2. Resiliency model

2.2 RMA Workbook (модель відмов)

ID	Component / Dependency Interactions	Failure Short Name	Failure Description	Response	Effects	Portion Affected	Detection	Resolution	Likelihood	Risk
1.1	Browser → API	Invalid Request	Невірний формат запиту або відсутні параметри	Відхилити запит	Запит не обробляється	Один користувач	Валідація на стороні API	Повідомлення про помилку, повторити запит	Medium	Low
1.2	Browser → API	Connection Loss	Втрата з'єднання між браузером і сервером	Повторити запит	Запит не доставлений	Один користувач	Таймаут запиту	Повторна спроба або повідомлення користувачу	Medium	Medium
1.3	Browser → API	Authentication Failure	Неавторизований доступ або завершена сесія	Перенаправлення на логін	Відмова в доступі	Один користувач	Статус код 401 / 403	Авторизація заново	Medium	Medium

ID	Component / Dependency Interactions	Failure Short Name	Failure Description	Response	Effects	Portion Affected	Detection	Resolution	Likelihood	Risk
2.1	API → Бізнес-логіка	Logic Error	API передає некоректні дані до логіки	Лог помилок	Некоректна поведінка	Багато користувачів	Помилки на backend	Виправлення коду	Medium	High

2.2	API → Бізнес-логіка	Request Overload	Надмірна кількість запитів перевантажує логіку	Обмеження запитів	Затримки в обробці	Усі користувачі	Моніторинг навантаження	Оптимізація або кешування	High	High
2.3	API → Бізнес-логіка	Missing Data	Відсутні потрібні параметри або дані	Повернення помилки	Неможливість виконання операції	Один або кілька користувачів	Валідація в логіці	Повідомлення про помилку	Medium	Medium

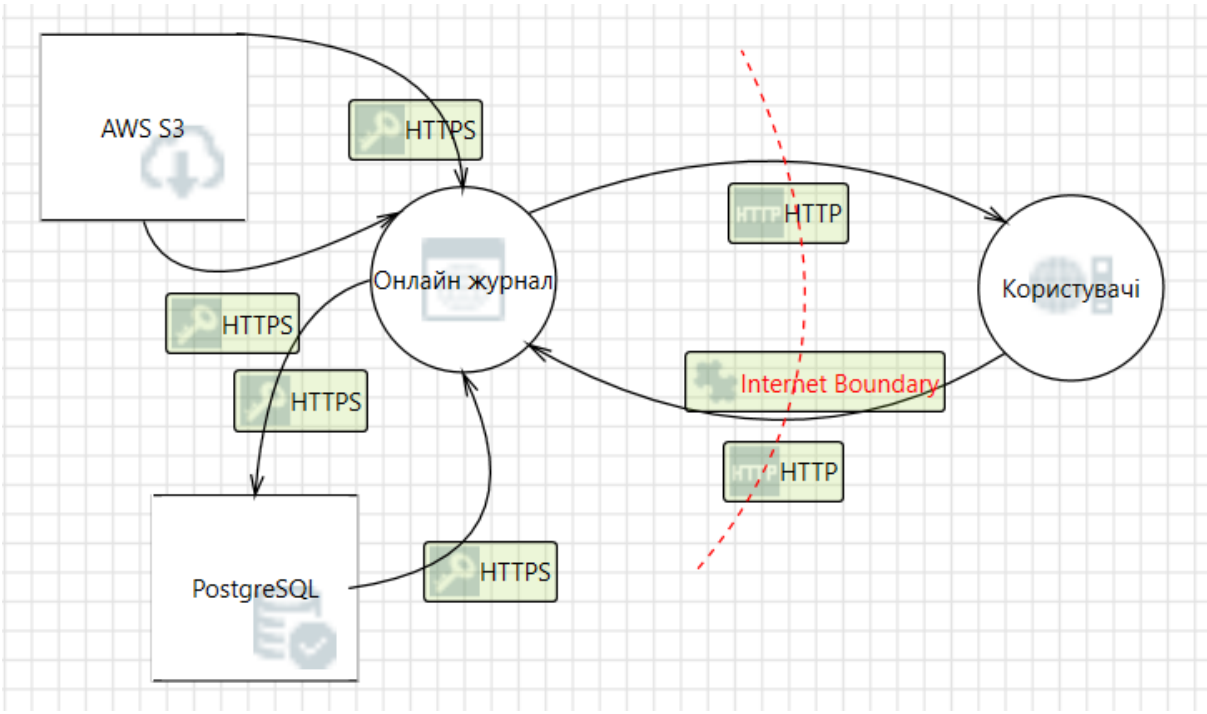
ID	Component / Dependency Interactions	Failure Short Name	Failure Description	Response	Effects	Portion Affected	Detection	Resolution	Likelihood	Risk
3.1	Бізнес-логіка → Шар доступу до даних	SQL Error	Помилка у синтаксисі або логіці SQL-запиту	Повернення помилки	Дані не зчитано/змінено	Один або більше користувачів	Лог запитів	Виправлення SQL	Medium	High
3.2	Бізнес-логіка → Шар доступу до даних	No Data Found	Відсутні потрібні записи в БД	Повернення пустого результату	Немає результату	Один або кілька користувачів	Перевірка на null	Додати дані в БД	Low	Medium
3.3	Бізнес-логіка → Шар доступу до даних	DB Access Error	Неможливо підключитися до БД	Повідомлення про помилку	Збої в роботі системи	Усі користувачі	Моніторинг з'єднання	Перезапуск, перевірка налаштувань	Medium	High

ID	Component / Dependency Interactions	Failure Short Name	Failure Description	Response	Effects	Portion Affected	Detection	Resolution	Likelihood	Risk
4.1	Шар доступу до даних → PostgreSQL DB	Timeout	Затримка або немає відповіді від БД	Повторити запит	Затримка в обробці	Усі користувачі	Таймаут запитів	Оптимізація або індексація	Medium	Medium
4.2	Шар доступу до даних → PostgreSQL DB	Data Corruption	Неправильне оновлення або запис	Повідомлення про помилку	Некоректні дані	Один або більше користувачів	Перевірка логів	Відновлення з резервної копії	Low	High
4.3	Шар доступу до даних → PostgreSQL DB	DB Connection Loss	Втрата з'єднання з БД	Повідомлення про помилку	Немає доступу до даних	Усі користувачі	Моніторинг, лог	Перезапуск, перевірка мережі	Medium	High

ID	Component / Dependency Interactions	Failure Short Name	Failure Description	Response	Effects	Portion Affected	Detection	Resolution	Likelihood	Risk
5.1	Mailtrap SMTP → Email	Invalid Email	Неправильна адреса електронної пошти	Не доставлено	Користувач не отримує лист	Один користувач	SMTP відповідь	Повідомити користувача	Medium	Low
5.2	Mailtrap SMTP → Email	SMTP Server Error	Помилки сервера під час надсилання	Повторити пізніше	Затримка або втрата повідомлення	Один або більше користувачів	SMTP лог	Налагодження сервера	Low	Medium
5.3	Mailtrap SMTP → Email	Spam Filtered	Повідомлення потрапляє до спаму	Повідомити користувача	Повідомлення не побачене	Один користувач	Логи пошти	Зміна формулювання листа	High	Low

3. Security model

3.1 Основні флови та моделювання загроз (Threat Model)



Потоки даних у моделі (Flows):

1. **Користувачі (студент/викладач/адміністратор) → Frontend**
    - HTTP(S)-запити (автентифікація, перегляд/редагування розкладу)
2. **Frontend → Backend API**
    - REST/GraphQL запити на обробку розкладу, повідомлень, нотаток.
3. **Backend → Database (PostgreSQL)**
    - Зберігання/отримання даних: заняття, групи, користувачі, аудиторії.
4. **Backend → AWS S3**
    - Завантаження/отримання доданих файлів або допоміжних матеріалів.

3.2 Mitigation Plan

№	Загроза	Категорія	Опис	Ризик	Mitigation Plan
1	**Data Flow Sniffing**	Information Disclosure	Дані, що передаються через HTTP, можуть бути перехоплені зловмисником.	Високий	Використовуйте HTTPS (TLS 1.2+), зашифровані канали, захищені сесії.
2	**Potential Process Crash or Stop for Користувачі**	Denial Of Service	Користувачі виходять з ладу, зупиняються, зупиняються або працюють повільно; у всіх випадках порушуючи метрику доступності	Високий	Моніторинг стану, резервні процеси, обробка помилок.
3	**Data Flow HTTP Is Potentially Interrupted**	Denial Of Service	Переривання потоку даних через довірену межу.	Високий	Виявлення DoS-атак, контроль трафіку, моніторинг пакетів.
4	**Користувачі May be Subject to Elevation of Privilege Using Remote Code Execution**	Elevation Of Privilege	Онлайн журнал може виконувати код від імені користувача.	Високий	Обмеження прав, sandboxing, перевірка інтерфейсів виконання.
5	**Elevation by Changing the Execution Flow in Користувачі**	Elevation Of Privilege	Зловмисник змінює логіку виконання через введені дані.	Високий	Статичний аналіз коду, валідація введених даних, контроль потоків.
6	**Cross Site Scripting (XSS)**	Tampering	Онлайн журнал вразливий до XSS, бо не фільтрує untrusted input.	Високий	Валідація вводу, escaping HTML, CSP-політики, бібліотеки санітизації.
7	**Spoofing of Source Data Store SQL Database**	Spoofing	PostgreSQL може бути підроблений і надати неправильні дані.	Високий	Аутентифікація джерела даних, перевірка підключень.
8	**Weak Access Control for a Resource (AWS S3)**	Information Disclosure	Невірні права дозволяють читати конфіденційні дані.	Високий	Мінімізація прав доступу, ACL, IAM-політики.

9	**Elevation Using Impersonation**	Elevation Of Privilege	Онлайн журнал імітує контекст користувача для привілеїв.	Високий	Використання перевірки ролей (RBAC), сесійна ізоляція.
10	**Persistent Cross Site Scripting (AWS S3)**	Tampering	Дані з S3 не санітизуються – XSS атака можлива.	Високий	Валідація файлів перед виводом, використання CDN з фільтрами.

5. Analytics model

5.1 Таблиця основних функціональних метрик

№	Назва метрики	Опис	Одиниця виміру	Джерело даних	Цільове значення
1	**Кількість створених розкладів**	Скільки разів адміністратор згенерував новий або оновив існуючий розклад	розкладів/місяць	Лог сервісу редагування розкладу	≥ 4 (щотижневі зміни)
2	**Кількість унікальних користувачів, що переглянули розклад**	Кількість студентів або викладачів, які відкрили розклад	користувачів/тиждень	Frontend трекінг або API лог	80–100% активних користувачів
3	**Частка редагованих занять**	Частка занять, які були змінені після початкового створення розкладу	% від усіх занять	Лог змін у розкладі	≤ 15%
4	**Кількість згенерованих звітів адміністратором**	Кількість використань функції створення звітів (PDF, Excel тощо)	звітів/місяць	API лог генерації	≥ 2
5	**Частка занять із примітками від викладачів**	Скільки занять мають прикріплені текстові замітки	% від усіх занять	База даних занять	≥ 10%
6	**Кількість сповіщень про зміни в розкладі**	Скільки повідомлень про зміни було надіслано (через email чи інтерфейс)	повідомлень/місяць	Сервіс сповіщень	Залежить від змін
7	**Частка використаних фільтрів при перегляді розкладу**	Скільки запитів до розкладу містили фільтри (за викладачем, групою тощо)	% від переглядів	Frontend/API лог	≥ 30%

8	**Середня кількість редагувань розкладу одним адміністратором**	Середня кількість змін до розкладу, зроблених одним користувачем із роллю "адміністратор"	змін/тиждень	Лог подій	Залежить від політики закладу
9	**Частка завершених сесій створення розкладу**	Кількість розпочатих і збережених сесій редагування, що завершилися успішно	%	Серверна аналітика	≥ 95%
10	**Кількість унікальних груп, для яких створено розклад**	Відображає покриття — чи всі групи охоплені актуальним розкладом	груп/навчальний період	База розкладів	100% зареєстрованих груп