Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Институт Информационных Технологий и Анализа Данных

**Название работы** – “Учетные записи и авторизация в Windows ”

Отчет по лабораторной работе “Лабораторная работа №2”

по дисциплине Информационная безопасность и защита информации

Вариант 1

Выполнил

Студент, номер группы ИСМб-19-1 \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.Д.Солопов

Дата: \_\_\_\_\_\_\_\_\_\_

Принял

Должность \_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В.Чумилин

Дата: \_\_\_\_\_\_\_\_\_\_

Иркутск 2021 г.

Содержание

[Цель работы 3](#_Toc66187235)

[Постановка задач 4](#_Toc66187236)

[Решение задач 5](#_Toc66187237)

Цель работы

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

Постановка задач

1) Изучите теоретический материал лабораторной работы. Знать определения: диспетчер учетных записей (SAM), монитор безопасности (SRM), маркер доступа (access token), идентификатор безопасности (SID), привилегии пользователя, права пользователя (user rights), права пользователя, объект доступа, субъект доступа, олицетворение (impersonation), список контроля доступа (ACE), учетная запись, домен.

2) Создайте пользователя User\_№ варианта, входящего в группу «Пользователи». Через графический интерфейс, через командную строку. Опишите на примерах возможности данного пользователя по изменению конфигурации системы (3 примера, скриншоты).

3) Создайте администратора Admin\_№ варианта, входящего в группу «Администраторы». Через графический интерфейс, через командную строку. Опишите на примерах ограничения данного пользователя по изменению конфигурации системы (3 примера, скриншоты).

4) Опишите параметры контроля учетных записей пользователей (UAC). (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.

**Варианты заданий:**

1. Настроить вход пользователя в систему по паролю. Рассмотреть и реализовать возможные способы усиления парольной защиты.

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

3. Проиллюстрировать принадлежность в ОС Windows буфера обмена рабочему столу – одновременно нескольким пользователям.

Решение задач

**Задача 1:**

Создайте пользователя User\_№ варианта, входящего в группу «Пользователи». Через графический интерфейс, через командную строку. Опишите на примерах возможности данного пользователя по изменению конфигурации системы (3 примера, скриншоты).

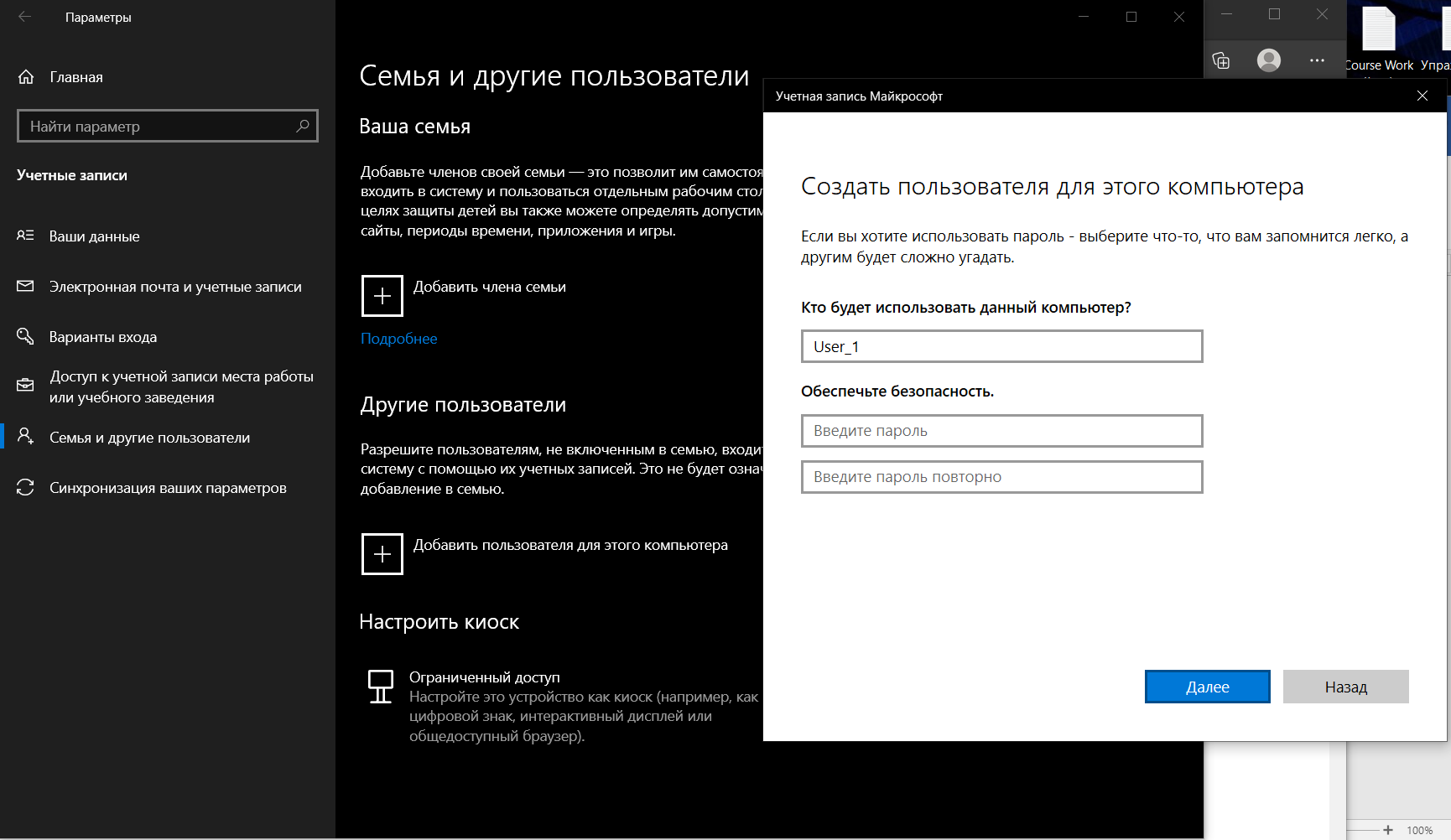


Рис. 1. Создание учётной записи пользователя через графический интерфейс

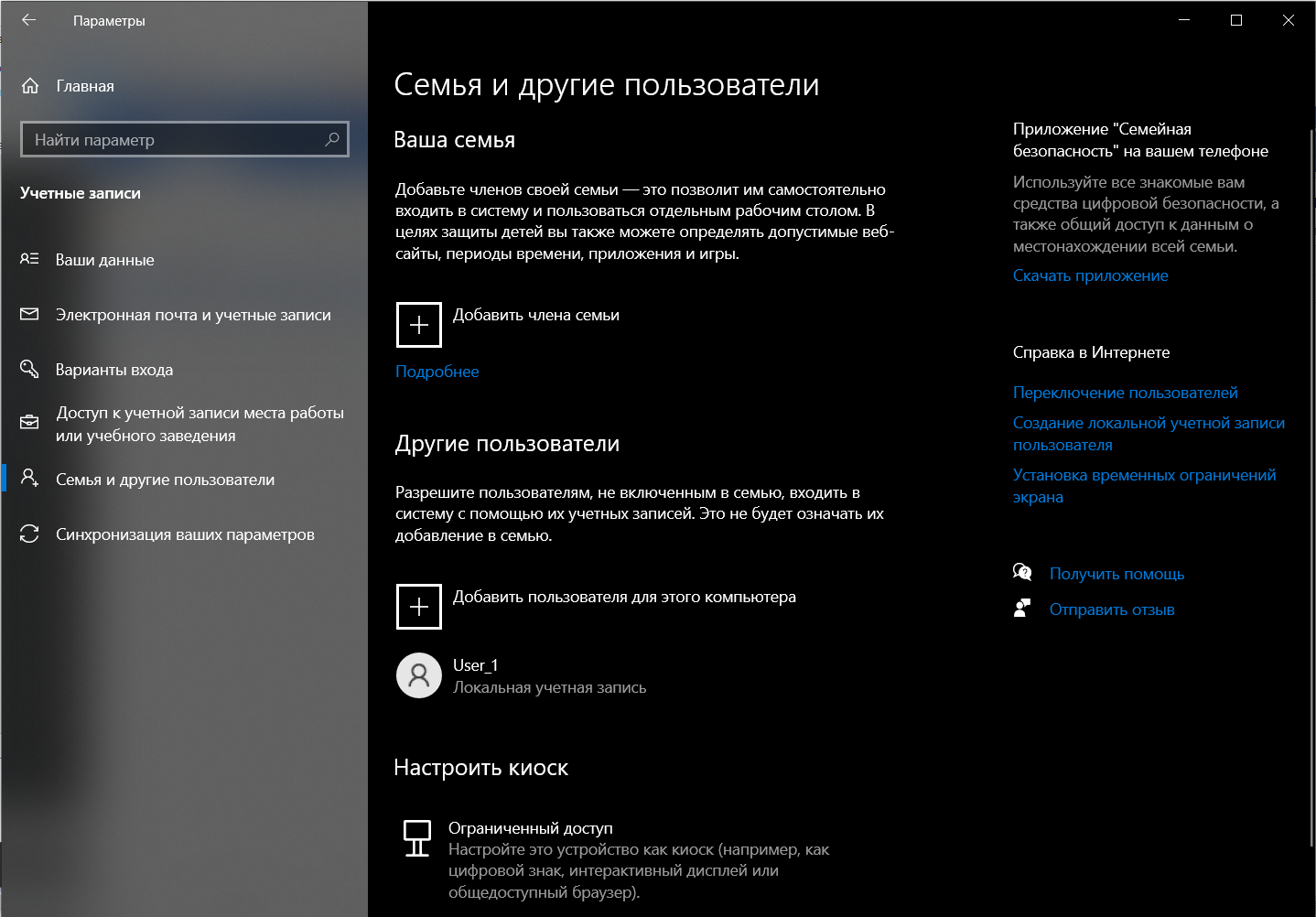


Рис.2. Результат создания учётной записи пользователя через графический интерфейс

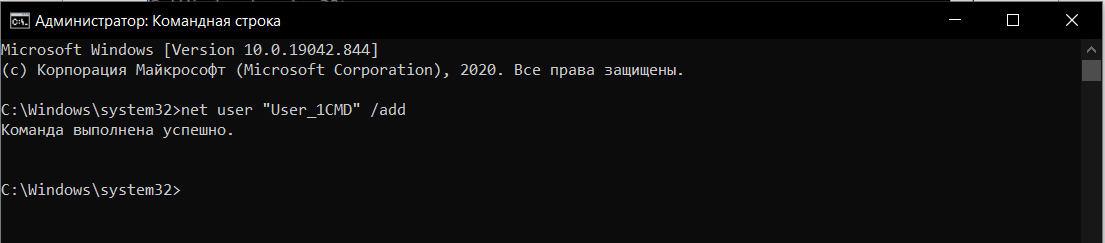


Рис. 3. Создание учётной записи пользователя через CMD

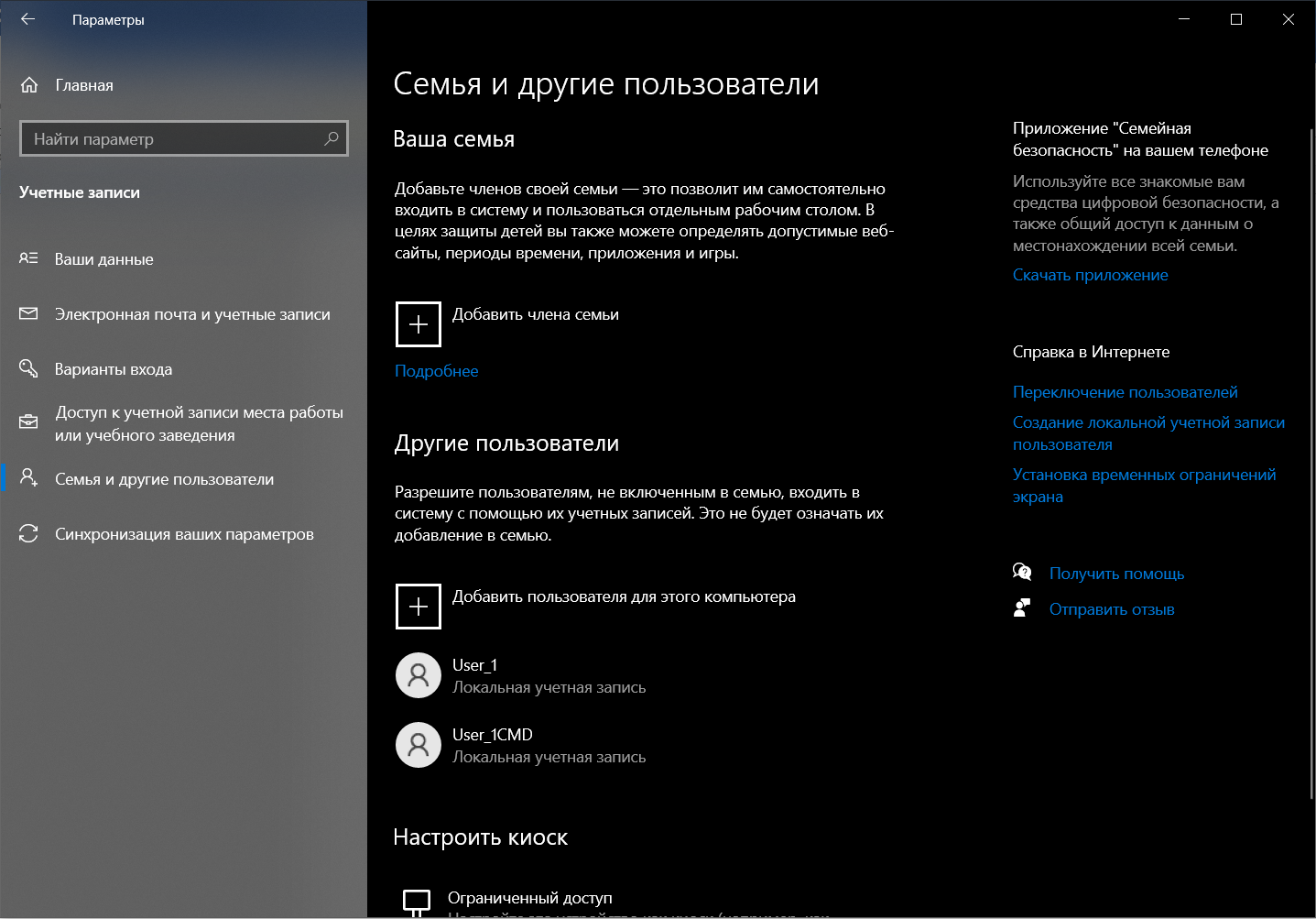


Рис. 4. Результат создания учётной записи пользователя черезCMD

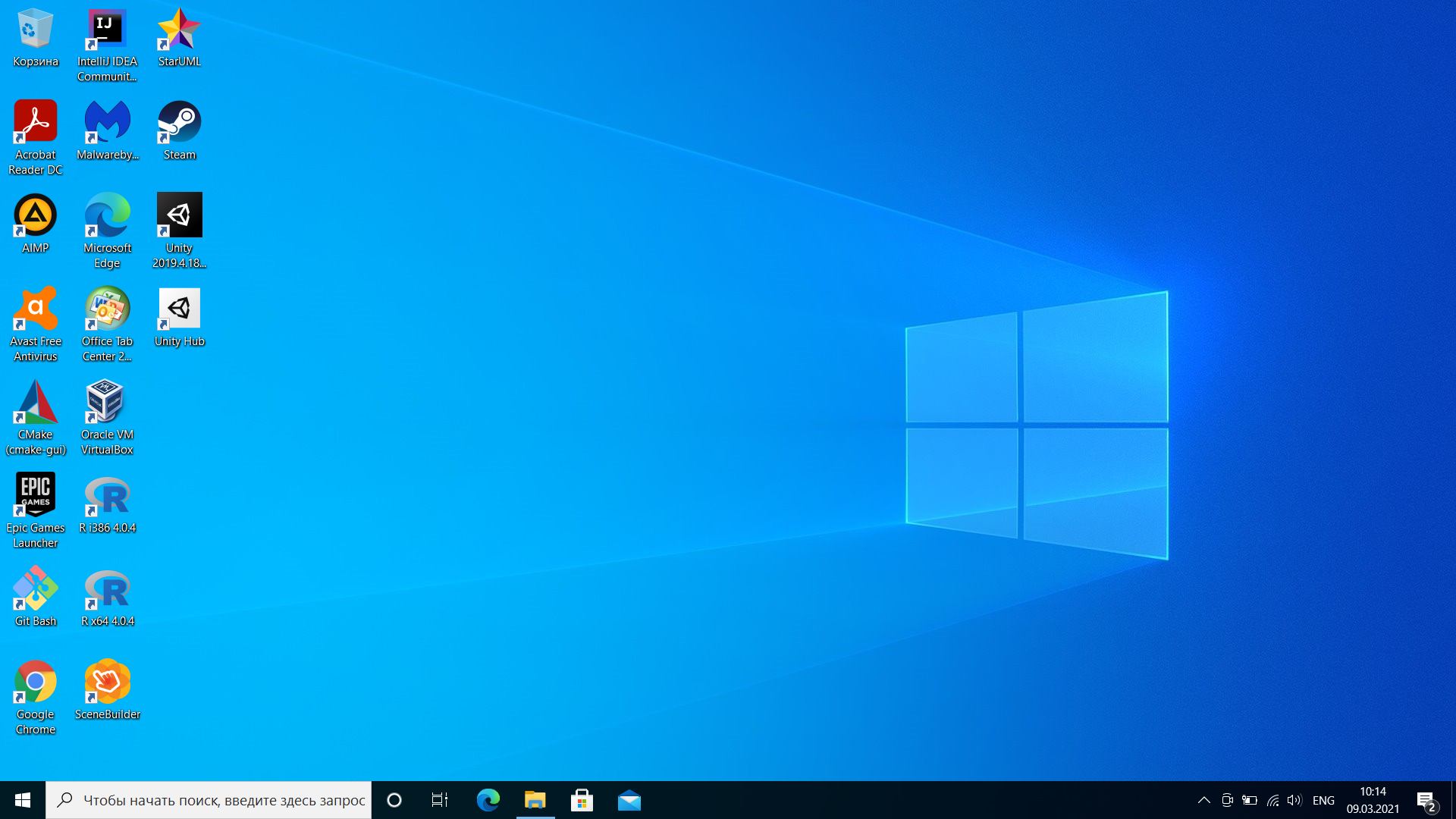


Рис. 5. Рабочий стол локальной учётной записи User\_1

**1 Ограничение**: нельзя изменить тип своей учётной записи (для локальных записей)

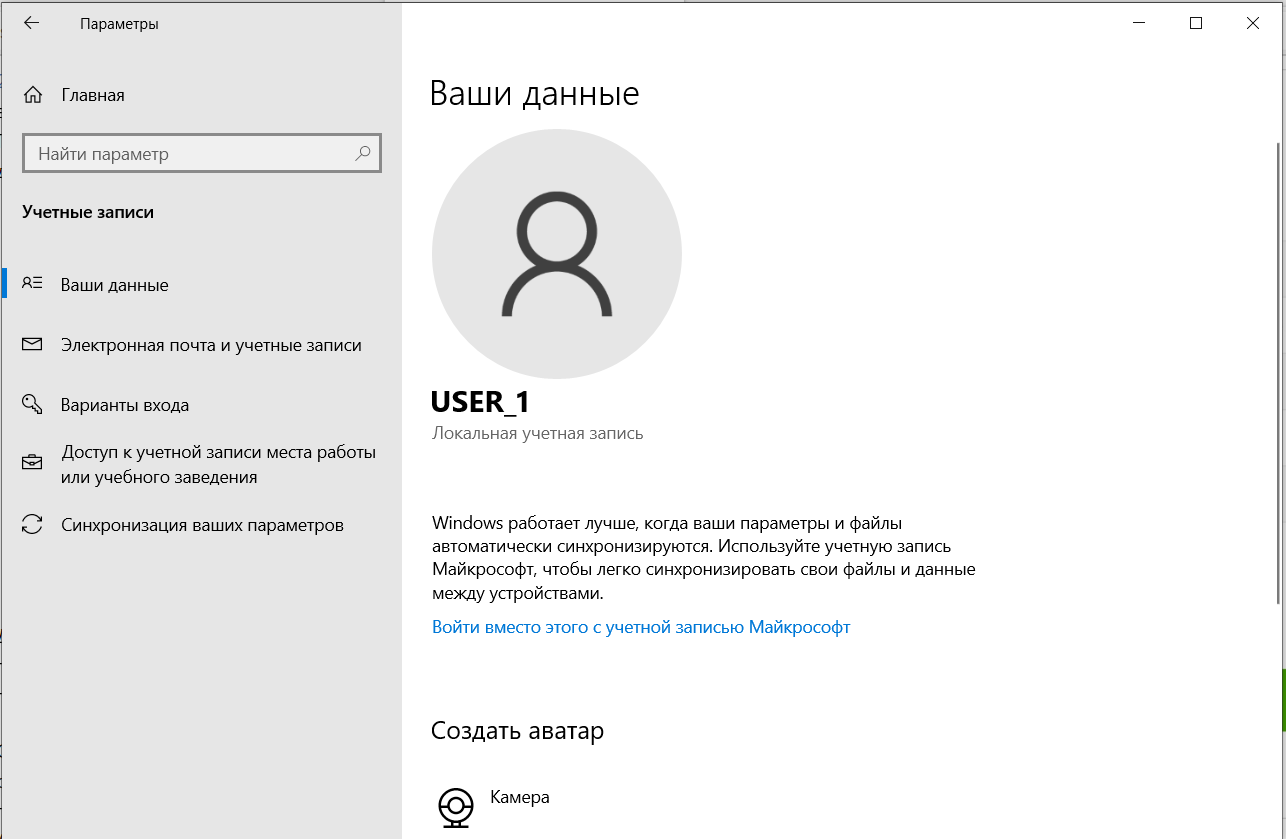


Рис. 6. Информация об учётной записи (отсутствует раздел “Семья и другие пользователи”, который позволяет добавлять или изменять тип учётной записи)

**2 Ограничение:** нельзя устанавливать программы без пароля администратора

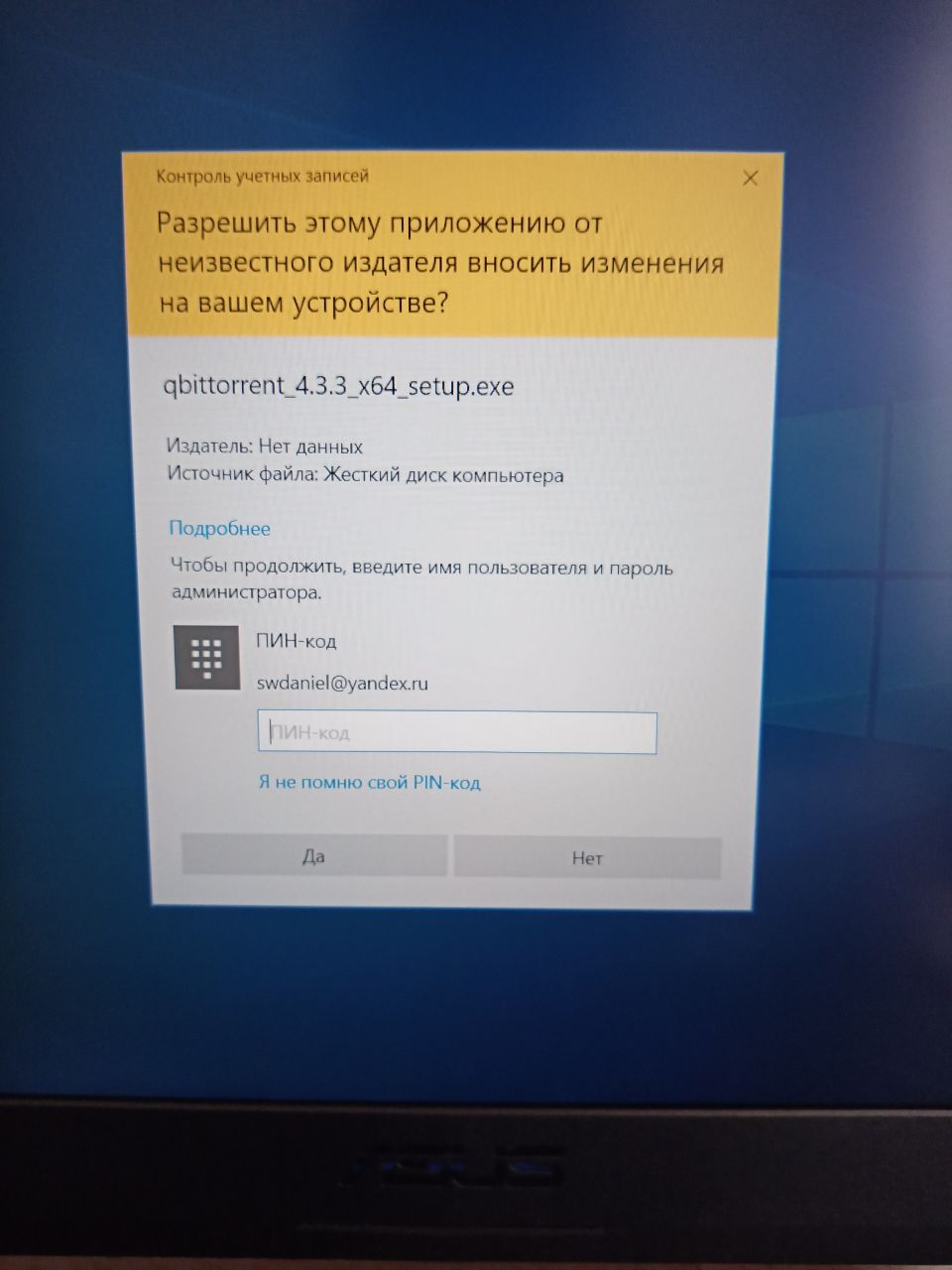


Рис. 7. Попытка установки программы qBittorrent

**3 Ограничение:** нельзя удалять программы

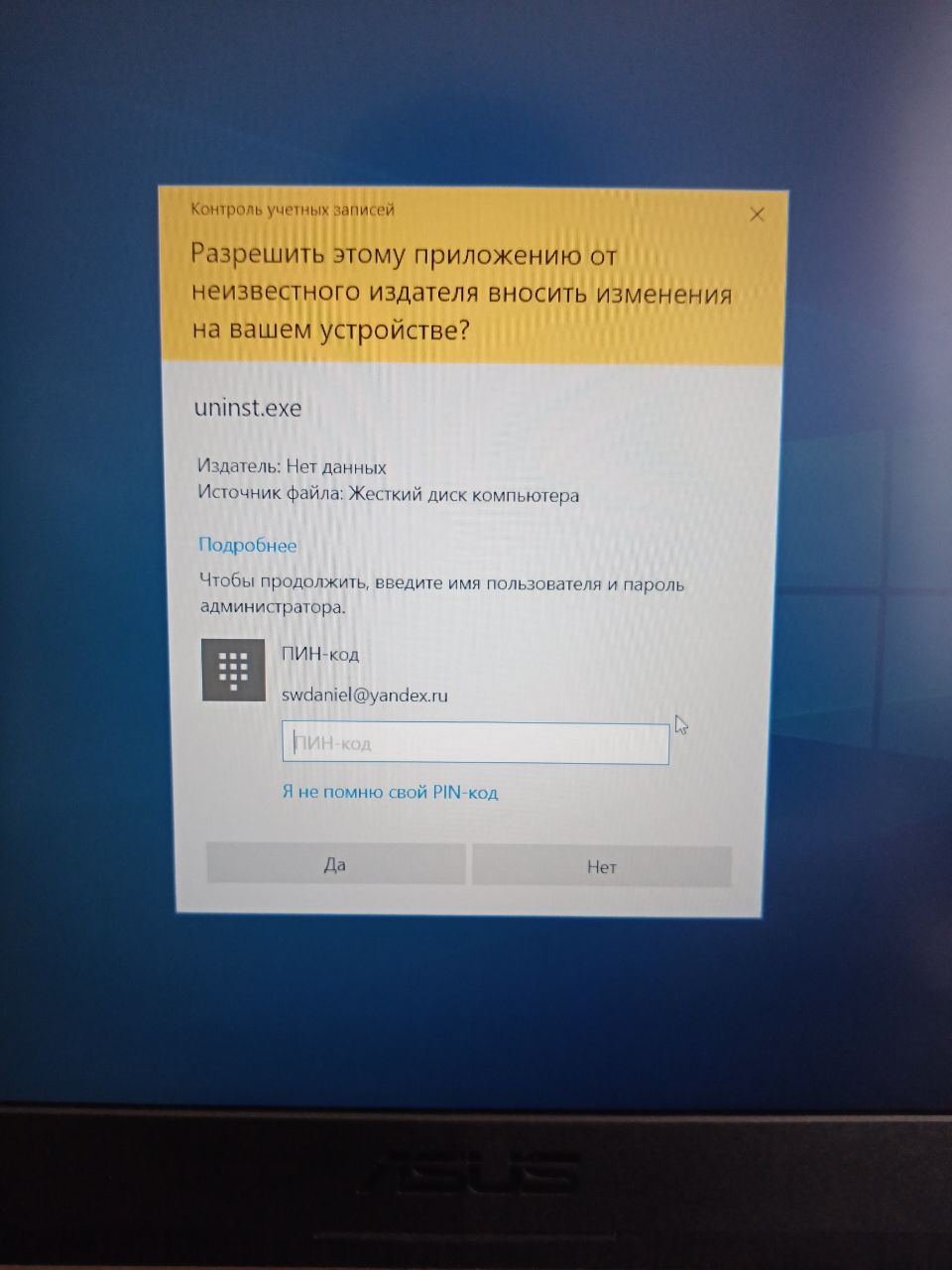


Рис. 8. Попытка удаления программы qBittorrent

**Задача 2:**

Создайте администратора Admin\_№ варианта, входящего в группу «Администраторы». Через графический интерфейс, через командную строку. Опишите на примерах ограничения данного пользователя по изменению конфигурации системы (3 примера, скриншоты).

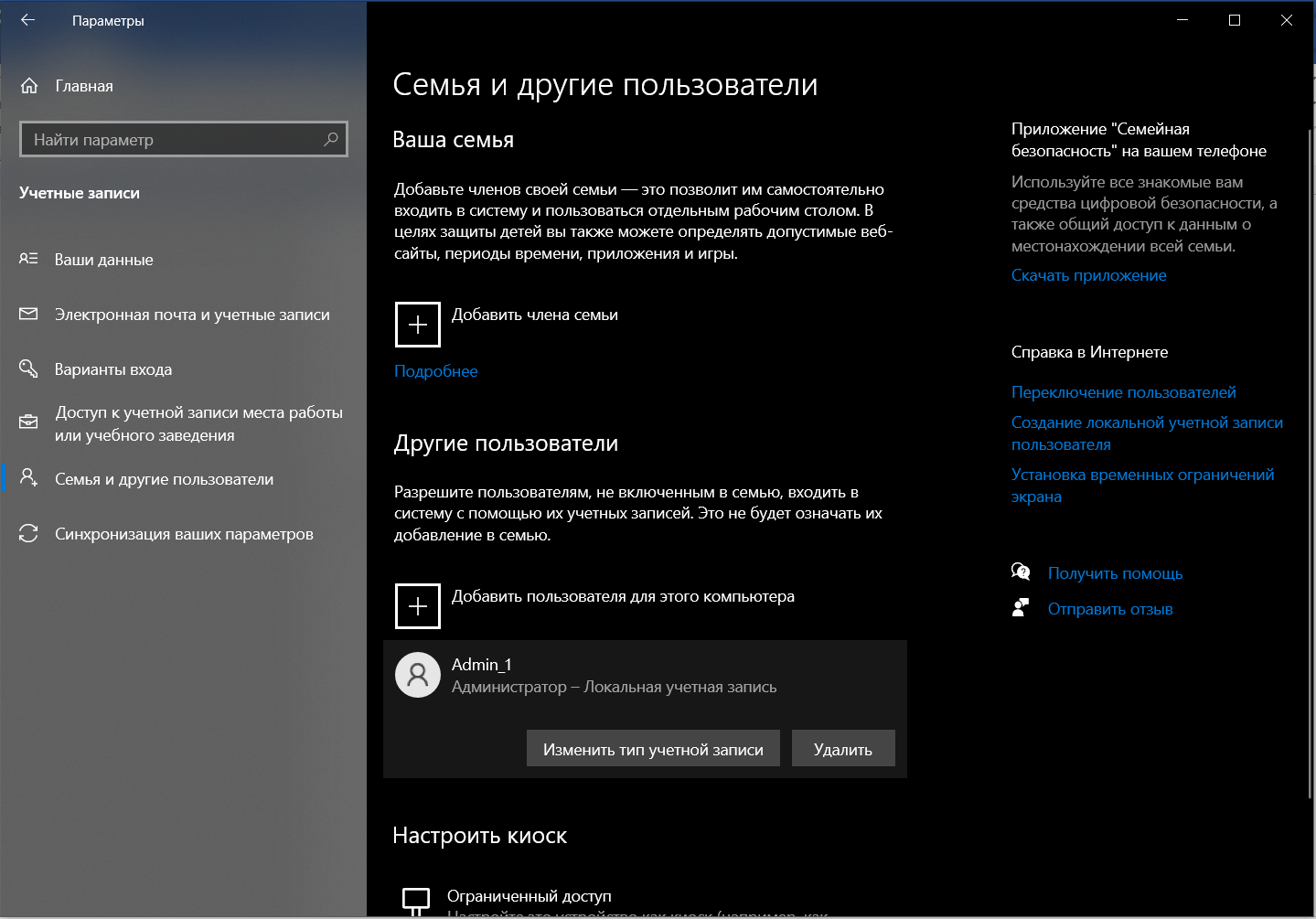


Рис. 9. Создание учётной записи администратора через графический интерфейс

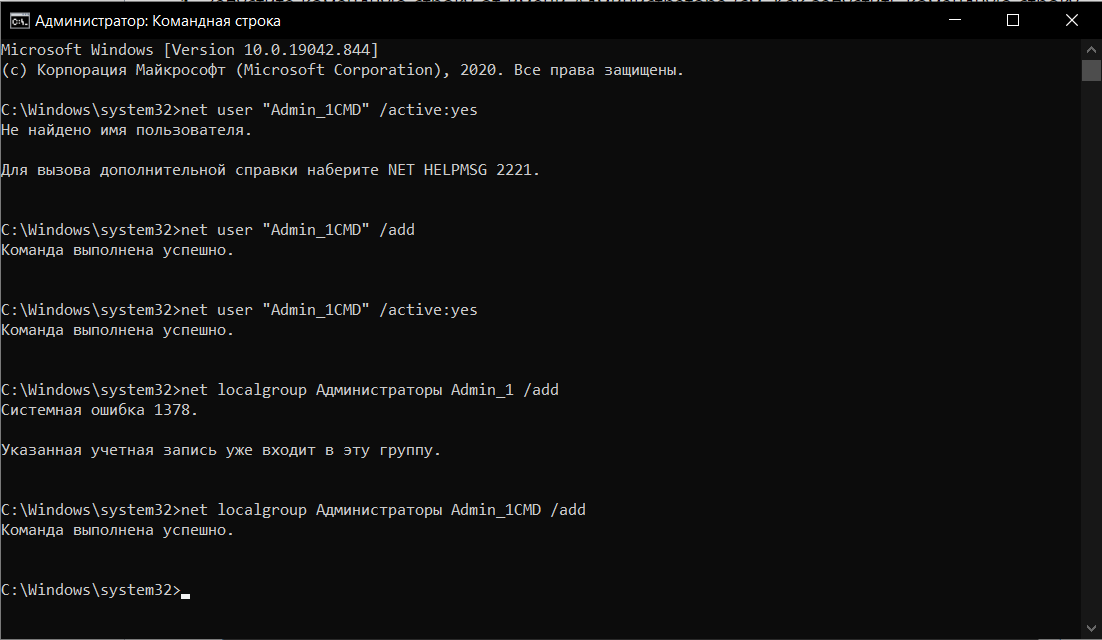


Рис. 10. Создание учётной записи администратора через командную строку

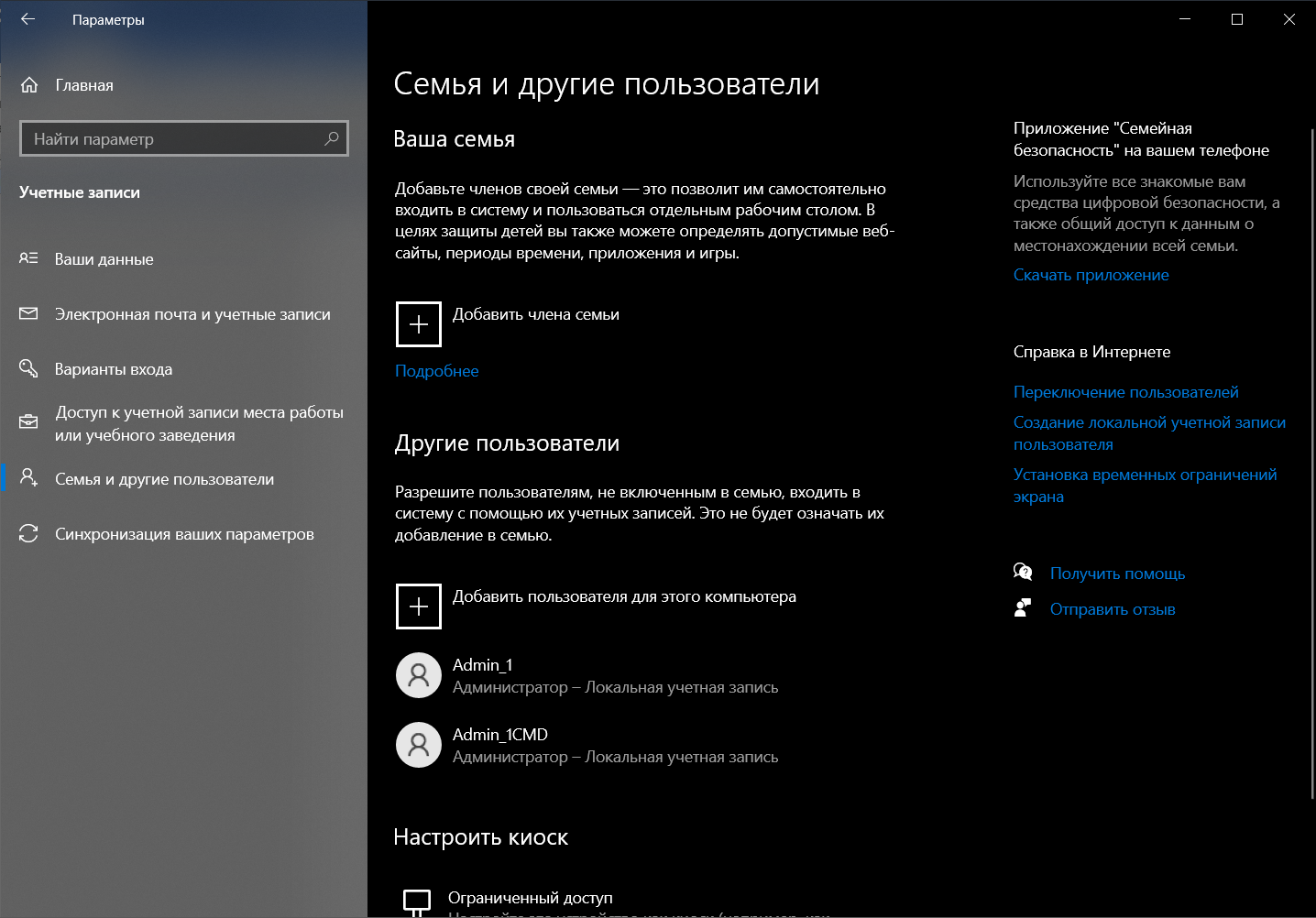


Рис. 11. Результат создания учётной записи администратора через командную строку

Для описания ограничения учётной записи администратора по изменению конфигурации системы, была установлена операционная система Windows 7на виртуальную машину, для демонстрации ограничений администратора, поскольку неизбежные изменения в основной операционной системе могут нанести вред конфигурации.

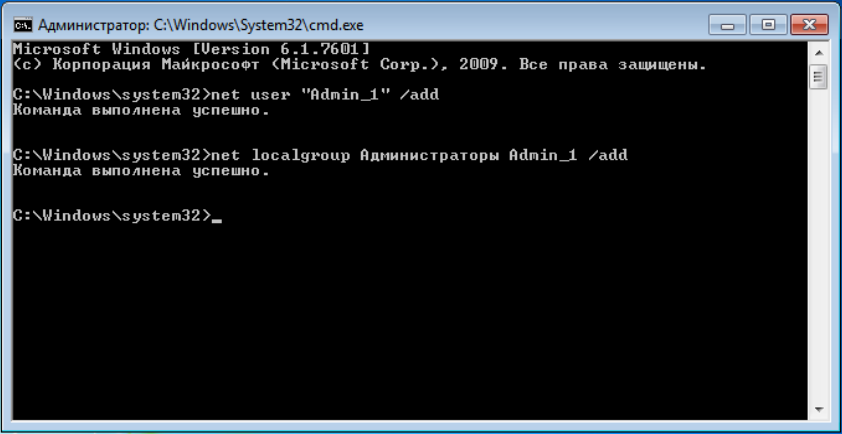


Рис. 12. Создание учётной записи администратора

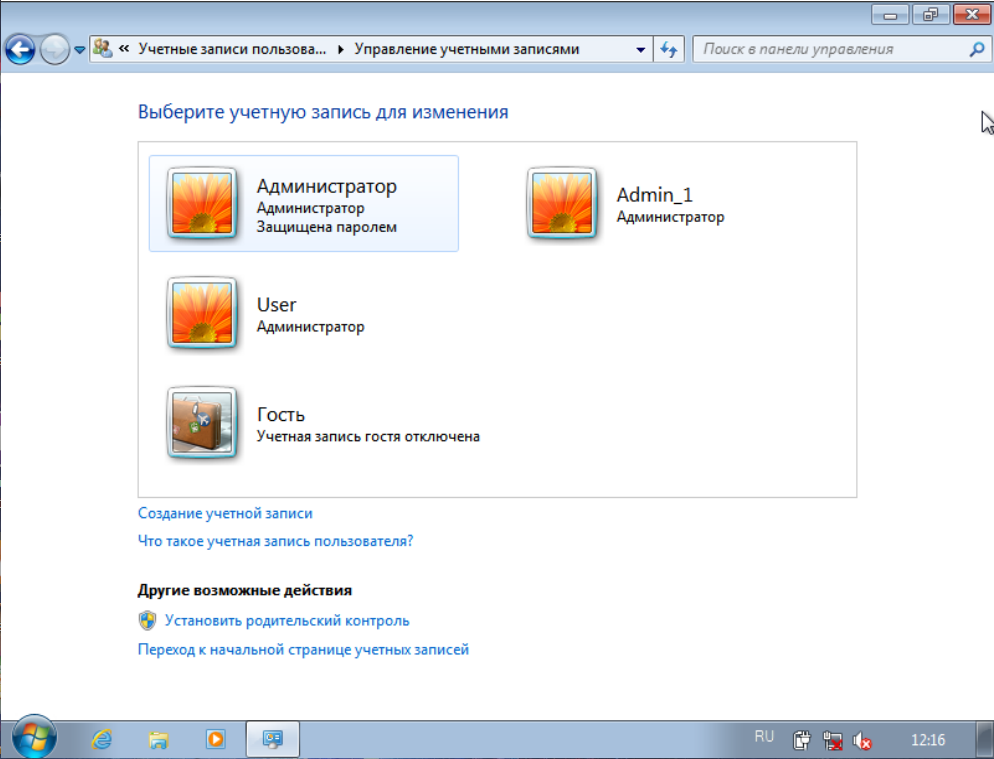


Рис. 13. Результат создания новой учётной записи администратора



Рис. 14. Рабочий стол учётной записи Admin\_1

**1 Ограничение:** нельзя удалять корневые каталоги операционной системы



Рис. 15. Попытка удаления папки Windows

**2 Ограничение:** нельзя удалить последнего администратора

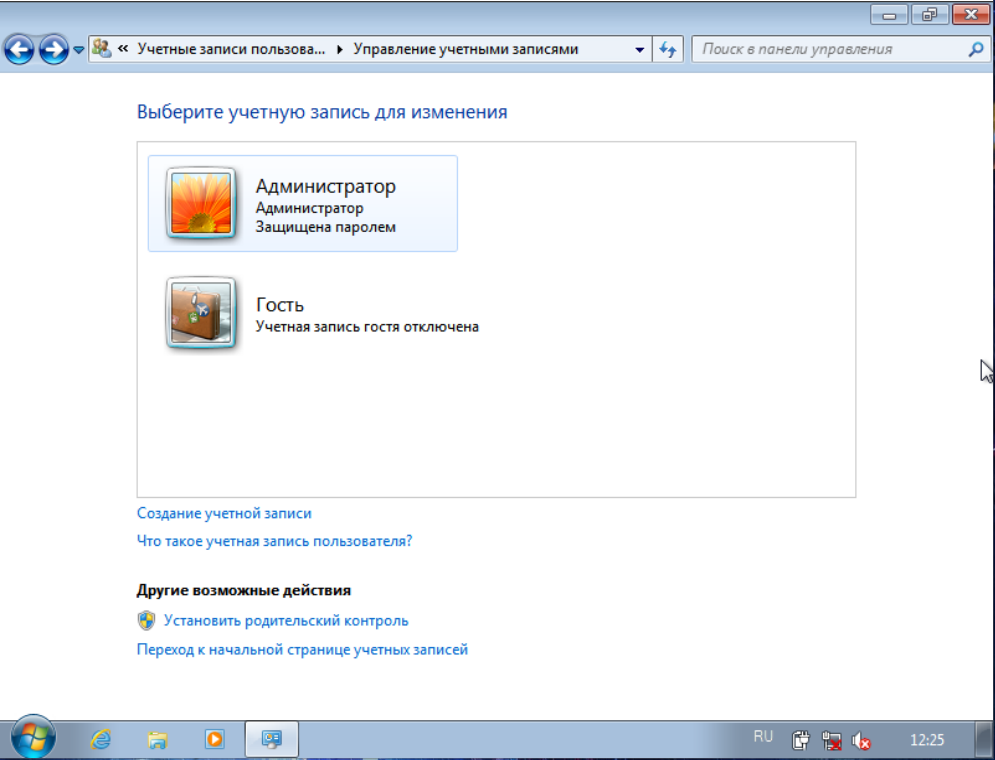


Рис. 16. Последняя учётная запись администратора

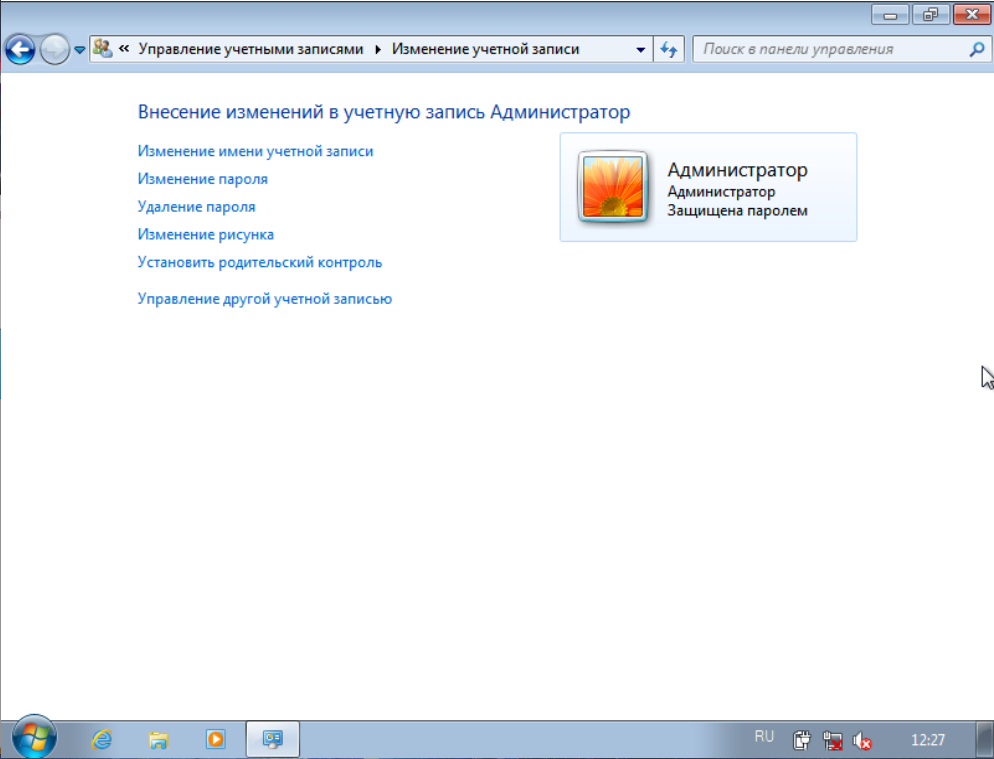


Рис. 17. Интерфейс управления учётной записью администратора

Как видно из рисунка 17, интерфейс управления учётной записью не позволяет удалить администратора, поскольку в таком случае система останется без управления.

**3 Ограничение:** нельзя удалить встроенную учётную запись администратора “Администратор” с других учётных записей, созданных самой учётной записью “Администратор”

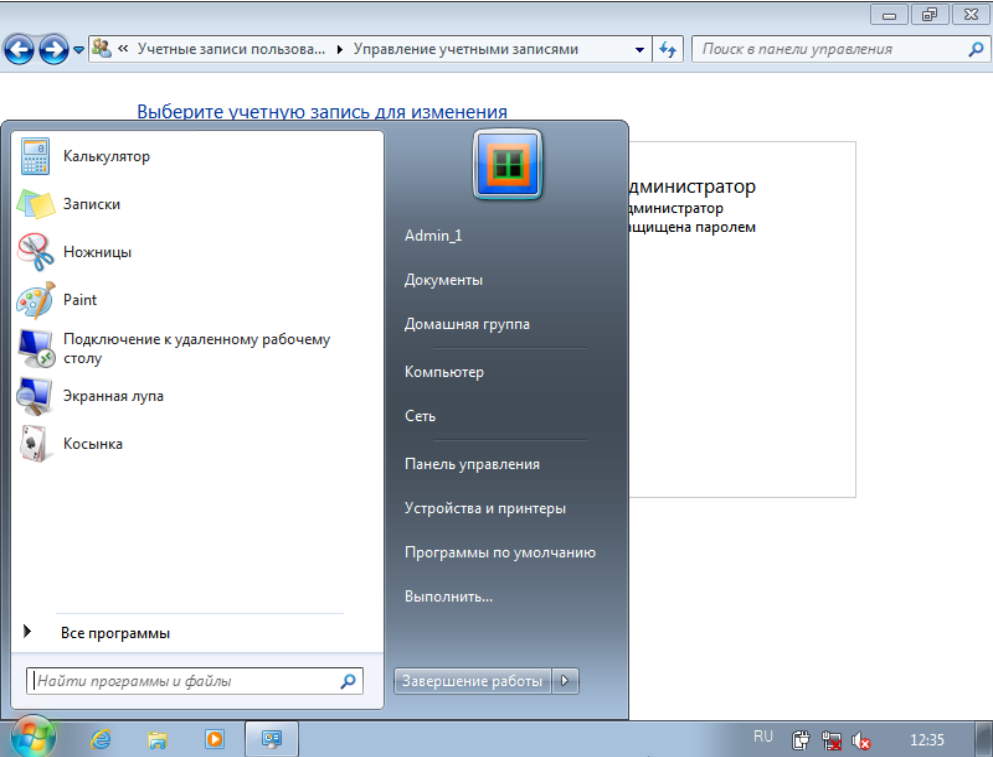


Рис. 18. Вход в учётную запись Admin\_1

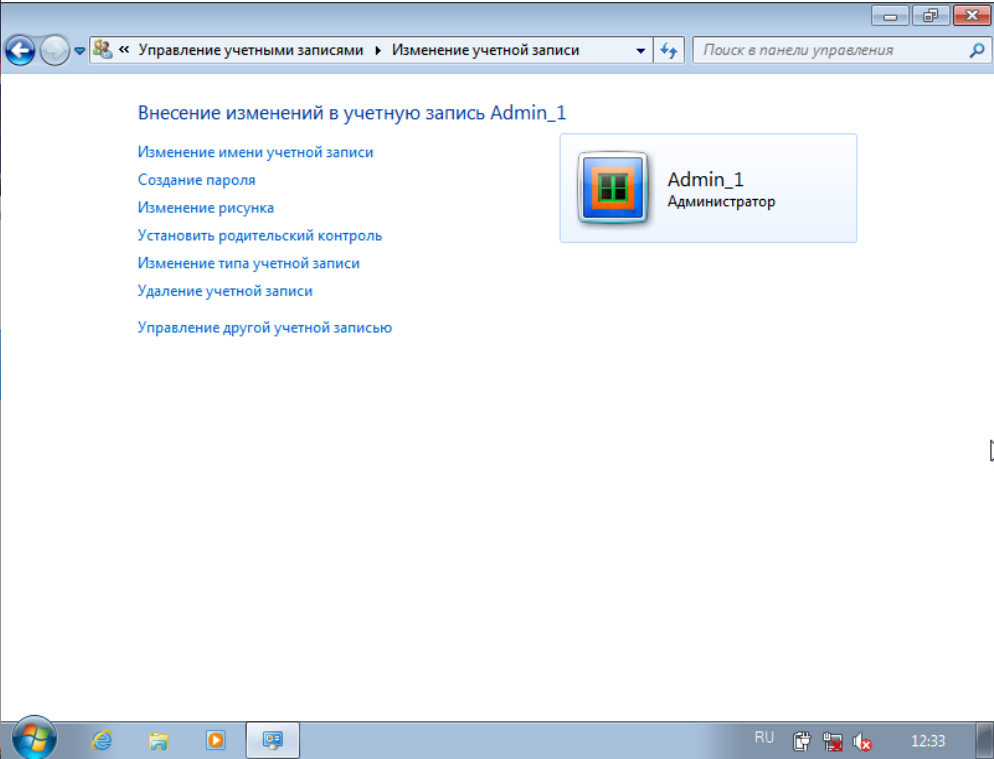


Рис. 19. Интерфейс внесения изменений для учётной записи администратора Admin\_1 (вход выполнен из Admin\_1)

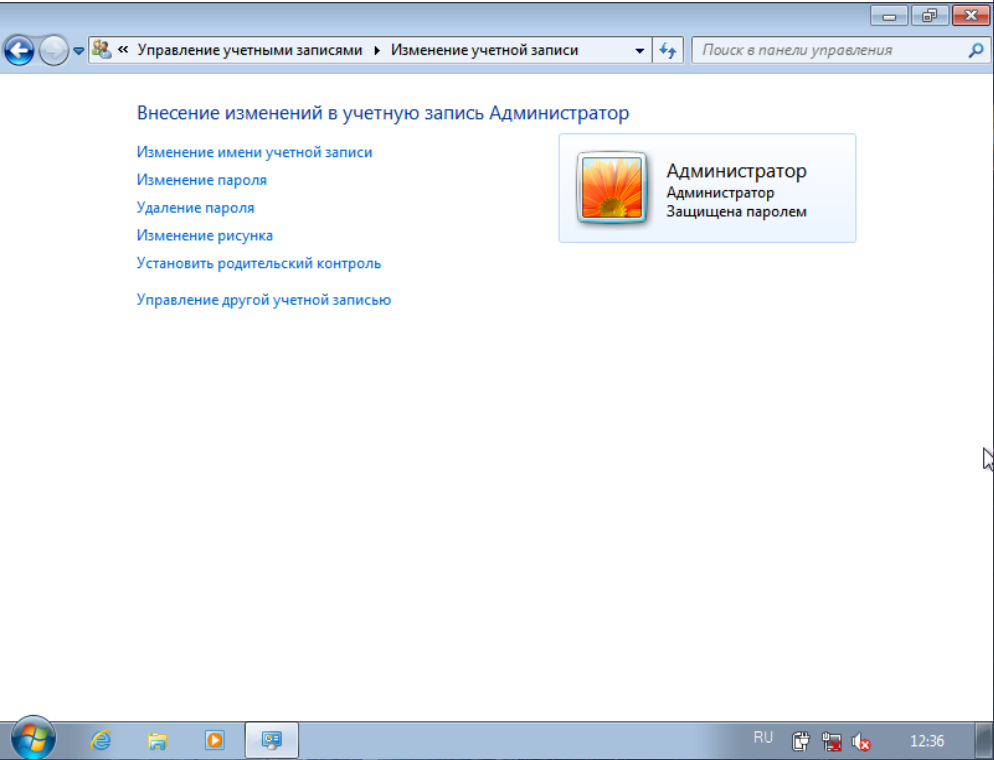


Рис. 20. Интерфейс внесения изменений для встроенной учётной записи “Администратор” (вход выполнен из Admin\_1)

**Задача 3:** Настроить вход пользователя в систему по паролю. Рассмотреть и реализовать возможные способы усиления парольной защиты.



Рис. 21. Создание пароля для учётной записи Admin\_1

Из рисунка 21 видно, что помимо создания пароля можно задать подсказку, которая будет видна всем, кто использует этот компьютер, на случай если пароль будет утерян. Для наибольшей степени защиты подсказку не стоит указывать. Сразу после создания пароля, при последующей попытке входе в систему необходимо будет ввести этот пароль (см. рис. 22).

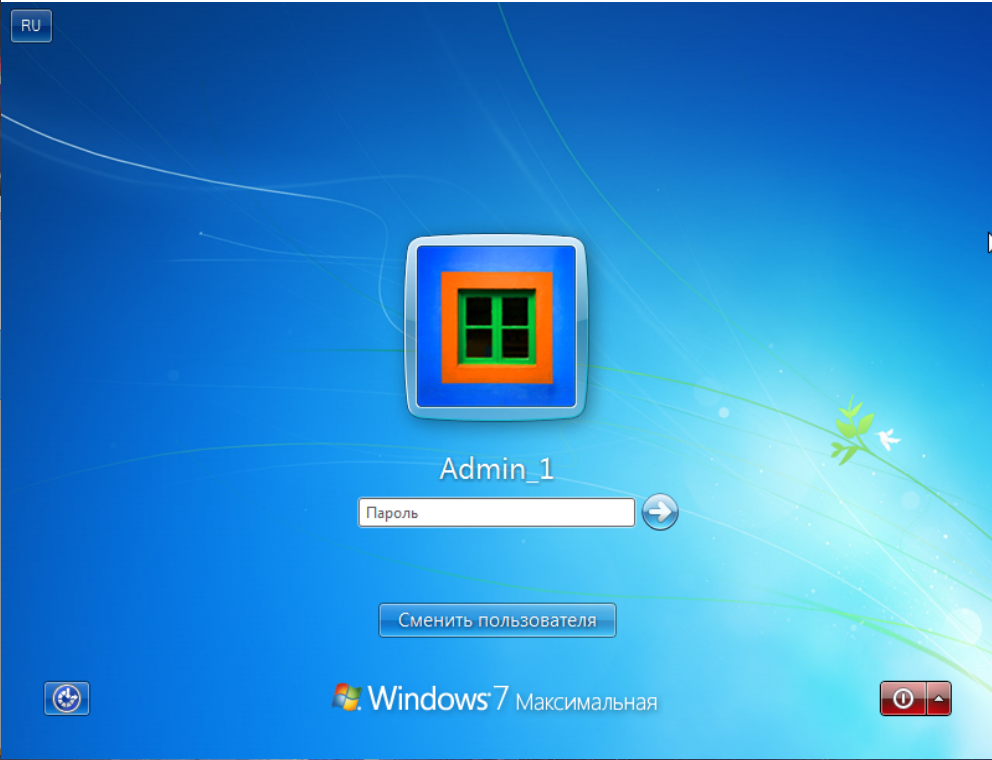


Рис. 22. Попытка входа в систему

Также, можно задать пароль для учётной записи с помощью командной строки. Для этого достаточно добавить после имени пользователя пароль.

Команда принимает следующий вид:

netuserимя\_пользователя пароль /add (для добавления пользователя)

netlocalgroupАдминистраторы имя\_пользователя /add (для выдачи прав администратора)

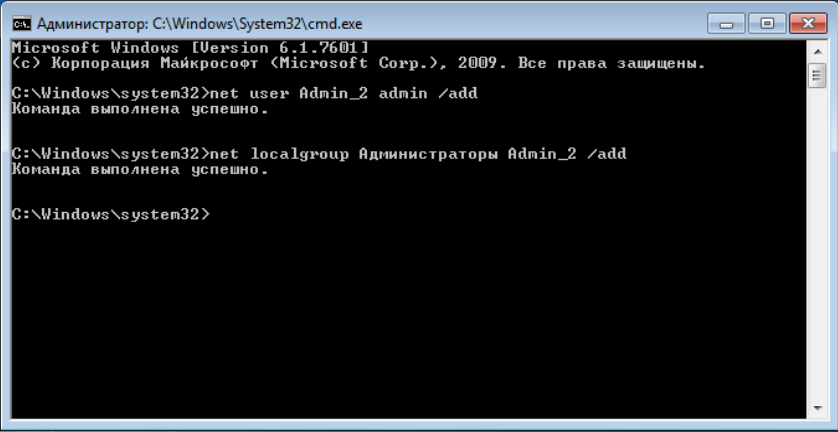


Рис. 23. Создание записи администратора с паролем в командной строке

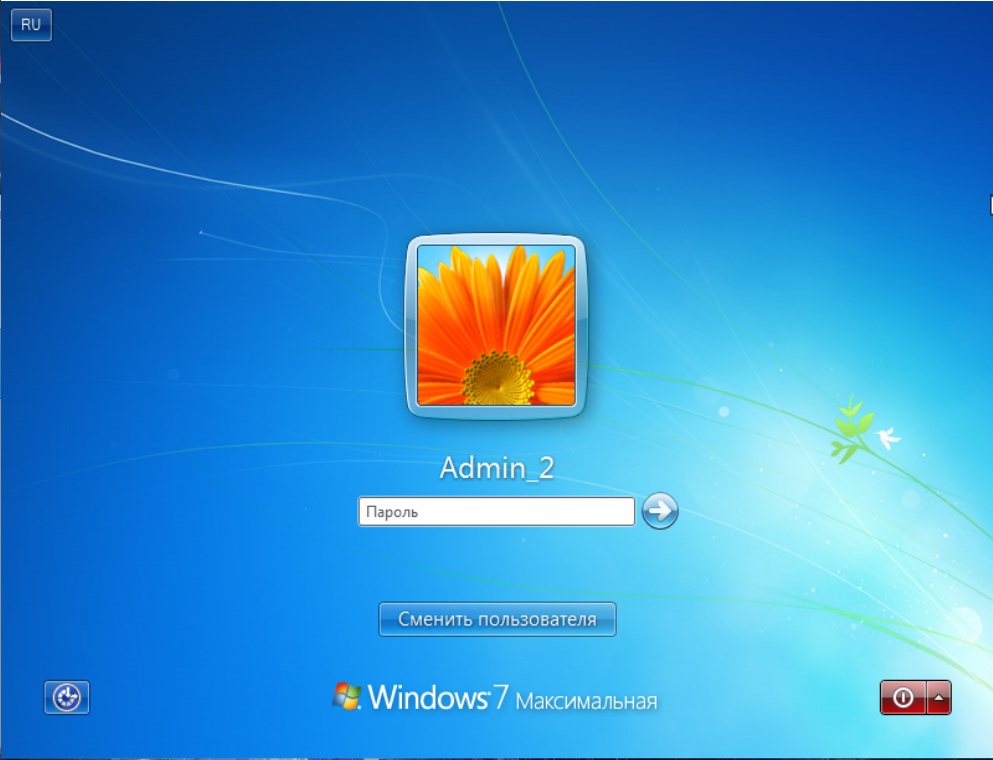


Рис. 24. Результат создания учётной записи Admin\_2 через командную строку

Для улучшения защиты учётной записи можно менять пароль на более сложный через каждый определённый промежуток времени. Например, менять пароль каждые 2-3 месяца.

При смене пароля система требует ввода текущего пароля для подтверждения операции.

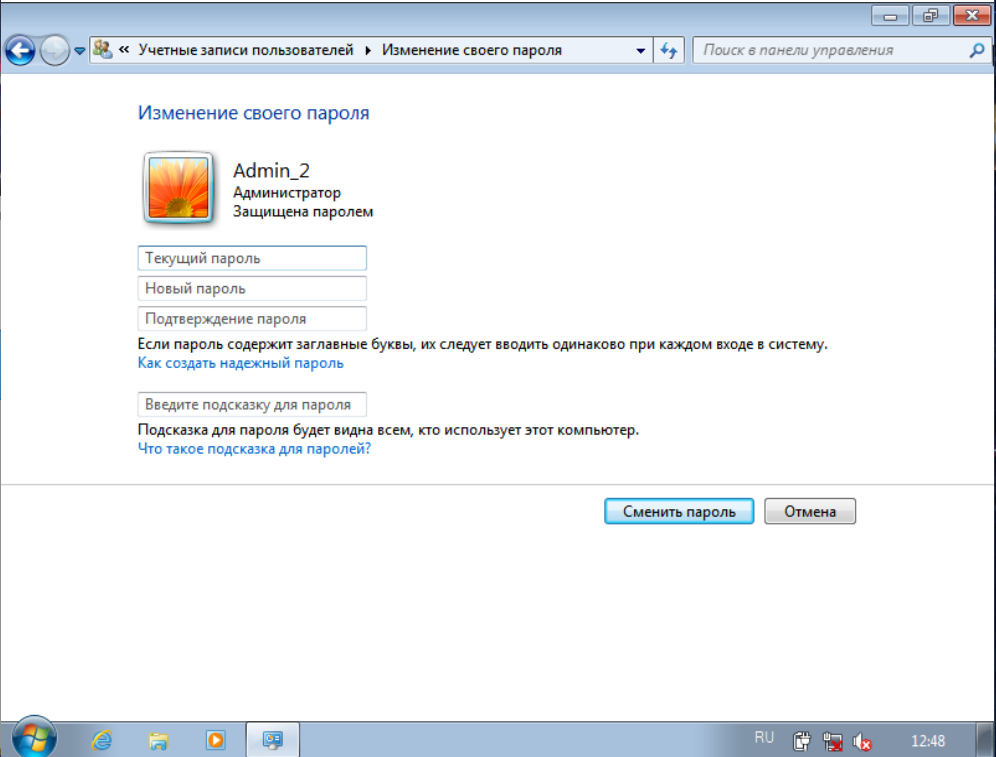


Рис. 25. Изменение пароля

**Задача 4:** Опишите параметры контроля учетных записей пользователей (UAC). (Перечислить параметры и дать им определение.).

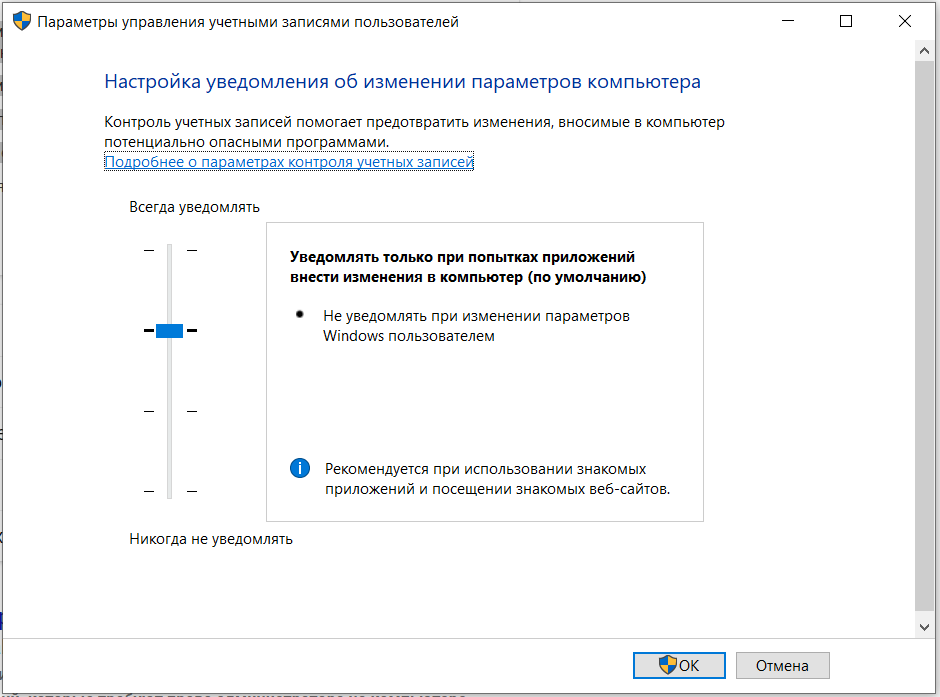


Рис. 26. Интерфейс управления параметрами управления учётными записями пользователей

Переместите ползунок, чтобы выбрать степень контроля функции "Контроль учетных записей" для обеспечения защиты от потенциально опасных изменений. Ниже приведены дополнительные сведения о каждом параметре.

**Параметр “Всегда уведомлять”**:

1.Вы будете получать уведомления при попытке программ установить программное обеспечение или внести изменения в компьютер.

2. Вы будете получать уведомления при изменении параметров Windows пользователем.

3. Другие задачи будут приостановлены до того, как пользователь среагирует на уведомление.

Примечание. Этот параметр рекомендуется использовать при частой установке нового программного обеспечения и посещении незнакомых веб-сайтов.

**Параметр “Уведомлять только при попытках программ внести изменения в компьютер”:**

1.Вы будете получать уведомления при попытке программ установить программное обеспечение или внести изменения в компьютер.

2. Вы не будете получать уведомления при изменении параметров Windows пользователем.

3. Другие задачи будут приостановлены до того, как пользователь среагирует на уведомление.

Примечание. Этот параметр рекомендуется использовать при частой установке нового программного обеспечения и посещении незнакомых веб-сайтов, но когда вы не хотите получать уведомления при внесении изменений в параметры Windows.

**Параметр “Уведомлять только при попытках программ внести изменения в компьютер (не затемнять рабочий стол)”:**

1.Вы будете получать уведомления при попытке программ установить программное обеспечение или внести изменения в компьютер.

2. Вы не будете получать уведомления при изменении параметров Windows пользователем.

3. Другие задачи не будут приостановлены или система не будет ждать ответа пользователя.

Примечание. Выбирайте этот параметр, только если затемнение рабочего стола компьютера занимает много времени. В противном случае рекомендуется выбрать один из параметров, описанных выше.

**Параметр “Никогда не уведомлять (Отключить UAC)”:**

1.Вы не будете получать уведомления при попытке программ установить программное обеспечение или внести изменения в компьютер.

2. Вы не будете получать уведомления при изменении параметров Windows пользователем.

3. Другие задачи не будут приостановлены или система не будет ждать ответа пользователя.

Примечание. Этот параметр не рекомендуется использовать из соображений безопасности.