Міністерство освіти і науки України
Чернівецький національний університет імені Юрія Федьковича

Інститут фізико-технічних та комп'ютерних наук
Кафедра програмного забезпечення комп'ютерних систем

ЗВІТ

про виконання лабораторної роботи №8
з курсу "Безпека програм та даних"

Тема: Підсистема реєстрації

Виконали: Неголюк О.О., Ратушняк М.А.
Перевірив: Остапов С.Е.

Чернівці – 2025

ЗМІСТ

ПРОТОКОЛ РОБОТИ

1.1. Представлення записів аудиту у базі даних

Для зберігання записів аудиту створено таблицю `action_logs` з наступними полями:

- `id` — унікальний ідентифікатор запису (автоінкремент);
- `timestamp` — мітка часу виконання дії (встановлюється автоматично при вставці);
- `action` — назва дії (до 60 символів), що відповідає імені функції-обробника запиту;
- `is_success` — логічне поле, що вказує на успішність виконання дії;
- `reason` — текстове поле з деталями виключення (якщо дія не була успішною);
- `user_id` — ідентифікатор користувача, який виконав дію.

Для забезпечення цілісності журналу аудиту створено тригери, що блокують операції UPDATE та DELETE на таблиці `action_logs`. Таким чином, журнал є append-only структурою — можливий лише запис нових логів та їх читання.

1.2. Реалізація аудиту доступу до об’єктів системи

Було реалізовано підсистему реєстрації (аудиту), що у вигляді декоратору `@audit`, використовує ім’я функції у якості `action` поля запису аудиту, а також опрацьовує можливі виключення, наприклад помилки авторизації чи невдала автентифікація, встановлюючи поле `is_success`. Додаткова інформація про

виключення (поле `detail` у екземпляра класу `HTTPException`) зберігається у полі `reason` запису аудиту.

Для веб-ресурсів, що потребують автентифікованого суб'єкта, декоратор використовує ідентифікатор користувача (за наявності) і записує у поле `user_id`.

Приклад використання:

```
@router.get("/users/{id}")
@audit()
@authorize(AccessLevel.CONFIDENTIAL)
async def read_user(
    id: Annotated[int, Path()], db: PostgresRunnerDep, subject:
CurrentSubjectDep
) -> UserResponse:
    return auth_service.get_user_by_id(id, db=db)
```

Для отримання записів аудиту з серверної частини реалізовано GET-ендпоінт `/audit/`, доступний лише для користувачів з рівнем доступу CONFIDENTIAL. Ендпоінт приймає два обов'язкових параметри запиту: `start` та `end` — ISO-формат дати, що визначають діапазон часу для вибірки записів.

Endpoint повертає список об'єктів `ActionLog`, кожен з яких містить: часову мітку, назву дії, статус виконання та причину помилки (якщо така була).

На рисунку зображено процес обробки запиту користувача у вигляді data flow діаграми:

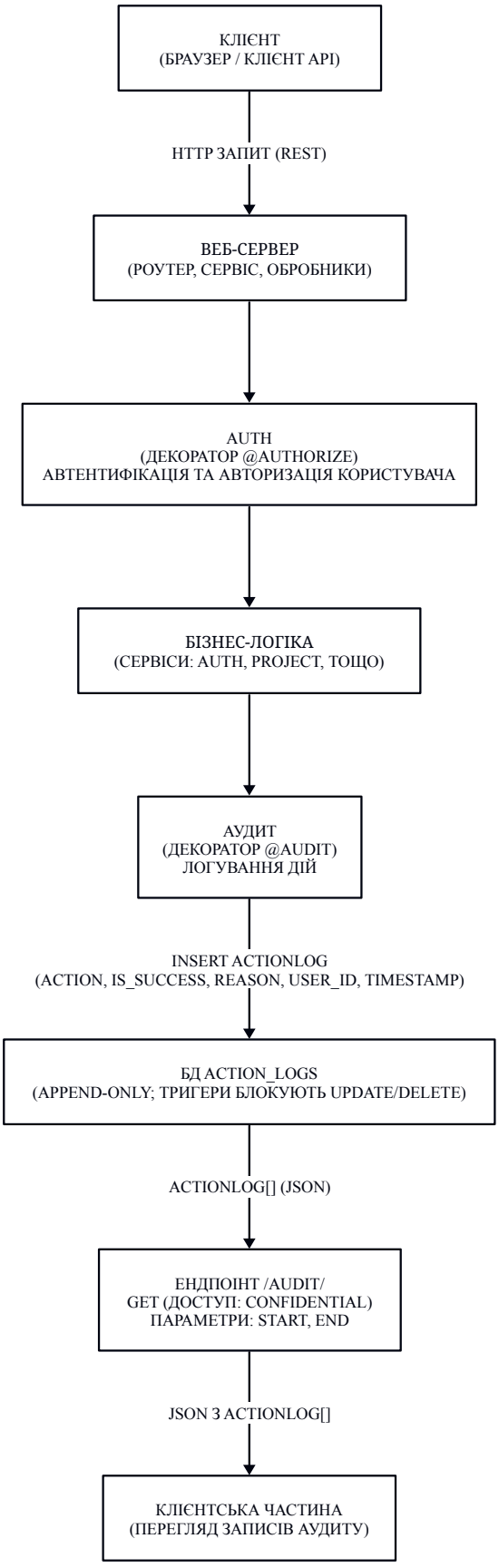

Рисунок 1.1 – Data flow діаграма підсистеми реєстрації

1.3. Відображення записів аудиту на клієнтській частині

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere.

ВІДПОВІДІ НА КОНТРОЛЬНІ ЗАПИТАННЯ

1. Спробуйте ідентифікувати ознаки тих чи інших порушень безпеки, спираючись на отриманий вами журнал реєстрації. Охарактеризуйте труднощі, що виникають при рішенні цієї задачі.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere.

2. Проаналізуйте взаємодію підсистеми реєстрації з підсистемами автентифікації та управління доступом в розробленій системі.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere.

3. Оцініть рівень реєстрації в розробленій системі згідно НД ТЗІ 2.5-004- 99. Що можна зробити, щоб його підвищити?

Дивись розділ 9.1. Реєстрація

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere.

ВИСНОВКИ

У ході виконання лабораторної роботи було реалізовано підсистему аудиту для серверної частини HearMyPaper. Створено міграцію бази даних для таблиці `action_logs` з тригерами, що забезпечують незмінність записів (append-only). Реалізовано модуль аудиту з репозиторієм, сервісом та роутером для керування записами. Розроблено декоратор `@audit()`, який автоматично логує всі запити до серверу, фіксуючи їх статус та деталі помилок. Декоратор застосовано до всіх ендпоінтів системи (auth, project, audit). Створено GET-ендпоінт для отримання записів аудиту в заданому діапазоні часу з рівнем доступу CONFIDENTIAL.