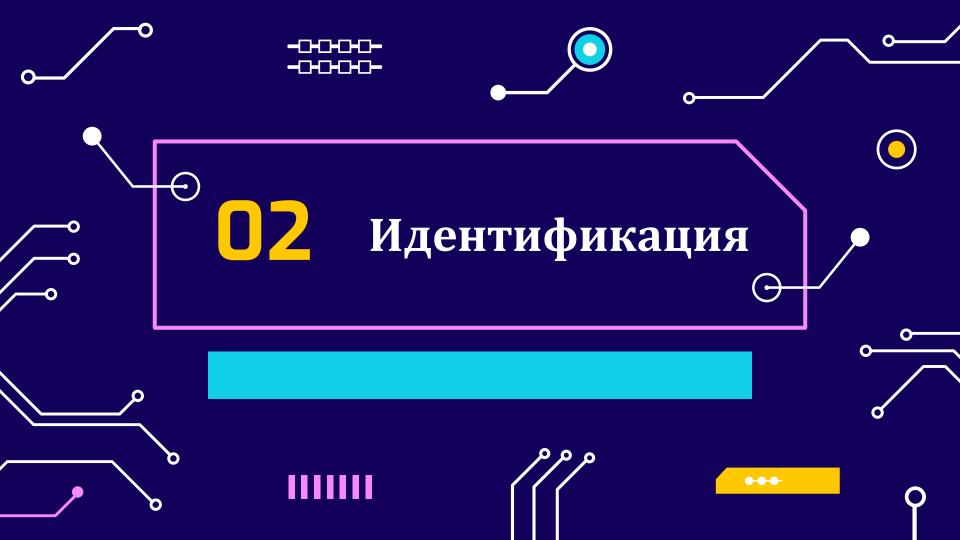




Определения

- <u>Идентификация</u> процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе.
- **Аутентификация** процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.
- <u>Авторизация</u> предоставление определенному лицу или группе лиц прав на выполнение определенных действий.



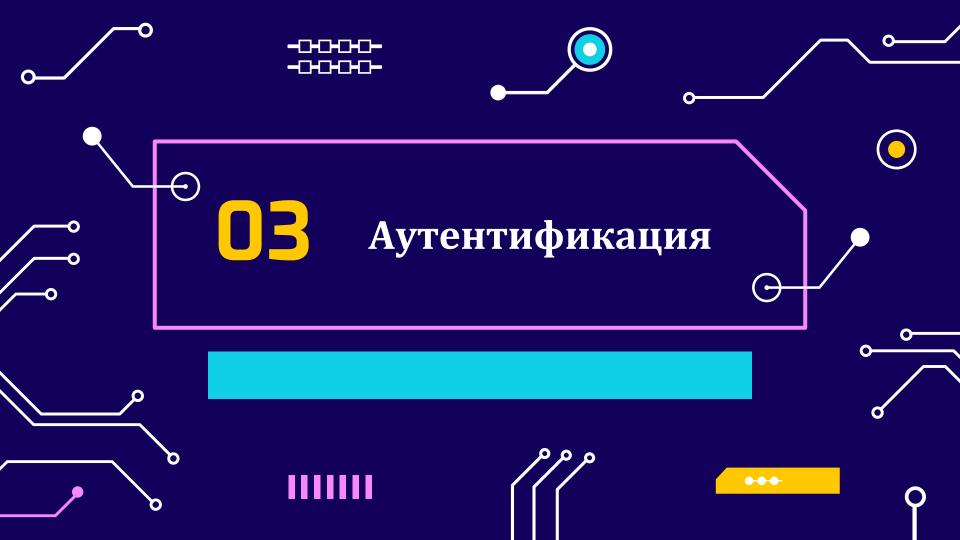
Идентификация

<u>Идентификация</u> – это первый шаг, с которого начинается взаимодействие пользователя с системой. На этом этапе система пытается установить, *кто* пытается получить доступ. Идентификация отвечает на вопрос: «**Кто вы?**». Она не проверяет подлинность личности, а лишь фиксирует её. Обычно идентификация происходит через логин, имя пользователя, номер телефона или другие уникальные идентификаторы, которые пользователь предоставляет.

Пример: на веб-сайте или в приложении пользователь вводит свое имя или логин в форму. Система получает это значение и начинает процесс поиска учетной записи, соответствующей предоставленному логину.

Основные принципы идентификации:

- 1. Уникальность: каждый идентификатор должен быть уникальным для пользователя;
- **2. Удобство использования**: пользователи должны иметь возможность легко идентифицировать себя, например, вводя свой логин или номер телефона;
- **3. Защита данных**: система должна хранить и обрабатывать идентификаторы безопасно.



Аутентификация

Аутентификация – это второй шаг, который проверяет, действительно ли пользователь является тем, за кого себя выдает. Она отвечает на вопрос: **«Докажите, что это действительно вы»**. Для этого пользователю необходимо предоставить доказательства своей подлинности, чаще всего это пароль, который хранится в системе в зашифрованном виде.

Существует несколько методов аутентификации:

- **1. По знанию** пароли и PIN-коды, то есть информация, известная только пользователю.
- **2. По владению** смарт-карты, ключи или одноразовые коды, отправляемые по SMS или генерируемые специальными приложениями.
- **3. По биометрическим данным** отпечатки пальцев, распознавание лиц, сканирование радужки глаза и другие уникальные физические характеристики.
- **4. Многофакторная аутентификация (MFA)** комбинация из нескольких методов, например, сочетание пароля и одноразового кода. Это повышает надежность защиты.

Пример: после ввода логина пользователь вводит пароль. Система сверяет введенный пароль с тем, что хранится в базе данных, и, если он совпадает, подтверждает подлинность пользователя.



Авторизация

Авторизация – это третий шаг, который обычно начинается после успешной аутентификации, но может происходить и без нее (например, в случае общедоступного Google Документа пользователи, у которых есть ссылка, могут просматривать документ без аутентификации). Она определяет, какие действия пользователь имеет право выполнять в системе, и отвечает на вопрос: **«Что вам разрешено делать?»**. Авторизация устанавливает права доступа пользователя к определенным данным и ресурсам на основании его роли, настроек или статуса в системе.

Пример: после успешной идентификации и аутентификации пользователю может быть разрешено видеть свой личный профиль, но запрещено редактировать данные других пользователей или получать доступ к административной панели.

Авторизация может быть реализована через несколько подходов:

- **1. Ролевая модель (RBAC Role-Based Access Control)** права пользователя определяются на основе его роли, например, "администратор", "пользователь", "гость".
- **2. Контроль на основе атрибутов (ABAC Attribute-Based Access Control**) доступ определяется на основе атрибутов пользователя (возраст, отдел, уровень доступа) и характеристик ресурсов.
- **3. Дискреционный контроль (DAC Discretionary Access Control)** право доступа может быть передано пользователем другим участникам системы.



Взаимосвязь и отличия

- Идентификация <u>определяет личность</u> пользователя, но <u>не проверяет подлинность</u>.
- **Аутентификация** *проверяет подлинность* личности, то есть доказывает, что человек *действительно является* тем, за кого себя выдает.
- **Авторизация** определяет, *что именно можно делаты* конкретному пользователю после успешного прохождения аутентификации.