МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИМ. В.Н.ТАТИЩЕВА

Факультет цифровых технологий и кибербезопасности

Кафедра информационных технологий

Форма обучения очная

**БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ**

**ЛАБОРАТОРНАЯ РАБОТА №3**

***Методы парольной защиты. Разработка программной парольной защиты***

|  |  |  |
| --- | --- | --- |
| Исполнитель:  студент группы ДПИ-25  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Мартынов В.А.  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2025 г.    Преподаватель:  Кафедра информационных технологий  Кандидат технических наук, доцент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Мартьянова А.Е.  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2025 г. |  |  |

Астрахань – 2025

1. **Практическая часть**

Для выполнения задания был выбран вариант №10:

* Длина пароля 8 символов.
* Используется кириллица (прописные и строчные буквы).
* При смене пароля происходит проверка на отсутствие повторяющихся символов.

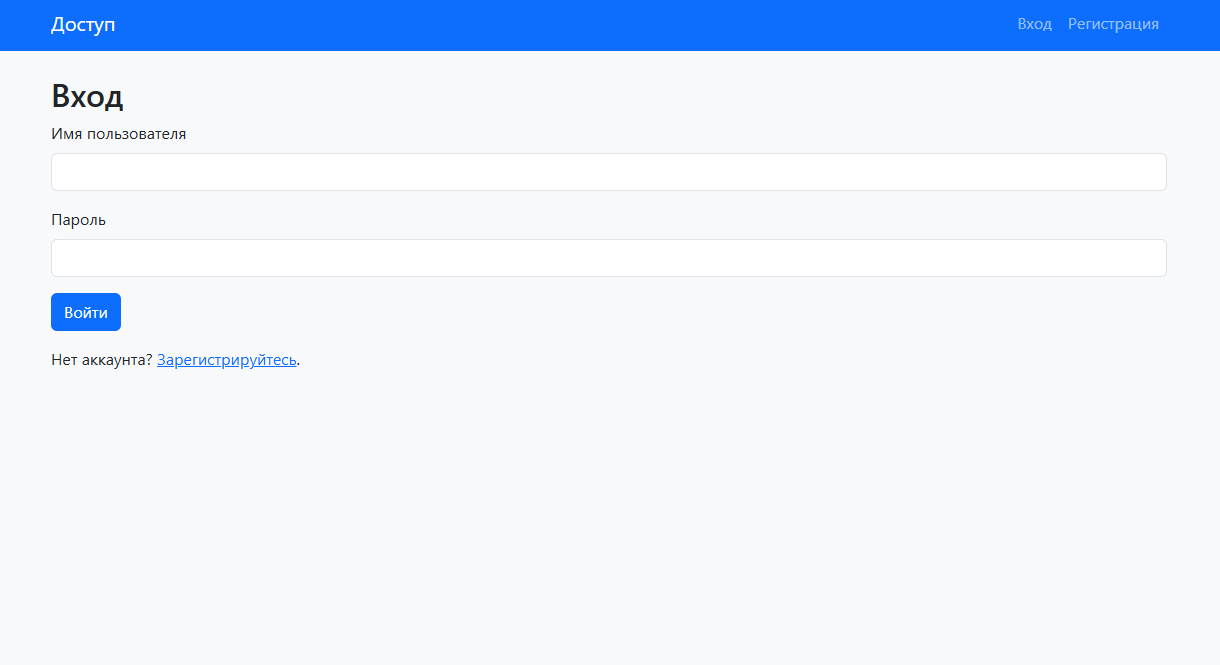


Рисунок 1 – Окно входа в систему

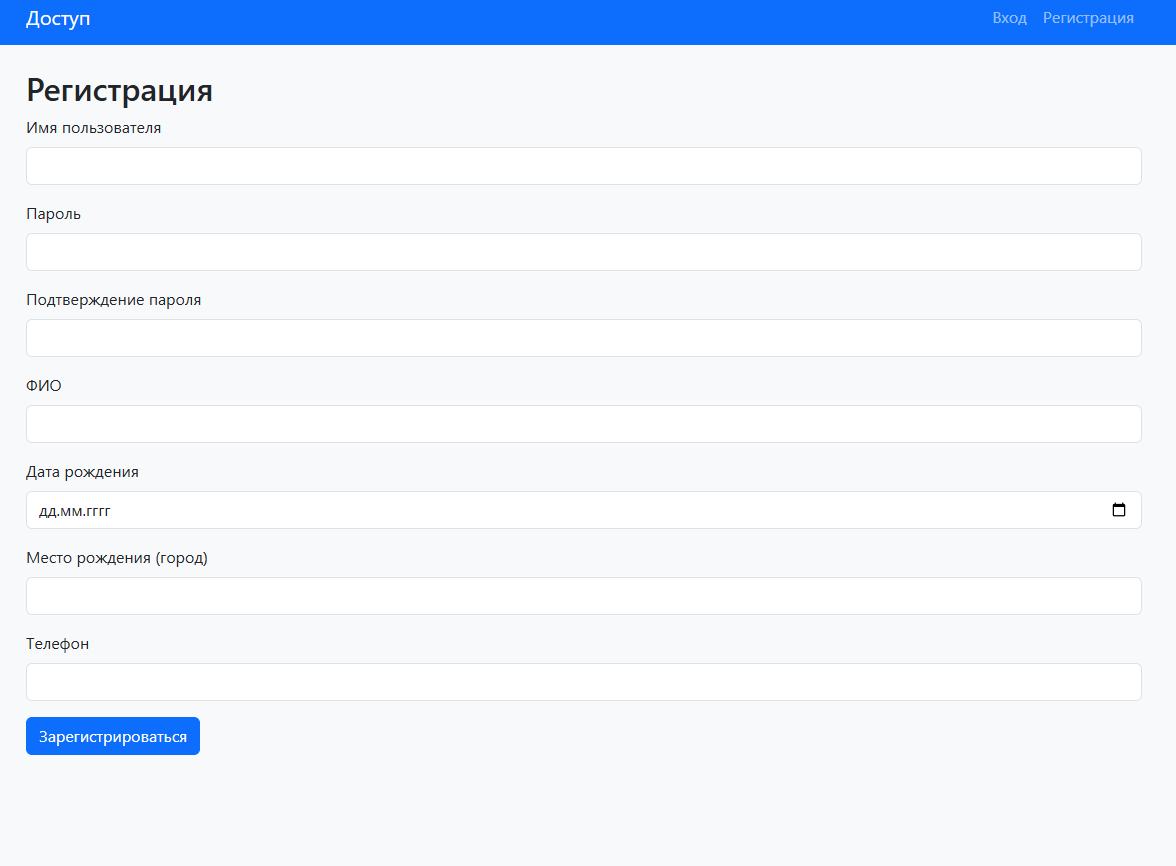


Рисунок 2 – Окно регистрации

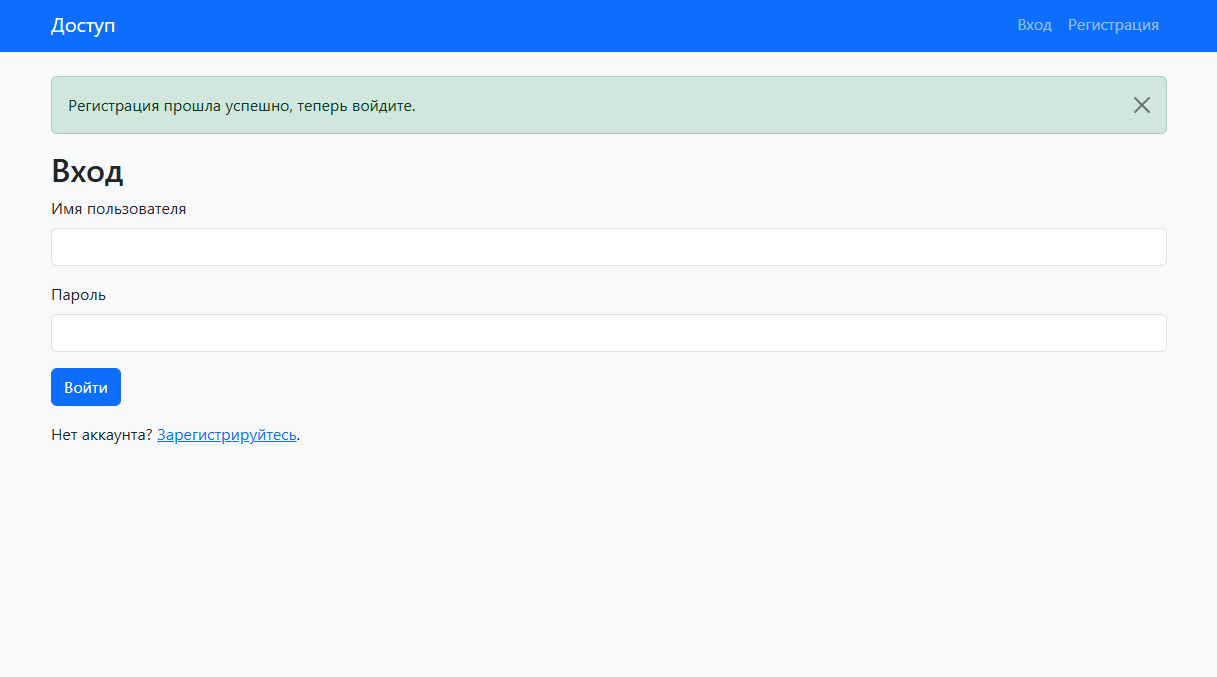


Рисунок 3 – Окно после регистрации

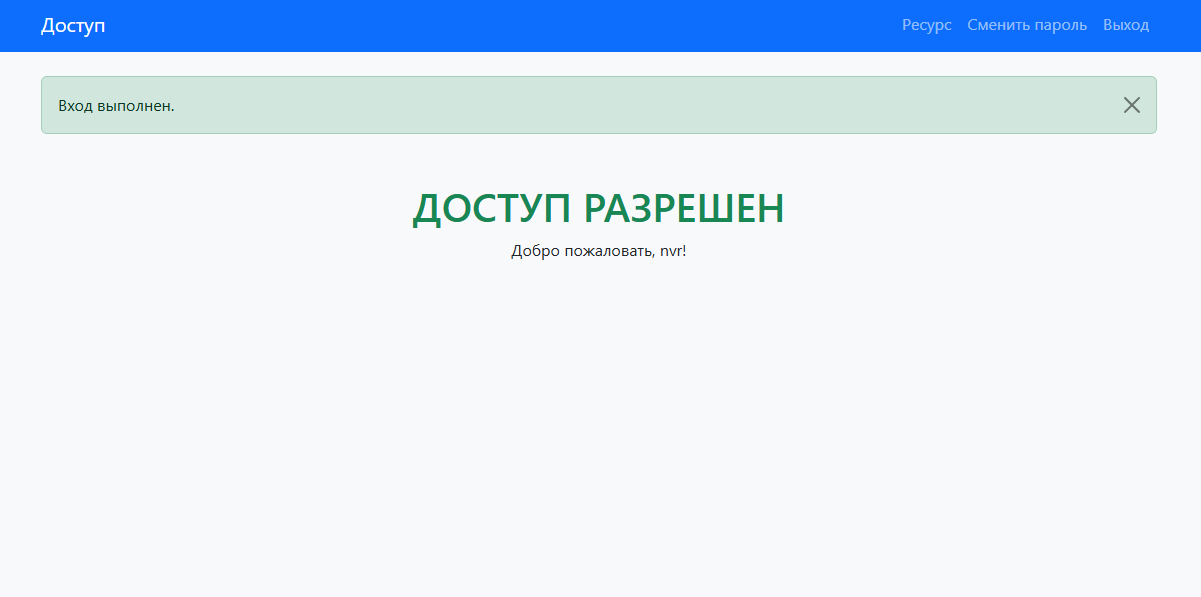


Рисунок 4 – Доступ получен

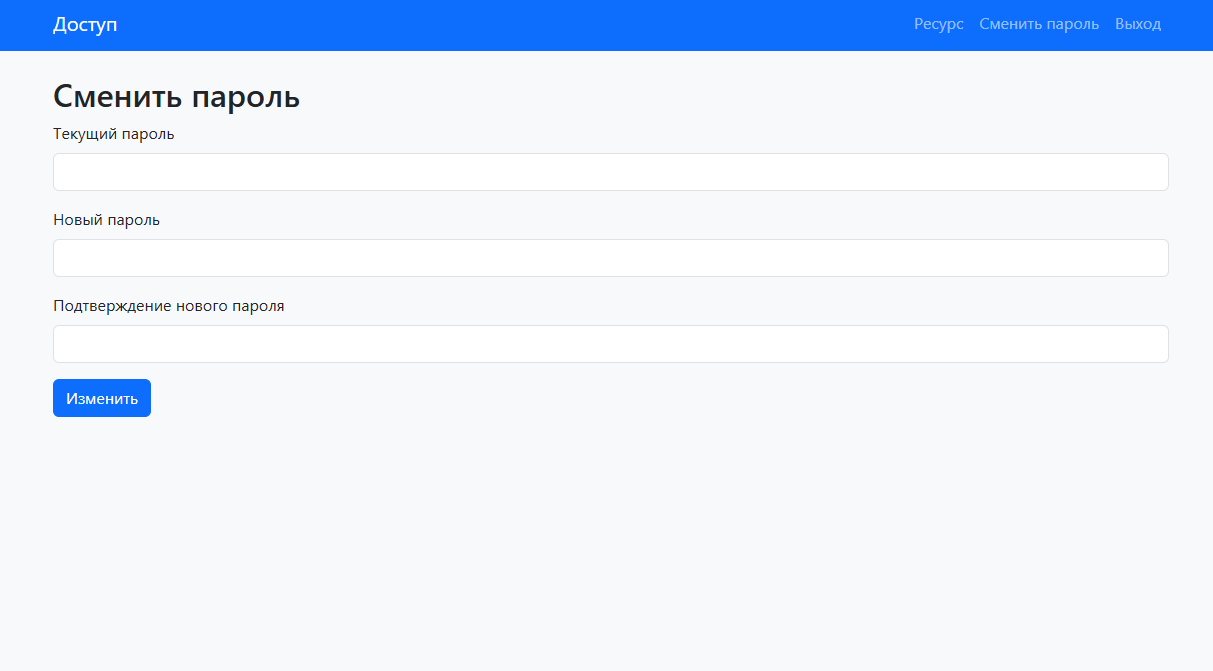


Рисунок 5 – Окно смены пароля

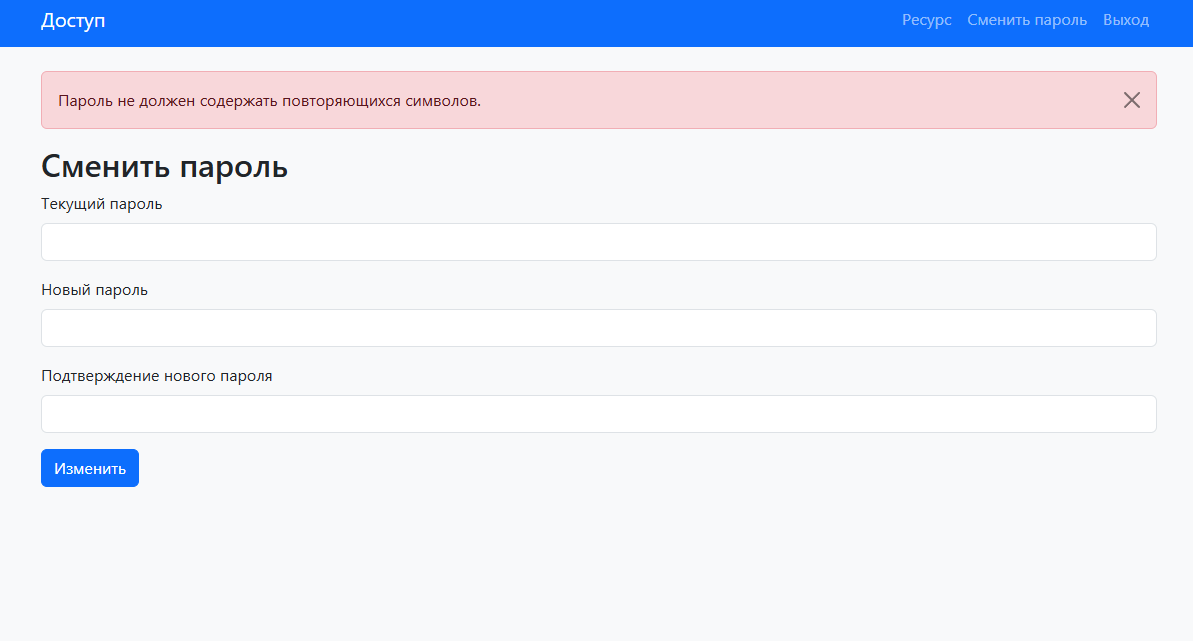


Рисунок 6 – Проверка на повторение символов

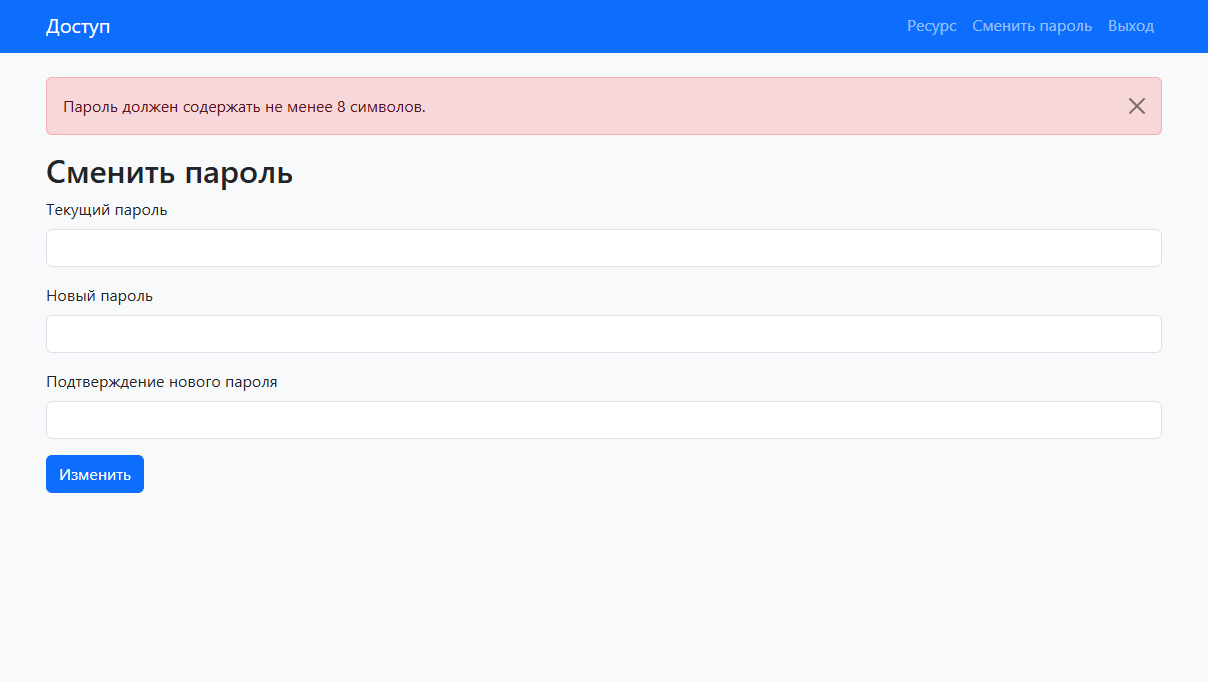


Рисунок 7 – Проверка на количество символов

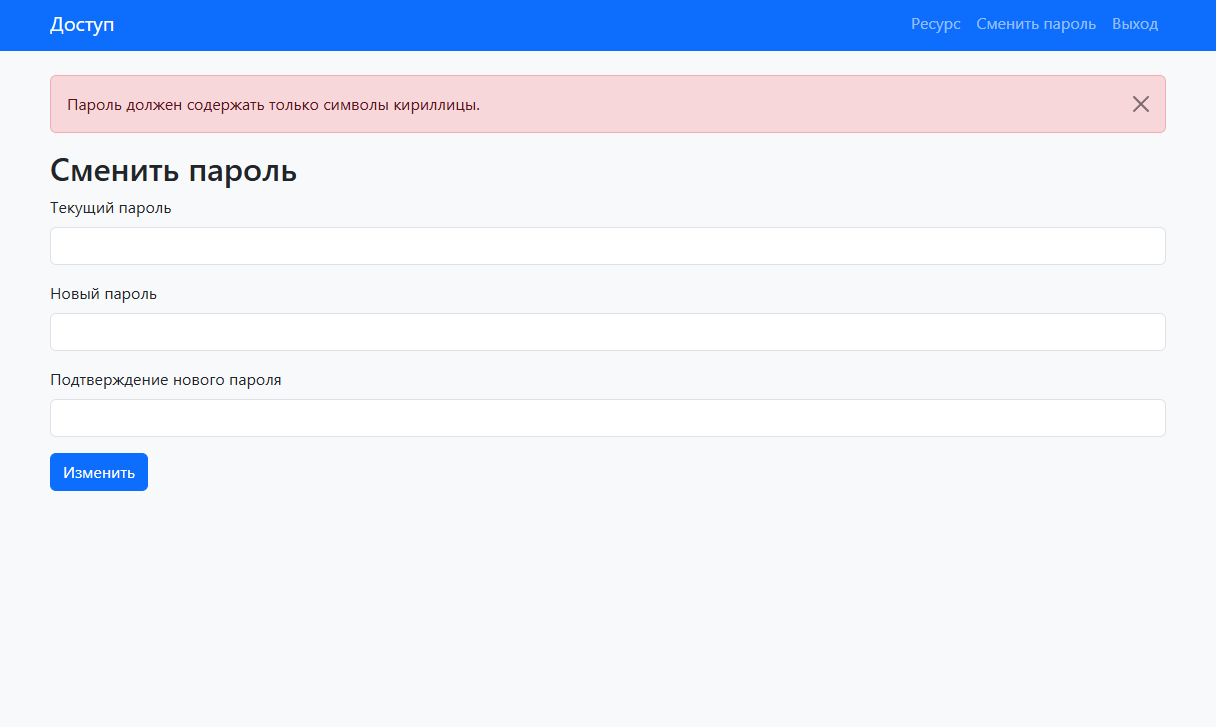


Рисунок 8 – Проверка на кириллицу

1. **Ответы на контрольные вопросы**
2. Аутентификация — это процесс проверки подлинности пользователя или системы, направленный на подтверждение их права доступа к определенным ресурсам или данным. Он происходит после идентификации (определения, кто именно пытается получить доступ) и предшествует авторизации (предоставлению прав доступа). Простыми словами, аутентификация подтверждает, что пользователь действительно тот, за кого себя выдает, например, с помощью пароля или биометрических данных.

Примеры аутентификации:

* Ввод логина и пароля при входе в аккаунт на сайте.
* Использование одноразового кода, присылаемого по SMS, вместе с паролем (двухфакторная аутентификация).
* Сканирование отпечатка пальца или распознавание лица для доступа к смартфону.

Существует несколько видов аутентификации:

* Однофакторная (например, только пароль).
* Двухфакторная (пароль + код из SMS).
* Многофакторная (пароль + код + биометрия и др.).

1. Идентификация в информационных системах — это процедура, в результате которой субъекту (пользователю или объекту) присваивается уникальный идентификатор, однозначно идентифицирующий его в системе. Идентификатор должен быть заранее назначен (например, при регистрации) и служит для того, чтобы система могла распознать, кто пытается получить доступ, отвечая на вопрос «Кто это?».

Процесс идентификации тесно связан с аутентификацией: после успешной аутентификации система подтверждает подлинность субъекта и определяет его идентификатор. Например, при входе в систему пользователь вводит логин (идентификация), а затем пароль для подтверждения личности (аутентификация).

Примеры идентификации:

Логин пользователя в системе.

* Номер банковской карты, считываемый при оплате.
* Штрих-код товара в магазине.
* Идентификатор сертификата электронной подписи.

1. Авторизация пользователя — это процесс предоставления пользователю определенных прав, разрешений и привилегий для доступа к ресурсам и функциям информационной системы после успешной идентификации и аутентификации. Авторизация определяет, что именно пользователь может делать в системе, какие данные просматривать, изменять или какие действия выполнять.

Иными словами, если идентификация отвечает на вопрос "кто ты?", аутентификация — "ты действительно тот, за кого себя выдаешь?", то авторизация отвечает на вопрос "что тебе разрешено делать?".

Пример: пользователь вводит логин (идентификация), затем пароль (аутентификация), и после этого система проверяет, имеет ли он право, например, читать, редактировать или удалять определенный файл — это авторизация.

1. Пароль — это строка символов, используемая для подтверждения личности пользователя и защиты доступа к системам, учетным записям и данным. Пароли могут состоять из букв, цифр, специальных символов и их комбинаций. Основная цель пароля — обеспечить аутентификацию пользователя и защиту информации от несанкционированного доступа.

Пароль служит уникальным секретом пользователя, который позволяет системе подтвердить его личность и предоставлять соответствующие права доступа. Если пароль состоит только из цифр, его иногда называют ПИН-кодом. Иногда для повышения безопасности используют парольные фразы — комбинации из нескольких слов.

Примеры использования паролей: вход в операционную систему, доступ к электронной почте, авторизация в интернет-банкинге.

Пароль является важным элементом информационной безопасности, и для его надежности рекомендуется использовать сложные комбинации с большой длиной, включающие разные типы символов.