Хмельницький національний університет

Факультет інформаційних технологій

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Колби Сергія Сергійовича

на здобуття ступеня вищої освіти магістра

Модель системи менеджменту інформаційної безпеки фінансової установи

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

Шифр КРМКБЗІ. 240192.24.01.07 ПЗ

Виконав студент 2 курсу група КБЗІм-24-1 Сергій КОЛБА

Керівник канд.техн.наук, доц. Віра ТІТОВА

Нормоконтролер д-р філософії, старший викладач Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

16 12 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Магістр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

1 09 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Колбі Сергію Сергійовичу

1 Тема Модель системи менеджменту інформаційної безпеки фінансової установи

Керівник роботи канд.техн.наук, доц.Віра ТІТОВА

Затверджено наказом ректора університету 25 08 2025 № 65

2 Строк подання студентом кваліфікаційної роботи на кафедру 1.12.2025

3 Вихідні дані до роботи Потрібно ідентифікувати та класифікувати загрози для критичних активів банку та розробити вдосконалену модель оцінювання системи менеджменту інформаційної безпеки, яка поєднує класичне моделювання загроз із кількісними методами для розрахунку ймовірності інцидентів та економічного обґрунтування захисту.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Необхідно розглянути теоретичні основи та механізми забезпечення інформаційної безпеки фінансової установи, проаналізувати фактори впливу та стратегічні напрями, розробити детальні моделі загроз конфіденційності, цілісності та доступності для типових банківських активів, сформулювати математичну модель оцінювання ризиків, виконати експериментальну перевірку запропонованої методики на прикладі відділення банку з розрахунком економічної ефективності впровадження комплексних контрзаходів.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 1 09 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Ґрунтовне ознайомлення та дослідження предметної галузі	15.09.2025	Виконано
Визначення змісту, структури магістерської роботи	22.09.2025	Виконано
Опрацювання першого розділу магістерської роботи	02.10.2025	Виконано
Опрацювання статті за результатами дослідження	15.10.2025	Виконано
Опрацювання другого розділу магістерської роботи	30.10.2025	Виконано
Опрацювання третього розділу магістерської роботи	10.11.2025	Виконано
Підготовка та опрацювання ілюстративного матеріалу	25.11.2025	Виконано
Оформлення магістерської роботи графічної та текстової частини	25.11.2025	Виконано
Попередній захист магістерської роботи	27.11.2025	Виконано
Захист магістерської роботи на засіданні ЕК	17.12.2025	Виконано

Студент _____ Сергій КОЛБА

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

АНОТАЦІЯ

Тема кваліфікаційної роботи: Модель системи менеджменту інформаційної безпеки фінансової установи

Автор роботи: студент групи КБЗІм-24-1 Колба С.С.

Керівник роботи: к.т.н., доц. Тітова В.Ю

Загальний обсяг роботи: 104 сторінки, 18 рисунків, 16 таблиць, 5 формул, 62 посилань.

Ключові слова: інформаційна безпека, інформаційні активи, фінансова установа, моделювання загроз, оцінювання ризиків, комплексні контрзаходи.

У кваліфікаційній роботі розглянуто теоретичні основи та механізми забезпечення інформаційної безпеки фінансової установи, проаналізовано фактори впливу та стратегічні напрями захисту. Здійснено ідентифікацію та класифікацію загроз для критичних активів банку, на основі чого розроблено детальні моделі загроз конфіденційності, цілісності та доступності.

Сформульовано вдосконалену математичну модель оцінювання системи менеджменту інформаційної безпеки, яка поєднує класичне моделювання загроз із кількісними методами для розрахунку ймовірності інцидентів. Виконано експериментальну перевірку запропонованої методики на прикладі відділення банку та здійснено розрахунок економічної ефективності впровадження комплексних контрзаходів для обґрунтування захисту.

01.12.2025р.

ABSTRACT

Theme of qualification work: Model of the Information Security Management System of a Financial Institution

Author of the work: student of group KBZIm-24-1, Kolba S.S.

Mentor: PhD in Technical Sciences, Associate Professor Titova V.Y.

Total volume of work: 104 pages, 18 figures, 16 tables, 5 formulas, 62 references.

Keywords: information security, information assets, financial institution, threat modelling, risk assessment, comprehensive countermeasures.

The thesis examines the theoretical foundations and mechanisms for ensuring the information security of financial institutions, analyses influencing factors and strategic directions for protection. Threats to critical bank assets have been identified and classified, on the basis of which detailed models of threats to confidentiality, integrity and availability have been developed.

An improved mathematical model for evaluating information security management systems has been formulated, combining classical threat modelling with quantitative methods for calculating the probability of incidents. The proposed methodology has been experimentally tested using a bank branch as an example, and the economic efficiency of implementing comprehensive countermeasures has been calculated to justify protection.

01.12.2025р.

ЗМІСТ

Вступ

Актуальність теми. Стрімкий розвиток фінансових технологій докорінно змінив діяльність банків, суттєво поліпшивши їхні робочі процеси. Але ця цифрова трансформація має й зворотній бік: вона породжує нові та складні проблеми з безпекою, значно розширюючи потенційні шляхи для атак. Тепер фінансові установи зіштовхуються з серйозними загрозами, які виходять за межі звичних методів захисту. Кібербезпека відіграє важливу роль у сталому фунціонуванню установ по всьому світу [1].

Сьогодні фінансові установи стикаються з безпрецедентним рівнем кіберзагроз. За даними міжнародних звітів, фінансовий сектор залишається однією з головних мішеней для кіберзлочинців через можливість отримання прямої монетизації атак та доступ до чутливих даних. Будь-яка негативна подія безпеки для банку – це не просто технічний збій чи тимчасовий простій. Це прямий удар по найціннішому активу фінансової установи – довірі клієнтів, партнерів та регуляторів. Втрата конфіденційності, цілісності або доступності даних може призвести до катастрофічних фінансових збитків, регуляторних штрафів та навіть банкрутства.

Особливої гостроти питання інформаційної безпеки набуває в умовах повномасштабної війни в Україні. Вітчизняний фінансовий сектор став об'єктом постійних кібератак з боку ворожих хакерських угруповань, що є частиною гібридної війни. DDoS-атаки на банківські сервіси, спроби деструктивного впливу на бази даних, фішинг та атаки на ланцюги постачання вимагають від українських банків не просто “відповідності стандартам”, а реальної кіберстійкості.

Крім того, євроінтеграційний курс України ставить перед вітчизняними установами нові вимоги щодо гармонізації законодавства з нормами ЄС, зокрема імплементації регламенту DORA (Digital Operational Resilience Act), який зміщує фокус з простого захисту на операційну стійкість. Водночас, застарілі підходи до побудови систем менеджменту інформаційної безпеки (СМІБ), що базуються

виключно на “паперовій” безпеці або розрізнених технічних засобах, часто перетворюються на стримуючий фактор для бізнесу.

Це протиріччя формує ключову науково-практичну проблему: існує нагальна потреба у трансформації підходів до управління ІБ. Система безпеки має виступати не “центром витрат”, а стратегічним партнером бізнесу. Необхідна адаптивна СМІБ, здатна динамічно реагувати на нові виклики, базуючись на активному управлінні ризиками та економічному обґрунтуванні контрзаходів. Розробка ефективної, математично обґрунтованої моделі оцінювання та менеджменту ІБ є для фінансової установи стратегічним завданням, життєво необхідним для забезпечення стабільності та конкурентоспроможності. Все вищезазначене підкреслює високу актуальність, своєчасність та доцільність обраної теми магістерської роботи, особливо в контексті посилення кіберзахисту критичної інфраструктури України.

Мета і завдання дослідження. Метою роботи є підвищення ефективності системи менеджменту інформаційної безпеки фінансової установи шляхом розробки комплексної методики оцінювання ризиків, що поєднує класичне моделювання загроз та імовірнісні методи для економічного обґрунтування захисту.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– проаналізувати сучасний стан, нормативну базу (ISO 27001, DORA, постанови НБУ) та фактори впливу на інформаційну безпеку фінансових установ;

– розробити детальні моделі загроз для критичних активів банку в розрізі властивостей конфіденційності, цілісності та доступності;

– вдосконалити методологію STRIDE шляхом інтеграції з параметричним Бета-розподілом та Байєсівськими мережами (модель noisy-OR) для кількісної оцінки ризиків;

– розробити методику розрахунку очікуваних річних збитків (ALE) для визначення граничного бюджету на систему захисту;

– експериментально перевірити ефективність запропонованої методики на прикладі типового відділення банку та обґрунтувати її економічну доцільність порівняно з класичними підходами.

Предмет дослідження – методи, моделі та засоби оцінювання ризиків та системи менеджменту інформаційної безпеки.

Об’єкт дослідження – процеси управління інформаційною безпекою у фінансових установах.

Методи дослідження. У роботі застосовано методи системного аналізу, моделювання загроз (STRIDE), теорію ймовірностей (Бета-розподіл), математичне моделювання (Байєсівські мережі, модель noisy-OR) та метод економічного аналізу (ALE). Для автоматизації розрахунків використано мову програмування Python.

Наукова новизна одержаних результатів полягає в удосконаленні методики оцінювання ризиків інформаційної безпеки фінансової установи на основі підходу STRIDE, яка, на відміну від існуючих аналогів, вперше інтегрує апарат Байєсівських мереж довіри та імовірнісну модель noisy-OR для автоматизованого переходу від якісних експертних оцінок загроз до кількісних показників імовірності інцидентів, а також у набутті подальшого розвитку застосування фінансового критерію очікуваних річних збитків (ALE) для бюджетування системи менеджменту інформаційної безпеки, що дозволяє математично обґрунтувати економічну доцільність переходу від фрагментарного захисту окремих активів до впровадження комплексних архітектурних платформ.

Практичне значення одержаних результатів. Запропонована методика дозволяє банкам знизити витрати на систему безпеки на 40–60% за рахунок усунення дублювання засобів захисту та забезпечити відповідність вимогам Постанови НБУ №95. Результати реалізовано у вигляді програмного скрипту та рекомендацій щодо впровадження комплексних платформ захисту.

Публікації. За темою роботи опублікована 1 праця.

Структура та обсяг роботи. Робота складається зі вступу, трьох розділів, висновків, списку джерел та додатку. Загальний обсяг становить 104 сторінки.

1 ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІНАНСОВОЇ УСТАНОВИ

1.1 Зміст, сутність та складові елементи інформаційної безпеки фінансової установи

Інформаційна безпека – це комплекс заходів, інструментів, процесів та порад, призначених для захисту корпоративної інформації від різноманітних загроз.

Сутність інформаційної безпеки (ІБ) фінансової установи полягає у забезпеченні захищеності її інформаційних активів, інфраструктури та бізнес-процесів від будь-яких загроз, що можуть призвести до фінансових чи репутаційних збитків. На відміну від інших галузей, для банку інформація часто є не лише допоміжним ресурсом, а основним активом та предметом надання послуг (дані про рахунки, транзакції, клієнтів) [2]. Протягом десятиліть теоретичною основою для визначення цілей ІБ слугувала так звана “тріада КЦД” – забезпечення трьох базових властивостей інформації: конфіденційності, цілісності та доступності [3].

Конфіденційність гарантує доступ до інформації лише авторизованим користувачам. Цілісність забезпечує захист даних від несанкціонованої зміни чи видалення, підтримуючи їх точність. Доступність означає, що авторизовані користувачі мають доступ до інформації, коли вона їм потрібна. Загальна мета ІБ – захистити делікатну інформацію незалежно від її місцезнаходження, чи то у хмарах, програмах, чи на кінцевих пристроях [4].

Еволюцію компонентів ІБ від класичної теорії до сучасної практики у фінансовій установі представлено у Таблиці 1.1 на наступній сторінці.

Інформаційна безпека у фінансовій установі розглядається не як статичний стан, а як безперервний процес. Цей процес, формується через систему менеджменту інформаційної безпеки [5]. Стандарт визначає СМІБ не просто як набір технічних засобів, а як комплексну систему, що є інтегрованою частиною загальних бізнес-процесів та системи управління банком або іншою фінансовою

установою. Вона заснована на ризик-орієнтованому підході та реалізується через безперервний цикл постійного вдосконалення “плануй–виконуй–перевіряй–дій” (PDCA), що охоплює розробку, впровадження, моніторинг та поліпшення СМІБ [6].

Таблиця 1.1 – Компоненти інформаційної безпеки у фінансовому секторі

Компонент	Класичне визначення	Сучасне практичне значення у СМІБ банку
Конфіденційність	Стан інформації, при якому доступ до неї здійснюють тільки авторизовані користувачі, процеси або системи.	Захист банківської таємниці, персональних даних, комерційної таємниці від витоку.
Цілісність	Гарантія того, що дані не були змінені неавторизованим чином під час зберігання, обробки чи передачі.	Забезпечення незмінності фінансових транзакцій, балансів клієнтів, звітності НБУ. Критично для платіжних систем.
Доступність	Властивість інформаційних ресурсів бути готовими до використання авторизованими користувачами на їхній запит.	Забезпечення безперервності діяльності. Гарантія доступу клієнтів до інтернет-банкінгу, додатків, АТМ 24/7.

У фінансовій установі сучасна СМІБ є багатовимірною структурою. Вона виходить за межі суто технічних засобів і, згідно з провідними міжнародними стандартами та регуляторними рамками, охоплює чотири ключові, взаємопов’язані складові:

– управління ризиками (Risk Management);

– управління інцидентами та звітність (Incident Management);

– тестування цифрової операційної стійкості (Resilience Testing);

– управління ризиками третіх сторін (Third-Party Risk).

Управління ризиками – центральний процес, на якому будується вся система безпеки. Оновлений міжнародний стандарт ISO/IEC 27001:2022 визначає це як обов'язковий та безперервний цикл [6]. Він вимагає від фінансової установи не просто набору статичних контролів, а постійного процесу ідентифікації, аналізу та оцінки інформаційних ризиків. Цей підхід є основоположним і для нового європейського регламенту DORA, який зобов’язує фінансовий сектор мати надійну та задокументовану основу управління ризиками ІКТ [7].

Управління проблемами та звіти є частиною, що визначає здатність організації знаходити проблеми у кіберпросторі, реагувати і відновлюватись після них. Цей процес складається не лише з технічних частин а й зрозумілих процедур класифікації і комунікацій. Регламент DORA крім цього, ще ставить для фінансових установ суворі вимоги: вони повинні записувати, аналізувати та обов'язково доповідати національним контролерам про важливі ІКТ-проблеми у вказані терміни [7]. Як зазначає Агентство ЄС з кібербезпеки (ENISA) у своєму огляді загроз для фінансового сектора за 2024-2025 рр. швидкість реагування на питання особливо які пов’язані із програмами-вимагачами це критично для мінімізації фінансових та операційних втрат [8].

Ефективність системи безпеки має регулярно та реалістично перевірятися. Resilience testing вимагає впровадження комплексної програми тестування, яка виходить за межі базового сканування вразливостей. Регламент DORA вводить обов'язкове проведення поглиблених тестувань на проникнення під керівництвом загроз для системно важливих фінансових установ [7]. Це, по суті, контрольована імітація дій реального, кваліфікованого зловмисника, що дозволяє перевірити стійкість не лише технологій, але й процесів виявлення та реагування персоналу.

Сучасні фінансові установи критично залежать від зовнішніх постачальників ІКТ-послуг, зокрема від хмарних провайдерів та розробників програмного забезпечення. Управління ризиками третіх сторін – це поширення політик безпеки установи на увесь ланцюг постачання. Цей процес, відомий як управління ризиками кібербезпеки ланцюга постачання (C-SCRM), ґрунтується на

розумінні того, що вразливості можуть бути успадковані від постачальників на будь-якому етапі життєвого циклу продукту чи послуги [9]. Це охоплює перевірку постачальників та чітке окреслення вимог безпеки у договорах, а також невпинний нагляд за їх виконанням. Управління ризиками третіх сторін є однією з головних сфер контролю, адже, як вказує Федеральна резервна система США у своєму звіті 2023 року, атаки через ланцюг постачання дедалі частіше стають одним із ключових шляхів компрометації фінансової галузі. [10].

1.1.1 Організації які беруть участь у розробці стандартів та актів для забезпечення інформаційної безпеки

Ефективна система менеджменту інформаційної безпеки (СМІБ) фінансової установи не існує у вакуумі. Вона спирається на складний, багаторівневий ландшафт стандартів, фреймворків та нормативних актів, які розробляються та підтримуються різноманітними організаціями. Ці організації можна класифікувати за їхнім масштабом та сферою впливу: від глобальних розробників стандартів до вузькогалузевих та національних регуляторів.

На глобальному рівні ключову роль відіграє Міжнародна організація зі стандартизації (ISO). Це незалежна, неурядова організація, що розробляє стандарти для забезпечення якості, безпеки та ефективності. У сфері ІБ її головна діяльність зосереджена у спільному технічному комітеті JTC 1/SC 27, який відповідає за розробку стандартів у галузі “інформаційної безпеки, кібербезпеки та захисту приватності”, зокрема фундаментальної серії ISO 27000 [11].

Коли йдеться про глобальні практики, неможливо ігнорувати відбиток національних інституцій США. Звісно, в першу чергу це Національний інститут стандартів і технологій (NIST). Цікаво, що NIST – це не регулятор. Це урядове агентство, місія якого – стимулювати інновації шляхом розробки стандартів. Але по факту, їхні публікації стали “золотим стандартом” для програм кібербезпеки по всьому світу, включно з банками [12]. Разом з ним працює CISA – Агентство з кібербезпеки та захисту інфраструктури. Їхня парафія – це вже загальнонаціональні зусилля США зі зниження ризиків для інфраструктури, як кібернетичної, так і фізичної. Вони надають практичні рекомендації та створюють

моделі зрілості, як-от Zero Trust [13].

На регіональному рівні в Європі центральну роль відіграє Агентство Європейського Союзу з кібербезпеки (ENISA). Місія ENISA полягає у досягненні високого спільного рівня кібербезпеки в усій Європі, вона діє як центр експертизи, надаючи рекомендації країнам-членам та бізнесу [14]. Специфічно для фінансового сектору ЄС, Європейський центральний банк (ЄЦБ) у ролі головного банківського наглядача встановлює пруденційні вимоги та наглядові пріоритети, які безпосередньо стосуються управління IT-ризиками та кіберстійкості банків [15].

Існують також впливові галузеві та професійні організації. У платіжній індустрії це Рада зі стандартів безпеки індустрії платіжних карток (PCI SSC) – глобальний форум, заснований провідними платіжними брендами (Visa, Mastercard та ін.) для розробки та управління стандартами безпеки даних, зокрема PCI DSS [16]. У сфері управління та аудиту IT ключовою є ISACA (Асоціація аудиту та контролю інформаційних систем). ISACA надає сертифікації, публікації та розробляє фреймворки, зокрема COBIT, який є провідною моделлю для управління та менеджменту IT та ризиків [17]. Поряд з нею діє OWASP Foundation (Open Web Application Security Project) – глобальна некомерційна спільнота, що займається покращенням безпеки програмного забезпечення, надаючи безкоштовні інструменти та посібники, як-от OWASP Top 10 [18].

Нарешті, на національному рівні в Україні ключовою інституцією є Національний банк України (НБУ). НБУ виступає регулятором банківської системи і в рамках своєї місії із забезпечення фінансової стабільності розробляє та впроваджує обов'язкові для виконання нормативно-правові акти, що регламентують вимоги до кіберзахисту та інформаційної безпеки в банках, зокрема через Постанову №95 [19].

1.2 Фактори впливу на інформаційну безпеку

Інформаційна безпека фінансової установи є динамічною системою, що перебуває під постійним тиском різноманітних факторів. Ці фактори визначають пріоритети, інвестиції та стратегію захисту. Їх можна умовно поділити на три основні групи: зовнішні (ландшафт загроз), внутрішні (технологічні та людські) та регуляторні.

1.2.1 Зовнішні фактори

Зовнішні фактори є найбільш динамічною та неконтрольованою групою ризиків, що формує середовище, в якому функціонує система безпеки фінансової установи. Вони визначаються мотивацією, інструментами та тактикою зловмисників. Для фінансового сектору, на відміну від багатьох інших, основна мотивація атак є абсолютно чіткою – пряма фінансова вигода. Це обумовлює не лише високу частоту атак, але і їхню зростаючу складність.

Згідно з детальним аналізом ландшафту загроз для фінансового сектору, опублікованим ENISA у 2025 році, саме фінансові установи залишаються головною мішенню для кіберзлочинців [8]. Основним інструментом тиску та монетизації атак стали програми-вимагачі. Сучасні атаки цього типу давно вийшли за межі простого шифрування даних. Зловмисники використовують тактику “подвійного вимагання”: вони спочатку викрадають значні обсяги чутливих даних (банківська таємниця, персональні дані клієнтів), а вже потім шифрують системи. Це дозволяє їм вимагати викуп не лише за відновлення доступу, але й під загрозою оприлюднення викраденої інформації, що створює для банку одночасно операційний, репутаційний та юридичний ризики [8].

Водночас, найскладніші технічні загрози, як правило, починаються з найпростішої вразливості – людського фактора, який експлуатується ззовні. Звіт Verizon Data Breach Investigations Report (DBIR) за 2024 рік, що аналізує тисячі реальних інцидентів, підтверджує, що переважна більшість порушень (68% у 2024 році) так чи інакше пов'язана з “людським елементом”, не пов'язаним зі зловживанням повноваженнями [20]. Це означає, що зовнішні зловмисники

активно використовують соціальну інженерію як основний вектор початкового доступу. Ці методи є успішними, оскільки вони маніпулюють фундаментальними людськими рисами, такими як довіра, страх або схильність допомагати, обходячи таким чином технологічні засоби контролю [21]. Найпоширенішими методами є фішинг та його більш цілеспрямований варіант Spear Phishing, а також компрометація ділової пошти. За допомогою обману співробітників зловмисники отримують легітимні облікові дані, що дозволяє їм обходити складні технічні засоби захисту периметра та діяти "зсередини" для подальшого розгортання програм-вимагачів або прямої крадіжки коштів [20].

Spear Phishing (цільовий фішинг) – це цілеспрямована кібератака, що, на відміну від масового фішингу, спрямована на конкретну особу, групу чи організацію. Атака є високо персоналізованою та використовує інформацію про жертву (ім'я, посаду, колег, проекти), щоб змусити її довіритися шахрайському повідомленню. Мета – змусити жертву розкрити конфіденційні дані, встановити шкідливе ПЗ або здійснити фінансовий переказ [22, 23].

Ключовим дестабілізуючим зовнішнім фактором для фінансового сектору України є повномасштабна військова агресія РФ. Аналіз звітів Урядової команди реагування на комп'ютерні надзвичайні події України (CERT-UA) демонструє не лише кількісне, але й якісне зростання кіберзагроз [24-26].

У другому півріччі 2023 року кількість зареєстрованих інцидентів зросла на 36% порівняно з першим півріччям, у другій половині 2024 року ця тенденція посилилась, демонструючи зростання кількості кіберінцидентів на 48%, а у 2025 році загальна кількість зафіксованих кібератак зросла вдвічі порівняно з 2022 роком [24-26].

Фінансовий сектор залишається однією з пріоритетних цілей (поряд з енергетикою, телеком та урядовими структурами). Зростає активність як фінансово-сфокусованих угруповань РФ (UAC-0050 та UAC-0006), так і державних виконавців (наприклад, Sandworm), що проводять складні операції з метою шпигунства та саботажу [24]. Окрім фінансової мотивації, атаки спрямовані на викрадення даних (угруповання UAC-0218, UAC-0219) та атаки на

військовослужбовців (UAC-0184, UAC-0200), що створює опосередковані ризики і для банків, які їх обслуговують [26].

Ключові тактики, техніки та процедури (TTPs), що використовуються в атаках на фінансовий сектор, також еволюціонують. Звіти CERT-UA [25] фіксують перехід до більш складних, скоординованих операцій, що включають:

– часте використання експлойтів нульового дня (атаки на відомі, але ще не виправлені в організаціях вразливості);

– атаки на ланцюги постачання (supply chain attacks), спрямовані на постачальників ПЗ або хмарних послуг;

– активне впровадження автоматизації для прискорення фаз атаки.

Систематизовані дані щодо еволюції ландшафту загроз представлено у таблиці 1.2.

Таблиця 1.2 – Ландшафт кіберзагроз для фінансового сектору України за даними CERT-UA 2023–2025 рр. [24-26]

Параметр	Друге півріччя (H2) 2023р.	Друга половина (H2) 2024р.	Перше півріччя (H1) 2025р.
Динаміка зростання інцидентів	+36% (порівняно з H1 2023)	+48% (порівняно з H1 2024)	~15 кібератак щодня.20 Загальна кількість у 2025 р. зросла вдвічі порівняно з 2022 р..
Пріоритетні цілі	Фінансовий сектор, енергетика, телеком, уряд, сектор безпеки та оборони.	Фінансовий сектор, оборонні підприємства, об'єкти критичної інфраструктури.	Фінансовий сектор, військовослужбовці, державні установи
Ключові TTPs та тенденції	Експлойти нульового дня, шпигунство, атаки на IT-системи.	Supply chain атаки, автоматизація атак, комбінування шпигунства та саботажу	Викрадення даних, фінансово вмотивовані атаки, комбінування шпигунства та саботажу
Основні виконавці	Sandworm, фінансово-сфокусовані угруповання РФ.	Спеціалізовані підрозділи головного управління генерального штабу РФ, нові хакерські угруповання.	Sandworm, UAC-0218, UAC-0226, UAC-0227, а серед фінансово вмотивованих: UAC-0050, UAC-0006

Таким чином, зовнішнє середовище тисне на фінансову установу через постійну активність високо мотивованих злочинців, які поєднують складні технічні атаки із психологічною маніпуляцією (соціальна інженерія) для досягнення своїх фінансових цілей.

1.2.2 Внутрішні фактори

На відміну від зовнішніх загроз, внутрішні фактори виникають безпосередньо всередині фінансової установи. Вони пов'язані з її власними бізнес-рішеннями, технологічною інфраструктурою та персоналом. Ці фактори є не менш небезпечними, оскільки вони створюють або розширюють вразливості, якими згодом користуються зовнішні зловмисники.

Основним внутрішнім чинником, що визначає сучасний світ ризиків, є швидка цифрова зміна. Шукаючи нововведень та поліпшення доброго досвіду для клієнтів, фінансові установи активно використовують нові технології, такі як мобільний банкінг, інтеграції фінтеху через API та гібридні хмарні сервіси. Хоча перенесення у хмари дає гнучкість вона однак створює велику операційну складність і розширює “поверхня атаки”. Аналітики Gartner у своєму огляді головних трендів кібербезпеки на 2024 рік звертають увагу на те що одна з основних проблем є гострий брак кваліфікованих кадрів які можуть належно захищати ці нові та складні середовища [27]. Це призводить до таких ненавмисних помилок працівниками, як неправильна конфігурація хмарних сервісів що є звичайною причиною витоку даних.

Ця технологічна залежність нерозривно пов'язана з другим значущим фактором – ризиками третіх сторін (Third-Party Risk). Сучасний банк не функціонує ізольовано, а покладається на складний ланцюг постачання, що включає постачальників ПЗ та хмарних провайдерів. Проблема полягає у зрілості внутрішніх процесів контролю. Глобальне дослідження ISACA щодо прогалин у безпеці ланцюгів постачання за 2022 рік виявило, що хоча залежність зростає, багатьом організаціям критично бракує видимості та моніторингу [28]. Згідно зі звітом, 53% компаній не проводять сканування вразливостей або тестування на проникнення своїх постачальників, а 39% не мають спільного плану реагування

на інциденти з партнерами. Ця прогалина у внутрішньому управлінні перетворює постачальника на слабку ланку, через яку може бути атакована сама фінансова установа [28].

Третім, і, можливо, найбільш непередбачуваним внутрішнім фактором, залишається людський елемент. Звіт IBM про ціну порушення безпеки даних за 2024 рік надає фінансову оцінку цього ризику [29]. Він підтверджує, що значна частина інцидентів починається зсередини. Сюди входять ненавмисні людські помилки (як-от помилки конфігурації або успішний фішинг), які залишаються одним з найпоширеніших векторів атак. Однак звіт також окремо виділяє загрозу зловмисного інсайдера. Хоча такі інциденти трапляються рідше, вони є набагато руйнівнішими та дорожчими для ліквідації, оскільки інсайдер вже знаходиться "всередині" периметра захисту і має легітимний доступ та знання про внутрішні системи [29].

1.2.3 Регуляторні та комплаєнс-фактори

Третім, і часто визначальним, фактором впливу на інформаційну безпеку фінансової установи є жорсткий регуляторний тиск. На відміну від інших галузей, у фінансовому секторі вимоги регуляторів є не просто рекомендаціями, а головним рушієм для формування стратегії, виділення бюджетів та впровадження конкретних заходів захисту, іноді навіть у випередженні реальних загроз.

Цей фактор має кілька рівнів [30]:

– стратегічні регіональні пріоритети;

– юридично обов'язкові локальні норми;

– обов'язкові договірні стандарти.

У стратегічному факторі найбільш значущим глобальним трендом є зміщення акценту від кібербезпеки (захисту) до кіберстійкості (здатності витримувати атаку та відновлюватись). Європейський центральний банк (ЄЦБ) у своїх наглядових пріоритетах на 2024-2026 роки визначив "Посилення стійкості до кібернетичних та ІТ-ризиків" як одне з трьох ключових завдань. Це вимагає від банків не просто мати захист, а й проводити реалістичні стрес-тести та гарантувати безперервність роботи навіть під час успішної кібератаки, особливо

щодо критичних IT-аутсорсерів [31].

Серед юридично обов’язкових локальних норм на рівні України ключовим фактором є політика Національного банку України. Головним регуляторним актом є Постанова № 95, яка була суттєво оновлена у 2024 році. Цей документ вимагає від банків імплементації комплексної, ризик-орієнтованої СМІБ. Він чітко регламентує процеси управління IT-ризиками, управління інцидентами, проведення аудитів та, що критично важливо, управління ризиками третіх сторін (зокрема, хмарних провайдерів). Невиконання цих вимог веде до прямих санкцій з боку НБУ [32].

Окрім державних регуляторів, фінансові установи зобов'язані дотримуватись обов'язкових приписів та стандартів платіжних систем. Найважливішим тут є стандарт PCI DSS (Payment Card Industry Data Security Standard). Випуск нової редакції v4.0 у 2022 році суттєво посилив вимоги до охорони даних платіжних карток [33]. Він вимагає від установ більш гнучких підходів до автентифікації, посиленого контролю та періодичної валідації заходів, що змушує банки невпинно адаптувати свої технічні системи безпеки.

1.3 Напрями та механізми забезпечення інформаційної безпеки фінансової установи

Забезпечення інформаційної безпеки (ІБ) у фінансовому секторі є комплексним завданням, що вимагає інтегрованого підходу, який поєднує стратегічні напрями (вектори розвитку) та практичні механізми (інструменти реалізації). Сучасна модель СМІБ відходить від реактивного захисту та будується на проактивних, стійких та бізнес-інтегрованих принципах.

1.3.1 Безперервний цикл PDCA як основа стандартів

У сфері управління інформаційною безпекою фундаментально відсутнє поняття “завершеного проєкту”. Безпеку неможливо розглядати як статичну стіну, яку можна збудувати один раз і забути. Це, за своєю суттю, динамічний процес,

що вимагає невпинної адаптації, оскільки і вектори загроз, і самі технології еволюціонують практично щодня.

Втіленням цієї ідеї процесності виступає цикл PDCA (Plan-Do-Check-Act, або “Плануй-Виконуй-Перевіряй-Дій”). Цей чотириетапний ітеративний підхід є визнаною моделлю для досягнення безперервного вдосконалення [34]. По суті, він став рушійною силою, що лежить в основі сучасних стандартів безпеки.

Цей зв'язок найбільш чітко простежується у стандарті ISO/IEC 27001:2022. Галузеві аналітики підкреслюють, що оновлена структура стандарту тепер повністю організована навколо моделі PDCA [35]. Так, фаза “Плануй” (Plan) охоплює всю підготовчу роботу, включно з розумінням контексту організації. Фаза “Виконуй” (Do) зосереджена на впровадженні та експлуатації контролів. Етап “Перевіряй” (Check) формалізує вимоги до моніторингу, аудитів та перегляду з боку керівництва. Нарешті, етап “Дій” (Act) замикає цикл, вимагаючи коригувальних дій та забезпечуючи постійне вдосконалення [35].

Ця ж філософія, хоч і з іншою термінологією, пронизує NIST Cybersecurity Framework (CSF). Його оновлена версія 2.0 (2024 р.) ввела нову центральну функцію “Govern” (Управління). Ця функція слугує “центральним хабом” (central hub), який інтегрує та пов'язує всі інші функції (Identify, Protect, Detect, Respond, Recover) в єдиний керований цикл [36]. Аналогічно, новий європейський регламент DORA (Digital Operational Resilience Act), по суті, законодавчо закріплює цей ітеративний підхід. Він вимагає від фінансових установ постійно управляти ризиками та регулярно проводити тестування на стійкість (Check), підвищуючи загальну планку операційної стійкості для галузі (Act) [37].

По суті, модель PDCA вирішує головну помилку в управлінні безпекою: вона не дозволяє ставитися до СМІБ як до одноразового завдання. Вона перетворює безпеку на живий бізнес-процес, який ніколи не “завершено”, а завжди знаходиться в стані вимірювання, аналізу та поліпшення [34].

1.3.2 Стратегічні напрями забезпечення інформаційної безпеки

Стратегічні напрями визначають фундаментальну філософію та довгострокові пріоритети, якими керується фінансова установа при побудові своєї

системи захисту. Вони відображають еволюцію поглядів на кібербезпеку: від реактивного захисту окремих активів до проактивного управління стійкістю всього бізнесу.

Серед основних напрямів, які розглянуто це:

– перехід від захисту до кібероперацій ної стійкості (Cyber Resilience);

– проактивне та ризик-орієнтоване управління (Risk-Based Approach);

– інтеграція безпеки в бізнес-процеси (Security-by-Design).

Cyber Resilience – це ключовий світоглядний та стратегічний зсув у сучасному фінансовому секторі. Традиційна модель безпеки, орієнтована на запобігання, базувалася на припущенні, що можна побудувати “непробивний” периметр. Сучасна парадигма визнає, що інциденти та успішні атаки є статистично неминучими.

Тому фокус зміщується на кіберстійкість (Resilience) – комплексну здатність установи: витримувати (поглинати вплив атаки без катастрофічного збою), продовжувати (забезпечувати безперервність надання критичних фінансових послуг навіть під час атаки) та відновлюватись (швидко повертати системи до нормального функціонування після інциденту) [7].

Цей пріоритет закріплений на найвищому міжнародному рівні. Банк міжнародних розрахунків (BIS) у своїх пріоритетах політики на 2023 рік визначив операційну стійкість як ключову мету для фінансового сектору [38]. Стійкість є головним пріоритетом для установ, які змушені адаптуватися до нових регуляторних вимог (як-от DORA) та зростаючих загроз.

Risk-Based Approach означає відмову від “шаблонного” підходу до безпеки, де установа просто виконує формальний список вимог чи “чек-лист”. Натомість впроваджується гнучкий підхід, заснований на постійному управлінні ризиками.

Цей підхід є ядром провідних фреймворків управління, таких як COBIT. Практичні дослідження, зокрема кейс-стаді впровадження COBIT 2019, демонструють, що цей фреймворк надає інструменти для управління ризиками (Risk Management), дозволяючи побудувати стратегію кібербезпеки, яка ґрунтується саме на ризик-орієнтованій моделі [39]. Замість того, щоб

впроваджувати всі можливі заходи захисту, установа повинна:

– ідентифікувати свої унікальні бізнес-процеси та інформаційні активи;

– оцінити конкретні загрози та вразливості, притаманні саме їй;

– пріоритезувати ризики (за ймовірністю та потенційним впливом).

Такий спосіб дозволяє банку концентрувати обмежені фінансові та людські ресурси на тих напрямах, де ризик є найбільшим (наприклад, на захисті системи інтернет-банкінгу, а не внутрішнього корпоративного порталу). Це робить безпеку економічно ефективною та адекватною реальним бізнес-потребам.

Сучасним трендом трансформації фінансового сектору є міграція критичних сервісів у хмарні середовища. Однак це створює нові виклики для систем безпеки, пов'язані з розмиванням периметра та моделлю спільної відповідальності. Згідно зі звітом Cloud Security Alliance (CSA) основними ризиками для хмарних фінансових систем є не стільки зовнішні атаки, скільки неправильна конфігурація хмарних ресурсів, недостатній контроль ідентифікації та небезпечні API інтерфейси [40]. Для нівелювання цих загроз міжнародна спільнота розробила стандарт ISO/IEC 27017, який надає специфічні рекомендації щодо контролю безпеки для хмарних сервісів, доповнюючи базовий ISO 27001 [41].

Інтеграція безпеки в бізнес-процеси являє собою фундаментальний зсув від традиційної, ізольованої моделі ІБ до її глибокої інтеграції у повсякденну діяльність та культуру фінансової установи. Традиційна модель, де відділ безпеки виступав як “контролер” або “гальмо” наприкінці бізнес-процесу, довела свою неефективність. Сучасний підхід (Security-by-Design) вимагає, щоб безпека була невід'ємною частиною будь-якого процесу з самого початку.

Методологія Security-by-Design на практиці реалізується через підхід DevSecOps, який передбачає інтеграцію інструментів безпеки безпосередньо у конвеєр розробки програмного забезпечення (CI/CD). Національний інститут стандартів і технологій США (NIST) у спеціальній публікації SP 800-204C (2022) визначає еталонну архітектуру DevSecOps, акцентуючи увагу на автоматизованому скануванні коду та управлінні секретами [42]. Згідно з дослідженнями 2024 року, впровадження DevSecOps у фінансових установах

дозволяє знизити вартість виправлення вразливостей у 30 разів порівняно з виправленням на етапі експлуатації, що підтверджує економічну ефективність цього підходу [43].

Потреба такої глибокої інтеграції зумовлюється оцінкою загроз. Дослідження демонструють, що людський чинник лишається однією з основних уразливостей. Звіт Deloitte “2024 Cyber Threat Trends” наголошує, що неправомірне використання дійсних облікових даних (добутих, наприклад, через фішинг) залишається одним із головних шляхів атак [44]. Це свідчить, що технічні заходи захисту є недостатніми, якщо самі бізнес-процеси та співробітники, які їх виконують, не мають “вбудованого” захисту.

Інтеграція безпеки – це, насамперед, культурна трансформація. Це еволюція від пасивного “ознайомлення з політиками” до активної участі. Дефіцит досвідчених фахівців та прогалини у культурі є одними з важливих викликів. Завдання – зробити безпеку спільною місією, а не клопотом одного підрозділу.

Практичне втілення цього напрямку включає впровадження фреймворків безпечної розробки (SSDF / DevSecOps) та “орієнтир” з безпеки.

У банківській сфері це означає впровадження практик, визначених, наприклад, у NIST Secure Software Development Framework. Цей підхід вимагає інтеграції безпеки на кожному етапі життєвого циклу розробки програмного забезпечення, включаючи перевірки коду, тестування безпеки та управління вразливостями ще до того, як продукт потрапить у виробництво [45].

Під “орієнтиром” з безпеки мається на увазі навчання та призначення відповідальних “агентів” безпеки безпосередньо у бізнес-підрозділах (кредитному, операційному тощо), що допомагає впроваджувати вимоги ІБ у локальні процеси [46].

Таким чином, стратегічна мета цього напряму – перетворити відділ безпеки з “департаменту 'Ні'“ на “партнера”, який допомагає фінансовій установі розвиватися та впроваджувати інновації безпечно з самого початку. Такий підхід забезпечує необхідний баланс між швидкістю впровадження інновацій та надійним захистом активів, що є критичною умовою для збереження довіри

клієнтів та стабільного розвитку фінансової установи в умовах сучасних загроз.

1.3.3 Ключові механізми забезпечення ІБ

Якщо стратегічні напрями визначають філософію захисту, то механізми – це конкретні інструменти, процеси та технології для її практичної реалізації. У сучасній фінансовій установі ці механізми поділяються на організаційно-управлінські, технічні та процедурні.

Організаційно-управлінські механізми (також відомі як адміністративні заходи контролю) формують каркас системи менеджменту інформаційної безпеки (СМІБ). Вони являють собою сукупність політик, процедур, стандартів та практик, які визначають, як фінансова установа керує ризиками та захищає свої активи [6]. На відміну від технічних механізмів, які фокусуються на технологіях, ці механізми фокусуються на людях та процесах.

Цей каркас починається з найвищого рівня – управління та лідерства (Governance), що забезпечує узгодженість цілей безпеки зі стратегічними цілями банку. Цей механізм включає, по-перше, визначення відповідальності, що передбачає формальне призначення керівника з інформаційної безпеки (CISO) та покладання кінцевої відповідальності за управління ризиками на вище керівництво. Управління IT-ризиками є невід'ємною частиною загального корпоративного управління [47]. По-друге, він включає визначення політики, де керівництво затверджує політику інформаційної безпеки – документ верхнього рівня, який декларує наміри та зобов'язання банку у сфері ІБ і слугує основою для розробки всіх інших процедур [48].

Практичною реалізацією цього управлінського бачення є формалізована система менеджменту (СМІБ). Це формальна структура, яка об'єднує всі елементи безпеки в єдиний, керований процес. Найпоширенішим механізмом для її побудови є стандарт ISO/IEC 27001:2022, який вимагає від установи визначити область застосування системи, провести оцінку ризиків та впровадити відповідні заходи контролю [6]. Ключовим управлінським механізмом у рамках ISO 27001 є ітеративний цикл “Плануй-Виконуй-Перевіряй-Дій” (PDCA), який забезпечує не статичний захист, а безперервне вдосконалення системи [6].

Ця система, своєю чергою, діє через набір ключових процесів управління. “мозком” СМІБ є процес управління ризиками (Risk Management), що вимагає наявності механізму ідентифікації, аналізу та обробки ризиків, дозволяючи установі приймати зважені рішення щодо їх мінімізації чи прийняття [48]. Оскільки людина є ключовим фактором ризику, критичним є процес управління персоналом (HR Security). Цей механізм охоплює весь життєвий цикл співробітника: від перевірки кандидатів (скринінгу) при прийомі на роботу до обов'язкового навчання з питань та формалізованих процедур при звільненні, що гарантують негайне блокування доступу. Нарешті, управління інцидентами є заздалегідь розробленим планом дій на випадок кібератаки, який визначає процедури локалізації загрози, повідомлення регуляторів (як-от НБУ) та відновлення роботи [48].

Операційним втіленням цих процесів є центр управління безпекою. SOC – це централізований операційно-управлінський механізм, команда, яка використовує технології для реалізації управлінських рішень на практиці. SOC відповідає за безперервний моніторинг, виявлення та аналіз загроз, а також за координацію негайного реагування на інциденти [33].

Технічні засоби є практичним втіленням організаційно-управлінських політик, являючи собою сукупність технологій та конфігурацій, що безпосередньо забезпечують охорону інформаційних ресурсів. Вони реалізують головні функції безпеки, як-от захист та виявлення, і постають підґрунтям сучасної оборони.

Традиційні моделі захисту периметра втрачають ефективність в умовах децентралізації банківських мереж. Відповіддю на ці виклики стала концепція Zero Trust Architecture (ZTA), яка базується на принципі “ніколи не довіряй, завжди перевіряй”. У 2023 році Агентство з кібербезпеки та захисту інфраструктури США (CISA) представило оновлену “Модель зрілості нульової довіри” (Version 2.0). Цей документ визначає п'ять стовпів реалізації стратегії: ідентичність, пристрої, мережі, додатки та дані. Для фінансових установ впровадження ZTA дозволяє мінімізувати ризики бічного переміщення зловмисника всередині мережі та забезпечити гранулярний контроль доступу [49].

Крім того, у 2024 році було розроблено деталізовані інструкції щодо захисту даних у середовищах Zero Trust, які наголошують на необхідності шифрування та безперервного моніторингу кожного запиту доступу [50].

Одним із головних механізмів є поділ мережі, який у теперішніх архітектурах, на кшталт Zero Trust (нульова довіра), трансформується мікросегментацію. Ця стратегія залишає застарілу ідею єдиного “надійного” периметру. Натомість кожен актив, як-от сервер чи сховище даних, вважається окремим ізольованим “острівцем” [51]. Такий метод ключовим для стримування нападів, оскільки він унеможливлює вільне пересування зловмисника, який здобув доступ до одного сегменту. Дієвість цього мережевого регулювання нерозривно пов'язана з управлінням ідентифікацією та доступом (IAM). Сучасні механізми вимагають сталої перевірки ідентичності, відкидаючи довіру що ґрунтується на розташуванні [51].

Вимога сильної автентифікації для кожної сесії доступу, що є основою “Ідентичності” як одного з п’яти стовпів безпеки, реалізується за допомогою специфічних механізмів [49]. До них належить сімейство контролів “Identification and Authentication” (IA) згідно з NIST SP 800-53, що охоплює такі практики, як багатофакторна автентифікація (MFA) та управління життєвим циклом облікових даних [52]. При цьому криптографічний захист слугує “останнім рубежем оборони”. Це охоплює захист даних як під час передачі.

Нарешті, для своєчасного виявлення атак використовуються механізми моніторингу, логування та виявлення. NIST SP 800-53 визначає цілий набір контролів “Audit and Accountability (AU)”, які вимагають, щоб усі дії в системі фіксувалися в захищених від модифікації журналах (логах) [52].

Для централізованого збору та аналізу логів SOC, застосовує технології SIEM (Security Information and Event Management). Це дозволяє корелювати дані та аналізувати їх у реальному часі для виявлення складних патернів атак та реагування на них [53].

Процедурні механізми являють собою набір процесів, відповідальних за те, щоб вся система безпеки ефективно функціонувала, постійно перевірялась

(валідувалась) та адаптувалася до змін. Вони слугують сполучною ланкою між організаційним управлінням і технічними засобами контролю, створюючи гарантії того, що політики втілюються в життя, а технології працюють коректно. У фінансових установах критичну вагу має механізм управління ризиками третіх сторін (TPRM), оскільки зростає залежність від аутсорсингу та хмарних сервісів. Регуляторні органи, наприклад, управління пруденційного регулювання (PRA) Великобританії, вимагають від установ впровадження надійних процесів для управління цими ризиками [54]. Це охоплює початкову “належну перевірку” постачальника, наявність чітких юридичних контрактів із закріпленими вимогами безпеки, і, що не менш важливо, наявність “планів виходу” на випадок збою в роботі партнера [54].

Іншим невід'ємним механізмом виступає тестування та валідація, мета якого – перевірити саме реальну ефективність захисту, а не його формальну наявність. Цей процес включає регулярні сканування вразливостей та тести на проникнення. Деякі галузеві стандарти, вимагають для веб-додатків (на кшталт інтернет-банкінгу) не просто автоматизованих перевірок, але й глибокого мануального тестування саме бізнес-логіки, щоб виявити прогалини, які сканери не помічають [55].

Завершує цю групу процедурний механізм реагування на інциденти та відновлення. Наявність формалізованих і заздалегідь протестованих планів є обов'язковою умовою. Цей процес визначає чіткий життєвий цикл для обробки інциденту. Він охоплює виявлення (Detection), аналіз (Analysis), стримування (Containment), ліквідацію (Eradication) та, зрештою, відновлення (Recovery) [52]. Саме ці механізми дають установі чіткий план дій для мінімізації збитків та повернення до нормальної роботи.

1.3.4 Методи моделювання і оцінки ризиків

У межах концепту “Secure by Design” методологія STRIDE продовжує відігравати роль основоположного інструменту, навіть за умов постійного ускладнення архітектурних рішень. Цей класичний метод є досить гнучким, адже він демонструє високу ефективність як для звичайного ПЗ, так і для новітніх

середовищ IoT та хмарних платформ [56]. Виконання вимог STRIDE на етапах проєктування та розробки забезпечує системний пошук вразливостей, що дозволяє значно оптимізувати бюджет, запобігаючи високих витрат на усунення дефектів на етапі експлуатації [57].

В основі методології лежить мнемонічна схема, що класифікує шість типів загроз відповідно до властивостей безпеки, на які вони посягають. Перша категорія, Spoofing (підміна), спрямована на компрометацію механізмів автентифікації; це дозволяє зловмиснику імітувати легітимного користувача або системний об'єкт, що становить критичну небезпеку для сучасних систем ідентифікації [58]. Загрози цілісності даних охоплюються категорією Tampering (фальсифікація), що є критично важливим аспектом для фінансових операцій та смарт-контрактів, де будь-яка неавторизована зміна загрожує прямими матеріальними втратами. Натомість категорія Repudiation (відмова від авторства) атакує властивість неспростовності, унеможливлюючи доведення причетності суб'єкта до певної дії, що підриває основи аудиту та юридичної сили електронних транзакцій [59].

Наступний блок загроз стосується аспектів конфіденційності та доступності. Information Disclosure (розкриття інформації) описує ризики витоку даних, що, як правило, стає головним вектором атак у хмарних середовищах через помилки в конфігурації сховищ. У свою чергу, атаки типу Denial of Service (відмова в обслуговуванні) мають на меті вичерпання ресурсів системи, блокуючи доступ до сервісів для легальних користувачів. Завершує цю структуру Elevation of Privilege (підвищення привілеїв) – загроза, що дозволяє обійти авторизацію та отримати адміністративні права, що часто слугує фінальним акордом у ланцюжку складних цільових атак [60].

Особливу увагу слід звернути на специфіку застосування STRIDE в середовищі Інтернету речей. Для IoT-систем, таких як розумні будинки, цей метод дозволяє ефективно виявляти специфічні вектори атак, наприклад, Man-in-the-Middle при передачі даних між сенсорами та шлюзом, а також ризики фізичного доступу до пристроїв [56]. У хмарних інфраструктурах STRIDE трансформується

для аналізу ризиків, пов'язаних із управлінням ідентифікацією (IAM) та безпекою API, дозволяючи архітекторам будувати більш стійкі мультихмарні рішення [60].

При порівняльному аналізі інструментів моделювання загроз STRIDE позиціонується як методологія, орієнтована передусім на розробників, на відміну від PASTA, що фокусується на бізнес-ризиках. Водночас фахівці радять поєднувати STRIDE з кількісними методами оцінки, наприклад DREAD, оскільки сам по собі STRIDE дозволяє лише ідентифікувати загрозу, не надаючи механізмів для визначення її ймовірності чи пріоритезації [61]. Такий комплексний підхід дає можливість організаціям вибудовувати ешелоновану систему захисту, що відповідає сучасним стандартам кіберстійкості.

1.4 Постановка задачі

Проведений у першому розділі теоретичний аналіз засвідчив, що сучасні фінансові установи функціонують в умовах агресивного гібридного ландшафту загроз та жорсткого регуляторного тиску. Попри наявність ґрунтовної нормативної бази, що включає стандарти ISO 27001, регламент DORA та вимоги НБУ, існуючі підходи до забезпечення інформаційної безпеки часто характеризуються суттєвими недоліками, такими як надмірна орієнтація на реактивний захист периметра, що втрачає ефективність в умовах використання хмарних технологій та зростання ризиків ланцюга постачання. Крім того, впровадження стандартів нерідко обмежується формальним комплаєнсом без глибинної інтеграції принципів безпеки у бізнес-процеси, що залишає критичні активи вразливими до людського фактору та логічних помилок, а стандартні моделі загроз не повною мірою враховують специфіку складних цільових атак та диверсійних дій.

Враховуючи виявлені проблеми, виникає об’єктивна необхідність переходу від теоретичних узагальнень до практичного моделювання комплексної системи менеджменту інформаційної безпеки, адаптованої до специфіки фінансової

установи. Розробка такої ризик-орієнтованої моделі дозволить чітко ідентифікувати критичні активи та деталізувати вектори атак на них, використовуючи методологію STRIDE для виявлення неочевидних вразливостей на рівні архітектури та процесів. Таким чином, основним завданням цього розділу є розробка та обґрунтування моделі СМІБ, яка гармонізує вимоги міжнародних стандартів з національними регуляціями, базується на циклі безперервного вдосконалення PDCA та пропонує конкретні контрзаходи для гарантування операційної стійкості фінансової установи в умовах сучасних викликів.

Для забезпечення об'єктивності прийняття рішень подальше дослідження передбачає удосконалення якісного аналізу загроз шляхом його інтеграції з імовірнісними математичними моделями та методами агрегації ризиків. Окремим завданням є економічне обґрунтування ефективності запропонованої системи захисту, що дозволить не лише мінімізувати ймовірність інцидентів, але й оптимізувати витрати на інформаційну безпеку.

2 МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІНАНСОВОЇ УСТАНОВИ

2.1 Моделі загроз конфіденційності

В умовах сучасного банкінгу конфіденційність залишається критичним параметром, порушення якого веде до найбільш резонансних наслідків. Аналіз активів фінансової установи через призму методології STRIDE дозволяє виділити ключові вектори атак, спрямовані на несанкціоноване розкриття інформації (Information Disclosure) та підвищення привілеїв (Elevation of Privilege). На даному етапі ми можемо використати цю методологію для оцінки ризиків, проте вона потребує вдосконалення.

Для побудови моделі загроз конфіденційності було зазначено 6 активів: база даних клієнтів, дані платіжних карток, облікові записи співробітників, електронний документообіг та мобільний додаток із Frontend кодом.

Схема першого активу вказана на рисунку 2.1.

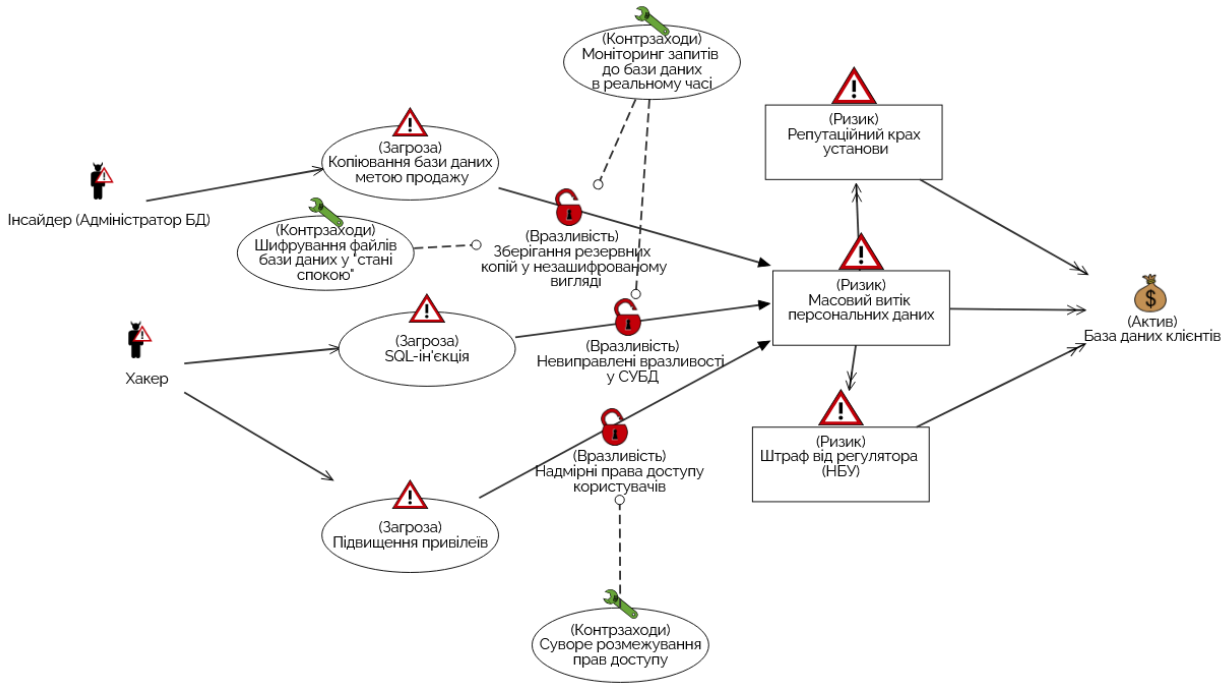

Рисунок 2.1 – Модель загроз бази даних клієнтів

База даних клієнтів є однією з основних частин банку, тому що там зберігаються паспортні дані, адреси та інша інформація, що пов'язана із користувачами послуг фінансової установи.

В створеній моделі загроз даного активу є два можливі джерела загроз: інсайдер, що може бути самим адміністратором бази даних, а також хакер. Також можна вважати, що в даному активі небезпеку становить не лише зовнішня загроза, а й внутрішня. До внутрішньої можна віднести копіювання бази даних співробітником із легітимними, але надмірними правами із метою продажу цієї інформації конкурентам. Зовнішня загроза являє собою впровадження зловмисником SQL-ін’єкції, тобто він впроваджує шкідливий код через веб-інтерфейс для вивантаження таблиць. Також отримавши доступ користувача, хакер може підвищити права до адміністратора через баг у ПЗ. Наслідками цих загроз можуть стати репутаційний крах установи, після якого довіру клієнтів і партнерів буде важко повернути, штраф з боку регуляторів (НБУ) та масовий витік персональних даних, через що буде порушено закон України “Про захист персональних даних” [62]. Для протидії цим ризикам та вразливостям офіцер безпеки спільно із адміністратором БД повинні організувати певні контрзаходи: завжди проводити моніторинг запитів до бази даних в реальному часі, встановити суворе обмеження прав доступу (до прикладу, рольову модель) та застосувати шифрування файлів “у стані спокою”.

Розглянемо модель загроз наступного активу (Рисунок 2.2). Дані платіжних карток являють собою один із найбільш критичних активів фінансової установи, оскільки вони обробляються процесинговим центром і включають конфіденційну інформацію, необхідну для проведення транзакцій.

В створеній моделі загроз даного активу основним джерелом небезпеки виступає фінансово вмотивований кіберзлочинець. Загрози, що ним створюються, включають перехоплення трафіку (Sniffing) та зчитування даних з оперативної пам'яті (RAM Scraping). Реалізація цих атак стає можливою через низку технічних вразливостей: вразливість “Heartbleed” або подібні недоліки у застарілих протоколах шифрування, передачу даних карти у відкритому вигляді

(використання HTTP замість HTTPS), а також заборонене стандартами зберігання CVV-кодів на дискових або flash-носіях. Наслідками цих загроз можуть стати пряма фінансова крадіжка коштів клієнтів, що призводить до матеріальних збитків, а також відкликання ліцензії на еквайринг з боку міжнародних платіжних систем (Visa/Mastercard), що є критичним для бізнесу. Для протидії цим ризикам та вразливостям захисники повинні організувати певні контрзаходи: впровадити токенізацію даних, забезпечити використання виключно актуальних протоколів шифрування каналів та налаштувати блокування передачі назовні форматів даних, схожих на номери карток.

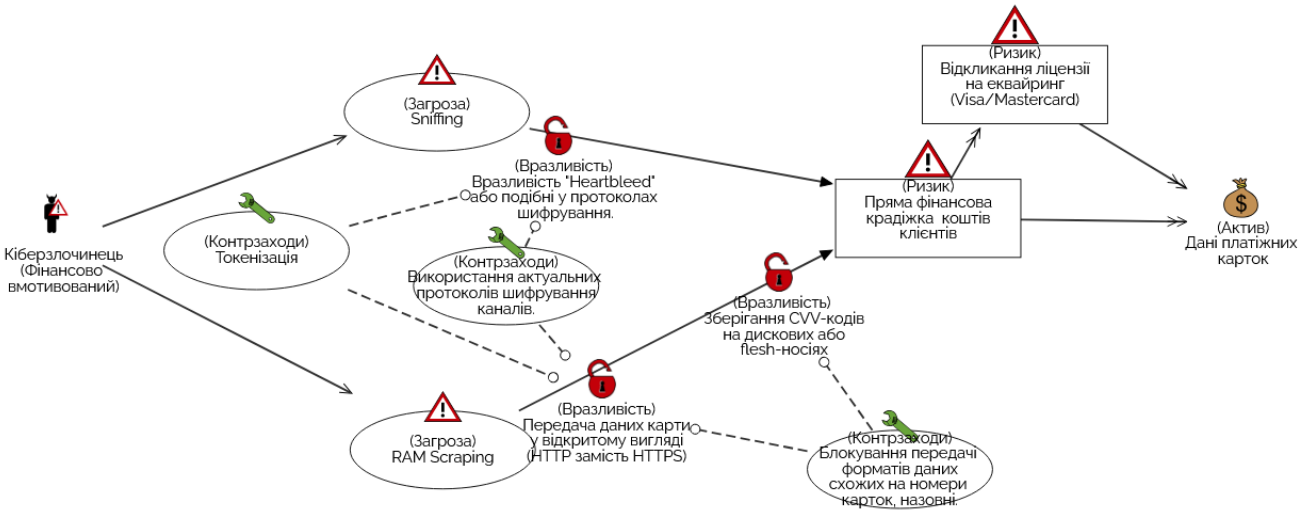

Рисунок 2.2 – Модель загроз даних платіжних карток

Облікові записи співробітників являють собою один із найбільш вразливих активів банку, оскільки вони складаються з логінів та паролів, що забезпечують доступ до внутрішньої корпоративної мережі. Фактично, ці дані є ключами до цифрової інфраструктури установи, і їх втрата дозволяє зловмисникам діяти від імені легітимних користувачів.

В створеній моделі загроз даного активу основним джерелом небезпеки визначено хакера (Рисунок 2.3). Вектори його атак спрямовані на використання як технічних недоліків, так і людського фактору. Зокрема, загроза фішингу стає успішною через недбале ставлення персоналу до безпеки, а саме – зберігання

паролів на стікерах або у незахищених файлах Excel. Технічні атаки, такі як Brute-force (автоматизований підбір паролів) та витягування хешів паролів з пам'яті комп'ютера, стають можливими через слабку політику паролів та наявність критичної вразливості у вигляді відсутності багатофакторної автентифікації. Наслідками цих загроз можуть стати несанкціонований доступ до корпоративної мережі та подальший розвиток атаки в середині мережі, що дозволяє зловмиснику підвищувати привілеї та діставатися до критичних даних. Для протидії цим ризикам та вразливостям потрібно організувати дієві контрзаходи, а саме: запровадити сувору політику парольного захисту, забезпечити обов'язкову багатофакторну автентифікацію та проводити регулярне навчання персоналу у сфері IT-безпеки.

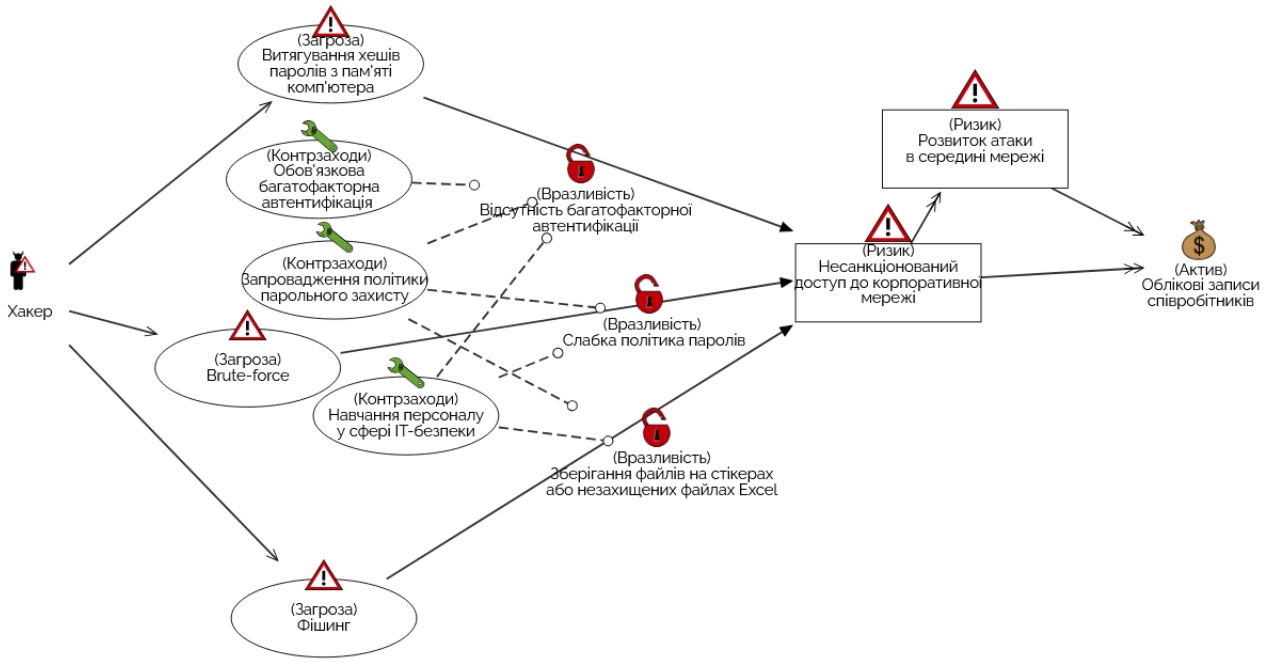

Рисунок 2.3 – Модель загроз облікових записів співробітників

Електронний документообіг (контракти, накази) також є одним із стратегічно важливих активів банку, оскільки він містить комерційну таємницю, стратегічні плани розвитку та конфіденційну інформацію про майбутні угоди чи злиття.

На рисунку 2.4 виділено два ключові джерела небезпеки: фінансово вмотивований кіберзлочинець що може працювати на конкурента та інсайдер, яким виступає недбалий співробітник. Зовнішня загроза проявляється у формі індустріального шпигунства, реалізація якого стає можливою через неправильно налаштовані права доступу до файлових шарів. Внутрішня загроза пов'язана з людським фактором – випадковою відправкою конфіденційного документа на зовнішню пошту. Цьому сприяють такі вразливості, як використання співробітниками публічних хмарних сервісів або месенджерів для робочих файлів, а також відсутність належного маркування документів (грифів обмеження доступу).

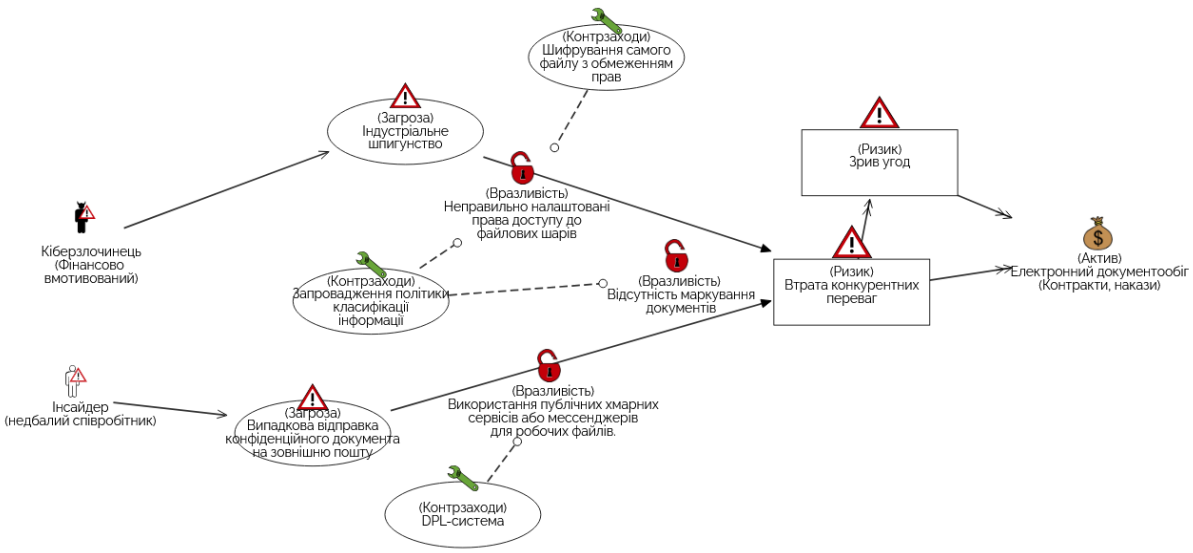

Рисунок 2.4 – Модель загроз електронного документообігу

Наслідками реалізації цих загроз можуть стати зрив важливих угод та втрата конкурентних переваг на ринку. Для протидії цим ризикам та усунення вразливостей юридичний департамент спільно з адміністратором безпеки повинні запровадити політику класифікації інформації для обов'язкового маркування даних, впровадити DLP-систему для моніторингу каналів передачі (включно з хмарними сервісами) та застосувати технології IRM/DRM для шифрування самих файлів із технічним обмеженням прав на їх поширення.

Приватні ключі шифрування та електронний цифровий підпис (ЕЦП) являють собою фундамент інформаційної безпеки фінансової установи. Вони є критично важливими даними, оскільки саме за їх допомогою забезпечується легітимність підписання фінансових транзакцій та конфіденційність каналів зв'язку.

В даній моделі загроз, що вказана на рисунку 2.5, вектори атак розгалужуються на два незалежні шляхи, кожен з яких має своє джерело та специфічні вразливості. Перший шлях ініціюється інсайдером (адміністратором чи розробником із легітимним доступом) або зовнішнім хакером, що отримав права суперкористувача (root). Загрозою тут виступає ексфільтрація ключів (Key Exfiltration) – фізичне копіювання файлів на зовнішні носії або їх передача мережею для використання поза банком. Реалізація цього сценарію стає можливою через вразливість програмного зберігання ключів, коли вони знаходяться на жорсткому диску у вигляді звичайних файлів, доступних для читання та копіювання операційною системою. Другий шлях пов'язаний із діяльністю зовнішніх зловмисників, чия загроза полягає у спробі математичного підбору ключа (криптоаналізу). Успіху цієї атаки сприяє вразливість відсутності ротації, тобто використання одного статичного ключа протягом років, що дає зловмисникам достатньо часу для злому.

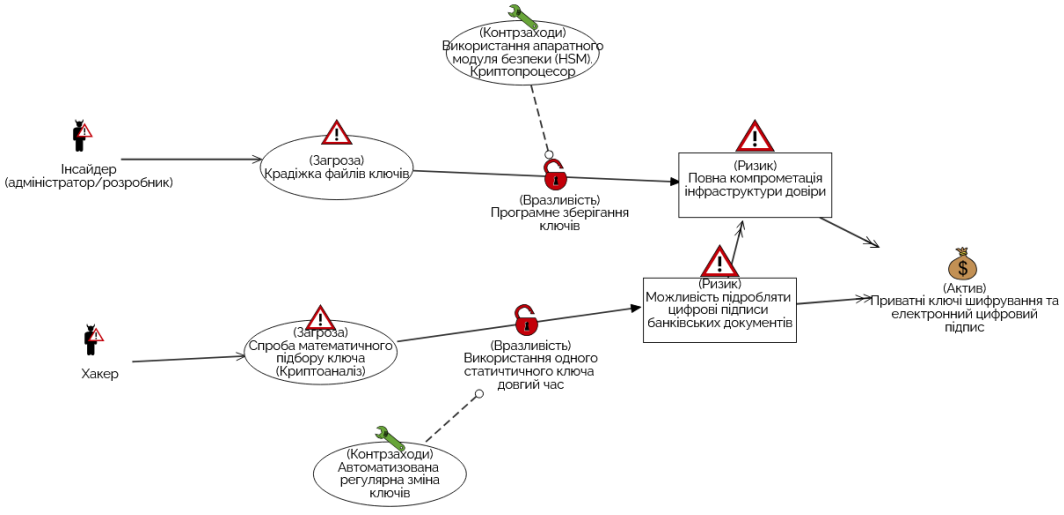

Рисунок 2.5 – Модель загроз приватних ключів шифрування та ЕЦП

Наслідками реалізації цих загроз можуть стати повна компрометація інфраструктури довіри (PKI), що дозволяє зловмисникам розшифрувати весь трафік (включно з архівним), а також виникнення ризику підробки особистості (Impersonation/Spoofing) – можливості фальсифікувати цифрові підписи банківських документів. Для протидії цим ризикам та усунення вразливостей PKI-адміністратор спільно з Архітектором безпеки повинні організувати різнопланові контрзаходи: для захисту від крадіжки впровадити використання апаратних модулів безпеки (HSM), де ключ генерується та живе виключно всередині чіпа, а для захисту від криптоаналізу – налаштувати політику автоматизованої регулярної зміни ключів, що знецінює вкрадені або старі ключі.

Мобільний додаток та веб-клієнт являють собою невід'ємну складову екосистеми дистанційного банкінгу, що виступає основною точкою входу для користувачів послуг. Унікальність та водночас критичність цього активу полягає в тому, що він функціонує за межами контрольованого периметра безпеки банку (безпосередньо на пристроях клієнтів), при цьому містить фрагменти бізнес-логіки, що належить певній організації та не є загальнодоступною, та здійснює обробку чутливих персональних даних у реальному часі.

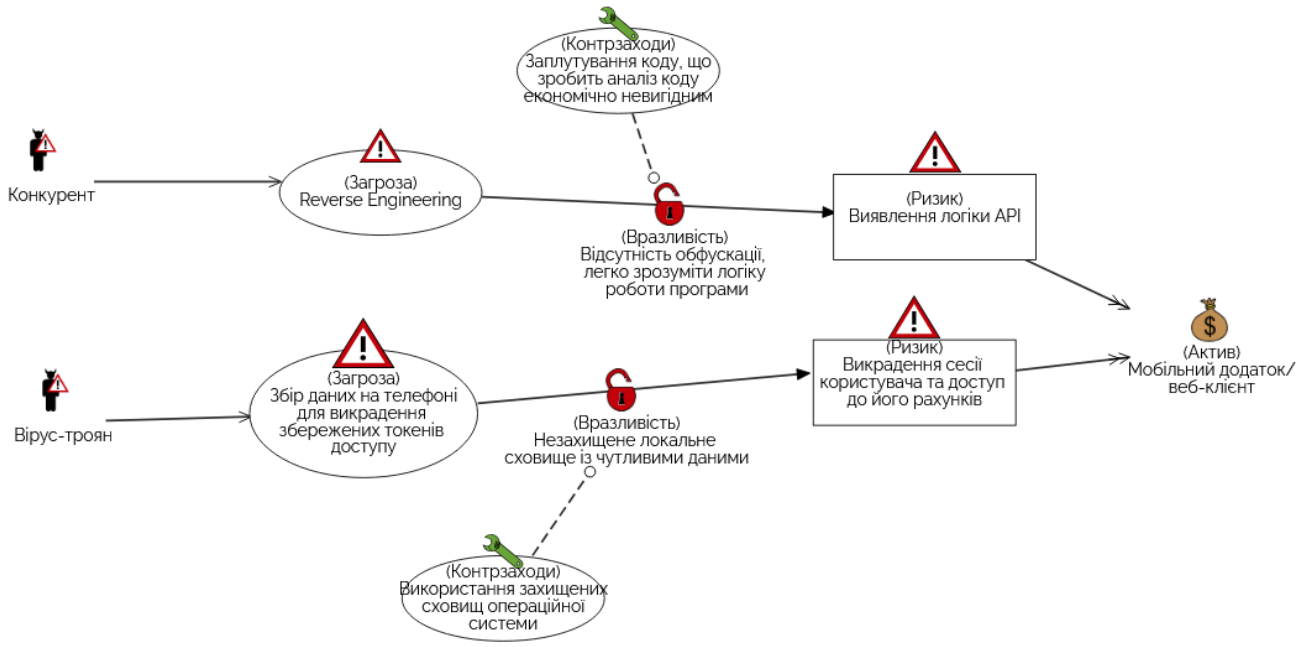

Рисунок 2.6 – Модель загроз мобільного додатку та веб-клієнта

Як і в минулих разах, вектори атак розгалужуються розділяються на дві частини. Перший шлях пов'язаний із діяльністю конкурентів, які створюють загрозу зворотної розробки (Reverse Engineering). Реалізація цього сценарію стає можливою через вразливість відсутності обфускації, коли “чистий” та читабельний код дозволяє стороннім особам легко зрозуміти логіку роботи програми. Другий шлях атаки реалізується шкідливим програмним забезпеченням (вірусом-трояном) безпосередньо на пристрої клієнта. Тут загрозою виступає збір даних на телефоні для викрадення збережених токенів доступу, що стає можливим через вразливість незахищеного локального сховища із чутливими даними.

Наслідками реалізації цих загроз можуть стати виявлення внутрішньої логіки API для підготовки подальших атак на сервер, а також викрадення сесії користувача (Account Takeover), що надає зловмисникам повний доступ до його рахунків. Для протидії цим ризикам та вразливостям розробники та QA-інженери з безпеки повинні створити такі контрзаходи, як впровадження заплутування коду (обфускацію), що зробить його аналіз економічно невигідним, та забезпечити використання захищених сховищ операційної системи (Keystore/Keychain) для шифрування даних апаратними засобами.

2.2 Моделі загроз цілісності

Якщо забезпечення конфіденційності є умовою збереження банківської таємниці, то гарантування цілісності виступає фундаментом коректності функціонування всієї фінансової системи. У цьому розрізі застосування методології STRIDE дозволяє змістити фокус аналізу на загрози категорії Tampering (фальсифікація/втручання). Дослідження активів через цю призму уможливлює виявлення векторів атак, спрямованих на несанкціоновану модифікацію платіжних транзакцій, балансів рахунків та журналів аудиту, де будь-яка зміна даних може призвести до прямих фінансових збитків. Хоча

STRIDE ефективно ідентифікує такі точки входу, для повноцінної побудови захисту необхідна подальша деталізація сценаріїв впливу.

Для побудови моделей загроз цілісності було зазначено також 6 активів: головна бухгалтерська книга та баланси рахунків, платіжні файли та повідомлення, довідкові дані та курси валют, вихідний код та виконувані файли ПЗ, налаштування мережевого обладнання, веб-контент офіційного сайту.

Головна бухгалтерська книга та баланси рахунків являють собою ключовий фінансовий реєстр банку, що відображає реальний стан активів клієнтів та самої установи. Забезпечення математичної точності та незмінності цих записів є критичною умовою стабільності, адже будь-яке викривлення даних підриває основи операційної діяльності. Повну схему із двома векторами атак можна розглянути на рисунку 2.7.

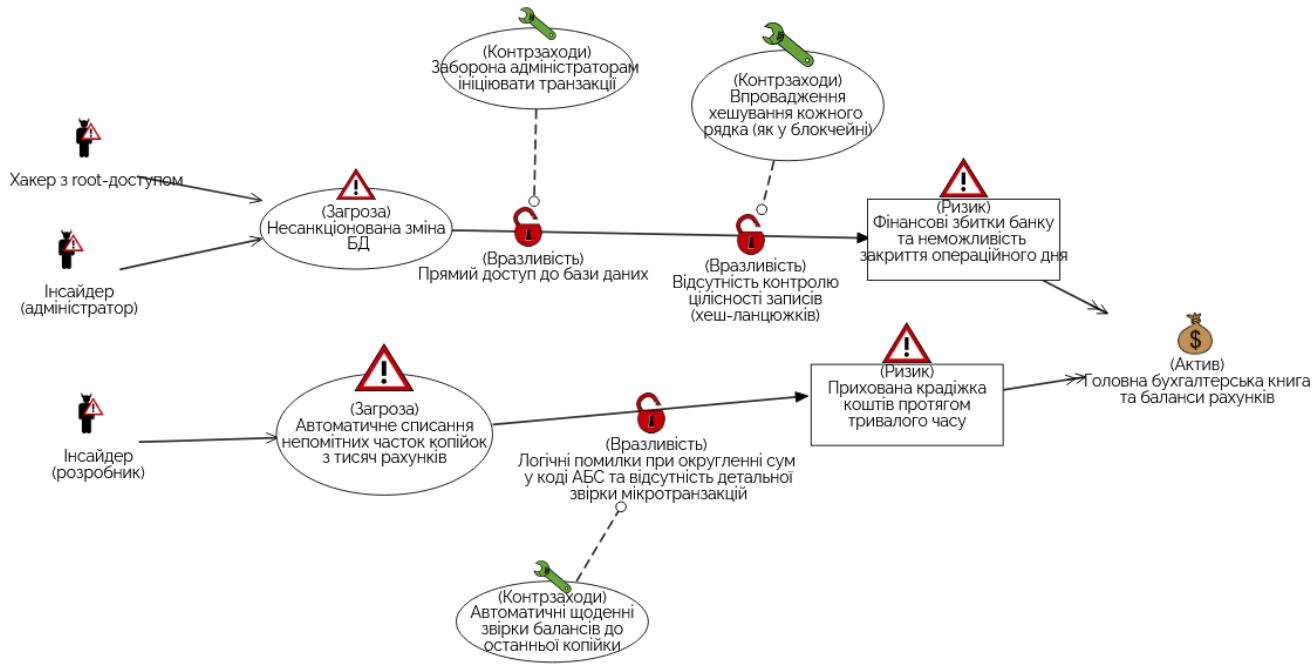

Рисунок 2.7 – Модель загроз головної бухгалтерської книги та балансу рахунків

Перший вектор атаки пов'язаний із грубим втручанням у базу даних. Джерелом цієї загрози виступає нечесний адміністратор (інсайдер) або зовнішній хакер, що отримав права суперкористувача. Вони створюють загрозу несанкціонованої модифікації, змінюючи значення балансів вручну через SQL-

запити. Реалізація цього сценарію стає можливою через критичні вразливості: наявність прямого доступу до таблиць в обхід бізнес-логіки АБС та відсутність контролю цілісності записів (хеш-ланцюжків). Наслідком таких дій стають прямі фінансові збитки через незабезпечену емісію грошей та неможливість закриття операційного дня. Для протидії цьому вектору Головний бухгалтер та IT-аудитори повинні забезпечити заборону адміністраторам ініціювати транзакції та впровадити криптографічне хешування кожного рядка, що зробить будь-яку ручну зміну очевидною.

Другий вектор атаки, що має більш прихований характер, ініціюється інсайдером-розробником. Загрозою тут виступає “Salami Attack” – автоматичне списання непомітних часток копійок із тисяч рахунків на користь зловмисника. Цей сценарій стає реальним через експлуатацію вразливості логічних помилок при округленні сум у коді та відсутності детальної звірки мікротранзакцій. Ризиком у даному випадку є прихована крадіжка коштів протягом тривалого часу, яку важко виявити стандартними методами. Ефективним контрзаходом для нівелювання цієї загрози є впровадження процесів автоматичної щоденної звірки балансів (Reconciliation Processes) до останньої копійки, що дозволяє системі миттєво сигналізувати про найменші розбіжності в розрахунках.

Платіжні файли та транзакцій (Payment Orders / SWIFT) також становлять критично важливий актив фінансової установи, оскільки вони виступають основним інструментом міжбанківської взаємодії та комунікації з процесинговими центрами й НБУ. Ці дані є фактичним цифровим еквівалентом грошей у русі, тому забезпечення їхньої незмінності під час передачі є пріоритетним завданням безпеки.

В створеній моделі загроз даного активу (рисунок 2.8) перший вектор атаки ініціюється хакером, який діє в мережі провайдера або на проміжному вузлі маршрутизації. Він створює загрозу атаки типу “Людина посередині” (Man-in-the-Middle), перехоплюючи пакет даних “на льоту” та непомітно змінюючи платіжні реквізити отримувача (IBAN) перед тим, як файл надійде до банку. Реалізація цього сценарію стає можливою через вразливість передачі структурованих файлів

(XML/JSON) без цифрового підпису та відсутність механізмів перевірки цілісності на стороні отримувача. Наслідком такої маніпуляції є безповоротний переказ коштів на рахунки шахраїв.

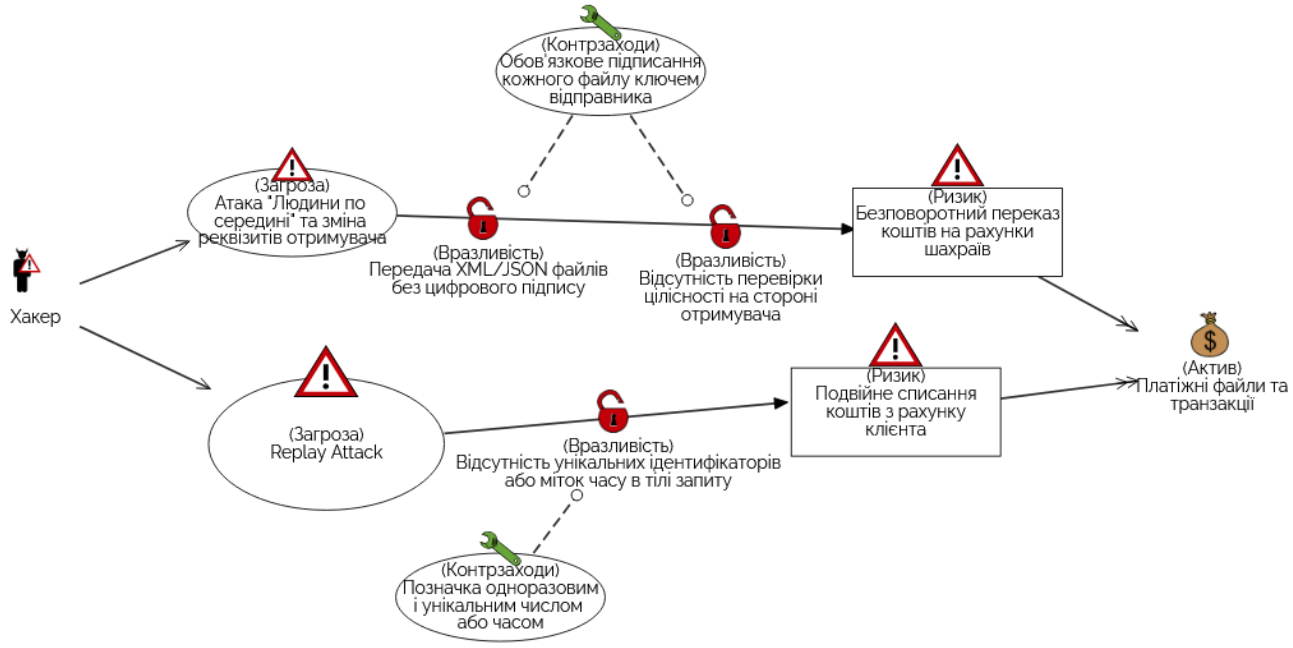

Рисунок 2.8 – Модель загроз платіжних файлів та транзакцій

Другий вектор атаки пов'язаний із категорією “Spoofing” і реалізується зловмисником, який пасивно прослуховує трафік. Загрозою тут виступає атака повторного відтворення (Replay Attack), коли хакер не змінює вміст файлу, а просто повторно надсилає перехоплений легітимний файл транзакції. Успіху цієї атаки сприяє технічна вразливість – відсутність унікальних ідентифікаторів або міток часу безпосередньо в тілі запиту, через що система не може відрізнити оригінал від дубліката. Це створює ризик помилкового подвійного списання коштів із рахунку клієнта. Для нейтралізації обох векторів криптограф та інженер з інтеграції повинні впровадити обов'язкове підписання кожного файлу ключем відправника (ЕЦП/КЕП) для захисту від змін, а також додати механізм перевірки міток часу або унікальних одноразових чисел для запобігання дублюванню.

Довідкові дані та курси валют є динамічним та критичним активом, оскільки вони включають бази даних із поточними курсами валют, відсотковими

ставками та комісійними тарифами, що використовуються автоматизованою банківською системою (АБС) для проведення всіх розрахунків. Забезпечення їх достовірності є ключовим для фінансової стабільності банку.

В моделі загроз цілісності даного активу виділено два вектори атак, що класифікуються як “Tampering” (Фальсифікація)(рисунок 2.9). Перший вектор пов'язаний із маніпуляцією ринковим курсом. Джерелом цієї загрози виступає нечесний трейдер (інсайдер) або зовнішній хакер, що отримав доступ до підсистеми казначейства. Загроза полягає у несанкціонованій зміні курсу обміну на короткий проміжок часу для проведення власних спекулятивних операцій за заниженою вартістю. Реалізація цього сценарію стає можливою через вразливість відсутності вхідного контролю, коли система приймає будь-які числові значення без перевірки на адекватність ринковим умовам. Наслідком є миттєва втрата величезних сум на різниці курсів (фінансовий арбітраж). Для протидії цьому Ризик-менеджер повинен впровадити лімітний контроль, який автоматично блокує аномальні зміни курсів.

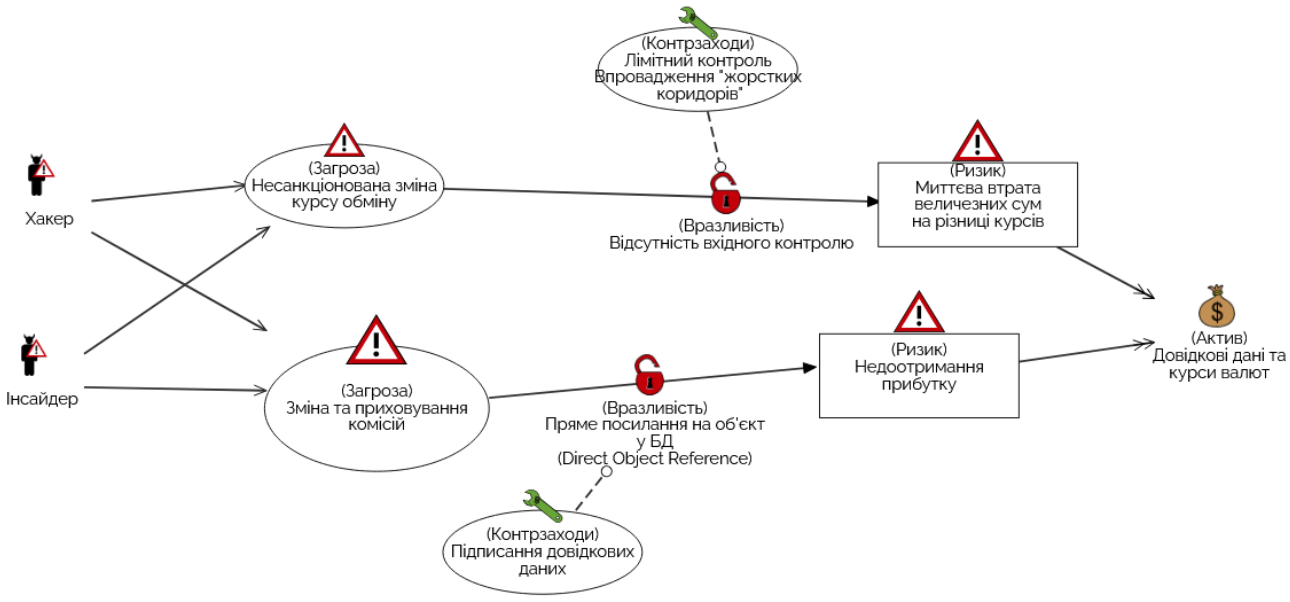

Рисунок 2.9 – Модель загроз довідкових даних та курсу валют

Другий вектор атаки спрямований на підміну тарифних планів. Джерелом виступає співробітник бек-офісу або зловмисник, що діє через SQL-ін'єкцію. Вони створюють загрозу приховування комісій, змінюючи параметри довідників так, щоб для певних клієнтів комісія становила 0%. Успіху атаки сприяє вразливість прямого посилання на об'єкт у БД (Direct Object Reference), коли таблиці тарифів не захищені від ручних змін. Ризиком у цьому випадку виступає недоотримання прибутку банком. Ефективним контрзаходом, який мають забезпечити технолог банку та адміністратор АБС, є підписання довідкових даних електронним ключем, що дозволяє системі перевіряти цілісність тарифів перед їх використанням.

Програмне забезпечення, що охоплює АБС, платформи веб-банкінгу та мобільні додатки, формує операційне ядро фінансової установи. Гарантування автентичності вихідного коду та виконуваних файлів є фундаментом довіри до цифрових сервісів, тому будь-яке неавторизоване втручання в ці компоненти класифікується як критична загроза фальсифікації (Tampering).

У межах аналізу цілісності системи особливу небезпеку становить атака на ланцюжок постачання (Supply Chain Attack) (рисунок 2.10). Її ініціаторами можуть виступати як внутрішні розробники зі злими намірами, так і хакери, що скомпрометували DevOps-інфраструктуру. Суть загрози полягає у непомітній інтеграції шкідливого функціоналу (бекдорів) безпосередньо на етапах створення чи компіляції продукту. Успішна реалізація цього сценарію зумовлена недостатньою захищеністю репозиторіїв коду (Git) та серверів автоматичної збірки (CI/CD). Це надає зловмисникам повний прихований контроль над системою через “чорний хід”. Ефективною відповіддю на цей виклик є впровадження обов'язкового цифрового підпису всіх бінарних файлів сертифікатом розробника, що блокує запуск будь-якого непідтвердженого компонента.

Інший напрямок атак експлуатує вразливості веб-інфраструктури, де зовнішні зловмисники намагаються завантажити веб-шелли – шкідливі скрипти, замасковані під легітимні документи чи зображення. Слабкою ланкою захисту в цьому випадку виступає дозвіл на виконання скриптів у директоріях завантажень

та відсутність інтегрованого моніторингу змін. Наслідком таких дій може стати непомітна модифікація бізнес-логіки, наприклад, підміна рахунків для зарахування комісій. Для нейтралізації цієї загрози DevSecOps-інженери зобов'язані розгорнути систему моніторингу цілісності файлів (FIM), яка забезпечує миттєве сповіщення про появу нових об'єктів або модифікацію існуючих.

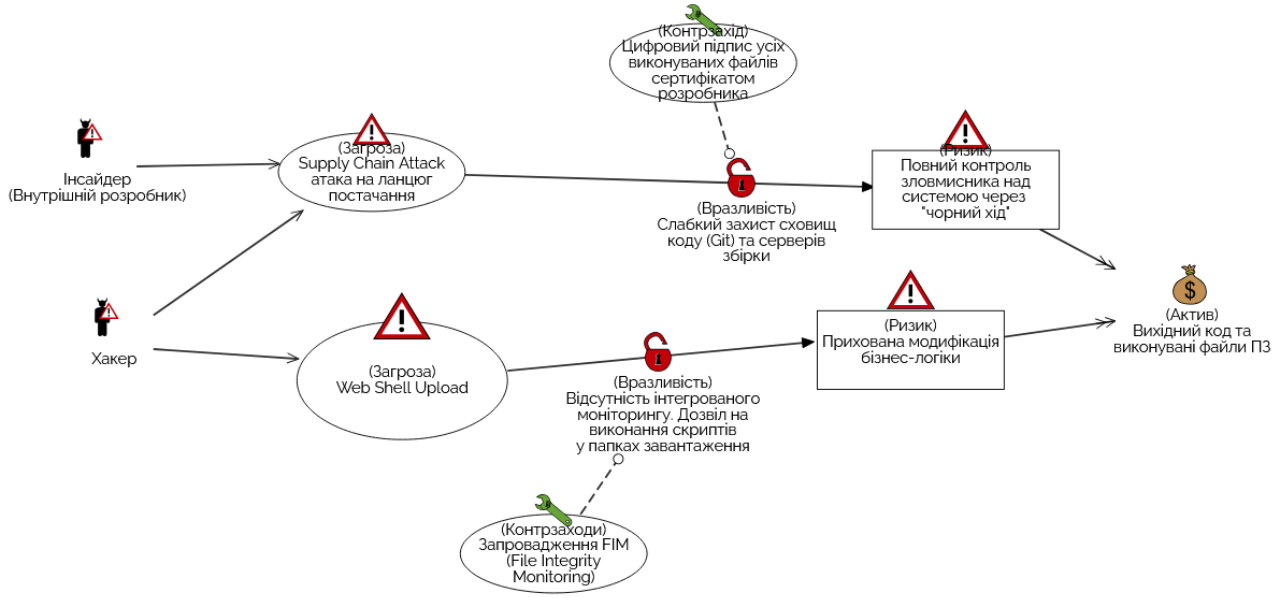

Рисунок 2.10 – Модель загроз вихідного коду та виконуваних файлів ПЗ

Налаштування мережевого обладнання, що охоплюють правила міжмережевих екранів (фаєрволів), таблиці маршрутизації та списки контролю доступу (ACL), виступають критичним активом, який визначає логіку руху інформаційних потоків та архітектуру безпеки банку. Несанкціоноване втручання в ці конфігурації здатне зруйнувати ізоляцію внутрішньої мережі.

У даній моделі загроз в наявності стільки ж векторів атак як і в попередніх активах (рисунок 2.11). Перший вектор спрямований на перехоплення трафіку і реалізується зовнішнім зловмисником, що вже проник у локальну мережу. Загроза полягає у маніпуляції таблицями маршрутизації (Route Poisoning), метою якої є перенаправлення потоків даних через підконтрольний хакеру вузол. Експлуатація

цієї загрози стає технічно можливою через використання незахищених протоколів управління (наприклад, Telnet) або стандартних паролів, що не забезпечують належного шифрування сесій адміністраторів. Це створює ризик появи прихованих каналів прослуховування або нелегітимного входу в мережу. Ефективною протидією є впровадження суворого контролю доступу за моделлю AAA (Authentication, Authorization, Accounting) із забороною незахищених протоколів.

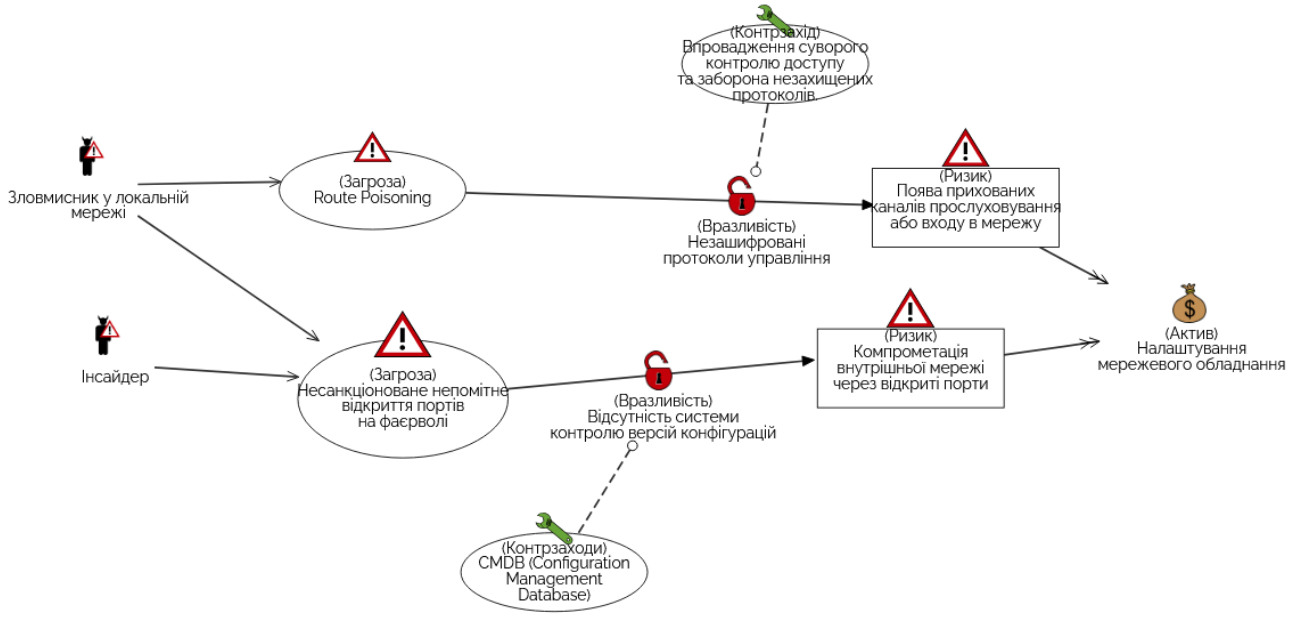

Рисунок 2.11 – Модель загроз налаштування мережевого обладнання

Другий вектор атаки фокусується на непомітному відкритті периметра безпеки. Його джерелом може бути як інсайдер, так і зовнішній зловмисник, що прагне модифікувати списки доступу (ACL Modification) для відкриття критичних портів з Інтернету. Успіху таких дій сприяє відсутність системи контролю версій конфігурацій, що унеможливлює оперативне виявлення несанкціонованих змін. Наслідком є пряма компрометація внутрішньої мережі через створені “діри” в захисті. Для нейтралізації цього ризику мережеві інженери та адміністратори інфраструктури повинні використовувати систему управління конфігураціями

(CMDB), яка забезпечує регулярний бекап налаштувань та автоматичне порівняння поточного стану обладнання з еталонним.

Веб-контент офіційного сайту, що включає новини, тарифні сітки та навігаційні елементи для входу в особисті кабінети, виконує функцію “цифрового обличчя” фінансової установи. Забезпечення незмінності та достовірності цієї інформації є критичним для підтримки довіри клієнтів.

Перший вектор атаки, що вказано на рисунку 2.12, має переважно ідеологічне або хуліганське підґрунтя та ініціюється політично вмотивованими хакерами (“хактивістами”). Загрозою тут виступає дефейс (Defacement) – демонстративна зміна головної сторінки сайту для розміщення сторонніх гасел, нецензурного контенту або фейкових повідомлень. Технічним підґрунтям для реалізації цього сценарію є експлуатація невиправлених помилок у системах управління контентом або їхніх плагінах. Наслідком таких дій стають катастрофічні репутаційні втрати та можлива паніка серед вкладників. Ефективним технічним бар'єром проти цього виступає Web Application Firewall (WAF), який аналізує вхідний HTTP-трафік та блокує специфічні запити, спрямовані на злом CMS.

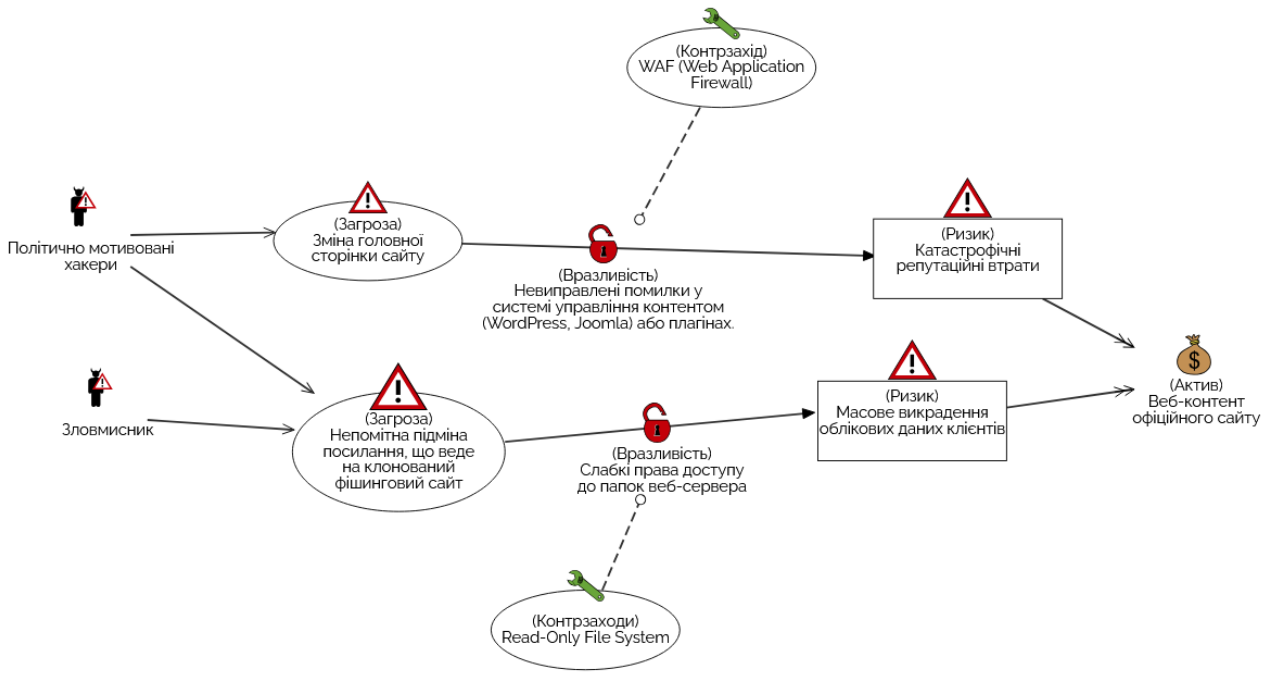

Рисунок 2.12 – Модель загроз веб-контенту офіційного сайту

Другий вектор атаки реалізується зловмисниками (фішерами) з корисливою метою. Суть загрози полягає у непомітній підміні посилання “Вхід в інтернет-банкінг” (Link Injection), що перенаправляє користувача на візуально ідентичний, але клонований фішинговий ресурс. Ця маніпуляція стає можливою через вразливість слабких прав доступу до директорій веб-сервера, що дозволяють запис стороннім користувачам. Ризиком у даному випадку є масове викрадення облікових даних клієнтів. Для нейтралізації цієї вразливості адміністратори повинні налаштувати файлову систему критичних каталогів у режим “тільки для читання” (Read-Only File System), дозволяючи внесення змін виключно через контрольований пайплайн розгортання.

2.3 Моделі загроз доступності

Якщо конфіденційність захищає дані від витоку, а цілісність – від спотворення, то доступність є гарантією безперервності надання сервісів, що для сучасної фінансової установи є синонімом її життєздатності. У контексті методології STRIDE основна увага зміщується на категорію загроз Denial of Service (відмова в обслуговуванні). Аналіз активів через цей вектор дозволяє ідентифікувати слабкі місця архітектури, спрямовані на вичерпання системних ресурсів або блокування легітимного доступу користувачів до банківських послуг. Хоча STRIDE дозволяє окреслити периметр таких атак, для побудови відмовостійкої інфраструктури необхідне глибше розуміння сценаріїв, що можуть призвести до критичних простоїв бізнесу.

Серед побудованих активів у частині доступності було зазначено такі: зовнішні канали зв’язку, публічні веб-сервіси, серверне обладнання, робочі дані та бази даних, мережа банкоматів, а також обліковий запис адміністратора домену.

Зовнішні канали зв'язку являють собою фундаментальний елемент інфраструктури доступності фінансової установи. Це фізичні та логічні з'єднання,

що забезпечують безперервний доступ банку до мережі Інтернет, міжнародних платіжних систем та Національного банку України. Втрата цих каналів фактично означає повну зупинку цифрових сервісів.

В створеній моделі загроз доступності даного активу (рисунок 2.13) виділено два ключові вектори атак, що класифікуються як “Denial of Service” (Відмова в обслуговуванні). Перший вектор має цифровий характер і реалізується оператором ботнету. Загрозою тут виступає об'ємна DDoS-атака, що полягає у спрямуванні на банк гігантського потоку “сміттєвого” трафіку. Успіх такої атаки зумовлений вразливістю обмеженої пропускної здатності каналів, які фізично не можуть впоратися з піковим навантаженням. Наслідком є повна цифрова ізоляція банку, що унеможливлює роботу клієнт-банку та банкоматів. Для протидії цьому необхідно впровадити маршрутизацію трафіку через спеціалізовані центри очищення (до прикладу, Cloudflare), які відфільтровують паразитні пакети до їх потрапляння в мережу банку.

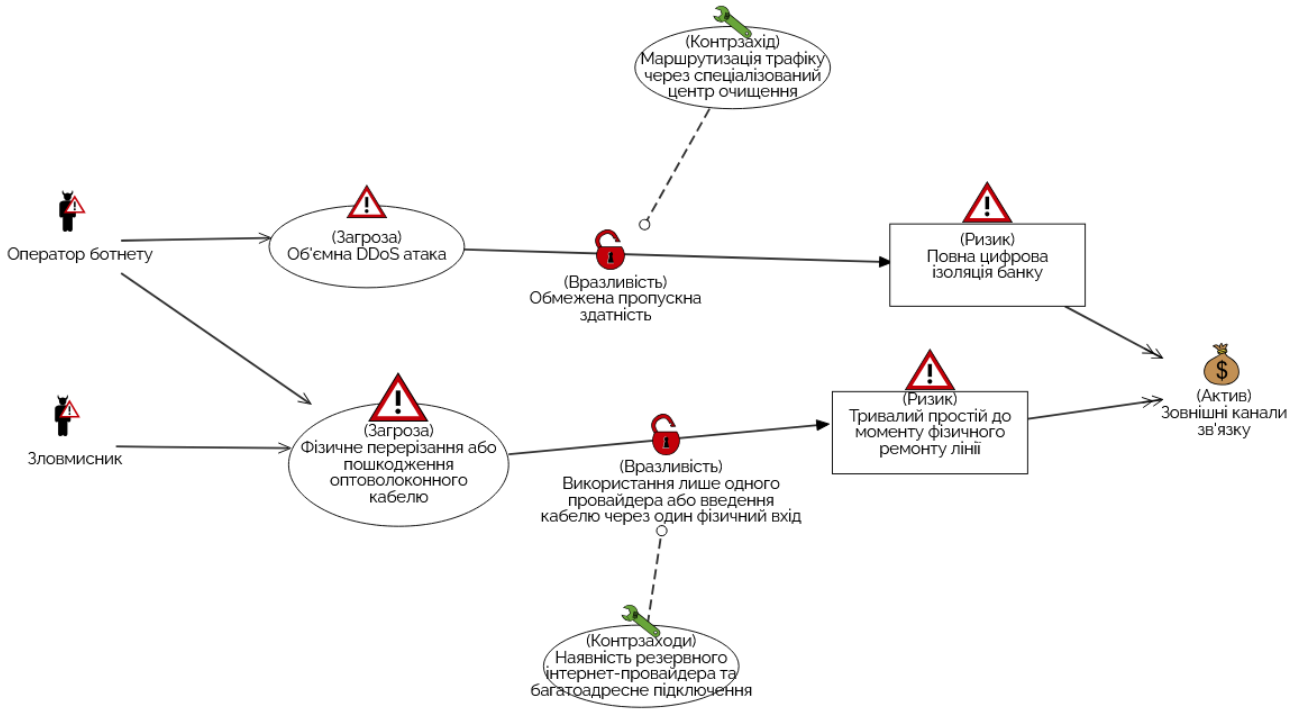

Рисунок 2.13 – Модель загроз зовнішніх каналів зв’язку

Другий вектор атаки пов'язаний із фізичним впливом, джерелом якого можуть бути вандали або диверсанти. Загроза полягає у фізичному перерізанні або пошкодженні оптоволоконного кабелю. Цей сценарій стає критичним через архітектурну вразливість “єдиної точки відмови” – використання лише одного провайдера або введення кабелів через один фізичний вхід. Ризиком у цьому випадку є тривалий простій установи до моменту фізичного ремонту лінії. Щоб нівелювати цю загрозу, мережевий архітектор повинен забезпечити підключення мінімум до двох незалежних провайдерів із географічно рознесеними маршрутами введення кабелів у будівлю.

Публічні веб-сервіси, до яких належать системи веб-банкінгу та мобільні API є критично важливим інтерфейсом взаємодії, що забезпечує цілодобове дистанційне обслуговування клієнтів. У контексті доступності (Availability) цей актив є найбільш вразливим до зовнішніх впливів, оскільки він за своєю природою має бути відкритим для світу.

В даному активі наявні два напрями атак (рисунок 2.14). Перший вектор спрямований на переповнення ресурсів і реалізується операторами ботнетів, хактивістами або конкурентами. Загрозою тут виступають масовані атаки на рівні додатку (HTTP Flood) або атаки “повільними” пакетами (Slowloris), що тримають з'єднання відкритими. Реалізація цих сценаріїв стає можливою через вразливості конфігурації: відсутність обмежень на кількість запитів з однієї IP-адреси та налаштування сервера чекати завершення запиту надто довго. Другий вектор атаки фокусується на виснаженні логічних ресурсів бази даних. Джерелом загрози виступає зловмисник, який надсилає спеціально сформовані “важкі” запити. Успіху таких дій сприяє наявність неоптимізованого коду бекенду, зокрема відсутність пагінації або лімітів на вибірку даних.

Наслідками реалізації цих загроз стають неможливість клієнтів отримати доступ до своїх рахунків (перевірити баланс, здійснити переказ) та повне падіння серверів баз даних, що паралізує роботу всіх залежних сервісів. Для протидії цим ризикам DevOps-інженер та адміністратор веб-сервера повинні організувати комплексний захист: впровадити інтелектуальну фільтрацію трафіку та жорсткі

обмеження за допомогою WAF, налаштувати автоматичне масштабування ресурсів, а також забезпечити балансування навантаження та оптимізацію запитів до бази даних.

Серверне обладнання та системи зберігання даних формують фізичний фундамент IT-ландшафту банку, охоплюючи критичну інфраструктуру: сервери, дискові масиви та комутаційні вузли. Безперебійна робота цих компонентів є запорукою доступності всіх банківських сервісів, тому будь-які збої в їх функціонуванні класифікуються як загроза відмови в обслуговуванні (Denial of Service).

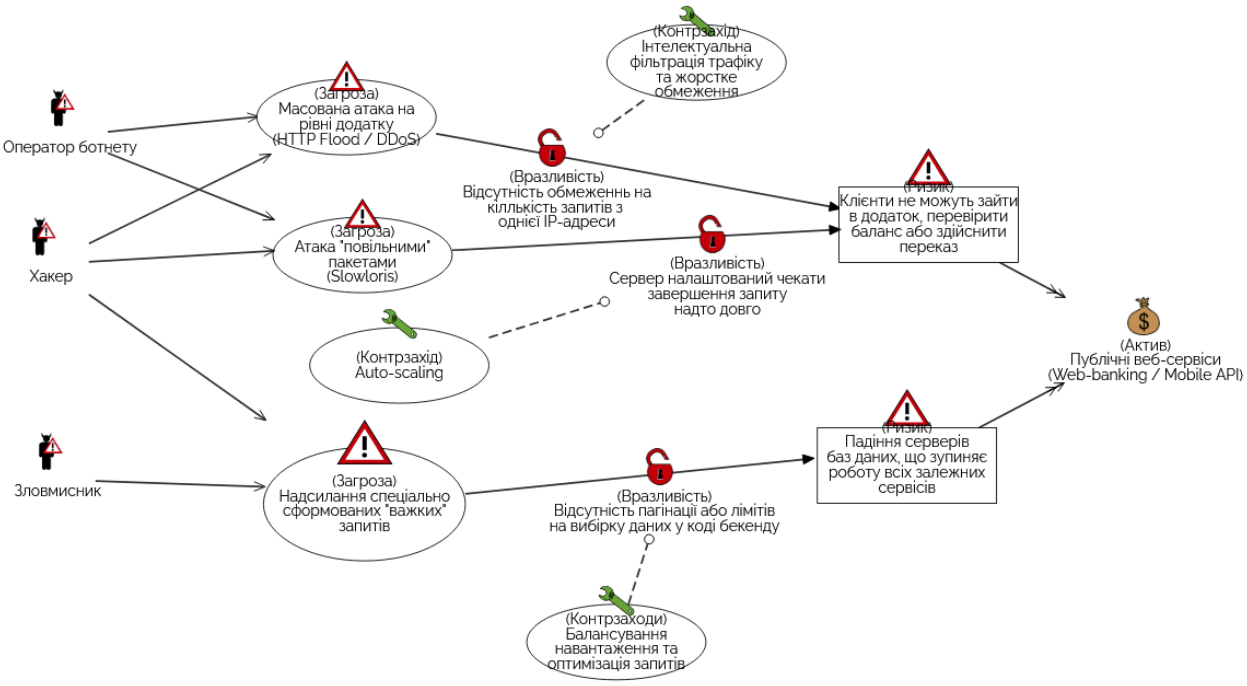

Рисунок 2.14 – Модель загроз публічних веб-сервісів

У перший вектор ризику зумовлений технологічними та природними чинниками, такими як фізичне зношення компонентів або виробничий брак (рисунок 2.15). Загроза тут проявляється у формі апаратного збою критичних вузлів (жорстких дисків, материнських плат), що стає критичним через архітектурну вразливість “єдиної точки відмови” – відсутність резервування та експлуатацію застарілого обладнання (End-of-Life). Наслідком таких інцидентів

стає фізична зупинка обробки даних та незворотна втрата інформації, що знаходилася в оперативній пам'яті. Для нівелювання цього ризику необхідно застосовувати технології віртуалізації та надлишковості: розгортання HA-кластерів (High Availability) для міграції навантажень та використання RAID-масивів (рівнів 6 або 10), тобто об’єднання багатьох дисків в один логічний том, що дозволяють пережити відмову носіїв без зупинки сервісу.

Другий сценарій загрози носить інфраструктурний характер і пов'язаний із форс-мажорними обставинами, такими як блекаути, пожежі або аварії систем життєзабезпечення. Вразливістю системи у цьому випадку є пряма залежність від міської електромережі та систем кондиціювання без належного дублювання. Це створює загрозу повного знеструмлення або аварійного вимкнення серверів через перегрів, що призводить до неконтрольованого тотального блекауту і потенційного пошкодження файлових систем. Завдання системних адміністраторів та інженерів з експлуатації центру обробки даних – забезпечити енергетичну автономність шляхом встановлення джерел безперебійного живлення (UPS), дизель-генераторів та двоконтурних систем охолодження.

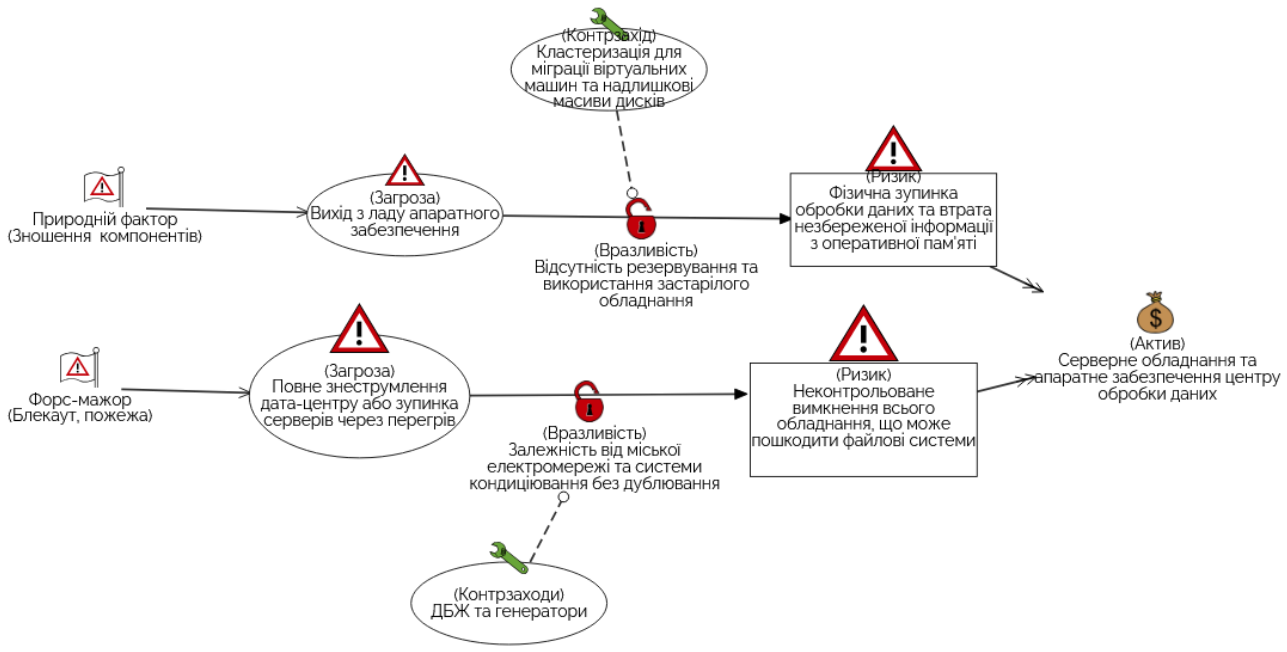

Рисунок 2.15 – Модель загроз серверного обладнання та апаратного забезпечення центру обробки даних

Робочі файли та бази даних становлять інформаційний фундамент операційної діяльності фінансової установи, забезпечуючи безперервність щоденних бізнес-процесів. Гарантування їх постійної наявності для читання та запису є важливим завданням.

У межах проведеного аналізу моделі доступності (рисунок 2.16), домінантним вектором зовнішньої загрози виступає діяльність кіберзлочинних угруповань, що спеціалізуються на атаках програм-вимагачів (Ransomware). Суть загрози полягає у тотальному шифруванні файлів на серверах і робочих станціях з вимогою викупу. Успішна реалізація цього сценарію стає можливою через поєднання критичних вразливостей: відсутності ізольованих “холодних” резервних копій (офлайн-бекапів) та несвоєчасного оновлення сигнатур антивірусного захисту. Наслідком атаки є повна паралізація операційної діяльності банку на дні або навіть тижні. Для нейтралізації цієї загрози Адміністратор резервного копіювання повинен забезпечити зберігання архівів на носіях, фізично відключених від мережі, та контроль актуальності засобів захисту.

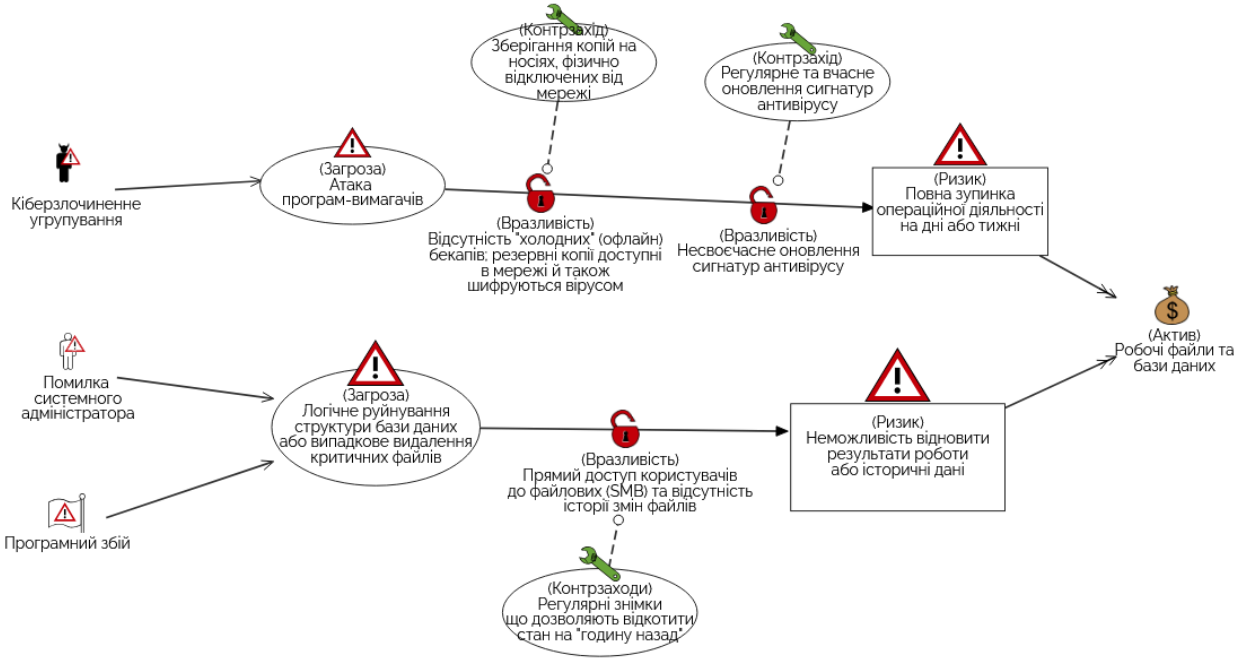

Рисунок 2.16 – Модель загроз робочих файлів та бази даних

Другий сценарій носить внутрішній техногенний характер і пов'язаний із людським фактором (помилкою системного адміністратора) або програмними збоями. Загроза проявляється у логічному руйнуванні структури бази даних або випадковому видаленні критичних файлів. Цьому сприяють такі архітектурні недоліки, як надання користувачам прямого доступу до файлових ресурсів (SMB) та відсутність історії змін (версійності). Ризиком у даному випадку є неможливість відновлення результатів роботи або історичних даних. Ефективним механізмом захисту виступає впровадження технології регулярних миттєвих знімків файлової системи (Snapshots), що надає можливість оперативного відкату стану даних на попередній часовий проміжок.

Мережа банкоматів (ATM) виступає ключовою ланкою інфраструктури самообслуговування, забезпечуючи фізичний доступ клієнтів до готівкових коштів у режимі 24/7. Стабільність функціонування цього каналу є критичною для репутації банку, тому будь-які перебої в роботі терміналів можуть теж привести до репутаційних втрат, хоч і в менших масштабах.

У межах схеми доступності виявлено, що перший вектор загрози фокусується на розриві комунікацій (рисунок 2.17). Його джерелом можуть бути як технічні збої на стороні мобільного оператора, так і цілеспрямовані дії злочинців, що використовують портативні пристрої для глушіння частот LTE/4G (Signal Jamming). Успішна реалізація атаки зумовлена архітектурною вразливістю – залежністю терміналу від єдиного каналу зв'язку без резервування. Наслідком стає втрата з'єднання з процесинговим центром та перехід банкомату в неробочий стан. Для забезпечення безперервності обслуговування служба моніторингу мережі повинна впровадити використання промислових роутерів із підтримкою двох активних SIM-карт різних операторів, що дозволить миттєво перемикати канал передачі даних у разі збою.

Другий вектор ризику має фізичну природу і пов'язаний з діями вандалів або грабіжників, які застосовують атаки типу “Black Box”. Загроза проявляється у механічному пошкодженні обладнання (розбиття екранів, залиття компонентів) або несанкціонованому підключенні до диспенсера для видачі готівки.

Експлуатації цих загроз сприяють легкий фізичний доступ до сервісних портів та кабелів, а також нестабільність застарілих операційних систем. Результатом таких інцидентів стають значні фінансові витрати на ремонт та тривалий простій точки обслуговування. Комплексний захист вимагає від служби інкасації та технічних спеціалістів встановлення датчиків вібрації та нахилу для оперативного сповіщення охорони, а також міграції парку банкоматів на сучасні захищені операційні системи.

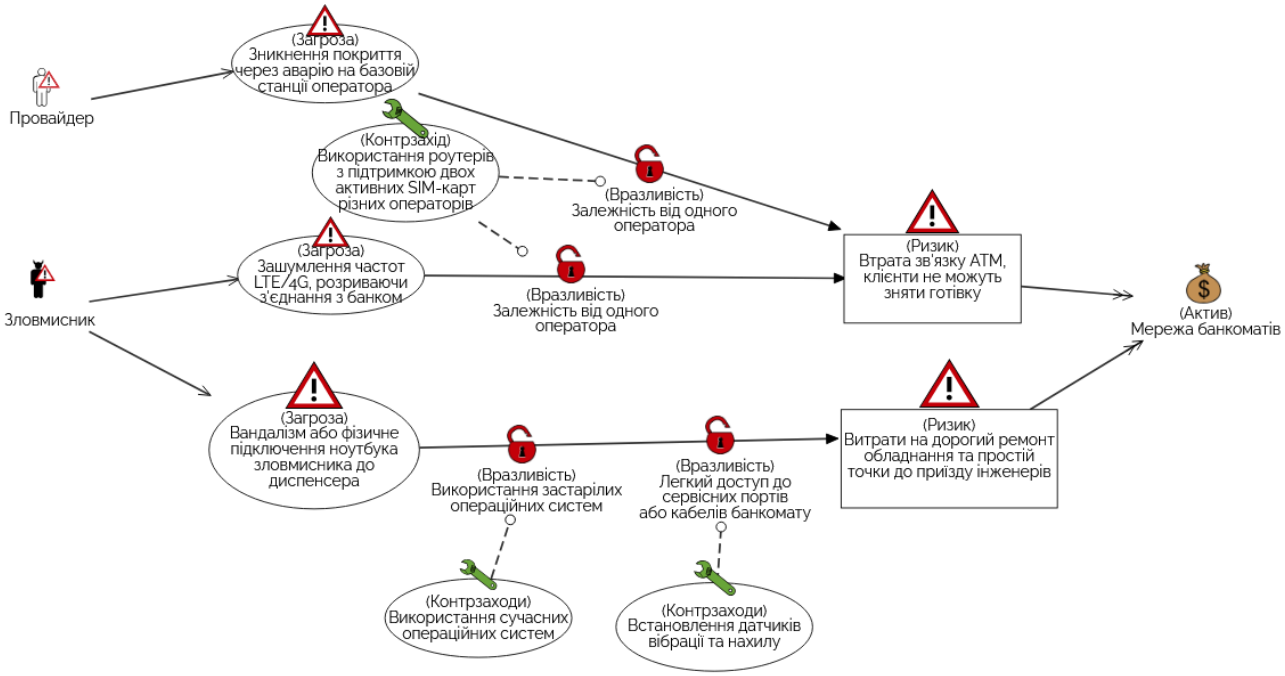

Рисунок 2.17 – Модель загроз мережі банкоматів

Обліковий запис “Адміністратор домену” виступає центральним елементом управління IT-інфраструктурою, надаючи повний контроль над системами банку. Його доступність для легітимного власника є критичною умовою безперервності бізнес-процесів, тому атаки на цей актив часто спрямовані саме на блокування можливості входу або перехоплення управління із зовнішнього периметра.

У межах аналізу доступності виявлено специфічний вектор атаки, де механізми захисту використовуються проти самої установи (рисунок 2.18). Зовнішні зловмисники або ботнети, скануючи публічні сервіси, ініціюють

масований підбір паролів (Brute-force). Метою цих дій є не стільки вгадування пароля, скільки провокування системи безпеки на автоматичну реакцію. Через вразливість глобальної політики блокування, яка не розрізняє джерела запитів, акаунт адміністратора переходить у статус “Locked”. Це призводить до адміністративного паралічу, коли відповідальна особа не може увійти в систему для реагування на інциденти. Для вирішення цієї проблеми IAM-архітектор повинен впровадити технологію Smart Lockout, яка інтелектуально фільтрує спроби входу, блокуючи лише підозрілі IP-адреси зловмисників, а не цільовий акаунт.

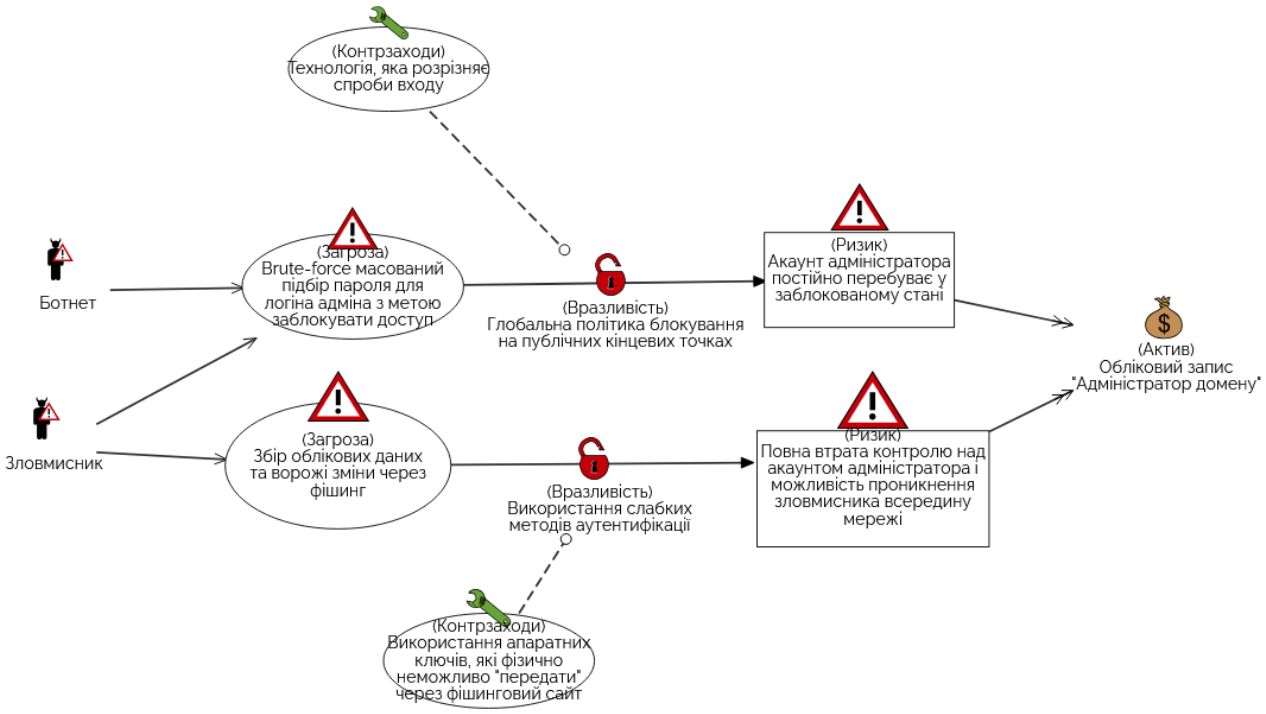

Рисунок 2.18 – Модель загроз облікового запису адміністратора домену

Паралельний вектор загрози реалізується методами соціальної інженерії (Spear Phishing) і спрямований на захоплення контролю ще до проникнення всередину мережі. Зловмисники виманюють облікові дані через підроблені сайти та миттєво змінюють пароль, відрізаючи легітимного власника від доступу. Успіх такої атаки зумовлений використанням слабких методів аутентифікації на зовнішніх порталах. Ризиком тут є повна втрата контролю над інфраструктурою

та можливість безперешкодного проникнення всередину. Ефективним бар'єром проти цього виступає використання апаратних ключів (Hardware Tokens), фізична наявність яких є обов'язковою умовою входу, що робить передачу доступу через фішинговий сайт неможливою.

2.4 Висновок до розділу

У другому розділі магістерської роботи проведено комплексне моделювання системи інформаційної безпеки фінансової установи, що базується на адаптованій методології STRIDE. Декомпозиція 12 ключових інформаційних активів дозволила сформувати та проаналізувати 40 детальних сценаріїв реалізації загроз у трьох ключових площинах: конфіденційності, цілісності та доступності.

Аналіз моделей конфіденційності підтвердив, що найбільш критичними активами є база даних клієнтів, дані платіжних карток та криптографічні ключі. Встановлено, що окрім класичних зовнішніх атак, значну небезпеку становлять інсайдери з легітимним доступом та недбалість персоналу, зокрема вразливість до фішингу та атак типу Mimikatz. Окрему увагу було приділено мобільним додаткам, де виявлено критичні ризики зворотної розробки (Reverse Engineering) та викрадення токенів доступу. Виявлено, що надійний захист цих активів вимагає переходу від статичних методів (парольний захист) до динамічних та багаторівневих (MFA, токенізація, використання HSM).

У розрізі забезпечення цілісності доведено, що фінансова стабільність установи безпосередньо залежить від незмінності транзакційних даних (SWIFT), довідників тарифів та вихідного коду програмного забезпечення. Моделювання показало вразливість системи перед прихованими маніпуляціями, такими як атаки на округлення («Salami attack») або підміна реквізитів у транзиті (MitM). Критично важливими контрзаходами визначено впровадження наскрізного криптографічного контролю (ЕЦП, хешування) та автоматизованих процедур звірки, які здатні виявляти аномалії, непомітні для ручного моніторингу.

Дослідження аспектів доступності виявило високу залежність безперервності бізнес-процесів від стійкості зовнішніх каналів зв'язку, мережі банкоматів та серверної інфраструктури. Загрози у цій сфері варіюються від грубих об'ємних DDoS-атак та фізичного вандалізму до витончених логічних атак на рівні веб-сервісів (HTTP Flood, Slowloris). Аналіз банкоматної мережі виявив проблему «єдиної точки відмови» через залежність від одного провайдера зв'язку. Визначено, що забезпечення прийнятних показників відновлення (RTO/RPO) неможливе без архітектурного резервування (HA-кластери, мультихомінг) та впровадження ізольованих систем резервного копіювання для захисту від програм-вимагачів.

Узагальнюючи результати розділу, можна стверджувати, що ефективна система менеджменту інформаційної безпеки фінансової установи не може будуватися виключно на технічних засобах. Вона вимагає синергії технологічних рішень (WAF, DLP, SIEM), організаційних заходів (політики, навчання персоналу) та архітектурних змін. Водночас, виявлена значна кількість різнорідних загроз та пропонованих локальних контрзаходів вказує на ризик надмірної фрагментації системи захисту. Це обґрунтовує необхідність переходу в наступному розділі до кількісного оцінювання ризиків та економічного моделювання, що дозволить дозволить виділити головні загрози та створити єдину й економічно вигідну систему захисту.

3 ОЦІНЮВАННЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Розробка моделі оцінювання системи менеджменту інформаційної безпеки

На основі графічних моделей загроз, розроблених у другому розділі, проведено систематизацію векторів атак згідно з класифікацією STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Метою цього етапу є трансформація візуальних схем причинно-наслідкових зв'язків у структурований реєстр, що дозволить формалізувати вимоги до системи захисту.

Для забезпечення повноти покриття ризиків, реєстр розділено на три частини відповідно до базових властивостей інформації: конфіденційність (Таблиця 3.1), цілісність (Таблиця 3.2) та доступність (Таблиця 3.3). Кожен запис у таблицях відображає унікальний шлях реалізації загрози: від джерела через вразливість до активу. Така деталізація дозволяє наочно продемонструвати різноманітність необхідних засобів захисту при використанні класичного підходу, що стане підґрунтям для подальшого обґрунтування необхідності оптимізації витрат

Таблиця 3.1 – Реєстр загроз порушення конфіденційності

ID	Актив	Категорія STRIDE	Опис загрози	Експлуатована вразливість	Запропонований контрзахід (STRIDE)
1	2	3	4	5	6
C-01	База даних клієнтів	I (Disclosure)	Insider Threat: Копіювання бази адміністратором для продажу конкурентам.	Зберігання резервних копій у незашифрованому вигляді; надмірні права доступу.	Шифрування файлів “у стані спокою” (TDE).
C-02	База даних клієнтів	I (Disclosure)	SQL Injection: Вивантаження таблиць через веб-інтерфейс.	Невиправлені вразливості у СУБД; відсутність санітизації вводу.	Моніторинг запитів (DAM).

Продовження таблиці 3.1

1	2	3	4	5	6
С-03	База даних клієнтів	E (Elevation)	Privilege Escalation: Підвищення прав до адміністратора через баг у ПЗ.	Невиправлені вразливості (патчі) в СУБД.	Суворе розмежування прав доступу (RBAC).
С-04	Дані платіжних карток	I (Disclosure)	Sniffing: Перехоплення трафіку в мережі.	Передача даних картки у відкритому вигляді (HTTP замість HTTPS); вразливість Heartbleed.	Використання актуальних протоколів шифрування (TLS 1.3).
С-05	Дані платіжних карток	I (Disclosure)	RAM Scraping: Зчитування даних з оперативної пам'яті серверів.	Зберігання даних в пам'яті у відкритому вигляді до моменту шифрування.	Токенізація даних.
С-06	Облікові записи персоналу	S (Spoofing)	Brute-force: Масований підбір паролів.	Слабка політика паролів (прості паролі); відсутність блокування.	Запровадження політики парольного захисту.
С-07	Облікові записи персоналу	S (Spoofing)	Phishing: Виманювання пароля через підроблені листи.	Відсутність багатофакторної автентифікації (MFA).	Обов'язкова MFA.
С-08	Облікові записи персоналу	I (Disclosure)	Mimikatz-атаки: Витягування хешів паролів з пам'яті комп'ютера.	Зберігання паролів у відкритому вигляді або слабке хешування в ОС.	Навчання персоналу та EDR-системи.
С-09	Електронний документообіг	I (Disclosure)	Industrial Espionage: Шпигунство конкурентів.	Неправильно налаштовані права доступу до файлових шарів.	Шифрування файлу з обмеженням прав (IRM/DRM).

Кінець таблиці 3.1

1	2	3	4	5	6
С-10	Електронний документообіг	I (Disclosure)	Misdelivery: Випадкова відправка документа на зовнішню пошту.	Використання публічних хмарних сервісів; відсутність маркування.	DLP-система (Data Loss Prevention).
С-11	Ключі шифрування (Private Keys)	I (Disclosure)	Key Exfiltration: Крадіжка файлів ключів інсайдером або хакером.	Програмне зберігання ключів на диску; доступність файлів для копіювання.	Використання апаратного модуля безпеки (HSM).
С-12	Ключі шифрування (Private Keys)	I (Disclosure)	Cryptanalysis: Спроба математичного підбору ключа.	Використання одного статичного ключа довгий час (відсутність ротації).	Автоматизована регулярна зміна ключів.
С-13	Мобільний додаток	I (Disclosure)	Reverse Engineering: Декомпіляція додатку для аналізу логіки.	Відсутність обфускації (“чистий” читабельний код).	Заплутування коду (Code Obfuscation).
С-14	Мобільний додаток	I (Disclosure)	Data Harvesting: Збір даних на телефоні (викрадення токенів).	Незахищене локальне сховище із чутливими даними.	Використання захищених сховищ ОС (Keystore/Keychain).

Аналіз загроз конфіденційності, наведений у таблиці 3.1, демонструє, що витік чутливої інформації можливий на всіх рівнях інфраструктури: від баз даних та мережевих каналів до кінцевих точок мобільних додатків. Характерно, що значна частина ризиків пов'язана не лише із зовнішніми технічними атаками, а й з інсайдерськими діями та людським фактором, що вимагає впровадження

різнопланових методів захисту – від шифрування та обфускації до організаційних політик та навчання персоналу.

Таблиця 3.2 – Реєстр загроз порушення цілісності

ID	Актив	Категорія STRIDE	Опис загрози	Експлуатована вразливість	Запропонований контрзахід (STRIDE)
1	2	3	4	5	6
I-01	Головна бухгалтерська книга	T (Tampering)	Unauthorized DB Mod: Ручна зміна балансів через SQL.	Прямий доступ до таблиць; відсутність хеш-контролю.	Хешування кожного рядка транзакції.
I-02	Головна бухгалтерська книга	T (Tampering)	Salami Attack: Автоматичне списання мікро-сум.	Логічні помилки округлення; відсутність мікро-звірки.	Автоматичні щоденні звірки балансів.
I-03	Платіжні файли (SWIFT)	T (Tampering)	MitM: Підміна реквізитів отримувача в транзиті.	Передача файлів без цифрового підпису.	Обов'язкове підписання кожного файлу.
I-04	Платіжні файли (SWIFT)	S (Spoofing)	Replay Attack: Повторне надсилання легітимної транзакції.	Відсутність унікальних ідентифікаторів (nonce) або міток часу.	Позначка одноразовим числом або часом.
I-05	Довідники курсів валют	T (Tampering)	Rate Manipulation: Зміна курсу для спекуляцій.	Відсутність вхідного контролю значень.	Лімітний контроль (“жорсткі коридори”).
I-06	Довідники курсів валют	T (Tampering)	Tariff Tampering: Приховування комісій для клієнтів.	Пряме посилання на об'єкт у БД.	Підписання довідкових даних.
I-07	Вихідний код ПЗ	T (Tampering)	Supply Chain Attack: Впровадження бекдору при розробці.	Слабкий захист репозиторіїв Git та CI/CD.	Цифровий підпис виконуваних файлів.

Кінець таблиці 3.2

1	2	3	4	5	6
I-08	Вихідний код ПЗ	T (Tampering)	Web Shell Upload: Завантаження скрипта на сервер.	Відсутність моніторингу цілісності; дозвіл на виконання скриптів.	Впровадження FIM (File Integrity Monitoring).
I-09	Налаштування мережі	T (Tampering)	Route Poisoning: Зміна маршрутизації для перехоплення.	Незашифровані протоколи управління (Telnet).	Впровадження суворого контролю доступу.
I-10	Налаштування мережі	T (Tampering)	ACL Modification: Відкриття портів на фаєрволі.	Відсутність системи контролю версій конфігурацій.	CMDB (Configuration Management Database).
I-11	Веб-контент сайту	T (Tampering)	Defacement: Зміна головної сторінки сайту.	Вразливості CMS або плагінів.	WAF (Web Application Firewall).
I-12	Веб-контент сайту	T (Tampering)	Link Injection: Підміна посилань на фішингові.	Слабкі права доступу до папок веб-сервера.	Read-Only File System.

Дані Таблиці 3.2 свідчать про критичність забезпечення незмінності як фінансових записів, так і програмного коду та конфігурацій інфраструктури. Загрози фальсифікаці можуть призвести до прямих фінансових втрат, прихованого шпигунства або репутаційного краху. Основними векторами захисту в цьому контексті визначено криптографічний контроль цілісності та автоматизовані звірки, які дозволяють виявляти несанкціоновані зміни на ранніх етапах.

Таблиця 3.3 – Реєстр загроз порушення доступності

ID	Актив	Категорія STRIDE	Опис загрози	Експлуатована вразливість	Запропонований контрзахід (STRIDE)
1	2	3	4	5	6
A-01	Зовнішні канали зв'язку	D (DoS)	Volumetric DDoS: Забивання каналу сміттєвим трафіком.	Обмежена пропускна здатність каналу.	Маршрутизація трафіку через центр очищення.
A-02	Зовнішні канали зв'язку	D (DoS)	Physical Sabotage: Фізичне перерізання або пошкодження кабелю.	SPOF: Використання лише одного провайдера (один ввід).	Наявність резервного провайдера (Multihoming).
A-03	Публічні веб-сервіси	D (DoS)	HTTP Flood / DDoS: Масована атака на рівні додатку.	Відсутність обмежень на кількість запитів з однієї IP-адреси.	Інтелектуальна фільтрація трафіку (WAF).
A-04	Публічні веб-сервіси	D (DoS)	Slowloris: Атака “повільними” пакетами, що тримають з'єднання.	Сервер налаштований чекати завершення запиту надто довго.	Жорстке обмеження тайм-аутів та Rate Limiting.
A-05	Публічні веб-сервіси	D (DoS)	Complex Query Attack: Надсилання “важких” запитів для перевантаження БД.	Відсутність пагінації або лімітів на вибірку даних у коді.	Балансування навантаження та оптимізація запитів.
A-06	Серверне обладнання	D (DoS)	Hardware Failure: Вихід з ладу апаратного забезпечення (зношення).	Відсутність резервування та використання застарілого обладнання.	Кластеризація та надлишкові масиви дисків (RAID).
A-07	Серверне обладнання	D (DoS)	Power Outage: Повне знеструмлення дата-центру або перегрів.	Залежність від міської мережі без дублювання охолодження.	ДБЖ та генератори (автономність).
A-08	Робочі файли та БД	D (DoS)	Ransomware: Шифрування файлів вірусом-вимагачем.	Відсутність офлайн-бекапів (Air-gapped) та застарілий антивірус.	Зберігання копій на носіях, відключених від мережі.

Кінець таблиці 3.3

1	2	3	4	5	6
A-09	Робочі файли та БД	D (DoS)	Data Corruption: Логічне руйнування структури бази або видалення файлів.	Прямий доступ користувачів до файлових шар; відсутність історії.	Регулярні знімки (Snapshots).
A-10	Банкоматна мережа	D (DoS)	Signal Loss: Зникнення покриття через аварію оператора.	Залежність від одного мобільного оператора.	Роутери з підтримкою двох SIM-карт різних операторів.
A-11	Банкоматна мережа	D (DoS)	Signal Jamming: Зашумлення частот LTE/4G (“глушилки”).	Відсутність резервного каналу зв'язку.	Автоматичне перемикання на резервний канал.
A-12	Банкоматна мережа	D (DoS)	Vandalism / Black Box: Фізичне підключення або пошкодження.	Легкий доступ до сервісних портів; застаріла ОС.	Встановлення датчиків вібрації та нахилу.
A-13	Адміністратор домену	D (DoS)	Account Lockout: Масований підбір пароля для блокування доступу.	Глобальна політика блокування на публічних точках.	Технологія Smart Lockout (аналіз IP).
A-14	Адміністратор домену	D (DoS)	Hostile Takeover: Захоплення контролю через фішинг.	Слабкі методи автентифікації на зовнішніх порталах.	Використання апаратних ключів (FIDO2).

Як видно з переліку в Таблиці 3.3, загрози доступності мають широкий спектр реалізації: від грубого фізичного пошкодження інфраструктури та комунікацій до витончених логічних атак на рівні додатків та облікових записів. Це підкреслює необхідність побудови ешелонованої оборони, що включає як архітектурне резервування (кластеризація, дублювання каналів), так і впровадження спеціалізованих засобів фільтрації трафіку та інтелектуального управління доступом.

Проведений аналіз за класичною методологією STRIDE дозволив

ідентифікувати 40 унікальних сценаріїв загроз для 12 ключових активів фінансової установи. Незважаючи на повноту охоплення, отримані результати демонструють суттєвий недолік класичного підходу: надмірну фрагментацію засобів захисту.

Як видно з таблиць 3.1–3.3, для кожного активу пропонується окремий набір контрзаходів. Наприклад, для захисту від вразливостей автентифікації в активах С-06, С-07, А-13 та А-14 пропонуються різні локальні рішення. Якщо реалізовувати систему захисту, слідуючи цим таблицям буквально, банк буде змушений закуповувати, налаштовувати та адмініструвати десятки розрізнених інструментів безпеки. Це неминуче призведе до дублювання функцій, відповідного зростання фінансових витрат та ускладнення управління інфраструктурою.

Для фінансових установ, що оперують в умовах обмежених бюджетів та високих ризиків, логічнішим є планування комплексного захисту за властивостями інформації, а не з прив’язкою до кожного окремого активу. Такий підхід дозволив би впроваджувати уніфіковані архітектурні рішення, що закривають цілі класи вразливостей для груп активів одночасно. Оскільки класичний STRIDE не надає інструментарію для такої оптимізації, виникає необхідність у його вдосконаленні шляхом інтеграції методів кількісної оцінки та моделювання спільного впливу контрзаходів. Це дозволить трансформувати суб'єктивні експертні висновки в об'єктивні показники ризику, що є необхідною умовою для прийняття фінансово обґрунтованих рішень щодо захисту.

3.2 Вдосконалення методу STRIDE шляхом інтеграції імовірнісних моделей та Байєсівських мереж

Для усунення недоліків класичного підходу STRIDE, пов'язаних із відсутністю пріоритезації загроз та економічною неефективністю, пропонується доповнити якісний аналіз кількісним моделюванням. Запропонована методика

базується на використанні Бета-розподілу для врахування невизначеності та Байєсівських мереж для розрахунку сукупних ризиків.

3.2.1 Імовірнісна оцінка загроз на основі Бета-розподілу

Першим етапом вдосконаленої методики є перетворення якісних оцінок загроз (отриманих в результаті STRIDE-аналізу) у кількісні показники. Для кожної загрози з моделі загроз (атомарна подія/вразливість) розраховуємо число $p \in [1, 0]$ – ймовірність успіху експлуатації в обраному часовому інтервалі. Враховуючи невизначеність щодо дій зловмисників та відсутність повної статистики інцидентів для конкретної установи, доцільно моделювати цю ймовірність p як випадкову величину, що підпорядковується Бета-розподілу:

$$p \sim Beta(\alpha, \beta)$$

Параметри цього розподілу в запропонованій методиці мають наступну інтерпретацію:

– α (альфа) – характеризує серйозність наслідків загрози та наявність вразливості. Чим вище це значення, тим більше факторів сприяють успішній атаці (наявність експлойту, відсутність патчу);

– β (бета) – характеризує складність реалізації загрози. Чим вище це значення, тим менш імовірним є успіх атаки (необхідність фізичного доступу, висока кваліфікація зловмисника, наявність базових бар'єрів).

Такий підхід дозволяє одразу врахувати наявність вразливості у розрахунку: критична вразливість збільшує α, що зміщує розподіл вправо і підвищує математичне очікування ймовірності загрози (E):

$$E(p) = \frac{\alpha}{\alpha+\beta}, \quad (1)$$

Отримане значення математичного очікування $E(p)$ надалі використовується як ймовірність реалізації загрози.

Для стандартизації процесу оцінювання у фінансовій установі пропонується використовувати наступну матрицю відповідності (Таблиця 3.4), яка адаптує теоретичні параметри розподілу до практичних сценаріїв кібербезпеки.

Таблиця 3.4 – Матриця оцінки ймовірностей на основі Бета-розподілу

Рівень загрози (STRIDE)	Характеристика вразливості та атаки	Параметри розподілу (α, β)	Очікувана ймовірність (E)
Критичний	Вразливість легко експлуатується автоматизованими засобами (публічні експлойти). Захист відсутній.	$\alpha = 9, \beta = 1$	$\frac{9}{9+1} = 0.90$
Високий	Відомі вектори атак (наприклад, Brute-force, Phishing), що не вимагають складної підготовки, але потребують часу.	$\alpha = 7, \beta = 3$	$\frac{7}{7+3} = 0.70$
Середній	Атака можлива, але вимагає специфічних умов (наприклад, перебування в локальній мережі або прав користувача).	$\alpha = 2, \beta = 2$	$\frac{2}{2+2} = 0.50$
Низький	Атака складна, вимагає високої кваліфікації, фізичного доступу або дій інсайдера.	$\alpha = 1, \beta = 9$	$\frac{1}{1+9} = 0.10$
Мінімальний	Форс-мажорні обставини або атаки, що вимагають збігу багатьох малоймовірних факторів.	$\alpha = 1, \beta = 19$	$\frac{1}{1+19} = 0.05$

Використання Бета-розподілу дозволяє уникнути надмірного спрощення, властивого дискретним шкалам, і забезпечує гнучкість моделі: при зміні умов (наприклад, появі нового експлойту) параметри α та β можуть бути скориговані, що автоматично оновить оцінку ризику. Отримані значення (E) є вхідними даними для побудови Байєсівських мереж.

3.2.2 Імовірнісна оцінка загроз на основі Бета-розподілу

На основі розробленої матриці оцінювання (таблиця 3.4) та моделей загроз, побудованих у другому розділі, проведемо розрахунок ймовірності успішної реалізації кожної атомарної загрози (p) в часовому інтервалі в один календарний рік. Розрахунок виконується за формулою математичного очікування Бета-розподілу, що вказана у формулі 1.

Таблиця 3.5 – Розрахунок ймовірностей загроз конфіденційності

Актив	Загроза (Threat)	Характеристика (Обґрунтування)	Параметри (α,β)	Ймовірність (p)
БД клієнтів	SQL Injection	Критична: Наявність автоматизованих інструментів, веб-вектор.	$\alpha = 9, \beta = 1$	0.90
БД клієнтів	Insider Threat	Низька: Адміністратор проходить перевірку, страх покарання.	$\alpha = 1, \beta = 9$	0.10
БД клієнтів	Privilege Escalation	Середня: Вимагає наявності специфічного багу в СУБД.	$\alpha = 2, \beta = 2$	0.50
Платіжні картки	Sniffing	Висока: Поширена атака в локальних мережах (HTTP).	$\alpha = 7, \beta = 3$	0.70
Платіжні картки	RAM Scraping	Середня: Вимагає проникнення на сервер для ін'єкції коду.	$\alpha = 2, \beta = 2$	0.50
Акаунти персоналу	Brute-force	Висока: Автоматизований підбір, слабкі паролі.	$\alpha = 7, \beta = 3$	0.70
Акаунти персоналу	Phishing	Висока: Людський фактор, масовість розсилок.	$\alpha = 7, \beta = 3$	0.70
Акаунти персоналу	Mimikatz (Хеші)	Середня: Вимагає локального доступу до ПК жертви.	$\alpha = 2, \beta = 2$	0.50
Електронний документообіг	Industrial Espionage	Низька: Складна цільова атака.	$\alpha = 1, \beta = 9$	0.10
Електронний документообіг	Misdelivery	Середня: Висока ймовірність помилки персоналу.	$\alpha = 2, \beta = 2$	0.50
Ключі шифрування	Key Exfiltration	Середня: Програмне зберігання файлів робить їх вразливими.	$\alpha = 2, \beta = 2$	0.50
Ключі шифрування	Cryptanalysis	Мінімальна: Математично надскладна задача.	$\alpha = 1, \beta = 19$	0.05
Мобільний додаток	Reverse Engineering	Критична: Код доступний публічно, інструменти безкоштовні.	$\alpha = 9, \beta = 1$	0.90
Мобільний додаток	Data Harvesting	Висока: Сканування файлової системи вірусами.	$\alpha = 7, \beta = 3$	0.70

Як видно з Таблиці 3.5, найвищі показники ймовірності (0.90) присвоєно технічним загрозам, що можуть бути повністю автоматизовані (SQL Injection, Reverse Engineering). Це свідчить про те, що периметр безпеки фінансової установи є вразливим до масових атак.

У таблиці 3.6 представлено аналіз ймовірностей несанкціонованої модифікації даних, що є критичним для фінансової звітності.

Таблиця 3.6 – Розрахунок ймовірностей загроз цілісності

Актив	Загроза (Threat)	Характеристика (Обґрунтування)	Параметри (α,β)	Ймовірність (p)
Головна бух. книга	Unauthorized DB Mod	Висока: Прямий доступ до БД, можливість SQL-запитів.	$\alpha = 7, \beta = 3$	0.70
Головна бух. книга	Salami Attack	Низька: Складна логічна атака інсайдера.	$\alpha = 1, \beta = 9$	0.10
Система SWIFT	MitM Attack	Середня: Атака на канали зв'язку вимагає ресурсів.	$\alpha = 2, \beta = 2$	0.50
Система SWIFT	Replay Attack	Низька: Вимагає перехоплення та повтору трафіку.	$\alpha = 1, \beta = 9$	0.10
Курси валют	Rate Manipulation	Середня: Зловживання правами доступу.	$\alpha = 2, \beta = 2$	0.50
Курси валют	Tariff Tampering	Середня: Модифікація довідників через вразливість.	$\alpha = 2, \beta = 2$	0.50
Вихідний код ПЗ	Supply Chain Attack	Низька: Складна атака на етапі розробки.	$\alpha = 1, \beta = 9$	0.10
Вихідний код ПЗ	Web Shell Upload	Висока: Поширена вразливість веб-серверів.	$\alpha = 7, \beta = 3$	0.70
Налаштув. мережі	Route Poisoning	Низька: Вимагає компрометації роутера.	$\alpha = 1, \beta = 9$	0.10
Налаштув. мережі	ACL Modification	Середня: Помилка конфігурації або дії інсайдера.	$\alpha = 2, \beta = 2$	0.50
Веб-сайт	Defacement	Висока: Атака на CMS через відомі експлойти.	$\alpha = 7, \beta = 3$	0.70
Веб-сайт	Link Injection	Висока: Підміна контенту через слабкі права.	$\alpha = 7, \beta = 3$	0.70

Аналіз таблиці 3.6 показує, що хоча складні атаки на ланцюжок постачання (Supply Chain) мають низьку ймовірність (0.10), загрози веб-рівня (Web Shell, Defacement) залишаються у зоні високого ризику (0.70) через поширеність вразливостей у системах управління контентом. Також варто відзначити високу ймовірність (0.70) несанкціонованої модифікації Головної бухгалтерської книги через прямий доступ до бази даних, що значно перевищує ризик реалізації складних логічних атак типу «Salami Attack» (0.10).

У таблиці 3.7 наведено розрахунок для загроз доступності, які безпосередньо впливають на безперервність бізнесу.

Таблиця 3.7 – Розрахунок ймовірностей загроз доступності

ID Активу	Загроза (Threat)	Характеристика (Обґрунтування)	Параметри (α,β)	Ймовірність (p)
1	2	3	4	5
Канали зв'язку	Volumetric DDoS	Критична: Легко замовити атаку, важко відбити без сервісу.	$\alpha = 9, \beta = 1$	0.90
Канали зв'язку	Physical Sabotage	Мінімальна: Рідкісний випадок вандалізму кабелів.	$\alpha = 1, \beta = 19$	0.05
Веб-сервіси	HTTP Flood	Критична: Атака рівня L7, важко відрізнити від клієнтів.	$\alpha = 9, \beta = 1$	0.90
Веб-сервіси	Slowloris	Середня: Специфічна атака на вичерпання з'єднань.	$\alpha = 2, \beta = 2$	0.50
Веб-сервіси	Heavy Query	Середня: Експлуатація логіки бази даних.	$\alpha = 2, \beta = 2$	0.50
Серверне обладнання	Hardware Failure	Середня: Природне зношення обладнання.	$\alpha = 2, \beta = 2$	0.50
Серверне обладнання	Power Outage	Середня: Залежність від зовнішніх мереж.	$\alpha = 2, \beta = 2$	0.50
Робочі файли та БД	Ransomware	Висока: Масові епідемії шифрувальників.	$\alpha = 7, \beta = 3$	0.70
Робочі файли та БД	Data Corruption	Низька: Випадкова помилка адміністратора.	$\alpha = 1, \beta = 9$	0.10
Банкоматна мережа	Signal Jamming	Мінімальна: Потребує спецобладнання (“глушилки”).	$\alpha = 1, \beta = 19$	0.05

Кінець таблиці 3.6

1	2	3	4	5
Банкоматна мережа	Vandalism	Висока: Банкомати знаходяться у публічних місцях.	$\alpha = 7, \beta = 3$	0.70
Банкоматна мережа	Signal Loss	Середня: Технічні проблеми оператора.	$\alpha = 2, \beta = 2$	0.50
Адміністратор домену	Account Lockout	Висока: Легко реалізувати через скрипт перебору.	$\alpha = 7, \beta = 3$	0.70
Адміністратор домену	Hostile Takeover	Середня: Фішинг на привілейованого користувача.	$\alpha = 2, \beta = 2$	0.50

Результати розрахунків у Таблиці 3.7 демонструють критичний рівень загрози для публічних сервісів. Ймовірність DDoS-атак оцінюється у (0.90), що робить інцидент недоступності сервісу майже гарантованим протягом року без застосування спеціалізованих засобів захисту. Отримані значення ймовірностей для всіх категорій загроз будуть використані на наступному етапі для побудови Байєсівських мереж та розрахунку інтегрального ризику.

3.2.3 Байєсівські мережі та агрегація ризиків (модель Noisy-OR)

Після отримання кількісних оцінок ймовірностей для окремих загроз, наступним кроком є визначення сукупного рівня ризику для кожного критичного активу. Оскільки в реальній інфраструктурі фінансової установи на один актив може одночасно впливати множина незалежних факторів (векторів атак), виникає необхідність математичної агрегації цих ймовірностей.

Для вирішення цього завдання пропонується використати апарат Байєсівських мереж довіри (Bayesian Belief Networks – BBN). Це ймовірнісна графічна модель, яка дозволяє представляти набір змінних та їхні умовні залежності у вигляді орієнтованого ациклічного графу (DAG).

У другому розділі роботи було розроблено графічні моделі загроз, які структурно складаються з джерел загроз, вразливостей та активів, поєднаних

причинно-наслідковими зв'язками. У контексті Байєсівського моделювання ця структура трансформується наступним чином:

– батьківські вузли: атомарні події або вразливості, для яких на попередньому етапі було розраховано ймовірність успішної експлуатації $p \in [1, 0]$;

– дочірні вузли: подія компрометації активу (порушення конфіденційності, цілісності або доступності);

– логічні шлюзи: тип зв'язку між батьківськими та дочірніми вузлами.

Аналіз моделей загроз, що є одночасно і нашими деревами атак, показує, що для більшості активів характерною є логіка “АБО” (OR-gate). Це означає, що актив вважається скомпрометованим, якщо успішною виявилася хоча б одна з можливих атак.

У класичних деревах атак використовується детермінована логіка: якщо подія-причина відбулася, то подія-наслідок настає з ймовірністю 1 (100%). Однак у кібербезпеці завжди існує фактор невизначеності: навіть за наявності критичної вразливості та активної загрози атака може не вдатися через випадкові фактори (збій у роботі експлойту, нестабільність каналу зв'язку, дії персоналу тощо).

Щоб врахувати цю невизначеність, у запропонованій методиці застосовується модель Noisy-OR. Вона базується на припущенні, що кожна загроза має певну ймовірність не спрацювати, навіть якщо вона активна. Ця ймовірність називається ймовірністю інгібування і позначається як q_i.

Алгоритм розрахунку сукупного ризику складається з трьох розрахунків ймовірностей: “невдачі” для кожної загрози, безпечного стану активу та підсумкової ймовірності компроментації.

При першому розрахунку за формулою (2), для кожної батьківської події A_i з ймовірністю успіху p_i (отриманою з Бета-розподілу) розраховується ймовірність того, що саме ця подія не призведе до компрометації активу:

$$q_i = 1 - p_i \,, \tag{2}$$

де p_i – математичне очікування ймовірності експлуатації вразливості.

Згідно з теорією ймовірностей, для незалежних подій ймовірність їх одночасного настання дорівнює добутку їхніх ймовірностей. У контексті безпеки нас цікавить сценарій, коли всі атаки зазнали невдачі. Тобто актив залишається у безпеці ($C = 0$) лише тоді, коли жодна із загроз не спрацювала:

$$\mathrm{P(Safe)} = \mathrm{P(C = 0)} = \prod_{i=1}^{n} q_i = \mathrm{q_1 \cdot q_2 \cdot \ldots \cdot q_n}\,, \qquad (3)$$

Ця формула (3) є ключовою відмінністю від простого додавання ризиків, оскільки вона гарантує, що підсумкова ймовірність ніколи не перевищить 1, навіть якщо сума окремих загроз є значно більшою.

Ймовірність того, що актив буде скомпрометовано ($C = 1$), є оберненою до ймовірності його безпечного стану за формулою (4). Це означає, що успішною виявилася хоча б одна з атак (або декілька одночасно):

$$\mathrm{P}(Total\_Risk) = \mathrm{P(C = 1)} = 1 - \mathrm{P}(Safe) = 1 - \prod_{i=1}^{n}(1 - p_i)\,, \qquad (4)$$

Продемонструвати роботу моделі можна на прикладі реального активу “База даних клієнтів” (C-01), для якого у розділі 2 було ідентифіковано три вектори атак із різними рівнями ймовірності:

– Загроза A (SQL Injection): критична загроза. Ймовірність успіху $p_A = 0.90$;

– Загроза B (Privilege Escalation): середня загроза. Ймовірність успіху $p_B = 0.50$;

– Загроза C (Insider Threat): низька загроза. Ймовірність успіху $p_C = 0.10$.

Застосуємо noisy-OR алгоритм для розрахунку сукупного ризику витоку даних. Визначимо ймовірність того, за формулою (2), що кожна конкретна атака зазнає невдачі:

$$q_A = 1.00 - 0.90 = 0.10$$
$$q_B = 1.00 - 0.50 = 0.50$$
$$q_C = 1.00 - 0.10 = 0.90$$

де q_A – ймовірність, що SQL-ін'єкція не спрацює

q_B – ймовірність, що експлойт підвищення прав не спрацює

q_C – ймовірність, що інсайдер не вчинить крадіжку

Актив залишається захищеним ($C = 0$) лише за умови, що всі три загрози одночасно не будуть реалізовані. Для цього використовується дана формула (3):

$$P(Safe) = q_A \cdot q_B \cdot q_C = 0.10 \cdot 0.50 \cdot 0.90 = 0.045$$

Тобто, ймовірність того, що база даних залишиться у безпеці протягом року за поточних умов та з наявними вразливостями, становить лише 4.5%.

Ймовірність витоку даних ($C = 1$) є оберненою до ймовірності безпеки використавши необхідну формулу (4):

$$P(Total\_Risk) = 1 - P(Safe) = 1 - 0.045 = 0.955$$

Як результат, сукупна ймовірність компрометації активу становить 95.5%. Цей показник відображає рівень притаманного ризику – тобто ймовірність успішної атаки протягом розрахункового періоду (1 рік) за умови збереження поточних вразливостей системи без впровадження додаткових засобів захисту.

Даний приклад наочно демонструє ефект синергії загроз: навіть наявність “слабких” векторів (як інсайдер) у поєднанні з критичними вразливостями (SQL) призводить до майже гарантованого інциденту.

3.2.4 Кількісний розрахунок сукупного ризику для властивостей інформації

Використовуючи значення ймовірностей атомарних загроз (P_i), отримані на першому етапі через Бета-розподіл, та математичну модель noisy-OR, проведемо

розрахунок сукупної ймовірності компрометації для кожного активу.

Почнемо з розрахунку сукупних ризиків конфіденційності за формулою (4).

Так як ймовірність компрометації першого активу конфіденційності був обрахований у минулому підпункті, то обрахунок почато із другого активу за формулою.

Дані платіжних карток, вектори атак: Sniffing ($p = 0.70$), RAM Scraping ($p = 0.50$).

$$P_{Total} = 1 - \big((1 - 0.70) \cdot (1 - 0.50)\big) = 1 - (0.30 \cdot 0.50) = 0.850 \quad (85.0\%)$$

Облікові записи персоналу, вектори: Brute-force ($p = 0.70$), Phishing ($p = 0.70$), Mimikatz ($p = 0.50$).

$$P_{Total} = 1 - (0.30 \cdot 0.30 \cdot 0.50) = 1 - 0.045 = 0.955 \quad (95.5\%)$$

Електронний документообіг. Вектори: Misdelivery ($p = 0.50$), Espionage ($p = 0.10$).

$$P_{Total} = 1 - (0.50 \cdot 0.90) = 0.550 \quad (55.0\%)$$

Ключі шифрування. Вектори: Key Exfiltration ($p = 0.50$), Cryptanalysis ($p = 0.05$).

$$P_{Total} = 1 - (0.50 \cdot 0.95) = 0.525 \quad (52.5\%)$$

Мобільний додаток. Вектори: Reverse Engineering ($p = 0.90$), Data Harvesting ($p = 0.70$).

$$P_{Total} = 1 - (0.10 \cdot 0.30) = 0.970 \quad (97.0\%)$$

Визначивши критичний рівень загроз витоку даних, особливо для баз даних та мобільних інтерфейсів, перейдемо до аналізу ризиків несанкціонованої модифікації, тобто порушення цілісності. Для даних активів результати моделювання noisy-OR зведено в Таблицю 3.8.

Таблиця 3.8 – Сукупні ймовірності порушення цілісності активів

Назва активу	Вектори загроз та їх ймовірності (p)	Розрахунок $(1 - \prod qi)$	Ризик (P_{Total})
Головна бух. Книга	1. Unauth. Mod (0.70) 2. Salami Attack (0.10)	$1 - (0.30 \cdot 0.90)$	0.730 (73.0%)
Платіжні файли (SWIFT)	1. MitM Attack (0.50) 2. Replay Attack (0.10)	$1 - (0.50 \cdot 0.90)$	0.550 (55.0%)
Довідники курсів	1. Rate Manipulation (0.50) 2. Tariff Tampering (0.50)	$1 - (0.50 \cdot 0.50)$	0.750 (75.0%)
Вихідний код ПЗ	1. Web Shell (0.70) 2. Supply Chain (0.10)	$1 - (0.30 \cdot 0.90)$	0.730 (73.0%)
Налаштування мережі	1. ACL Modification (0.50) 2. Route Poisoning (0.10)	$1 - (0.50 \cdot 0.90)$	0.550 (55.0%)
Веб-контент сайту	1. Defacement (0.70) 2. Link Injection (0.70)	$1 - (0.30 \cdot 0.30)$	0.910 (91.0%)

Переглянувши таблицю, варто зазначити, що найбільш вразливим активом у категорії цілісності є публічний Веб-сайт (91%). Це пояснюється високою ймовірністю експлуатації вразливостей CMS зовнішніми зловмисниками.

На відміну від порушень конфіденційності, які можуть залишатися непоміченими тривалий час, атаки на доступність мають миттєвий ефект і призводять до прямих фінансових та репутаційних втрат з першої хвилини простою. Результати розрахунку ймовірностей для активів, що забезпечують безперервність бізнесу, тобто властивості доступності, представлено у таблиці 3.9.

Таблиця 3.9 – Сукупні ймовірності порушення доступності активів

Назва активу	Вектори загроз та їх ймовірності (p)	Розрахунок $(1 - \prod qi)$	Ризик (P_{Total})
Зовнішні канали	1. Volumetric DDoS (0.90) 2. Phys. Sabotage (0.05)	$1 - (0.10 \cdot 0.95)$	0.905 (90.5%)
Веб-сервіси	1. HTTP Flood (0.90) 2. Slowloris (0.50) 3. Heavy Query (0.50)	$1 - (0.90 \cdot 0.50 \cdot 0.50)$	0.975 (97.5%)
Сервери (ЦОД)	1. Hardware Fail (0.50) 2. Power Outage (0.50)	$1 - (0.50 \cdot 0.50)$	0.750 (75.0%)
Файли та БД	1. Ransomware (0.70) 2. Data Corruption (0.10)	$1 - (0.30 \cdot 0.90)$	0.730 (73.0%)
Банкомати (АТМ)	1. Vandalism (0.70) 2. Signal Loss (0.50) 3. Jamming (0.05)	$1 - (0.30 \cdot 0.50 \cdot 0.95)$	0.858 (85.8%)

Кількісне моделювання підтверджує, що в рамках класичного підходу STRIDE (без застосування архітектурних контрзаходів) рівень притаманного ризику є критичним. Особливе занепокоєння викликає категорія доступності, де Публічні веб-сервіси мають найвищий показник ризику серед усіх активів установи – 97.5%. Поєднання високоймовірних DDoS-атак з логічними вразливостями протоколів робить інцидент майже неминучим. Також до зони критичного ризику потрапляють зовнішні канали зв'язку (90.5%) та банкоматна мережа (85.8%), що вказує на системну вразливість інфраструктури до фізичних та об'ємних атак. Фактично, такі високі показники свідчать про те, що інциденти простою перестають бути випадковістю і стають прогнозованою операційною реальністю, яка унеможливлює гарантування безперервності послуг (SLA). Отримані значення P_{Total} будуть використані в наступному підрозділі для розрахунку очікуваних фінансових збитків.

3.2.5 Шкала оцінювання вартості активів та розрахунок очікуваних збитків

за властивостями інформації

Згідно з сучасними стандартами управління інформаційною безпекою, процес оцінювання ризиків не може вважатися завершеним лише на етапі визначення ймовірності інциденту. Для прийняття обґрунтованих управлінських рішень необхідно трансформувати ймовірнісні показники у фінансовий еквівалент, що дозволить визначити гранично допустимий бюджет на систему захисту.

Вартість контрзаходів не повинна перевищувати вартість активу або розмір потенційних збитків від його компрометації. Якщо ця умова не виконується, впровадження захисту є економічно недоцільним, і ризик доцільніше прийняти або передати (наприклад, через страхування кіберризиків).

Для порівняння ефективності класичного підходу (STRIDE) з пропонованим комплексним методом, у роботі використовується показник очікуваних річних збитків (Annual Loss Expectancy – ALE). Розрахунок виконується за формулою (5):

$$ALE = P_{Total} \cdot V_{Asset}\ , \tag{5}$$

де P_{Total} – сукупна ймовірність успішної атаки на актив протягом року; V_{Asset} – цінність активу, виражена у грошовому або умовному еквіваленті.

Такий підхід дозволяє перейти від абстрактних категорій “високий/низький ризик” до конкретних числових значень, які можна безпосередньо порівнювати з вартістю ліцензій на ПЗ та апаратного забезпечення.

Оскільки реальна балансова вартість інформаційних активів та інфраструктури банківської установи є комерційною таємницею, а також може динамічно змінюватися, у даній роботі пропонується використовувати метод експертного оцінювання в умовних балах (у.о.).

Такий підхід дозволяє уніфікувати розрахунки та ранжувати активи не за їхньою номінальною вартістю, а за рівнем критичності для бізнесу у разі

інциденту. Вартість активу (V_{Asset}) визначається як сукупність прямих (відновлення даних) та непрямих втрат (штрафи регуляторів, відтік клієнтів, простій сервісів).

Для оцінювання розроблено шкалу, яка поділена на чотири рівні (Таблиця 3.10), де максимальний бал присвоюється активам, втрата яких несе суттєву загрозу для установи.

Хоча якісна класифікація активів (рівні “Критичний”, “Високий” тощо) дозволяє пріоритезувати напрямки захисту, вона не придатна для математичного розрахунку очікуваних збитків. Для реалізації формули (5) необхідно провести квантифікацію (оцифрування) цінності активів.

Таблиця 3.10 – Шкала оцінки вартості інформаційних активів

Рівень критичності	Бали (V)	Критерії віднесення активу до категорії
Критичний (Critical)	1000	Активи, компрометація яких призводить до повної зупинки операційної діяльності, відкликання банківської ліцензії або катастрофічних фінансових втрат. Відновлення вимагає значних ресурсів і часу.
Високий (High)	500	Активи, що забезпечують роботу основних каналів обслуговування клієнтів. Інцидент призводить до значних репутаційних втрат, масових скарг клієнтів та тимчасового простою сервісів.
Середній (Medium)	250	Активи, що підтримують внутрішні бізнес-процеси. Компрометація ускладнює роботу персоналу, призводить до локальних збоїв, але не зупиняє обслуговування зовнішніх клієнтів.
Низький (Low)	100	Технічні активи та допоміжні системи, втрата яких має обмежений локальний вплив, не несе репутаційних ризиків і може бути швидко компенсована адміністративними методами.

Використовуючи визначену вартість активів та розраховані ймовірності компрометації (P_{Total}), проведемо розрахунок сумарного ризику окремо для конфіденційності (таблиця 3.11), цілісності(таблиця 3.12) та доступності (таблиця 3.13). Це дозволить визначити граничну вартість системи захисту (бюджет) для кожної властивості.

Таблиця 3.11 – Ризики порушення конфіденційності

Найменування Активу	ID загроз (з п. 3.1)	Ймовірність (P_{Total})	Вартість (V)	Очікуваний збиток (ALE)
База даних клієнтів	C-01, C-02, C-03	0.955	1000	955.0 у.о.
Дані платіжних карток	C-04, C-05	0.850	1000	850.0 у.о.
Облікові записи персоналу	C-06, C-07, C-08	0.955	250	238.75 у.о.
Мобільний додаток	C-13, C-14	0.970	500	485.0 у.о.
Електронний документообіг	C-09, C-10	0.550	250	137.5 у.о.
Ключі шифрування	C-11, C-12	0.525	250	131.25 у.о.
СУМА (Total Loss)				2797.5 у.о.

Як видно з розрахунків, левову частку потенційних збитків у категорії конфіденційності (близько 65%) формують два критичні активи: база даних клієнтів та дані платіжних карток. Це пояснюється поєднанням їхньої максимальної вартості (1000 у.о.) та надзвичайно високої ймовірності компрометації (85-95%) за відсутності комплексного захисту. Таким чином, основний бюджет має бути спрямований на захист сховищ даних.

Таблиця 3.12 – Ризики порушення цілісності

Найменування Активу	ID загроз (з п. 3.1)	Ймовірність (P_{Total})	Вартість (V)	Очікуваний збиток (ALE)
Головна бух. книга	I-01, I-02	0.730	1000	730.0 у.о.
Система SWIFT	I-03, I-04	0.550	1000	550.0 у.о.
Веб-сайт банку	I-11, I-12	0.910	500	455.0 у.о.
Довідники курсів	I-05, I-06	0.750	250	187.5 у.о.
Вихідний код ПЗ	I-07, I-08	0.730	250	182.5 у.о.
Налаштування мережі	I-09, I-10	0.550	100	55.0 у.о.
СУМА (Total Loss)				2160.0 у.о.

У категорії цілісності значний внесок у ризик (455 у.о.) робить публічний веб-сайт. Незважаючи на меншу номінальну вартість порівняно з головною бухгалтерською книгою, критично висока ймовірність його дефейсу (сторінка вебсайту замінюється на іншу) (91%) робить цей актив одним із пріоритетних для

захисту з точки зору мінімізації репутаційних втрат.

Таблиця 3.13 – Ризики порушення цілісності

Найменування Активу	ID загроз (з п. 3.1)	Ймовірність (P_{Total})	Вартість (V)	Очікуваний збиток (ALE)
Веб-сервіси (API)	A-03, A-04, A-05	0.975	500	487.5 у.о.
Зовнішні канали	A-01, A-02	0.905	500	452.5 у.о.
Банкоматна мережа	A-09, A-10, A-11	0.858	500	429.0 у.о.
Серверне обладнання	A-05, A-06	0.750	250	187.5 у.о.
Робочі файли та БД	A-07, A-08	0.730	250	182.5 у.о.
Адмін домену	A-13, A-14	0.850	250	212.5 у.о.
СУМА (Total Loss)				1951.5 у.о.

Аналіз ризиків доступності виявляє цікаву закономірність: тут відсутні активи з найвищою номінальною вартістю (1000 у.о.), проте сумарний збиток є співмірним з іншими категоріями. Це зумовлено тим, що група активів “Високої” критичності (веб-сервіси, канали, банкомати) має екстремально високі показники ймовірності відмови (90-97%). Фактично, без впровадження систем захисту від DDoS та резервування, ці активи генерують майже гарантовані збитки, що робить інвестиції в забезпечення доступності (зокрема, у хмарні технології) найбільш окупними з точки зору частоти інцидентів.

Узагальнюючи отримані результати, можна сформулювати економічний критерій для достатнього захисту: для забезпечення безпеки певної властивості інформації достатньо застосувати контрзаходи у сумі, яка не перевищує розраховані очікувані збитки (ALE), оскільки загальна загроза (у нашому випадку в умовних одиницях) не перевищить такої суми. Цей принцип дозволяє уникнути поширеної помилки «надлишкового захисту», коли вартість впровадження та підтримки засобів безпеки перевищує цінність самих активів, які вони захищають.

3.3 Перевірка моделі на прикладі типового відділення банку

Для практичного підтвердження розробленої методики, розрахунок параметрів розподілу ймовірностей (Бета-розподіл) та агрегація ризиків через Байєсівські мережі (модель noisy-OR) було реалізовано програмно з використанням мови програмування Python (бібліотеки scipy.stats та pandas). Це дозволило автоматизувати обробку множини векторів атак та уникнути помилок при розрахунку сукупного ризику.

Для порівняльного аналізу економічної ефективності класичного підходу (STRIDE) та запропонованого комплексного методу, розглянемо об'єкт критичної інфраструктури – типове регіональне відділення банку.

Мета перевірки довести, що застосування комплексних архітектурних контрзаходів для захисту властивостей інформації є економічно доцільнішим, ніж впровадження окремих засобів захисту для кожного активу, як це передбачає класична методологія.

3.3.1 Опис сценарію та аналіз захисту конфіденційності

Об'єктом дослідження є банківське відділення, у якому функціонують робочі станції персоналу (менеджери, касир), локальний сервер для кешування даних, комунікаційне обладнання та банкомат у зоні самообслуговування. Для аналізу обрано по 2–3 найбільш критичні активи для кожної властивості інформації. Для кожного активу враховано повний спектр загроз, визначених у таблицях 3.1-3.3 та 3.3, а також розраховано граничний бюджет на основі даних таблиць 3.11-3.12 та на основі формул (1-5), що були описані у попередньому пункті.

Аналіз захисту було почато із конфіденційності.

Серед активів було обрано: облікові записи персоналу, електронний документообіг та база даних клієнтів. Кожен із них має свої загрози:

– перший актив вразливий до Brute-force (С-06), фішингу(С-07) та Mimikatz атак (С-08);

– у електронному документообігу – Industrial Espionage (С-09) та

Misdelivery (C-10);

– у базі даних клієнтів – Insider Threat (C-01), SQL Injection (C-02) та Privilege Escalation (C-03).

Сумарний граничний бюджет відповідно до таблиці 3.11:

$$ALE_{Conf} = 238.75(\text{Акаунти}) + 137.5(\text{Документи}) + 955.5(\text{БД}) = 1331.25 \text{ у. о.}$$

Перша стратегія захисту за класичним STRIDE передбачає нейтралізацію кожної окремої загрози окремим інтрументом:

– захист акаунтів: закупівля апаратних USB-токенів (300 у.о.) та ліцензії на EDR-антивірус проти Mimikatz (150 у.о.);

– захист документів: Впровадження DLP-системи для контролю пошти та USB (400 у.о.);

– захист БД: ПЗ для шифрування дисків та система моніторингу запитів (DAM) проти ін’єкцій (500 у.о.).

Вартість захисту перевищує потенційні збитки (1350 > 1331.25), тому інвестиція є економічно невиправданою.

За іншою стратегією є комплексний захист, що впроваджує єдину архітектуру Zero Trust Workspace (SASE). Це хмарне середовище, яке системно усуває причини загроз:

– ідентифікації (проти C-06, C-07) – вхід без паролів (FIDO2/біометрія) робить фішинг та брутфорс технічно неможливими;

– віртуалізація (проти C-01, C-02, C-03, C-08) – використання VDI (віртуальних робочих столів) означає, що база даних та хеші паролів фізично відсутні на комп'ютерах відділення;

– інформаційний захист (проти C-09, C-10): Вбудовані мітки конфіденційності автоматично шифрують документи, роблячи їх нечитабельними для сторонніх осіб навіть у разі перехоплення.

Вартість підписки (на офіс) становитиме 450 у.о.

Результат:

$$Cost_{Complex}(450) < ALE(1331.25) < Cost_{STRIDE}(1350)$$

Одне архітектурне рішення нейтралізує 8 різнорідних загроз для 3 активів, а також воно економічно вигідніше на 66%.

3.3.2 Аналіз захисту цілісності

Активи цілісності: платіжні файли (SWIFT/СЕП) та веб-інтерфейс порталу.

До першого активу відносяться такі загрози як: MitM Attack (I-03) – підміна реквізитів та Replay Attack (I-04) – повторюване надсилання тієї ж транзакції для дублювання списання.

Загрози веб-порталу: Defacement (I-11) – зміна змісту головної сторінки та Link Injection (I-12) – впровадження посилань на фішингові ресурси.

Їх сумарний граничний бюджет становить:

$$ALE_{Integ} = 550(\text{Платежі}) + 445(\text{Веб}) = 1005 \text{ у. о.}$$

Стратегія за методологією STRIDE:

– захист платежів - купівля ПЗ для накладання ЕЦП та організація ручної звірки транзакцій бухгалтером (500 у.о.);

– захист веб-порталу – встановлення локального WAF (Web Application Firewall) на сервері відділення та сканера цілісності файлів (400 у.о.).

Сукупна вартість: 900 у.о.

За розробленою методологією впроваджуємо концепцію Immutable Infrastructure (“Незмінна інфраструктура”), що у свою чергу містить:

– Blockchain-like Logging (проти I-03, I-04) – транзакції автоматично хешуються та підписуються в захищений ланцюжок блоків. Будь-яка модифікація або повтор транзакції призводить до невалідності хешу всього блоку;

– Read-Only System (проти I-11, I-12) – сервер веб-порталу працює в режимі

“тільки читання”. Будь-яка спроба запису (ін'єкція коду або дефейс) блокується на рівні ядра ОС, а система автоматично перезавантажує “еталонний образ” за секунди.

Вартість провадження даної стратегії 450 у.о.

$$Cost_{Complex}(450) < Cost_{STRIDE}(900) < ALE(1005)$$

В результаті нашого комплексного захисту система переходить від реактивного виявлення змін до архітектурної неможливості їх внесення, а також приносить економічну вигоду у 50%.

3.3.3 Аналіз захисту доступності

Як і в попередніх підпунктах зазначимо основні активи: зовнішні канали зв’язку, банкоматна мережа (ATM), серверне обладнання.

Загрози:

– Volumetric DDoS (A-01) – переповнення каналу сміттєвим трафіком;

– фізичне пошкодження кабелю – фізичний саботаж (A-02) ;

– втрата сигналу (A-10) – збій на стороні мобільного оператора;

– Signal Jamming (A-11) – зашумлення частот;

– вандалізм (A-12) – фізичне пошкодження обладнання;

– Hardware Failure (A-06) – вихід з ладу компонентів;

– знеструмлення відділення (A-07).

Перші дві загрози відносяться до зовнішніх каналів зв’язку, A-10, A-11, A-12 – до ATM, а решта – до серверного обладнання.

Сумарний граничний бюджет:

$$ALE_{Avail} = 452.5 + 429.0 + 187.5 = 1069 \text{ у. о.}$$

Класичний метод STRIDE потребує значних вкладень в додаткове обладнання, а саме:

– мережа: прокладання дублюючого фізичного кабелю (400 у.о.) та контракт Anti-DDoS (300 у.о.);

– АТМ: встановлення окремого резервного 4G-модему та сигналізації (300 у.о.);

– сервер: купівля джерел безперебійного живлення (UPS) та запасних дисків (300 у.о.).

Сукупна вартість становить 1300 у.о.. Ця вартість перевищує збитки, тому Проєкт є збитковим.

За нашою стратегією комплексного захисту використаємо Smart Resilience & Risk Transfer, тобто смарт-стійкість і передачу ризиків. Впровадження екосистеми SD-WAN, IoT та Cloud. Замість намагання зробити фізичні активи “незнищенними”, застосовується інтелектуальне управління та фінансова передача ризику.

Першою частина є SD-WAN (Connectivity) – це один пристрій, що забезпечує зв'язок і для офісу, і для АТМ, автоматично перемикаючись на LTE/4G при аваріях (вирішує А-01, А-02, А-10, А-11).

Наступним є IoT & Insurance (Physical Security) – замість дорогого бронювання банкомату (проти А-12) використовується дешевий датчик вібрації, підключений до SD-WAN, а фінансовий ризик руйнування покривається страховим полісом (передача ризику).

Та останнє, але не менш важливий Cloud (Serverless) – перенесення сервісів у хмару знімає потребу в локальному енергозабезпеченні (проти А-06, А-07).

Вартість підписки та страхового внеску – 600 у.о. і як результат:

$$Cost_{Complex}(600) < ALE(1069) < Cost_{STRIDE}(1300)$$

Комплексний метод перетворив збитковий проект захисту на прибутковий, забезпечивши економію понад 50%.

3.3.4 Узагальнені висновки ефективності

Результати порівняльного моделювання, проведеного для повного спектру загроз, зведено у підсумкову таблицю 3.14. Ці дані наочно демонструють, що запропонований комплексний підхід забезпечує суттєву економічну перевагу над класичною стратегією точкового захисту, дозволяючи знизити сукупні витрати на інформаційну безпеку майже на 60%. Аналіз підтверджує, що на відміну від методу STRIDE, який у ряді випадків (зокрема для забезпечення доступності) вимагає інвестицій, що перевищують потенційні збитки, впровадження уніфікованих платформних рішень гарантує рентабельність системи захисту для всіх властивостей інформації.

Таблиця 3.14 – Підсумкова ефективність впровадження комплексної методики

Властивість інформації	Граничний бюджет (ALE)	Вартість STRIDE (Набір засобів)	Вартість Complex (Єдина платформа)	Економія
Конфіденційність	1331.25 у.о.	1350 у.о. (Збиток)	450 у.о. (SASE)	66%
Цілісність	1005.00 у.о.	900 у.о.	450 у.о. (Immutable)	50%
Доступність	1069.00 у.о.	1300 у.о. (Збиток)	600 у.о. (SD-WAN)	53%
РАЗОМ	3405.25 у.о.	3550 у.о.	1500 у.о.	~58%

3.4 Висновки до розділу

У третьому розділі магістерської роботи вирішено задачу вдосконалення процесу оцінювання системи менеджменту інформаційної безпеки фінансової установи шляхом розробки комплексної методики, що поєднує класичне моделювання загроз із кількісним ризик-аналізом. На початковому етапі, на основі методології STRIDE, було розроблено детальні реєстри загроз для властивостей конфіденційності, цілісності та доступності, що охоплюють 40 унікальних сценаріїв атак на 12 критичних активів. Проведений аналіз показав, що застосування класичного підходу STRIDE у чистому вигляді призводить до надмірної фрагментації засобів захисту, дублювання функцій та, як наслідок, економічної неефективності.

Для усунення цих недоліків запропоновано та реалізовано методику кількісної оцінки ризиків, яка інтегрує параметричний Бета-розподіл для врахування невизначеності атомарних загроз та Байєсівські мережі довіри (модель noisy-OR) для агрегації сукупного ризику. Проведені розрахунки виявили критичний рівень притаманного ризику для активів із зовнішніми інтерфейсами, зокрема для публічних веб-сервісів (97,5%) та баз даних клієнтів (95,5%), що підтверджує необхідність їх пріоритетного захисту. З метою забезпечення економічної доцільності впроваджено розрахунок очікуваних річних збитків (ALE) як об'єктивного фінансового критерію для визначення граничного бюджету на безпеку, що дозволило трансформувати абстрактні технічні ризики у конкретні фінансові показники та встановити чітку межу рентабельності інвестицій.

Практична верифікація методики, реалізована програмно мовою Python на прикладі типового відділення банку, довела значну перевагу запропонованого комплексного підходу над стратегією точкового захисту. Порівняльний аналіз продемонстрував, що перехід від захисту окремих активів до впровадження уніфікованих архітектурних платформ, таких як Zero Trust SASE, Immutable Infrastructure та SD-WAN, дозволяє скоротити сукупні витрати на інформаційну безпеку на 58%. Окрім того, стратегічна оптимізація показала, що для категорії доступності класичні методи фізичного резервування є економічно збитковими, оскільки вартість захисту перевищує ризики, тоді як запропоновані рішення на базі хмарних технологій та передачі ризиків забезпечують високу рентабельність. Таким чином, розроблена модель дозволяє фінансовій установі перейти від реактивного усунення вразливостей до побудови економічно обґрунтованої, стійкої та автоматизованої системи кібербезпеки.

ВИСНОВОК

У даній кваліфікаційній роботі вирішено актуальне науково-практичне завдання підвищення ефективності системи менеджменту інформаційної безпеки (СМІБ) фінансової установи шляхом розробки комплексної моделі, що поєднує класичне моделювання загроз із кількісними методами оцінювання ризиків. У ході дослідження проведено детальний аналіз теоретичних основ та нормативної бази забезпечення ІБ, який показав, що сучасні фінансові установи функціонують в умовах агресивного ландшафту загроз та жорстких вимог регуляторів, таких як Постанова НБУ №95, стандарти ISO 27001 та регламент DORA. Встановлено, що традиційні підходи до захисту часто характеризуються фрагментарністю та реактивністю, що зумовлює необхідність переходу до ризик-орієнтованих стратегій та впровадження концепцій кіберстійкості та Zero Trust.

На основі адаптованої методології STRIDE розроблено детальні моделі загроз для 12 критичних інформаційних активів банку, що дозволило ідентифікувати 40 унікальних векторів атак у розрізі конфіденційності, цілісності та доступності. Серед них критичними визначено SQL-ін'єкції для баз даних, DDoS-атаки на веб-сервіси та високу ймовірність несанкціонованої модифікації (дефейсу) веб-ресурсів. Аналіз продемонстрував, що застосування класичного методу STRIDE у чистому вигляді призводить до формування надмірної кількості розрізнених контрзаходів, що ускладнює управління системою безпеки.

Для усунення цих недоліків удосконалено методику оцінювання ризиків шляхом інтеграції якісного аналізу з математичним апаратом теорії ймовірностей. Використання параметричного Бета-розподілу дозволило врахувати невизначеність реалізації загроз, а застосування Байєсівських мереж довіри (модель noisy-OR) забезпечило коректну агрегацію сукупних ризиків для активів. Проведені розрахунки підтвердили критичний рівень вразливості для публічних веб-сервісів (97,5%) та зовнішніх каналів зв'язку (90,5%). З метою економічного обґрунтування системи захисту розроблено алгоритм розрахунку очікуваних річних збитків (ALE), який виступає об'єктивним критерієм для визначення

граничного бюджету на ІБ та дозволяє встановити чітку межу рентабельності інвестицій.

Експериментальна перевірка ефективності розробленої моделі, реалізована програмно мовою Python на прикладі типового відділення банку, довела перевагу запропонованого комплексного підходу над стратегією точкового захисту. Порівняльний аналіз засвідчив, що перехід від захисту окремих активів до впровадження уніфікованих архітектурних платформ, таких як SASE, Immutable Infrastructure та SD-WAN, дозволяє знизити сукупні витрати на інформаційну безпеку на 58%. Результати моделювання також довели стратегічну доцільність зміни підходів, зокрема для категорії доступності, де класичні методи фізичного резервування часто є економічно збитковими, тоді як запропоновані рішення на базі хмарних технологій та передачі ризиків забезпечують високу рентабельність та відповідність бізнес-цілям фінансової установи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications / ed. by S. Saeed et al. Hershey, PA : IGI Global, 2023. 552 p. DOI: 10.4018/978-1-6684-5284-4.

2. Cybersecurity for financial services: Definitions & Examples [Електронний ресурс] / Darktrace. Режим доступу: https://www.darktrace.com/cyber-ai-glossary/cybersecurity-for-financial-services (дата звернення: 23.09.2025).

3. ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary [Електронний ресурс]. 5th ed. Geneva : ISO/IEC, 2018. 30 p. Режим доступу: https://www.iso.org/standard/73906.html (дата звернення: 23.09.2025).

4. What is information security (InfoSec)? [Електронний ресурс] / Microsoft Security. Режим доступу: https://www.microsoft.com/en-us/security/business/security-101/what-is-information-security-infosec (дата звернення: 23.09.2025).

5. Information Security Management Principles / A. Taylor, D. Alexander, A. Finch, D. Sutton. 3rd ed. London : BCS, The Chartered Institute for IT, 2020. 268 p.

6. ISO/IEC 27001:2022. Інформаційна безпека, кібербезпека та захист приватності. Системи менеджменту інформаційної безпеки. Вимоги [Електронний ресурс]. Geneva : International Organization for Standardization, 2022. Режим доступу: https://www.iso.org/standard/27001.html (дата звернення: 24.09.2025).

7. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA) [Електронний ресурс]. Official Journal of the European Union. 2022. L 333/1. Режим доступу: https://eur-lex.europa.eu/eli/reg/2022/2554/oj (дата звернення: 24.09.2025).

8. ENISA Threat Landscape: Finance Sector. January 2023 to June 2024 [Електронний ресурс] / European Union Agency for Cybersecurity (ENISA). Athens : ENISA, 2024. 33 p. DOI: 10.2824/5410466.

9. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations [Електронний ресурс] / J. Boyens et al. Gaithersburg : National Institute

of Standards and Technology, 2022. (NIST Special Publication ; 800-161r1). DOI: 10.6028/NIST.SP.800-161r1-upd1.

10. Third-Party Cybersecurity Risk Management — Updates for a Changing Risk Environment. Community Banking Connections [Електронний ресурс] / Federal Reserve System. 2023. Issue 2. Режим доступу: https://www. communitybankingconnections.org/Articles/2023/I2-I3/third-party-cybersecurity (дата звернення: 25.09.2025).

11. ISO/IEC JTC 1/SC 27: Information security, cybersecurity and privacy protection [Електронний ресурс] / ISO. Режим доступу: https://www.iso.org/ committee/45306.html (дата звернення: 25.09.2025).

12. Cybersecurity at NIST [Електронний ресурс] / NIST. Режим доступу: https://www.nist.gov/cybersecurity (дата звернення: 25.09.2025).

13. About CISA [Електронний ресурс] / CISA. Режим доступу: https://www.cisa.gov/about (дата звернення: 25.09.2025).

14. Who we are [Електронний ресурс] / ENISA. Режим доступу: https://www.enisa.europa.eu/about-enisa/who-we-are (дата звернення: 26.09.2025).

15. Our role [Електронний ресурс] / European Central Bank. Режим доступу: https://www.bankingsupervision.europa.eu/about/working-at-the-ecb/html/index.en.html (дата звернення: 26.09.2025).

16. About Us: Who We Are [Електронний ресурс] / PCI Security Standards Council. Режим доступу: https://www.pcisecuritystandards.org/about_us/ (дата звернення: 26.09.2025).

17. About Us [Електронний ресурс] / ISACA. Режим доступу: https://www.isaca.org/about-us (дата звернення: 26.09.2025).

18. About The OWASP Foundation [Електронний ресурс] / OWASP. Режим доступу: https://owasp.org/about/ (дата звернення: 27.09.2025).

19. Стратегія Національного банку [Електронний ресурс] / Національний банк України. Режим доступу: https://bank.gov.ua/ua/about/strategy (дата звернення: 24.10.2025).

20. 2024 Data Breach Investigations Report [Електронний ресурс] / Verizon.

New York : Verizon, 2024. 100 p. Режим доступу: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf (дата звернення: 27.09.2025).

21. Social Engineering in Cybersecurity: Threats and Defenses / ed. by H. L. Gururaj, V. Janhavi, V. Ambika. Boca Raton : CRC Press, 2024. 242 p.

22. The NIST Cybersecurity Framework (CSF) 2.0 [Електронний ресурс] / National Institute of Standards and Technology. Gaithersburg : NIST, 2024. (NIST Cybersecurity White Paper ; 29). DOI: 10.6028/NIST.CSWP.29.

23. 2025 Data Breach Investigations Report [Електронний ресурс] / Verizon. New York : Verizon, 2025. 117 p. Режим доступу: https://www.verizon.com/business/resources/Tbf3/reports/2025-dbir-data-breach-investigations-report.pdf (дата звернення: 27.09.2025).

24. Російські кібероперації: аналітика за друге півріччя 2023 року (H2 '2023) [Електронний ресурс] / Державна служба спеціального зв’язку та захисту інформації України. Київ, 2024. Режим доступу: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=64621&embedded=true&a=bi (дата звернення: 27.09.2025).

25. Російські кібероперації: аналітика за перше півріччя 2024 року (H1 '2024) [Електронний ресурс] / Державна служба спеціального зв’язку та захисту інформації України. Київ, 2024. Режим доступу: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=68752&embedded=true&a=bi (дата звернення: 27.09.2025).

26. Російські кібероперації: аналітика за друге півріччя 2024 року (H2 '2024) [Електронний ресурс] / Державна служба спеціального зв’язку та захисту інформації України. Київ, 2025. Режим доступу: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=71278&embedded=true&a=bi (дата звернення: 27.09.2025).

27. Gartner Identifies the Top Cybersecurity Trends for 2024 [Електронний

ресурс] / Gartner. 2024. Feb 22. Режим доступу: https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024 (дата звернення: 29.09.2025).

28. Supply Chain Security Gaps: A 2022 Global Research Report [Електронний ресурс] / ISACA. Schaumburg : ISACA, 2022. Режим доступу: https://www.isaca.org/supply-chain-security (дата звернення: 29.09.2025).

29. Cost of a Data Breach Report 2025 [Електронний ресурс] / IBM. Armonk : IBM, 2025. 31 p. Режим доступу: https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91 (дата звернення: 29.09.2025).

30. What to expect from global financial services regulation in 2024 — Americas and EMEIA [Електронний ресурс] / EY. 2024. Jan 24. Режим доступу: https://www.ey.com/en_ly/media/webcasts/2024/01/what-to-expect-from-global-financial-services-in-2024-americas-and-emeia (дата звернення: 1.10.2025).

31. ECB Banking Supervision: SSM supervisory priorities for 2024-2026 [Електронний ресурс] / European Central Bank. 2023. Dec 11. Режим доступу: https://www.bankingsupervision.europa.eu/framework/priorities/html/ssm.supervisory_priorities202312~a15d5d36ab.en.html (дата звернення: 1.10.2025).

32. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України [Електронний ресурс] : Постанова Правління НБУ від 28.09.2017 р. № 95 (зі змін.). Режим доступу: https://zakon.rada.gov.ua/laws/show/v0095500-17 (дата звернення: 1.10.2025).

33. Payment Card Industry Data Security Standard: Requirements and Testing Procedures. Version 4.0 [Електронний ресурс] / PCI Security Standards Council. 2022. 360 p. Режим доступу: https://www.commerce.uwo.ca/pdf/PCI-DSS-v4_0.pdf (дата звернення: 2.10.2025).

34. What is the Plan-Do-Check-Act (PDCA) Cycle? [Електронний ресурс] / ASQ. Режим доступу: https://asq.org/quality-resources/pdca-cycle (дата звернення: 2.10.2025).

35. ISO 27001:2013 vs ISO 27001:2022 [Електронний ресурс] / Neumetric. 2024. Режим доступу: https://www.neumetric.com/iso-270012013-vs-iso-27001-2022/

(дата звернення: 2.10.2025).

36. Ko P. P. NIST Cybersecurity Framework 2.0: What is new and how to prepare [Електронний ресурс] / P. P. Ko. 2024. May 23. Режим доступу: https://www.ssh.com/
academy/compliance/nist-cybersecurity-framework-2-0 (дата звернення: 2.10.2025).

37. D'Silva A. DORA: raising the bar for operational resilience [Електронний ресурс] / A. D'Silva. FOW. 2023. Aug 14. Режим доступу: https://www.fow.com/ insights/dora-raising-the-bar-for-operational-resilience (дата звернення: 3.10.2025).

38. Operational resilience: international policy priorities [Електронний ресурс] / Bank for International Settlements (BIS). 2023. July 17. Режим доступу: https://www.bis.org/publ/bcbs_nl31.htm (дата звернення: 3.10.2025).

39. Solikhah M., Magdalena L., Hatta M. Implementation of the COBIT 2019 Framework on Information Technology Governance and Risk Management. Eduvest - Journal of Universal Studies. 2024. Vol. 4, No. 7. P. 5922–5944. DOI: 10.59141/ eduvest.v4i7.1188.

40. Top Threats to Cloud Computing: The Pandemic Eleven [Електронний ресурс] / Cloud Security Alliance (CSA). 2022. 35 p. Режим доступу: https:// cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven
(дата звернення: 3.10.2025).

41. ISO/IEC 27017:2015. Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services [Електронний ресурс]. Geneva : ISO/IEC, 2015. Режим доступу: https://www.iso.org/
standard/43757.html (дата звернення: 3.10.2025

42. Chandramouli R. Implementation of DevSecOps for a Microservices-based Application with Service Mesh [Електронний ресурс]. Gaithersburg : NIST, 2022. (NIST Special Publication ; 800-204C). DOI: 10.6028/NIST.SP.800-204C.

43. Myrbakken H., Colomo-Palacios R. DevSecOps in Financial Services: A Systematic Mapping Study. Journal of Software: Evolution and Process. 2024. Vol. 36, iss. 2. DOI: 10.1002/smr.2638

44. Global Cyber Threat Intelligence (CTI) Annual Cyber Threat Trends [Електронний ресурс] / Deloitte. 2024. 25 р. Режим доступу: https://www.deloitte.com /content/dam/assets-zone3/cbc/en/docs/services/risk-advisory/2024/us-deloitte-annual-cyber-threat-trends-2024.pdf (дата звернення: 4.10.2025).

45. Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities [Електронний ресурс] / M. Souppaya et al. Gaithersburg : NIST, 2022. (NIST Special Publication ; 800-218). DOI: 10.6028/NIST.SP.800-218.

46. Cybersecurity considerations 2024: Technology innovations demand strategic pragmatism [Електронний ресурс] / KPMG. 2024. 41 р. Режим доступу: https:// assets.kpmg.com/content/dam/kpmg/xx/pdf/2024/01/cyber-considerations-report.pdf (дата звернення: 4.10.2025).

47. Implementing the NIST Cybersecurity Framework Using COBIT 2019 [Електронний ресурс] / ISACA. Schaumburg : ISACA, 2019. 48 р. Режим доступу: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoYtEAK (дата звернення: 4.10.2025).

48. Whitman M. E., Mattord H. J. Management of Information Security. 6th ed. Boston : Cengage Learning, 2018. 672 p.

49. Zero Trust Maturity Model [Електронний ресурс] : Version 2.0 / Cybersecurity and Infrastructure Security Agency (CISA). Washington : CISA, 2023. 29 р. Режим доступу: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity _model_v2_508.pdf (дата звернення: 5.10.2025).

50. Federal Zero Trust Data Security Guide [Електронний ресурс] / Chief Information Officers Council. Washington : CIO Council, 2024. Режим доступу: https://www.cio.gov/assets/files/Zero-Trust-Data-Security-Guide_Oct24-Final.pdf (дата звернення: 5.10.2025).

51. Zero Trust Architecture [Електронний ресурс] / S. Rose et al. Gaithersburg : NIST, 2020. (NIST Special Publication ; 800-207). DOI: 10.6028/NIST.SP.800-207.

52. Security and Privacy Controls for Information Systems and Organizations [Електронний ресурс] / Joint Task Force. Gaithersburg : NIST, 2020. (NIST Special Publication ; 800-53r5). DOI: 10.6028/NIST.SP.800-53r5.

53. Dimitrov W. et al. Conceptual Model for a Shared Cybersecurity Operations Center for ICS. Data Science and Intelligent Systems (CoMeSySo 2021). Lecture Notes in Networks and Systems. Vol. 231. Cham : Springer, 2021. P. 493–503. DOI: 10.1007/978-3-030-90321-3_40.

54. Outsourcing and third party risk management [Електронний ресурс] : Supervisory Statement SS2/21 / Prudential Regulation Authority. 2021 (Updated 2023). Режим доступу: https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss (дата звернення: 8.10.2025).

55. OWASP Web Security Testing Guide (WSTG) [Електронний ресурс] : Version 4.2 / OWASP. 2020. Режим доступу: https://owasp.org/www-project-web-security-testing-guide/v42/ (дата звернення: 8.10.2025).

56. Ouaissa M., Ouaissa M. Analyzing and Mitigating Attacks in IoT Smart Home Using a Threat Modeling Approach-Based STRIDE. International Journal of Interactive Mobile Technologies. 2025. Vol. 19, no. 2. P. 126–142. DOI: 10.3991/ijim.v19i02.52377.

57. Threat Modeling Methodology: STRIDE [Електронний ресурс] / IriusRisk. 2025. Режим доступу: https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride (дата звернення: 8.10.2025).

58. STRIDE Threat Model: A Complete Guide [Електронний ресурс] / Jit.io. 2025. Режим доступу: https://www.jit.io/resources/app-security/stride-threat-model-a-complete-guide (дата звернення: 13.10.2025).

59. Conducting a STRIDE-based threat analysis [Електронний ресурс] / GOV.UK. 2024. Режим доступу: https://www.gov.uk/government/publications/secure-connected-places-playbook-documents/conducting-a-stride-based-threat-analysis (дата звернення: 13.10.2025).

60. Understanding Cloud Security with the STRIDE Model [Електронний

ресурс] / Tech Reformers. Режим доступу: https://www.techreformers.com/understanding-cloud-security-with-the-stride-model/ (дата звернення: 13.10.2025).

61. STRIDE vs PASTA – A Comparison of Threat Modeling Methodologies [Електронний ресурс] / Aptori. 2023. Режим доступу: https://www.aptori.com/blog /stride-vs-pasta-a-comparison-of-threat-modeling-methodologies (дата звернення: 14.10.2025).

62. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 14.10.2025).

ДОДАТОК А

МЕТОДИКА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІНАНСОВОЇ УСТАНОВИ

У статті розглядається питання аналізу ризиків інформаційної безпеки, зокрема ризиків інформаційної безпеки у фінансових установах. Це питання заслуговує на особливу увагу, оскільки подібні установи переважно працюють із персональними даними клієнтів, заволодіння якими може надати несанкціонований доступ до фінансових ресурсів. Крім того, кожна подібна установа зобов'язана забезпечувати захист збережених клієнтських даних і дотримуватися режиму банківської таємниці.

На сьогоднішній день не існує стандартизованої методики аналізу та оцінювання ризиків інформаційної безпеки для фінансових установ. Тому у даній роботі розроблено конкретну методику аналізу та оцінювання ризиків інформаційної безпеки в подібних установах, створену на основі чинних стандартів і методик побудови системи захисту інформації на підприємств.

Ключові слова: оцінювання ризиків, CRAMM, RiskWatch, якісний аналіз, кількісний аналіз, конфіденційність, цілісність, доступність.

METHODOLOGY FOR ASSESSING INFORMATION SECURITY RISKS IN A FINANCIAL INSTITUTION

The relevance of this study lies in the necessity to devote special attention to information security risks within financial institutions. This necessity arises from the high value of information assets in such organizations. Their significance increases due to the presence of clients' personal data, as unauthorized access to such data could potentially enable illicit access to financial resources.

Therefore, the information used in the operations of financial institutions requires enhanced protection to preserve its key properties: confidentiality, integrity, and availability.

However, to date, there is no standardized methodology for information security risk analysis and assessment that would be mandatory for all financial institutions. The existing and widely applied methodologies are largely generic, designed for organizations across various economic sectors, and fail to take into account the unique characteristics and specific operational contexts of each institution.

Thus, there is a clear need to develop a specific methodology for the analysis and assessment of information security risks in the financial sector, grounded in existing international standards.

This article addresses the issue of information security risk analysis, with particular attention to risks within financial organizations. This topic warrants special consideration, as such institutions primarily operate with clients' personal data, possession of which may potentially provide access to financial resources. Moreover, every financial institution is obliged to ensure the protection of stored client data and to maintain banking confidentiality.

At present, there is no standardized methodology for the analysis and assessment of information security risks specifically designed for financial organizations. Therefore, this study proposes a dedicated methodology for analyzing and assessing information security risks in such institutions, developed on the basis of existing standards and approaches to building information protection systems within enterprises.

Keywords: risk assessment, CRAMM, RiskWatch, qualitative analysis, quantitative analysis, confidentiality, integrity, availability.

Постановка проблеми

Сьогодні аналізу складних ризиків інформаційної безпеки (ІБ) приділяється дедалі більше уваги. Це пояснюється низкою основних причин:

– безперервним зростанням використання інформаційних технологій у діяльності практично будь-якої сучасної організації;

– підвищенням цінності інформації, що обробляється та генерується в процесі роботи компанії;

– інтеграцією різноманітних інформаційних продуктів з метою задоволення всіх потреб підприємства.

Актуальність даної статті полягає у необхідності приділення особливої уваги ризикам ІБ в фінансових установах. Це зумовлено високою вартістю інформаційних ресурсів у подібних компаніях. Їхня цінність зростає через наявність персональних даних клієнтів, адже особа, яка має доступ до таких даних, потенційно може отримати несанкціонований доступ до фінансових ресурсів.

Отже, інформація, що використовується у діяльності фінансових установ , потребує особливого захисту від втрати своїх ключових властивостей, таких як: конфіденційність, цілісність та доступність.

Однак на сьогоднішній день не існує стандартизованої методики аналізу та оцінки ризиків ІБ, яка була б обов'язковою для застосування у всіх фінансових установах. Усі розроблені та активно використовувані методики є досить загальними для організацій, що працюють у різних секторах економіки, і не враховують особливостей та специфіки діяльності кожної організації окремо. Водночас існує методика аналізу та оцінки ризиків ІБ в установах банківської системи, запропонована стандартом ISO 27001 [1], однак вона має лише рекомендаційний характер.

Таким чином, є потреба у розробці конкретної методики аналізу та оцінки ризиків ІБ у фінансовій сфері на основі існуючих стандартів.

Огляд існуючих рішень

Управління ризиками ІБ є ключовим елементом побудови ефективної системи захисту інформації фінансової установи. Серед найпоширеніших методик і програмних засобів аналізу ризиків виділяються Microsoft Risk Management Framework, CRAMM, FRAP та RiskWatch. Кожен із підходів має власні переваги, обмеження та сферу доцільного застосування.

Методика Microsoft базується на чотирьох етапах управління ризиками [2]. Це оцінка, прийняття рішень, реалізація контролю та оцінка ефективності. Використовується разом із програмним засобом Microsoft Security Assessment Tool (MSAT), який допомагає виявляти уразливості в IT-середовищі. Переваги: зрозуміла структура, підтримка якісної та кількісної оцінки, наявність безкоштовного інструменту MSAT. Недоліки: обмежена глибина аналізу технологічних процесів, орієнтація переважно на середні організації.

CRAMM (CCTA Risk Analysis and Management Method) поєднує якісну та кількісну оцінку ризиків [3]. Програмне забезпечення автоматизує ідентифікацію ресурсів, визначення загроз, уразливостей і формування рекомендацій щодо контрзаходів. Переваги: точність, комплексність, можливість формування різних сценаріїв аналізу. Недоліки: значна трудомісткість і потреба у кваліфікованих експертах; висока вартість ліцензії.

FRAP (Facilitated Risk Analysis Process) орієнтований на якісний аналіз ризиків і використовує прості інструменти збору експертних оцінок, такі як опитування, мозковий штурм, статистичний аналіз [3]. Переваги: швидкість проведення, невисока вартість, доступність для невеликих компаній. Недоліки: суб'єктивність результатів, низький рівень деталізації та відсутність автоматизованої підтримки.

RiskWatch – це програмний продукт, що реалізує кількісну оцінку ризиків на основі показників Annual Loss Expectancy (ALE) та Return on Investment (ROI) [4]. Переваги: точна економічна оцінка збитків і ефективності заходів захисту, автоматизація процесу, генерація детальних звітів. Недоліки: висока вартість програмного забезпечення, потреба в значному обсязі вхідних даних, орієнтація на великі корпоративні структури.

Узагальнюючи вищевикладене, можна зазначити, що Microsoft забезпечує стратегічний рівень управління безпекою. Методика FRAP є доцільною для швидкої попередньої оцінки або навчальних цілей. Найбільш збалансованими для застосування у фінансових установах можна вважати CRAMM та RiskWatch.

Порівняльний аналіз методів виявлення аномалій в мережевому трафіку

Методика аналізу та оцінювання ризиків ІБ для фінансової установи повинна забезпечувати якісну та кількісну оцінку ризику, що базується на визначенні ступеня ймовірності реалізації загроз ІБ виявленими та/або потенційними джерелами загроз, а також на оцінюванні тяжкості наслідків реалізації загрози.

В основу якісного методу оцінювання ризику доцільно покласти алгоритм, який використовується в методиці CRAMM, оскільки він передбачає розподіл рівнів ризику за шкалою від 1 до 7. Це дозволяє застосовувати більш гнучкий підхід до визначення категорій ризиків. Як вхідні дані в цьому методі використовуються три основні показники:

- рівень загрози («дуже високий», «високий», «середній», «низький», «дуже низький»);
- рівень уразливості ресурсу («високий», «середній», «низький»);
- критичність ресурсу (розмір очікуваних фінансових втрат) за шкалою від 1 до 7.

Співвідношення критичності ресурсу, рівня загрози та вразливості є наступним (табл. 1).

Таблиця 1

Співвідношення критичності ресурсу, рівня загрози та вразливості

Рівень вразливості / **Рівень загрози**	дуже низький	низький	середній	високий	дуже високий	
низький	1	2	3	4	5	**Критичність ресурсу**
середній	2	3	4	5	6	
високий	3	4	5	6	7	

Кількісний метод доцільно запозичити з алгоритму методики RiskWatch, оскільки для фінансових установ особливо важливим є поділ оцінок за типами загроз із акцентом на вразливостях.

Ризик загрози розраховується для конкретної вразливості:

$$TR = \frac{ER}{100} \times \frac{P(VL)}{100}, \quad (1)$$

де ER – критичність реалізації загрози у %;

$P(VL)$ – імовірність реалізації загрози через дану вразливість у %.

Отримуємо рівень загрози через вразливість в діапазоні від 0 до 1.

Розраховуємо ризик за ресурсом:

$$R = \max(TR \times CR), \quad (2)$$

де CR – критичність ресурсу, яка задається в грошовому еквіваленті або у вигляді рівнів.

Ризики в межах 0-2 вважаються прийнятними. Ризики в межах 2,01-5 потребують мінімізації з подальшою переоцінкою. Ризики вище 5 визнаються критичними та потребують негайного реагування.

Таблиця 2

Відповідність якісного та кількісного аналізу ризиків ІБ

ER		$P(VL)$	
0-20%	дуже низький	0-33%	низький
21-40%	низький	34-66%	середній
41-60%	середній	67-100%	високий
61-80%	високий		
81-100%	дуже високий		

В якості прикладу для перевірки запропонованої методики візьмемо робоче місце працівника фінансової установи. Інформаційним ресурсом є робоча станція, яка містить: персональні дані клієнтів; інформацію про рахунки; інформацію про транзакції; корпоративну пошту.

Далі складемо перелік загроз та уразливостей. Величини критичності реалізації загроз та ймовірності їх реалізації були отримані шляхом експертного оцінювання.

Загроза 1. Халатність співробітника: залишив робоче місце, не вийшовши з системи.

$ER = 100\%$

Вразливість 1. Автоматичний вихід із системи відбувається лише через 15 хвилин бездіяльності користувача.

$P(VL) = 50\%$

Загроза 2. Доступ сторонньою особою до логіна та пароля працівника.

$ER = 100\%$

Вразливість 2.1. Співробітник зберігає логін і пароль під клавіатурою.

$P(VL) = 30\%$

Вразливість 2.2. Відсутність мережевого захисту від несанкціонованого доступу.

$P(VL) = 80\%$

Для **загрози 1** критичність ресурсів становить $CR = 6$. Для **загрози 2**, яка реалізується через **вразливість 2.1** критичність ресурсів $CR = 5$. Для загрози 2, яка реалізується через **вразливість 2.2** критичність ресурсів становить $CR = 7$.

Розрахуємо ризик загрози за кожною вразливістю, для чого використаємо (1).

$$TR_1 = \frac{ER_1}{100} \times \frac{P(VL)_1}{100} = 0.5$$

$$TR_{2.1} = \frac{ER_2}{100} \times \frac{P(VL)_{2.1}}{100} = 0.3$$

$$TR_{2.2} = \frac{ER_2}{100} \times \frac{P(VL)_{2.2}}{100} = 0.8$$

Розраховуємо ризик за ресурсом (2):

$$R = \max((TR_1 \times CR_1), (TR_{2.1} \times CR_{2.1}), (TR_{2.2} \times CR_{2.2})) = \max((3), (1.5), (5.6))$$

З отриманих розрахунків можна зробити висновки, що ризик **загрози 2** через **вразливість 2.1** можна вважати прийнятним, і це логічно, бо імовірність, що хтось зі сторонніх осіб скористається логіном та паролем під клавіатурою, зайнявши місце співробітника, є невисокою. Ризик **загрози 1** потребує мінімізації, наприклад зменшення часу бездіяльності до автоматичного виходу з систему до 5 хвилин. Ризик **загрози 2** через **вразливість 2.2** – викрадення логіну та паролю працівника через зовнішні канали зв'язку є критичним та потребує негайного реагування, зокрема встановлення мережевого захисту.

Остаточним приймається ризик найвищого рівня, тому що він має найбільший вплив.

Висновки

У статті були розглянуті та враховані стандарти у сфері захисту інформації та аналізу ризиків ІБ. У процесі дослідження було вирішено такі завдання:

- систематизовано інформацію про ризики ІБ, визначено важливість їх аналізу та оцінювання для побудови системи захисту інформації на підприємстві;
- розглянуто та враховано наявні рекомендації у сфері аналізу ризиків ІБ фінансових установ;

– проаналізовано та зіставлено існуючі методики оцінювання ризиків ІБ в контексті розробки системи управління ІБ фінансової установи.

Критерії порівняння було обрано на основі інформації про діяльність фінансових установ. За результатами порівняння виокремлено дві методики, які стали основою для створення рекомендацій щодо аналізу та оцінювання ризиків.

Розроблена методика враховує не лише особливості структури та діяльності фінансових установ, але й накопичений досвід у сфері розробки алгоритмів аналізу та оцінювання ризиків інформаційної безпеки.

Її основу становить процес оцінювання ризиків ІБ методом аналізу загроз і вразливостей. Спочатку рівень ризику визначається якісним методом, після чого було розраховується коефіцієнт кількісного показника.

У подальшому розроблена методика може застосовуватися для аналізу та оцінювання ризиків ІБ фінансових установ.

Література

1. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги.

2. Zhai, Xinyu. Risk Management Analysis on Microsoft Corporation// Highlights in Business, Economics and Management. 2023. Vol. 8. P. 373-378. DOI: 10.54097/hbem.v8i.7232.

3. Memon, M.; Hameed, S. Information Security Risk Plans within Enterprise Architecture Framework// International Journal of Advanced Computer Science and Technology. 2019. Т. 8, № 10. С. 82-88. https://doi.org/10.30534/ijacst/2019/018102019

4. Kaur, Ekaspreet; Kaur, Simrata; Singh, Harjot; Kaur, Bisman; Pannu, H. S. Riskwatch: A Model for Improved Preoperative Risk Assessment of Anesthesia in Medical Science Using Machine Learning. 2024. DOI: 10.21203/rs.3.rs-4742242/v1

References

1 ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

2. Zhai, Xinyu. Risk Management Analysis on Microsoft Corporation// Highlights in Business, Economics and Management. 2023. Vol. 8. P. 373-378. DOI: 10.54097/hbem.v8i.7232.

3. Memon, M.; Hameed, S. Information Security Risk Plans within Enterprise Architecture Framework// International Journal of Advanced Computer Science and Technology. 2019. Т. 8, № 10. С. 82-88. https://doi.org/10.30534/ijacst/2019/018102019.

4. Kaur, Ekaspreet; Kaur, Simrata; Singh, Harjot; Kaur, Bisman; Pannu, H. S. Riskwatch: A Model for Improved Preoperative Risk Assessment of Anesthesia in Medical Science Using Machine Learning. 2024. DOI: 10.21203/rs.3.rs-4742242/v1

Завідувачу кафедри кібербезпеки
канд.техн.наук, доц. Кльоцу Ю.П.
здобувача вищої освіти
Колби Сергія Сергійовича
студента ФІТ, 2 курсу, групи КБЗІм-24-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений. Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений. Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

01.12.2025р
дата

підпис

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Колба Сергій Сергійович

Співавтор:

Назва: Модель системи менеджменту інформаційної безпеки фінансової установи

Науковий керівник: ТІтова Віра Юріївна

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:1.3%

Коефіцієнт подібності 2:0.1%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-12-11 09:56:58.0

Після аналізу Звіту подібності констатую наступне:

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

Дата 12.12.25р. експерт

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 0.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 8%**

	Document		Sum coincidence on the DB	
ID: 252306 Title: Модель системи менеджменту інформаційної безпеки фінансової установи Added in a DB: 2025-12-10 Authors: Колба Сергій Сергійович Heads: ТІтова В.Ю. Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	131631	1012	829 (1%)	12 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва: Модель системи менеджменту інформаційної безпеки фінансової установи

Автор: Колба Сергій Сергійович

Освітня програма: освітньо-професійна

Рівень вищої освіти магістр

Спеціальність: 125 – Кібербезпека та захист інформації

Науковий керівник: Тітова Віра Юріївна, канд. техн. наук, доцент

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 98,7%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 100%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високим рівнем унікальності тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Дата: 10.12.2025

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Гарант освітньої програми _____ Віра ТІТОВА

Керівник кваліфікаційної роботи _____ Віра ТІТОВА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «магістр»

Студент Колба Сергій Сергійович
Тема: «Модель системи менеджменту інформаційної безпеки фінансової установи»
Галузь знань 12 «*Інформаційні технології*»
Спеціальність 125 «*Кібербезпека та захист інформації*»
Освітня програма «Кібербезпека та захист інформації»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «магістр»: кількість листів креслень ____; кількість сторінок записки 99;

1. Короткий зміст КР та прийнятих рішень У кваліфікаційній роботі досліджено проблему забезпечення інформаційної безпеки фінансової установи в умовах зростання кіберзагроз. Проаналізовано теоретичні основи ІБ, фактори впливу та нормативні вимоги, виконано ідентифікацію та класифікацію загроз для критичних банківських активів за властивостями конфіденційності, цілісності та доступності. Розроблено вдосконалену модель оцінювання системи менеджменту інформаційної безпеки на основі STRIDE з інтеграцією імовірнісних методів та Байєсівських мереж, а також методику економічного обґрунтування захисту через показник очікуваних річних збитків (ALE). Проведено експериментальну перевірку моделі на прикладі типового відділення банку та підтверджено її практичну та економічну доцільність.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовано актуальність теми, чітко сформульовано мету, завдання, об'єкт і предмет дослідження з урахуванням сучасного стану кіберзагроз та регуляторних вимог. У першому розділі виконано ґрунтовний аналіз теоретичних основ інформаційної безпеки фінансових установ, розглянуто сучасні стандарти та нормативні документи (ISO/IEC 27001:2022, DORA, вимоги НБУ), узагальнено сучасні наукові підходи та передові практики управління ІБ. У другому розділі розроблено та систематизовано моделі загроз конфіденційності, цілісності та доступності для типових банківських активів із використанням сучасних методів моделювання загроз, що відповідають актуальному ландшафту кіберзагроз. У третьому розділі запропоновано вдосконалену модель оцінювання системи менеджменту інформаційної безпеки з використанням сучасних досягнень науки і техніки: імовірнісних методів, Байєсівських мереж, моделі noisy-OR та економічних показників (ALE). Проведено практичну перевірку моделі на прикладі банківського відділення.

4. Позитивні сторони кваліфікаційної роботи Робота вирізняється актуальністю тематики та практичною спрямованістю. Обґрунтовано поєднання класичних методів моделювання загроз із сучасними імовірнісними моделями та економічними показниками. Запропоновані рішення мають прикладну цінність, підтверджену експериментальною перевіркою, і можуть бути використані у практиці фінансових установ.

5. Негативні сторони кваліфікаційної роботи: Можливе глибше висвітлення програмної реалізації запропонованої моделі та її апробації на ширшому колі об'єктів дослідження. Зазначені зауваження не мають принципового характеру та не знижують загальної якості виконаної роботи.

6. Оцінка графічного оформлення та пояснювальної записки роботи. оформлення відповідає вимогам

7. Відгук про роботу в цілому Кваліфікаційна робота виконана на належному науково-методичному рівні та відповідає вимогам, що висуваються до магістерських робіт. Тема є актуальною, має практичне значення для фінансових установ в умовах сучасних кіберзагроз. Автор продемонстрував уміння працювати з науковими джерелами, нормативною базою та сучасними підходами до менеджменту інформаційної безпеки. Матеріал викладено логічно, послідовно й аргументовано, поставлені мета і завдання досягнуті, отримані результати мають практичну цінність. Робота свідчить про достатній рівень теоретичної підготовки, самостійність мислення та вміння застосовувати сучасні методи дослідження.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «добре» (86/B).

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) професор кафедри телекомунікацій, медійних та інтелектуальних технологій, доктор технічних наук, професор Бойко Юлій Миколайович

« 10 » грудня 2025. (підпис)