Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: «Метод аналізу ризиків витоку конфіденційної інформації у системах онлайн-банкінгу»

Виконавець: студент IV курсу, групи КБ-42

_____ **Нікіта СИРОТА**
(підпис) (ім'я, прізвище)

	Підпис	**Ім'я ПРІЗВИЩЕ**
Керівник		Юрій ЩЕБЛАНІН
Нормоконтроль		Яніна ШЕСТАК

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-42** (група) **Сироті Нікіті Святославовичу** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Метод аналізу ризиків витоку конфіденційної інформації у системах онлайн-банкінгу

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Архітектура систем онлайн-банкінгу, методи аналізу ризиків

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно проаналізувати функціонування систем онлайн-банкінгу, визначити типи конфіденційної інформації та джерела загроз її витоку. Ознайомитися з існуючими методами аналізу ризиків, оцінити їх ефективність і на цій основі розробити власний метод кількісної оцінки ризику витоку інформації.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблений метод для кількісної оцінки ризиків витоку конфіденційної інформації в системах онлайн-банкінгу.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видав _____ Юрій ЩЕБЛАНІН
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Нікіта СИРОТА
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 27.01.2025	*виконано*
2	Аналіз літератури	28.01.2025 – 11.02.2025	*виконано*
3	Обґрунтування вибору рішення	12.02.2025 – 24.02.2025	*виконано*
4	Дослідження архітектури онлайн-банкінгу	25.02.2025 – 24.03.2025	*виконано*
5	Аналіз типів інформації в системах онлайн-банкінгу	25.03.2025 – 07.04.2025	*виконано*
6	Виявлення та класифікація джерел загроз витоку інформації	08.04.2025 – 20.04.2025	*виконано*
7	Оцінка ефективності існуючих методів аналізу ризиків	21.04.2025 – 05.05.2025	*виконано*
8	Розробка концепції та архітектури методу	06.05.2025 – 20.05.2025	*виконано*
9	Порівняння результатів із існуючими методами	21.05.2025 – 04.06.2025	*виконано*
10	Оформлення пояснювальної записки	05.06.2025 – 08.06.2025	*виконано*
11	Підготовка до захисту кваліфікаційної роботи	09.06.2025 – 13.06.2025	*виконано*

Завдання видав _____ Юрій ЩЕБЛАНІН
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Нікіта СИРОТА
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 62 сторінок основного тексту, 12 таблиць та 5 рисунків. Список використаних джерел містить 24 найменування і займає 3 сторінки.

Метою роботи є підвищення ефективності аналізу ризиків витоку конфіденційної інформації в системах онлайн-банкінгу.

Об'єктом дослідження є процеси аналізу ризиків витоку конфіденційної інформації в системах онлайн-банкінгу.

Предметом дослідження є методи аналізу ризиків витоку конфіденційної інформації в системах онлайн-банкінгу.

Методи дослідження:

- теоретичний аналіз;
- структурний аналіз;
- синтез, моделювання.

Практична цінність полягає у вдосконаленні процесів виявлення загроз витоку конфіденційної інформації, що сприятиме підвищенню рівня безпеки онлайн-банківських систем.

Ключові слова: аналіз ризиків, онлайн-банкінг, конфіденційна інформація, витік даних, інформаційна безпека, методи аналізу ризиків, захист даних, банківські системи, загрози безпеці, управління ризиками, оцінка ризиків, вразливості.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІБ	–	Інформаційна безпека
ІС	–	Інформаційна система
ІТ	–	Інформаційні технології
ІКС	–	Інформаційно-комунікаціна система
ЦКД	–	Цілісність, конфіденційність, доступність
НСД	–	Несанкціонований доступ
ПЗ	–	Програмні засоби, програмне забезпечення
ОБ	–	Онлайн-банкінг
КІ	–	Конфіденційна інформація
API	–	Інтерфейс прикладного програмування
КЕП	–	Кваліфікований електронний підпис
MFA	–	Багатофакторна автентифікація
PCI DSS	–	Стандарт безпеки платіжних карток
NIST	–	Національний інститут стандартів і технологій США

ВСТУП

Актуальність роботи зумовлена зростанням кількості кібератак на банківські системи, у тому числі фішингу, атак типу «людина посередині», зловмисного програмного забезпечення, спрямованого на крадіжку даних, а також технічних і організаційних вразливостей, що сприяють витоку конфіденційної інформації. У зв’язку з цим зростає потреба у впровадженні ефективних методів аналізу ризиків, які дозволяють своєчасно ідентифікувати потенційні загрози та мінімізувати наслідки інцидентів

Метою роботи є підвищення ефективності аналізу ризиків витоку конфіденційної інформації в системах онлайн-банкінгу.

Для досягнення зазначеної мети кваліфікаційної роботи поставлено наступні **завдання:**

- проаналізувати особливості функціонування систем ОБ;
- виявити основні джерела загроз витоку конфіденційної інформації;
- проаналізувати та оцінити ефективність існуючих методів аналізу ризиків в інформаційній безпеці у контексті онлайн-банкінгу;
- розробити та обґрунтувати метод аналізу ризиків витоку конфіденційної інформації для систем онлайн-банкінгу;

Об’єктом дослідження є процеси аналізу ризиків витоку конфіденційної інформації в системах онлайн-банкінгу.

Предметом дослідження є методи аналізу ризиків витоку конфіденційної інформації в онлайн-банківських системах.

Методи дослідження: теоретичний аналіз, структурний аналіз, синтез, моделювання.

Практична цінність роботи полягає у вдосконаленні процесів виявлення і аналізу ризиків витоку конфіденційної інформації, що дозволить банківським установам ефективніше реагувати на загрози, підвищити стійкість до кіберінцидентів та забезпечити збереження довіри клієнтів.

РОЗДІЛ 1
АНАЛІЗ РИЗИКІВ БЕЗПЕКИ В СИСТЕМАХ ОНЛАЙН-БАНКІНГУ

1.1 Структура та принципи функціонування систем онлайн-банкінгу

Онлайн-банкінг - це сукупність технологій та інформаційно комунікаційних сервісів, які забезпечують дистанційний доступ клієнтів до банківських продуктів і послуг через мережу Інтернет. Такі системи дозволяють користувачам цілодобово здійснювати фінансові операції (перекази, оплата рахунків, управління депозитами), переглядати баланс рахунків, отримувати виписки, комунікувати з банком та керувати особистими фінансами без фізичної присутності у відділенні банку [1, 2].

Системи ОБ реалізуються у вигляді багаторівневої клієнт-серверної архітектури, яка забезпечує безпечну обробку даних, масштабованість та гнучкість інтеграції з внутрішніми й зовнішніми сервісами.

1.1.1 Основні компоненти архітектури

Для розуміння характеру ризиків, пов’язаних із витоком КІ в ОБ, першочергово необхідно розглянути типову структуру таких систем. Архітектура ОБ є багаторівневою та включає низку функціональних компонентів, які забезпечують обробку, передачу й зберігання даних, а також реалізацію банківських послуг у цифровому середовищі. На рисунку 1.1 схематично подано основні складові типової системи ОБ та взаємозв’язки між ними. Кожен із цих елементів виконує специфічні функції та становить потенційну точку концентрації ризиків, що потребує окремого аналізу.

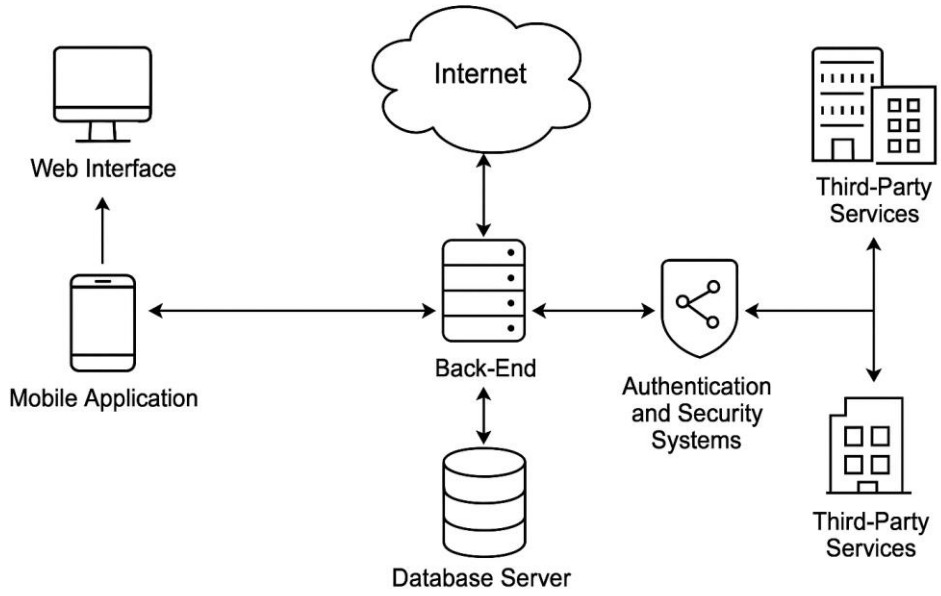

Рисунок 1.1 – Компоненти архітектури ОБ

Основні компоненти архітектури онлайн-банкінгу включають:

• Клієнтська частина (Front-end) - включає веб-інтерфейс (через браузер) та мобільні застосунки, за допомогою яких клієнти взаємодіють з банківськими послугами. Інтерфейс відображає дані з серверної частини, дозволяє надсилати транзакції, підтвердження операцій, запити та повідомлення. Front-end повинен бути сумісним з різними операційними системами, мати сучасні UX/UI характеристики, а також підтримувати шифрування та цифровий підпис [3].

• Серверна частина (Back-end) - логічне ядро системи, яке відповідає за обробку бізнес-логіки, зберігання даних, автентифікацію, управління транзакціями, зв’язок з базами даних та зовнішніми API. Саме тут відбувається основна обробка запитів клієнтів, взаємодія з внутрішніми банківськими системами (Core Banking Systems), зокрема модулями платіжних доручень, консолідації рахунків, кредитування тощо [4].

• База даних - критичний компонент, де зберігаються персональні, фінансові та операційні дані клієнтів: імена, рахунки, історія платежів, автентифікаційна інформація (хеші паролів, токени, сеансові ключі). Дані мають бути захищеними відповідно до вимог стандартів ISO/IEC 27001 та PCI DSS, зокрема з використанням шифрування, резервного копіювання та контрольованого доступу [5].

• Системи автентифікації та безпеки - забезпечують ідентифікацію користувачів (наприклад, через логін/пароль, OTP, біометрію), контроль доступу, шифрування з'єднання (TLS 1.3), захист сесій, моніторинг активності, управління цифровими сертифікатами. Також до цього сегмента належать системи виявлення вторгнень (IDS), захисту API, засоби боротьби з фішингом та автоматизованими ботами [6].

• API-шлюзи - особливо актуальні в контексті відкритого банкінгу (Open Banking), що регулюється директивою PSD2. API надають стороннім сервісам контрольований доступ до банківських функцій, зокрема для фінансових агрегаторів, платіжних сервісів, мобільних застосунків. Невірно сконфігуровані або незахищені API становлять серйозну загрозу витоку КІ [4].

• Системи моніторингу, журналювання та виявлення загроз (SIEM, SOC) - збирають інформацію про події, дії користувачів, помилки, підозрілу активність; аналізують і корелюють події в реальному часі для попередження атак. Це дозволяє оперативно виявляти спроби компрометації та формувати аналітику для реагування [6].

1.1.2 Функціональні засади реалізації

Проєктування та реалізація систем ОБ ґрунтується на низці ключових принципів, які забезпечують їхню надійність, стійкість до загроз, масштабованість та відповідність вимогам регуляторів. До основних принципів побудови систем ОБ належать:

1) Конфіденційність

Захист персональних даних клієнтів є пріоритетним завданням систем ОБ. Усі канали передачі даних між клієнтом і сервером повинні бути зашифровані за допомогою криптографічних протоколів, а автентифікаційні дані - зберігатися у вигляді хешів з додатковим сілом. Доступ до КІ повинен бути суворо контрольований згідно з принципами мінімальних привілеїв та обмеження прав доступу.

2) Цілісність

Дані в системі повинні зберігати свою достовірність і залишатися незмінними без відповідного дозволу. Для забезпечення цілісності застосовуються електронні цифрові підписи (ЕЦП), контрольні суми, механізми журналювання дій та контроль транзакцій. Кожна транзакція має проходити перевірку логіки та відповідності умовам банку.

3) Доступність

Система ОБ повинна бути доступною 24/7/365, із гарантією безперервного функціонування навіть у разі часткового виходу з ладу окремих компонентів. Це досягається шляхом використання кластеризації серверів, балансування навантаження, георезервування центрів обробки даних (ЦОД), а також впровадження планів аварійного відновлення (Disaster Recovery Plans, DRP) і забезпечення високої готовності (High Availability, HA).

4) Масштабованість і модульність

Система ОБ має бути здатною до розширення без потреби повної перебудови. Масштабованість досягається за рахунок використання мікросервісної архітектури, контейнеризації (Docker, Kubernetes), а також горизонтального і вертикального масштабування компонентів. Такий підхід дозволяє додавати нові функції, інтегрувати зовнішні сервіси (API, фінтех-платформи) та адаптуватися до змін попиту.

5) Інтегрованість з іншими банківськими системами

Система ОБ повинна взаємодіяти з внутрішніми модулями банку - такими як Core Banking System (CBS), CRM, KYC/AML системами, платіжними шлюзами тощо. Для цього використовуються стандартизовані протоколи обміну даними (SOAP, REST та ін.), а також сервіси інтеграційної шини (ESB).

6. Безперервний моніторинг і аудит

Усі події, що стосуються доступу, авторизації, транзакцій, змін даних - мають реєструватися в системі журналювання. Для цього застосовуються SIEM-системи, SOC-платформи, засоби поведінкової аналітики (UEBA) та засоби виявлення загроз у режимі реального часу. Це дозволяє оперативно реагувати на інциденти та зменшувати потенційні наслідки.

Доцільним є узагальнення принципів у вигляді аудиторської таблиці (табл. 1.1), яка демонструє відповідність ключових архітектурних вимог міжнародним стандартам ІБ. Таблиця може бути використана як інструмент оцінювання поточної реалізації безпеки або як орієнтир для проектування системи ОБ, здатної протистояти актуальним загрозам. Таким чином, вона виконує роль методичного шаблону для внутрішнього контролю або попереднього технічного аудиту.

Таблиця 1.1

Аудит дотримання принципів побудови системи онлайн-банкінгу

Принцип	**Аудиторське питання**	**Джерело / стандарт**	**Ознака відповідності**
1	2	3	4
Конфіденційність	Чи використовується шифрування при передачі та зберіганні даних?	ISO/IEC 27001, PCI DSS	TLS 1.3, AES-256, хешування паролів
Цілісність	Чи застосовуються механізми контролю змін і цифрового підпису?	ISO/IEC 27005, PCI DSS	ЕЦП, логування змін, контрольні суми
Доступність	Чи забезпечено безперервну роботу системи (24/7)?	ISO/IEC 22301, DRP/BCP	SLA, резервування, HA, кластеризація
Масштабованість і модульність	Чи дозволяє архітектура легко додавати нові функції/компоненти?	Архітектурні практики (TOGAF)	Мікросервіси, API, контейнеризація

продовження таблиці 1.1

1	2	3	4
Інтегрованість	Чи є підтримка обміну даними з іншими системами (CBS, CRM, KYC)?	PSD2, ISO 20022	REST/SOAP API, ESB, інтеграційні шлюзи
Безперервний моніторинг	Чи впроваджені системи виявлення інцидентів безпеки?	ISO/IEC 27035, NIST SP 800-92	SIEM, SOC, журналювання
Відповідність нормативам	Чи відповідає система вимогам НБУ, PCI DSS, GDPR?	НБУ №95, PCI DSS, GDPR	Сертифікати, політики, аудити
Орієнтація на користувача	Чи враховані UX-аспекти безпеки в інтерфейсі?	OWASP, HCI guidelines	Захист сесій, повідомлення, тайм-аут

Таким чином, застосування принципів побудови в поєднанні з системним аудитом дозволяє створити захищене, стійке до збоїв та нормативно сумісне середовище для функціонування ОБ.

1.2 Класифікація інформації за рівнем доступності

Класифікація інформації за рівнем доступності є ключовим інструментом організації заходів безпеки в системах ОБ. Вона дозволяє визначити обсяг необхідного захисту, встановити політику доступу до даних і забезпечити відповідність вимогам чинного законодавства.

Згідно зі статтею 21 Закону України «Про інформацію» [7], за порядком доступу вся інформація поділяється на:

- відкриту інформацію;
- інформацію з обмеженим доступом, до якої належить:

- конфіденційна інформація;
- таємна інформація;
- службова інформація.

У системах ОБ, що обслуговують фізичних та юридичних осіб, фактично обробляються лише дві категорії інформації – відкрита та з обмеженим доступом, насамперед конфіденційна.

Відкрита інформація - це дані, доступ до яких не обмежено законодавством і які можуть бути вільно використані. Вона охоплює загальні умови обслуговування клієнтів (тарифи, порядок надання послуг), адреси відділень та банкоматів, нормативні документи, які публікуються на вимогу законодавства, відкриті API-ендпоінти, призначені для публічної взаємодії з системами (наприклад, в рамках стандарту PSD2).

Компрометація такої інформації зазвичай не має критичних наслідків, проте її неконтрольоване масове поширення або підробка можуть нести репутаційні ризики.

Інформація з обмеженим доступом включає інформацію, обмежену в доступі законом, внутрішніми політиками банку або контрактними умовами. В онлайн-банкінгу найпоширенішою формою такої інформації є конфіденційна інформація, що охоплює персональні дані клієнтів - ПІБ, ІПН, паспортні дані, адреса проживання, облікові дані - логіни, паролі, OTP, токени, біометричні шаблони, фінансова інформація - номери рахунків, історія транзакцій, залишки коштів, цифрові сертифікати - ключі електронного підпису, сеансові токени.

Захист цієї категорії інформації регулюється Законом України «Про захист персональних даних», Положенням про захист інформації в ІКС (НД Т31 2.5-010-03), а також міжнародними стандартами, зокрема стандартами ISO.

Варто відзначити, що Закон України «Про державну таємницю» [8] визначає державну таємницю як вид інформації у сфері оборони, національної безпеки, зовнішньої політики, розвідки тощо, розголошення якої може завдати шкоди інтересам держави. Така інформація підлягає обробці лише в спеціальних

режимах із застосуванням засобів технічного та криптографічного захисту, що мають відповідні атестати.

У системах ОБ, які обслуговують клієнтів у цивільному секторі, обробка державної таємниці не здійснюється. Їх архітектура, програмне забезпечення та захисні засоби, як правило, не атестовані для роботи з інформацією, що становить державну таємницю. Обіг такої інформації можливий лише у виняткових випадках (наприклад, при виконанні оборонних замовлень або роботі з військовими фінансовими структурами), і здійснюється через окремі захищені канали зв'язку поза межами стандартної ОБ інфраструктури.

Для наочності класифікаційних ознак та відповідних механізмів захисту інформації різного рівня доступності в ОБ, у таблиці 1.2 подано узагальнення ключових параметрів кожної категорії.

Таблиця 1.2

Категорії інформації в онлайн-банкінгу за доступністю

Категорія доступу	**Приклади інформації**	**Правове регулювання**	**Захисні механізми**
Відкрита	Тарифи, API-метадані, адреси відділень, публічні повідомлення	ЗУ «Про інформацію», вимоги НБУ	Моніторинг доступу, контроль версій
З обмеженим доступом	Персональні та фінансові дані, OTP, IBAN, електронні підписи	ЗУ «Про захист персональних даних», НД ТЗІ 2.5-010-03, ISO/IEC 27001	Шифрування, MFA, протоколювання, RBAC
Державна таємниця	Не застосовується в ОБ	ЗУ «Про державну таємницю»	Не підтримується в системах ОБ

1.3 Джерела формування, місця зберігання та обробки інформації

Інформація, що обробляється в системах онлайн-банкінгу, виникає на різних етапах взаємодії користувача із системою, формується як безпосередньо клієнтом, так і генерується автоматизовано на серверному боці або в результаті взаємодії з внутрішніми й зовнішніми інформаційними ресурсами.

Узагальнена структура джерел та місць зберігання основних типів інформації наведена в таблиці 1.3.

Таблиця 1.3

Джерела формування та місця зберігання інформації в системах ОБ

Тип інформації	**Джерело формування**	**Місце зберігання**	**Системний рівень**
Дані автентифікації	Користувач під час реєстрації або входу	Сервер авторизації, СУБД, HSM	Back-end
Персональні дані	Користувач, служба верифікації	Центральна база клієнтів (CRM, KYC)	Back-end, окрема СУБД
Транзакційна інформація	Користувач, платіжні шлюзи	Журнал транзакцій, база даних	Back-end, логіка обслуговування
Дані про пристрій	Агрегація під час сесії користувача	Лог-файли, SIEM-система	Front-end, сервер моніторингу
Електронні підписи, токени	Генерація банком або КЕП-сервісом	HSM, сертифікатне сховище	Криптографічний модуль
Відомості про запити API	Зовнішні/внутрішні застосунки	API Gateway, лог-файли	Інтеграційний рівень

1.3.1 Ключові сховища інформації в системах ОБ

До ключових сховищ інформації в системах ОБ належать:

1. Системи керування базами даних (СУБД): Центральне сховище критичної інформації (включаючи персональні та фінансові дані), як правило, розміщене в ізольованих сегментах внутрішньої мережі банку. Для забезпечення цілісності та конфіденційності даних застосовуються політики шифрування, резервного копіювання, багаторівневого контролю доступу;

2. Модулі апаратного шифрування (HSM): Відповідають за зберігання ключів, токенів, криптографічних сертифікатів та електронних підписів. Встановлюються в середовищах, що відповідають стандартам FIPS 140-2 або аналогічним;

3. Системи логування та моніторингу (SIEM, лог-сервери): Обробляють і зберігають службову інформацію: спроби входу, транзакції, збої, виклики API. Застосовуються для виявлення інцидентів безпеки, відповідності політикам і подальшої аудиторської перевірки;

4. Інтерфейсні шари (Front-end): Обробляють тимчасові сесійні токени, кешовані елементи UI, push-сповіщення. На цьому рівні не повинна зберігатися конфіденційна інформація у відкритому вигляді. Використання локального сховища повинно бути жорстко контрольоване;

Структура зберігання інформації в онлайн-банкінгу характеризується чітким функціональним розмежуванням між рівнями, що обробляють конфіденційні дані, і зонами, відповідальними за взаємодію з клієнтом. Компоненти з найвищим ступенем критичності зазвичай фізично або логічно ізольовані, а доступ до них здійснюється лише через захищені канали. Потоки даних між підсистемами мають бути суворо регламентовані, з урахуванням типів інформації та її контексту. Залежно від моделі доступу, рівень ризику витоку може значно варіюватися навіть для одного й того самого активу. Для візуалізації просторового розподілу компонентів, відповідальних за зберігання та обробку

інформації, а також потоків передачі даних між ними, у системі онлайн-банкінгу на рисунку 1.2 подано узагальнену структурну схему.

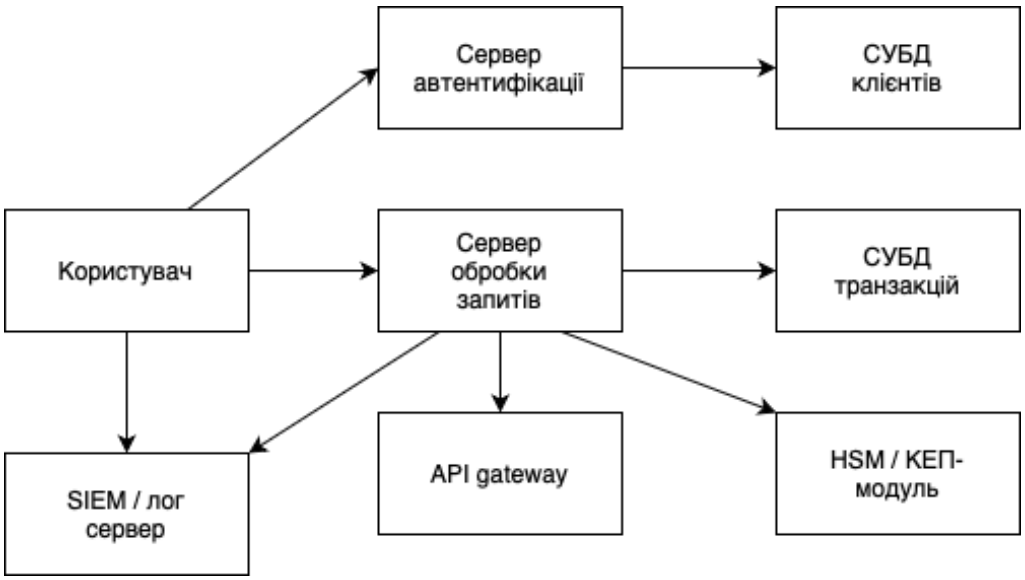

Рисунок 1.2 – Структура розподілу та зберігання інформації

Як показано на рисунку 1.2, інформаційні потоки в онлайн-банкінгу циркулюють між низкою логічних компонентів, кожен з яких виконує окрему функцію з формування, обробки, зберігання або контролю даних.

На початковому етапі ініціативу взаємодії бере на себе клієнт через інтерфейс (front-end), що може реалізовуватися як вебзастосунок або мобільний клієнт. Усі запити від користувача надходять до серверів банку через захищене з'єднання (наприклад, TLS 1.3), де обробляються залежно від типу запиту.

Сервер автентифікації здійснює перевірку облікових даних користувача (логін, пароль, OTP), звертаючись до централізованої бази даних клієнтів, яка також містить персональні дані, контактну інформацію та параметри банківських продуктів. Сервер обробки запитів виконує бізнес-логіку: опрацювання транзакцій, запитів до рахунків, виконання операцій з платіжними інструментами.

Фінансова інформація, що виникає в результаті транзакцій, зберігається в окремій базі даних транзакцій, що структурно та фізично відокремлена від довідників клієнтів. Під час підпису транзакцій або автентифікації через

сертифікати залучаються модулі апаратного шифрування (HSM) або сервіси електронного підпису (КЕП/ПЕП), які відповідають за зберігання криптографічних ключів.

Взаємодія з зовнішніми або внутрішніми сервісами (наприклад, партнерські платіжні шлюзи, API-додатки) здійснюється через API Gateway, що фільтрує запити, застосовує політики доступу, а також логування.

Важливою складовою архітектури є системи моніторингу та журналювання (SIEM, лог-сервери), які отримують дані про події з усіх ключових компонентів. Це забезпечує постійний аудит дій користувачів, адміністративних операцій, транзакцій та інцидентів безпеки.

Зазначена схема дозволяє не лише простежити, де саме формується і зберігається кожен тип інформації, а й окреслити критичні точки для подальшого аналізу ризиків витоку КІ.

1.4 Ризики витоку конфіденційної інформації в онлайн-банкінгу

Згідно з міжнародним стандартом ISO/IEC 27005:2022, ризик ІБ визначається як "потенційна ймовірність порушення конфіденційності, цілісності або доступності інформації, що може мати негативні наслідки для організації" [9]. У рамках цього підходу ризик розглядається як взаємозв’язок трьох елементів:

- загроза (кібератака, фішинг і т.ін.);
- вразливість (слабка автентифікація і т.ін.);
- актив (банківський застосунок, персональні дані клієнтів і т.ін.).

Управління ризиками в ІБ – це безперервний процес, який включає послідовне виявлення, оцінювання, обробку та контроль ризиків з метою забезпечення прийнятного рівня безпеки інформаційних активів.

Цей процес охоплює такі етапи:

1. Ідентифікацію активів та загроз;
2. Оцінювання ризиків (враховуючи ймовірність і рівень впливу);
3. Розробку та впровадження заходів контролю;

4. Моніторинг і перегляд ризиків на постійній основі.

Методології ISO/IEC 27005, NIST SP 800-30 та COSO ERM є визнаними міжнародними підходами до управління ризиками, що застосовуються у сфері ІБ, зокрема й у системах ОБ.

ISO/IEC 27005:2022 надає комплексну модель управління ризиками ІБ відповідно до вимог ISO/IEC 27001 [10]. Методологія охоплює весь життєвий цикл ризику: від ідентифікації активів, загроз і вразливостей - до вибору заходів реагування та постійного моніторингу. Особливістю ISO/IEC 27005 є чітка структуризація процесу управління ризиками в контексті ІБ та його інтеграція в систему менеджменту ІБ [9].

NIST SP 800-30 (Risk Management Guide for Information Technology Systems), розроблений Національним інститутом стандартів і технологій США, пропонує детальний процес оцінювання ризиків для IT-систем, включаючи побудову сценаріїв загроз, використання матриць ризиків, аналіз ймовірностей та впливу, а також визначення рівня ризику (низький, помірний, високий). Методологія активно використовується в державному секторі США та корпоративному середовищі, а її гнучкість дозволяє адаптувати її під галузеві специфіки, зокрема банківську сферу [11].

COSO ERM (Enterprise Risk Management - Integrated Framework) орієнтована на стратегічний рівень управління ризиками і широко застосовується у фінансовому секторі. Вона охоплює вісім ключових компонентів, включаючи формування внутрішнього контрольного середовища, ідентифікацію подій, оцінку та реагування на ризики, моніторинг і звітність [12].

1.4.1 Класифікація ризиків та методів їх оцінки в системах онлайн-банкінгу

Системи ОБ є складними інформаційними середовищами, які взаємодіють із великою кількістю зовнішніх і внутрішніх компонентів. Тому ризики, що виникають у таких системах, мають різну природу і потребують чіткої

класифікації. Це дозволяє ефективніше виявляти вразливості, визначати пріоритети захисту та будувати відповідні моделі реагування.

На рисунку 1.3 наведено узагальнену класифікацію ризиків за основними критеріями, що може бути адаптована для ОБ.

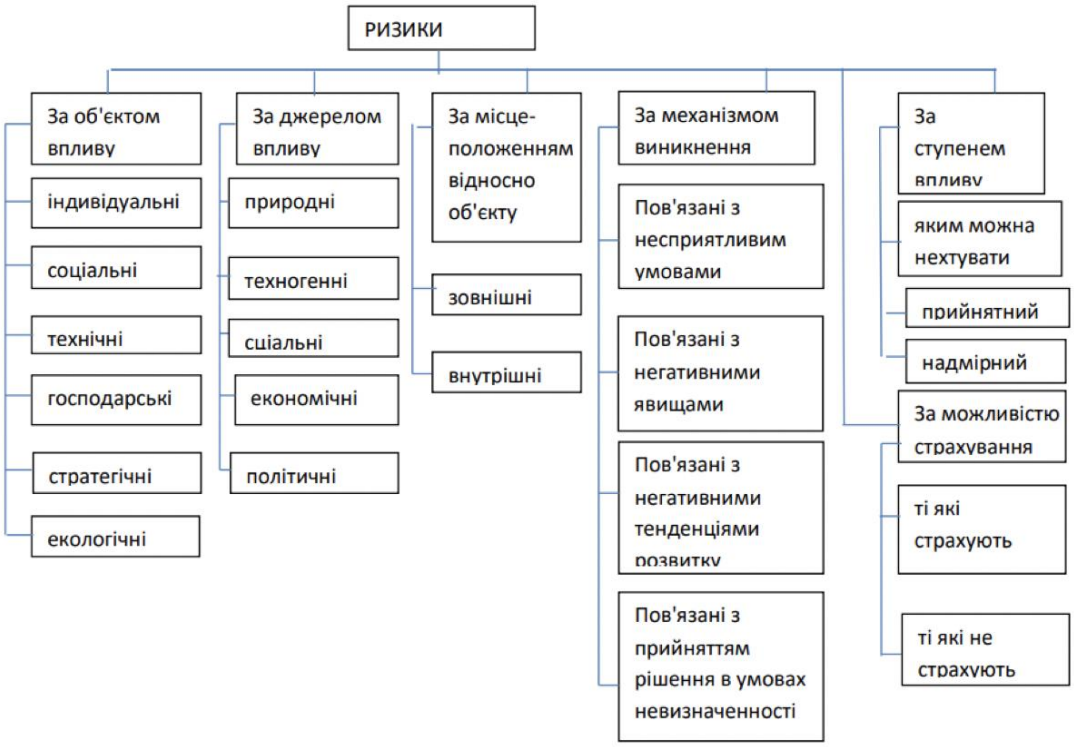

Рисунок 1.3 – Класифікація ризиків

На практиці особливу увагу приділяють саме технічним, соціальним та економічним ризикам, адже вони є найбільш поширеними в сфері ОБ. Наприклад, технічні ризики включають DDoS-атаки, збої в роботі серверів, проблеми з оновленнями програмного забезпечення; соціальні - фішинг, викрадення персональних даних через маніпуляції; економічні - втрати клієнтських коштів внаслідок шахрайських дій. Вони відрізняються як за джерелами виникнення, так і за механізмами впливу на цілісність і конфіденційність інформації.

Паралельно з класифікацією ризиків важливо систематизувати й методи їх оцінювання. У таблиці 1.4 наведено основні типи методів оцінки ризиків, які застосовуються в банківській сфері.

Таблиця 1.4

Класифікація методів оцінки ризиків

Критерій класифікації	**Типи методів**	**Короткий опис / приклади**
За характером підходу	Якісні	Експертна оцінка, SWOT-аналіз, метод сценаріїв. Оцінка суб'єктивна, базується на досвіді й інтуїції спеціалістів.
	Кількісні	Статистичні моделі, аналіз очікуваних втрат (Expected Loss), метод Монте-Карло. Використовуються числові дані та формули.
За джерелами даних	Фактологічні (емпіричні)	Аналіз історичних інцидентів, журналів подій, звітів безпеки.
	Прогнозні (моделювання)	Побудова моделей на основі можливих сценаріїв, трендів і припущень.
За рівнем деталізації	Макрорівень	Оцінка глобальних загроз, ризиків для всієї інфраструктури банку.
	Мікрорівень	Оцінка ризиків на рівні конкретного додатка, транзакції або користувача.
За часовим горизонтом	Поточна оцінка (ex-post)	Аналіз після інциденту - що вже сталося.

продовження таблиці 1.4

За суб'єктом оцінювання	Внутрішній аудит	Проводиться співробітниками банку.
	Зовнішній аудит	Незалежні компанії або аудитори (наприклад, під час сертифікації PCI DSS).
Спеціалізовані методи ІБ	STRIDE, DREAD, OCTAVE, FAIR, PASTA	Стандартизовані підходи в аналізі кіберризиків та уразливостей.

Таким чином, правильний вибір методики оцінки ризиків дозволяє зменшити потенційні збитки, уникнути правових наслідків та підвищити довіру клієнтів до цифрових сервісів.

1.4.2 Основні ризики за рівнями системи онлайн-банкінгу

Архітектура онлайн-банкінгу є багаторівневою і охоплює взаємодію між користувачем, банківською інфраструктурою та зовнішніми сервісами. Відповідно до функціональної ролі кожного рівня, змінюється і природа ризиків витоку конфіденційної інформації.

Клієнтський рівень вважається найуразливішим, оскільки не контролюється банком напряму. Компрометація відбувається через зараження пристрою або соціальну інженерію.

Канали зв’язку піддаються атакам у публічному середовищі, особливо при використанні нестійких конфігурацій TLS або вбудованих проксі.

Сервери автентифікації часто є цілями атак через помилки реалізації MFA або зберігання паролів у застарілих форматах.

Транзакційний рівень може стати точкою логічної атаки, якщо перевірка прав доступу не є контекстно-залежною.

HSM і сервіси підпису - критично важливі. Їх компрометація відкриває шлях до фальсифікації операцій.

API-шлюзи, особливо в умовах відкритого банкінгу (PSD2), мають ризик витоку через погано налаштовані політики доступу.

SIEM та журнали можуть містити непрямі персональні дані або бізнес-інформацію. Витік логів означає потенційне масштабування атаки.

У таблиці 1.5 узагальнено типові ризики, характерні для ключових рівнів системи ОБ.

Таблиця 1.5

Ризики витоку конфіденційної інформації за рівнями онлайн-банкінгу

Рівень системи	**Компоненти**	**Потенційні ризики**	**Приклади реалізації загроз**
Клієнтський інтерфейс	Вебзастосунок, мобільний застосунок	Компрометація облікових даних через фішинг; витік OTP через заражений пристрій; відсутність захисту сесії	Підробка інтерфейсу входу, кейлогери, викрадення токенів
Канал зв’язку	TLS-з’єднання, мобільна мережа, Wi-Fi	Підміна сертифікатів, протокол downgrade	Атаки через публічні Wi-Fi, невалідні сертифікати
Сервер автентифікації	Бекенд авторизації, СУБД користувачів	Недостатній захист паролів; вразливі механізми MFA	Використання слабких алгоритмів хешування

продовження таблиці 1.5

Сервер транзакцій	Обробник запитів, логіка бізнес-процесів	Некоректна перевірка прав доступу; можливість обману логіки транзакцій; зловживання API	Масштабування через API без авторизації, обхід RBAC
Бази даних	СУБД клієнтів, транзакційні БД	SQL-ін’єкції; витік резервних копій; надмірні права доступу	Атаки через web-інтерфейси, необмежене зчитування таблиць
API / шлюзи інтеграції	API Gateway, Open Banking інтерфейси	Витік токенів доступу; недостатній контроль дозволів сторонніх сервісів	Перевищення дозволів (over-privileged tokens), replay-атаки
HSM / КЕП-модулі	Апаратні криптомодулі, сертифікати	Компрометація приватних ключів; несанкціонований доступ до підпису транзакцій	Зберігання ключів без HSM; старі сертифікати без перевірки
Лог-сервери / SIEM	Агрегація подій, логування	Витік критичних журналів; відсутність контролю цілісності логів	Доступ до логів через вразливі веб-інтерфейси або API

Як видно з таблиці, кожен рівень архітектури системи має свої унікальні уразливості, що потребують окремих засобів контролю та захисту. Виявлення таких точок є критично важливим етапом для побудови ефективної системи управління інформаційними ризиками в ОБ.

1.5 Нормативно-правове забезпечення аналізу ризиків в інформаційній безпеці

Забезпечення ефективного управління ризиками в сфері ІБ неможливе без дотримання відповідних нормативних актів, міжнародних стандартів та галузевих рекомендацій. Ці документи визначають загальні принципи, методики та вимоги до організації процесів оцінювання, моніторингу та зниження ризиків ІБ у сфері електронних транзакцій.

1.5.1 Міжнародні стандарти

Одним з основоположних документів є стандарт ISO/IEC 27005:2022, який містить детальний опис процесу управління ризиками ІБ як частини загальної системи управління інформаційною безпекою (СУІБ). Його застосування забезпечує структурований і повторюваний підхід до аналізу ризиків, що адаптується до конкретних умов організації. Стандарт визначає ключові етапи: ідентифікацію активів, виявлення загроз і вразливостей, оцінку наслідків та ймовірностей, формування заходів реагування [9]. Застосування ISO/IEC 27005 особливо доцільне в середовищах з високим ступенем регуляторних вимог і складною багаторівневою архітектурою. Цей підхід дозволяє уніфікувати процес прийняття рішень щодо захисту конфіденційної інформації та формалізувати оцінку залишкових ризиків. Додатково, варто згадати такі міжнародні документи:

• ISO/IEC 27001:2022 - визначає вимоги до створення, впровадження та підтримки СУІБ [10];

• ISO/IEC 27002:2022 - містить практичні рекомендації щодо реалізації заходів безпеки [13];

• NIST SP 800-30 Rev.1 (Risk Management Guide for Information Technology Systems) - надає практичний підхід до аналізу ризиків у системах інформаційних технологій, включаючи кількісні й якісні методи [11].

1.5.2 Європейське регулювання

У сфері захисту персональних даних та управління інформаційними ризиками на території Європейського Союзу основоположним документом є Загальний регламент про захист даних (GDPR, Regulation (EU) 2016/679). Він запроваджує принципи "privacy by design" а "privacy by default"', що передбачають впровадження належного рівня безпеки вже на етапі проєктування інформаційних систем [14].

Згідно зі статтею 32 GDPR, контролери та оператори даних повинні реалізовувати технічні та організаційні заходи, що забезпечують рівень безпеки, адекватний ризику, з урахуванням:

• Потенційних наслідків для прав і свобод суб’єктів даних;

• Ймовірності настання інцидентів;

• Вразливостей інформаційної інфраструктури.

Важливо, що GDPR вимагає проведення оцінки впливу на захист даних (DPIA), якщо обробка даних може призвести до високих ризиків для прав і свобод осіб. Така оцінка є аналогом якісного аналізу ризиків і передбачає:

• Ідентифікацію загроз;

• Оцінку ймовірності та наслідків;

• Розробку пом’якшуючих заходів.

Цей підхід фактично інтегрує аналіз ризиків у правове поле та зобов’язує організації розглядати безпеку даних не як опцію, а як обов’язкову умову ведення діяльності. Таким чином, положення GDPR узгоджуються з підходами, закладеними у стандартах ISO/IEC та методиках NIST, забезпечуючи єдиний напрямок у регулюванні ризик-орієнтованої безпеки.

1.5.3 Банківське регулювання та галузеві підходи

У міжнародному контексті основу регуляторного підходу становлять вимоги Базельського комітету з банківського нагляду, викладені в документах Basel II та Basel III. Згідно з цими рамками:

- Інформаційні інциденти класифікуються як операційні ризики;
- Банки зобов'язані ідентифікувати джерела ризиків, включаючи кібератаки, витоки даних, технічні збої та людський фактор [15].

Basel II також підтримує підхід AMA (Advanced Measurement Approach), що дозволяє використовувати внутрішні моделі оцінки ризиків. Це заохочує фінансові установи розробляти власні методики збору даних про інциденти, сценарного моделювання, а також розрахунку ймовірностей та збитків.

В межах галузевих практик, міжнародні платіжні системи, такі як SWIFT, зобов'язують банки дотримуватися обов'язкової програми Customer Security Programme (CSP), яка включає:

- Щорічну самооцінку безпеки;
- Впровадження 23 контрольних заходів;
- Постійний моніторинг ризиків і вразливостей [16].

Крім того, існують наступні спеціалізовані банківські стандарти:

- PCI DSS - стандарт безпеки для обробки, зберігання та передачі даних платіжних карт;
- FFIEC Cybersecurity Assessment Tool - інструмент, рекомендований в США для оцінки кіберстійкості фінансових установ;
- Вимоги Національного банку України, зокрема Положення № 95, яке вимагає від банків реалізації системи управління ІБ, що базується на аналізі ризиків [17].

Таким чином, нормативна та галузева база створює багаторівневу архітектуру управління інформаційними ризиками в банківському середовищі, орієнтовану як на дотримання формальних вимог, так і на підвищення реальної стійкості систем до загроз.

Висновки за розділом 1

У першому розділі кваліфікаційної роботи було здійснено системний аналіз архітектури функціонування сучасних систем ОБ, визначено джерела обробки, зберігання та передачі конфіденційної інформації, класифіковано її за рівнем доступності згідно з вимогами чинного законодавства України та міжнародних стандартів у сфері ІБ. На основі дослідження функціональної структури онлайн-банкінгу проаналізовано її ключові компоненти: клієнтський інтерфейс, сервери автентифікації та обробки запитів, бази даних клієнтів і транзакцій, криптографічні модулі та API-шлюзи. Встановлено логіку циркуляції інформації між цими компонентами, що дозволило визначити критичні точки потенційного витоку КІ.

У роботі сформовано класифікацію ризиків за рівнями системи. Для кожного з них визначено типові механізми реалізації загроз, можливі наслідки витоку та приклади вразливих місць. У цьому контексті проаналізовано також нормативно-методичну базу, зокрема стандарти ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, а також керівництво NIST SP 800-30 Rev.1. Особлива увага приділена стандарту ISO/IEC 27005:2022, який забезпечує структурований і повторюваний підхід до аналізу ризиків, адаптований до конкретних умов функціонування інформаційної системи.

У результаті виконання першого етапу дослідження було проаналізовано особливості архітектури та функціонування ОБ, визначено та класифіковано основні джерела загроз витоку КІ, а також сформовано базис для подальшої оцінки методів аналізу ризиків. З урахуванням виявлених проблем і особливостей предметної області, у наступному розділі буде розглянуто сучасні підходи до оцінювання ризиків ІБ, а також їхню адаптивність до середовища ОБ. Це дозволить визначити, які з існуючих моделей можуть бути використані в умовах реальних банківських систем, і стане основою для розробки власної методики аналізу ризиків витоку КІ, що буде представлена в розділі 3.

РОЗДІЛ 2
ОСОБЛИВОСТІ ЗАСТОСУВАННЯ МЕТОДІВ АНАЛІЗУ РИЗИКІВ В СИСТЕМАХ ОНЛАЙН-БАНКІНГУ

2.1 Теоретичні засади аналізу інформаційних ризиків

Аналіз інформаційних ризиків є фундаментальним етапом управління ІБ, що дозволяє організаціям своєчасно виявляти потенційні загрози, оцінювати рівень небезпеки та приймати обґрунтовані рішення щодо впровадження заходів захисту.

У сучасних умовах цифровізації фінансового сектора, особливо в контексті ОБ та електронних транзакцій, аналіз ризиків повинен враховувати не лише технічні аспекти, а й організаційні, правові та поведінкові чинники.

Теоретичні засади аналізу ризиків ІБ базуються на низці міжнародних стандартів, зокрема ISO/IEC 27001 та ISO/IEC 27005. Відповідно до положень цих документів, процес аналізу ризиків включає такі етапи:

- Визначення контексту аналізу - ідентифікація цілей організації, структури ІБ, правових і нормативних вимог, а також обсягів і типів інформаційних активів, що підлягають захисту;
- Ідентифікація ризиків - виявлення активів, потенційних загроз і відповідних вразливостей, які можуть бути використані для реалізації цих загроз;
- Оцінка ризиків - визначення ймовірності реалізації кожного ризику та оцінка можливих наслідків у разі його настання. Застосовуються як якісні, так і кількісні підходи;
- Порівняння ризиків з критеріями прийнятності - визначення того, які ризики потребують негайного реагування, а які можуть бути прийнятними;
- Документування та моніторинг ризиків - регулярне оновлення результатів аналізу та контроль змін у середовищі загроз.

Ключовим поняттям у теорії аналізу ризиків є ризик-орієнтований підхід (risk-based approach), який передбачає впровадження заходів захисту

пропорційно до рівня визначеного ризику. Це дозволяє оптимізувати використання ресурсів і зосередити зусилля на найбільш критичних напрямках.

У рамках аналітичного процесу також використовується карта ризиків - інструмент для візуального представлення і ранжування ризиків за рівнем впливу та ймовірністю. Вона дозволяє сформувати пріоритети в реалізації політики безпеки.

Теоретичні положення аналізу ризиків також враховують зміну середовища функціонування ІС, розвиток нових типів загроз і технологій атак. Тому оцінювання ризиків повинно бути регулярним і циклічним, забезпечуючи своєчасне оновлення заходів захисту. Цей підхід формує динамічну модель безпеки, що адаптується до змін у внутрішньому й зовнішньому середовищі.

2.2 Методи аналізу ризиків витоку інформації

Методи аналізу ризиків ІБ є інструментами для виявлення, класифікації та оцінювання ризиків, що виникають у процесі функціонування інформаційних та ІКС. Їх застосування дозволяє організаціям обґрунтовано приймати рішення щодо доцільності впровадження певних заходів захисту, оптимізуючи витрати та підвищуючи рівень безпеки.

Методи аналізу ризиків поділяються на якісні, кількісні та змішані (комбіновані). Кожен підхід має власні переваги та сфери застосування.

Якісні методи передбачають експертну оцінку ризиків на основі описового аналізу без використання точних числових значень. Основна мета - визначити відносний рівень ризику (низький, середній, високий).

До найпоширеніших якісних методів належать :

• SWOT-аналіз - оцінка сильних і слабких сторін системи безпеки, а також можливостей і загроз із боку зовнішнього середовища;

• Метод контрольних списків - виявлення потенційних проблем на основі заздалегідь визначених критеріїв;

• Оцінка за матрицею ризиків - побудова двовимірної таблиці з ймовірністю реалізації ризику та ступенем його впливу.

Перевагами якісних методів є простота застосування та швидке отримання загальної картини. Проте вони не дозволяють точно оцінити фінансові чи операційні наслідки реалізації ризиків.

Кількісні методи ґрунтуються на числовій оцінці параметрів ризику та використовуються для більш точного прогнозування потенційних збитків. Такі методи дозволяють оцінювати ефективність різних заходів захисту з економічної точки зору. Їх застосування особливо актуальне в умовах обмежених ресурсів та необхідності обґрунтування витрат на ІБ.

Серед основних кількісних методів:

• ALE (Annual Loss Expectancy) - оцінка очікуваних щорічних втрат від конкретного ризику;

• Метод Монте-Карло - застосовується для моделювання множинних сценаріїв на основі випадкових змін параметрів ризику;

• Аналіз дерева рішень - графічне представлення альтернатив управління ризиками з урахуванням ймовірності та очікуваних наслідків.

Кількісні методи забезпечують більшу обґрунтованість, проте вимагають точних вхідних даних, які не завжди доступні.

У сучасній практиці широко використовуються комплексні моделі, що поєднують якісні та кількісні оцінки. Прикладами є:

• OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - методика, яка включає ідентифікацію активів, загроз і вразливостей, а також визначення пріоритетів захисту;

• STRIDE - модель Microsoft для класифікації загроз (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) ;

• DREAD - система оцінки ризиків за п’ятьма критеріями: масштаб шкоди, відтворюваність атаки, простота експлуатації, кількість уражених користувачів, виявлення;

• FAIR (Factor Analysis of Information Risk) - структурований підхід до кількісного аналізу інформаційних ризиків, орієнтований на оцінку втрат та ймовірності.

Для порівняльної характеристики розглянутих методів аналізу ризиків доцільно узагальнити їх ключові особливості у табличній формі (табл. 2.1).

Таблиця 2.1

Порівняння методів аналізу ризиків ІБ

Метод	**Тип аналізу**	**Ключові характеристики**	**Переваги**	**Недоліки**
1	2	3	4	5
Матриця ризиків	Якісний	Побудова шкали впливу таймовірності подій	Простота, візуалізація	Суб’єктивність оцінки
SWOT-аналіз	Якісний	Оцінка сильних/слабких сторін, можливостей, загроз	Комплексний підхід	Не дає кількісної оцінки ризиків
ALE	Кількісний	Розрахунок очікуваних щорічних збитків	Конкретність, фінансове обґрунтування	Потребує точних даних
Метод Монте-Карло	Кількісний	Імітаційне моделювання сценаріїв	Гнучкість, точність	Складність реалізації, велика кількість даних
OCTAVE	Змішаний	Ідентифікація активів, загроз, вразливостей, оцінка ризиків	Системний підхід, орієнтований на організацію	Трудомісткість

продовження таблиці 2.1

1	2	3	4	5
STRIDE	Змішаний	Класифікація загроз за типами (спуфінг, модифікація тощо)	Підходить для IT-систем і ПЗ	Не оцінює фінансовий ризик
DREAD	Змішаний	Оцінювання шкоди, відтворюваності, простоти атаки тощо	Напівформалізована шкала	Певна суб'єктивність
FAIR	Змішаний (з ухилом у кількісний)	Формалізований підхід до оцінки ймовірності та втрат	Висока точність, орієнтація на бізнес-ризики	Потребує навчання і глибокого розуміння моделі

Як видно з таблиці, кожен метод має свої переваги та обмеження. Вибір конкретного підходу залежить від цілей аналізу, наявних ресурсів, рівня підготовки фахівців та специфіки системи ОБ.

2.2.1 Метод STRIDE

Модель STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) була запропонована корпорацією Microsoft як інструмент систематизації загроз у процесі розробки безпечних інформаційних систем [18]. Її основна концепція полягає в класифікації кожної потенційної загрози за однією з шести категорій, які охоплюють усі ключові аспекти ІБ - конфіденційність, цілісність, доступність, автентичність і контроль дій.

У системах ОБ STRIDE доцільно застосовувати на етапі проєктування архітектури, особливо при побудові компонентів веб- та мобільного застосунку, API-шлюзів і систем автентифікації. Наприклад, загроза підміни особи може реалізовуватися через фішингові інтерфейси або підроблені TLS-сертифікати, а загруза витоку інформації - через незахищені параметри у HTTP-запитах або недостатній контроль доступу до логів [19].

Особливістю методу є його сумісність із побудовою діаграм потоків даних (Data Flow Diagrams), які дозволяють візуалізувати пункти передачі, обробки та зберігання даних. Наприклад, при моделюванні API-запиту з мобільного додатку до серверу банку можна визначити потенційні загрози підміни параметрів транзакції, відсутності цифрового підтвердження дії та використанні токена з розширеними правами.

Слабкою стороною STRIDE є відсутність можливостей для кількісної оцінки ризиків та економічного обґрунтування впровадження засобів захисту. Метод не враховує ймовірність реалізації загрози або масштаб фінансових наслідків. Водночас, STRIDE ефективно інтегрується як початковий етап моделювання загроз у рамках складніших методик, таких як FAIR або NIST RMF [18], [9].

У найпростішому вигляді результат STRIDE-аналізу може бути представлений у формі матриці загроз, де кожній загрозі присвоюється суб’єктивна оцінка ймовірності реалізації та очікуваного впливу. Навіть без точних числових значень такий підхід дозволяє здійснити пріоритезацію ризиків (формула 2.1).

$$R_i = P_i \times C_i, i = \overline{1,n}\ , \qquad (2.1)$$

де R_i - зважене значення ризику для загрози;

P_i - суб’єктивна оцінка ймовірності реалізації;

C_i - очікуваний вплив;

n - загальна кількість виявлених загроз.

Наприклад, у випадку спрощеної автентифікації без двофакторного захисту значення P (ймовірність успішного spoofing-нападу) може бути високим, а значення C (наслідки) - критичним, оскільки компрометація облікового запису може дати повний доступ до рахунку клієнта.

Таким чином, метод STRIDE доцільно застосовувати на етапах технічного проєктування систем онлайн-банкінгу для виявлення архітектурних та логічних вразливостей, пов’язаних із взаємодією з кінцевим користувачем, каналами передачі та логікою авторизації. Його використання формує підґрунтя для подальшої кількісної оцінки в рамках більш формалізованих моделей.

2.2.2 Метод FAIR

Методика FAIR (Factor Analysis of Information Risk) є однією з небагатьох формалізованих моделей, що забезпечують кількісну оцінку інформаційних ризиків. Вона була запропонована FAIR Institute та рекомендована до застосування провідними організаціями, зокрема NIST, ISACA, Open Group і ISO [20], [9]. Основна мета методу - надати управлінцям і фахівцям з ІБ інструмент, здатний виміряти ймовірність реалізації загрози та її вплив у грошовому вираженні.

Модель базується на розкладанні ризику на базові змінні. Формально, ризик у FAIR описується через втрату, зумовлену подією (формула 2.2).

$$\text{Ризик} = \text{LEF} \times \text{PLM}\ , \qquad (2.2)$$

де LEF - частота виникнення події втрати;

PLM - очікуваний розмір збитків у разі реалізації події.

Частота виникнення події втрати своєю чергою, залежить від контактів загрози з активом і ймовірності успішної реалізації (формула 2.3).

$$\text{LEF} = TEF \times V\ , \qquad (2.2)$$

де TEF - частота контактів загрози з активом;

V - ймовірність успішної реалізації.

Очікуваний розмір збитків у разі реалізації події складається з чотирьох компонентів: первинні фінансові збитки, витрати на відновлення, штрафи та вторинні наслідки (втрата довіри, додаткові перевірки тощо). У моделі допускається використання як точкових, так і інтервальних оцінок (наприклад, через Monte Carlo симуляцію або діапазон ймовірностей) [20].

У системах ОБ FAIR забезпечує практичний інструментарій для обґрунтування витрат на впровадження засобів захисту. Наприклад, при оцінці загрози витоку даних через сторонній API-запит банк може оцінити:

- кількість потенційних інцидентів на рік;
- ймовірність того, що атака буде успішною через вразливість;
- очікувані прямі втрати від витоку, включаючи компенсації клієнтам, штрафи, юридичні витрати.

До сильних сторін методу належить його узгодженість зі стандартами ISO/IEC 27005:2022 та NIST SP 800-30 Rev.1, підтримка кількісної та ймовірнісної логіки, орієнтація на економічну оцінку ризику. Метод легко інтегрується в загальну систему управління ІБ в організації, є придатним для аудиту та фінансового звітування.

Недоліком FAIR є потреба у достатньо точних даних для розрахунків, що не завжди можливо у нових або малих системах. Також він потребує спеціалізованої підготовки фахівців і доступу до аналітичного інструментарію.

Таким чином, FAIR є однією з небагатьох моделей, що дозволяють перейти від якісного до кількісного управління інформаційними ризиками в системах ОБ. У контексті складної багатокомпонентної архітектури, необхідності відповідати регуляторним вимогам і обмежених бюджетів на ІБ, цей підхід дає змогу приймати стратегічні рішення на основі оцінених імовірностей і фінансових наслідків.

2.2.3 Метод OCTAVE

Метод OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) був розроблений як структурована методика якісного аналізу ризиків

ІБ для критично важливих активів організації [21]. На відміну від технікоорієнтованих підходів (STRIDE) або суто економікоорієнтованих (FAIR), OCTAVE фокусується на комплексному аналізі вразливостей, які залежать як від технічних умов, так і від організаційного середовища.

У межах системи ОБ, OCTAVE доцільно застосовувати на рівні корпоративного аудиту ІБ, а також при розробці середньо- та довгострокових стратегій захисту даних. Методика охоплює три фази:

1. Ідентифікація активів, що мають критичну цінність (дані клієнтів, транзакційні записи, криптографічні ключі).
2. Виявлення загроз, вразливостей та слабких сторін управління ІБ (наприклад, відсутність контролю доступу до резервних копій).
3. Формування плану дій і визначення пріоритетності заходів реагування.

У практиці ОБ OCTAVE добре себе зарекомендував під час:

- впровадження СУІБ відповідно до вимог ISO/IEC 27001;
- підготовки до аудиту НБУ або міжнародних аудитів;
- оцінки політик контролю доступу та збереження даних [5].

Модель не є кількісною: всі оцінки здійснюються на основі експертних інтерв'ю, анкетування, аналізу документації, що унеможливлює пряме фінансове прогнозування наслідків. Водночас це надає гнучкість в умовах обмеженої статистики, яка часто характерна для банків малого та середнього масштабу.

Методика формує матрицю ризиків, що відображає вплив загроз на активи, при цьому інтегруючи організаційний, технічний та людський аспекти. У спрощеному вигляді, результат оцінки ризику для активу можна подати за формулою 2.3.

$$R_j = \mathrm{f}(S_j, T_j, V_j)\ , \qquad (2.3)$$

де S_j - ступінь важливості активу;

V_j - наявність вразливостей у відповідних зонах ІТ-інфраструктури;

T_j - перелік релевантних загроз;

Найбільше методика OCTAVE підходить для внутрішнього IT-менеджменту, розробки політик доступу, аналізу ефективності адміністративних заходів, а також моніторингу відповідності внутрішніх процесів до ISO/IEC 27001:2022. У комбінації з іншими підходами, вона дозволяє побудувати цілісну систему оцінювання та реагування на ризики.

Завдяки орієнтації на організаційні процеси та активну участь персоналу, OCTAVE виявляється особливо ефективною в умовах банків із розгалуженою структурою доступу та складною регламентною політикою.

Таким чином, OCTAVE в ОБ виконує роль організаційно-методичного каркасу, який надає змогу охопити не лише IT-інфраструктуру, а й людський фактор, політики, процедури й культуру безпеки в установі.

2.2.4 Метод DREAD

Модель DREAD є однією з класичних методик оцінки ризиків, розроблених для суб'єктивної оцінки критичності загроз, що можуть бути виявлені під час моделювання атак [22]. Назва моделі є акронімом п'яти ключових критеріїв: Damage potential (шкода), Reproducibility (повторюваність), Exploitability (простота експлуатації), Affected users (кількість постраждалих), Discoverability (виявлюваність загрози).

Кожному критерію присвоюється оцінка за шкалою (найчастіше від 1 до 10), після чого обчислюється середнє значення за формулою 2.4.

$$R_i = \frac{D_i + R_{P_i} + E_i + A_i + D_{V_i}}{5}, \qquad (2.4)$$

де R_i - підсумковий бал ризику для загрози i;

D_i - оцінка шкоди (Damage potential);

R_{P_i} - оцінка повторюваності (Reproducibility);

E_i - оцінка простоти реалізації (Exploitability);

A_i - кількість постраждалих користувачів (Affected users);

D_{V_i} - вірогідність виявлення (Discoverability).

DREAD може застосовуватися для оцінки конкретних атак на мобільні та веб-застосунки, включно з атаками на API, уразливості автентифікації або витоки персональних даних.

Метод має низку переваг для практичного застосування в ОБ:

- дозволяє здійснювати швидку оцінку ризиків у прикладних системах;
- підходить для порівняльного аналізу атак;
- легко реалізується в середовищі Secure Development Lifecycle (SDL) [22].

Основні обмеження DREAD - це його суб'єктивність, залежність від досвіду експертів, а також відсутність економічної або правової оцінки наслідків, що обмежує його застосовність для прийняття стратегічних управлінських рішень.

DREAD може бути особливо корисним для DevSecOps-команд банків, які відповідають за безпеку клієнтського застосунку або сервісної логіки. У поєднанні з STRIDE або CVSS він може використовуватись як інструмент оперативної класифікації загроз, у тому числі для щотижневого тріажу знайдених вразливостей.

2.2.5 Метод NIST RMF

Методика Risk Management Framework (RMF), розроблена NIST, є комплексною рамковою моделлю для впровадження процесу управління ризиками в інформаційних системах [11]. Її ключова особливість полягає в поетапному підході, що охоплює весь життєвий цикл системи ОБ - від категоризації інформаційних ресурсів до моніторингу залишкового ризику після впровадження контрзаходів.

У редакції NIST SP 800-37 Rev. 2 [23] процес RMF охоплює сім етапів, які взаємопов'язані з вимогами стандартів ISO/IEC 27001, 27005, а також практиками управління ITIL та COBIT. Ці етапи включають:

1. Категоризацію інформаційних активів;
2. Вибір заходів контролю безпеки;
3. Впровадження обраних засобів захисту;
4. Оцінку їхньої ефективності;
5. Прийняття рішення щодо залишкового ризику;
6. Авторизацію (акредитацію) системи;
7. Безперервний моніторинг безпеки.

RMF дозволяє інтегрувати ризик-орієнтовану безпеку в бізнес-процеси. Наприклад, після виявлення ризику витоку КЕП на етапі оцінки, організація може змінити порядок генерації ключів, задіяти HSM-модуль і забезпечити контроль журналів операцій у режимі реального часу.

У методиці передбачено використання як якісних, так і кількісних оцінок ризиків, що дозволяє її адаптувати до специфіки банку: від невеликої установи до великої фінансової групи. Показник ризику для компонента системи можна розрахувати як добуток ймовірності загрози на рівень потенційного впливу, з урахуванням рівня залишкового ризику (формула 2.5).

$$\mathrm{R} = (\mathrm{P} \times \mathrm{C}) - M\,, \qquad (2.5)$$

де P - ймовірність реалізації загрози;

C - очікуваний вплив на актив;

M - ефективність застосованого контрзасобу.

На рисунку 2.1 представлено загальну концептуальну модель управління ризиками, що узгоджується з підходами RMF. У ній відображено зв’язок між ключовими елементами: стратегічним управлінням (на рівні ради директорів та менеджменту), ризик-орієнтованим плануванням, операційною реалізацією заходів безпеки та зворотним контролем за станом ризиків у динаміці.

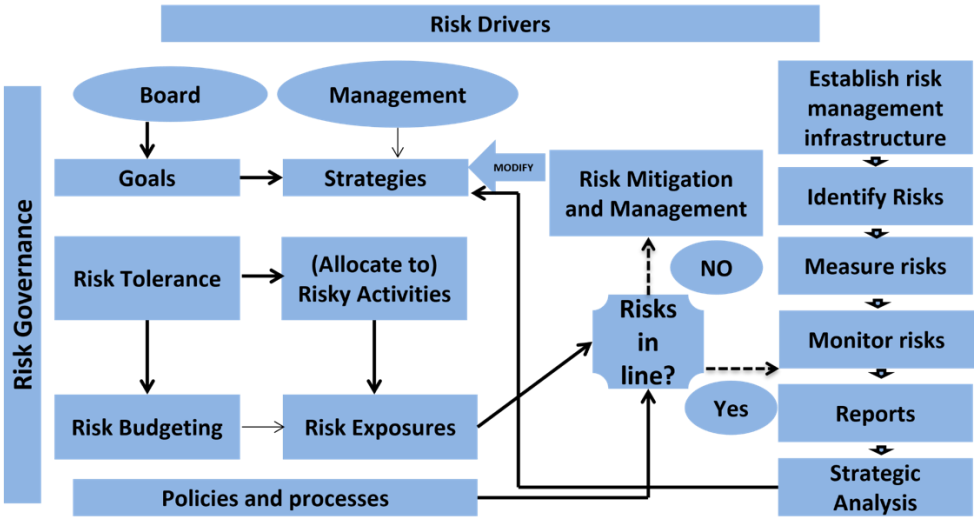

Рисунок 2.1 – Інтегрована модель управління ризиками RMF

Модель чітко демонструє, що процес управління ризиками не є лінійним, а складається з циклічних етапів: ідентифікації, вимірювання, моніторингу та аналізу ризиків, а також прийняття рішень щодо їх допустимості або необхідності коригування стратегії. Особливе значення надається рівню «Risk Governance», який регламентує цілі, допуски, бюджети та політики - тобто той шар, що формує рамку безпеки на рівні всього банку.

Основними недоліками є складність впровадження, потреба у спеціалізованій команді та тривалість повного циклу оцінки. Водночас саме RMF часто є основою для побудови систем захисту в державних і комерційних фінансових установах, особливо в США, Канаді, країнах ЄС, а також при участі в проектах із зовнішнім фінансуванням або аудитом за стандартами Basel II/III.

Таким чином, RMF доцільно використовувати як організаційний каркас управління ризиками на рівні всієї IT-інфраструктури ОБ, особливо у випадках масштабування систем, інтеграції з новими сервісами, та в проектах з високими вимогами до аудиту.

2.3 Критерії ефективності методів аналізу ризиків у системах онлайн-банкінгу

Системи ОБ функціонують у середовищі підвищеної динаміки загроз, високої регуляторної відповідальності та вимог до стійкості до інцидентів.

Ефективність методів аналізу ризиків у такому середовищі визначається не лише точністю оцінки, а й здатністю до адаптації, практичного застосування, підтримки прийняття управлінських рішень та інтеграції з існуючими системами ІБ.

Зростання складності архітектур, активне використання відкритих інтерфейсів та мобільних клієнтських застосунків посилює вимоги до гнучкості та деталізації моделей ризику. Банківські установи дедалі частіше стикаються з потребою у методах, здатних забезпечити як стратегічне планування, так і оперативне реагування.

Саме тому формування комплексного критеріального підходу до оцінки методів стає ключовим для забезпечення релевантності й практичності обраного рішення.

Для обґрунтованого вибору або комбінування методів доцільно застосовувати систему оцінки за критеріями, які охоплюють як технічні, так і організаційні аспекти:

- Ступінь формалізації - наскільки метод має чітко визначені процедури, алгоритми чи формули;
- Підтримка кількісної оцінки - можливість оцінити ризики в числовому або економічному вигляді;
- Відповідність нормативним вимогам - здатність інтегруватися у СУІБ відповідно до стандартів;
- Адаптивність до специфіки банківської ІКС - можливість урахування мобільних клієнтів, API, криптографічних механізмів тощо;
- Масштабованість - придатність методу для установ з різними обсягами активів і складністю систем;
- Інтеграція в життєвий цикл розробки - можливість використання у DevSecOps, CI/CD, SDL-процесах;
- Простота впровадження та інтерпретації результатів - зрозумілість висновків для нефахових користувачів.

У таблиці 2.2 представлено порівняльну оцінку розглянутих методів за зазначеними критеріями у шкалі від 0 до 3, де 0 - відсутня властивість, 1 - часткова реалізація, 2 - середній рівень, 3 - повна відповідність.

Таблиця 2.2

Порівняння методів аналізу ризиків за критеріями релевантності

Метод	**Формалізація**	**Кількісність**	**Відповідність ISO/NIST**	**Адаптація до ОБ**	**Масштабованість**	**DevSecOps/SDL**	**Простота впровадження**
1	2	3	4	5	6	7	8
STRIDE	2	0	2	3	2	3	2
FAIR	3	3	3	3	3	1	1
OCTAVE	2	1	3	2	3	0	2
DREAD	1	1	1	2	2	3	3
NIST RMF	3	2	3	3	3	1	1

Аналіз таблиці свідчить, що найбільш збалансованими за всіма критеріями є FAIR та NIST RMF, які забезпечують не лише повноту охоплення ризиків, а й економічну інтерпретацію їхніх наслідків. Метод STRIDE виявляється оптимальним для операційного рівня (включення у процес розробки й моделювання загроз), тоді як OCTAVE та DREAD доцільно застосовувати в середовищах із сильною управлінською або DevSecOps-культурою.

Таким чином, жоден з методів не є універсальним, однак їх поєднання у багаторівневому підході до аналізу ризиків дозволяє створити комплексну

модель, що охоплює всі рівні управління - від аудиту до стратегічного планування.

Висновки за розділом 2

У другому розділі кваліфікаційної роботи було розглянуто і системно проаналізовано основні методи оцінки ризиків в системах ОБ. Деталізовано п’ять провідних підходів - STRIDE, FAIR, OCTAVE, DREAD і NIST RMF - з урахуванням архітектурних, регуляторних та практичних вимог, характерних для банківського цифрового середовища.

Оцінювання здійснювалося з позицій формалізації, відповідності міжнародним стандартам, наявності кількісної складової, а також здатності до інтеграції у життєвий цикл ІС. Показано, що кожен з розглянутих методів має окремі переваги та обмеження, які зумовлюють доцільність їх застосування у різних сценаріях - від проєктування клієнтських додатків до стратегічного управління залишковим ризиком у масштабах банку. Зокрема, метод STRIDE є ефективним для виявлення технічних загроз на етапі розробки, OCTAVE - для внутрішнього аудиту та аналізу організаційних вразливостей, FAIR - для економічно орієнтованої оцінки ризиків, тоді як RMF виступає як універсальний рамковий підхід для побудови процесів управління ризиками в межах усієї установи.

Проведена порівняльна оцінка методів дозволила сформувати базу для виконання наступного завдання дослідження - обґрунтування і створення власного підходу до аналізу ризиків витоку КІ в системах ОБ. Враховуючи складність циркуляції даних, багаторівневу архітектуру банківських систем та високу чутливість оброблюваної інформації, виникає необхідність синтезу гібридного методу, який би поєднував кількісну оцінку, моделювання технічних загроз та врахування організаційних чинників.

У третьому розділі буде представлено розроблений підхід, що враховує результати попереднього аналізу та спрямований на забезпечення ефективного й адаптивного управління ризиками витоку КІ в ОБ.

РОЗДІЛ 3
РОЗРОБКА ТА ВПРОВАДЖЕННЯ МЕТОДУ АНАЛІЗУ РИЗИКІВ І ЗАХОДІВ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В СИСТЕМАХ ОНЛАЙН-БАНКІНГУ

3.1 Мета, вимоги та завдання методу

Сучасні системи ОБ функціонують у високодинамічному середовищі, де циркулює значна кількість критичної інформації, включаючи персональні дані, банківські реквізити, криптографічні ключі, платіжні транзакції тощо. Згідно з дослідженнями ENISA [24], саме системи дистанційного банкінгу є однією з найбільш уразливих ланок фінансового сектора, оскільки поєднують в собі мобільність, глибоку інтеграцію з іншими сервісами (API, інтернет-платежі), а також відкритість до масового користувача. З огляду на це, актуальним є завдання створення спеціалізованої методики аналізу ризиків витоку КІ, яка враховуватиме не лише класичні технічні загрози, а й специфіку обробки даних в ОБ.

Метою методу є забезпечення адаптивної, формалізованої та практично орієнтованої моделі аналізу ризиків витоку КІ в архітектурах систем ОБ, яка дозволяє враховувати як критичність активу, так і особливості його циркуляції та вразливість до зовнішнього впливу. На відміну від існуючих підходів, метод не обмежується фіксованим списком загроз або експертною оцінкою, а пропонує обчислювальну модель, засновану на індексах критичності (ASI), ймовірності реалізації ризику (RRI) та множинності або відкритості обробки активу (DCE).

Основні вимоги до розроблюваного методу включають:

- здатність формалізувати і обчислювати ризик для кожного сегменту обробки даних на основі прозорих критеріїв;
- гнучкість у застосуванні до різних типів активів (аутентифікаційні токени, API-запити, сесійні ключі, запити до БД);

- підтримку інтеграції в процедури внутрішнього аудиту, технічного моделювання та оцінки залишкового ризику згідно з ISO/IEC 27005:2022 [9];

- можливість масштабування для банківських установ різного типу - від невеликих регіональних до транснаціональних.

У межах реалізації методу ARC-Bank вирішуються такі завдання:

1. Побудова концептуальної моделі циркуляції даних в ОБ з ідентифікацією точок, де формується або обробляється КІ;
2. Визначення шкал для індексів ASI (Asset Sensitivity Index), RRI (Risk Realization Index) та DCE (Data Circulation Exposure) з урахуванням технологічних, організаційних і нормативних факторів;
3. Розробка інтегрованої формули обчислення ризику для кожної оброблюваної сутності та сукупного ризику по системі;
4. Побудова алгоритму застосування методу до конкретної банківської архітектури;
5. Проведення порівняльної апроксимації результатів з існуючими методами у контексті виявлення переваг і недоліків.

Таким чином, розроблюваний метод є не лише інструментом оцінки ризику, а концептуальною моделлю мислення в площині захисту КІ, яка враховує багатоступеневу логіку її обробки, реальні вектори атак і технологічну реалізацію системи ОБ. Саме ця модель буде детально розглянута і формалізована у наступному підпункті.

3.2 Архітектура та логіка функціонування методу

Запропонований метод базується на принципі поетапного аналізу КІ в точках її обробки в межах архітектури системи ОБ. В основі підходу лежить гіпотеза про те, що ризик витоку інформації не є сталою величиною, а формується як результат взаємодії критичності активу, його технічної вразливості та складності маршруту циркуляції у системі.

На рисунку 3.1 представлено архітектурну модель функціонування методу, яка відображає послідовну обробку даних у ключових функціональних зонах

системи ОБ. Кожен блок відповідає окремому логічному рівню, через який проходить КІ.

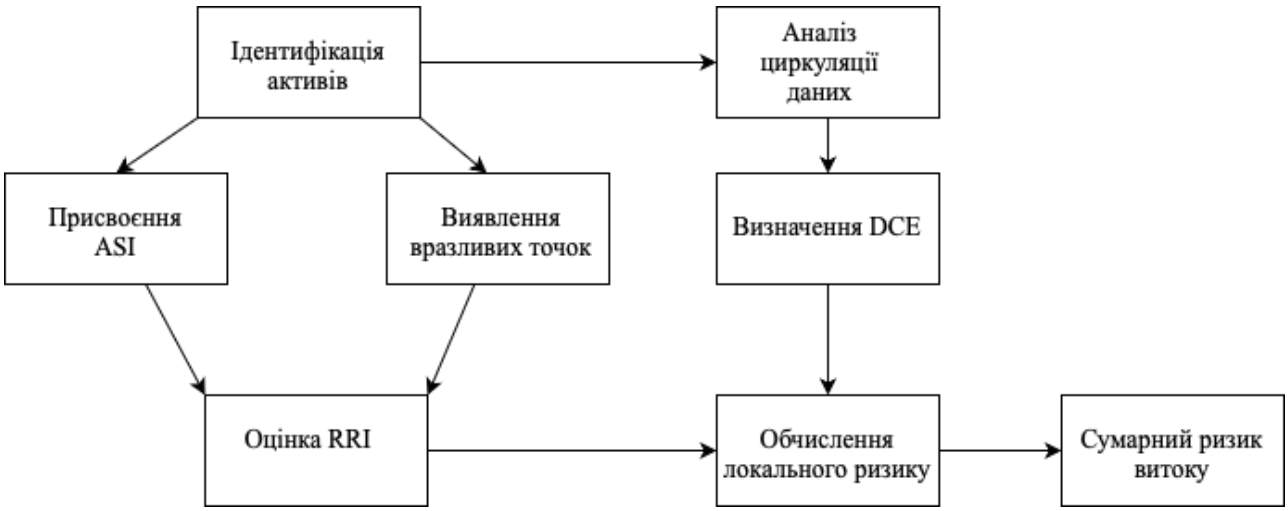

Рисунок 3.1 – Концептуальна схема методу

Як видно з рисунка, метод охоплює 8 основних етапів, які умовно розділено на два рівні: верхній рівень обробки (взаємодія з користувачем, комунікації, API) та внутрішній рівень обробки (сховище, журнали, криптографічна інфраструктура). У кожній точці аналізується:

- Оцінка критичності активу (ASI). Наприклад, автентифікаційний токен матиме ASI = 5, а заголовок запиту - ASI = 2;

- Ймовірність реалізації загрози в даній точці (RRI). Визначається на основі типових атак, наявності контрзаходів і історії інцидентів;

- Множинність обробки активу (DCE) - визначає, скільки копій або точок доступу до нього існує. Наприклад, дані, які дублюються у логах і кешах, мають DCE = 3.

Кожен з індексів визначається незалежно, що дозволяє адаптувати метод як до ручного аудиту, так і до автоматизованих систем моніторингу.

Узагальнений ризик обчислюється як добуток трьох індексів, що забезпечує прозорість розрахунку й можливість локалізації найуразливіших точок у системі.

Результатом оцінки є інтегральна формула 3.1.

$$R_{total} = \sum_{i=1}^{n} ASI_i \times RRI_i \times DCE_i \,, \qquad (3.1)$$

де ASI - оцінка критичності активу;

RRI - ймовірність реалізації загрози в даній точці;

DCE - множинність обробки активу.

Ця формула дає змогу побудувати матричну модель ризику, в якій кожен компонент системи ОБ оцінюється окремо, а результат - агрегується у загальний рівень ризику витоку КІ в системі.

Метод орієнтований на використання в середовищі DevSecOps або аудиті СУІБ, де він може бути вбудований як блок до оцінки ризику за ISO/IEC 27005:2022. Його перевага полягає у здатності виявляти критичні точки без введення повної моделі загроз, надавати кількісні результати на базі формалізованих індексів, адаптуватися до будь-якої банківської архітектури шляхом зміни набору точок циркуляції.

Завдяки архітектурній незалежності та модульному підходу даний метод може бути застосований у банках з різним рівнем цифрової зрілості - від традиційних веб-застосунків до API-орієнтованих платформ, хмарних сервісів і мобільних клієнтів.

3.3 Формалізація індексів методу

Метод базується на формалізованій оцінці локального ризику витоку конфіденційної інформації у кожній точці її циркуляції. Кожен об’єкт оцінювання (актив або операція з ним) характеризується трьома незалежними індексами: ASI (оцінка критичності активу), RRI (ймовірність реалізації загрози в даній точці) та DCE (множинність обробки активу).

Наведені нижче шкали розроблено з урахуванням практик ENISA, OWASP, ISO/IEC 27005 та рекомендацій НБУ. Такий підхід дозволяє врахувати як технічні характеристики середовища, так і реальні маршрути обробки конфіденційних даних в онлайн-банкінгу.

3.3.1 Оцінка критичності активу (ASI)

Значення ASI має визначатися у співпраці між фахівцями з інформаційної безпеки та власниками активів. Коректно присвоєний індекс критичності є основою для подальшої об’єктивної оцінки ризику. Індекс ASI визначає критичність активу - ступінь шкоди у разі його витоку або компрометації. Його значення присвоюється з урахуванням:

- категорії даних (загальнодоступна, службова, конфіденційна, критична);
- контексту використання;
- вимог регуляторів.

Шкалу для оцінювання ASI наведено в таблиці 3.1, де розмежовано п’ять рівнів критичності - від загальнодоступної інформації до ключових елементів безпеки.

Таблиця 3.1

Шкала ASI

Значення	**Критерій оцінки**	**Приклад**
1	Публічна або службова інформація	Статична HTML-сторінка банку
2	Внутрішня інформація з обмеженим доступом	Конфігурація клієнтського застосунку
3	Персональні або платіжні дані	ПІБ, номер картки
4	Інформація, що підпадає під регулювання	Паролі, сервіси авторизації
5	Ключові елементи системи безпеки	Приватні ключі, КЕП, сесійні токени

3.3.2 Ймовірність реалізації загрози в точці (RRI)

RRI показує ймовірність успішної реалізації загрози в конкретній точці обробки або циркуляції даних. Визначається за такими параметрами:

- наявність відомих вразливостей;
- історія інцидентів;
- захищеність каналу;
- контроль доступу, моніторинг, шифрування.

Залежно від рівня захищеності, активу присвоюється значення RRI в діапазоні від 0 до 1, як показано у таблиці 3.2.

Таблиця 3.2

Шкала RRI

Значення	**Інтерпретація**	**Приклад**
0.1	Дуже низька ймовірність	Захищений HSM з апаратною автентифікацією
0.3	Низька	Внутрішній API з контролем доступу
0.5	Середня	Веб-форма з TLS, без MFA
0.7	Висока	Зовнішній API без обмежень
0.9	Дуже висока	Публічна зона без шифрування

3.3.3 Множинність обробки активу (DCE)

DCE - індекс, що показує ступінь відкритості або багатоетапності циркуляції даних. Визначається кількістю:

- систем або компонентів, через які проходить актив;
- копій активу (в логах, кешах, резервних копіях);

- відкритих інтерфейсів або джерел доступу.

Таблиця 3.3 подає шкалу для оцінки DCE залежно від складності маршруту циркуляції інформації.

Таблиця 3.3

Шкала DCE

Значення	**Характеристика**	**Приклад**
1	Актив обробляється лише в одному компоненті	Ключ у HSM
2	Дані циркулюють між двома рівнями	API, бекенд
3	Дані мають кілька копій / відкритих каналів	API, кеш, лог, репліка БД

У наступному підпункті буде розроблено покроковий алгоритм застосування методу у реальному банківському середовищі, з урахуванням життєвого циклу ІС, технічних обмежень та можливості автоматизації оцінювання.

3.4 Алгоритм застосування методу

Метод передбачає системний аналіз конфіденційних активів ОБ на основі їх критичності, вразливості та характеру циркуляції. Для практичного впровадження в середовище банку розроблено покроковий алгоритм, який охоплює увесь цикл аналізу ризиків - від ідентифікації активів до підсумкового ранжування загроз.

Нижче подано формалізований алгоритм методу, який може бути реалізований у середовищах внутрішнього аудиту, технічного аналізу безпеки, а також у процесах DevSecOps.

1) Ідентифікація активів, що обробляють КІ;

Аналізуються всі об’єкти, через які проходить конфіденційна інформація: токени, дані автентифікації, API-запити, внутрішні транзакції, лог-файли, сервіси шифрування тощо. Активи каталогізуються за типом, контекстом і місцем розташування в архітектурі банківської системи.

2) Присвоєння індексу ASI;

Кожному активу присвоюється значення ASI згідно з таблицею 3.1. Це значення може бути присвоєне вручну (на основі політик ІБ) або автоматизовано через тегування активів у системі моніторингу.

3) Виявлення точок потенційної компрометації;

Для кожного активу визначається список точок, де його можна перехопити, видозмінити або несанкціоновано прочитати: відкриті API, кешування, канали передачі, логування.

4) Оцінка RRI для кожної точки;

Кожній точці присвоюється індекс RRI, який відображає ймовірність реалізації загрози, згідно з таблицею 3.2. Оцінка може базуватись на CVSS-аналізі вразливостей, результатах пентестів, історичних інцидентах і т.ін.

5) Аналіз маршруту циркуляції активу та визначення DCE;

Оцінюється кількість копій або місць зберігання активу, наявність дублювання у логах, резервних копіях, проміжних сервісах. Значення DCE призначається відповідно до таблиці 3.3.

6) Розрахунок локального ризику для кожної точки та агрегація результатів;

Застосовується формула 3.1. Цей етап може бути повністю автоматизований у вигляді скрипта або SQL-процедури. Результати по всіх точках зводяться в таблицю й підсумовуються для отримання інтегрального ризику.

7) Виведення таблиці результатів.

З метою візуалізації формується зведена таблиця, приклад якої подано нижче (таблиця 3.4).

Таблиця 3.4

Приклад оцінки ризику для активів розробленим методом

Актив	**ASI**	**RRI**	**DCE**	**Локальний ризик Ri**
Токен автентифікації	5	0.5	2	5.0
API-запит до балансу	3	0.7	3	6.3
Лог-файл транзакції	2	0.3	3	1.8
Репліка бази з ПІБ	4	0.4	2	3.2
Приватний ключ КЕП	5	0.1	1	0.5
Сума	-	-	-	16.8

Цифрове значення інтегрального ризику дозволяє прийняти рішення щодо додаткових заходів захисту або перегляду політик. Крім того, візуальна сегментація за шкалою дозволяє швидко локалізувати критичні вузли в системі ОБ.

3.5 Порівняння результатів створеного методу з існуючими

Для верифікації ефективності запропонованого методу доцільно провести його порівняння з методами, які є найбільш релевантними до банківського сектора - зокрема, FAIR і STRIDE. Обидва методи вже використовуються у практиці оцінки ризиків в системах ОБ, однак мають різну логіку, цілі та рівень формалізації.

Для забезпечення порівнянності використовувалася умовна архітектура ОБ середнього банку, що включає веб- і мобільні клієнтські додатки, шлюз автентифікації (OAuth 2.0), API-інтерфейси до облікових даних та транзакцій,

серверну логіку з базою даних і криптографічним модулем, систему журналювання подій. Результати оцінки (табл. 3.5) за кожним методом приведено до уніфікованої шкали за трьома вимірами:

• Точність (формалізованість результату) - наскільки обґрунтовано можна обчислити рівень ризику (0–5);

• Глибина (відображення повного життєвого циклу активу) - чи враховано циркуляцію, зберігання, дублювання тощо (0–5);

• Придатність до онлайн-банкінгу - наскільки метод враховує специфіку систем ОБ (розподіленість, API, мобільність) (0–5).

Таблиця 3.5

Порівняння створеного методу з FAIR, STRIDE

Метод	**Точність**	**Глибина**	**Придатність до ОБ**	**Пояснення результату**
Створений	5	5	5	Обчислює формалізований локальний ризик; враховує критичність, маршрут, вразливості
FAIR	5	3	4	Формалізований і кількісний, але не враховує технічну циркуляцію даних
STRIDE	3	2	3	Виявляє загрози, але без обчислень або врахування циркуляції КІ

Згідно з таблицею 3.5, створений метод продемонстрував найвищий рівень комплексності та відповідності до банківської специфіки. Його основна перевага - це локалізована оцінка ризику з урахуванням маршрутів циркуляції та ступеня поширення активу, що особливо важливо в системах із складною багаторівневою архітектурою.

FAIR залишається цінним методом для стратегічного та фінансового моделювання наслідків інцидентів, однак потребує доповнення технічним аналізом. STRIDE, у свою чергу, забезпечує виявлення загроз на ранніх етапах, але не надає кількісної оцінки ризику.

Таким чином, запропонований метод заповнює функціональну нішу між технічним і стратегічним плануванням, що дозволяє застосовувати його у внутрішньому аудиті, оцінці залишкового ризику, DevSecOps-процесах та процедурі акредитації ІКС згідно з вимогами ISO/IEC.

Висновки за розділом 3

У третьому розділі кваліфікаційної роботи було розроблено авторський метод аналізу ризиків витоку КІ в системах ОБ, що враховує як технологічні, так і організаційні особливості функціонування сучасних банківських систем. Метод передбачає комплексну оцінку рівня ризику на основі трьох ключових параметрів: критичності активу, ймовірності реалізації загрози в точці обробки та ступеня відкритості або дублювання активу в системі.

Розроблений підхід відрізняється формалізованістю, прозорістю критеріїв оцінки, можливістю кількісного аналізу, а також придатністю до автоматизації в різних середовищах і внутрішнього аудиту. Метод дозволяє здійснювати локалізовану оцінку ризиків, виявляти найуразливіші ділянки обробки інформації та приймати обґрунтовані управлінські рішення щодо впровадження технічних і адміністративних заходів захисту.

Порівняльний аналіз із відомими методами, засвідчив переваги створеного методу, зокрема у здатності враховувати маршрути циркуляції даних, кількість точок доступу до активу та залишкову вразливість компонентів. Результати моделювання підтвердили ефективність обраної концепції.

Загалом, створений метод може бути використаний як складова системи управління ризиками ІБ в банках, а також як інструмент для підвищення точності оцінки ризиків при проектуванні, супроводі та аудиті систем ОБ.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було реалізовано комплексне дослідження, спрямоване на вивчення, оцінку та вдосконалення підходів до аналізу ризиків витоку КІ в системах ОБ. Актуальність теми зумовлена високим рівнем загроз, що супроводжують цифровізацію банківського сектору, та обмеженою ефективністю традиційних методів ризик-менеджменту в умовах багаторівневої та динамічної ІТ-інфраструктури банків.

На першому етапі було проведено структурний аналіз функціонування типових архітектур ОБ. Встановлено, що циркуляція КІ в таких системах має складну багатоканальну структуру, яка охоплює клієнтські додатки, API-шлюзи, серверні компоненти, бази даних, журнали подій та криптомодулі. Окреслено класифікацію інформації за рівнем доступності, ідентифіковано критичні активи та точки потенційного витоку даних.

Наступним кроком було виявлення та узагальнення основних джерел загроз витоку КІ. Встановлено, що найбільшу небезпеку становлять атаки на зовнішні API, компрометація автентифікаційних токенів, інциденти, пов’язані з журналюванням та кешуванням, а також порушення цілісності внутрішньої криптографічної інфраструктури.

У другому розділі здійснено системний аналіз існуючих методів аналізу ризиків з урахуванням їх застосовності до банківського середовища. Проведено порівняльну оцінку ефективності кожного методу за критеріями формалізованості, глибини охоплення загроз, підтримки кількісної оцінки та придатності до архітектури ОБ. З’ясовано, що жоден із розглянутих підходів не забезпечує повної відповідності потребам сучасної банківської системи в частині локалізованої оцінки ризику витоку КІ.

У третьому розділі було запропоновано, обґрунтовано та реалізовано власний метод аналізу ризиків. Запропонований підхід базується на формалізованій оцінці трьох параметрів: критичності активу, ймовірності реалізації загрози та множинності обробки даних. Побудовано архітектурну

модель, алгоритм застосування, визначено шкали індексів, а також проведено апробацію методу на умовній системі ОБ. Результати моделювання засвідчили ефективність методу у виявленні найбільш ризикових точок системи, а порівняння з існуючими методами підтвердило його переваги в точності та адаптованості до банківського контексту.

Таким чином, поставлені в роботі завдання були повністю реалізовані, а отримані результати можуть бути використані як у теоретичних дослідженнях, так і у практиці внутрішнього аудиту, інформаційного моніторингу, оцінки залишкового ризику та побудови СУІБ у фінансових установах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. European Central Bank. (2021). Internet Banking and Security Issues.
2. OWASP. Online Banking Security Guide [Електронний ресурс]. Режим доступу: https://owasp.org/www-project-online-banking-security-guide/
3. National Institute of Standards and Technology. Guide for Conducting Risk Assessments (NIST SP 800-30 Revision 1) [Електронний ресурс]. Gaithersburg, MD: U.S. Department of Commerce, 2012. Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
4. M2P Fintech. (2023). 7 Core Banking Modules Every Banker Needs to Know. [Електронний ресурс]. Режим доступу: https://m2pfintech.com/blog/7-core-banking-modules-every-banker-needs-to-know
5. PCI Security Standards Council. Payment Card Industry Data Security Standard (Version 4.0) [Електронний ресурс]. 2022. Режим доступу: https://www.pcisecuritystandards.org
6. IBM Security. (2023). Modern SIEM Platforms and Threat Monitoring.
7. Про інформацію: Закон України від 02.10.1992 № 2657-XII [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text
8. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/3855-12#Text
9. International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection – Guidance on managing information security risks (ISO/IEC Standard No. 27005:2022).
10. International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC Standard No. 27001:2022).

11. National Institute of Standards and Technology. Guide for Conducting Risk Assessments (NIST SP 800-30 Revision 1) [Електронний ресурс]. Gaithersburg, MD: U.S. Department of Commerce, 2012. Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

12. Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management – Integrated Framework. COSO, 2017.

13. International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC Standard No. 27002:2022).

14. Regulation (EU) 2016/679 of the European Parliament and of the Council. General Data Protection Regulation (GDPR) [Електронний ресурс]. 2016. Режим доступу: https://eur-lex.europa.eu/eli/reg/2016/679/oj

15. Basel Committee on Banking Supervision. Basel II and Basel III Frameworks. Bank for International Settlements. [Електронний ресурс]. 2016. Режим доступу: https://www.bis.org/publ/bcbs189.htm

16. SWIFT. Customer Security Programme [Електронний ресурс]. Режим доступу: https://www.swift.com/swift-csp

17. Національний банк України. Про затвердження Положення про організацію заходів забезпечення інформаційної безпеки в банківській системі України: Постанова № 95 від 11.09.2017 [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/v0095500-17

18. Microsoft. (2022). Threat Modeling: STRIDE Approach.

19. National Institute of Standards and Technology. (2016). NIST SP 800-154: Guide to Data-Centric System Threat Modeling.

20. FAIR Institute. (2022). Introduction to FAIR Model. [Електронний ресурс]. Режим доступу: https://www.fairinstitute.org/fair

21. Carnegie Mellon University, SEI. (2003). OCTAVE Method Implementation Guide Version 2.0. [Електронний ресурс]. Режим доступу: https://insights.sei.cmu.edu/documents/17/2001_012_001_51564.pdf

22. OWASP. (2021). DREAD Threat Model. [Електронний ресурс]. Режим доступу: https://owasp.org/www-community/Threat_Modeling

23. National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations (NIST SP 800-37 Rev. 2). [Електронний ресурс]. Режим доступу: https://csrc.nist.gov/pubs/sp/800/37/r2/final

24. European Union Agency for Cybersecurity (ENISA). (2025). Threat Landscape for the Financial Sector. [Електронний ресурс]. Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector