48. Авторизация. Часть 2

Цель:

Познакомиться со следующими особенностями авторизации:

- структура JWT

План занятия:

- структура JWT
    - header
    - payload
    - signature

Конспект:

JSON Web Token (**JWT**) — это открытый стандарт (RFC 7519) для создания токенов доступа, основанный на формате JSON. Как правило, используется для передачи данных для аутентификации в клиент-серверных приложениях. Токены создаются сервером, подписываются секретным ключом и передаются клиенту, который в дальнейшем использует данный токен для подтверждения своей личности.

Структура JWT

- header
- payload
- signature

Header: Хедер *JWT* содержит информацию о том, как должна вычисляться *JWT* подпись.

header = { "alg": "HS256", "typ": "JWT"}

- поле alg, которое определяет алгоритм хеширования. Он будет использоваться при создании подписи. HS256. Это единственное обязательное поле

Необязательные ключи:

- **typ:** тип токена (*type*).
- **cty:** тип содержимого (*content type*)

Payload: это полезные данные, которые хранятся внутри *JWT*. Эти данные также называют *JWT-claims* (заявки). Это тоже объект. Существует список стандартных ***заявок*** для *JWT* payload — вот некоторые из них:

- *iss* (issuer) — определяет приложение, из которого отправляется токен.
- *sub* (subject) — определяет тему токена.
- *exp* (expiration time) — время жизни токена.

Signature: вычисляется на основании headers и payload и зависит от выбранного алгоритма (в случае использования неподписанного JWT может быть опущен). Токены могут быть перекодированы в компактное представление (JWS/JWE Compact Serialization): к заголовку и полезной нагрузке применяется алгоритм кодирования Base64-URL, после чего добавляется подпись и все три элемента разделяются точками («.»).