

Міністерство освіти і науки України
Національний технічний університет України «Київський політехнічний
інститут імені Ігоря Сікорського»
Факультет інформатики та обчислювальної техніки
Кафедра інформаційних систем та технологій

ЗВІТ

про переддипломну _____ практику
(назва практики)

на ННЦ ІКТ «Неткрекер» _____
(назва підприємства, місто)


з « 01 » _____ 09 _____ 2024 р. по « 26 » _____ 10 _____ 2024 р.

Керівники практики:
від підприємства

Писаренко А.В. _____
(прізвище, ініціали) (підпис)

(дата)

Студент 6 курсу, групи ІА-31мп

Гулящий І.С. _____ 
(прізвище, ініціали) (підпис)

(дата)

від інституту

Хмелюк М. С. _____
(прізвище, ініціали) (підпис)

(дата)

Захищено _____
(дата)

з оцінкою _____

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ, СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ	3
ВСТУП.....	4
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ.....	6
1.1 Змістовний опис і аналіз предметної області.....	6
1.2 Аналіз існуючих рішень.....	6
1.2.1 Платформа LiqPay.....	6
1.2.2 Платформа WayForPay	8
1.2.3 Платформа UAPAY	9
1.3 Аналіз різновидів платежів.....	10
1.3.1 Різновиди e-commerce платежів	11
1.4 Аналіз підтвердження платежу	11
1.5 Аналіз PCI DSS сертифікації	13
2 ВИБІР ТЕХНОЛОГІЙ ТА ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ.....	16
2.1 Архітектура серверної частини	16
2.2 Бази даних	17
2.2.1 Проектування структури бази даних	17
2.3 Вимоги згідно PCI DSS сертифікації.....	19
2.3.1 Вимоги до способу зберігання чутливої інформації	19
2.3.2 Вимоги до адміністрування	20
2.3.3 Вимоги до інтеграції з еквайринговою платформою	20
2.4 Вибір технологій для роботи зі штучним інтелектом	21
ВИСНОВКИ	22
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	23

ПЕРЕЛІК ТЕРМІНІВ, СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

PCI DSS – Payment Card Industry Data Security Standard;

БД – База даних;

P2P – Person to Person;

3DS – 3-D Secure;

API – Application Programming Interface;

CVV – Card Verification Value.

ВСТУП

У сучасному бізнес-середовищі електронна комерція стає невід'ємною складовою діяльності компаній різного масштабу. З розвитком інформаційних систем і поширенням інтернету все більше підприємств переходять до онлайн-продажів, задовольняючи попит споживачів на зручні й швидкі платежі. У цьому контексті особливо важливими стають технології, що дозволяють забезпечити безпечний і ефективний процес обробки фінансових транзакцій. Онлайн-платформам потрібна сертифікація та проходження аудиту для проведення платежів, а також інтеграція з банками-еквайрами для виконання фінансових операцій.

Еквайрінгові платформи забезпечують обробку транзакцій і інтеграцію з банками. Вони значно спрощують процес роботи з платежами, допомагаючи бізнесу різного масштабу отримувати оплату від клієнтів у зручний та безпечний спосіб. Окрім технічної інтеграції, еквайрінгові платформи сприяють оптимізації бухгалтерської звітності, оскільки беруть на себе ведення фінансової документації, що полегшує процес оподаткування та контроль доходів.

Малий бізнес також отримує значні переваги від використання таких платформ. Підприємства, де працює лише одна або кілька осіб, можуть легко інтегрувати еквайрінгові рішення в свою діяльність, відкривши особистий рахунок у банку та підписавши договір з еквайрінговою платформою. Це забезпечує легалізацію доходів і спрощує фінансову звітність. Крім того, еквайрінгові платформи дозволяють вибирати найвигідніші умови серед банків-еквайрів, залежно від обсягу транзакцій, кількості платежів або підтримки платіжних систем, таких як Google Pay і Apple Pay.

Одним із основних завдань сучасних еквайрінгових платформ є забезпечення безпеки фінансових операцій. Технології штучного інтелекту відіграють усе більшу роль у цьому процесі, дозволяючи відслідковувати підозрілу активність, запобігати шахрайству та контролювати коректність

транзакцій. Штучний інтелект здатен працювати в режимі реального часу, забезпечуючи вищий рівень надійності й ефективності еквайрінгових рішень.

Еквайрингова платформа допоможе підприємствам будь-якого масштабу безпечно й ефективно працювати в електронній комерції, що стане важливим кроком до підвищення їхньої конкурентоспроможності та зручності для клієнтів.

Тож в ході розроблення будуть вирішуватись наступні задачі:

- створення єдиної централізованої платформи для різних варіантів використання;
- створення платіжної сторінки, яку клієнти зможуть використовувати в якості отримання оплати за послуги, які останні надають;
- створення фрейму, який можна інтегрувати в існуючі веб-рішення клієнтів;
- створення веб-інтерфейсу для надання послуг еквайрінговою платформою клієнтам, що допоможе вести бухгалтерію, а також контролювати доходи, витрати на комісію, а також в ручному форматі використовувати систему, для створення посилань на оплату послуг.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Змістовний опис і аналіз предметної області

Еквайрингова платформа є важливим компонентом сучасної фінансової інфраструктури, забезпечуючи обробку платежів для торговців і підприємств шляхом інтеграції з платіжними системами та банками. Еквайринг стосується процесу прийняття та обробки безготівкових платежів, що здійснюються за допомогою платіжних карт. Еквайрингова платформа виступає посередником між торговцями, які приймають оплату картами, та банками-еквайрами, які здійснюють обробку фінансових операцій.

Враховуючи, що кількість бізнесів зростає, а Україна все більше і більше цифровізується, з'являються нові схеми обходу системи оподаткування, незаконного збагачення, відмивання грошей, цифрових крадіжок. Еквайрингова платформа є невід'ємною частиною кожного бізнесу, який пов'язаний з продажами, тож ці схеми частково стосуються і цієї ніші. Розглянемо найпопулярніші еквайрингові платформи, задля аналізу їх системи безпеки. Також виконаний огляд функціоналу і можливостей цих систем, щоб зрозуміти переваги та недоліки в конкурентному середовищі.

1.2 Аналіз існуючих рішень

Оскільки темою дослідження є еквайрингові платформи, то доцільно буде оцінювати якість систем, які безпосередньо є конкурентами. Було розглянуто три подібних сервіси, оскільки переважна більшість мають однаковий функціонал.

1.2.1 Платформа LiqPay

LiqPay – це українська платіжна система, заснована ПриватБанком, яка дозволяє підприємствам і приватним особам приймати онлайн-платежі. Платформа підтримує широкий спектр платіжних інструментів, таких як

банківські картки, мобільні платежі, перекази через соціальні мережі та інші методи, що робить її зручною для різних типів користувачів. LiqPay є популярною серед малого та середнього бізнесу, особливо в Україні, завдяки своїй простоті інтеграції та доступності.

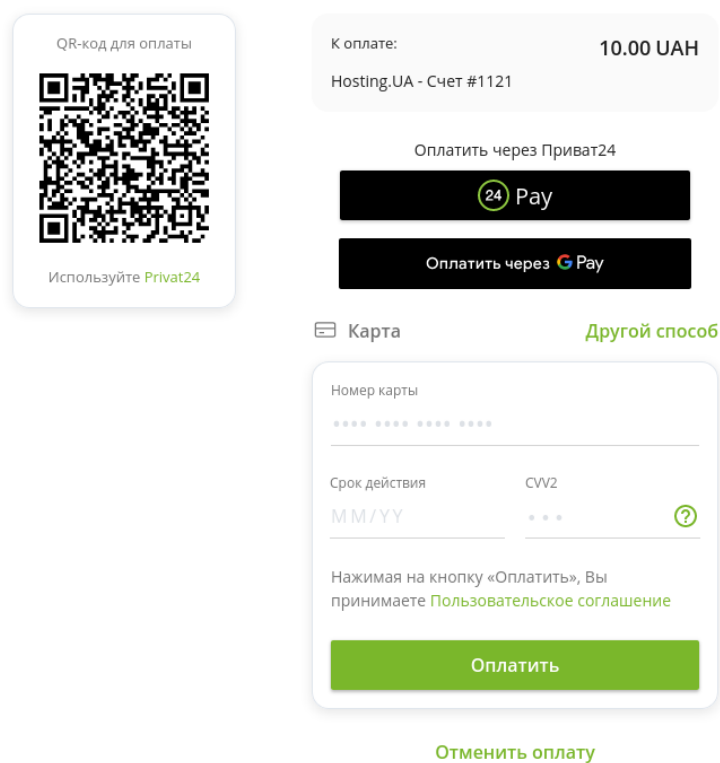


Рисунок 1.1 – Платіжна сторінка LiqPay [1]

Її можливості:

- перекази з карти на рахунок;
- перекази з рахунку на карту;
- фрейм для токенизації карти. Це допоможе для кастомізації платіжної сторінки і повної інтеграції з LiqPay;
- оплата за допомогою мобільного додатку Privat24. Але ця можливість є лише у клієнтів цього банку.

Недоліки:

- неможливість вибирати кращі тарифи для користування, оскільки інтеграція відбувається виключно з банком-еквайром – «ПриватБанк»;

- особливість оплати за допомогою додатку Privat24, є перевагою та недоліком одночасно, оскільки не всі платники є клієнтами цього банку;
- немає можливості P2P переказу.

Також не було знайдено жодної згадки використання штучного інтелекту, або інших механізмів, для покращення конверсії чи то збільшення безпеки клієнтів.

1.2.2 Платформа WayForPay

WayForPay – українська еквайрингова платформа, яка не має жодного банку, як основного екваєру. Послуги, які надаються:

- P2P перекази;
- створення інвойсу, рахунку на оплату;
- онлайн кредитування;
- антифрод API;
- переказ коштів з рахунку на рахунок.

В цій платформі є антифрод API, який надається клієнтам, але це означає, що він опціональний. Тобто кожен, хто не хоче витратити час та ресурси на повну інтеграцію – залишиться в потенційній небезпеці.

Недоліки:

- немає власної кастомізації платіжної сторінки. Тобто клієнти зобов'язані користуватись тією сторінкою, яку надає платформа;
- немає можливості оплати GooglePay чи ApplePay (рисунок 1.2).

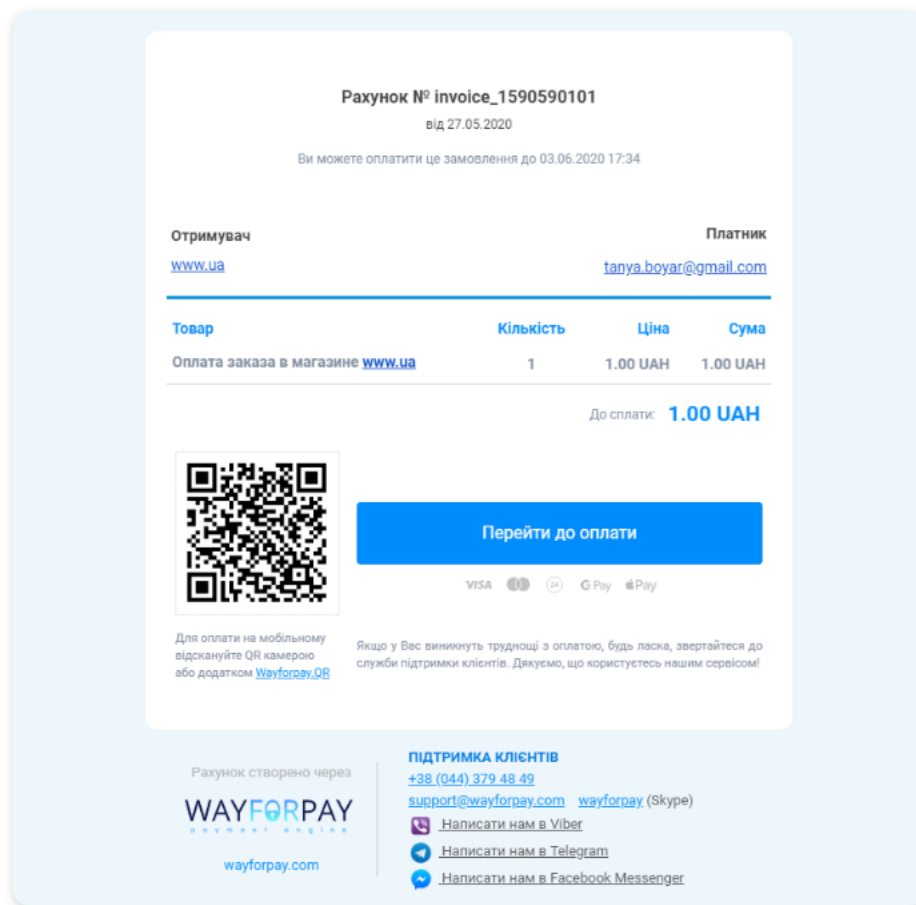


Рисунок 1.2 – Платіжна сторінка WayForPay [2]

В відкритій документації не було згадки використання штучного інтелекту.

Загалом WayForPay надає більше різних способів використань аніж LiqPay, але також має і недоліки.

1.2.3 Платформа UAPAY

UAPAY – українська еквайрингова платформа, яка є одним із партнерів OLX, але також має відкритий API для проведення транзакцій.

Функціонал, який надає дана платформа:

- оплата за інвойсом, на платіжній сторінці (рисунок 1.3);
- картковий фрейм, для повної інтеграції;

— панель адміністрування мерчантом, де можна створити посилання на оплату на платіжну сторінку.

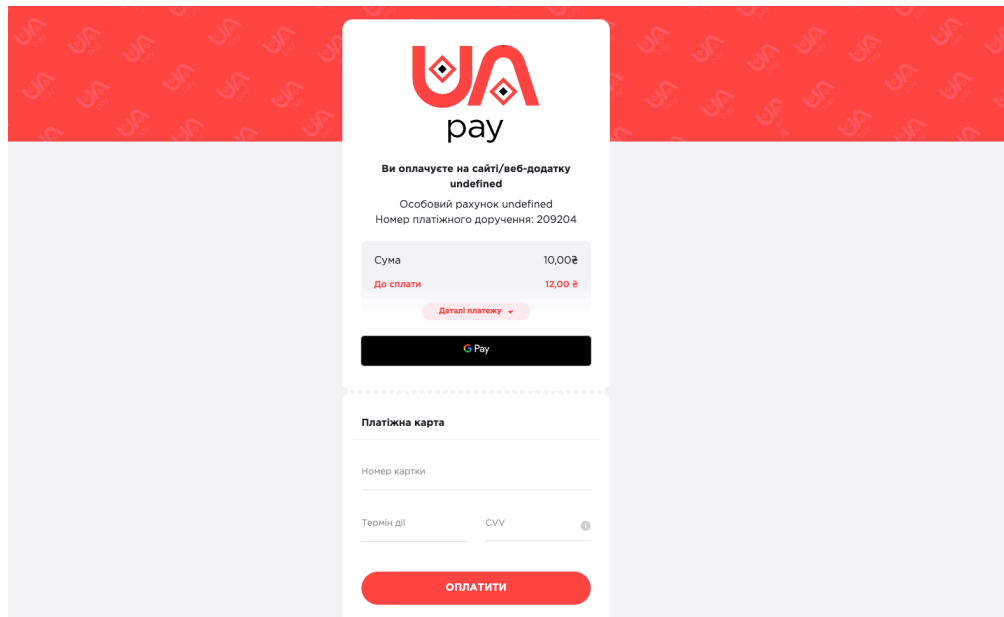


Рисунок 1.3 – Платіжна сторінка UAPAY [3]

Недоліки:

— для повної інтеграції недоступна оплата GooglePay та ApplePay;

— відсутність будь-яких інструментів для забезпечення безпеки, чи протидії фроду.

1.3 Аналіз різновидів платежів

Платежі, які проводяться в еквайринговій платформі зазвичай поділяються на два види:

— P2P – переказ з карти на карту. Тобто перекидання грошей від фізичної особи до фізичної особи;

— E-commerce – перекази з картки на рахунок. Тобто оплата грошей з карти на юридичний рахунок, ФОП рахунок, будь-який рахунок IBAN.

Враховуючи, що система має слідкувати за шахрайством, а заробіток в обхід оподаткуванню – є шахрайством, платформа буде надавати можливість проводити лише e-commerce платежі.

1.3.1 Різновиди e-commerce платежів

E-commerce платежі також поділяються на декілька типів[4]:

- авторизаційний платіж. Платіж який знімає одразу вказану суму з карти платника на користь отримувача;
- преавторизаційний платіж. Це платіж, який відбувається в два етапи. Перший, коли кошти бронюються на рахунку платника, очікуючи другий етап. Та другий етап – коли підтверджується списання коштів, але із вказанням суми. В свою чергу, сума може бути менша або більша згідно договору;
- рекурентний платіж. Платіж-підписка, який відбувається з підтвердженням зі сторони платника лише одноразово, і в залежності від умов повторно списує гроші коли підходить термін списання.

Для гнучкості в наданні послуг розроблена еквайрингова платформа підтримуватиме усі види e-commerce платежів.

1.4 Аналіз підтвердження платежу

Важливу роль відіграє безпека зі сторони платника, щоб унеможливити списання коштів з фізичної карти, або у випадку зламу, платіжних даних.

Для цього існують різні типи підтвердження платежу платником. Розглянемо основні типи підтвердження платежу: 3DS та LOOKUP.

LOOKUP більш простий в реалізації. Його суть полягає в тимчасовому блокуванні певної суми коштів, які повертаються після підтвердження за допомогою коду з СМС повідомлення. Повна послідовність зображена на рисунку 1.4.

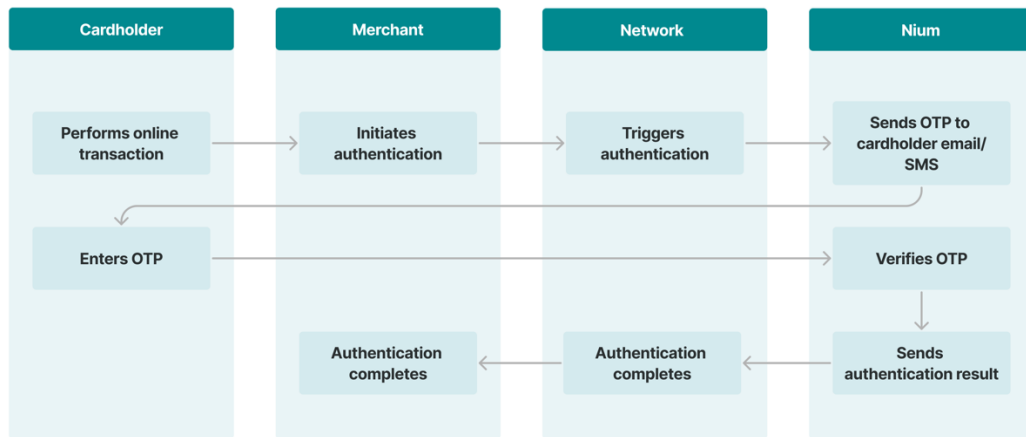


Рисунок 1.4 – Послідовність підтвердження платежу за допомогою LOOKUP [5]

Перехопити СМС повідомлення в час розвитку технологій не так складно, а отже запроваджений новий тип підтвердження платежу – 3DS. Послідовність зображено на рисунку 1.5.

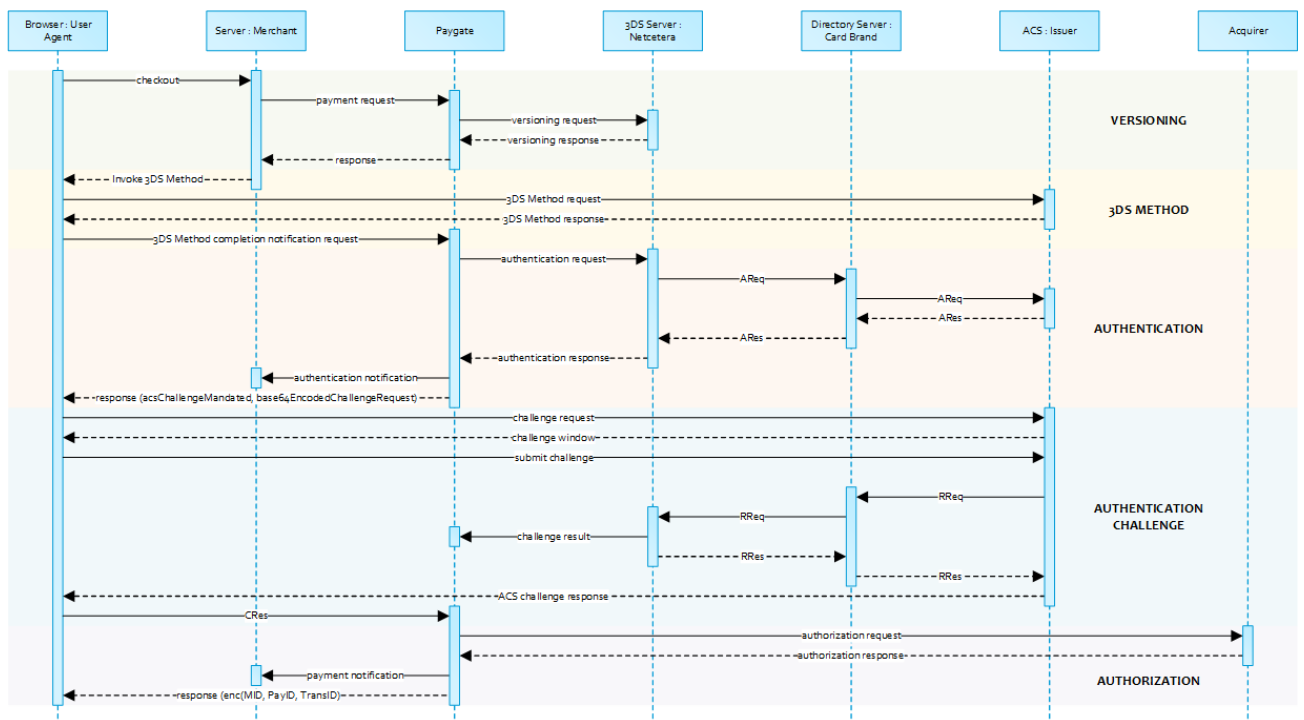


Рисунок 1.5 – Послідовність проходження 3DS перевірки [6]

Основна особливість такого підходу – залученість усіх трьох сторін: банк-екваєр, банк-емітент та ініціатор платежу. Старі версії цього протоколу також відправляють СМС, але починаючи з другої версії підтвердження відбувається в додатку банку-емітенту за його наявності в платника [6].

1.5 Аналіз PCI DSS сертифікації

PCI DSS – це набір вимог і рекомендацій, розроблених для забезпечення безпеки даних платіжних карт. Стандарт впроваджений Радою зі стандартів безпеки індустрії платіжних карт до якої входять провідні платіжні системи, такі як Visa, MasterCard, American Express, Discover та JCB. Основною метою PCI DSS є захист конфіденційної інформації платіжних карток від несанкціонованого доступу, шахрайства та витоків даних. Ліцензія зображена на рисунку 1.6.



Рисунок 1.6 – PCI DSS ліцензія [7]

Важливою особливістю стандарту є його гнучкість у застосуванні, оскільки він дозволяє адаптувати вимоги до конкретних умов бізнесу. Однак недотримання стандарту може призвести до значних штрафних санкцій, втрати довіри з боку клієнтів і платіжних систем, а також підвищених ризиків витоку даних.

У контексті еквайрінгових платформ, відповідність PCI DSS є основною вимогою для забезпечення безпеки фінансових транзакцій та захисту даних користувачів. Використання штучного інтелекту в таких системах може сприяти підвищенню рівня безпеки через автоматичне виявлення аномалій та потенційних загроз у режимі реального часу, що полегшує дотримання стандартів безпеки.

Стандарт містить 12 основних вимог, які охоплюють різні аспекти безпеки інформаційних систем і процесів обробки платіжних карт. Ці вимоги поділяються на шість основних категорій і охоплюють різні аспекти захисту інформації, яка обробляється, зберігається або передається під час використання платіжних карт.

Перша категорія – забезпечення безпечної мережі. Вона включає в себе:

- підтримку та встановлення безпечної мережевої інфраструктури, використовуючи брендмауери;
- використання належної конфігурації безпеки для всіх систем і виключення можливості використовувати стандартні паролі та інші налаштування, надані постачальником.

Друга категорія – захист даних власників платіжних карт. Вона включає:

- захист збережених даних власників карт;
- шифрування даних карт при передачі по відкритих мережах.

Третя категорія – підтримка системи управління вразливостями:

- зобов'язання використовувати й регулярно оновлювати антивірусне програмне забезпечення або інші механізми захисту, встановлення та виправлення знайдених вразливостей;

- всі програми та системи мають оновлюватись постійно до найновіших версій.

Четверта категорія – контроль доступу:

- обмеження доступу до даних карт;
- призначення і використання унікальних ідентифікаційних даних кожному користувачеві, що має доступ до системи;
- обмеження фізичного доступу до даних карт, захист фізичних серверів.

П'ята категорія – моніторинг і тестування мережі:

- відстеження та контроль всіх доступів до мережевих ресурсів і даних карт;
- регулярне тестування системи безпеки та процесів.

Шоста категорія – підтримка політики безпеки інформації. Зобов'язує підтримувати політику безпеки для всього персоналу.

Ці вимоги включають контроль доступу до даних, шифрування інформації, моніторинг мережевої активності, регулярне тестування системи безпеки та забезпечення належного захисту від шкідливого програмного забезпечення. PCI DSS призначений для всіх організацій, які зберігають, передають або обробляють дані платіжних карт, незалежно від їх розміру чи обсягу операцій.

2 ВИБІР ТЕХНОЛОГІЙ ТА ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ

2.1 Архітектура серверної частини

Еквайрингова платформа матиме велике навантаження. Основною вимогою до такої системи є стабільність та відмовостійкість, оскільки це опрацювання мільйонів платежів, тисячі генерацій бухгалтерських звітів, десятки інтеграцій та багато всього іншого. Тож прийняте рішення використовувати мікросервісну архітектуру.

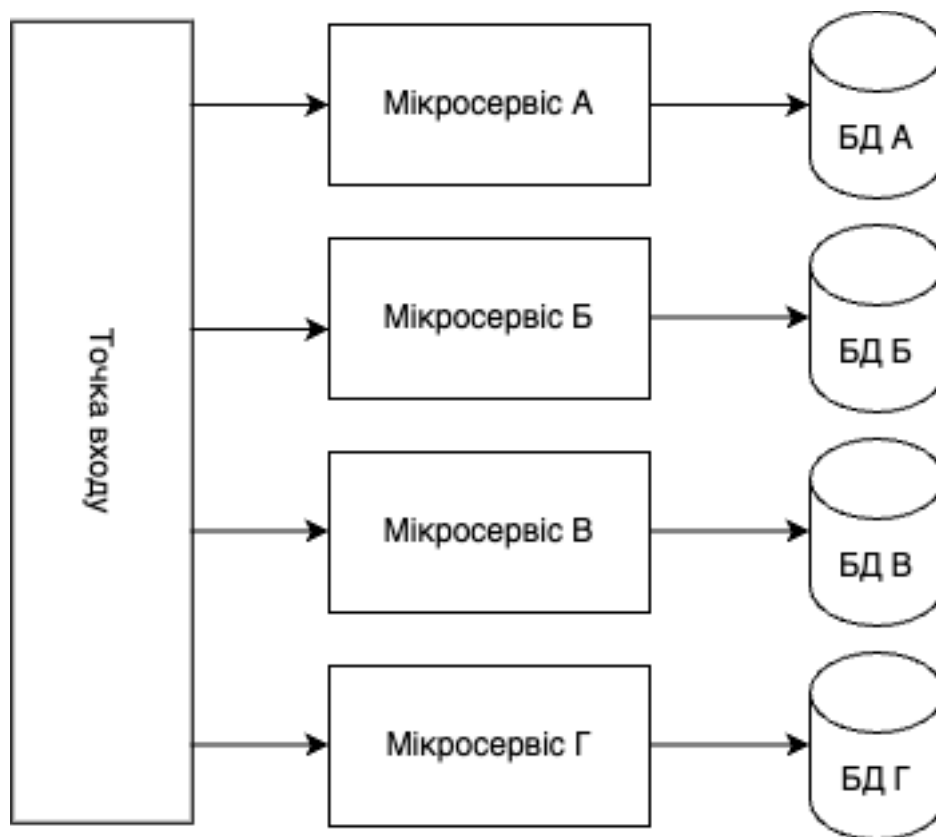


Рисунок 2.1 – Мікросервісна архітектура

Головними перевагами такого підходу є:

- легкість масштабування. В свою чергу масштабування є горизонтальне та вертикальне. Горизонтальне – це збільшення кількості екземплярів певного мікросервісу. Вертикальне – це збільшення ресурсів віртуальної чи фізичної машини;

- відмовостійкість. Кожен мікросервіс має свою базу даних, тож при непередбачуваних обставинах лише частина функціоналу усієї системи не буде працювати, допоки не відбудеться відновлення;
- розподілене розроблення. В такій великій системі повинна бути присутня підтримка усієї екосистеми, а це і декілька веб-проектів, і підтримка різних інтеграцій, і підтримка бекенду, який в свою чергу має обслуговувати усі ці кінцеві продукти, і підтримка мобільної інтеграції. Тож, розділивши усе це на міні-проекти та бекенд на мікросервіси, буде не складно розділити відповідальність між різними командами, які мають компетенцію в конкретній галузі.

2.2 Бази даних

2.2.1 Проектування структури бази даних

Проектування структури БД є настільки ж важливим, як і вибір технологій чи вибір архітектури. Гарно спроектована БД завжди дається в знаки – легко підтримувати, легко розширювати. Проектування БД для еквайрингової платформи розділимо на три частини:

- проектування основної частини;
- проектування частини адміністрування;
- проектування зберігання чутливої інформації про карти.

Зберігання чутливих даних карток зображено на рисунку 2.3.

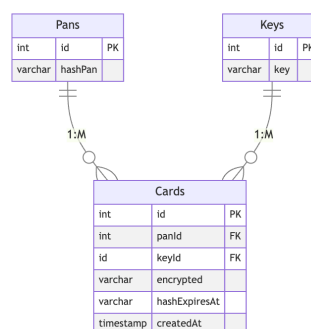


Рисунок 2.2 – Структура БД зберігання чутливої інформації

Проектування основної частини знаходиться на рисунку 2.3.

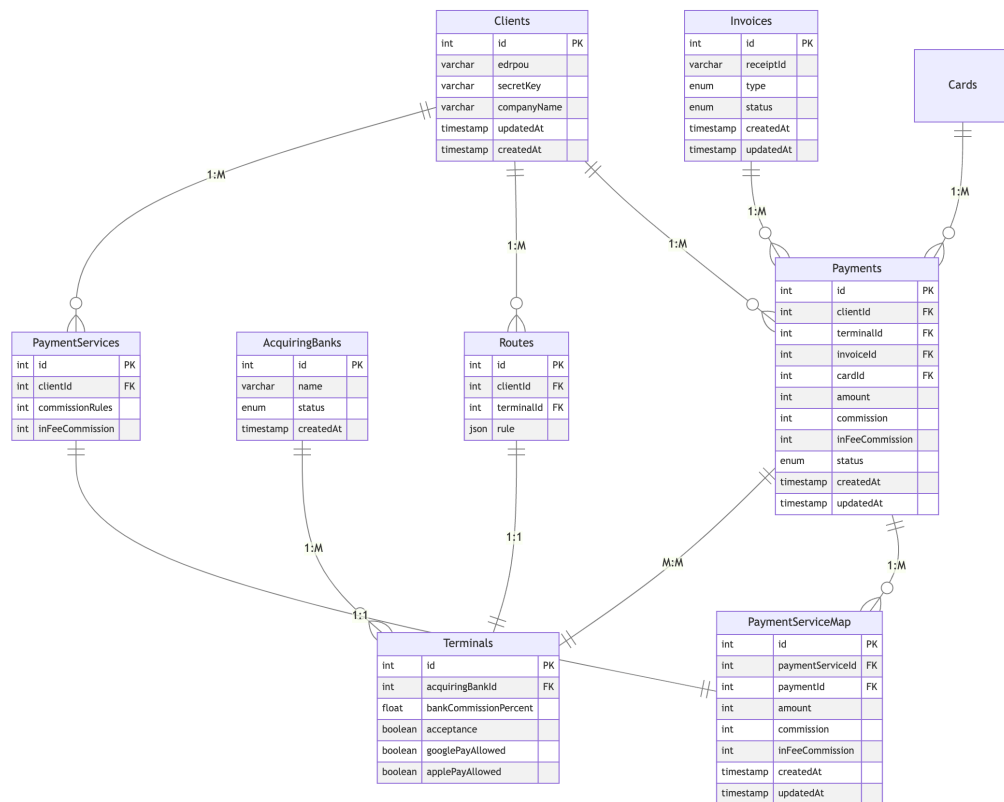


Рисунок 2.3 – Структура БД основної частини

Проектування частини адміністрування зображено на рисунку 2.4.

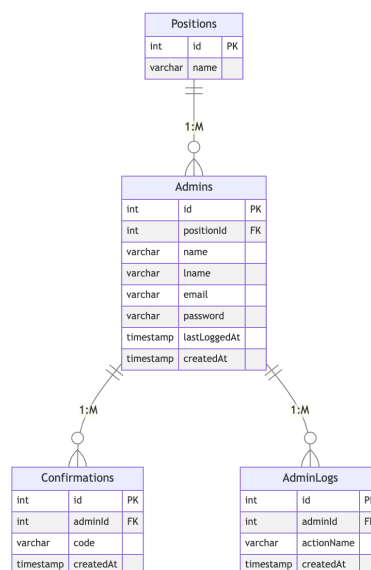


Рисунок 2.4 – Структура БД адміністративної частини

2.3 Вимоги згідно PCI DSS сертифікації

Вище розглянуті вимоги до PCI DSS сертифікації, згідно якої аудит відбувається для кожної еквайрингової платформи без виключення. Ці вимоги дуже загальні, тож потрібно висвітити підходи, які використані в ході розроблення програмного забезпечення, щоб відповідати даним вимогам.

2.3.1 Вимоги до способу зберігання чутливої інформації

Щоб відповідати вимозі зберігання чутливої інформації, поставлені наступні задачі:

- в БД ніколи не має зберігатись CVV карти платника. Код підтвердження карти потрібен лише на момент оплати для передачі банкам-екваєрам, а отже, не зберігаючи CVV, знімається відповідальність з системи, у разі інцидентів з витоком даних;
- в БД ніколи не має зберігатись інформація про номер карти та дата придатності в відкритому вигляді, а отже тільки в зашифрованому. Такий підхід дозволить вберегти чутливу інформацію, навіть у випадку витоку і злому БД;
- пошук карти платника може відбуватись за допомогою контрольної суми, тобто хешу. З таким підходом, не потрібно кожен раз розшифровувати чутливу інформацію, щоб дізнатися чи існує така карта;
- побудувати процес зміни ключа шифрування. Проєктування БД, яке розглянуто раніше, дозволяє використовувати різні ключі шифрування. Що в свою чергу дозволить безболісно оновлювати і перешифровувати дані, не вимикаючи сервіс, оскільки чутлива інформація, яка ще не була перешифрована, може використати старий ключ шифрування для передачі інформації;
- передача інформації про карту платника, при спілкуванні з банками-екваєрами має відбуватись тільки зашифрованому вигляді.

Дотримуючись усіх цих підходів, система буде відповідати вимозі зберігання і шифрування чутливої інформації.

2.3.2 Вимоги до адміністрування

Четверта, п'ята та шоста вимоги – про безпеку, контроль доступу, моніторинг системи. Щоб дотримуватися цих вимог, поставлені наступні задачі:

- чітка сітка ролей і їх доступів до можливостей адміністрування. Спроектowana БД для адміністрування включає можливість розділення адміністраторів на ролі, і відповідно на можливості в адміністративній панелі;
- авторизація має відбуватися кожні 15хв;
- авторизація має відбуватися за допомогою двофакторного підтвердження;
- логування і контроль дій адміністраторів. Спроектowana БД записує усі дії адміністраторів;
- адміністратори не мають прав на перегляд чутливої інформації. Оскільки уся інформація зашифрована, адміністрація може користуватись автоматичними механізмами і ідентифікаторами, для завершення дій пов'язаних з платежами: зарахування, повернення тощо.

2.3.3 Вимоги до інтеграції з еквайринговою платформою

Еквайрингова платформа надає гнучкі можливості для клієнтів в способі використання:

- готова платіжна сторінка;
- клієнтська панель адміністрування, де можна створити посилання на готову платіжну сторінку;
- повна інтеграція, задля кастомізації своєї сторінки оплати.

Останній пункт дуже чутливий, оскільки клієнт, який не матиме PCI DSS ліцензії, зможе реалізувати власні рішення. За таких обставин дуже важливо дотримуватися вимоги зберігання чутливої інформації.

Отже, щоб відповідати цим вимогам, треба:

- ізолювати інтеграцію клієнта від створення карткових даних в нашій системі. Цей пункт легко вирує реалізація фрейму для створення карти платника в системі;
- не мати в відкритому API точок входу, які віддають чутливу інформацію.

2.4 Вибір технологій для роботи зі штучним інтелектом

Інтеграція штучного інтелекту в систему керування платежами стає основним інструментом для забезпечення високої точності та ефективності у виявленні підозрілих транзакцій і прийнятті рішень щодо їх подальшої обробки.

Python є ідеальним вибором для задач виявленню фроду завдяки таким факторам:

- розвинена екосистема бібліотек. Бібліотеки для машинного та глибинного навчання PyTorch, TensorFlow [9] спрощують процес створення, навчання та тестування моделей;
- інтеграція з БД та API. Python забезпечує підключення до БД, що полегшує збір і обробку транзакційних даних.

Зважаючи на вимоги до точності та швидкості, глибинні нейронні мережі на базі TensorFlow є оптимальним рішенням. Цей підхід дозволить:

- виявити складні, приховані шаблони в транзакціях;
- забезпечити масштабованість у випадку збільшення обсягів даних;
- інтегрувати рішення в еквайрингову систему.

Такий набір технологій дозволить вирішувати завдання визначення безпеки транзакцій і прийняття рішень без додаткової перевірки, забезпечуючи високу точність і швидкість обробки.

ВИСНОВКИ

Під час проходження практики проведено комплексний аналіз існуючих рішень для еквайрингових платформ, зокрема LiqPay, UAPAY та WayForPay. Це дозволило визначити основні підходи й функціональні можливості, які забезпечують ефективну обробку платежів та мінімізацію ризиків для учасників фінансових операцій. Розгляд основних типів платежів, таких як p2p та e-commerce, дозволив вивчити їхні особливості, а також визначити можливості для інтеграції у різні бізнес-моделі.

Дослідження різновидів транзакцій для e-commerce, включаючи авторизаційні, преавторизаційні та рекурсивні платежі, підкреслило потребу в гнучкому та адаптивному підході до обробки транзакцій. Це, своєю чергою, обумовило вибір архітектури серверної частини, яка здатна ефективно масштабуватися й забезпечувати стабільну роботу платформи за різних умов навантаження.

Проектування бази даних стало наступним важливим етапом роботи, що дозволило визначити ефективну структуру для зберігання та обробки транзакційних даних.

На завершення обрані технології штучного інтелекту, які інтегруються з серверною частиною платформи та здатні забезпечити виявлення підозрілих транзакцій і підтримку процесу прийняття рішень щодо додаткових перевірок. Вибір зроблено на користь глибинного навчання з використанням бібліотеки TensorFlow, що дозволяє досягти високої точності виявлення потенційного фроду. Це рішення допоможе забезпечити баланс між швидкістю обробки даних та надійністю безпеки платежів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про LiqPay – Режим доступу до ресурсу: <https://www.liqpay.ua/doc>
2. Про WayForPay – Режим доступу до ресурсу: <https://wiki.wayforpay.com/>
3. Про UAPAY – Режим доступу до ресурсу: <https://uapayua.atlassian.net/wiki/spaces/AC/pages/753795086>
4. Про E-commerce – Режим доступу до ресурсу: <https://interkassa.com/blog/shho-take-elektronna-komerciya-e-commerce-dlya-pochatkivciv>
5. Про LOOKUP – Режим доступу до ресурсу: <https://docs.nium.com/apis/docs/otp-based-3ds-authentication-flow>
6. Про 3DS – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/3-D_Secure
7. Про PCI DSS сертифікацію – Режим доступу до ресурсу: <https://getpci.com/>
8. Про використання mermaid – Режим доступу до ресурсу: <https://mermaid.js.org/>
9. Про TensorFlow – Режим доступу до ресурсу: <https://www.tensorflow.org/>