

Национальный Исследовательский Университет ИТМО
Факультет программной инженерии и компьютерной техники

Лабораторная работа №1
по дисциплине «Информационная безопасность»
Вариант 6

Выполнил: Ларочкин Г.И
Группа: Р3400
Преподаватель: Маркина Т.А.

Санкт-Петербург
2021 г.

Постановка задачи

1. Дайте определение терминам: диспетчер учетных записей (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), права пользователя, объект доступа, субъект доступа, олицетворение (impersonation), список контроля доступа (ACL - Access Control List), учетная запись, домен (в отчете: не надо писать определения).
2. Создайте пользователя User_№ варианта, входящего в группу «Пользователи». Опишите все способы создания, а также (на примерах) возможности данного пользователя по изменению конфигурации системы (минимум 3 примера) (в отчете: подробное описание выполнения задания со скриншотами).
3. Создайте администратора Admin_№ варианта, входящего в группу «Администраторы». Опишите все способы создания, а также (на примерах) ограничения данного пользователя по изменению конфигурации системы (минимум 3 примера) (в отчете: подробное описание выполнения задания со скриншотами).
4. Опишите параметры контроля учетных записей пользователей (UAC) (в отчете: перечислить параметры и дать им определение).
5. Выполните настройки механизмов защиты ОС Windows в соответствии с вариантом. Проанализируйте выполненные Вами настройки механизма защиты в части выполнения ими требований руководящих документов в области защиты информации. Сформулируйте, в чем не выполняются данные требования. Проанализируйте реализацию в ОС Windows механизма защиты в целом (не конкретно для Вашего примера) (в отчете: подробное описание выполнения задания со скриншотами, анализ выполненных настроек, ответ на вопрос о невыполнении требований, анализ реализации в ОС).

Задание 6-ого варианта

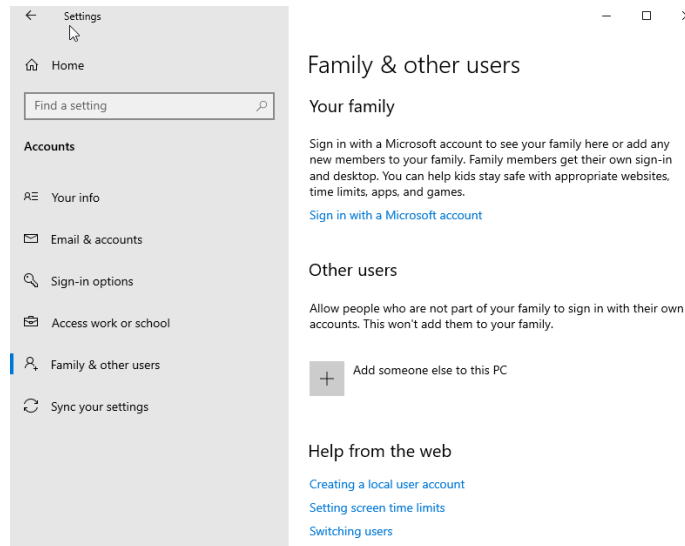
Реализовать и проиллюстрировать возможность запуска приложения под другой учетной записью после аутентификации.

Ход работы

Создание локальных пользователей

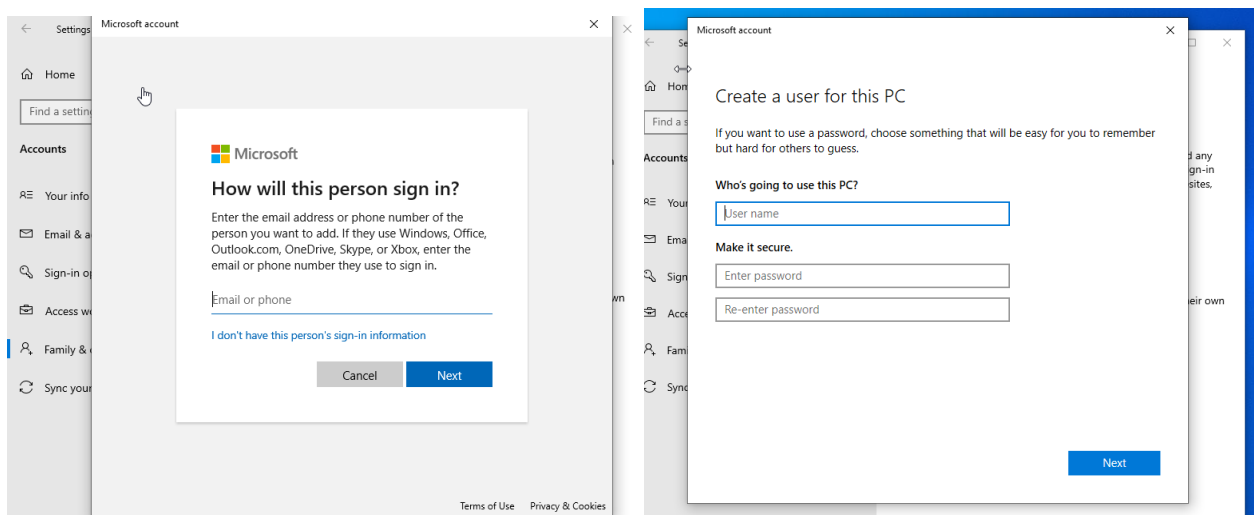
Способ 1 – через настройки windows

1. Переходим в Settings -> Accounts -> Family & other users
2. Нажимаем на кнопку Add someone else to this PC



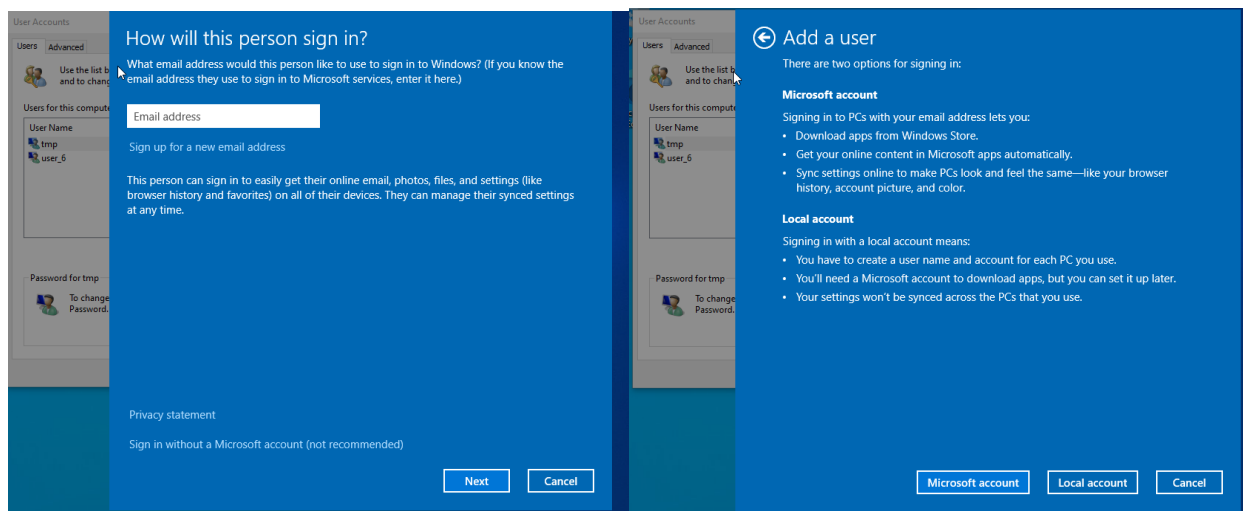
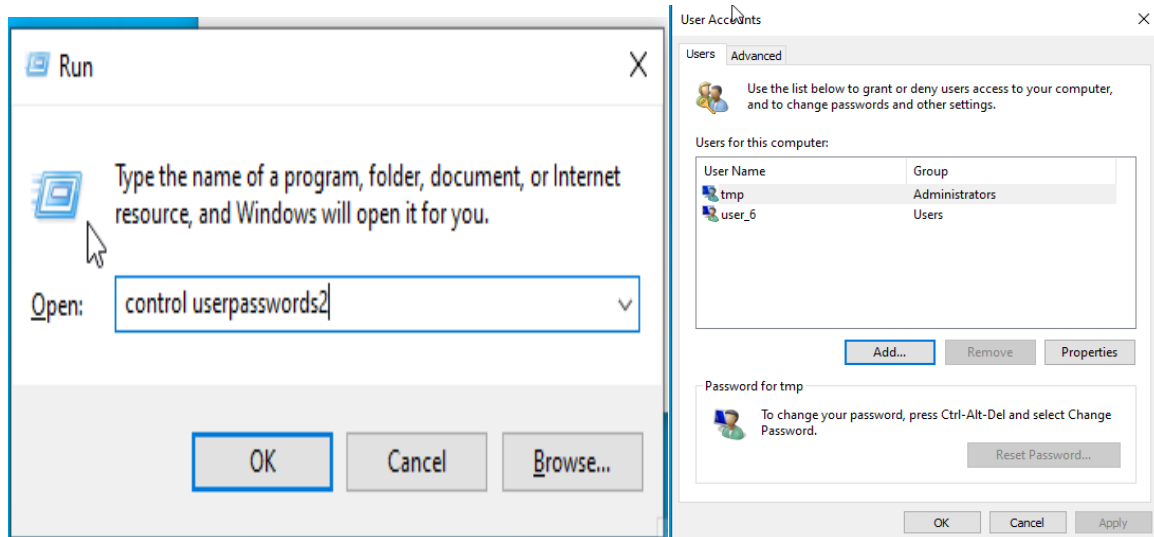
Тут возможны два варианта:

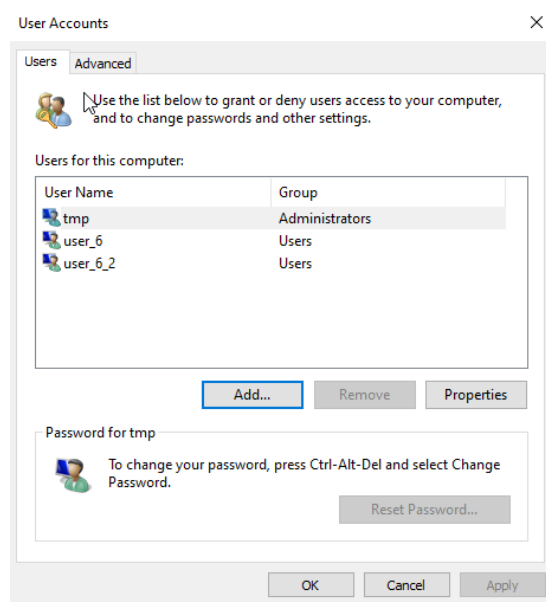
- Если у вас есть доступ к интернету, то откроется окно, предлагающее зайти с помощью Microsoft аккаунт. Нажимаем на *I don't have this person's sign-in information* и затем *create without Microsoft account*. Откроется окно создания локального пользователя.
- Если у вас нет доступа к интернету, то сразу откроется окно создания локального пользователя.



Способ 2 –control userpasswords2

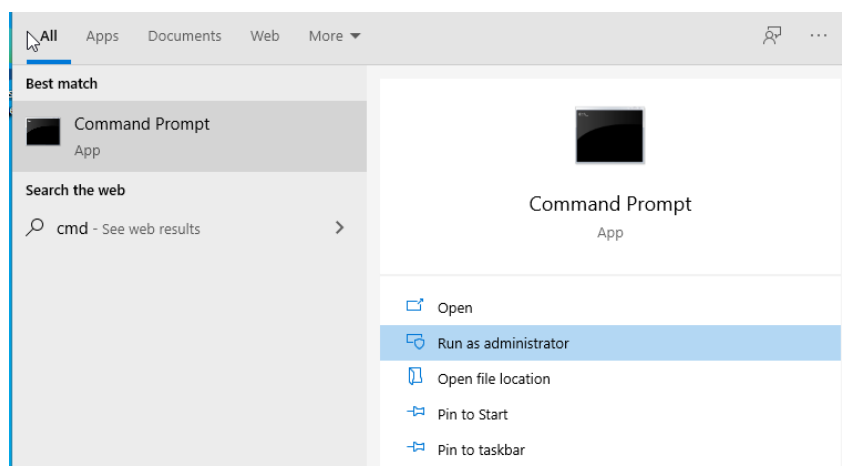
1. Нажимаем Win+R и запускаем команду *control userpasswords2*. Откроется окно User Accounts.
2. Нажимаем кнопку Add. Откроется синее окно.
3. Нажимаем Sign in without Microsoft account
4. Выбираем *Local account* и вводим имя-пароль





Способ 3 – командная строка cmd

1. Запускаем cmd от имени администратора
2. Вводим команду `net user username password /add`

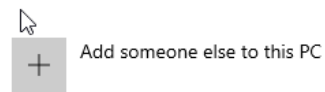


```
C:\Windows\system32>net user user_6_3 user_6_3 /add
The command completed successfully.

C:\Windows\system32>
```

Other users

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.



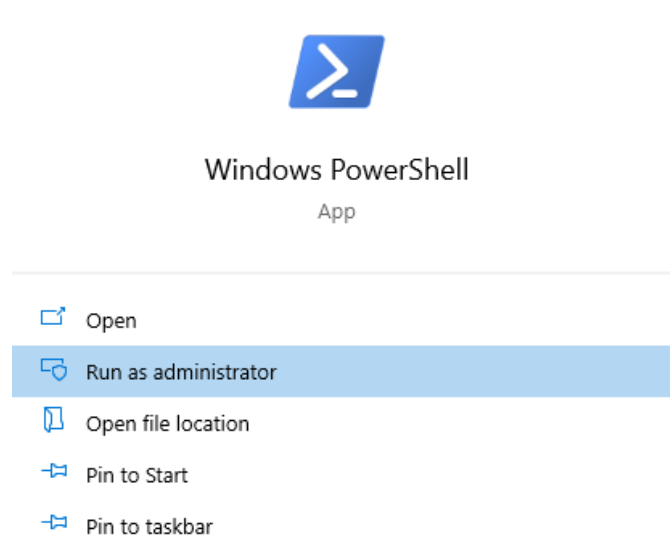
user_6
Local account

user_6_2
Local account

user_6_3
Local account

Способ 4 – командная строка PowerShell

1. Запускаем PowerShell от имени администратора
2. Записываем пароль в переменную: `$Password = Read-Host -AsSecureString`
3. Выполняем команду добавления пользователя: `New-LocalUser username -Password $Password`
4. Добавляем пользователя в группу Users: `Add-LocalGroupMember -Group users -Member username`




```
Administrator: Windows PowerShell
PS C:\Windows\system32> $Password = Read-Host -AsSecureString
*****
PS C:\Windows\system32> New-LocalUser user_6_4 -Password $Password


Name      Enabled Description
----      -
user_6_4  True


PS C:\Windows\system32> Add-LocalGroupMember -Group users -Member user_6_4
PS C:\Windows\system32>
```


Other users


Allow people who are not part of your family or work accounts. This won't add them to your family or work accounts.

 Add someone else to this PC

 user_6
Local account

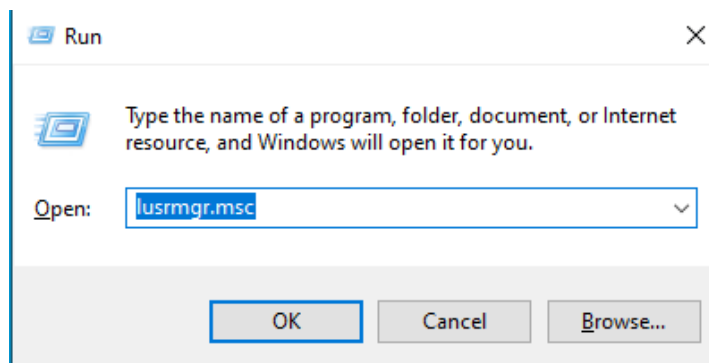
 user_6_2
Local account

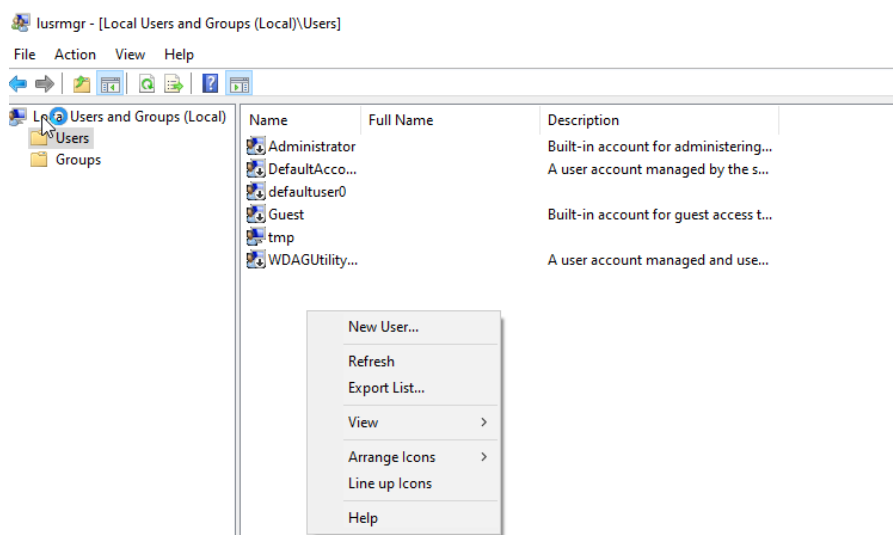
 user_6_3
Local account

 user_6_4
Local account

Способ 5 – lusrmgr.msc (не работает на win 10 home)

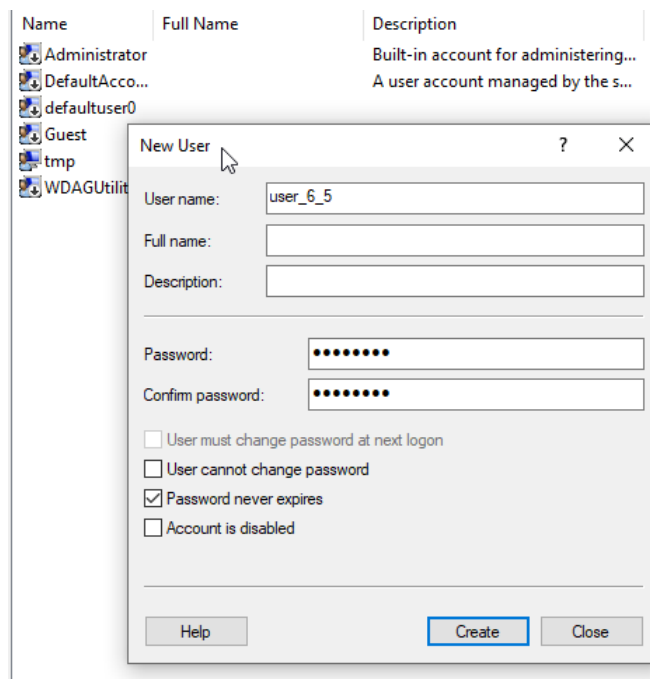
1. Нажимаем Win+R, запускаем lusrmgr.msc
2. Выбираем слева *Users*
3. Нажимаем ПКМ и кнопку *New user*





Возможности обычного пользователя

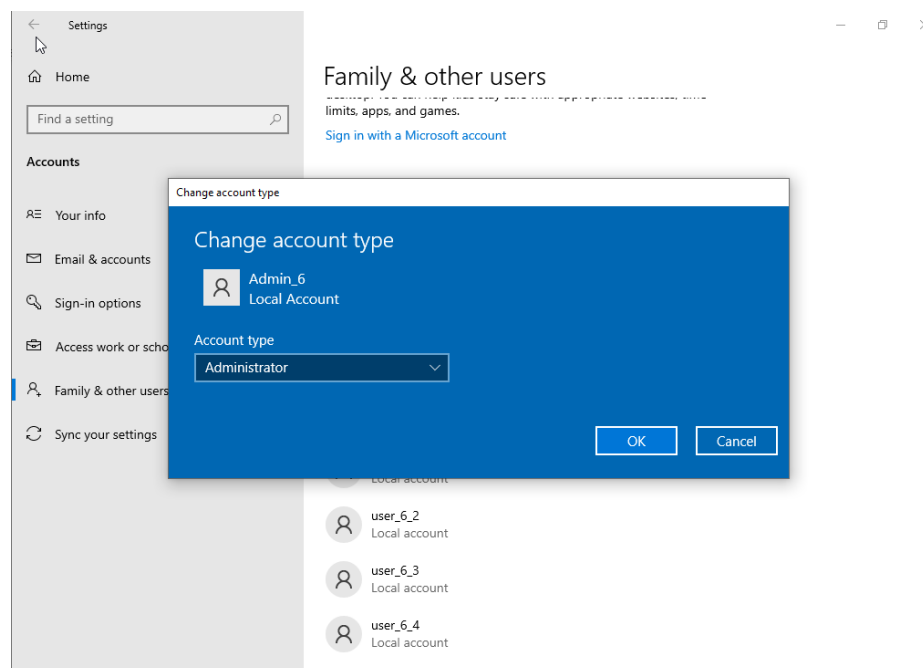
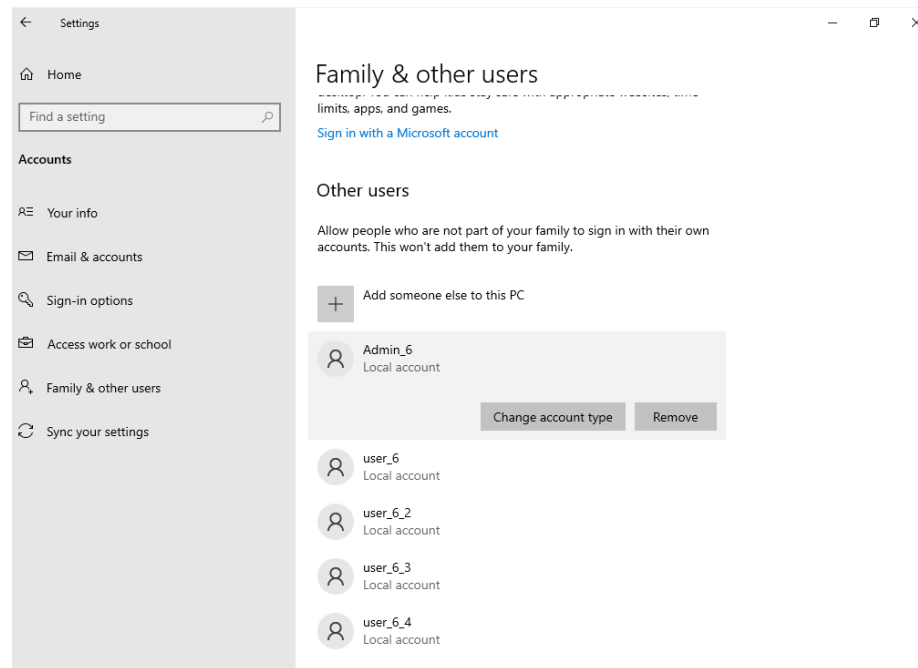
Аккаунты обычных пользователей предназначены для повседневной работы, они обеспечивают защиту системы от несанкционированных операций. Им не позволено редактировать, просматривать, удалять системные файлы и файлы других пользователей (если явно это не разрешено). Также они не могут изменять системные настройки операционной системы. Однако они могут создавать/редактировать/удалять свои файлы, а также запускать программы, не требующие повышения прав. Также такие пользователи могут изменять права доступа на те файлы, владельцами которых они являются.



Создание пользователей-администраторов

Способ 1 – через настройки windows

1. Создаем локального пользователя одним из вышеперечисленных способов
2. Переходим в Settings -> Accounts -> Family & other users
3. Нажимаем Change account type
4. Выбираем Account type - Administrator

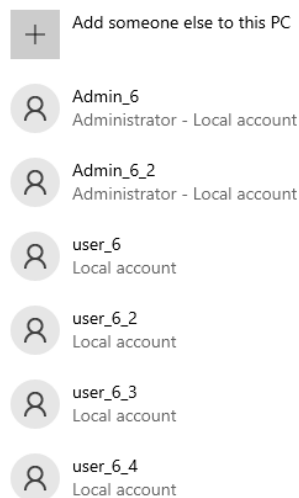


Способ 2 – командная строка cmd

1. Создаем локального пользователя одним из вышеперечисленных способов
2. Запускаем cmd.exe от имени администратора
3. Выполняем команду: `net localgroup administrators username /add`

```
C:\Windows\system32>net localgroup administrators Admin_6_2 /add
The command completed successfully.

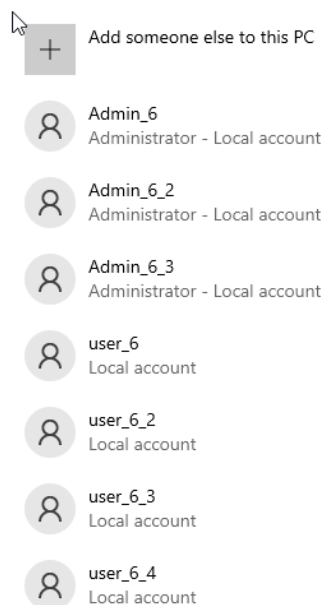
C:\Windows\system32>
```



Способ 3 – командная строка PowerShell

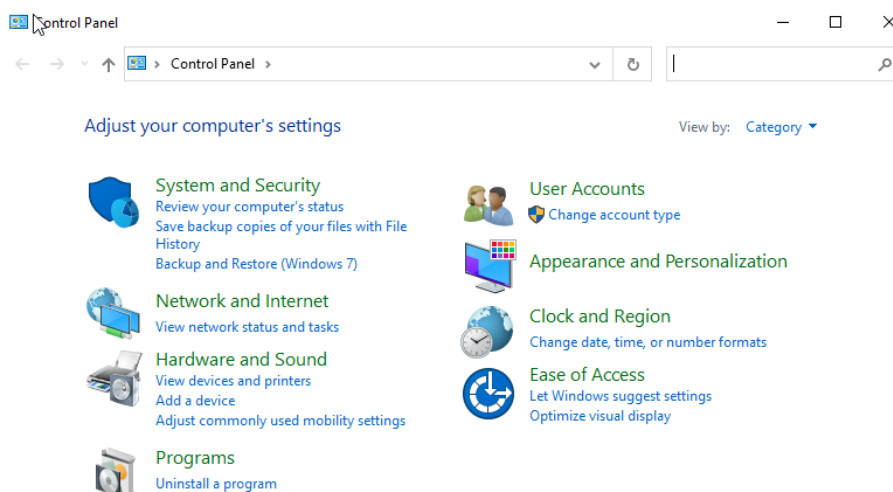
1. Создаем локального пользователя одним из вышеперечисленных способов
2. Запускаем PowerShell от имени администратора
3. Выполняем команду: `net localgroup administrators username /add`

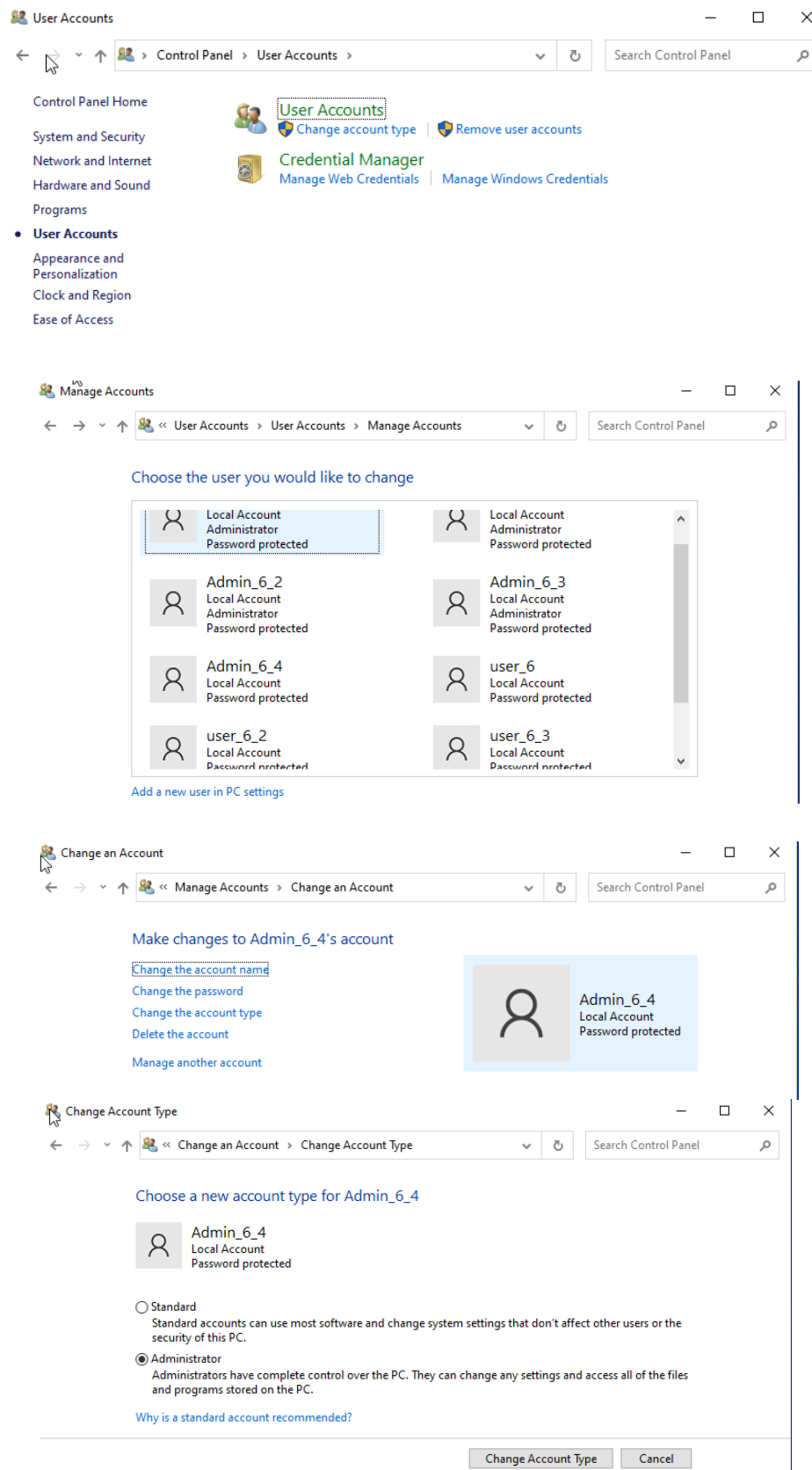
```
Administrator: Windows PowerShell
PS C:\Windows\system32> Add-LocalGroupMember -Group administrators -Member Admin_6_3
PS C:\Windows\system32>
```



Способ 4 – control panel

1. Создаем локального пользователя одним из вышеперечисленных способов
2. Открываем окно *Control Panel*
3. Открываем вкладку *User Accounts*
4. Нажимаем *Change account type*
5. Выбираем необходимый аккаунт и кликаем на него
6. Нажимаем *Change the account type*
7. Выбираем *Administrator* и сохраняем (*Change Account Type* кнопка)

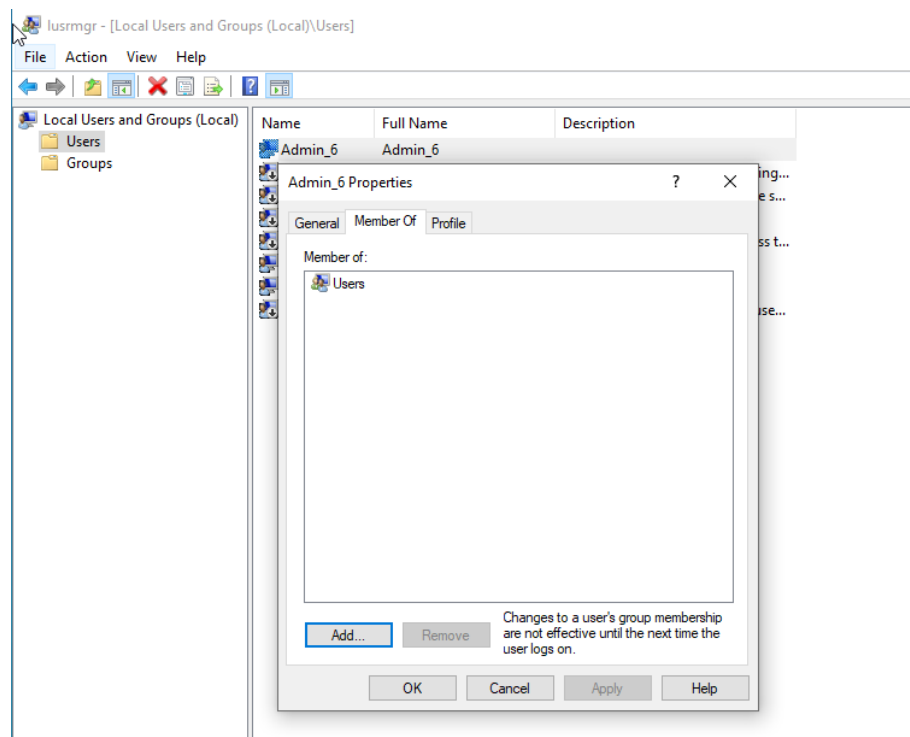




Способ 5 – lusrmgr.msc (не работает на windows 10 home)

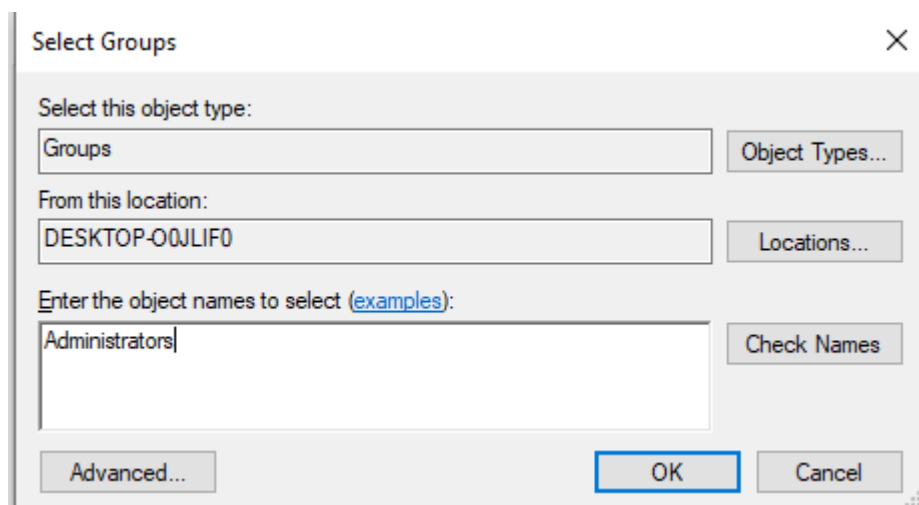
1. Создаем локального пользователя одним из вышеперечисленных способов

2. Нажимаем Win+R, выполняем команду `lusrmgr.msc`
3. Выбираем нужного пользователя и кликаем два раза
4. Открываем вкладку MemberOf, нажимаем *Add...*
5. Вписываем группу *Administrators* и сохраняем



Ограничения пользователей-Администраторов

Такой тип пользователей имеют полный и неограниченный доступ операционной системе. Они могут изменять системные настройки, редактировать/удалять системные защищенные файлы и т.д. Единственное отличие от встроенного администратора – это включенный UAC.



Описание параметров контроля учетных записей (UAC)

Это компонент, который запрашивает подтверждение действий, требующих прав администратора, в целях защиты от несанкционированного использования компьютера. Имеет следующий ряд настроек:

Admin Approval Mode для встроенного Администратора

Если включено, то при операции, требующей прав администратора, будет требоваться подтверждение действий. Если выключено, то все операции будут выполнены с административными привилегиями.

Повышение прав для UIAccess

Позволяет включить или выключить подсказки для повышения прав при использовании программ доступа рабочего стола

Поведение запроса на повышение прав для администраторов

Позволяет изменить способы подтверждения на повышение прав. Например, ввод логина-пароля на безопасном рабочем столе, выбор “Запретить”-“Разрешить” на защищенном рабочем столе, выбор “Запретить”-“Разрешить” на защищенном рабочем столе для программ не Microsoft.

Поведение запроса на повышение прав для обычных пользователей

Позволяет изменить поведение подтверждения на повышение прав для обычных пользователей.

- Ввод логина-пароля администратора
- Отключение повышения прав
- Ввод логина-пароля администратора на защищенном рабочем столе

Запрос на повышение прав при установке приложений

Позволяет включить или выключить запрос на повышение прав при установке приложений.

Проверка сертификата приложения при повышении прав

Позволяет включить или выключить проверку сертификата приложения при запросе на повышение прав.

Повышение прав UIAccess приложений установленных в безопасных

местах

Позволяет включить запрос на повышение прав только для UIAccess приложений, которые установлены в защищенных местах файловой системы. (Program Files, Program Files x86, Windows\system32)

Режим подтверждения

Позволяет включить или выключить контроль учетных записей, независимо от настроек UAC.

Переключение к безопасному рабочему столу

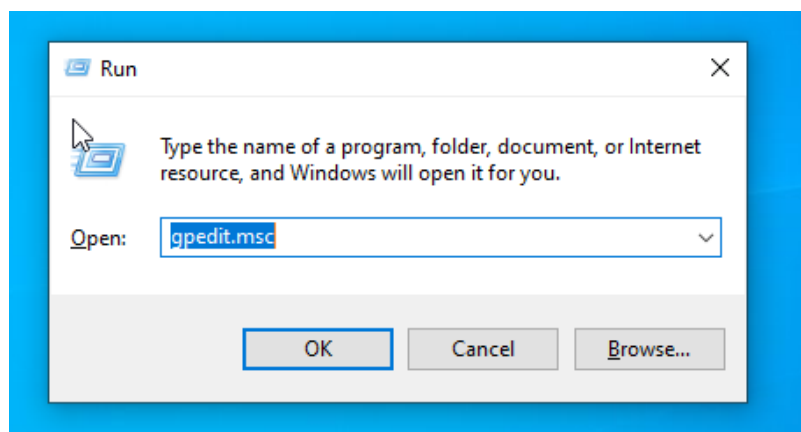
Позволяет перенаправить запросы на повышение прав на защищенный рабочий стол, независимо от настроек UAC.

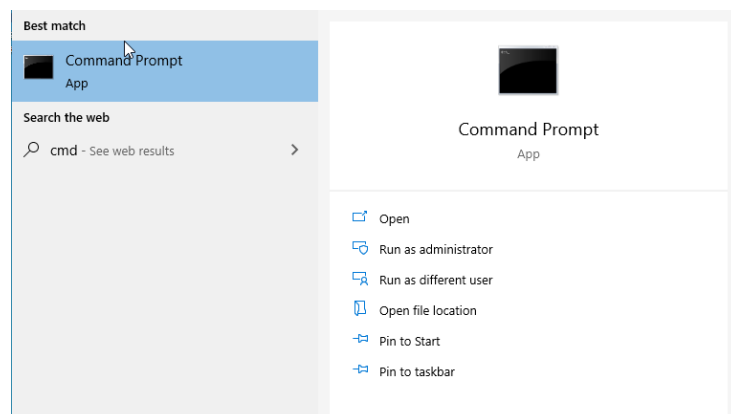
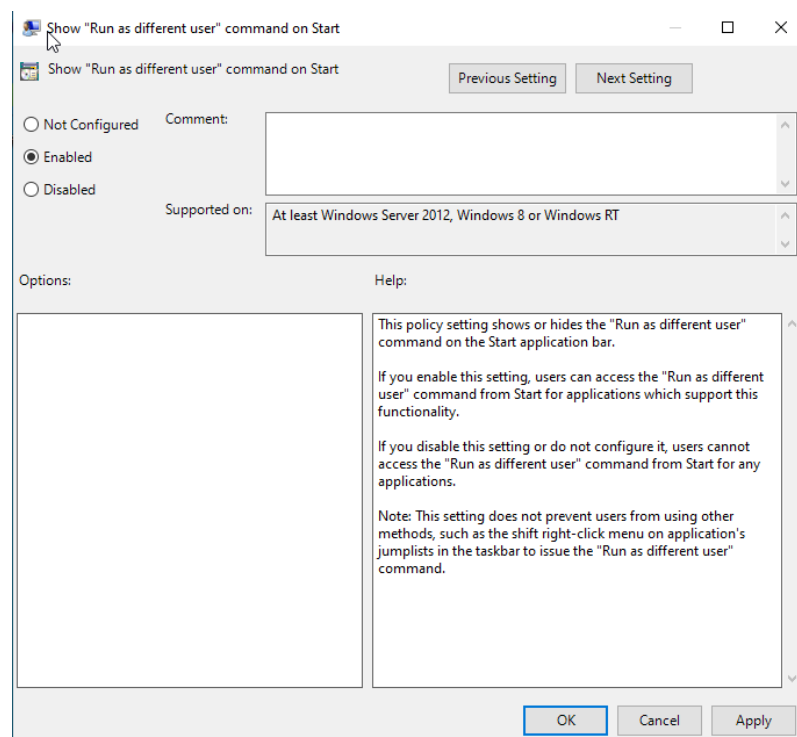
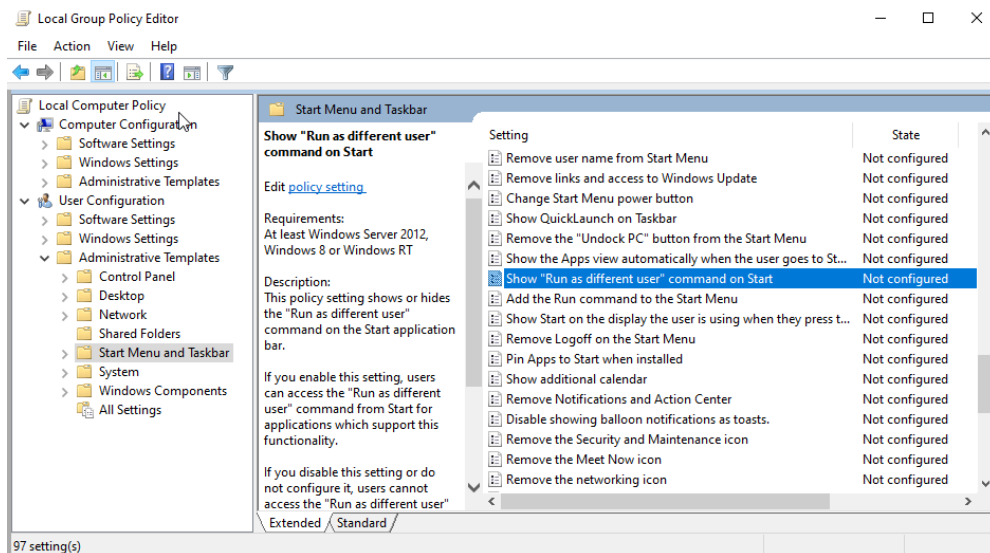
Виртуализация записей сбоев

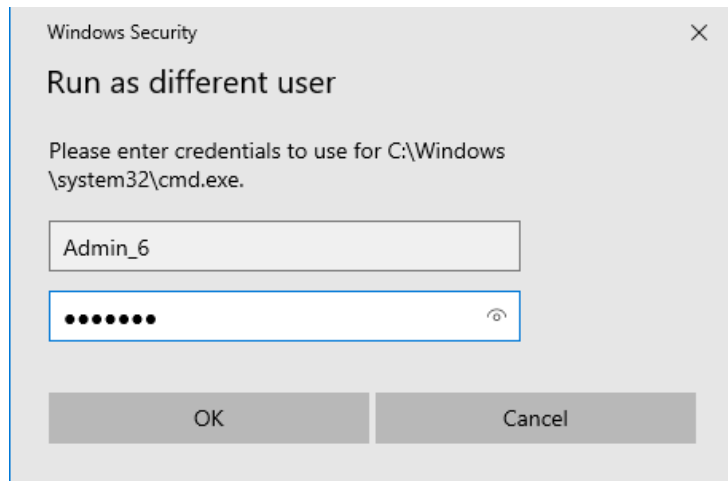
Если включено, то записи о сбоях приложения перенаправляются во время исполнения в соответствующее место в файловой системе и реестре. Если выключено, то запрещена при записи данных в защищенное место в файловой системе.

Запуск программы от имени другого пользователя

1. Нажать Win+R, выполнить команду *gpedit.msc*
2. Перейти в User Configuration -> Administrative Templates -> Start menu and Taskbar
3. Найти в списке настроек Show “Run as different user” command on Start и кликнуть 2 раза
4. Выбрать Enabled, нажать Apply -> Ok
5. Попробовать запустить программу от другого пользователя







```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\tmp>whoami
desktop-o0jlif0\admin_6

C:\Users\tmp>
```

Анализ выполненных настроек

Согласно документу ГОСТ Р ИСО/МЭК 27001-2006 “Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования”, в пункте *A.11 Контроль доступа* сказано, что предоставление и использование привилегий должно быть ограниченным и контролируемым, однако в данной реализации все пользователи имеют возможность запустить от имени другого пользователя, а также нет возможности контролировать этот процесс.

Также должна быть установлена и задокументирована политика контроля доступа, однако это не входит в рамки данной лабораторной работы.

Анализ механизмов защиты в ОС Windows

В access control модели каждый пользователь и группа (security principle) идентифицируются с помощью идентификатора безопасности (SID), который определяет то, какие права доступа имеет данный субъект. Владелец объекта может устанавливать права для пользователей или групп с помощью ACL.

При аутентификации пользователя ОС производит access token, который описывает субъект и его права. Операционная система использует токен при взаимодействии пользователя с защищенными объектами. При входе в систему как Администратор, система производит отдельный Full administrator access token, который используется при выполнении административных задач.

Для access token используется технология цифровой подписи, для верификации токена в его подлинности, таким образом, злоумышленник не сможет получить доступ к объектам, даже если у него есть валидный SID.