Лабораторная работа № 1

**Создание базовой конфигурации**

Цель работы: Изучить типы учетных записей пользователей,

ознакомиться с основными принципами управления учетными записями. Изучить основы разграничение доступа пользователей.

Операционные системы: Windows 7, Windows 8.1, Windows 10

Краткий теоретический материал

Учетная запись пользователя определяет схему взаимодействия пользователя с компьютером и персонализирует ее. Например, учетная запись пользователя определяет, к каким приложениям, папкам и файлам у вас есть доступ, какие изменения вы можете вносить в работу компьютера, а также задает персональные настройки, такие как макет начального экрана, фон рабочего стола и заставка. При создании отдельных учетных записей для разных пользователей не обязательно дублировать параметры для них. Это означает, что вы можете ограничить доступ к папке входящих писем, социальным сетям и другим файлам, а также устанавливать различные цвета и фоны рабочего стола для разных учетных записей.

Учетная запись в операционной системе Windows - это не что иное, как способ идентификации пользователей, благодаря чему операционная система может применять конкретные параметры для каждого пользователя.

В операционных системах Windows тип учетной записи пользователя определяет, какие задачи может выполнять на компьютере пользователь, в некоторых случаях могут потребоваться права администратора для выполнения некоторых задач или для использования некоторых приложений. Ниже описаны три типа учетных записей на компьютере с системой Windows:

* Учетные записи обычных пользователей предназначены для повседневной работы.
* Учетные записи администратора предоставляют полный контроль над компьютером и должна использоваться только при необходимости.
* Учетные записи гостя предназначены для временного доступа на компьютер.

По способу авторизации можно выделить две группы:

* локальная учетная запись;
* сетевая учетная запись, для авторизации под которой нужно соединяться с удаленным сервером Microsoft.

Особенностью сетевых записей является то, что именно используя их, Вы получаете все возможности новой операционной системы, а также доступ ко всем сервисам. Единственная проблема этих записей: если не будет соединения с сервером авторизации Microsoft, то вход в компьютер не будет выполнен. Что касается локальных записей, то они ограничены по доступу к сетевым службам системы, но для полноценной работы более чем самодостаточны.

Существует несколько способов создания учетных записей:

* Создание учетных записей пользователей для компьютеров, состоящих в рабочей группе:
  + Создание учетной записи при помощи диалога «Управление учетными записями пользователей».
  + Создание учетной записи при помощи диалога «Учетные записи пользователей».
  + Создание учетной записи при помощи оснастки «Локальные пользователи и группы».
  + Создание учетной записи при помощи командной строки (команда net user).
* Создание учетных записей пользователей для компьютеров, состоящих в домене:
  + Создание пользователей при помощи оснастки «Active Directory - пользователи и компьютеры».
  + Создание пользователей с помощью командной строки (команда dsadd user).
  + Импорт пользователей с помощью команды CSVDE.
  + Импорт пользователей с помощью команды LDIFDE.
  + Создание пользователей с помощью Windows PowerShell.
  + Создание пользователей с помощью VBScript.

Для того чтобы произвести изменения в учетный записей, Вы должны обладать правами администратора, так как именно наличие этих прав и даст возможность проводить манипуляции с учетной записью. Сразу следует отметить, что нельзя удалить единственного администратора, а также перевести его в разряд пользователей, так как это приведет к неуправляемости компьютером. Администратор может управлять любой учетной записью, даже не имея пароля к ней.

Для того чтобы сменить тип учетной записи, нужно открыть «Панель управления», переключить режим отображения в «Категория» после чего выбрать раздел «Учетная запись». После этого стоит перейти по ссылке «Изменение типа учетной записи». Далее нужно выбрать нужную учетную запись и изменить ее тип, использовав появившееся меню. Далее выбрать роль учетной записи (администратор или обычный пользователь).

Изменение пароля выполняется также из панели управления, далее «Учетная запись», затем «Изменение типа учетной записи» (это поможет отобразить сразу всех пользователей). Выбираем нужного пользователя, после чего изменяем нужные данные. Пароль меняется администратором без сохранения предыдущего. Чтобы изменить имя или пароль следует воспользоваться пунктами меню. После чего подтвердить изменения, нажав на кнопку. Имя пользователя изменяется аналогичным образом.

Файловая система (file system) - способ организации данных в виде файлов на устройствах внешней памяти (жестких и оптических дисках, устройствах флеш-памяти и т. п.). Файловая система представляет собой иерархическое хранилище пользовательских и системных файлов, а также областей данных. В операционных системах существует большое количество файловых систем.

Windows поддерживает несколько файловых систем для различных внешних устройств:

* NTFS - основная файловая система семейства Windows NT;
* FAT (File Allocation Table - таблица размещения файлов) - простая файловая система используемая Windows для устройств флеш памяти, а также для совместимости с другими операционными системами при установке на диски с множественной загрузкой. Основным элементом этой файловой системы является таблица размещения файлов FAT (по имени которой названа вся файловая система), необходимая для определения расположения файла на диске. Существует три варианта FAT, отличающихся разрядностью идентификаторов, указывающих размещение файлов: FAT12, FAT16 и FAT32;
* exFAT (Extended FAT - расширенная FAT) - развитие файловой системы FAT, использующее 64 разрядные идентификаторы. Применяется в основном для устройств флеш-памяти;
* CDFS (CD ROM File System) - файловая система для CD дисков, объединяющая форматы ISO 96601 и Joliet2;
* UDF (Universal Disk Format - универсальный формат дисков) - файловая система для CD и DVD дисков, разработанная для замены ISO 9660.

Основу политики безопасности для компьютерной системы любой организации составляют правила разграничения доступа к объектам компьютерной системы. Разграничение доступа к компьютерным ресурсам базируется на различных моделях управления доступом.

Дискреционная модель разграничения доступа предполагает назначение каждому объекту списка контроля доступа, элементы которого определяют права доступа к объекту конкретного субъекта. Правом редактирования дискреционного списка контроля доступа обычно обладают владелец объекта и администратор безопасности. Эта модель отличается простотой реализации, но возможна утечка конфиденциальной информации даже в результате санкционированных действий пользователей.

В операционных системах Microsoft Windows обычно применяется дискреционное управление доступом к объектам. Объекты разграничения доступа в Windows имеют дескриптор безопасности, содержащий информацию о владельце объекта (его идентификаторе безопасности SID, Security Identifier) и дискреционном списке управления доступом к объекту (Discretionary Access Control List, DACL), правом редактирования которого обладают владелец объекта и администратор. Владелец файла может лишить администратора права изменения разрешений на доступ к объекту. Администратор обладает специальной привилегией смены владельца на другого пользователя, обладающего такой же специальной привилегией (например, на самого себя).

Разграничение доступа к файлам и папкам возможно с помощью Проводника Windows (вкладки Безопасность функций Свойства контекстного меню выделенного объекта).

Права доступа к объектам в операционной системе Windows делятся на специальные, стандартные (общие) и родовые (generic). Специальные права зависят от типа объекта разграничения доступа. Например, к файлам и папкам могут применяться следующие специальные права:

* обзор папок (выполнение файлов);
* содержание папки (чтение данных из файла);
* чтение атрибутов;
* чтение дополнительных атрибутов;
* создание файлов (запись данных в файл);
* создание папок (дозапись данных в файл);
* запись атрибутов;
* запись дополнительных атрибутов;
* удаление подпапок и файлов (только для папок).

Стандартные права доступа к объектам операционной системы Windows не зависят от типа объекта. Определены следующие стандартные права доступа:

* удаление;
* чтение разрешений;
* смена разрешений;
* смена владельца;
* синхронизация.

Каждое из родовых разрешений представляет собой логическую группу специальных и стандартных разрешений. Например, для файлов и папок родовое право доступа «Изменение» включает все разрешения кроме «Удаление подпапок и файлов», «Смена разрешений» и «Смена владельца».

Существующие разрешения для пользователя:

* полный доступ - пользователь, принадлежащий к указанной группе, может выполнять любые операции над папкой;
* изменить - означает возможность модификации файлов или папки, в зависимости от того, чем является защищаемый объект;
* чтение и выполнение - возможность чтения и исполнения файлов папки;
* список содержимого папки - доступ к списку содержимого папки;
* чтение - доступ на чтение содержимого папки;
* запись - разрешение на запись означает возможность, изменять или создавать новые файлы, а если такое право доступа стоит для одного файла, то и возможность записи в него группе пользователей или одному пользователю, для которого рядом с этим правом доступа стоит флажок;
* особые разрешения - используются для уточнения набора прав, которым может обладать пользователь, для их редактирования следует нажать кнопку Дополнительно, выбрать из списка требуемого пользователя, а потом нажать кнопку «Изменить».

Существующий в Windows механизм наследования облегчает администраторам задачи назначения разрешений и управления ими. Благодаря этому механизму разрешения, установленные для контейнера, автоматически распространяются на все объекты этого контейнера. Например, файлы, создаваемые в папке, наследуют разрешения этой папки.

Если требуется предотвратить наследование разрешений, при настройке особых (отличающихся от родовых) разрешений на доступ к родительской папке (разделу реестра) можно выбрать режим «Применять эти разрешения к объектам и контейнерам только внутри этого контейнера». В случаях, когда необходимо отменить наследование разрешений только для некоторых файлов или подпапок (подразделов реестра), можно отменить режим «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне».

Запрещение права доступа имеет более высокий приоритет, чем его разрешение, если только объект не наследует от различных папок противоречащие друг другу значения этих параметров. В таких случаях в силу вступает значение, унаследованное от родительского контейнера, ближайшего к объекту в иерархической структуре. Дочерние объекты наследуют только наследуемые разрешения.

Для разграничения прав доступа существует несколько способов, наиболее удобными считаются:

* Вкладка «Безопасность» в свойствах файла или папки.
* Системная утилита icacls.exe.
* Файловый менеджер.
* Средства защиты информации от несанкционированного доступа.
* Один из простых способов посмотреть какие права получит пользователь к файлу или папке. Для этого в свойствах файла или папки откройте вкладка «Действующие разрешения» окна «Дополнительные параметры безопасности». Для проверки установленных прав следует:

1. перейти во вкладку Действующие разрешения окна Дополнительные параметры безопасности и нажать кнопку «Выбрать»;
2. в появившемся новом окне нажать кнопку «Типы объектов»;
3. из списка выбрать объект (Пользователь, Группа) и нажать кнопку «ОК»;
4. в окне «Выбор»: Пользователь или группа нажать кнопку «Дополнительно»;
5. появится новое окно «Выберите тип объекта»;
6. нажать кнопку «Поиск»;
7. из раскрывшегося списка выбрать пользователя или группу и нажать «ОК»;
8. появится окно с выбранным объектом, нажать кнопку «ОК»;
9. появится список действующих разрешений для выбранного пользователя или выбранной группы.

Задание

1. Создать 4-х пользователей (администратор, 2 студента, гость). Созданных пользователей разбить на группы (роли) (<http://windows.microsoft.com/ru-ru/windows/user-groups#1TC=windows-7>).
2. Создать папку (п1) в которой будут папка (п2) с текстовым файлом (ф1) и текстовой файл (ф2). Разграничить права на эти файлы так, чтобы гость не мог зайти и просматривать п1, но мог туда писать. Студенты не могут зайти и писать в п2, но могут читать ее файлы по прямой ссылке (п1/п2/ф1). Так же студенты могут только читать ф2.
3. В политике безопасности (локальная политика безопасности) задать следующие пункты:
   1. Требования сложности пароля
   2. Максимальный срок действия
   3. Минимальный срок действия
   4. Время сброса счетчика блокировки
   5. Пороговое значение блокировки
   6. Продолжительность блокировки

**Отчет необходимо оформить по шаблону с сайта «ЛЭТИ»(титульник, цель работы, ход выполнения работы, вывод) и сопроводить скриншотами с этапами выполнения задания.**

**Отчеты присылать на почту** [**ZOC.leti@yandex.ru**](https://vk.com/write?email=ZOC.leti@yandex.ru) **. В теме письма должно содержаться имя, фамилия, группа, номер лабораторной работы и слово «Windows».**