Система забезпечення інформаційної безпеки обліково-бухгалтерського додатку

Ст. групи ТІ-51с Семененко А.С.

Актуальність теми

- Захист інформації в сучасних комп’ютерних інформаційних системах (ІС) є пріоритетним завданням. Викрадення конфіденційної інформації, знищення даних, викривлення інформації, виведення з ладу комп’ютерних систем (КС) – далеко не повний перелік усіх ризиків, що виникають у процесі експлуатації та використання сучасних ІС.

Мета роботи

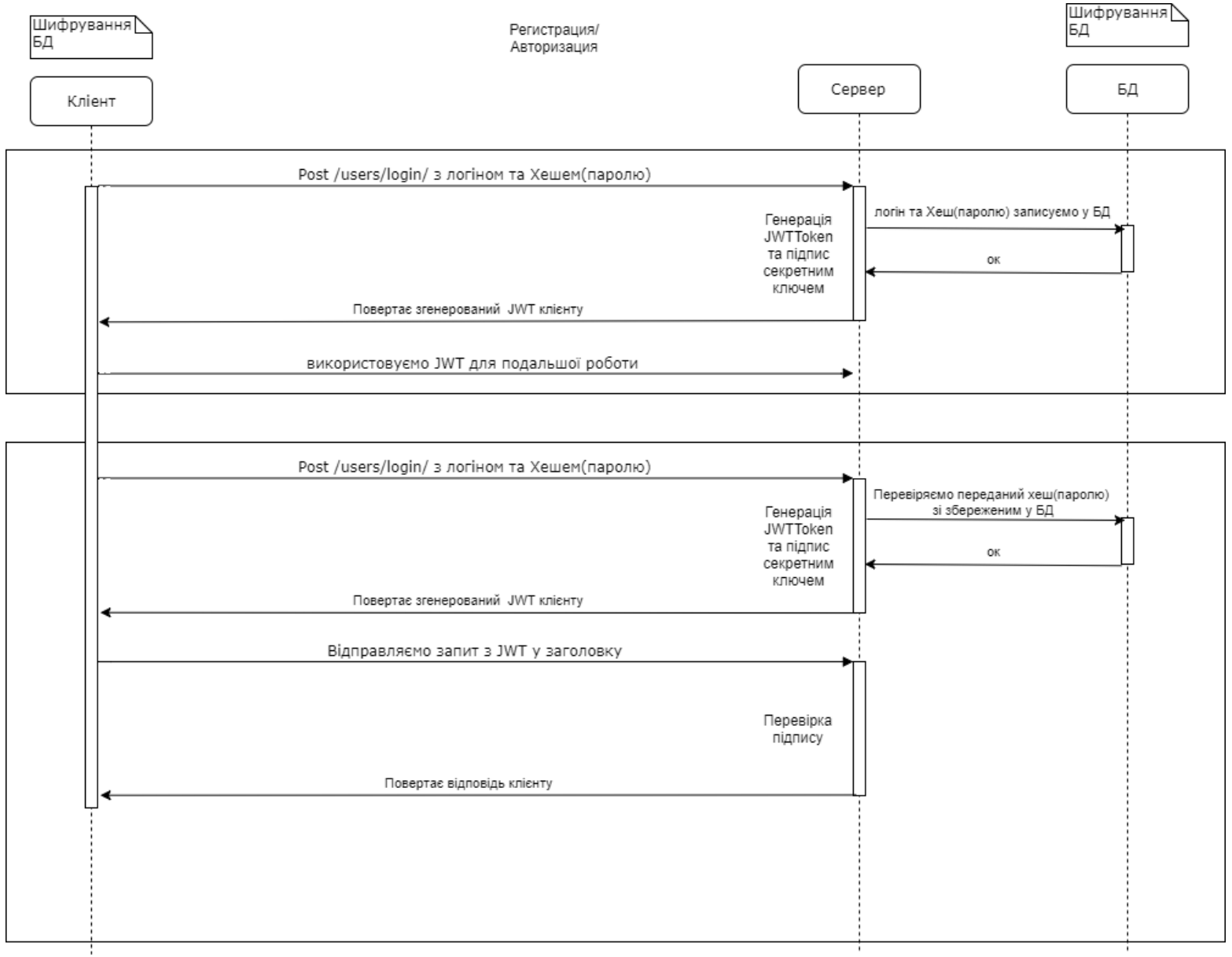
Забезпечити інформаційну безпеку обліково-бухгалтерського додатку:

- Виокремити можливі загрози втрати або порушення цілостності інформації.
- Знайти можливі варіанти вирішення даних проблем.
- Впровадити засоби забезпечення захисту інформації.

Огляд завдань забезпечення інформаційної безпеки:

- Забезпечення обмеження доступу до інформаційних ресурсів(авторизація)
- Забезпечення захисту каналів зв’язку між клієнтом та сервером.
- Забезпечення захисту збережених даних у БД.

Авторизація



JWT(Json web token)

JWT — це підписаний об'єкт JSON, містить що-небудь корисне (наприклад, id користувача, його права/ролі), закодований у base64 і складається з трьох частин розділений точками:

Header, Payload, Signature

і зазвичай виглядає так

aaaaaaa.bbbbbb.cccccc

Більш детально:

- Header — містить тип токена і назву хешуючого алгоритму:

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

- Payload — об'єкт містить будь-які потрібні нам дані:

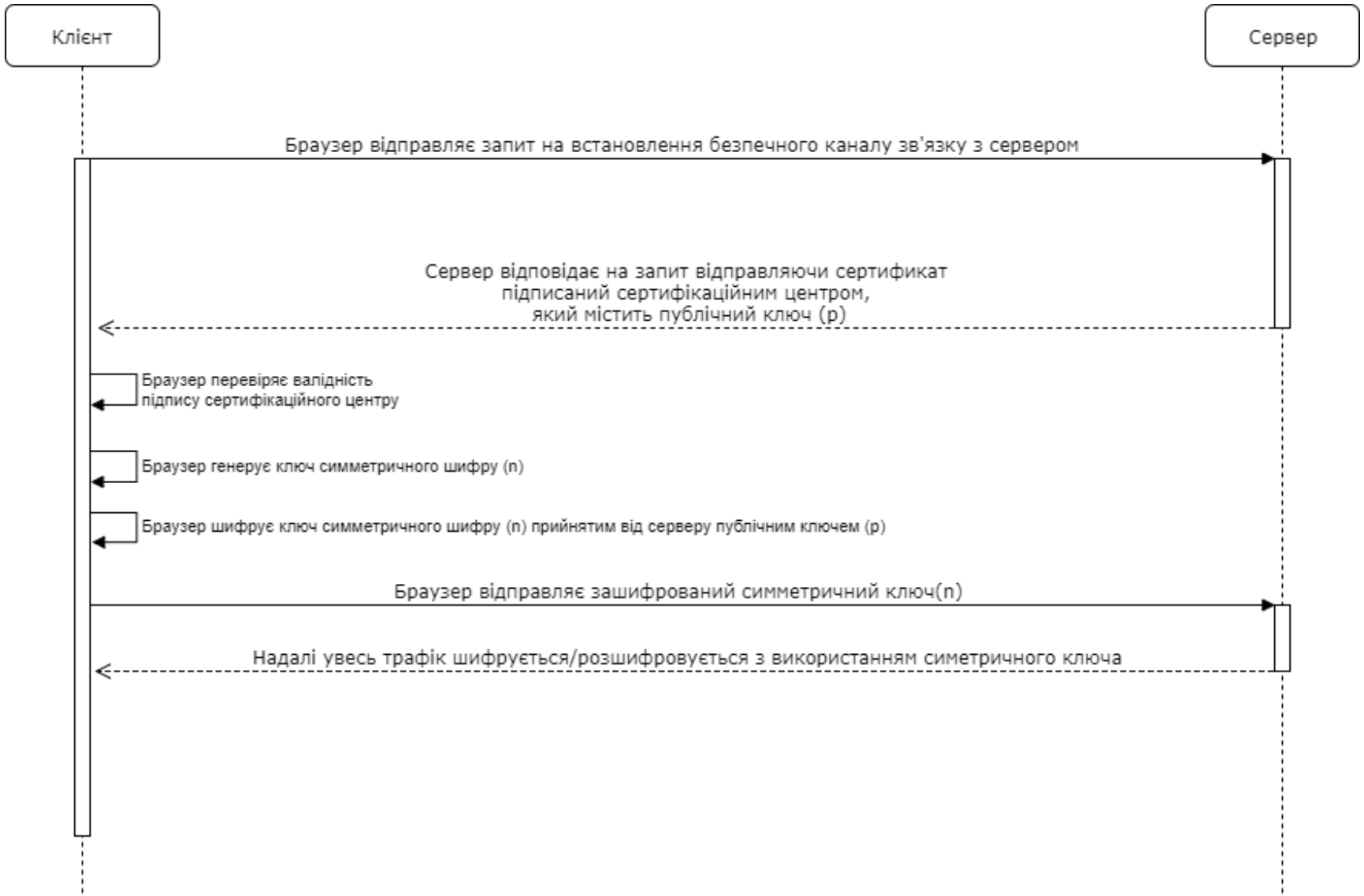
{ "email": "temp@jwt.ru", "user_id": "57dc51a3389b30fed1b13f91" }

- Signature — необхидна для перевірки відправника: що він той, за кого себе видає, а також перевіряє що повідомлення не було змінено.

SSL/https

- SSL (англ. Secure Sockets Layer — рівень захищених сокетів) — криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером.

SSL/https принцип роботи



Перевірка Паролей

- Забезпечення цілісності збереженої конфіденційної інформації у БД.

email	password
test@example.com	hash("StrongPassword123"+salt)