## федеральное государственное автономное образовательное учреждение высшего образования

**МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ (ВЫСШАЯ ШКОЛА ПЕЧАТИ И МЕДИАИНДУСТРИИ)**

**(Факультет информационных технологий)**

***(Институт Принтмедиа и информационных технологий)***

***Кафедра Информатики и информационных технологий***

## направление подготовки 09.03.02

**«Информационные системы и технологии»**

ЛАБОРАТОРНАЯ РАБОТА № 9

## Дисциплина: Операционные системы Тема: Управление правами доступа Windows

**Выполнил(а): студент(ка) группы 221-3711**

Ежов Т.А.

(Фамилия И.О.)

**Дата, подпись**

(Дата) (Подпись)

## Проверил:

(Фамилия И.О., степень, звание) **(Оценка)**

**Дата, подпись**

(Дата) (Подпись)

## Замечания:

**Москва 2023**

# Задачи:

1. Изучить систему распределения прав доступа в Windows;
2. Изучить создание пользователей и групп;
3. Создать персонализированные директории;
4. Создать обменную директорию, в которой права записи имеет

отдельная группа пользователей, а права чтения – все пользователи;

# Система распределения прав доступа

Компьютеры под управлением поддерживаемой версии Windows могут управлять использованием системных и сетевых ресурсов с помощью

взаимосвязанных механизмов проверки подлинности и авторизации. После проверки подлинности пользователя операционная система Windows

использует встроенные технологии авторизации и управления доступом для реализации второго этапа защиты ресурсов: определения того, имеет ли пользователь, прошедший проверку подлинности, правильные разрешения на доступ к ресурсу.

Общие ресурсы доступны пользователям и группам, не являющимся владельцем ресурса, и они должны быть защищены от

несанкционированного использования. В модели управления доступом пользователи и группы (также называемые субъектами безопасности) представлены уникальными идентификаторами безопасности (SID). Им назначаются права и разрешения, которые информируют операционную

систему о том, что может сделать каждый пользователь и группа. У каждого ресурса есть владелец, который предоставляет разрешения субъектам

безопасности. Во время проверка управления доступом эти разрешения проверяются, чтобы определить, какие субъекты безопасности могут получить доступ к ресурсу и как они могут получить к нему доступ.

Субъекты безопасности выполняют действия (включая чтение, запись, изменение или полный контроль) с объектами. Объекты включают файлы, папки, принтеры, разделы реестра и объекты доменные службы Active Directory (AD DS). Общие ресурсы используют списки управления доступом

(ACL) для назначения разрешений. Это позволяет диспетчерам ресурсов применять управление доступом следующими способами:

* Запрет доступа для несанкционированных пользователей и групп
* Установка четко определенных ограничений на доступ, предоставляемый авторизованным пользователям и группам

Владельцы объектов обычно предоставляют разрешения группам

безопасности, а не отдельным пользователям. Пользователи и компьютеры, добавленные в существующие группы, принимают разрешения этой группы. Если объект (например, папка) может содержать другие объекты (например, вложенные папки и файлы), он называется контейнером. В иерархии

объектов связь между контейнером и его содержимым выражается путем ссылки на контейнер в качестве родительского. Объект в контейнере

называется дочерним, а дочерний наследует параметры управления доступом родительского объекта. Владельцы объектов часто определяют разрешения для объектов-контейнеров, а не для отдельных дочерних объектов, чтобы упростить управление доступом

## Практическое применение

Администраторы, использующие поддерживаемую версию Windows, могут уточнить приложение и управление доступом к объектам и субъектам, чтобы обеспечить следующую безопасность:

* Защитите большее количество и разнообразие сетевых ресурсов от неправильного использования.
* Подготовьте пользователей для доступа к ресурсам в соответствии с политиками организации и требованиями их заданий.
* Разрешить пользователям получать доступ к ресурсам с различных устройств в различных расположениях.
* Регулярно обновляйте возможность доступа пользователей к ресурсам по мере изменения политик организации или при изменении заданий пользователей.
* Учитывайте растущее число сценариев использования (например, доступ из удаленных расположений или с быстро расширяющегося спектра устройств, таких как планшетные компьютеры и мобильные телефоны).
* Выявляйте и устраняйте проблемы с доступом, когда законные пользователи не могут получить доступ к ресурсам, которые им необходимы для выполнения своих задач.

## Разрешения

Разрешения определяют тип доступа, который предоставляется пользователю или группе для объекта или свойства объекта. Например, группе "Финансы" можно предоставить разрешения на чтение и запись для файла с именем Payroll.dat.

С помощью пользовательского интерфейса управления доступом можно задать разрешения NTFS для таких объектов, как файлы, объекты Active Directory, объекты реестра или системные объекты, такие как процессы. Разрешения могут быть предоставлены любому пользователю, группе или компьютеру. Рекомендуется назначать разрешения группам, так как это повышает производительность системы при проверке доступа к объекту.

Для любого объекта можно предоставить разрешения на:

* Группы, пользователи и другие объекты с идентификаторами безопасности в домене.
* Группы и пользователи в этом домене и любых доверенных доменах.
* Локальные группы и пользователи на компьютере, где находится объект.

Разрешения, присоединенные к объекту, зависят от типа объекта. Например, разрешения, которые могут быть присоединены к файлу, отличаются от

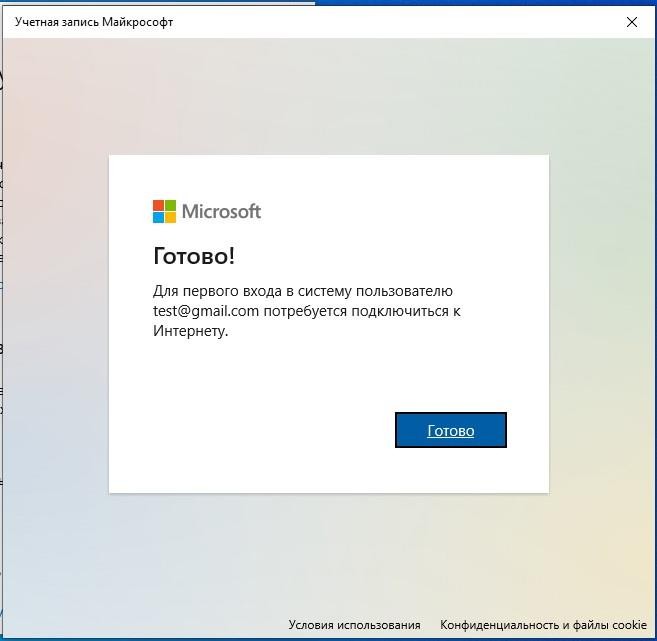
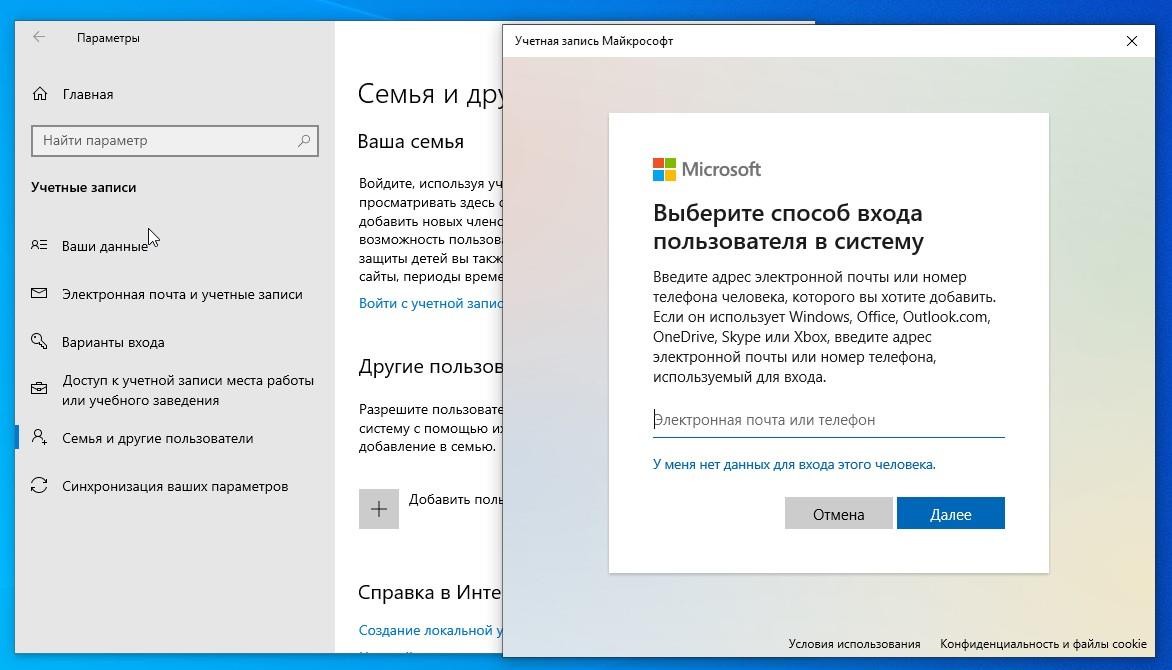
разрешений, которые могут быть присоединены к разделу реестра. Однако некоторые разрешения являются общими для большинства типов объектов. Ниже перечислены распространенные разрешения.

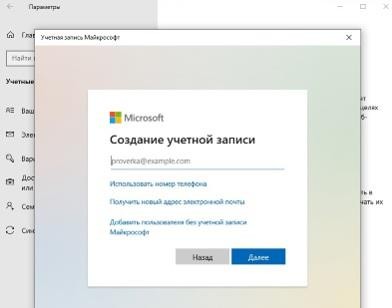
* Read
* Изменить Смена владельца
* Delete

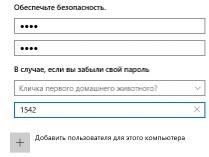
При настройке разрешений вы указываете уровень доступа для групп и пользователей. Например, можно разрешить одному пользователю читать содержимое файла, другому пользователю вносить изменения в файл и запретить другим пользователям доступ к файлу. Вы можете задать аналогичные разрешения на принтерах, чтобы некоторые пользователи могли настроить принтер, а другие — только печать.

Если необходимо изменить разрешения на файл, можно запустить Windows Обозреватель, щелкнуть имя файла правой кнопкой мыши и выбрать **пункт Свойства**. На вкладке

**Безопасность** можно изменить разрешения для файла Создание пользоаваткль и групп

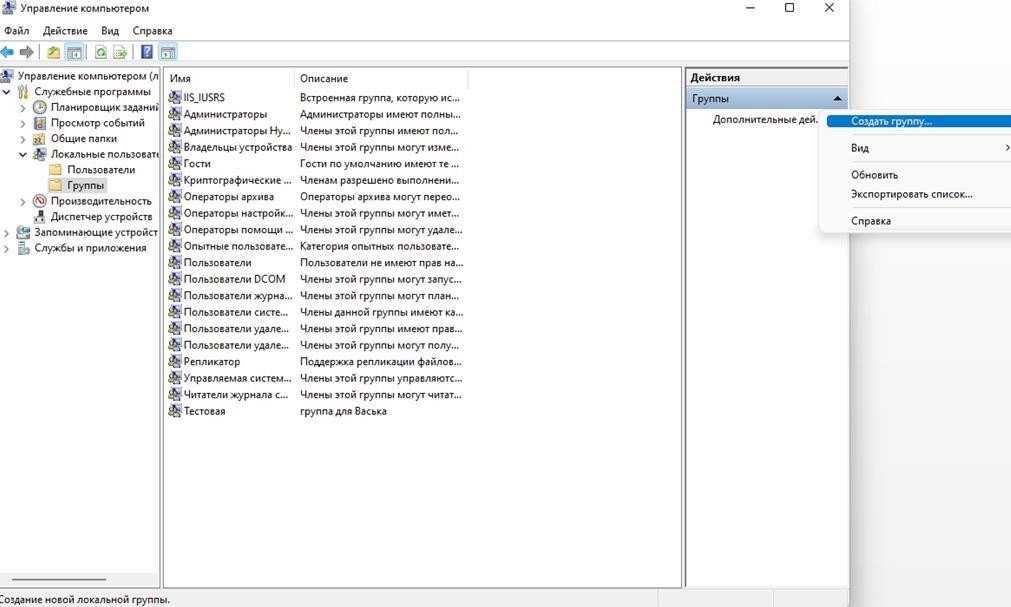


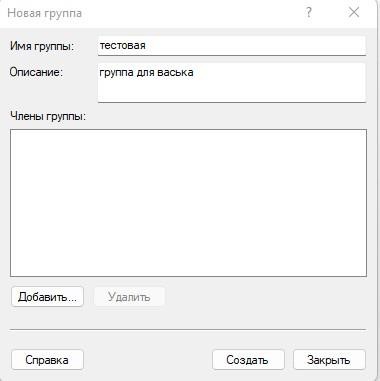


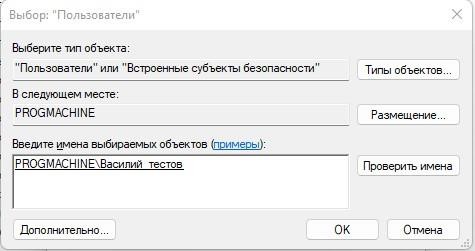


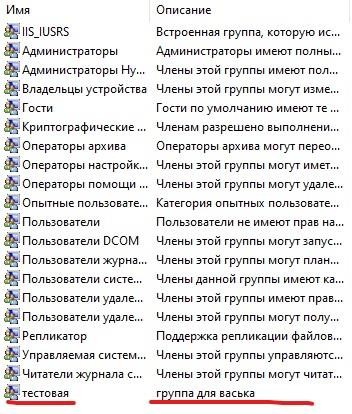
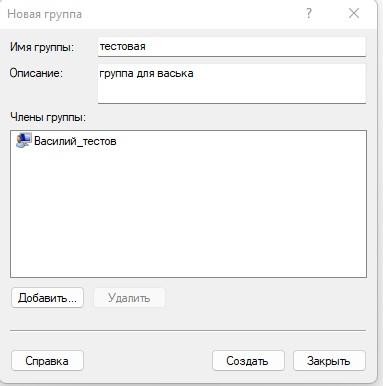
Для добавление группы заходим в управление

компьютером>>служебные>>программы>>локальные>>пользовате ли>>группы

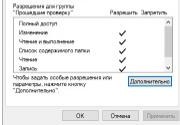


Создаем группу





Создание персонализированной директории Создадим папку

жмем

дополнительно

Далее добавить и устанавливаем необходимые разрешения

Теперь для нашего пользователя, например, нельзя переименовать папку

Создание обменной директории

Нажимаем дополнительные параметры безопасности папки и добавляем наш субъект. Из общих разрешений для субъекта выбираем только чтение



Разрешаем только чтение

Папка откроется. Но ,чтобы создать папку, у нас нету прав.