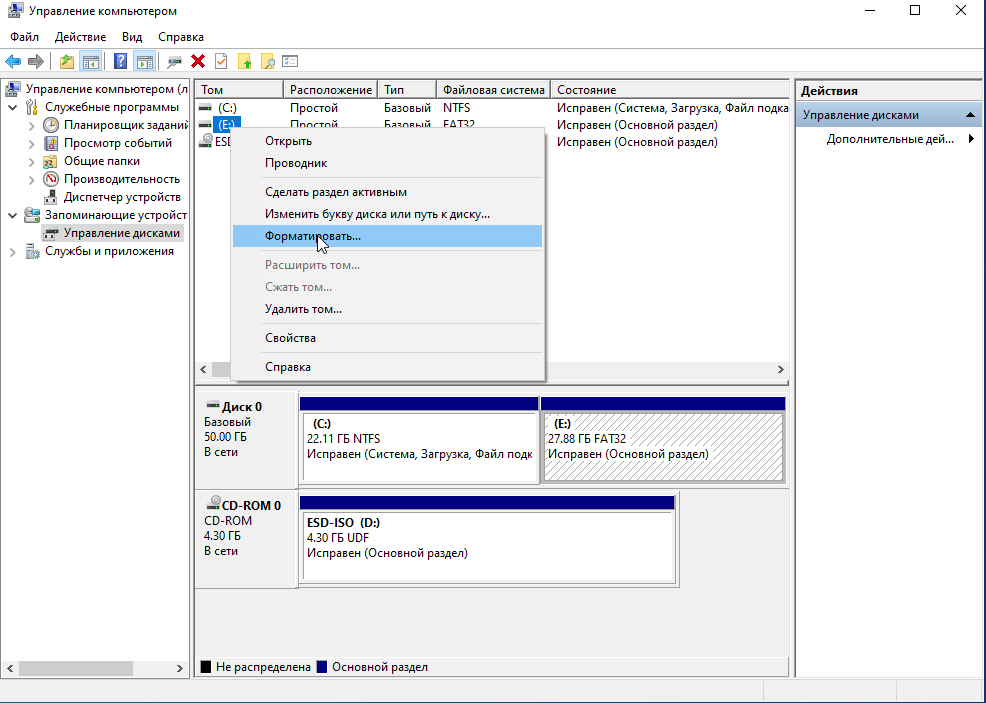
Открываем «Администрирование»



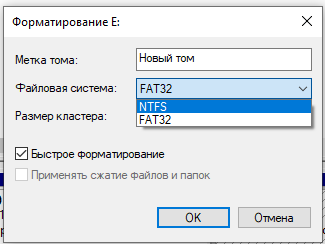
Дважды нажимаем на «Управление компьютером»



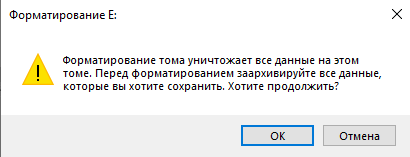
На расположенной слева панели в разделе «Запоминающие устройства» выбрать «Управление дисками». И теперь приступим к преобразованию файловой системы из FAT32 в NTFS Нажимаем правой кнопкой мыши по Тому -> Форматировать.



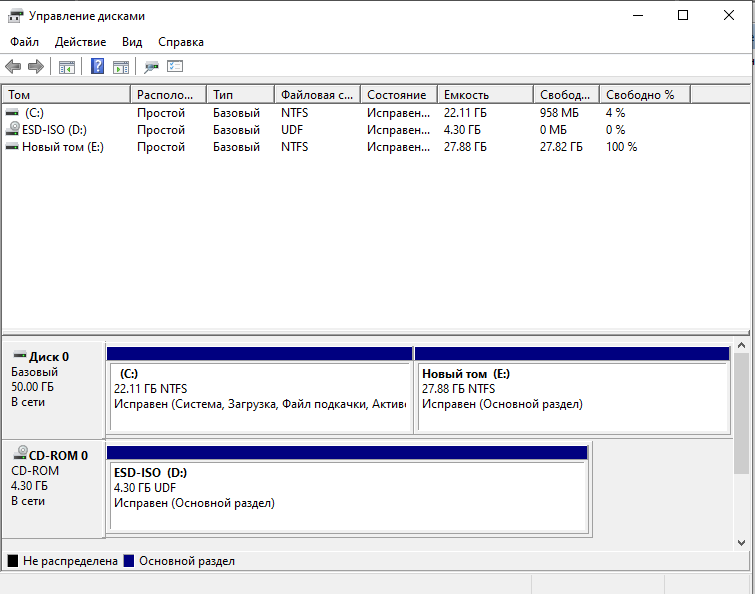
Выбираем NTFS в качестве файловой системы и нажимаем “ОК



Нас предупреждают, что данные будут уничтожены. А мы просто нажимаем “ОК”

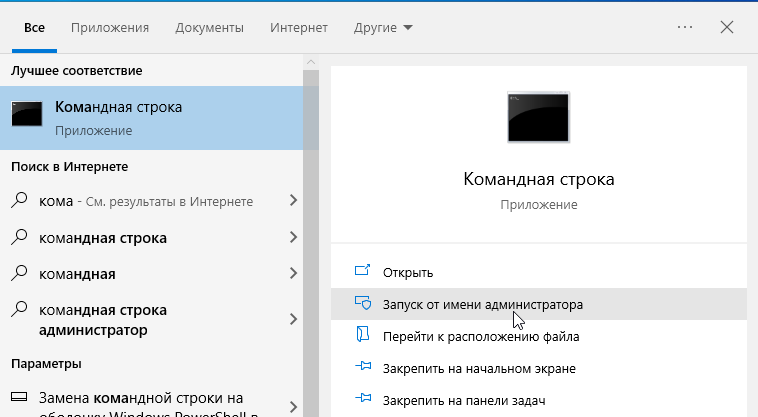


Проверяем, что все получилось



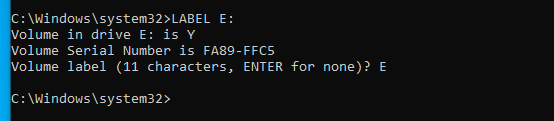
### **Способ 2:**

Запускаем “Командная строка” от имени администратора.

****

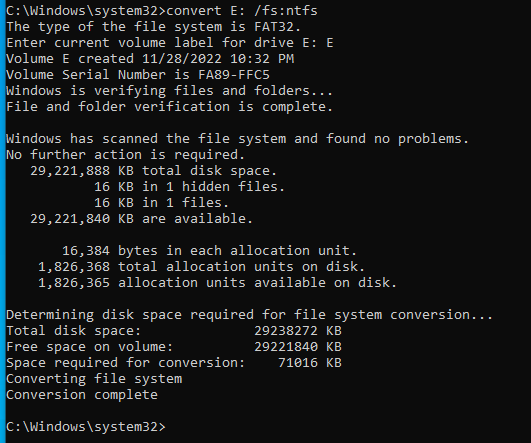
Выбираем необходимый том с помощью команду: LABEL E:

Далее вводим метку тома: E

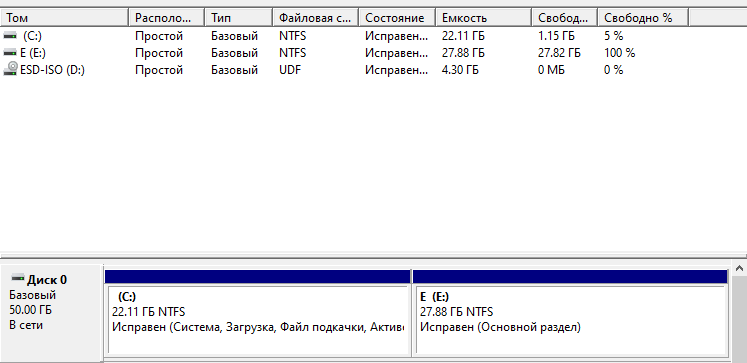
****

Для преобразования файловой системы вводим команду: convert E: /fs:ntfs

Далее вводим метку тома: E

****

Проверяем, что все получилось

****

## **Выполните задание в соответствии с номером варианта, 1 – для нечетных вариантов, 2 – для четных вариантов. Для выполнения задания нужно создать файл с названием «№варианта.txt» и папку «№варианта», в которую поместить созданный файл (в отчете: расписать права доступа, продемонстрировав на скриншотах).**

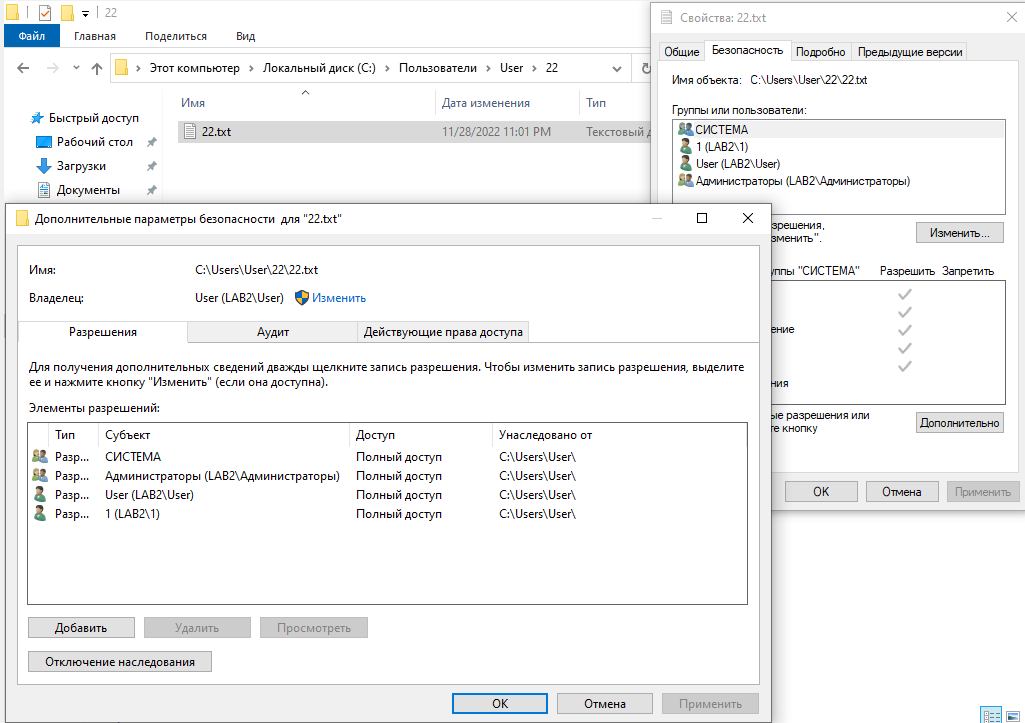
### **Вариант:**

Номер варианта 22.

Какие разрешения (права доступа) будут у Пользователя и у Администратора на файл «№варианта.txt», если владельцем папки «№варианта» является Пользователь, для пользователя установлено 15 разрешение «Чтение» («Read»), для Администратора установлено разрешение «Полный доступ» («Full control»), а для группы «Все» («Everyone») (оба пользователя входят в группу) – не установлены разрешения (установлено «No Access»)?

### **Решение:**

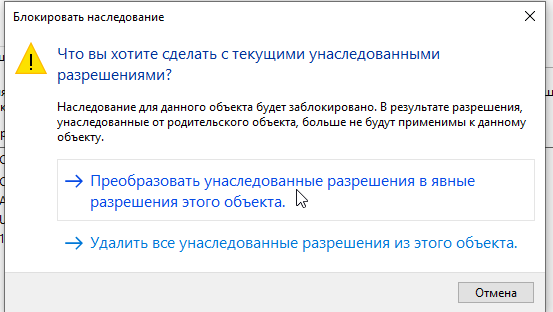
Создадим папку с названием 22 и в ней создадим файл с названием 22.txt Права на файл наследуются от прав на директорию, поэтому у Пользователя на файл есть полный доступ, и у Администратора - полный доступ. Ниже показаны права доступа на файле. Изначально у Пользователей было разрешение «Полный доступ», который возможно было отключить только при отключении наследования.

****

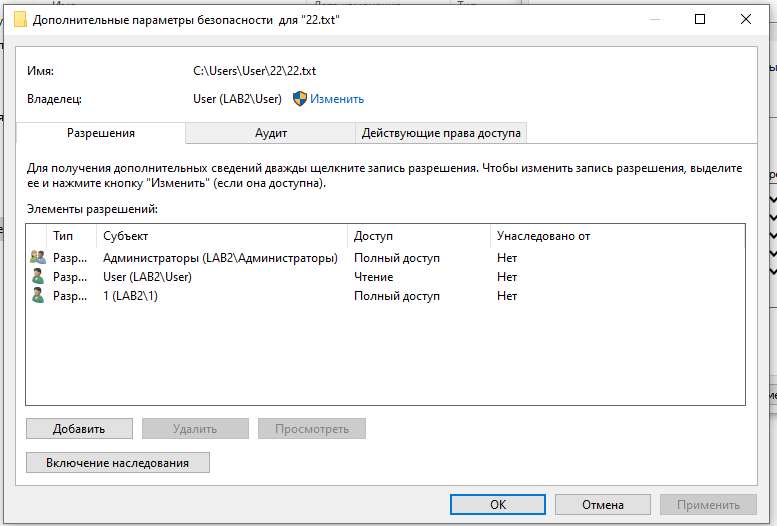
Отключим наследование:

****

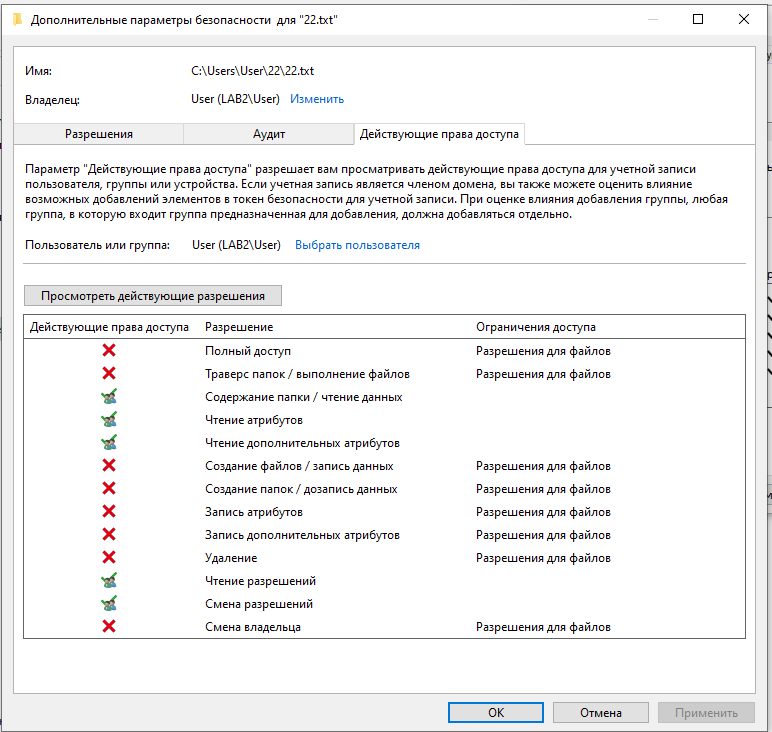
Нам всплывает предупреждение, просто нажимаем на «Преобразовать унаследованные разрешения в явные разрешения этого объекта»:

****

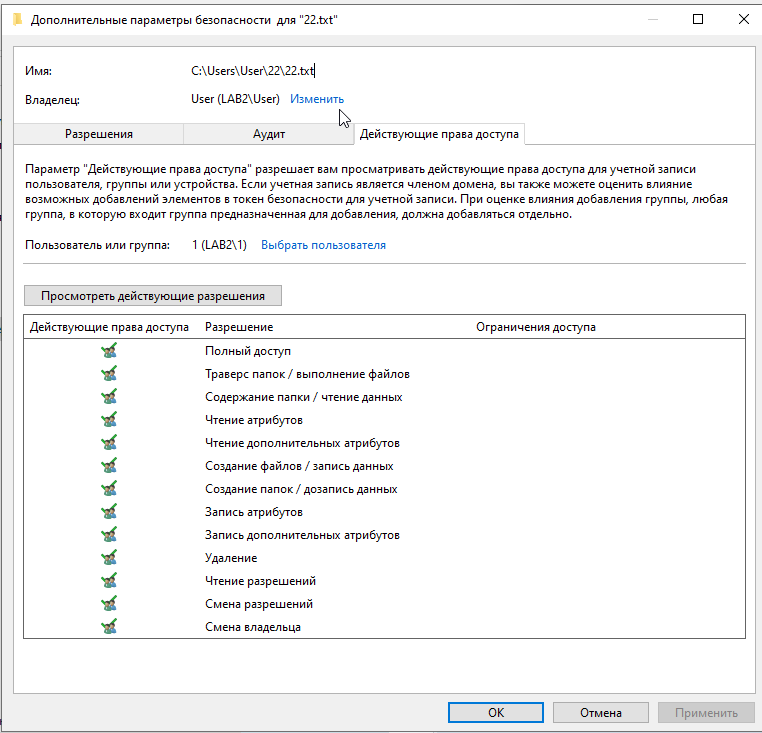
Изменяем права групп согласно заданию

****

Дополнительные разрешения для Пользователей. Как видно, пользователю доступно только чтение файла

****

Дополнительные разрешения для Администратора. Он может делать что угодно.

****

## **Выполните задание в соответствии с номером варианта, номер задания соответствует второй цифре номера варианта (например, 40 вариант – 10 задание, 34 вариант – 4 задание и т.п.). Выполните настройки встроенных механизмов защиты ОС Windows в соответствии с заданием (в отчете: подробное описание настроек встроенных механизмов защиты и выполненных действий со скриншотами).**

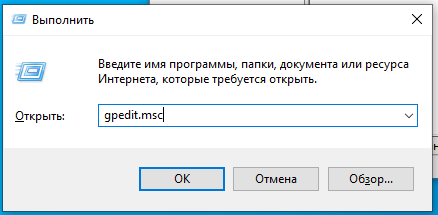
### **Вариант:**

Номер варианта 22.

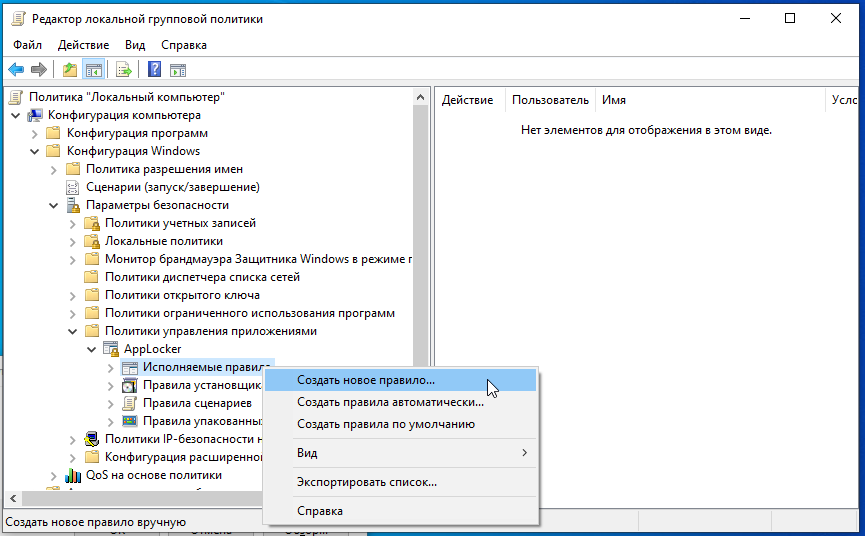
Разрешить встроенными средствами ОС Windows только пользователю System запуск процессов из системного диска. Предотвратить возможность его модификации. Проанализировать возможность и сложность настройки.

### **Решение:**

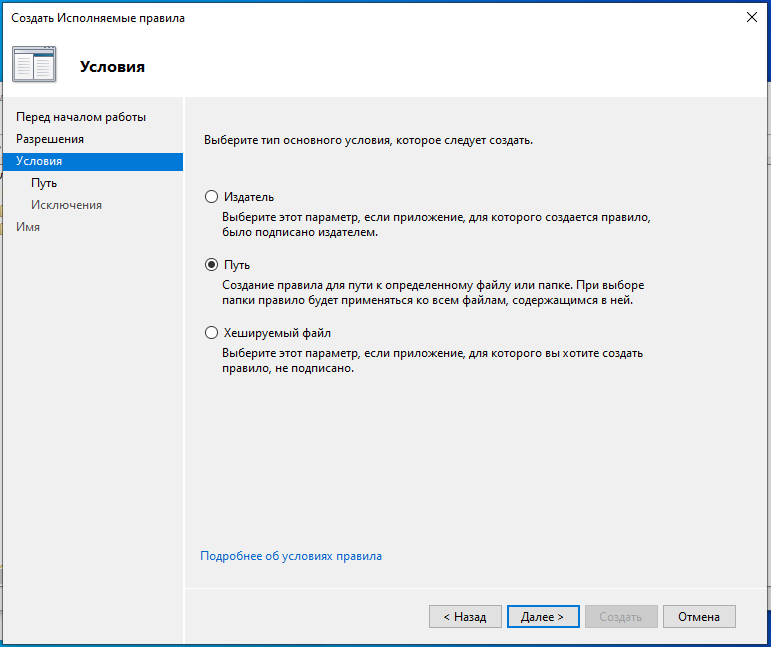
С помощью win+R открываем окно “Выполнить” и пишем:



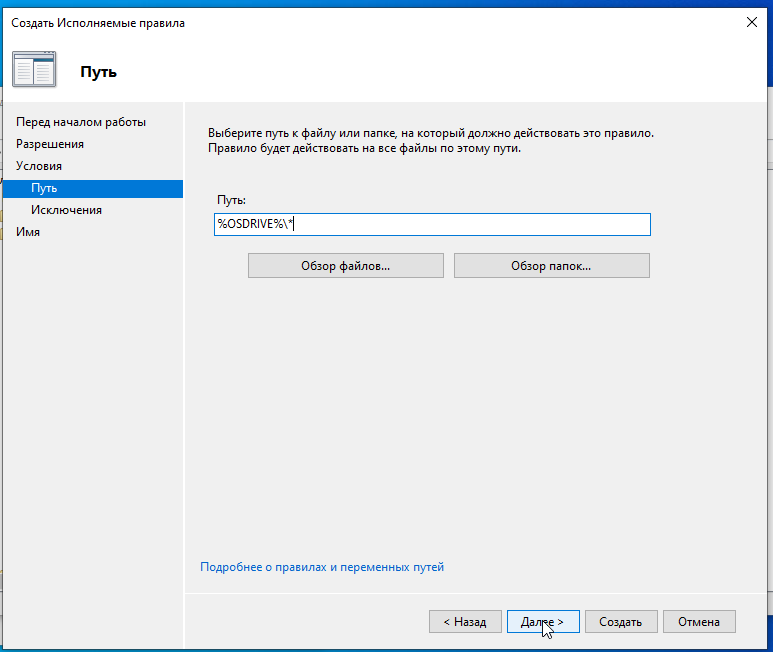
Далее открываем «Политика Локальный компьютер» -> «Конфигурация компьютера» -> «Конфигурация Windows» -> «Параметры безопасности»->«Политики управления приложениями»-> «AppLocker» -> «Используемые правила»:



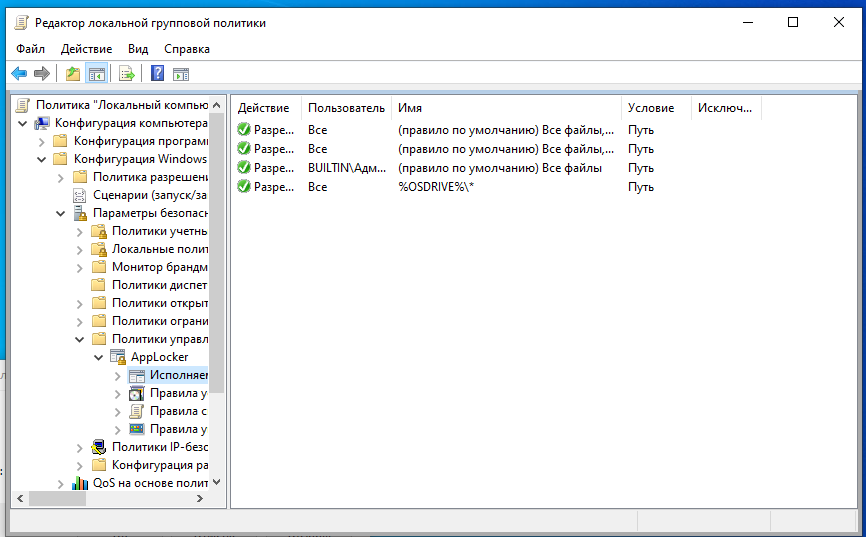
Далее нажимаем правой кнопкой мыши на «Исполняемые правила» и создаем запрет по пути т.е во вкладке «Условия» выбираем «Путь»:



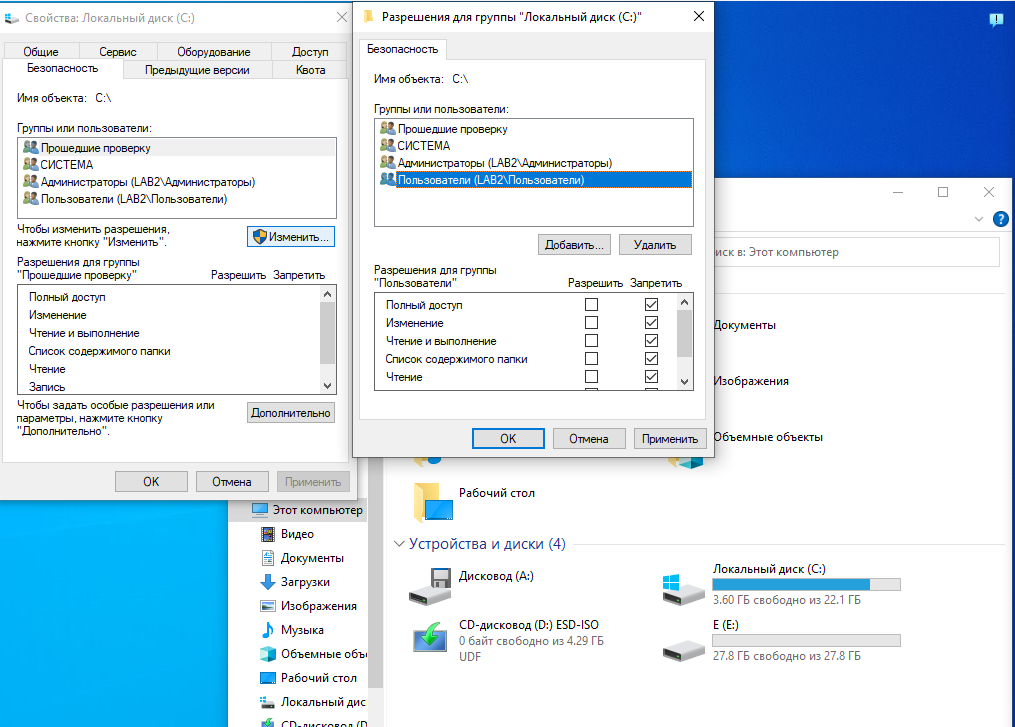
и указываем путь, собственно, во вкладке Path:

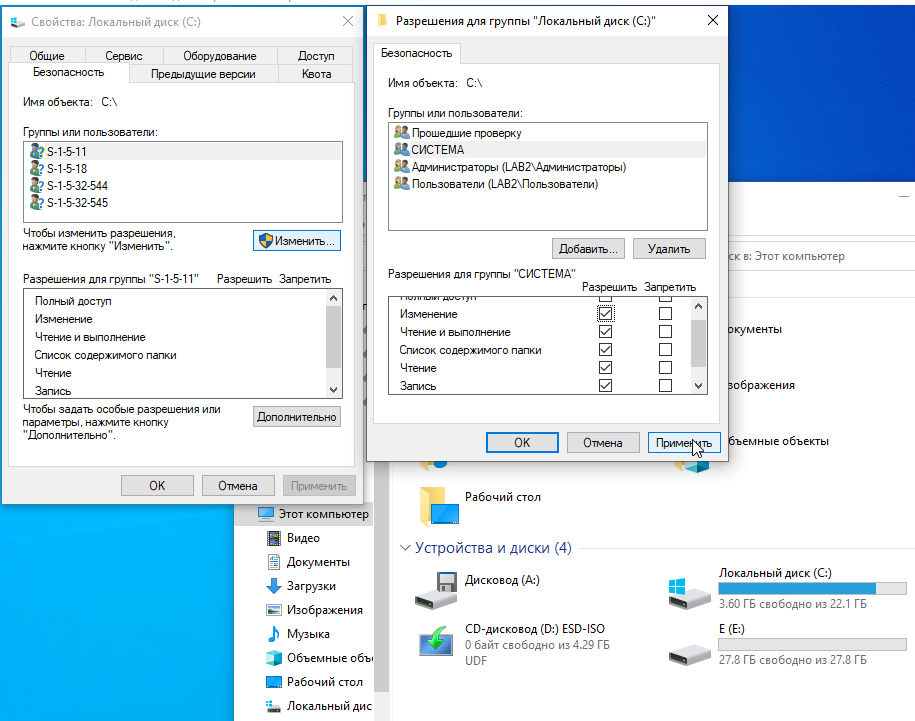


Проверяем:



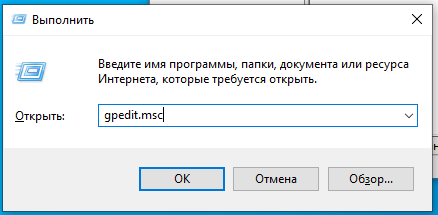
Теперь ограничим модификацию файлов и папок. Для этого в проводнике кликаем правой кнопкой мыши по системному диску (в моем случае диск С: выбираем свойства, переходим на вкладку безопасность и жмем на изменить. И выставляем галочки на запрещение.



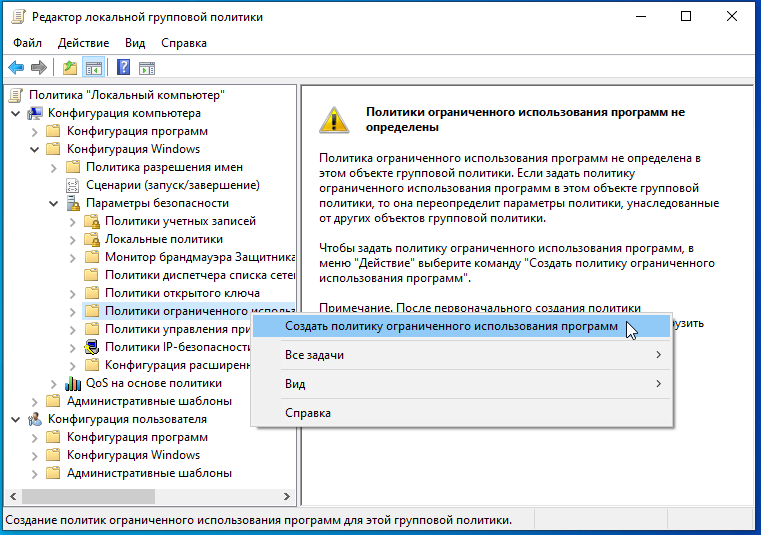


## **Разрешите средствами операционной системы выполнять системные и прикладные программы только из папок %ProgramFiles% и %SystemRoot% (в отчете: подробное описание выполнения задания со скриншотами).**

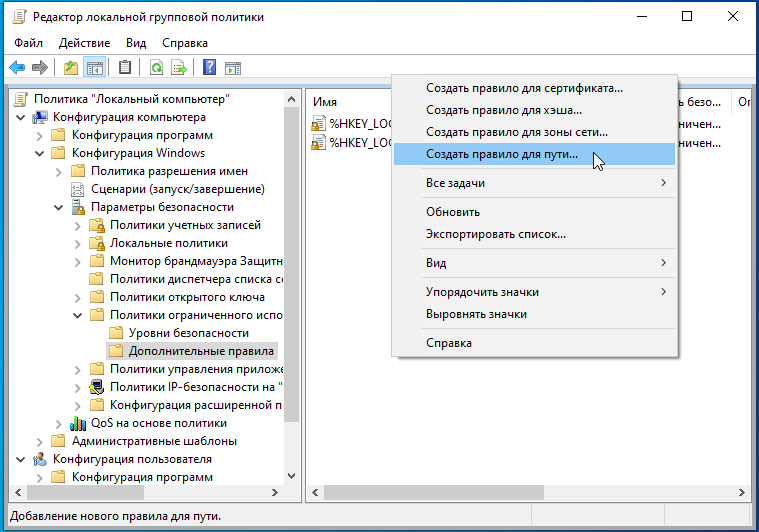
С помощью win+R открываем окно “Выполнить” и пишем:



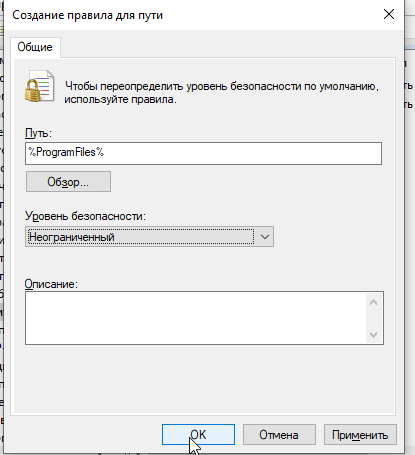
Далее открываем «Политика Локальный компьютер» -> «Конфигурация компьютера» -> «Конфигурация Windows» -> «Параметры безопасности»-> «Политика ограниченного использования программ» и Кликаем правой кнопкой мыши по «Политики ограниченного использования программ», потом «Создать политику ограниченного использования программ»:



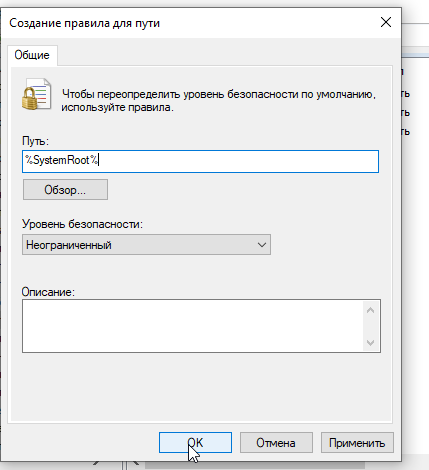
Переходим в подкаталог «Дополнительные правила» и «Создаем новое правило по пути…»:



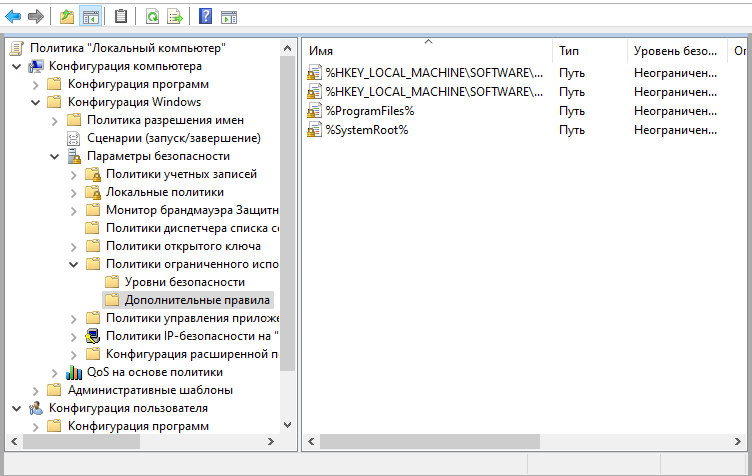
Для папки %ProgramFiles%:



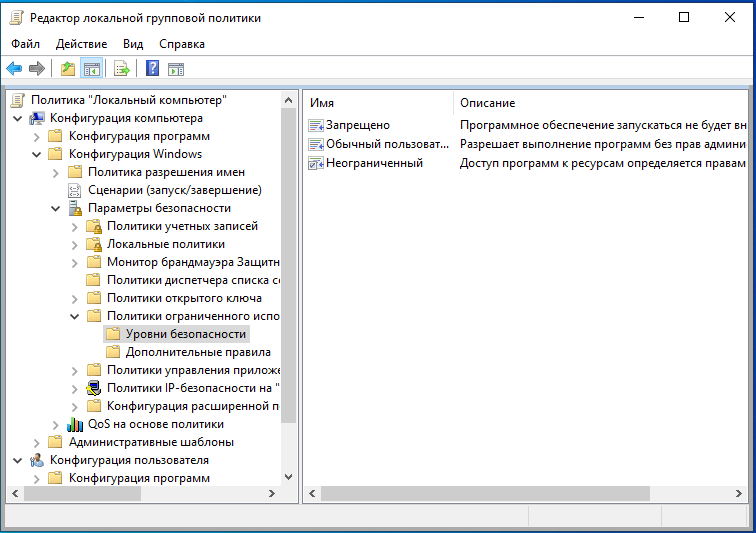
Для папки %SystemRoot%:



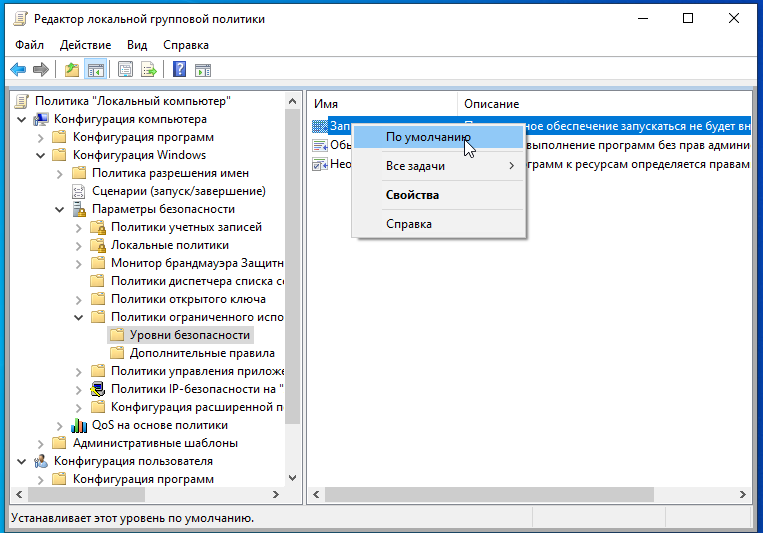
Результат:



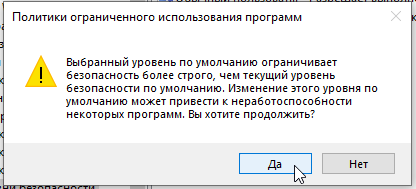
Переходим в каталог «Уровни безопасности»



Устанавливаем «Запрещено по умолчанию». Это необходимо для того, чтобы запретить выполнение всех программ кроме тех, которые находятся в директориях. Которые мы указали ранее.



Соглашаемся



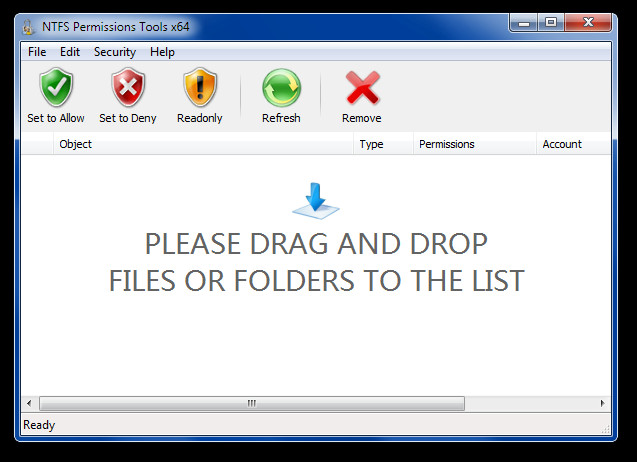
# **Дополнительная часть**

## **Опишите на примерах работу с разрешениями NTFS дополнительных системных программ сторонних производителей (в отчете: описание работы всех программ со скриншотами). Приведите перечень подобных программ (не менее пяти).**

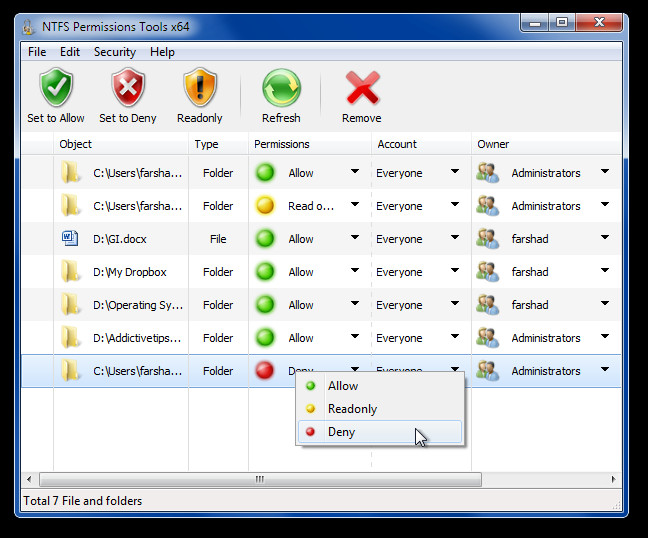
### **Программа 1:**

**Инструмент разрешений NTFS** — портативное приложение, которое позволяет легко назначать права доступа к файлам и папкам, чтобы ограничить доступ новичков или проблемных пользователей к вашим данным (например, на общем компьютере). Часто бывает целесообразно создать несколько учетных записей пользователей на одном ПК и ограничить права локальных пользователей, чтобы гарантировать, что они не вносят нежелательных изменений в систему.

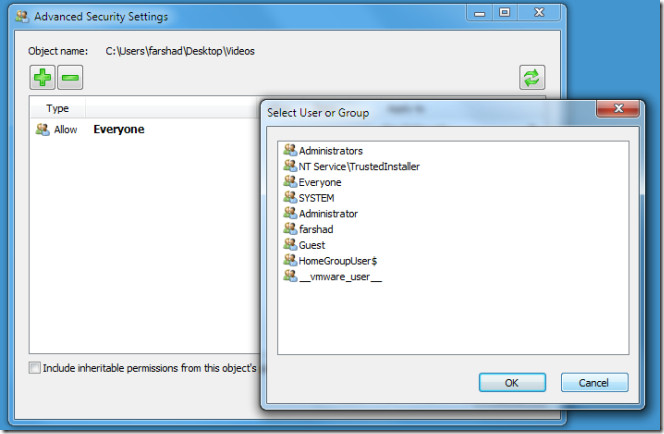
Просто перетащите файлы в основной интерфейс приложения, чтобы начать распределение прав пользователей.



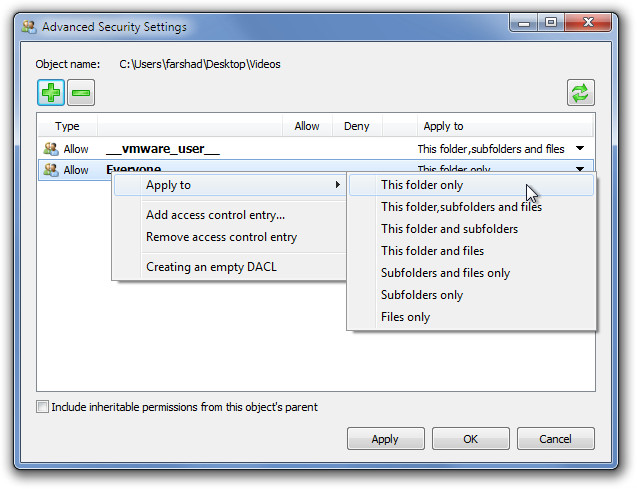
После добавления файлов и папок вы можете назначить права (только чтение, запретить и разрешить) для всех пользователей системы. Если вы впервые используете разрешения NTFS, убедитесь, что вы не выбрали «Разрешить» для «Все», если только вы не хотите сделать файл или папку доступными для всех локальных пользователей, которые имеют доступ к системе.



Поскольку разрешения NTFS влекут за собой довольно сложные процедуры управления правами пользователей, вы можете получить доступ к подробным параметрам, дважды щелкнув любой документ, добавленный в это приложение. Расширенные параметры включают распределение прав в соответствии с группами по умолчанию и созданными пользователем группами на диске NTFS. Вы можете назначать объекты определенным группам (например, «Все» или «Группа домашних пользователей»), чтобы предоставлять или запрещать разрешения конкретному пользователю в соответствии с определенной политикой группы пользователей. Чтобы убедиться, что наследуемые разрешения также применяются во время распределения группы, проверьте *Наследование* флажок.



После выбора группы вы можете дополнительно уточнить настройки, управляя правами пользователей на уровне подпапок, а также добавляя записи управления доступом и создавая пустой DACL (Discretionary Access Control).

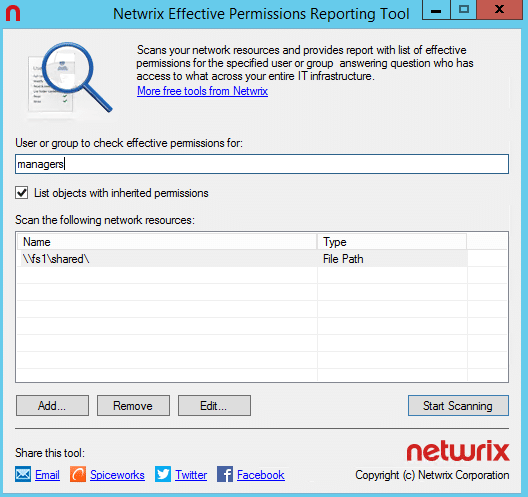


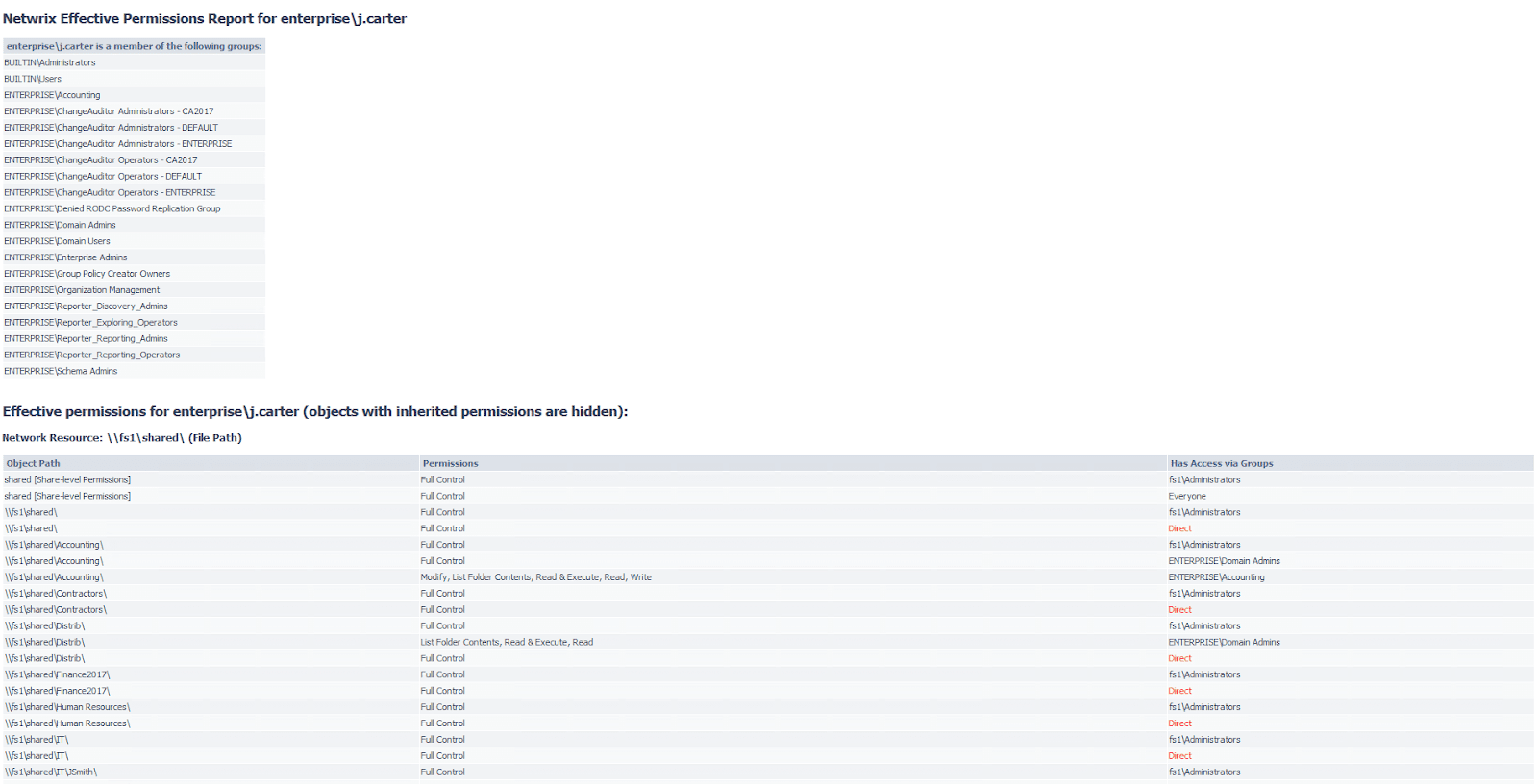
Инструмент разрешений NTFS работает в Windows XP, Windows Vista и Windows 7.

### **Программа 2:**

**Netwrix Effective Permissions Reporting Tool**

Netwrix Effective Permissions Reporting Tool используется для контроля распределения прав работников на файлы в соответствии с разделением по ролям. Она предоставляет отчеты о том у кого на что есть права и каким образом был получен доступ. Бесплатная утилита достаточно проста в использовании, нужно только ввести имя пользователя или группы чтобы посмотреть права. Однако, не предоставляет возможность смотреть права на папки в бесплатной версии, но такая возможность есть у Netwrix Auditor for File Servers (доступен 20 дневный бесплатный период)

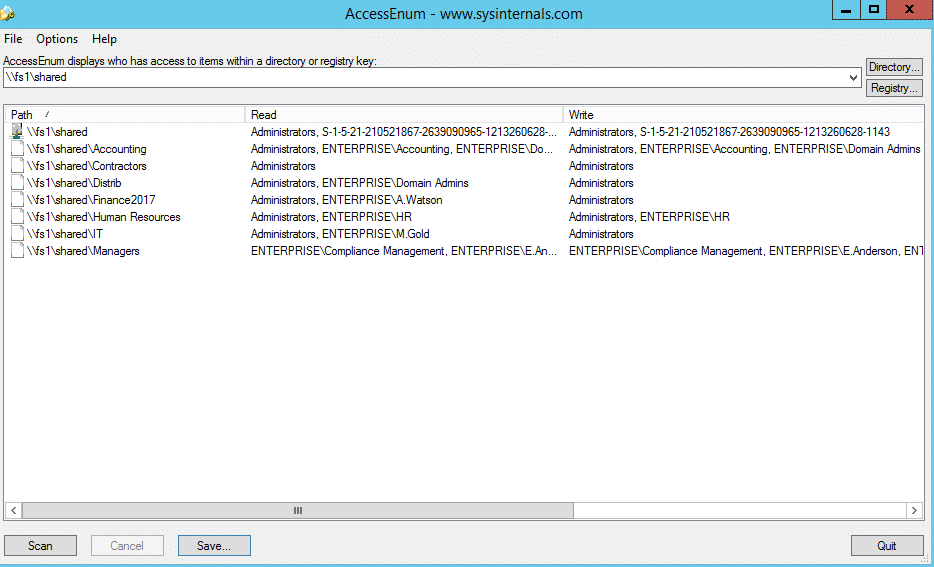


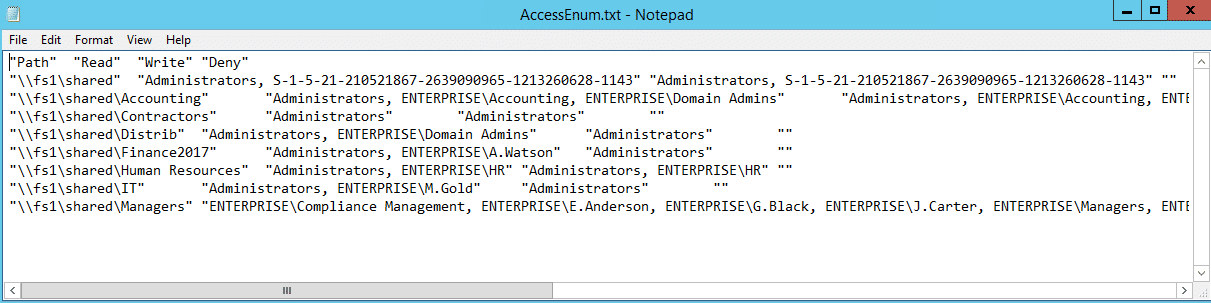


### **Программа 3:**

Microsoft’s Access Enum

AccessEnum это утилита, которая дает возможность посмотреть на всю файловую систему и настройки безопасности в табличном представлении прав на файлы. Но есть ограничение, вывод можно сохранить только в формате txt файла.

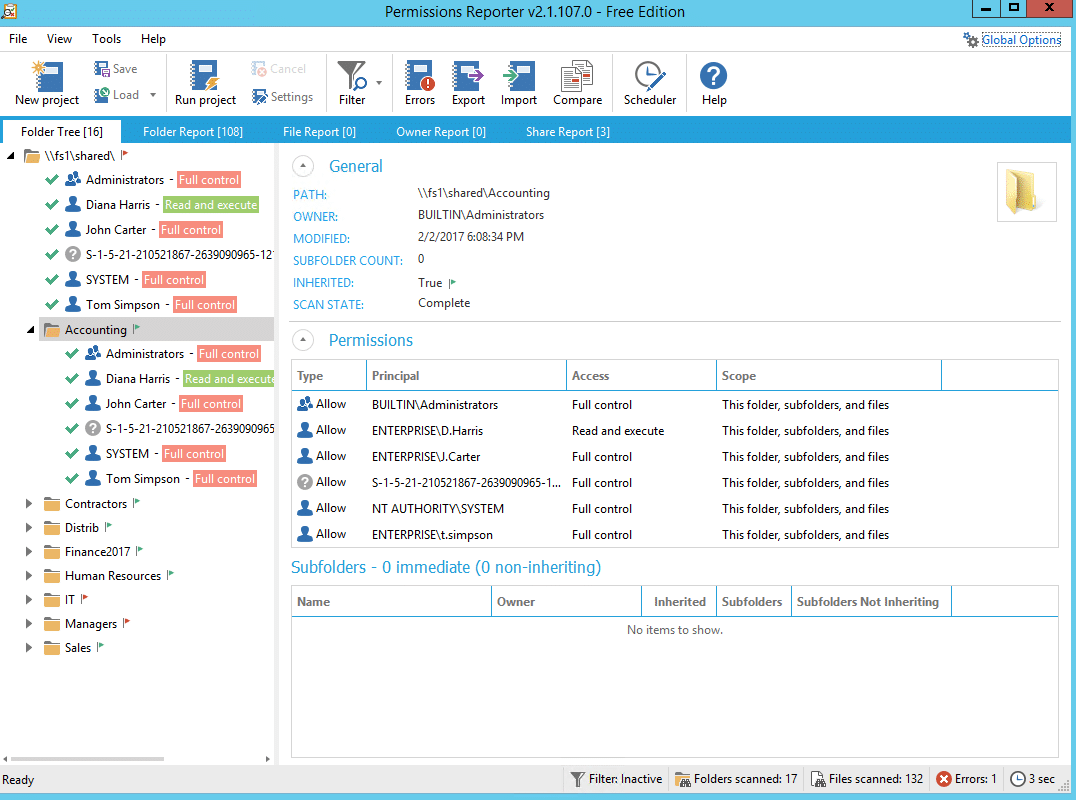


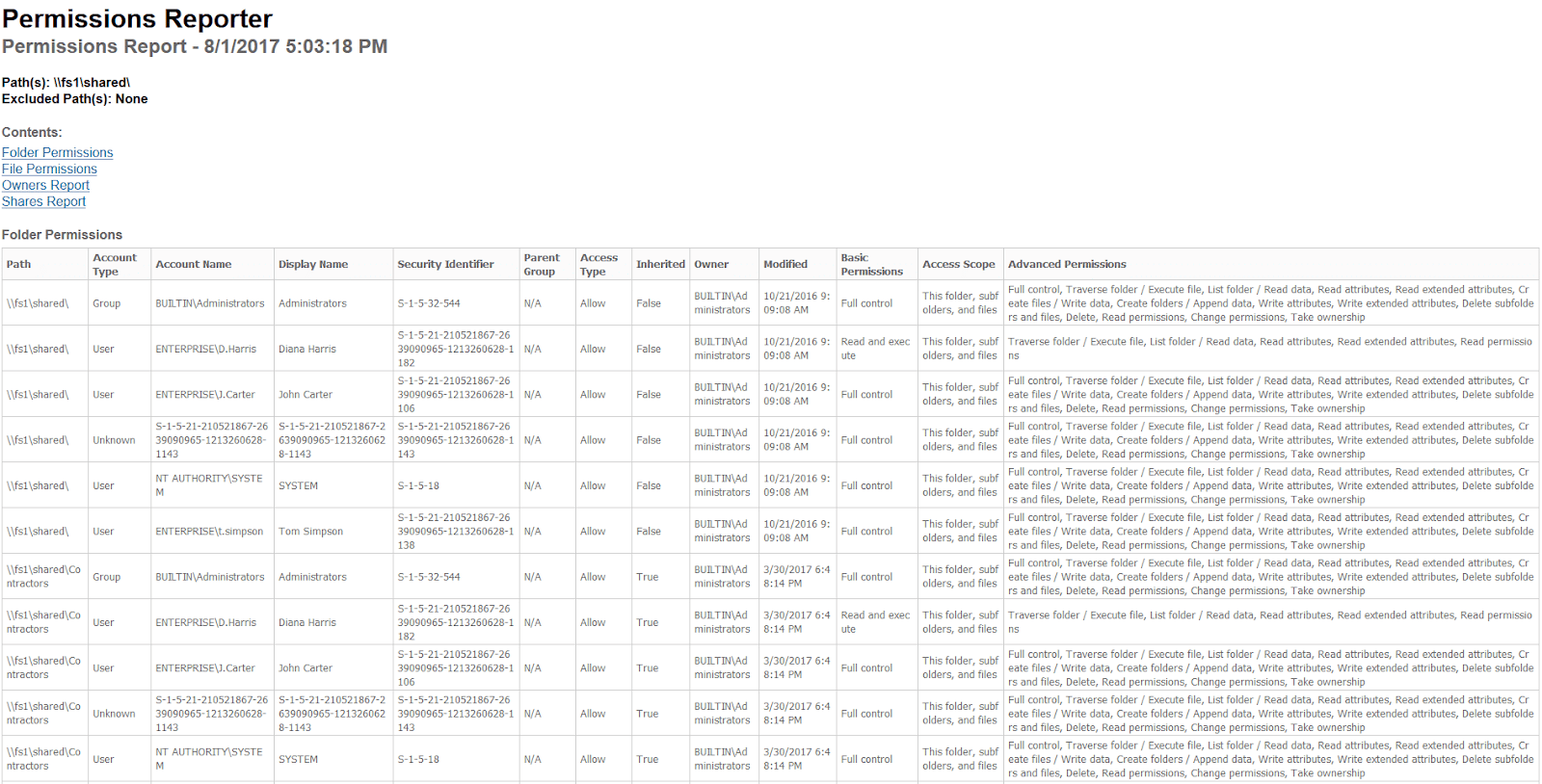


### **Программа 4:**

Permissions Reporter from Key Metric Software

Permissions Reporter - достаточно неплохая утилита для мониторинга разрешений NTFS. С примерно такой же функциональностью, что и у Cjwdev’s NTFS Permissions Reporter tool, но с более приятным глазу интерфейсом. Кроме того, более простой и удобной генерацией и сохранением отчетов. Но сканирование всех разрешений занимает некоторое время и показывает только NTFS разрешения на папку или файл, но не права пользователя.

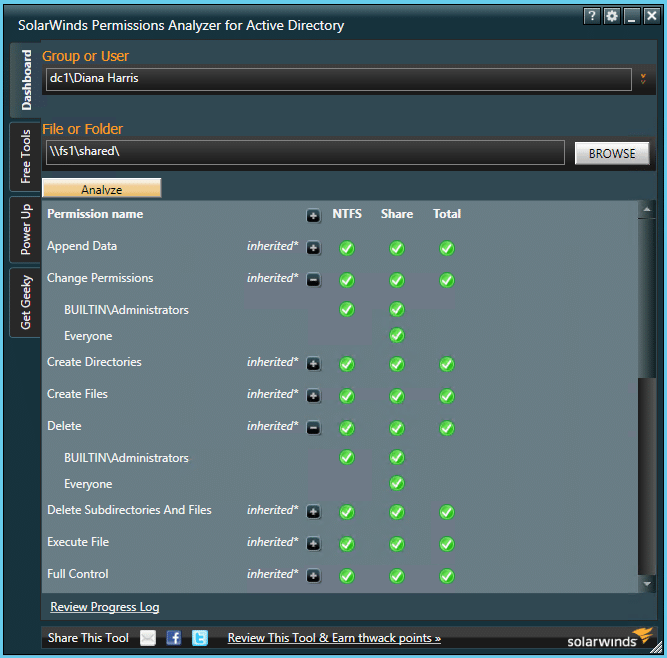




### **Программа 5:**

Permissions Analyzer from SolarWinds

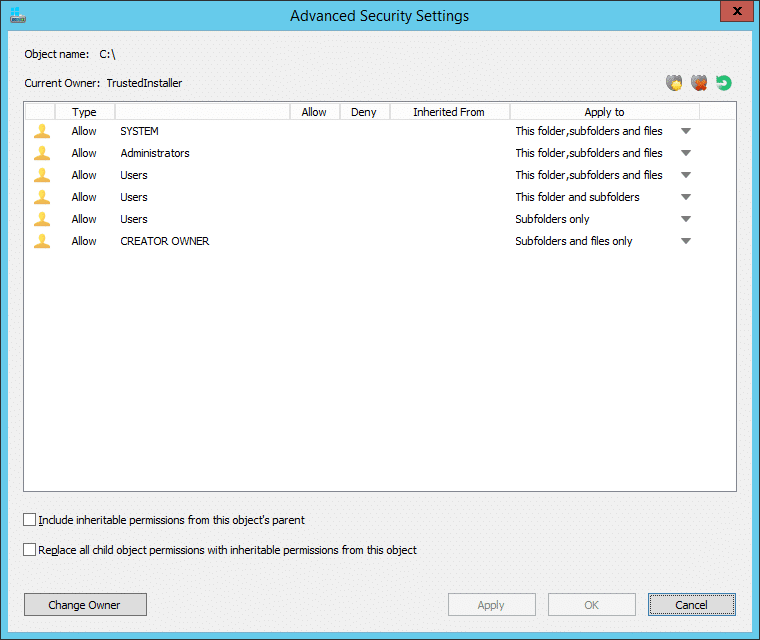
Permissions Analyzer не предоставляет возможность экспорта полученной информации, но для тех, кому нужна детальная информация по правам пользователей, утилита может оказаться полезной. Она достаточно быстро определяет как были получены права пользователя, поддерживает поиск по группе или пользователю и анализирует их, основываясь на принадлежности к группам и выданным правам.



### **Программа 6:**

NTFS Permissions Tools from MajorGeeks.com

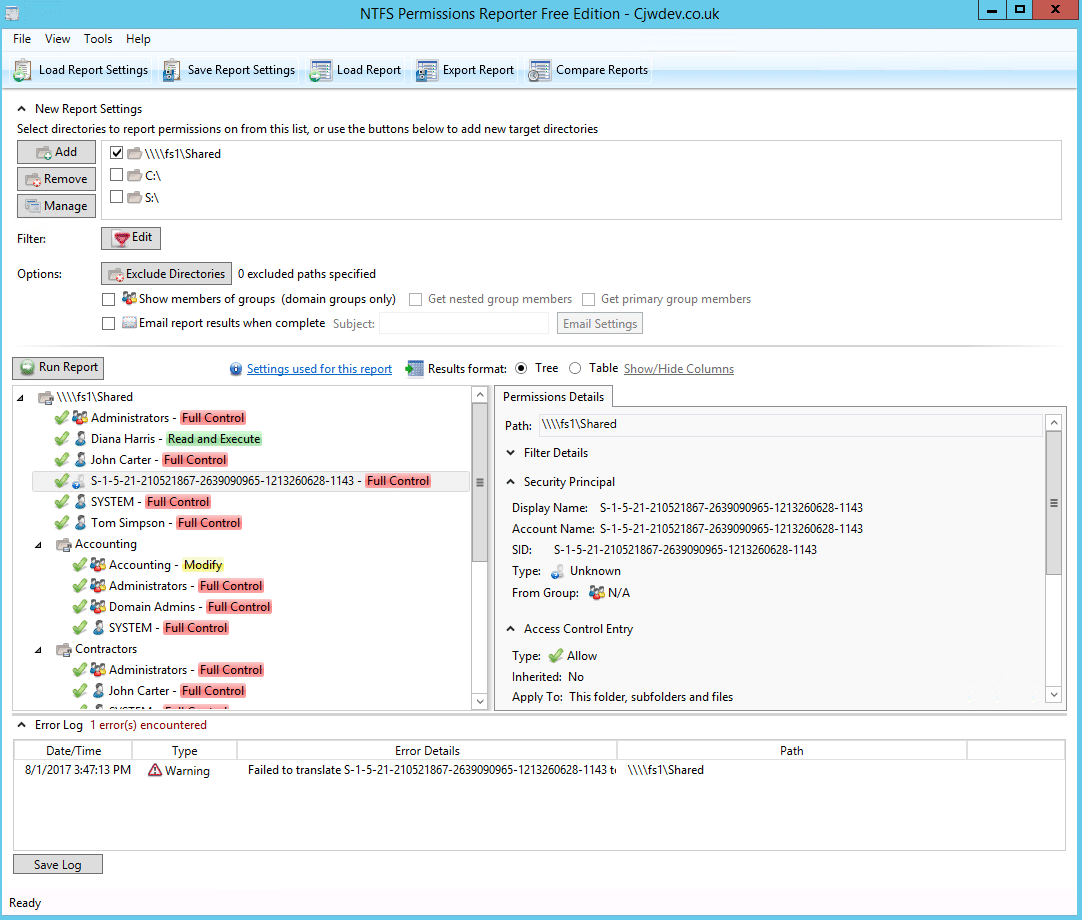
NTFS Permissions Tools представляет возможность за раз применять множество настроек безопасности и разрешений NTFS и делает это быстрее, чем встроенные средства Windows

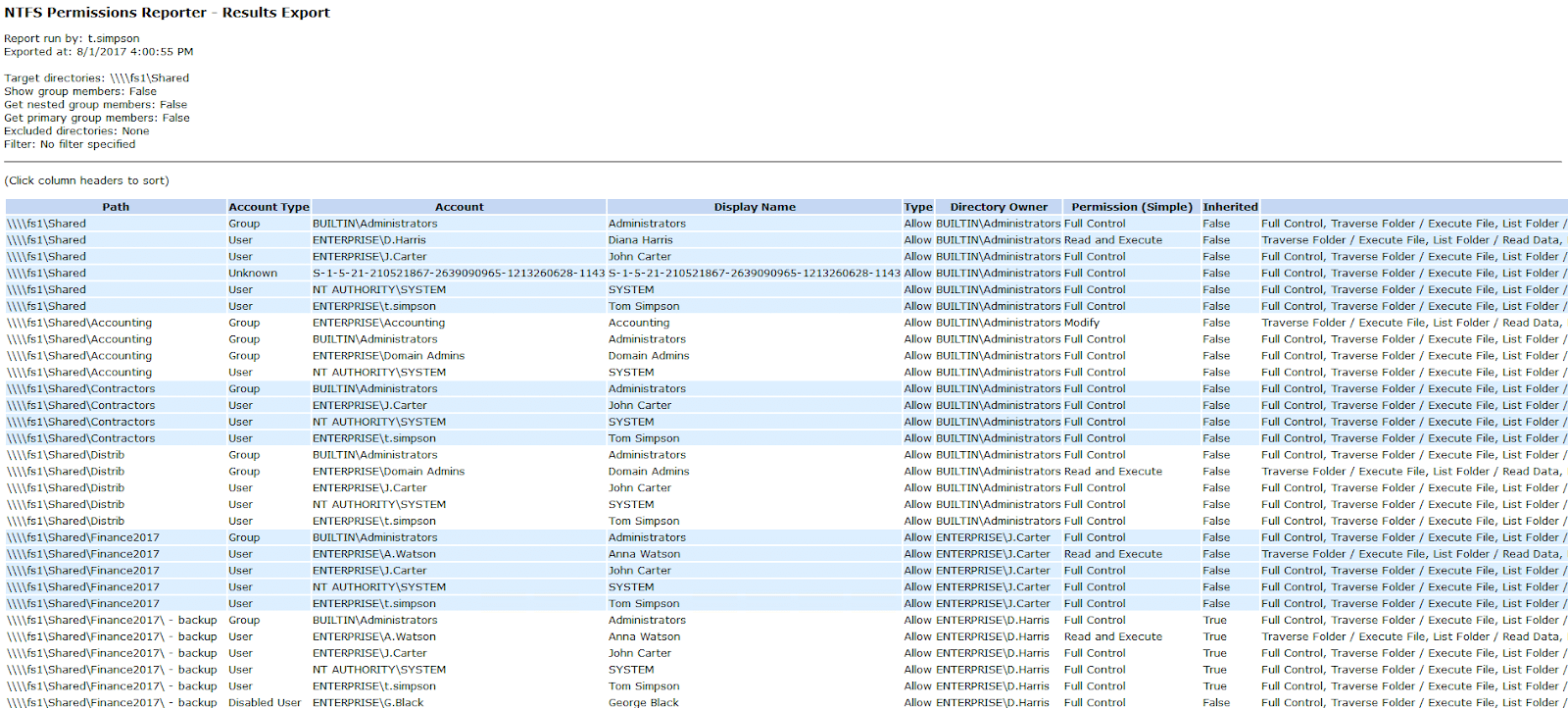


### **Программа 7:**

NTFS Permissions Reporter Free Edition from Cjwdev

Cjwdev’s NTFS Permissions Reporter - неплохая утилита, которая предоставляет возможность экспорта прав на файлы и папки. Она отображает членов группы прямо в отчетах, плюс есть возможность выбора формата отчета (дерево или таблица), помимо этого разные права окрашены разным цветом. Утилита представляет широкие возможности кастомизации и достаточно проста в использовании, но интерфейс может показаться несколько перегруженным и сканирование всех разрешений может занять длительное время. Утилита предоставляет возможность получать отчеты в виде HTML файла. Но нет возможности просмотра разрешений по пользователю, только по папкам и файлам. ц





## **Сравните файловые системы FAT и NTFS (в отчете: сравнение выполнить в виде таблицы).**

***Таблица размещения файлов FAT*** — это файловая система, в основе которой лежит электронная таблица данных. Существуют две наиболее популярные разновидности данной системы: FAT16 и FAT32. По сути, это однотипные таблицы размещения информации с одной лишь разницей: использование 16-ти или 32-х разрядных адресаций кластеров.

***NTFS*** – файловая система, в основе которой лежит использование сводной таблицы с информацией о файлах в начале раздела диска, а уже потом размещаются сами файлы. Данная файловая система использует специализированные структуры данных, что позволяет обеспечить высокую надежность и эффективность использования места на жестком диске.

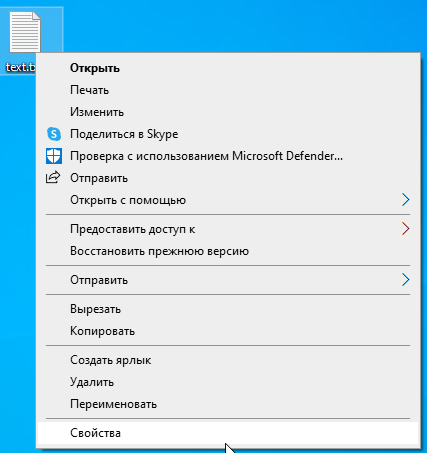
|  |  |  |
| --- | --- | --- |
|  | NTFS | FAT |
| Совместимость | Windows, Linux, Xbox One, и только чтение в Mac | Windows, Mac, Linux, игровые консоли |
| Плюсы | * журналируемая * большие лимиты на размер раздела и файла * шифрование * автоматическое восстановление * рациональное использование места на носителе * высокая производительность при работе с большими файлами * значительная надежность * поддержка сжатия * восстановление системы при сбоях. | * кроссплатформенность * легкость * значительная скорость доступа к файлам средних и малых размеров * низкая требовательность к оперативному запоминающему устройству * меньший износ жесткого диска |
| Минусы | * ограниченная кроссплатформенность * высокая требовательность к объему оперативной памяти * отсутствие доступа NTFS-томов в MS-DOS * снижение производительности при работе с малыми объемами томов | * максимальный размер файла 4 ГБ и раздела 16 ГБ * не журналируемая * уязвимость и возможности сбоя системы * медленные запросы при работе с большими каталогами файлов * отсутствие поддержки малых кластеров * необходимость фрагментации пространства на диске |
| Использование | для установки Windows | внешние носители |

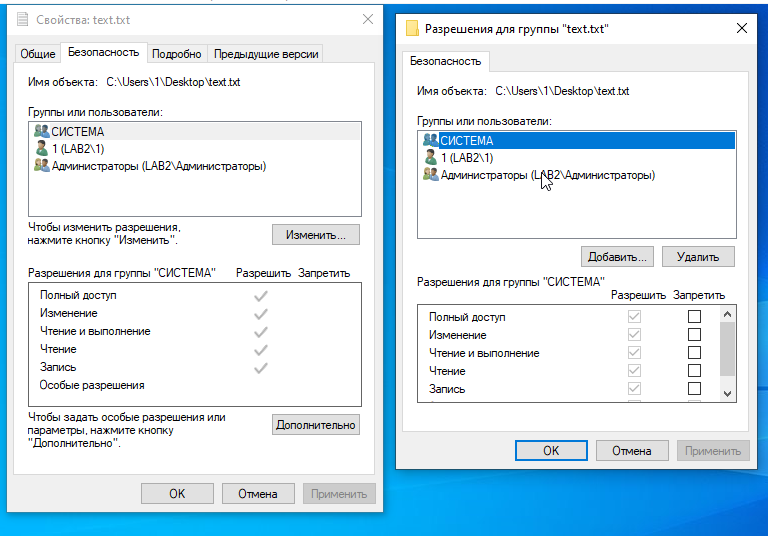
## **Опишите все возможные способы задания разрешений (прав доступа) к файлам и папкам (в отчете: подробное описание выполнения задания со скриншотами).**

### **Способ 1:**

**Проводник**

1. В Проводнике выбрать файл или папку для просмотра параметров безопасности и щелкнуть правой кнопкой мыши.
2. В контекстном меню выбрать команду Свойства и перейти на вкладку Безопасность диалогового окна.
3. В списке Имя выбрать пользователя, контакт, компьютер или группу разрешения которых нужно изменить





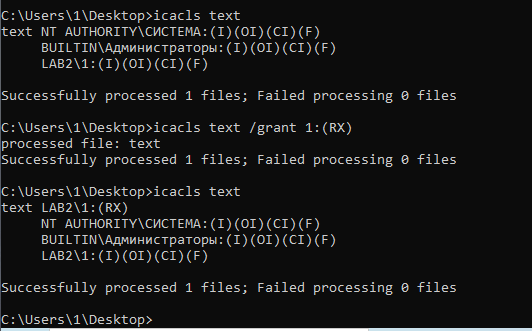
### **Способ 2:**

**icacls**

Используя команду: icacls "<путь до папки/файла>" /grant <кому>:

Основные права:

* F (full access)
* M (modify access)
* RX (read and execute access)
* R (read-only access)
* W (write-only access)



# **Вывод**

В результате выполнения данной лабораторной работы я познакомился с файловыми системами FAT32 и NTFS. Кроме того, я узнал об работе программы с разрешениями и научился задавать права доступа на различные файлы.