Министерство образования и науки Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

—

Институт кибербезопасности и защиты информации

**Кафедра «Информационная безопасность компьютерных систем»**

**ЛАБОРАТОРНАЯ РАБОТА № 1**

«**Идентификация, аутентификация, авторизация. Настройка учетной записи Windows**»

по дисциплине «Цифровая грамотность»

Выполнил Соколов Родион Сергеевич

студент гр. 5131001/40003

Преподаватель Вагисаров Виктор Борисович

Санкт-Петербург

2024

**СОДЕРЖАНИЕ**

**Цель работы**………………………………………….………………………………3

**Задачи**…………………………………………………………………………………3

**Теоретические исследования**…………………………………………………….3-4

**Ход работы**………………………………………………………………………….4-5

**Вывод**………………………………………………………………………………….5**￼**

**Приложение**………………………………………………………………………..5-9

**Цель работы:**

Изучить типы числовых переменных в языке программирования С.

**Задачи:**

1. Узнать, что такое прямой, дополнительный и обратный коды.
2. Выяснить, как хранятся числа с плавающей запятой.
3. Написать программу, которая находит минимальное и максимальное значение для всех типов числовых переменных в С.

**Теоретические исследования**

**Идентификация** – это процесс определения пользователя в автоматизированной системе с использованием уникального свойства, известного как идентификатор. Для этого пользователь должен предоставить свой признак системе. Идентификатором может быть имя пользователя в системе, цифровой или буквенно-цифровой код, электронная подпись или другая информация. Ключевым условием является то, что этот признак не должен совпадать у нескольких пользователей.

Примером идентификации может служить процесс входа в учетную запись электронной почты. Когда вы хотите войти в свою учетную запись, вы вводите свое имя пользователя (идентификатор) и пароль. В этом случае ваше имя пользователя является уникальным признаком, который позволяет системе определить именно вас как пользователя. Если кто-то другой попытается использовать ваше имя пользователя с другим паролем, система не сможет его идентифицировать, так как комбинация этих данных необщая.

**Аутентификация** – это процесс проверки личности человека, который стремится получить доступ к системе. В этом процессе идентификатор сопоставляется с соответствующим ему подтверждающим фактором. Аутентификация часто осуществляется одновременно с идентификацией или после нее. Для подтверждения доступа могут использоваться текстовые пароли, цифровые коды, аппаратные или программные устройства, а также биометрические данные. В многофакторной аутентификации применяется несколько методов подтверждения параллельной

Примером аутентификации является процесс входа в банковское мобильное приложение. Когда пользователь вводит свое имя пользователя (идентификатор), система затем запрашивает пароль (подтверждающий фактор), чтобы проверить подлинность пользователя.

**Авторизация** – это процесс предоставления конкретному человеку или группе людей прав на выполнение определенных действий, а также проверка этих прав в момент попытки их осуществления. Это также может включать возможность передачи данных прав другому лицу.

**Разделение пользователей** по группам в операционных системах Windows необходимо для управления правами доступа и упрощения администрирования. Вот несколько основных причин, почему это важно:

1. Управление правами доступа: Группы позволяют устанавливать права и разрешения для нескольких пользователей одновременно. Вместо того чтобы назначать права каждому пользователю индивидуально, администраторы могут назначить права группе, и все ее члены автоматически получают эти права.
2. Упрощение администрирования: Работая с группами, администраторы могут легче управлять пользователями. Например, если необходимо изменить доступ к ресурсу, администратору нужно изменить права только для группы, а не для каждого отдельного пользователя.
3. Безопасность: Разделение пользователей на группы позволяет реализовать принципы минимальных привилегий. Это значит, что пользователи получают только те права, которые необходимы для выполнения их работы, что снижает риск несанкционированного доступа и ошибок.

Таким образом, разделение пользователей на группы в ОС Windows является важным инструментом для управления доступом, повышения безопасности и упрощения администрирования.

**Учетная запись Гостя** в операционных системах Windows обычно **отключена** по умолчанию по нескольким причинам:

1. Безопасность: Учетная запись Гостя предоставляет минимальные права доступа к системе, но оставляет возможность другим пользователям получать доступ к компьютеру. Это может представлять риск, так как злоумышленник может попытаться воспользоваться учетной записью для несанкционированного доступа или выполнения вредоносных действий.
2. Отсутствие контроля: Учетная запись Гостя не требует создания индивидуального пароля и может создавать проблемы с отслеживанием действий, выполняемых пользователями. Это затрудняет админис­траторам управление системой и мониторинг, кто и какие действия выполнял.
3. Сохранение данных: Учетная запись Гостя обычно не сохраняет пользовательские данные или настройки, что может приводить к путанице среди пользователей. Более того, потенциально это может вызвать проблемы с совместным использованием ресурсов, например, файлов и принтеров.
4. Функциональность: В большинстве случаев пользователям не требуется доступ к системе через учетную запись Гостя. Вместо этого они могут быть созданы специальные учетные записи для временных пользователей с ограниченными правами, что дает больший контроль над доступом.

Таким образом, отключение учетной записи Гостя по умолчанию обеспечивает повышенный уровень безопасности и контроль над системой, что критически важно в современных условиях киберугроз.

**Ход работы**

С помощью командной строки, запущенной от имени администратора, были созданы учетные записи из групп «Пользователи» (polzovatel), «Администраторы» (admin), а также была активирована гостевая учетная запись (gost).(Рисунок 1 и 2)

Используемые команды:

- net user <username> <password> /add - создание нового пользователя.

- net localgroup <group\_name> <username> /add - добавление пользователя в группу.

Был выполнен вход в учетную запись «polzovatel», создана новая директория «polzovatel», в которой был создан файл «polzovatel.txt». (Рисунок 3, 4)

Был выполнен вход в учетную запись «admin», создана новая директория «admin», в которой был создан файл «admin.txt». (Рисунок 5, 6)

От имени «polzovatel» была произведена попытка записи данных в файл «admin.txt», в результате «polzovatel» было отказано в доступе. (Рисунок 7)

От имени «admin» была произведена попытка записи данных в файл «polzovatel», в результате «admin» имел доступ, чтобы изменить файл. (Рисунок 8, 9)

От имени «gost» была произведена попытка добавить записи в файлы «admin.txt», «polzovatel.txt», в результате «gost» было отказано в доступе к обоим файлам. (Рисунок 10)

**Вывод**

В ходе работы были приобретены навыки управления учетными записями в операционной системе Windows, освоены основы работы в командной строке и навыки настройки прав доступа к объектам ОС. Также были изучены термины идентификация, аутентификация и авторизация. В процессе исследования была обозначена необходимость регулирования прав различных категорий пользователей.

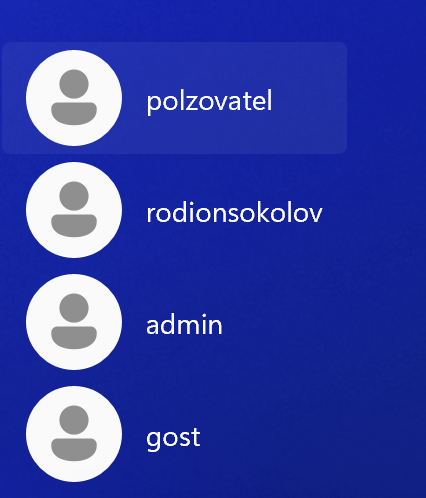
**Приложение**

Рисунок 1.

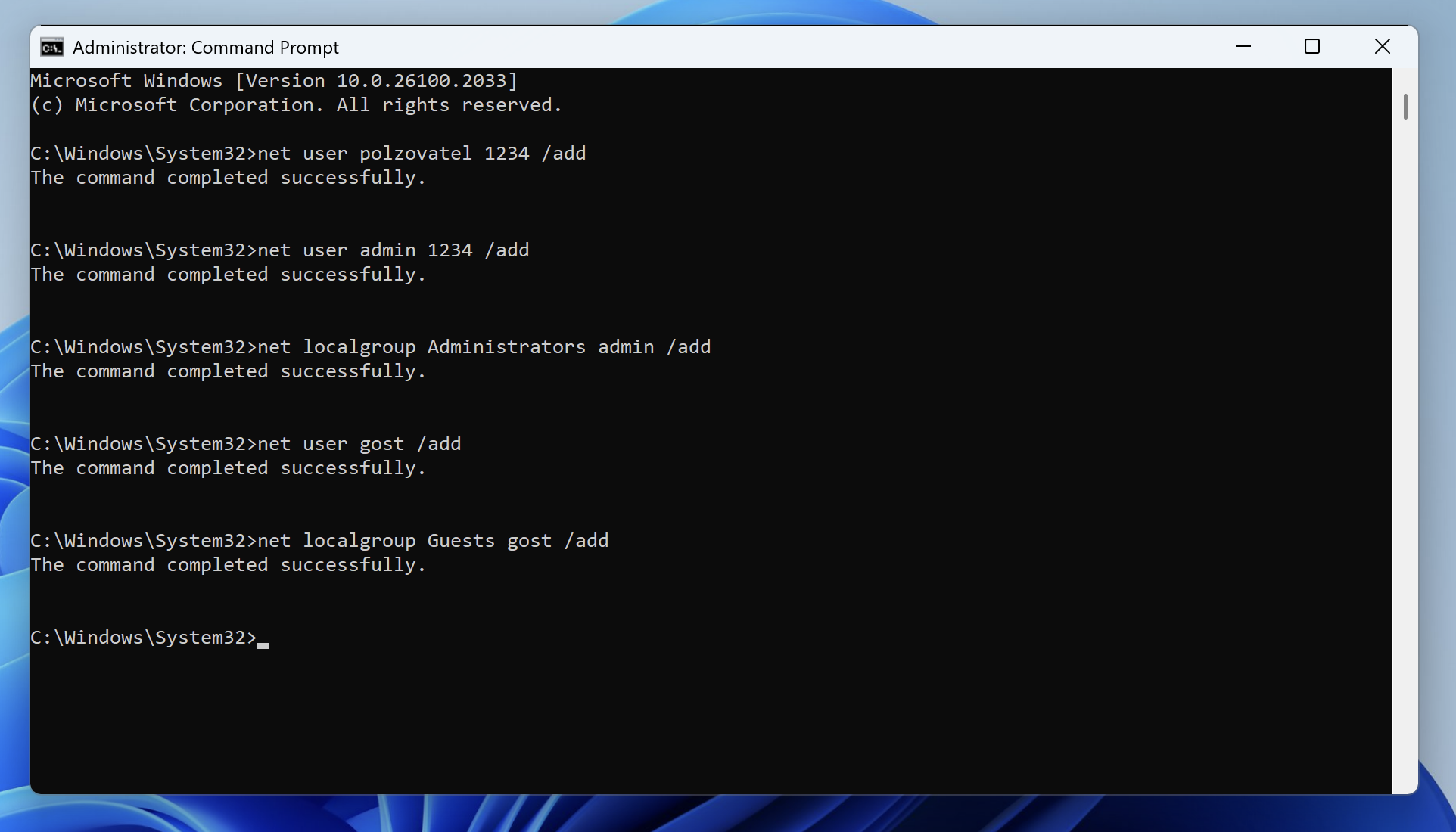
Рисунок 2.

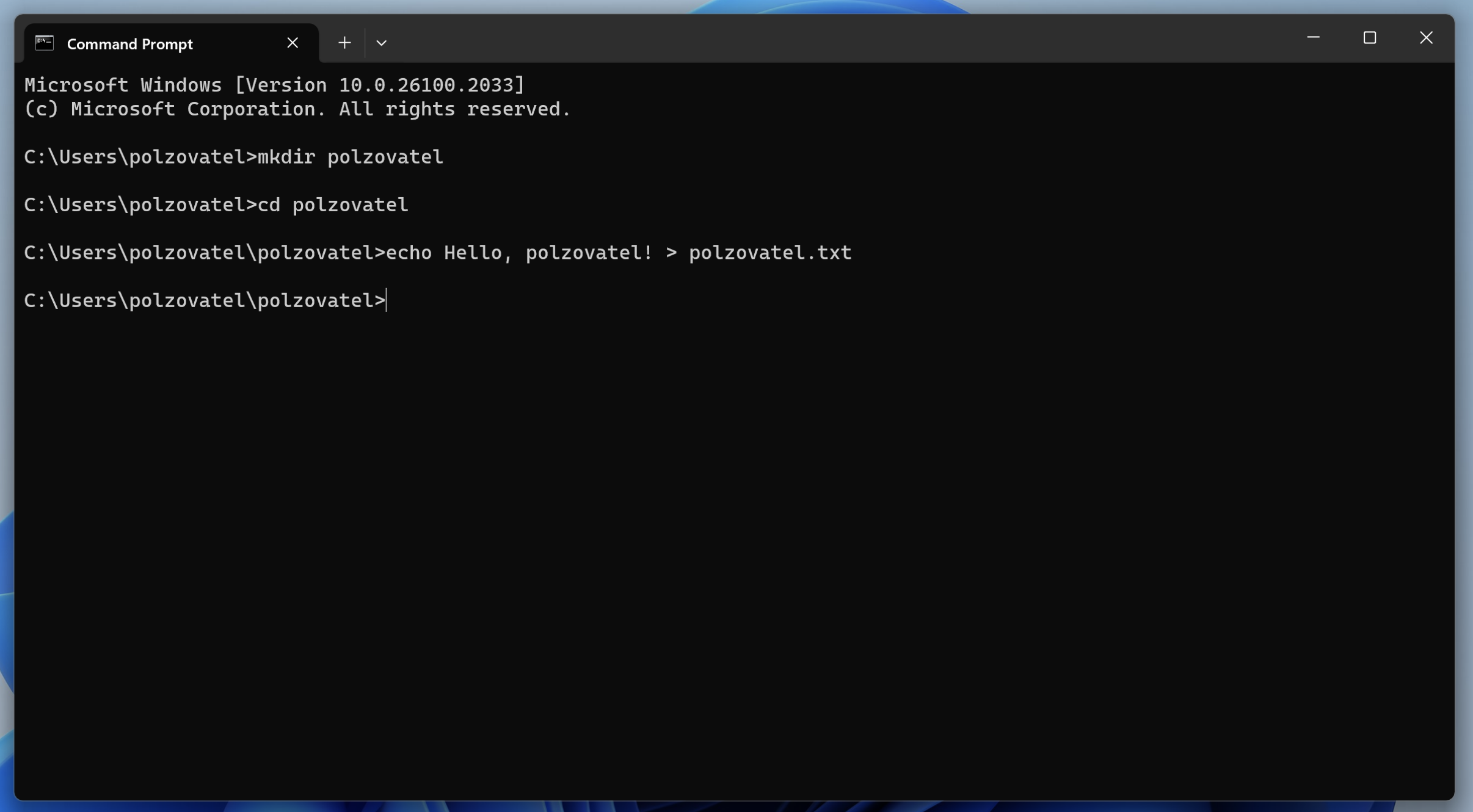
Рисунок 3.

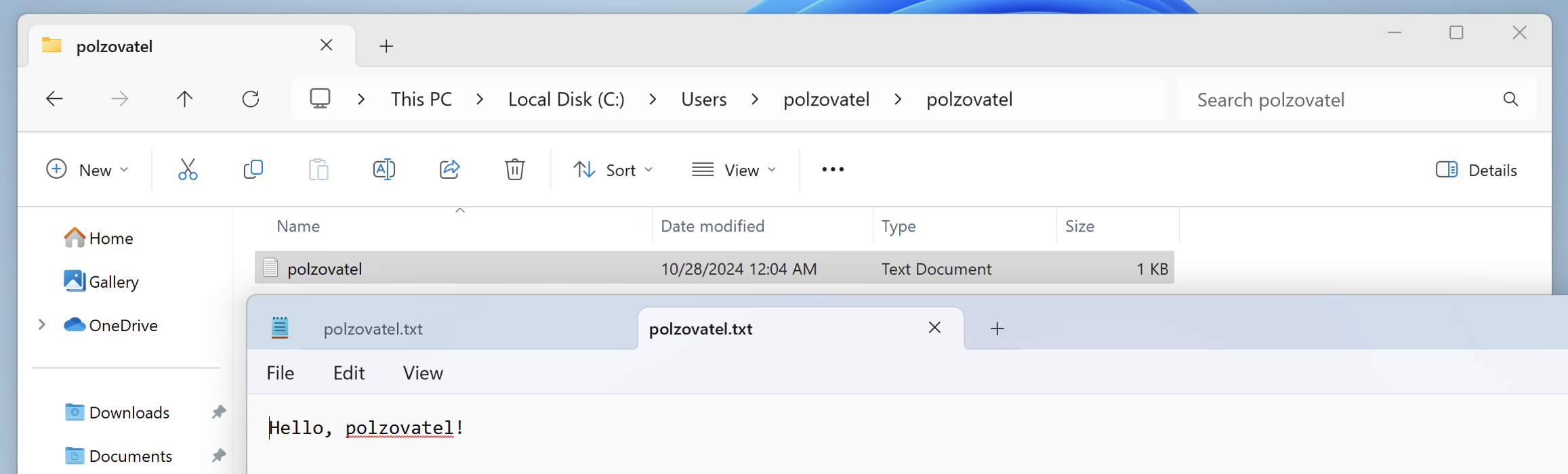
Рисунок 4.

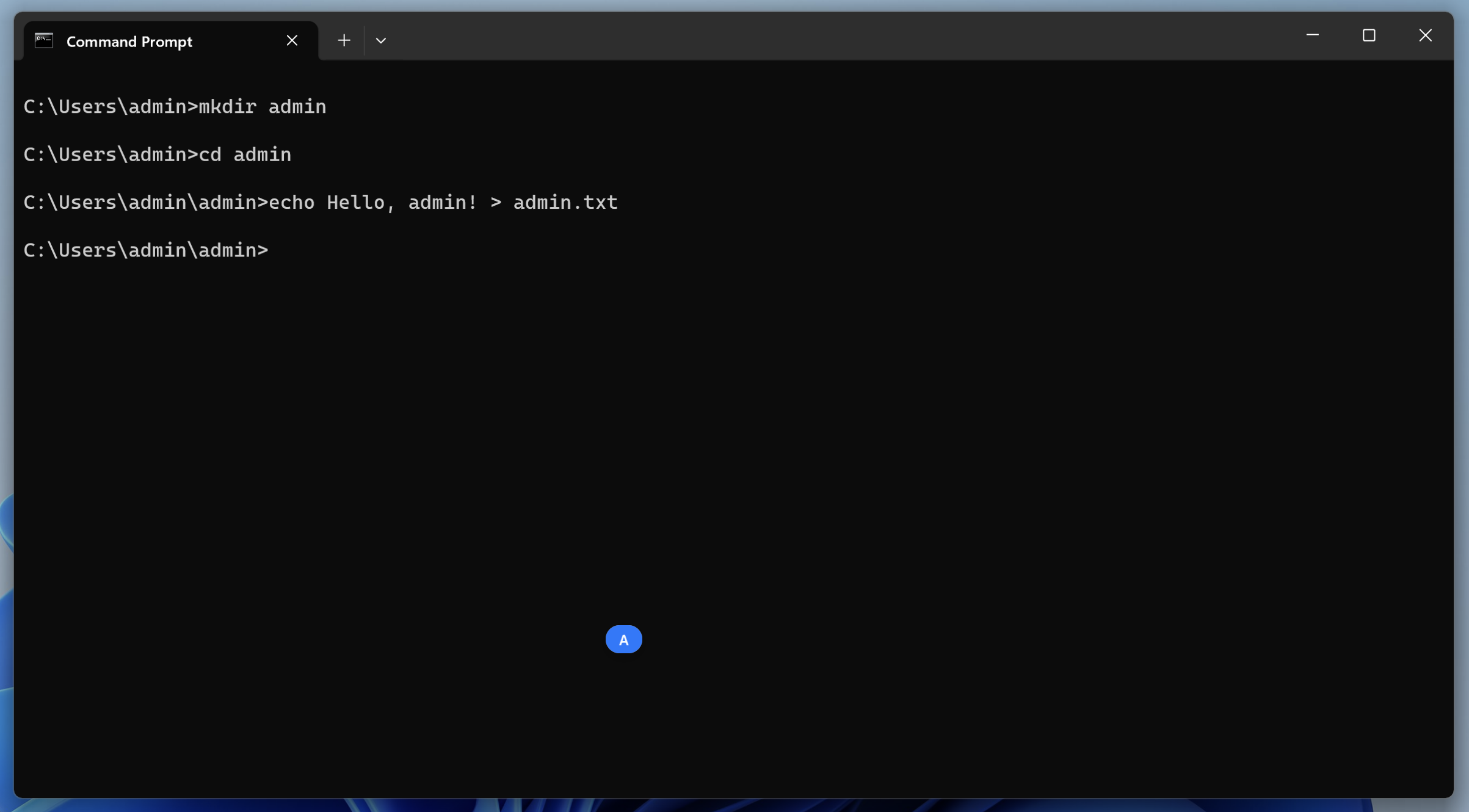
Рисунок 5.

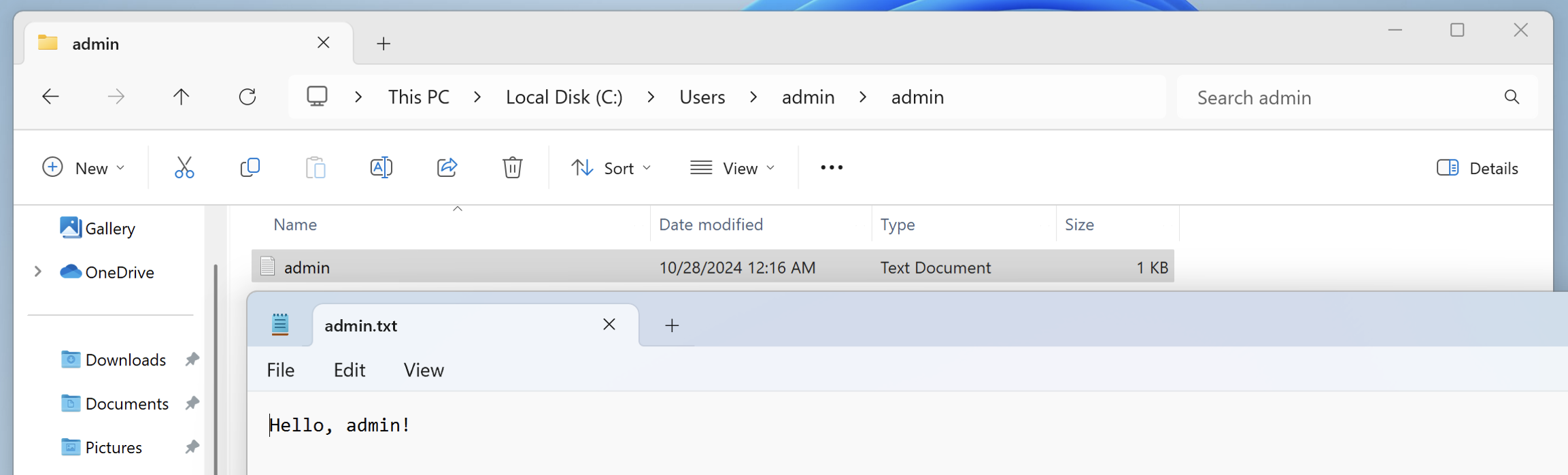
Рисунок 6.

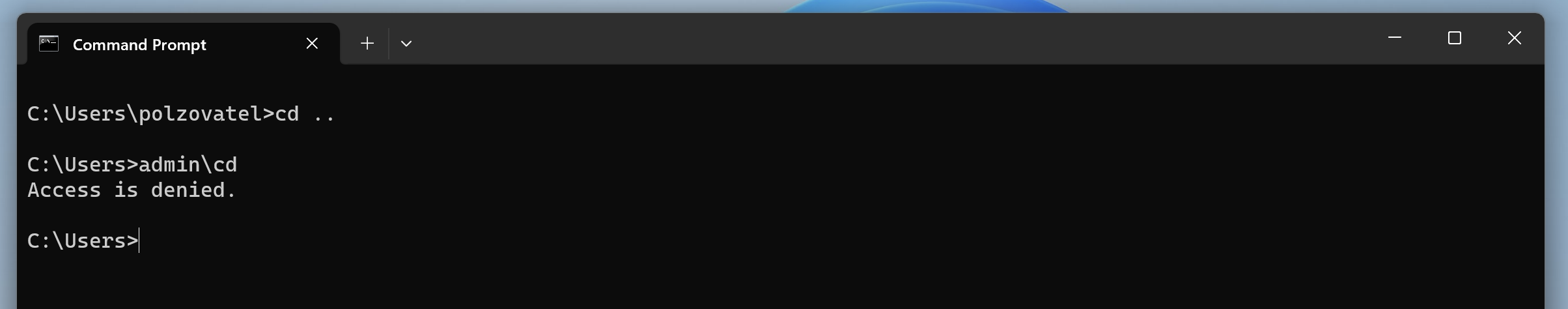
Рисунок 7.

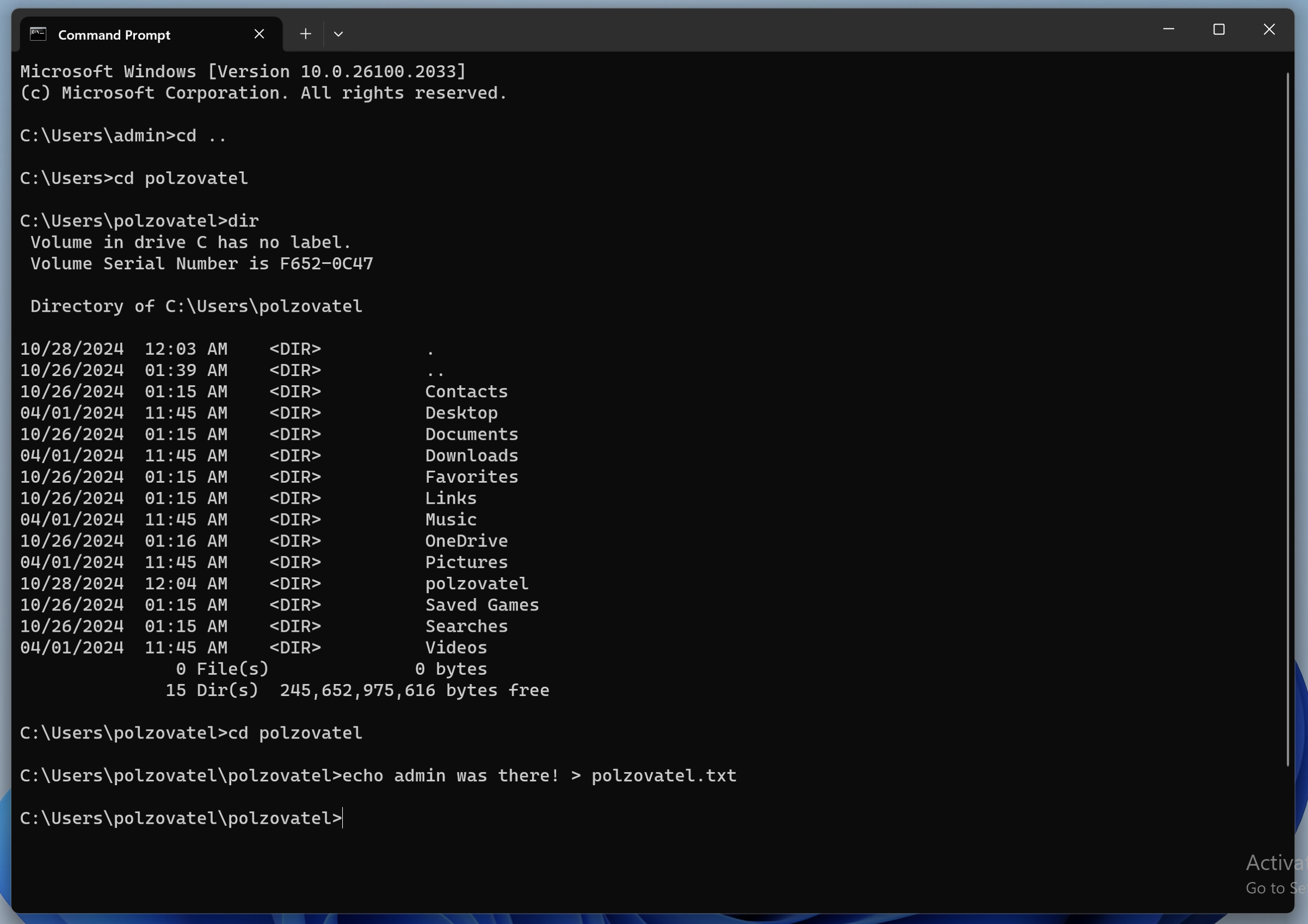
Рисунок 8.

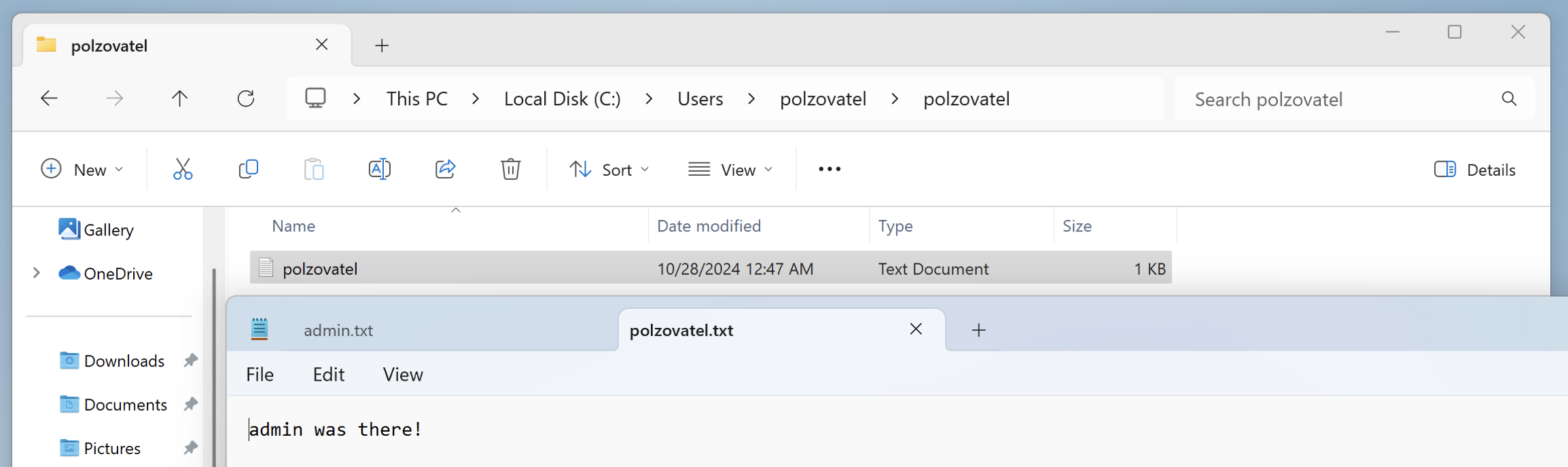
Рисунок 9.

Рисунок 10.