Министерство образования и науки РФ

Федеральное государственное автономное

образовательное учреждение высшего образования

«Университет ИТМО»

**факультет программной инженерии и компьютерной техники**

**ЛАБОРАТОРНАЯ РАБОТА № 1**

по дисциплине

‘Информационная безопасность’

‘Учетные записи и авторизация в ОС Windows’

Вариант №9

*Выполнил:*

Студент группы P34111

Павлов Александр Сергеевич

*Преподаватель:*

Маркина Т.А.

Изображение выглядит как Шрифт, логотип, Графика, белый

Автоматически созданное описание

Санкт-Петербург, 2024

# Цель работы

Изучить типы учетных записей пользователей, ознакомиться с основными принципами управления учетными записями. Изучить основные способы авторизации пользователей.

Вариант: написать программу, на которой проиллюстрировать возможности сервисов олицетворения для смены пользователя при доступе к ресурсам. Рассмотреть, в чем состоит задача аутентификации.

# Программные и аппаратные средства

Процессор: Intel Core i5-11400F 2.6GHz 12 ядер

Видеокарта: NVIDIA GeForce RTX 2060

Объем оперативной памяти: 32 GB

# Основная часть

1. Основные определения

* Диспетчер учетных записей̆ (SAM - Security Account Manager);
* Монитор безопасности (SRM - Security Reference Monitor);
* Маркер доступа (access token)
* Идентификатор безопасности (SID - Security Identifier)
* Привилегии пользователя
* Права пользователя (user rights)
* Объект доступа
* Субъект доступа
* Олицетворение (impersonation)
* Список контроля доступа (ACL - Access Control List)
* Учетная запись
* Домен

1. Создание пользователя
   1. Управление учетными записями в основных параметрах

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

* 1. Учетные записи пользователей в панели управления

Изображение выглядит как текст, Человеческое лицо, снимок экрана, человек

Автоматически созданное описание

* 1. Командная строка CMD

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

* 1. Утилита lusrmgr.msc

Изображение выглядит как текст, программное обеспечение, Значок на компьютере, веб-страница

Автоматически созданное описание

* 1. Учетные данные пользователей (control userpasswords2)

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Возможности пользователя по изменению конфигурации системы:

Пользователь может:  
1. Персонализировать рабочее пространство

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

2. Управлять файлами в собственном пространстве

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Автоматически созданное описание

Пользователь не может:

1. Создавать новых пользователей

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Автоматически созданное описание

1. Просматривать рабочие пространства других пользователей

Изображение выглядит как текст, программное обеспечение, Шрифт, веб-страница

Автоматически созданное описание

1. Редактировать параметры безопасности (при редактировании всплывает окно, которое невозможно заскринить – там просит ввести данные администратора)

Изображение выглядит как текст, снимок экрана, Шрифт, документ

Автоматически созданное описание

1. Создание администратора
   1. Изменение типа учетной записи в основных параметрах

Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

* 1. Изменение типа учетной записи (control userpasswords2)

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

* 1. Создание нового пользователя и его присоединение к группе администраторов через командную строку

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Возможности администратора по изменению конфигурации системы:

Администратор может:

Совершать все действия, которые доступны обычному пользователю + операции управления другими пользователями

1. Управлять всеми процессами и службами

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

1. Изменять параметры реестра системы

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

1. Изменять свой тип, если в системе больше одного администратора

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

1. Политики UAC

Контроль учетных записей Windows – механизм для защиты от изменений, которые могут потенциально нанести вред компьютеру.

Всего предусмотрено четыре уровня контроля:

* 1. Самый высокий уровень - предупреждения при любых попытках модифицировать системные настройки и файлы, а также при установке программного обеспечения

Изображение выглядит как текст

Автоматически созданное описание

* 1. Второй уровень – предупреждения только при попытках внести изменения в системную конфигурацию и настройки пользователя

Изображение выглядит как текст

Автоматически созданное описание

* 1. Третий уровень – предупреждения только при попытках внести изменения в системную конфигурацию

Изображение выглядит как текст

Автоматически созданное описание

* 1. Четвертый уровень – полное отключение UAC.

Изображение выглядит как текст

Автоматически созданное описание

1. Задание по варианту

Листинг программы:

class User:

    def \_\_init\_\_(self, username, password):

        self.username = username

        self.password = password

class AuthService:

    def \_\_init\_\_(self):

        self.users = {}

        self.current\_user = None

    def register(self, username, password):

        if username in self.users:

            print("Пользователь уже существует!")

        else:

            self.users[username] = User(username, password)

            print(f"Пользователь {username} зарегистрирован!")

    def login(self, username, password):

        user = self.users.get(username)

        if user and user.password == password:

            self.current\_user = user

            print(f"Добро пожаловать, {username}!")

        else:

            print("Неверное имя пользователя или пароль!")

    def logout(self):

        if self.current\_user:

            print(f"Пользователь {self.current\_user.username} вышел из системы.")

            self.current\_user = None

        else:

            print("Вы не авторизованы!")

    def access\_resource(self):

        if self.current\_user:

            print(f"Доступ к ресурсу для {self.current\_user.username} предоставлен.")

        else:

            print("Доступ запрещен! Необходимо войти в систему.")

auth\_service = AuthService()

auth\_service.register("user1", "password123")

auth\_service.login("user1", "password123")

auth\_service.access\_resource()

auth\_service.logout()

auth\_service.access\_resource()

Аутентификация — это процесс проверки идентичности пользователя или системы. Цель аутентификации — убедиться, что пользователь действительно тот, за кого себя выдает. Есть несколько методов аутентификации

1. Пользовательское имя и пароль — самый распространенный метод.
2. Двухфакторная аутентификация (2FA) — добавление дополнительного уровня безопасности (например, SMS-код или через специальное приложение).
3. Биометрическая аутентификация — использование отпечатков пальцев или распознавания лица.

Анализ реализации механизма защиты в ОС Windows 10

В операционной системе Windows механизм защиты включает в себя разнообразные аспекты, направленные на обеспечение безопасности системы и защиту данных пользователей.

1. Аутентификация пользователей

- Пользователи и группы: Windows использует концепцию учетных записей пользователей и групп для управления доступом к ресурсам. Каждому пользователю назначаются права и разрешения, определяющие, что именно он может делать.

- Пароли и учетные данные: Система требует наличие пароля для аутентификации пользователей. Кроме того, возможна реализация двухфакторной аутентификации (2FA) для повышения уровня безопасности.

2. Разграничение доступа

- ACL (Access Control Lists): Windows использует списки управления доступом для определения прав на файлы и ресурсы. Каждому объекту в системе (файлу, папке, реестру и т.д.) присваиваются ACL, которые определяют, какие пользователи или группы могут выполнять определенные действия с этим объектом.

- Контроль учетных записей (UAC): UAC (User Account Control) помогает предотвратить несанкционированные изменения в системе, требуя подтверждения от администратора при выполнении задач, требующих повышенных привилегий.

3. Шифрование данных

- BitLocker: Windows предлагает встроенное шифрование дисков через механизм BitLocker, который шифрует весь диск и защищает данные, хранящиеся на нем, даже в случае кражи устройства.

4. Безопасность сети

- Брандмауэр Windows: Встроенный брандмауэр контролирует входящий и исходящий сетевой трафик, позволяя пользователям настраивать правила для различных программ и служб.

- Защита от вредоносных программ: Windows включает в себя Windows Defender, который предоставляет антивирусную защиту и инструменты для обеспечения безопасности веб-серфинга и работы с файлами.

В целом, механизмы защиты в Windows представляют собой комплексный подход к обеспечению безопасности системы. Они помогают контролировать доступ, защищать данные и предотвращать несанкционированные изменения.

# Вывод

При выполнении лабораторной были изучены основы администрирования ОС Windows и управление учетными записями.