МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп’ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Зубрович Едуард Ростиславович

Алгоритми захисту інформації в системах віддаленого інтернет-банкінгу / Algorithms for information protection in remote internet banking systems

спеціальність: 123 - Комп’ютерна інженерія
освітньо-професійна програма - Комп’ютерна інженерія
Кваліфікаційна робота

Виконав студент групи КІм-21

Е. Р. Зубрович

_____

Науковий керівник:

к.т.н., доц. Н.Я. Савка

_____

ТЕРНОПІЛЬ – 2025

АНОТАЦІЯ

Зубрович Р.Е. Алгоритми захисту інформації в системах віддаленого інтернет-банкінгу. – Рукопис.

Кваліфікаційна робота на здобуття освітнього ступеня «магістр» за спеціальністю 123 «Комп'ютерна інженерія», освітньо-професійна програма. Західноукраїнський національний університет, Тернопіль, 2025.

Робота написана обсягом 77 сторінок і містить 11 рисунків, 15 таблиць, 1 додаток та 38 джерел за переліком посилань.

Метою роботи є підвищення рівня захисту інформаційних ресурсів у системах віддаленого інтернет-банкінгу на основі комплексних алгоритмів безпеки, що грунтуються на основі методів шифрування, багатофакторної автентифікації та блокчейн-технологій.

Проведено аналіз існуючих підходів до забезпечення інформаційної безпеки у системах віддаленого інтернет-банкінгу, розглянуто основні методи та технології, які застосовуються для захисту даних. Досліджено особливості впровадження багатофакторної автентифікації, методів шифрування даних та використання блокчейн-технологій у системах віддаленого банкінгу. Обґрунтовано необхідність комплексного підходу до забезпечення інформаційної безпеки, що включає інтеграцію різних методів та технологій для захисту даних і транзакцій.

Практичне значення – модель комплексного захисту може бути використана для розробки та впровадження безпечних систем віддаленого інтернет-банкінгу, а також для модернізації існуючих банківських систем з метою підвищення їхньої безпеки та захисту від кібератак.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ІНТЕРНЕТ-БАНКІНГ, БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ, ШИФРУВАННЯ ДАНИХ, БЛОКЧЕЙН-ТЕХНОЛОГІЇ, ЗАХИСТ ТРАНЗАКЦІЙ.

ANNOTATION

Zubrovych R.E. Algorithms for information protection of the remote internet banking systems. – Manuscript.

Qualification work for the Bachelor degree in specialty 123 “Computer Engineering”, educational and professional program. Western Ukrainian National University, Ternopil, 2025.

The work is written in 77 pages and contains 11 figures, 15 tables, 1 appendice and 38 references.

The purpose of the qualification work is to enhance the level of information resource protection in remote internet banking systems based on comprehensive security algorithms that rely on encryption methods, multi-factor authentication, and blockchain technologies.

An analysis of existing approaches to ensuring information security in remote internet banking systems has been conducted, and the main methods and technologies used for data protection have been examined. The peculiarities of implementing multi-factor authentication, data encryption methods, and the use of blockchain technologies in remote banking systems have been studied. The necessity of comprehensive approach to information security, which includes the integration of various methods and technologies for protecting data and transactions has been substantiated.

The practical significance of the work lies in the proposed comprehensive security model, which can be applied in the development and implementation of secure remote internet banking systems, as well as in the modernization of existing banking systems to enhance their security and protection against cyberattacks.

Keywords: INFORMATION SECURITY, INTERNET BANKING, MULTI-FACTOR AUTHENTICATION, DATA ENCRYPTION, BLOCKCHAIN TECHNOLOGIES, TRANSACTION PROTECTION.

ЗМІСТ

ВСТУП

Стрімкий розвиток цифрових фінансових послуг та зростання популярності віддаленого інтернет-банкінгу ставлять питання забезпечення захисту інформації одним із ключових для стабільного функціонування банківської сфери. Кількість користувачів банківських послуг щоразу збільшується, що одночасно підвищує потенційні ризики несанкціонованого доступу, шахрайства та кібератак. Саме тому ефективні алгоритми захисту інформації мають першочергове значення для підтримки довіри клієнтів та фінансової стійкості банківських установ.

Сучасні кібератаки стають дедалі складнішими, зловмисники активно використовують, шкідливе програмне забезпечення, фішинг атаки типу «людина посередині», підбір і перехоплення облікових даних, а також експлуатацію уразливостей мобільних та веб-додатків. За таких умов традиційні методи захисту не забезпечують належного рівня безпеки, що зумовлює потребу у впровадженні багаторівневих алгоритмів шифрування, автентифікації та контролю доступу.

В той же час зростає обсяг персональних та фінансових даних, які передаються каналами зв’язку та зберігаються в хмарних середовищах банківських систем. Порушення конфіденційності або цілісності таких даних може призвести до суттєвих фінансових збитків, правової відповідальності, репутаційних ризиків. Зважаючи на це, алгоритми захисту інформації повинні забезпечувати не лише надійність, але й високу швидкодію, стійкість до підроблення, можливість масштабування та дотримання міжнародних стандартів інформаційної безпеки (ІБ).

Окрему увагу слід приділити вимогам регуляторів та стандартам, які постійно оновлюються, що потребує адаптації та модернізації існуючих механізмів захисту. У контексті розвитку технологій штучного інтелекту, біометрії та поведінкової аналітики з’являються нові підходи до захисту

користувацьких даних і транзакцій, зокрема технології блокчейн, як інструмент децентралізованого зберігання інформації на принципах прозорості, цілісності та надійності.

Таким чином, забезпечення ІБ в системах віддаленого інтернет-банкінгу є важливою завдачею, яка потребує детального вивчення сучасних алгоритмів шифрування, автентифікації, виявлення загроз та запобігання кібератакам. Ефективність таких алгоритмів визначає рівень захисту банківських систем, стабільність роботи фінансового сектору та безпека користувачів. Із вищезазначеного, можна сформувати мету дослідження, а саме – розробка моделі системи захисту інформації віддаленого інтернет-банкінгу (ВІБ), яка враховує особливості сучасних загроз й ґрунтується на алгоритмах шифрування та технології блокчейн.

Завдання дослідження:

– проаналізувати сучасний стан та методи забезпечення ІБ в системах ВІБ;

– визначити основні види інтернет-шахрайства та уразливості в системах ВІБ;

– дослідити сучасні технології та механізми захисту інформації в системах ВІБ;

– сформувати вимоги до сучасних систем захисту інтернет-банкінгу;

– розробити модель безпечної системи ВІБ, яка включає сучасні методи захисту інформації;

– розробити модель бази даних інтернет-банкінгу;

– удосконалити систему захисту інтернет-банкінгу на основі блокчейн та хмарних технологій.

Кваліфікаційну роботу виконано на основі основних положень та вимог, що зазначено у працях [25, 26].

Об’єкт дослідження – системи віддаленого інтернет-банкінгу.

Предмет дослідження: алгоритми, засоби та технології забезпечення ІБ в системах ВІБ.

Методи дослідження: аналіз літературних джерел з питань інформаційної безпеки в інтернет-банкінгу, емпіричні методи для збору та аналізу даних про сучасні загрози та інциденти в інтернет-банкінгу, моделювання для розробки та оцінки ефективності запропонованих рішень, порівняльний аналіз для існуючих технологій та механізмів захисту інформації, проєктування баз даних для розробки моделей реляційної бази дпаних.

Наукова новизна:

– розроблено комплексну модель системи забезпечення ІБ в системах ВІБ, що враховує сучасні загрози та ризики;

– розроблено архітектуру бази даних на основі реляційного підходу та блокчейн-технологій для підвищення рівня безпеки інтернет-банкінгу.

Практичне значення. Удосконалена системи захисту віддаленого інтернет-банкінгу.

Публікація та апробація результатів. Результати, отримані при виконанні кваліфікаційної роботи опубліковано на XVIII Міжнародній науково-практичній конференції «Інформаційні технології і автоматизація – 2025» та III Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Інтелектуальні комп’ютерні системи та мережі» [9, 16]. Копії публікацій розміщено у додатку А.

У першому розділі проведено дослідження основних принципів безпеки систем ВІБ. Проаналізовано найпоширеніші загрози та атаки на системи такого типу й охарактеризовано методи протидії цим загрозам. Обґрунтовано необхідність розробки комплексної моделі системи захисту інтернет-банкінгу, що ґрунтується на сучасних технологіях.

У другому розділі проаналізовано засоби технічного захисту даних інтернет-банкінгу, методи автентифікації користувачів й перспективність застосування двофакторної автентифікації. Досліджено сучасні технології забезпечення конфіденційності даних, зокрема, блокчейн та хмарні технології. Розроблено алгоритм захисту інформації в системах ВІБ на основі комплексної моделі бази даних.

У третьому розділі спроєктовано архітектуру безпечної системи ВІБ на основі сформульованих вимог до сучасних систем безпеки у банківській діяльності. розроблено модель бази даних інтернет-банкінгу на сонові реляційного підходу та технології блокчейн.

У додатках містяться копії публікацій основних результатів дослідження.

РОЗДІЛ 1 АНАЛІЗ ПРОЦЕСУ ЗАБЕЗПЕЧЕННЯ ІБ В СИСТЕМАХ ВІДДАЛЕНОГО ІНТЕРНЕТ-БАНКІНГУ

1.1 Аналіз методів забезпечення ІБ в системах ВІБ

У сучасних умовах питання забезпечення інформаційної безпеки у системах віддаленого інтернет-банкінгу стає дедалі важливішим. Зростання масштабів використання таких сервісів супроводжується підвищенням кількості кіберзлочинів та інцидентів безпеки. ВІБ забезпечує користувачам швидкий доступ до послуг банку у будь-який час і з будь-якого місця, однак одночасно створює нові ризики та виклики, що потребують ефективних механізмів захисту конфіденційності, цілісності та доступності інформації. Архітектуру інтернет-банкінгу представлено на рисунку 1.1.

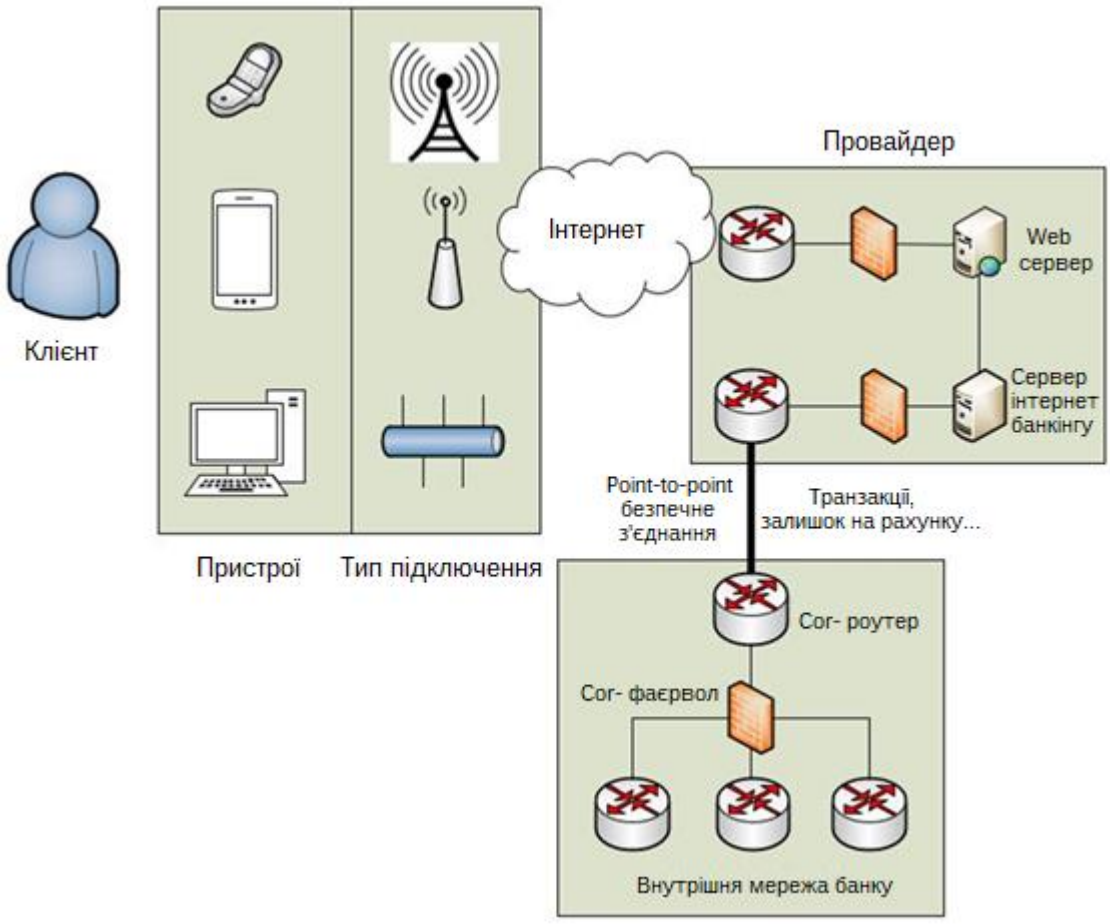

Рисунок 1.1 – Архітектура ВІБ [8]

Сучасні дослідження у сфері ІБ в системах ВІБ охоплюють широкий спектр питань, починаючи від загальних принципів побудови безпечних систем до конкретних методів захисту даних. У таблиці 1.1 зібрано основні методи забезпечення ІБ в системах ВІБ.

Таблиця 1.1 – Методи забезпечення ІБ в системах ВІБ

Метод	Опис	Переваги	Недоліки
Багатофакторна автентифікація	Використання кількох незалежних методів підтвердження особи	Підвищений рівень безпеки, ускладнюючи отримання несанкціонованого доступу	Потребує додаткових ресурсів для впровадження та підтримки
Шифрування даних	Перетворення інформації у криптографічно захищений формат, доступний лише авторизованим користувачам	Гарантує конфіденційність даних, навіть якщо вони були перехоплені	Управління ключами; можливе зниження продуктивності через операції шифрування та дешифрування
Цифровий підпис	Криптографічний механізм для автентичності та цілісності електронних документів	Забезпечує захист від підроблення та порушення цілісності даних	Підтримка інфраструктури відкритих ключів, ризик компрометації приватних ключів

Продовження таблиці 1.1

Системи ідентифікації та запобігання вторгненням (IDS/IPS)	Аналіз трафіку мережі та поведінки користувачів з метою виявлення і блокування несанкціонованих дій	Уможливлює виявлення та запобігання загрозам в реальному часі, підвищуючи рівень мережевої безпеки	Можливі хибні спрацьовування; необхідність регулярного оновлення баз сигнатур і правил
Блокчейн	Децентралізований механізм зберігання транзакцій із використанням криптографічних технологій для підвищення прозорості та захисту	Висока стійкість до маніпуляцій, можливість застосування смартконтрактів	Значне навантаження на обчислювальні ресурси; потенційні проблеми зі масштабованістю
Хмарні технології	Використання хмарних сервісів для підвищення гнучкості, масштабованості та оптимізації витрат на інфраструктуру	Висока доступність і надійність, резервне копіювання та швидке відновлення даних	Існують ризики безпеки даних у хмарі; потрібен постійний контроль та моніторинг роботи провайдерів хмарних послуг

Одним із ключових напрямів досліджень є розвиток методів автентифікації користувачів. Враховуючи швидкий розвиток технологій та зростання кількості кіберзагроз, традиційні методи автентифікації, такі як

паролі, стають менш ефективними. Сучасні тенденції свідчать про необхідність впровадження мультифакторної автентифікації, яка поєднує кілька різних методів для підвищення рівня захисту. Як приклад, комбінація паролів з біометричними даними (відбитками пальців, розпізнаванням обличчя або голосу) дозволяє суттєво знизити ризик несанкціонованого доступу. Крім того, актуальними є дослідження у сфері використання смарт-карт та USB-токенів, які забезпечують додатковий рівень захисту [8, 13, 14].

Ще одним важливим напрямом є захист комунікаційних каналів між користувачем і банківською системою. Зважаючи на те, що більшість транзакцій здійснюється через інтернет, забезпечення конфіденційності та цілісності даних під час їх передачі є критично важливим. Тому особлива увага приділяється дослідженню та вдосконаленню протоколів шифрування, таких як SSL/TLS. Окрім цього, актуальними є питання забезпечення безпеки мобільних додатків для інтернет-банкінгу, що включає використання захищених каналів передачі даних та шифрування на рівні додатку.

У контексті забезпечення ІБ в системах ВІБ важливу роль відіграє контроль доступу до ресурсів банківської системи а основі різних засобів, що продемонстровано на рисунку 1.2.

Рисунок 1.2 – Засоби віддаленого доступу клієнта до банку

Різні моделі доступу, такі як рольова модель (RBAC) та атрибутивна модель (ABAC), потребують детального аналізу та вдосконалення з метою

забезпечення мінімізації прав доступу та зниження ризиків несанкціонованого доступу. Важливим аспектом є також впровадження контекстно-орієнтованих моделей доступу, які враховують додаткові фактори, такі як місце перебування користувача й тип використовуваного пристрою.

Окремий блок досліджень присвячений питанням виявлення та запобігання інтернет-шахрайству. Актуальними є розробка та вдосконалення алгоритмів для виявлення підозрілих транзакцій, зокрема на основі машинного навчання й моніторингу поведінки користувачів. Методи на основі правил, які дозволяють визначати аномальні дії, також потребують подальшого вдосконалення для підвищення точності та швидкості виявлення шахрайства. Крім того, актуальними є дослідження у сфері фішингу та соціальної інженерії, що дозволяє розробляти ефективні механізми захисту від таких атак [8].

Управління ризиками є ще одним важливим напрямом досліджень у сфері забезпечення ІБ. Оцінка ризиків та розробка стратегій управління ризиками дозволяють банківським установам ефективно захищати свої інформаційні ресурси та знижувати вплив можливих загроз. Важливим є також дослідження питань відповідності нормативним вимогам та стандартам, таким як PCI DSS та GDPR, які встановлюють високі вимоги до захисту даних. Впровадження цих стандартів у практичну діяльність банків дозволяє забезпечити відповідність найкращим практикам у сфері ІБ.

Застосування сучасних технологій для підвищення рівня ІБ є одним із пріоритетних напрямів сучасних досліджень. Зокрема, блокчейн-технології, які забезпечують високу прозорість і захищеність фінансових операцій, відкривають значні можливості для розвитку інтернет-банкінгу. Створення нових підходів до впровадження блокчейну сприяє ефективному захисту даних від несанкціонованих змін і підвищує довіру користувачів до банківських сервісів.

Крім того, важливу роль відіграють дослідження у галузі хмарних технологій, що дозволяють оптимізувати витрати на інфраструктуру та підвищувати гнучкість банківських систем. Водночас використання хмари

потребує додаткових заходів безпеки для захисту інформації в хмарному середовищі. У таблиці 1.2 подано порівняльний аналіз методів забезпечення інформаційної безпеки.

Не менш значущими є й організаційні аспекти безпеки. Розробка ефективних моделей управління ІБ, формування дієвих політик безпеки та регулярне навчання персоналу є невід'ємними складовими успішного функціонування захищених банківських систем.

Таблиця 1.2 – Порівняльний аналіз методів забезпечення ІБ

Метод	Технології	Рівень безпеки	Зручність для користувачів	Вартість впровадження	Приклади використання
Багатофакторна автентифікація	Паролі, OTP, біометрія	Високий	Середня	Висока	Google Authenticator, YubiKey
Шифрування даних	AES, RSA, TLS	Високий	Висока	Середня	HTTPS, PGP
Цифровий підпис	RSA, DSA, ECDSA	Високий	Середня	Висока	Електронні контракти, документообіг
Системи IDS/IPS	Snort, Suricata, Zeek	Високий	Висока	Висока	Захист мереж корпоративного рівня

Продовження таблиці 1.2

Блокчейн	Ethereum, Hyperledger Fabric	Високий	Середня	Висока	Криптовалюти, розумні контракти
Хмарні технології	AWS, Microsoft Azure, Google Cloud	Високий	Висока	Середня	Хмарні обчислення, зберігання даних

Таким чином, вибір конкретних методів та технологій для детального аналізу та впровадження обґрунтовується необхідністю підвищення рівня захисту банківських систем від сучасних загроз. Це включає розвиток методів автентифікації користувачів, захист комунікаційних каналів, контроль доступу, виявлення та запобігання інтернет-шахрайству, управління ризиками, використання інноваційних технологій та організаційні аспекти забезпечення безпеки.

1.2 Основні концепції та принципи ВІБ

Основні положення віддаленого інтернет-банкінгу ґрунтуються на принципах надання послуг через Інтернет-мережу із метою забезпечення максимальної зручності та доступності для користувачів. Системи ВІБ дають змогу клієнтам здійснювати різноманітні фінансові операції, переглядати стан рахунків, оплачувати послуги та керувати власними коштами незалежно від місця перебування та часу.

Однією з визначальних рис ВІБ є його доступність. Користувачі можуть отримувати банківські послуги з будь-якого пристрою, що має доступ до

Інтернету – чи то комп’ютер, смартфон, планшет або інший мобільний гаджет. Можливість працювати з банківськими сервісами цілодобово забезпечує гнучкість та комфорт, що дозволяє отримати задоволеного клієнта. Крім того, інтернет-банкінг робить фінансові послуги доступними в регіонах, де відсутні фізичні відділення банків.

Зручність використання є однією з ключових характеристик систем віддаленого інтернет-банкінгу. Інтерфейси таких сервісів створюються з урахуванням потреб користувачів, що забезпечує інтуїтивно зрозумілий доступ до банківських операцій. Завдяки простій навігації та швидкому виконанню транзакцій клієнти можуть без зайвих зусиль управляти власними фінансами. Чимало банків також пропонують мобільні додатки, які ще більше розширюють можливості користувачів, дозволяючи виконувати фінансові операції безпосередньо зі смартфонів чи планшетів.

Безпека є одним із фундаментальних принципів ВІБ. Для банківських установ критично важливо гарантувати конфіденційність, цілісність і доступність даних на основі застосування сучасних методів шифрування, автентифікації та контролю доступу. Протоколи SSL/TLS забезпечують захищений канал обміну інформацією між клієнтом і банком, а багатофакторна автентифікація значно зменшує ймовірність несанкціонованого доступу [35]. Додатково банки впроваджують системи виявлення та запобігання шахрайським операціям, що дозволяє оперативно ідентифікувати підозрілі дії та уникати фінансових втрат.

Масштабованість – ще одна важлива складова ВІБ. Системи інтернет-банкінгу мають здатність обробляти зростаючі обсяги транзакцій без погіршення якості обслуговування. Це вимагає використання надійних і гнучких архітектур, здатних адаптуватися до зміни навантаження. Все більшого значення набувають хмарні рішення, які забезпечують ефективне масштабування, високу доступність сервісів та оптимізацію витрат на інфраструктуру.

Окрім основних концепцій, сучасний ВІБ включає інтеграцію з іншими фінансовими сервісами та платформами. Це дає можливість клієнтам отримувати доступ до цілісної екосистеми фінансових продуктів – від інвестицій та страхування до управління активами. Така інтеграція підвищує зручність користування і дозволяє здійснювати комплексне управління фінансами [28].

Успішне впровадження систем віддаленого інтернет-банкінгу потребує не лише технічних рішень, а й організаційних трансформацій. Банкам необхідно формувати ефективні стратегії управління змінами, проводити навчання персоналу, удосконалювати внутрішні процеси й запроваджувати нові політики безпеки. Це сприяє як підвищенню якості обслуговування, так і надійному захисту даних клієнтів.

Особливу роль також відіграє дотримання нормативних та стандартних вимог. Банківські установи мають відповідати міжнародним і національним нормам, що регулюють захист даних, проведення фінансових операцій та безпеку інформаційних систем. До таких вимог належать стандарти на кшталт PCI DSS, GDPR та інші, що встановлюють високі критерії безпечної роботи з інформацією [3, 11].

Отже, гарантування високого рівня захисту даних, інтеграція з іншими фінансовими платформами та відповідність нормативним вимогам є ключовими умовами ефективного функціонування систем ВІБ. Реалізація цих принципів дозволяє банкам забезпечувати клієнтів сучасними, надійними та безпечними послугами. Принципи захищеного електронного документообігу в інтернет-банкінгу базуються на забезпеченні конфіденційності, цілісності та автентичності даних, що досягається завдяки використанню криптографічних методів, електронного підпису та інших технологій [13].

1.3 Види інтернет-шахрайства при використанні інтернет-банкінгу

Фішинг та фальшиве страхування є одними з найбільш розповсюджених видів інтернет-шахрайства, які націлені на користувачів систем ВІБ. Ці види шахрайства використовують різні методи обману для отримання конфіденційної інформації, зокрема, логіни, паролі, номери платіжних карт та інші персональні дані.

Зловмисники розробляють фіктивні веб-сайти, які подібні візуально на офіційні банківські сайти або інтернет-сторінки інших фінансових установ, і надсилають користувачам електронні листи або повідомлення з проханням перейти на ці сайти та ввести свої персональні дані. Такі листи часто містять повідомлення про необхідність підтвердження облікового запису, оновлення інформації або повідомлення про підозрілі транзакції. Користувачі, які не підозрюють обману, переходять на фальшиві сайти і вводять свої дані, які потім потрапляють до зловмисників [36].

Фальшиве страхування є іншим поширеним видом інтернет-шахрайства, який націлений на користувачів інтернет-банкінгу. Зловмисники пропонують вигідні умови страхування або інші фінансові послуги, які насправді не існують. Користувачам надсилаються пропозиції придбати страхові поліси або інвестувати в нібито прибуткові проєкти з великими знижками або іншими привабливими умовами. Після того як користувачі сплачують кошти за такі послуги, зловмисники зникають, залишаючи жертв без грошей та без страхового покриття.

Наслідки фішингу та фальшивого страхування можуть бути дуже серйозними для користувачів. Окрім фінансових втрат, жертви таких атак можуть зіткнутися з компрометацією особистої інформації, що може спричинити подальші шахрайські дії, таких як крадіжка особистості або використання їхніх даних для здійснення інших незаконних операцій. Відновлення після таких атак може вимагати значних зусиль та часу,

включаючи зміну паролів, блокування кредитних карт, звернення до банків та правоохоронних органів.

Захист від фішингових атак та шахрайських схем зі «страхуванням» потребує підвищеної обережності та уважності з боку користувачів. Серед основних рекомендацій – ретельна перевірка отриманих електронних листів і повідомлень, уникнення переходу за підозрілими посиланнями, а також введення особистої інформації виключно на офіційних вебресурсах банків та інших фінансових організацій. Водночас банки мають активно інформувати клієнтів про потенційні ризики та надавати поради щодо безпечного використання сервісів інтернет-банкінгу.

Крім того, банки можуть використовувати технічні засоби для захисту своїх клієнтів від фішингу та фальшивого страхування. Це включає впровадження мультифакторної автентифікації, використання протоколів шифрування для захисту даних під час їх передачі, а також впровадження систем виявлення та запобігання шахрайству, які дозволяють виявляти підозрілі транзакції та активність у реальному часі. Важливим є також регулярне оновлення та вдосконалення систем безпеки для протидії новим загрозам та атакам.

Фіктивні P2P-перекази та шкідливе програмне забезпечення є ще одними з поширених методів інтернет-шахрайства, які використовуються зловмисниками для крадіжки інформації та фінансових ресурсів користувачів систем ВІБ [37]. Фіктивні P2P-перекази (peer-to-peer перекази) є однією з форм шахрайства, де зловмисники розробляють фальшиві платформи для переказу грошей між користувачами. Ці платформи, зазвичай, виглядають як легітимні сервіси, які обіцяють швидкі та зручні перекази грошей. Зловмисники заманюють користувачів на такі платформи, обіцяючи низькі комісії або інші привабливі умови. Після того як користувачі вводять свої особисті дані та здійснюють перекази, зловмисники отримують доступ до їхніх фінансових ресурсів і зникають, залишаючи жертв без грошей.

Зловмисники також розробляють різні види шкідливих програм, які можуть проникати у комп'ютери та мобільні пристрої користувачів через електронні листи, завантажені файли або заражені веб-сайти. Після того як шкідливе ПЗ потрапляє на пристрій, воно може виконувати різні шкідливі дії, зокрема, крадіжку паролів, зняття коштів з банківських рахунків, перехоплення даних кредитних карт та іншу незаконну діяльність.

Схеми швидкого збагачення та небезпечні інвестиції також є поширеними методами шахрайства в інтернеті. Зловмисники пропонують користувачам можливість швидко заробити великі суми грошей через інвестиції у фіктивні проекти або фінансові схеми. Такі пропозиції часто виглядають дуже привабливо, обіцяючи високі прибутки з мінімальними ризиками. Однак після того як користувачі інвестують свої кошти, зловмисники зникають, залишаючи жертв без грошей та без жодних можливостей для повернення інвестицій.

Захист від подібних видів шахрайства потребує від користувачів підвищеної уважності та дотримання базових принципів безпеки, зокрема, відмова від переходу за підозрілими посиланнями, завантаження файлів лише з перевірених джерел, регулярне оновлення програмного забезпечення та використання сучасних антивірусних рішень.

1.4 Аналіз розповсюджених ризиків та уразливостей інтернет-банкінгу

Технічні ризики та уразливості є ключовими елементами забезпечення інформаційної безпеки в системах онлайн-банкінгу, оскільки вони пов’язані з інфраструктурою, що включає сервери, клієнтські додатки, мережеві протоколи та інші компоненти системи. Аналіз таких ризиків дозволяє своєчасно виявляти потенційні загрози та впроваджувати заходи щодо їх усунення.

Серед основних технічних ризиків виділяють атаки на сервери. Наприклад, DDoS-атаки (розподілені атаки на відмову в обслуговуванні) призводять до перевантаження серверів та їх недоступності для користувачів, що може спричинити фінансові втрати та шкоду репутації банку. Для захисту застосовуються апаратні та програмні рішення, системи виявлення та запобігання DDoS, а також фільтрація трафіку. Ще однією поширеною загрозою є SQL-ін’єкції, які уможливлюють виконання несанкціонованих запитів до баз даних, що зумовлює крадіжку даних або їх модифікацію. Для запобігання таким атакам використовують валідацію даних, підготовлені та параметризовані запити, а також регулярне оновлення серверного програмного забезпечення.

Клієнтські додатки також піддаються ризику атак, зокрема через уразливості до міжсайтового скриптингу (XSS), який уможливлює вставку шкідливого коду у веб-сторінки та викрадення облікових данихї користувачів. Захист включає екранування та валідацію даних, політики безпеки вмісту (CSP) і регулярне оновлення клієнтського ПЗ.

Мережеві протоколи можуть стати мішенню MITM-атак (атаки "людина посередині"), які дозволяють перехоплювати та змінювати передані дані, що загрожує крадіжкою конфіденційної інформації та підробкою фінансових транзакцій. Захист забезпечується шифруванням даних (SSL/TLS) та автентифікацією серверів. Крім того, атаки на DNS можуть призвести до направлення користувачів на фейкові ресурси, що потребує застосування DNSSEC та політик захисту DNS-серверів.

Вразливості програмного забезпечення та систем управління доступом також відносяться до технічних ризиків. Проблеми в операційних системах, серверному ПЗ чи клієнтських додатках можуть бути використані для несанкціонованого доступу. Захист включає оновлення програмного забезпечення, застосування патчів, IDS/IPS та регулярні аудити безпеки. Мобільні додатки піддаються атакам шкідливого ПЗ, що може викрадати дані або виконувати несанкціоновані транзакції, тому для їх захисту застосовують

шифрування, автентифікацію користувачів та політики безпеки мобільних пристроїв.

Організаційні ризики пов’язані з управлінням персоналом, політиками безпеки та процедурами контролю доступу. Недостатня кваліфікація співробітників, слабкі політики безпеки та недосконалі процедури управління доступом збільшують ймовірність витоку даних та фінансових втрат. Для зменшення ризиків важливо впроваджувати регулярне навчання персоналу, принцип найменших привілеїв і чіткі процедури надання та відкликання доступу.

Недостатнє управління інцидентами безпеки призводить до затримок у реагуванні та відновленні систем, тому необхідно розробляти процедурні моделі управління інцидентами, включно з виявленням, класифікацією, повідомленням відповідальних, аналізом причин та відновленням систем. Управління змінами та ланцюгами постачань також є критичними: впровадження нових технологій чи робота з постачальниками без належного контролю створюють додаткові уразливості. Для мінімізації цих ризиків застосовують стандартизовані процедури управління змінами та аудити безпеки постачальників.

Не менш важливим є управління фізичною безпекою об’єктів інфраструктури, включно з серверними приміщеннями та робочими місцями, для запобігання несанкціонованому доступу або крадіжкам. Крім того, загрозою є соціальна інженерія, що використовує психологічні методи впливу на персонал для отримання конфіденційної інформації. Їй протидіють навчанням співробітників та впровадженням політик безпеки. Наслідки зазначених технічних та організаційних ризиків включають як фінансові, так і репутаційні втрати, як зазначено у таблиці 1.3.

Таблиця 1.3 – Аналіз ризиків ІБ у віддалених банківських системах

Ризик	Можливі наслідки	Рекомендовані заходи
Фінансові втрати	Втрата коштів банку та клієнтів, зниження довіри клієнтів	Впровадження надійних методів автентифікації, моніторинг транзакцій, системи IDS/IPS
Репутаційні втрати	Втрата клієнтів, зниження прибутків, негативна реклама	Прозора політика безпеки, швидке реагування на інциденти, покращення комунікації з клієнтами
Юридичні наслідки	Штрафи, судові позови, регуляторні санкції	Дотримання стандартів та регуляторних вимог, впровадження політик захисту даних
Витік конфіденційної інформації	Зниження довіри, фінансові та репутаційні втрати	Шифрування даних, контроль доступу, регулярні аудити безпеки
Компрометація системи	Перебої у роботі сервісів, фінансові втрати, зниження продуктивності	Використання захисних механізмів, регулярне тестування системи, планування відновлення після збоїв

Зважаючи на вищепроведений аналіз у наступному розділі перейдемо до аналізу вимог до сучасних систем захисту інтернет-банкінгу та розробки комплексної моделі безпеки на основі сучасних методів шифрування хмарних та блокчейн-технологій.

1.5 Постановка задачі кваліфікаційної роботи

Сучасні системи ІБ – це ключовий елемент фінансової інфраструктури, яка забезпечує користувачам оперативний, зручний та безперервний доступ до банківських послуг. Однак, поряд із зручністю, такі системи стикаються з численними загрозами ІБ. Щодня зростає кількість випадків несанкціонованого доступу до облікових записів, фішингових атак, шахрайських транзакцій, а також експлуатації технічних та організаційних уразливостей систем.

Більшість систем захисту ВІБ спирається на традиційні методи безпеки, зокрема, фаєрволи, антивірусні програми та статичні правила контролю доступу, що обмежує їхню здатність до швидкого реагування на нові види загроз, включаючи складні багаторівневі атаки та «нульові» вразливості. Впроваджена багатофакторна автентифікація часто базується на SMS або електронних повідомленнях, що робить її вразливою до фішингу, перехоплення повідомлень.

Технічні недоліки веб- та мобільних додатків, такі як вразливості API або помилки у сесійному управлінні, надають можливості для SQL-ін’єкцій, XSS-атак та несанкціонованого доступу до даних користувачів. Крім того, системи моніторингу, зазвичай, використовують статичні правила або прості алгоритми, що обмежує їхню здатність виявляти складні схеми шахрайства та аномальні патерни поведінки.

Управління правами доступу в банках часто є громіздким і не завжди оновлюється оперативно, що підвищує ризик внутрішніх загроз. Традиційні системи також погано інтегруються з сучасними технологіями, такими як блокчейн, хмарні платформи та IoT-пристрої, що зменшує можливості масштабування та прозорості операцій. Крім того, велика частина захисних механізмів покладається на користувача, його обізнаність і дотримання правил безпеки, що робить систему вразливою через людський фактор, зокрема через слабкі паролі, неуважність або вплив соціальної інженерії.

Це підкреслює необхідність розробки комплексної моделі безпеки, яка дозволить забезпечити конфіденційність, цілісність та доступність фінансових даних користувачів. Зважаючи на це, метою роботи є розробка моделі безпечної системи ВІБ, що інтегрує сучасні алгоритми захисту інформації, ефективні механізми контролю доступу, моніторингу аномалій та управління ризиками.

Досягнення зазначеної мети вимагає вирішення таких задач:

– розробити модель безпечної системи ВІБ, яка включає сучасні методи захисту інформації;

– розробити модель бази даних інтернет-банкінгу;

– удосконалити систему інтернет-банкінгу на основі блокчейн та хмарних технологій;

У наступних розділах розглянемо детально зазначені задачі із детальним аналізом та висновками.

1.6 Висновки до розділу

Розглянуто основні аспекти забезпечення ІБ в системах інтернет-банкінгу. Визначено, що основні концепції ВІБ включають забезпечення доступності, зручності використання, безпеки та масштабованості систем. Аналіз принципів захищеного електронного документообігу показав, що шифрування даних, використання електронного підпису, цифрових сертифікатів, хеш-функцій та протоколів безпечної передачі даних є важливими для забезпечення конфіденційності, цілісності та автентичності даних у системах інтернет-банкінгу. Аналіз основних видів інтернет-шахрайства дозволив виявити основні загрози для користувачів інтернет-банкінгу та розробити рекомендації щодо їхнього захисту.

РОЗДІЛ 2 АЛГОРИТМИ ЗАБЕЗПЕЧЕННЯ ІБ В СИСТЕМАХ ВІДДАЛЕНОГО ІНТЕРНЕТ-БАНКІНГУ

2.1 Алгоритми технічного захисту ресурсів інтернет-банкінгу

Алгоритми технічного захисту ресурсів інтернет-банкінгу ґрунтуються на комплексному підході, який охоплює шифрування даних, автентифікацію користувачів, захист мережевої інфраструктури та моніторинг активності в режимі реального часу. Передача інформації між клієнтом і сервером здійснюється через захищені канали зв'язку із застосуванням протоколів TLS, які забезпечують конфіденційність і цілісність даних. Важливу роль відіграє автентифікація користувача, що реалізується за допомогою двофакторних або багатофакторних механізмів, де окрім пароля використовуються одноразові коди, біометричні параметри чи апаратні токени.

У таблиці 2.1 проаналізовано найбільш поширені засоби захисту конфіденційної інформації із зазначенням її переваг та недоліків при застосуванні у банківських системах.

Таблиця 2.1 – Технічні методи захисту ресурсів інтернет-банкінгу

Метод	Опис	Переваги	Недоліки
USB-токени	Апаратні пристрої, що зберігають цифрові сертифікати та ключі шифрування, підключаються через USB-порт	Високий рівень захисту, фізичний контроль доступу, неможливість копіювання	Можливість втрати або крадіжки токена, потреба в додаткових пристроях

Продовження таблиці 2.1

Смарт-карти	Пластикові картки з вбудованим мікропроцесором для зберігання криптографічних ключів	Високий рівень захисту, зручність використання, підтримка біометрії	Потреба в спеціальних рідерах, можливість втрати або крадіжки картки
Мобільні токени	Програмні додатки на смартфонах, що генерують одноразові паролі або зберігають ключі шифрування	Зручність використання, висока мобільність, можливість інтеграції з мобільними додатками	Залежність від мобільного пристрою, ризик компрометації через шкідливе ПЗ
Апаратні модулі безпеки	Пристрої для зберігання та управління криптографічними ключами	Високий рівень захисту, швидка обробка криптографічних операцій	Висока вартість, складність впровадження
Біометричні пристрої	Пристрої для сканування відбитків пальців, розпізнавання обличчя або райдужної оболонки ока	Унікальність біометричних даних, висока точність автентифікації	Високі вимоги до захисту біометричних

USB-токени є одним із найбільш ефективних засобів технічного захисту ресурсів інтернет-банкінгу, оскільки вони забезпечують високий рівень безпеки даних. Це апаратні пристрої, призначені для зберігання цифрових сертифікатів і

ключів шифрування, які відіграють важливу роль у запобіганні несанкціонованому доступу до інформації [8, 33].

Основна перевага USB-токенів полягає в їх фізичній формі, що додає додатковий рівень захисту. Для отримання доступу до даних необхідно фізично підключити токен до комп'ютера та ввести PIN-код. Такий двофакторний метод автентифікації значно ускладнює завдання зловмисникам. Навіть у випадку компрометації комп'ютера користувача, без наявності токена та знання PIN-коду доступ до даних залишиться неможливим.

USB-токени використовуються для зберігання цифрових сертифікатів, що підтверджують особу користувача під час автентифікації в системах інтернет-банкінгу та захищають від несанкціонованого доступу. Підключення токена до комп'ютера активує запит цифрового сертифіката, і лише після успішної автентифікації користувач отримує доступ до банківських послуг. Крім того, токени застосовуються для зберігання ключів шифрування, що необхідні для безпечної передачі даних через мережу Інтернет. Шифрування перетворює інформацію у форму, недоступну для сторонніх осіб.

USB-токени також уможливлюють зменшення ризиків фішингових атак та інших способів перехоплення персональних даних. Навіть у разі випадкового розкриття користувачем своїх даних шахраям, фізична відсутність токена робить неможливим несанкціонований доступ до банківського рахунку.Додатково, USB-токени забезпечують високий рівень захисту від атак на основі кейлогерів та інших шкідливих програм, що можуть записувати натискання клавіш на клавіатурі. Оскільки для доступу до USB-токена використовується PIN-код, який вводиться безпосередньо на пристрої, зловмисники не можуть легко отримати цей код через кейлогери.

Смарт-карти також відносяться до методів технічного захисту в інтернет-банкінгу. Вони оснащені вбудованим мікропроцесором, який дозволяє зберігати та обробляти криптографічні ключі, необхідні для автентифікації користувачів і підписання транзакцій. Завдяки своїм технічним

характеристикам та функціональним можливостям, смарт-карти убезпечують від несанкціонованого доступу та різноманітних кіберзагроз [29].

Основною перевагою смарт-карт є їх здатність забезпечувати двофакторну автентифікацію користувачів. Для доступу до даних, збережених на смарт-карті, користувач повинен не лише мати фізичну карту, але й знати PIN-код. Цей підхід суттєво підвищує рівень безпеки, оскільки зловмисник не зможе отримати доступ до інформації лише з одним із факторів автентифікації. Навіть якщо карта буде вкрадена, без знання PIN-коду зловмисник не зможе скористатися нею для доступу до банківського рахунку чи здійснення транзакцій.

Вбудований мікропроцесор смарт-карт забезпечує надійне зберігання криптографічних ключів, які використовуються для шифрування даних та підписання транзакцій. Ці ключі генеруються всередині карти і ніколи не залишають її, що значно ускладнює задачу для зловмисників, які намагаються викрасти ці ключі. Процесор смарт-карти також виконує криптографічні операції, такі як шифрування та дешифрування даних, розробка та перевірка цифрових підписів.

Крім автентифікації, смарт-карти також використовуються для підписання фінансових транзакцій. Під час здійснення транзакції користувач вводить свій PIN-код, після чого смарт-карта генерує цифровий підпис, який додається до транзакції. Цифровий підпис підтверджує автентичність транзакції та забезпечує її цілісність, запобігаючи можливості підробки або зміни даних. Завдяки цьому, фінансові установи можуть бути впевнені в тому, що транзакції були здійснені саме авторизованими користувачами і не були змінені під час передачі.

У наступному підрозділі детально розглянемо сет орди атентифікації користувачів, які використовуються у сучасних ІС.

2.2 Методи автентифікації користувачів

Мультифакторна автентифікація (multi-factor authentication, MFA) є одним із найпоширеніших засобів забезпечення безпеки в системах інтернет-банкінгу. MFA передбачає використання кількох факторів для підтвердження особи користувача, зокрема, пароль, смарт-карта, відбиток пальця або одноразовий пароль (OTP). Цей підхід суттєво ускладнює задачу для зловмисників, які намагаються отримати доступ до банківських систем, оскільки для успішної автентифікації потрібно мати доступ до кількох незалежних факторів [33].

Основний принцип мультифакторної автентифікації полягає у використанні трьох категорій факторів: те, що користувач знає (пароль або PIN-код), те, що користувач має (смарт-карта, USB-токен або мобільний пристрій), і те, ким користувач є (біометричні дані – відбиток пальця, розпізнавання обличчя або голосу). Комбінація цих факторів зумовлює багатошаровий захист.

Перший фактор, який часто використовується в MFA, – це те, що користувач знає. Це можуть бути паролі, PIN-коди або відповіді на секретні питання. Паролі є найпоширенішим методом автентифікації, але самі по собі вони не забезпечують достатнього рівня захисту, оскільки можуть бути вкрадені або вгадані зловмисниками. Використання довгих і складних паролів, які регулярно змінюються, може підвищити рівень безпеки, але навіть тоді вони залишаються вразливими до атак соціальної інженерії та фішингу.

Другий фактор – те, що користувач має. Це можуть бути смарт-карти, USB-токени, мобільні пристрої або одноразові паролі (OTP), які генеруються спеціальними додатками або надсилаються через SMS. Смарт-карти та USB-токени зберігають криптографічні ключі та сертифікати, які використовуються для автентифікації користувачів, як зазначено у попередньому підрозділі. Мобільні пристрої можуть використовуватися для отримання OTP через додатки або SMS, що додає додатковий рівень захисту. Навіть якщо

зловмисник отримає пароль користувача, він не зможе отримати доступ до системи без фізичного пристрою або одноразового пароля.

Третій фактор – те, ким користувач є. Біометричні дані, які використовуються для підтвердження користувача. Біометричні методи є одними з найнадійніших, оскільки вони базуються на унікальних фізичних характеристиках користувача, які важко підробити або вкрасти. Впровадження біометричних методів у інтернет-банківські системи забезпечує високий рівень захисту, але вимагає спеціалізованого обладнання для їх зчитування [36, 38].

Комбінація зазначених факторів є основою багатошарового підходу до автентифікації користувачів у системі. Наприклад, для успішної автентифікації користувач може бути зобов'язаний ввести свій пароль, вставити смарт-карту в зчитувач і підтвердити свою особу за допомогою відбитка пальця. Навіть якщо зловмисник отримає один із факторів, він не зможе отримати доступ до системи без інших факторів.

MFA також забезпечує захист від таких поширених атак, як фішинг, кейлогери та атаки на основі соціальної інженерії, а також слугує додатковим рівенем захисту від шкідливого програмного забезпечення. Впровадження MFA в інтернет-банківські системи також сприяє відповідності міжнародним стандартам ІБ.

Деякі банки впроваджують системи, що вимагають від клієнтів підтвердження великих транзакцій за допомогою біометричної автентифікації, зокрема, відбитка пальця чи розпізнавання обличчя. Це гарантує високий рівень захисту і дозволяє уникнути шахрайських транзакцій. Такий метод захисту є найефективніший і найнадійніший, оскільки індивідуальні дані практично не можливо підробити.

Відбитки пальців є одним із найпоширеніших методів біометричної автентифікації. Така ідентифікація широко використовуються в смартфонах, банкоматах та інших пристроях для забезпечення безпеки. Процес автентифікації за допомогою відбитків пальців передбачає зчитування візерунка пальця за допомогою спеціального сканера та порівняння його з

попередньо збереженими даними. Цей метод є швидким і зручним для користувачів, а також забезпечує високий рівень захисту від несанкціонованого доступу.

Розпізнавання обличчя вимагає використання камер для зчитування унікальних характеристик обличчя користувача – форми обличчя, розташування очей, носа та рота. Після зчитування ці дані порівнюються з попередньо збереженими зображеннями для підтвердження особи. Цей метод є зручним для користувачів, оскільки не потребує введення паролів чи інших даних [38].

Розпізнавання райдужної оболонки ока вважається одним із найбільш точних способів біометричної автентифікації. Унікальна структура райдужки формує складний візерунок, який не повторюється в різних людей і зберігається незмінним упродовж усього життя. Для ідентифікації застосовують спеціалізовані камери, що фіксують деталі цього візерунка та зіставляють отримане зображення з еталонними даними, записаними в базі.

Розпізнавання голосу також вважають перспективним методом біометричної автентифікації, який використовує унікальні акустичні характеристики голосу користувача для підтвердження його особи. Такий метод забезпечує високий рівень захисту і є зручним для користувачів, оскільки не потребує додаткового обладнання чи введення даних, однак голос змінюється при хворобах, емоційних станах.

Біометрична автентифікація сьогодні є одним із надійних методів захисту даних, проте її впровадження пов’язане з певними викликами. Необхідно гарантувати безпеку біометричних даних, оскільки їхнє викрадення або несанкціонований доступ можуть мати серйозні наслідки для користувачів. Слід враховувати конфіденційність та етичні аспекти обробки біометричної інформації. Впровадження біометричних систем вимагає суттєвих фінансових витрат на обладнання та програмне забезпечення.

У наступному підрозділі розкриємо питання технологій забезпечення конфіденційності даних, зокрема, методи шифрування.

2.3 Технології забезпечення конфіденційності у системах ВІБ

У результаті проведеного дослідження можна виділити найбільш поширені методи забезпечення конфіденційності даних, які мають свої переваги та недоліки, зокрема, симетричне та асиметричне шифрування, електронні цифрові підписи, транспортний рівень безпеки.

Симетричне шифрування є одним із найпоширеніших і ефективних методів забезпечення конфіденційності даних у системах інтернет-банкінгу, що передбачає використання одного й того самого ключа для шифрування та дешифрування, що спрощує реалізацію і забезпечує високу швидкість обробки інформації.

Принцип роботи симетричного шифрування ґрунтується на тому, що відправник та одержувач використовують один секретний ключ, який має залишатися відомим лише обом сторонам. Відправник шифрує відкритий текст за допомогою ключа, перетворюючи його у зашифрований текст, який передається одержувачу. Одержувач, використовуючи такий же ж ключ та дешифрує повідомлення назад у відкритий текст. Такий підхід гарантує конфіденційність даних, оскільки стороння особа без знання секретного ключа не зможе розшифрувати інформацію [20].

Одним із найпоширеніших алгоритмів симетричного шифрування є AES (Advanced Encryption Standard), який використовує блочне шифрування. Дані розбиваються на блоки фіксованої довжини (зазвичай 128 біт), і кожен блок шифрується окремо. AES підтримує ключі різної довжини, зокрема, 128, 192 та 256 біт, що дозволяє вибирати рівень безпеки відповідно до вимог конкретної системи.

Оскільки AES базується на блоках даних фіксованого розміру, під час шифрування використовується масив 4×4 байт, що називається станом даних (State). Для ключа довжиною 128 біт алгоритм виконує 10 раундів шифрування, у межах яких State проходить через послідовність базових перетворень:

Крок 1. SubBytes. На цьому етапі кожен байт State замінюється іншим згідно з наперед визначеною таблицею замін (S-box). Це нелінійне перетворення, яке підсилює криптостійкість алгоритму.

Крок 2. ShiftRows. Рядки State циклічно зсуваються вліво – перший рядок залишається незмінним, тоді як другий, третій і четвертий зміщуються відповідно на 1, 2 та 3 байти. Це забезпечує перемішування даних між стовпцями.

Крок 3. MixColumns. Кожен стовпець розглядається як поліном над кінцевим полем $GF(2^8)$ і перемножується з фіксованим поліномом:

$$a(x)=03x^3+01x^2+01x+02,$$

(множення здійснюється за модулем x^4-1). Операція забезпечує ефективну дифузію даних у межах стовпця.

4. AddRoundKey. До State додається відповідний раундовий ключ шляхом виконання побітової XOR-операції. Тобто до кожного стовпця State застосовується слово розширеного ключа $W_{4r}+i$, де r – номер раунду (починаючи з 1), а $i=0…3$.

5. Розшифрування здійснюється шляхом виконання обернених до наведених операцій у протилежній послідовності. Спочатку до шифртексту застосовується AddRoundKey (оскільки XOR є самозворотною операцією), причому використовуються останні чотири слова розширеного ключа W_{4R}, $W_{4R}+1$, $W_{4R}+2$, $W_{4R}+3$ де R – номер останнього раунду. Далі виконуються зворотні варіанти операцій SubBytes, ShiftRows та MixColumns, що дозволяє відновити початковий відкритий текст.

Високий рівень безпеки AES обумовлений складністю алгоритму та величезною кількістю можливих ключів. Для того щоб зловмисник підібрав ключ методом перебору (брутфорс), знадобляться астрономічні обчислювальні ресурси та час, що робить AES надзвичайно стійким до атак.

Оскільки для шифрування та дешифрування використовується один і той самий ключ, обробка даних відбувається швидко й ефективно. Це робить симетричне шифрування оптимальним для захисту фінансових транзакцій, де важлива оперативність обробки інформації.

Проте симетричне шифрування має обмеження. Основним викликом є безпечна передача секретного ключа між відправником і одержувачем. У разі перехоплення ключа зловмисником, він зможе дешифрувати всі дані. Для вирішення цієї проблеми часто застосовують гібридні криптосистеми, де симетричне шифрування поєднується з асиметричним. У таких системах асиметричне шифрування забезпечує безпечну передачу ключа, а самі дані шифруються симетричним алгоритмом.

Ще однією проблемою є управління ключами, особливо в великих системах із численними користувачами. Потрібно забезпечити їх надійне зберігання, розподіл і оновлення, що є складною задачею. Для цього використовують спеціалізовані системи управління ключами (KMS), які автоматизують зберігання, розподіл і ротацію ключів.

На відміну від симетричного, асиметричне шифрування ґрунтується на парі ключів – відкритому та закритому. Відкритий ключ використовують для шифрування, а закритий – для дешифрування даних. Навіть якщо відкритий ключ стає відомим стороннім особам, вони не зможуть розшифрувати інформацію без закритого ключа.

Кожен користувач асиметричної системи має два ключі – відкритий, який можна вільно розповсюджувати і використовувати для шифрування, та закритий, який зберігають в таємниці і застосовують для дешифрування даних, які зашифровані відкритим ключем. Це забезпечує односторонній процес шифрування, при якому доступ до інформації має лише власник закритого ключа.

Одним із найвідоміших алгоритмів асиметричного шифрування є RSA (Rivest-Shamir-Adleman), який ґрунтується на складності факторизації великих чисел [15]. Під час генерації ключів створюються два великі прості числа p та q,

на основі яких обчислюються відкритий і закритий ключі. Відкритий ключ складається з модуля n і експоненти e, де $1<e<\varphi(n)$ та використовується для шифрування даних. Ключ закритий також містить модуль n і іншу експоненту d, яка задовольняє умову $d \cdot e \equiv 1 (\mathrm{mod} \varphi(n))$ і застосовується для дешифрування. Таким чином формується пара ключів: відкритий (e, n) та закритий (d, n).

Асиметричне шифрування має кілька важливих переваг. Воно забезпечує конфіденційність даних, оскільки лише власник закритого ключа може їх розшифрувати, гарантувавши доступ до інформації лише авторизованим особам. Метод забезпечує цілісність даних, адже будь-які зміни зашифрованого повідомлення робить процес дешифрування некоректним, що дозволяє виявити спроби підробки чи модифікації інформації.

Крім того, RSA широко використовується для створення та перевірки цифрових підписів, що підтверджує автентичність і цілісність повідомлень або документів [8, 36]. Цифровий підпис розробляють на основі закритого ключа відправника, який генерує унікальний підпис для даних. Одержувач може перевірити підпис на основі відкритого ключа відправника й підтвердити, що інформація не була змінена і справді надійшла від конкретного користувача. Це особливо важливо в інтернет-банкінгу для підтвердження транзакцій та інших критично важливих операцій. Процедуру перевірки ЕЦП показано на рисунку 2.1.

Асиметричні алгоритми, зокрема RSA, потребують значних обчислювальних ресурсів для шифрування та дешифрування, що може впливати на продуктивність систем, особливо тих, які обробляють велику кількість транзакцій у реальному часі. Щоб подолати ці обмеження, широко застосовуються гібридні криптосистеми, що поєднують симетричне та асиметричне шифрування. У таких системах асиметричне шифрування використовується для безпечної передачі симетричного ключа, який надалі застосовується для шифрування і дешифрування даних.

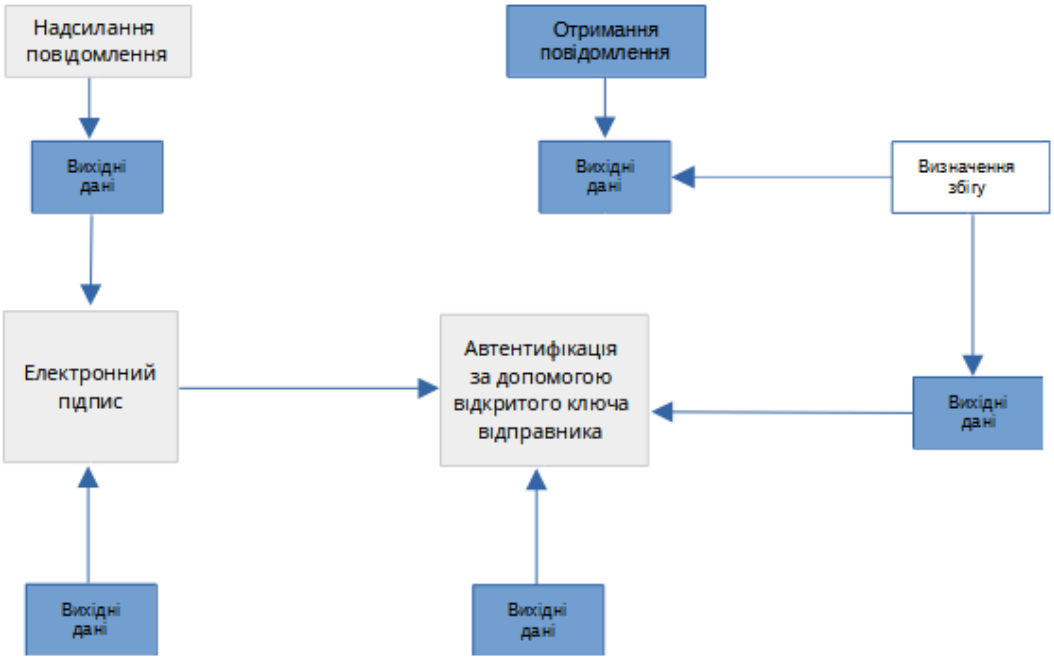

Рисунок 2.1 – Схема перевірки електронного цифрового підпису

Інфраструктура відкритих ключів (PKI) є важливим елементом управління асиметричними ключами в системах інтернет-банкінгу [14]. PKI забезпечує розробку, зберігання, управління та розподіл цифрових сертифікатів, які підтверджують автентичність відкритих ключів. Сертифікаційні центри видають сертифікати, що пов’язують відкриті ключі з конкретними особами або організаціями, створюючи довіру до відкритих ключів і дозволяючи користувачам безпечно шифрувати дані та перевіряти цифрові підписи.

Асиметричне шифрування також забезпечує масштабованість і гнучкість систем інтернет-банкінгу [13]. Відкриті ключі можуть вільно розповсюджуватися, що дозволяє будь-якому користувачу шифрувати дані для іншого користувача без необхідності обміну секретними ключами. Це спрощує розширення системи при додаванні нових користувачів. Крім того, у разі компрометації ключів їх можна легко відкликати або замінити, що забезпечує додатковий рівень безпеки.

2.4 Блокчейн-технологій у віддаленому інтернет-банкінгу

«Блокчейн-технологія є інноваційним підходом до зберігання даних, що забезпечує децентралізацію та високу стійкість до атак і маніпуляцій. Основна ідея блокчейну полягає у створенні децентралізованої бази даних, де кожен блок містить запис транзакцій, захищений криптографічними методами та пов’язаний з попереднім блоком. Це формує безперервний і незмінний ланцюг блоків, що підвищує прозорість і довіру до даних» [17, 21, 24, 36].

На відміну від централізованих систем, де існує єдина точка відмови, у блокчейні дані одночасно зберігаються на багатьох вузлах мережі. Кожен вузол містить копію всього блокчейну, і будь-які зміни в ланцюзі потребують погодження всіх вузлів (див. рисунок 2.2) Така структура підвищує безпеку та цілісність даних, роблячи систему стійкою до атак типу DoS та інших маніпуляцій.

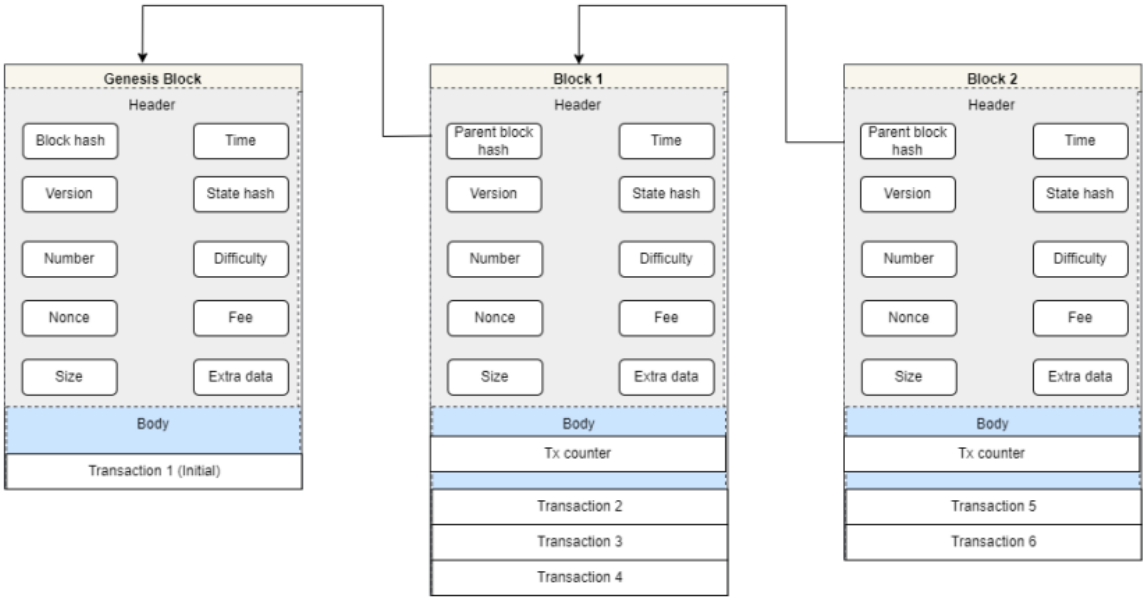

Рисунок 2.2 – Структурна схема ланцюга вузлів блокчейну

Кожен блок включає інформацію про транзакції, таймстамп і криптографічний хеш попереднього блоку. Хешування перетворює вхідні дані

у фіксовану бітову послідовність, унікальну для конкретного вмісту. Будь-яка модифікація даних призводить до видозміни хешу, що порушує ланцюг блоків. Інші вузли швидко виявляють зміни і відкидають неправдивий блок, забезпечуючи незмінність блокчейну.

Однією із переваг блокчейн-технології є прозорість. Всі транзакції доступні для перевірки учасниками мережі, що підвищує довіру і дозволяє контролювати автентичність і цілісність даних. У системах інтернет-банкінгу це сприяє прозорості фінансових операцій і запобігає шахрайству [17].

Децентралізація забезпечує високу доступність системи. Оскільки дані дублюються на багатьох вузлах, вихід з ладу одного або кількох вузлів не впливає на роботу системи, що критично для безперервного доступу до фінансових даних і транзакцій.

Крім того, блокчейн уможливлює забезпечення конфіденційності даних. Хоч транзакції видимі для учасників мережі, їх деталі можуть бути зашифровані, що гарантує доступ до конфіденційної інформації лише авторизованим користувачам. Це створює баланс між прозорістю та конфіденційністю, що є важливим для інтернет-банкінгу.

Блокчейн також підтримує використання розумних контрактів – програмних алгоритмів, які автоматично виконуються при настанні визначених умов. Розумні контракти дозволяють автоматизувати фінансові транзакції та договірні відносини, зменшуючи ризик помилок, пов’язаних з людським фактором. У системах інтернет-банкінгу вони можуть застосовуватися для автоматизації процесів виплат, кредитування та страхування, забезпечуючи підвищену надійність і швидкість виконання операцій [23].

Важливою перевагою блокчейн-технології є її стійкість до цензури. Оскільки дані зберігаються на багатьох вузлах мережі, жоден окремий учасник не може контролювати або змінювати інформацію без погодження з іншими учасниками. Це забезпечує захист від спроб цензури або маніпуляцій з боку урядів, корпорацій або інших впливових організацій. У контексті інтернет-

банкінгу це дозволяє забезпечити незалежність і цілісність фінансових транзакцій.

Впровадження блокчейн-технології в інтернет-банкінгу також сприяє зниженню витрат. Традиційні банківські системи часто вимагають значних ресурсів для управління та обробки транзакцій, зокрема через необхідність централізованого управління даними і забезпечення безпеки. Блокчейн-технологія з її децентралізованою архітектурою, дозволяє знизити ці витрати за рахунок автоматизації процесів і забезпечення безпеки на рівні самої технології. Це дозволяє банкам зосередитися на наданні якісних послуг і зменшити операційні витрати.

Для успішної інтеграції блокчейн-технології в існуючі банківські системи необхідно забезпечити сумісність з існуючими протоколами і стандартами. Це включає стандартизацію форматів даних, протоколів обміну інформацією і процедур управління безпекою. Сумісність і стандартизація забезпечують ефективну інтеграцію блокчейн-технології і дозволяють банкам використовувати її переваги без значних змін у існуючих системах. На основі проведеного аналізу сформовано таблицю 2.2 із зазначенням можливостей блокчейн-технологій.

Таблиця 2.2 – Блокчейн-технології для безпеки інтернет-банкінгу

Технологія	Переваги	Недоліки
Розподілений реєстр	Висока прозорість, стійкість до маніпуляцій, безпека даних	Високе навантаження на обчислювальні ресурси, в потреба в сховищі даних
Розумні контракти	Автоматизація угод, зниження ризиків шахрайства, забезпечення виконання умов	Складність розробки, необхідність аудиту безпеки коду

Продовження таблиці 2.2

Криптографічні протоколи	Високий рівень безпеки, стійкість до злому, конфіденційність даних	Висока складність реалізації, потреба в управлінні ключами
Децентралізовані додатки (DApps)	Стійкість до цензури, прозорість, безпека даних	Складність розробки та впровадження, висока потреба в ресурсах

Отже, блокчейн-технологія забезпечує децентралізований підхід до зберігання даних, що підвищує стійкість системи до атак і маніпуляцій. Вона гарантує високий рівень прозорості, довіри та безпеки фінансових транзакцій у системах інтернет-банкінгу, забезпечуючи автентичність, цілісність і конфіденційність даних. Враховуючи це, доцільно інтегрувати блокчейн у базу даних системи захисту інтернет-банкінгу для підвищення загального рівня інформаційної безпеки.

У наступному підрозділі розглянемо основні можливості хмарних технологій для системи захисту ВІБ й опишемо удосконалений алгоритм системи захисту інтернет-банкінгу на основі описаних технологій.

2.5 Хмарні технології в системах ВІБ

Сучасні системи інтернет-банкінгу значною мірою опираються на хмарні сервіси, адже вони дають змогу фінансовим установам оперативно адаптувати свої ресурси під потреби користувачів, швидко розширювати обчислювальні потужності та суттєво зменшувати витрати на утримання власного обладнання. Використання хмарних сервісів дозволяє швидко адаптувати ресурси під зміни навантаження, забезпечуючи високу доступність і надійність банківських послуг. Крім того, хмарні платформи надають можливість автоматичного

резервного копіювання даних і відновлення після збоїв, що критично важливо для безперервного функціонування фінансових систем [8, 36].

У традиційних IT-інфраструктурах масштабування ресурсів часто є складним і затратним процесом. Хмарні сервіси дозволяють оперативно збільшувати або зменшувати обчислювальні потужності відповідно до поточних потреб, що особливо важливо під час пікових навантажень, наприклад, у святкові дні або під час проведення акцій. Використання хмарних платформ також дозволяє знизити витрати на придбання, обслуговування та оновлення фізичного обладнання. Моделі оплати «pay-as-you-go» забезпечують економічну ефективність, оскільки банк сплачує лише за фактично використані ресурси.

Хмарні сервіси підвищують безпеку та надійність систем. Провайдери інвестують значні ресурси у захист даних, впроваджуючи шифрування, автентифікацію та моніторинг безпеки. Розподілені дата-центри і резервні копії гарантують високу доступність і можливість відновлення після технічних збоїв. Крім того, хмарні платформи часто відповідають вимогам регуляторних стандартів, таких як GDPR або PCI DSS, що дозволяє банкам забезпечити відповідність нормативним вимогам без необхідності впроваджувати складні внутрішні системи захисту.

Хмарні платформи відкривають доступ до сучасних технологічних механізмів, зокрема, штучного інтелекту, машинного навчання та інструментів аналізу великих масивів даних. Це дає змогу банкам удосконалювати взаємодію з клієнтами, підвищувати ефективність роботи внутрішніх систем і формувати рішення, засновані на точних даних та прогнозах.

Водночас використання хмарних технологій потребує ретельного управління та контролю. Основними ризиками є несанкціонований доступ до даних у багатокористувацькому середовищі, а також потенційні порушення конфіденційності та відповідності регуляторним вимогам. Для мінімізації цих ризиків банки застосовують шифрування даних при передачі та зберіганні, багаторівневий контроль доступу, автентифікацію користувачів, управління

ролями і правами доступу, а також моніторинг активності користувачів [34]. Регулярний контроль діяльності хмарних провайдерів, оновлення програм та проведення тестів на проникнення забезпечують дотримання політик безпеки і конфіденційності.

Таким чином, проведений аналіз дозволяє удосконалити схему функціонування системи захисту інтернет-банкінгу на основі алгоритмів шифрування, блокчейн-технологій та хмарних сервісів (див. рисунок 2.3). Авторизація користувачів у системі здійснюється за допомогою двофакторної автентифікації.

Рисунок 2.3 – Удосконалена схема системи забезпечення ІБ в інтернет-банкінгу

Дані транзакцій шифруються алгоритмами симетричного та асиметричного шифрування, резервні копії зберігаються у хмарному середовищі, а ключі – у блокчейні. Така багаторівнева система захисту дозволяє знизити ризики втрати конфіденційної інформації, перехоплення транзакцій та забезпечує актуалізацію журналу інцидентів.

Таким чином, удосконалений алгоритм базується принципах надійності, підвищеного рівня безпеки та відновлюваності й включає процедури виявлення аномалій, що уможливлює вчасне реагування та актуалізації політик безпеки.

2.6 Висновки до розділу

Розглянуто основні методи, механізми та технології забезпечення ІБ в системах ВІБ. Дослідження дозволило виявити ключові аспекти захисту даних та автентифікації користувачів й при цьому оцінити ефективність сучасних технологій у забезпеченні безпеки фінансових операцій. Обґрунтовано доцільність розробки комплексної моделі захисту фінансових даних на основі поєднання різних методі автентифікації користувачів, шифрування та сучасних технологій зберігання даних. Проаналізовано основні методи технічного захисту даних у системах ВІБ, розроблено основні рекомендації до їх застосування. Обгрунтовано застосування блокчейн-технологій для автоматизації банківських трансакцій на основі розумних контрактів та хмарних технологій з метою гнучкості та масштабованості.

РОЗДІЛ 3 МОДЕЛЬ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІБ В ІНТЕРНЕТ-БАНКІВСЬКИХ СИСТЕМАХ

3.1 Аналіз вимог до системи захисту фінансових даних

Основні вимоги до побудови системи захисту ВІБ в ІТ-інфраструктурі банків охоплюють широкий комплекс характеристик – від захисту даних і стійкості до кібератак до зручності використання, можливості масштабування та інтеграції з іншими ІС. Сучасні банківські платформи повинні відповідати підвищеним стандартам надійності й продуктивності, забезпечуючи стабільне та безпечне надання фінансових послуг у межах інтернет-банкінгу [1–7].

Одним із ключових аспектів є забезпечення високого рівня захищеності даних і транзакцій. В умовах постійного зростання кіберзагроз банки зобов’язані впроваджувати багаторівневу систему безпеки, що включає сучасні криптографічні методи для захисту інформації як під час передавання, так і під час збереження. Значну роль відіграють також багатофакторна автентифікація, антивірусні програми, системи моніторингу мережевої активності та фаєрволи. Проведення регулярних аудитів захисту та тестувань на проникнення дозволяє своєчасно виявляти слабкі місця та підвищувати стійкість системи.

Не менш важливою вимогою є забезпечення безперервної роботи інтернет-банкінгу. Сервіси мають бути доступними 24/7, незалежно від навантаження чи зовнішніх факторів. Для цього використовують резервовану та розподілену інфраструктуру, системи балансування навантаження, а також комплекси резервного копіювання і плани аварійного відновлення (Disaster Recovery Plan), що гарантують оперативне відновлення функціональності у разі збоїв.

Масштабованість ІТ-системи є також важливою для банків, що працюють в умовах постійного зростання кількості користувачів і транзакцій. Інтернет-банкінг повинен легко розширюватися, дозволяючи додавати нові функції без радикальної зміни архітектури системи.

Використання хмарних технологій суттєво підсилює гнучкість та дає змогу швидко реагувати на зміну ринкових тенденцій і впроваджувати нові продукти [11, 13–15].

Зручність і простота використання також відіграють важливу роль, оскільки напряму впливають на рівень задоволеності користувачів. Інтерфейс інтернет-банкінгу повинен бути інтуїтивним, адаптивним до різних пристроїв та забезпечувати швидкий доступ до основних функцій. Зрозуміла навігація та стабільність роботи підсилюють лояльність клієнтів.

Інтеграція з внутрішніми банківськими та зовнішніми сервісами є ще однією обов'язковою вимогою. Система має безперешкодно взаємодіяти з модулями управління рахунками, платіжною інфраструктурою, CRM-рішеннями та іншими платформами. Це забезпечує узгодженість бізнес-процесів і підвищує ефективність роботи всіх підрозділів банку.

Для підтримання конкурентоспроможності інтернет-банківські системи повинні мати можливість упровадження інноваційних технологій, зокрема, блокчейн, смарт-контракти, штучний інтелект чи машинне навчання [18, 35]. Завдяки цьому банки можуть розширювати перелік функцій, оптимізувати процеси та підвищувати якість обслуговування.

Окрему увагу слід приділити конфіденційності даних клієнтів. Банківські установи мають реалізовувати політики захисту персональної інформації відповідно до міжнародних і національних стандартів. Це передбачає застосування сучасних методів шифрування, чіткі процедури контролю доступу та регулярні перевірки безпеки. Надійний захист конфіденційних даних формує довіру клієнтів до банку.

Аналітика та звітність є важливими елементами керування банківською діяльністю. Системи інтернет-банкінгу повинні забезпечувати збір, обробку та зберігання інформації про транзакції та поведінку користувачів. Це надає можливість своєчасно виявляти тенденції, оцінювати ризики, удосконалювати сервіси та забезпечувати відповідність регуляторним вимогам.

Не менш важливою є підтримка широкого спектра платіжних інструментів – переказів, транзакцій з банківськими картками, електронних гаманців та криптовалют [20]. Це розширює можливості клієнтів та підвищує зручність здійснення різних фінансових операцій.

Отже, вимоги до системи ВІБ в ІТ-інфраструктурі банку охоплюють захищеність, надійність, масштабованість, зручність користування, інтеграційні можливості, інноваційність, забезпечення конфіденційності, підтримку аналітичних інструментів, різноманітність платіжних механізмів та якісну підтримку користувачів. Дотримання цих вимог формує міцну основу для ефективної, стабільної та безпечної роботи систем інтернет-банкінгу.

З огляду на те, що базою функціонування інтернет-банківських сервісів є саме база даних, важливим напрямом модернізації є впровадження додаткових засобів її захисту. Йдеться, насамперед, про використання блокчейн-технологій для зберігання криптографічних ключів, а також хмарних сервісів для розробки надійних резервних копій даних.

У наступному підрозділі буде детально описано безпечну модель системи ВІБ із позначенням компонентів, що потребують удосконалення.

3.2 Модель безпечної системи ВІБ

Побудова моделі безпечної системи ВІБ є складною задачею, яка вимагає врахування багатьох аспектів, зокрема, забезпечення безпеки даних, інтеграція з внутрішніми та зовнішніми системами, використання новітніх технологій та забезпечення зручності для користувачів. В основі моделі безпечної інтернет-банківські системи модульний підхід, причому кожен блок забезпечує різноманітні функції та сервіси, а також механізмів захисту, які гарантують цілісність та доступність та конфіденційність даних. На рисунку 3.1 показано узагальнену структурну схему моделі захисту.

Одним із основних модулів системи є модуль автентифікації користувачів. З метою забезпечення відповідного рівня безпеки модуль підтримує багатофакторну автентифікацію, що включає використання паролів, одноразових паролів (OTP), смарт-карт та біометричних даних (наприклад, відбитків пальців). Поєднання декількох факторів автентифікації значно ускладнює доступ зловмисникам і підвищує захищеність системи від несанкціонованого входу.

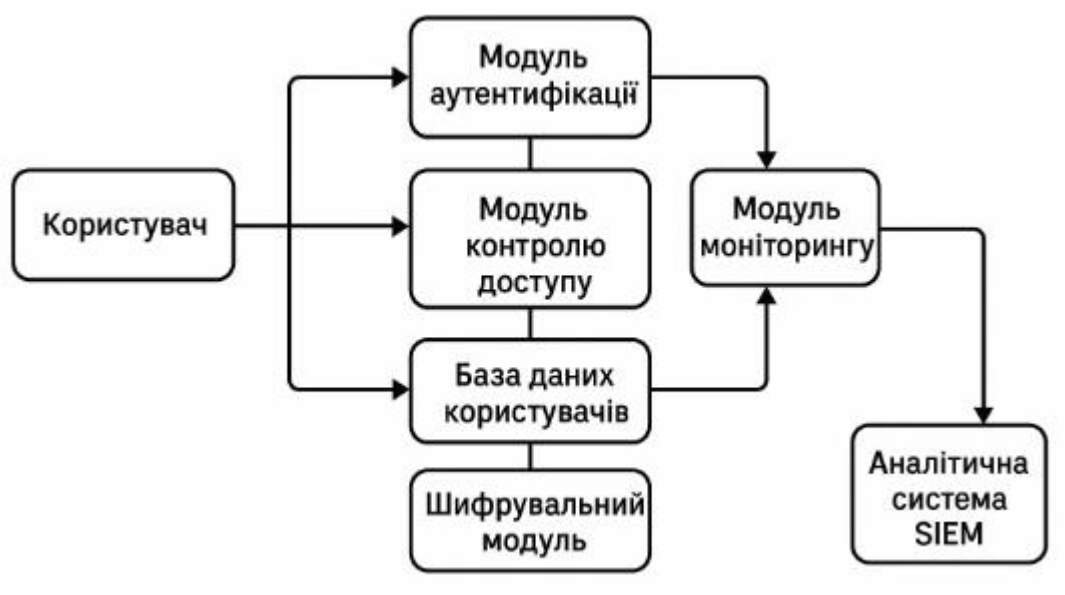

Рисунок 3.1 – Структурна схема моделі захисту інтернет-банкінгу

Модуль управління доступом є важливим компонентом системи інтернет-банкінгу, який контролює права користувачів відповідно до їх ролей та привілеїв. Це дозволяє обмежити доступ до конфіденційної інформації та критичних функцій, зменшуючи ризик несанкціонованого доступу та забезпечуючи принцип мінімальних привілеїв.

Модуль шифрування даних забезпечує захист інформації як під час передачі, так і при зберіганні. Для цього застосовуються сучасні криптографічні алгоритми симетричного шифрування (AES) та асиметричні методи (RSA). Навіть у разі перехоплення даних зловмисник не матиме можливості їх використати без відповідного ключа розшифрування. Надійність системи

підвищується завдяки використанню апаратних модулів безпеки (HSM) для генерації, зберігання та керування криптографічними ключами [8].

Модуль виявлення та запобігання вторгненням (IDS/IPS) відповідає за безперервний аналіз мережевого трафіку та дій користувачів у реальному часі. Застосування алгоритмів машинного навчання дозволяє системі визначати аномальні патерни та потенційно шкідливу активність. Завдяки цьому забезпечується оперативне виявлення кіберзагроз та своєчасне реагування з метою мінімізації можливих ризиків.

Модуль моніторингу включає підмодуль управління інцидентами безпеки, який забезпечує виявлення, реєстрацію, аналіз та реагування на інциденти. Він передбачає розробку планів реагування, визначення відповідальних осіб та впровадження заходів для мінімізації наслідків, що дозволяє ефективно протидіяти кіберзагрозам і підтримувати безперервну роботу системи.

Інтеграція з внутрішніми та зовнішніми системами забезпечує єдину платформу для управління фінансовими операціями та даними клієнтів. Взаємодія з платіжними процесорами, іншими банками та державними сервісами дозволяє здійснювати різні операції та надавати комплексні послуги.

Для підвищення захисту та прозорості реалізації фінансових операцій використовується блокчейн. Він забезпечує верифікацію автентичності та цілісності транзакцій, а розумні контракти автоматизують виконання умов угод, знижуючи ризики шахрайства.

Методи штучного інтелекту використано для автоматизації системи обслуговування клієнтів та аналізу фінансових даних. Наприклад, чат-боти можуть швидко відповідати на запити клієнтів, а методи машинного навчання аналізують транзакції та виявляють підозрілі операції.

Інтерфейс системи має бути інтуїтивно зрозумілим, зручним і адаптивним для різних пристроїв, забезпечуючи легкий доступ до сервісів та інформації. Система також повинна збирати, аналізувати та зберігати дані про операції та поведінку клієнтів для покращення сервісу, виявлення тенденцій і

ризиків, а також забезпечення відповідності регуляторним вимогам.Для побудови моделі безпечної системи ВІБ розроблено архітектуру, яка включає модулі та компоненти, що забезпечують захист даних і фінансових операцій. Нижче наведено основні компоненти моделі.

1. Модуль автентифікації користувачів:

2. Модуль керуавнян доступом – управління ролями та привілеями, призначення прав доступу, що відповідають поточній ролі, контроль доступу, моніторинг активності користувачів.

3. Модуль шифрування даних – симетричне та асиметричне шифрування, цифрові підписи.

4. Модуль ідентифікації та запобігання вторгненням – підсистема виявлення вторгнень, підсистема запобігання вторгнень, підсистема аналізу поведінки користувачів.

5. Модуль керуванян інцидентами безпеки – підсистема виявлення інцидентів, підсистема реєстрації інцидентів, підсистема, що реагує на інциденти.

6. Модуль захисту фінансових операцій (блокчейн технології, методи машинного навчання)

7. Модуль захисту даних (хмарні технології для розробки резервних копій,

Така модель включає всі необхідні компоненти для побудови безпечної, ефективної та зручної системи ВІБ, що забезпечує комплексний захист даних та трансакцій на основі технологій блокчейн [71].

Архітектура інтернет-банківські системи включає такі компоненти (див рисунок 3.2):

– клієнтський додаток – інтерфейс користувача для доступу до банківських послуг. Може бути реалізований у вигляді веб-додатку та мобільного додатку;

– серверна частина – сервер, який обробляє запити користувачів та взаємодіє з внутрішніми та зовнішніми системами;

– бази даних – сховища даних для зберігання інформації про клієнтів та їх рахунки, здійснені транзакції;

– модулі безпеки – компоненти для забезпечення автентифікації, управління доступом, шифрування даних, ідентифікації та протидії вторгненням, а також управління інцидентами безпеки.

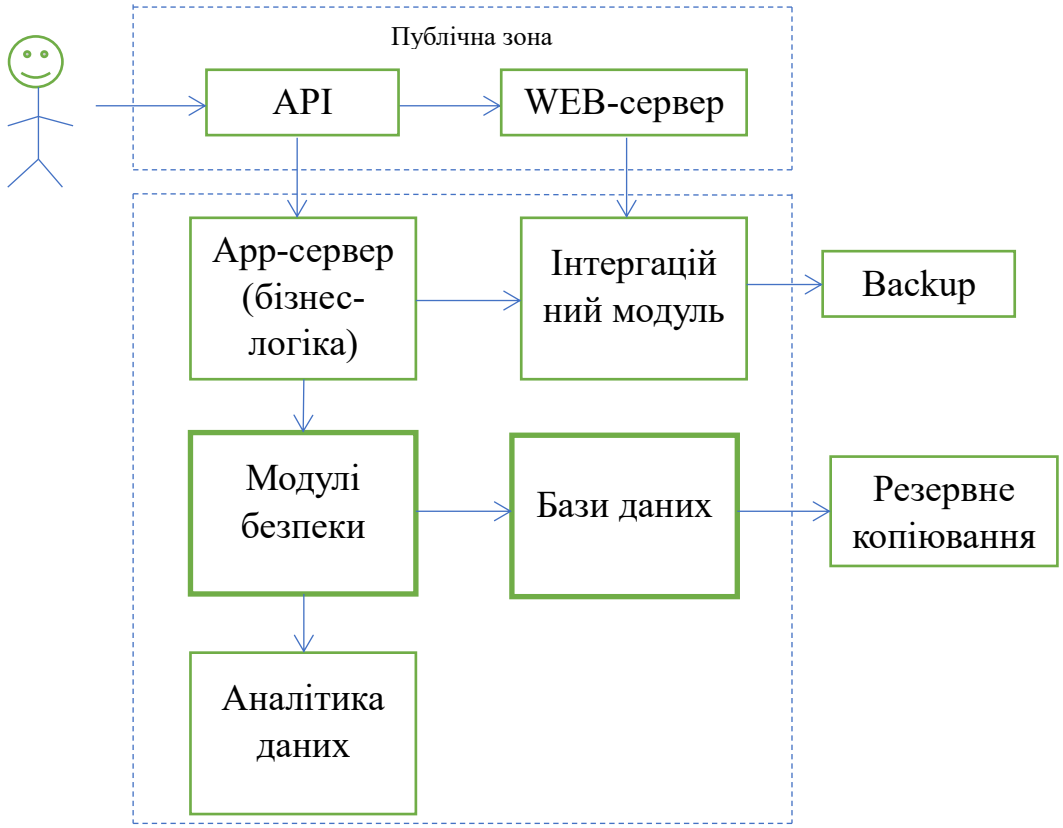

Рисунок 3.2 – Архітектура системи інтернет-банкінку

Користувач взаємодіє з клієнтським додатком для виконання банківських операцій, зокрема, перевірка балансу рахунку, переказ коштів чи здійснення оплат рахунків. Додаток передає запити до серверної частини через захищене з'єднання, наприклад, HTTPS. Сервер обробляє ці запити, виконуючи автентифікацію користувачів через спеціальний модуль, контролює доступ до ресурсів, шифрує та дешифрує дані, а також моніторить мережевий трафік і активність користувачів за допомогою IDS/IPS. Крім того, сервер взаємодіє з базами даних для збереження та отримання інформації, а також з внутрішніми й зовнішніми системами для виконання транзакцій та інших операцій.

Бази даних зберігають інформацію про клієнтів, рахунки, транзакції та інші дані, забезпечуючи їх захист за допомогою шифрування. Модель даних інтернет-банкінгу включає інтеграцію блокчейну, що передбачає розподіл інформації між on-chain та off-chain, що детальніше буде розглянуто у наступному підрозділі.

Таким чином, розробка прототипу інтернет-банківські системи включає розробку комплексної архітектури, яка забезпечує надійність, безпеку, зручність та ефективність надання банківських послуг через інтернет. Модулі безпеки та баз даних повинні працювати в поєднанні для підвищення рівня безпеки.

3.3 Модель бази даних інтернет-банкінгу

Модель бази даних ВІБ включає реляційну базу даних із збереженням даних про клієнтів, рахунки, трансакції, ролі та блокчейн для збереження даних, які є незмінними, верифікованими та підлягають публічній перевірці без порушення конфіденційності. Таким чином, нижче розглянемо детально архітектуру бази даних інтернет-банківські системи.

У таблиці 3.1 наведено елементи блокчейну із коротким описом. Таким чином, із аналізу таблиці бачимо, що у блокчейні зберігаються лише хеші транзакцій та метадані, а не фінансові чи особисті дані. Верифікація автентичності транзакцій відбувається без розкриття їх змісту.

У Off-chain зберігаються операційні дані, які потребують гнучкого оновлення, шифрування та швидкого доступу. Доступ до даних обмежений через автентифікацію та контроль ролей. Кожна зміна запису супроводжується побудовою нового хешу, який записується on-chain для підтвердження цілісності. У таблиці 3.2 показано елементи Off-chain із коротким їх описом.

Взаємодія між on-chain та off-chain відбувається на основі реалізації таких кроків:

Таблиця 3.1 – Елементи блокчейну

Елемент	Тип даних	Опис
transaction_hash	CHAR(64)	Унікальний хеш транзакції (SHA-256)
block_hash	CHAR(64)	Хеш блоку, що містить транзакцію
previous_block_hash	CHAR(64)	Посилання на попередній блок (ланцюг цілісності)
timestamp	DATETIME	Час побудови блоку
status	ENUM ('pending', 'confirmed', 'rejected')	Статус підтвердження транзакції
digital_signature	VARBINARY(256)	Підпис системного вузла або клієнта
proof	VARBINARY(128)	Доказ виконання операції (Proof-of-Authority або PoS)

– користувач ініціює транзакцію через клієнтський додаток;

– транзакція записується у off-chain базу (Transactions);

– система формує хеш транзакції (SHA-256 від сукупності ID, суми, часу, підпису);

– хеш передається у блокчейн – записується у on-chain журнал (BlockchainLedger);

– після підтвердження блоком, статус транзакції (confirmed або failed) оновлюється у off-chain базі.

Таблиця 3.2 – Елементи бази даних

Елемент	Тип даних	Опис
client_data	Таблиця Clients	Ім’я, адреса, контакти, ID у зашифрованому вигляді
account_data	Таблиця Accounts	Номери рахунків, баланс, валюта
transaction_details	Таблиця Transactions	Повна інформація про суму, одержувача, опис платежу
security_events	Таблиця AccessLogs	Логи дій користувачів, IP, час, статус
backup_records	Таблиця Backups	Метадані про резервні копії
blockchain_links	Таблиця BlockchainLedger	Відображення між внутрішніми записами і хешами блокчейну (transaction_id ↔ transaction_hash)

У разі аудиту система перевіряє чи існує хеш у блокчейні, чи відповідає він локальному обчисленню від поточних даних, тобто підтверджує цілісність. Логічну модель даних представлено у таблиці 3.3.

Таблиця 3.3 – Логічна модель даних інтернет-банківські системи

Рівень	Таблиці	Тип зберігання	Призначення
Користувачі	Clients, UserRoles	Off-chain	Ідентифікація, автентифікація
Рахунки	Accounts	Off-chain	Баланси, валюта, доступ
Транзакції	Transactions	Off-chain	Детальна фінансова інформація
Хеші транзакцій	BlockchainLedger	On-chain	Гарантія цілісності даних

Продовження таблиці 3.3

Статуси блоків	BlockchainLedger. status	On-chain	Верифікація стану
Журнали	AccessLogs, Backups	Off-chain	Контроль безпеки, аудити
Криптографічні ключі	HSM / KeyVault	Off-chain (захищене середовище)	Шифрування, підписи

Приклад зв’язку між блокчейном та базою даних показано на рисунку 3.3 у вигляді фрагменту програмного коду.

```
Transactions (off-chain)
  ├── transaction_id = 1025
  ├── amount = 2500.00
  ├── timestamp = 2025-11-10 18:25
  └── → SHA256 hash = 0xB3F9A...

BlockchainLedger (on-chain)
  ├── transaction_hash = 0xB3F9A...
  ├── block_id = 305
  ├── previous_block_hash = 0x98DD...
  └── status = "confirmed"
```

Рисунок 3.3 – Візуалізація зв’язку між off-chain та on- chain

Тепер розглянемо структуру бази даних на інтернет-банкінку, зважаючи на безпеку, шифрування даних та зв’язок з блокчейном. Проектування бази даних здійснено на основі реляційного підходу, оскільки для системи інтернет-банкінгу важливою є чітка структурованість. База даних містить таблиці «Клієнти», «Рахунки», «Трансакції», «Блокчейн-журнал», «Ролі», «Журнал безпеки», «Резервні копії», основні з яких які описано у таблицях 3.4-3.10.

Таблиця 3.4 – Клієнти

Поле	Тип даних	Особливості
client_id	INT (PK)	AUTO_INCREMENT
first_name	VARCHAR(100)	
last_name	VARCHAR(100)	
email	VARCHAR(150)	Унікальне
phone_number	VARCHAR(20)	Зашифроване
password_hash	VARBINARY(256)	bcrypt
created_at	DATETIME	
status	ENUM('active','blocked')	

Таблиця 3.5 – «Рахунки»

Поле	Тип даних	Особливості
account_id	INT (PK)	AUTO_INCREMENT
client_id	INT (FK)	FOREIGN KEY → Clients(client_id)
account_number	VARBINARY(128)	Зашифрований AES
currency	VARCHAR(10)	
balance	DECIMAL(18,2)	
created_at	DATETIME	

Таблиця 3.6 – «Трансакції»

Поле	Тип даних	Особливості
transaction_id	INT (PK)	AUTO_INCREMENT
from_account	INT (FK)	FOREIGN KEY → Accounts(account_id)
to_account	INT (FK)	FOREIGN KEY → Accounts(account_id)
amount	DECIMAL(18,2)	
timestamp	DATETIME	
status	ENUM('pending','completed','failed')	
transaction_hash	CHAR(64)	Унікальний
signature	VARBINARY(256)	RSA

Таблиця 3.7 – «Ролі»

Поле	Тип даних	Опис
role_id	INT (PK)	Ідентифікатор ролі
role_name	VARCHAR(50)	Назва ролі (Admin, Operator, Auditor, User)

Таблиця 3.8 – «Журнал блокчейн»

Поле	Тип даних
block_id	INT (PK)
previous_hash	CHAR(64)
data_hash	CHAR(64)
timestamp	DATETIME
nonce	INT
created_by	VARCHAR(50)

Таблиця 3.9 – «Журнал безпеки»

Поле	Тип даних	Опис
log_id	INT (PK)	Унікальний запис
client_id	INT (FK)	Хто виконував дію
action	VARCHAR(255)	Тип дії (login, transfer, view_balance)
ip_address	VARCHAR(45)	IP користувача
timestamp	DATETIME	Час події
result	ENUM('success','failure')	Результат авторизації або дії

Таблиця 3.10 – «Резервні копії»

Поле	Тип даних	Опис
backup_id	INT (PK)	Ідентифікатор копії
backup_date	DATETIME	Час створення
storage_location	VARCHAR(255)	Шлях до сховища
checksum	CHAR(64)	Контрольна сума
encrypted	BOOLEAN	Чи зашифровано копію

Як бачимо, таблиці містять записи, що відповідають безпеці даних, зокрема, методи шифрування, генерації ключів, автентифікації, розробки копій.

На рисунку 3.4 наведено ER-модель бази даних, якак забезпечує поділ основних сутностей на Off-chain та On-chain частини.

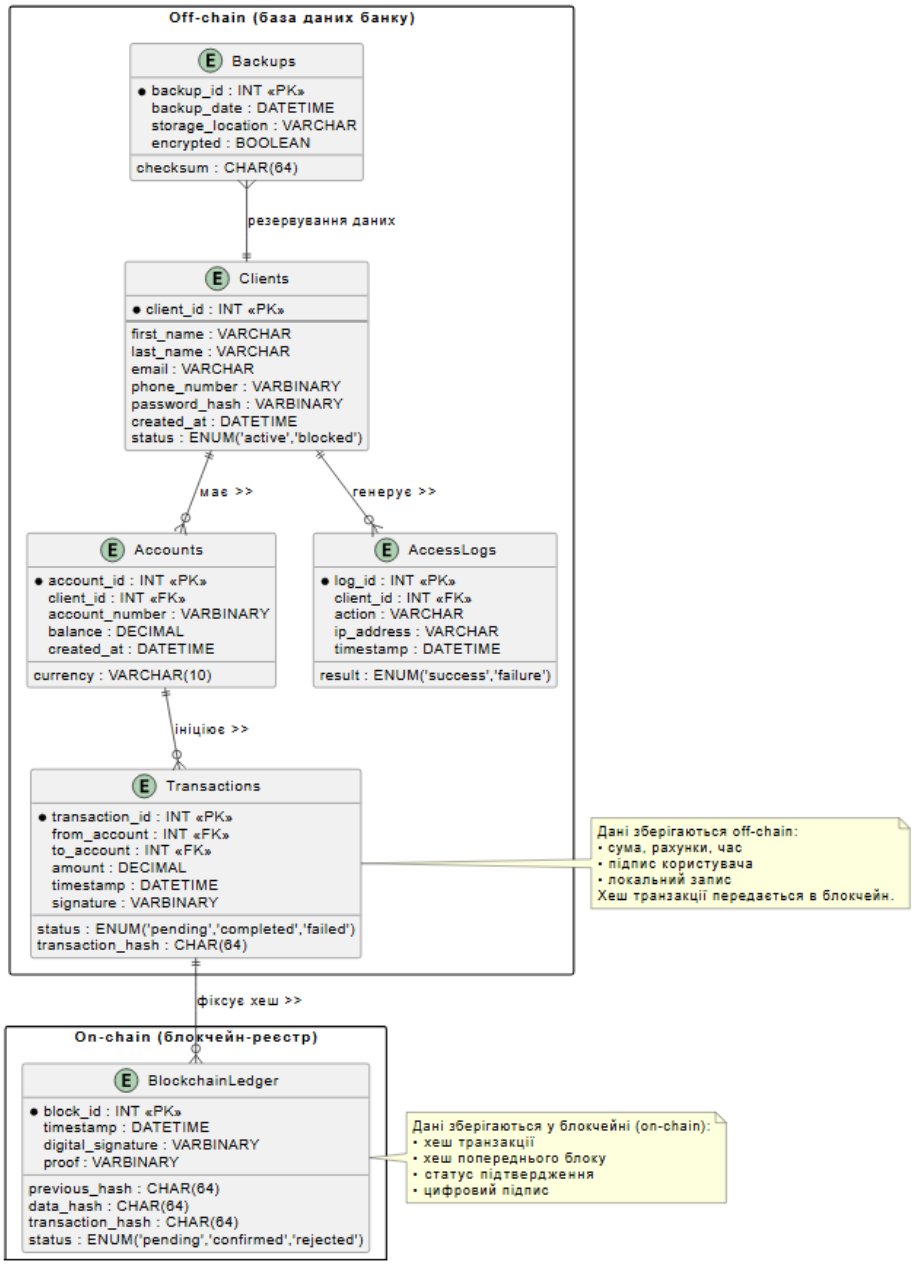

Рисунок 3.4 – Частина ER-моделі бази даних інтернет-банкінгу

Off-chain частина – це реляційна база даних інтернет-банківські системи, яка характеризується високою швидкістю обробки трансакцій, шифрування даних, доступ через автентифікацію). On-chain частина – це блокчейн-журнал (BlockchainLedger), який зберігає лише хеші та метадані для підтвердження цілісності. Кожна транзакція (Transactions.transaction_hash) має відповідний запис у блокчейні (BlockchainLedger.transaction_hash). На рисунку 3.5 наведено узагальнену (повну) ER-модель бази даних.

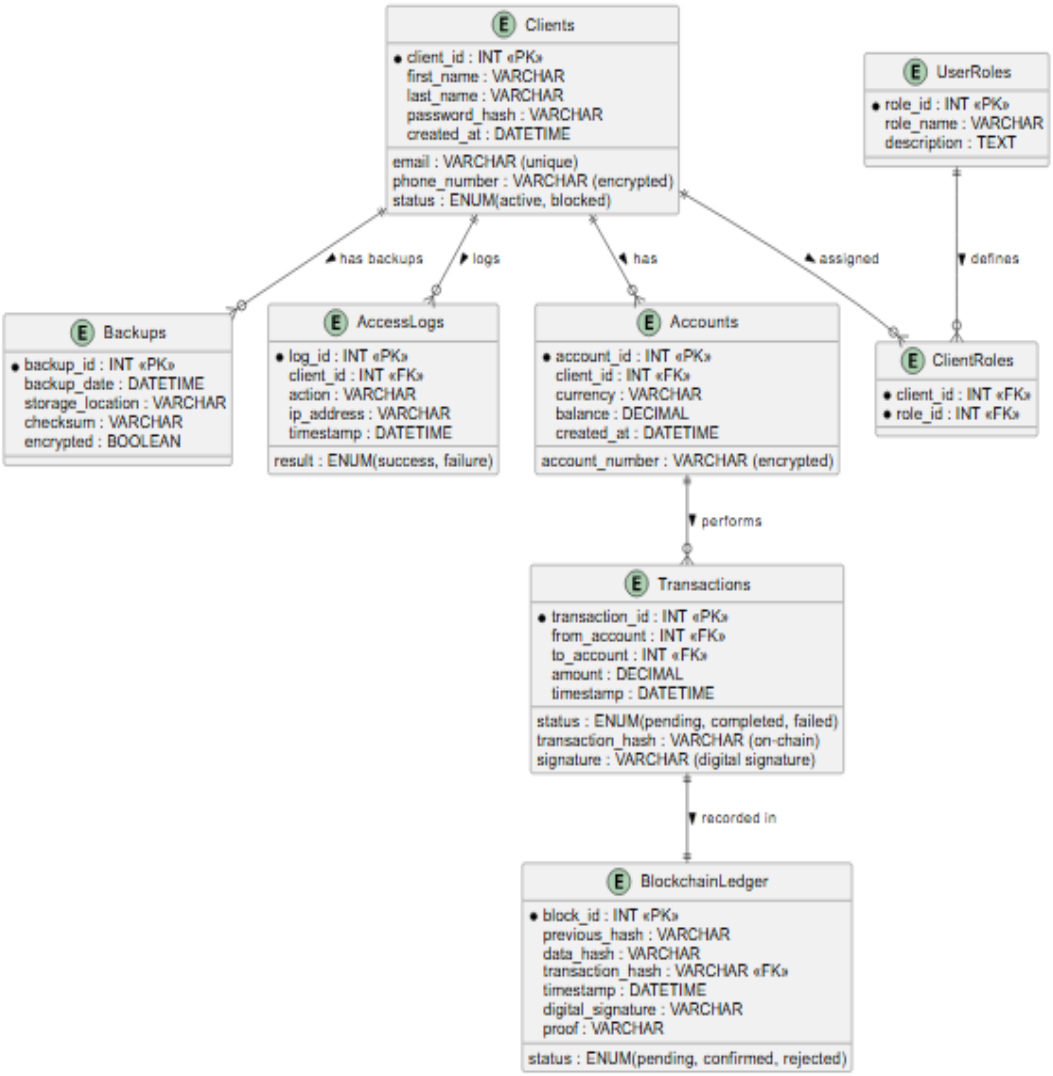

Рисунок 3.5 – Узагальнена ER-модель бази даних інтернет-банківської системи

Із аналізу моделі бази даних бачимо, що один клієнт може мати декілька рахунків, кожен рахунок може ініціювати кілька трансакцій (from_account) й отримувати багато трансакцій (to_account).

Кожна трансакцій має свій запис у блокчейн-журналі. Один клієнт генерує багато записів у журналі (дані клієнта логуються). В той же час клієнт може мати декілька ролей. Лише одну роль можна призначити кільком клієнтам. Існує можливість робити резервні копії даних клієнта.

Така модель бази даних містить засоби захисту даних, ґрунтується на принципах надійності, стійкості до збоїв та безпеки. На рисунку 3.6 наведено діаграму діяльності, що забезпечує безпечну обробку трансакцій у системі

інтернет-банкінгу й показує послідовність дій користувача та системи при виконанні трансакцій.

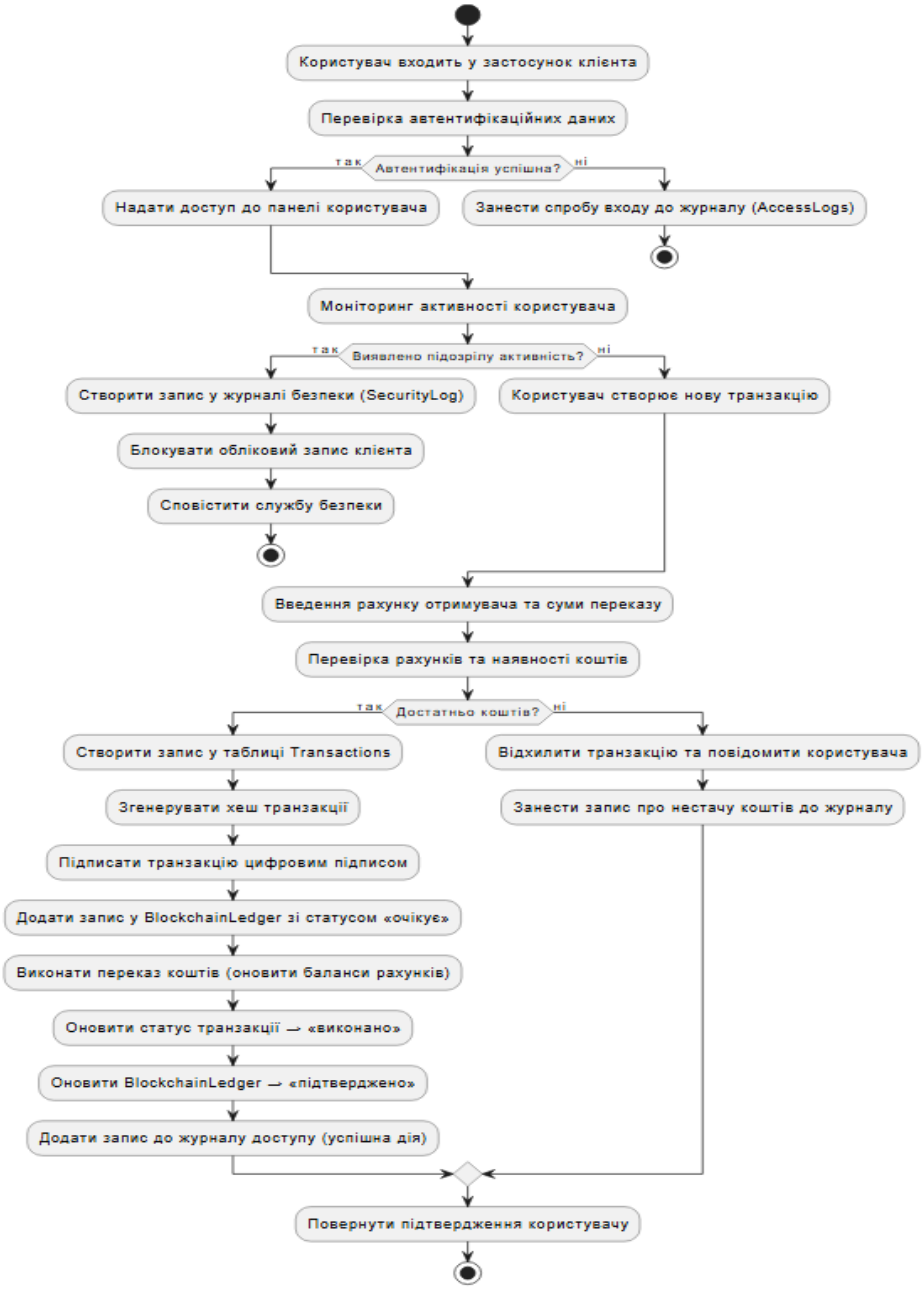

Рисунок 3.6 – Діаграма діяльності

Така діаграма забезпечує наочність взаємодії між компонентами інтернет-банківські системи, дозволяє виявити потенційні загрози безпеці й допомагає оптимізувати бізнес-логіку банківських операцій.

3.4 Висновки до розділу

Спроектовано комплексну модель безпечної інтернет-банківські системи, спрямовану на забезпечення захисту фінансових даних користувачів. На основі проведеного аналізу сформовано вимоги до безпеки, що включають автентифікацію, керуавння доступом, шифрування даних, моніторинг активності користувачів та реагування на інциденти. Побудована архітектура системи передбачає інтеграцію модулів безпеки у всі рівні – від клієнтського додатку до бази даних. Модель використовує технології блокчейн для фіксації транзакцій, що забезпечує їх незмінність та прозорість, а також механізми резервного копіювання для збереження цілісності даних. Розроблено модель бази даних, що забезпечує структуроване, надійне та захищене зберігання інформації про клієнтів, рахунки й транзакції.

ВИСНОВКИ

У роботі досліджено актуальну задачу розробки алгоритмів захисту інформації в системах ВІБ. При цьому отримано наукові та практичні результати.

1. Досліджено особливості та сучасний стан інформаційної безпеки у віддалених банківських системах та методи її забезпечення, виявлено ключові проблеми та тенденції в захисті банківських систем, а також сформовано базу знань для розробки безпечної системи інтернет-банкінгу

2. Визначено основні види інтернет-шахрайства та вразливості, характерні для систем інтернет-банкінгу, що дало змогу конкретизувати загрози та слабкі місця систем націлені на ефективні методи захисту.

3. Досліджено сучасні технології та механізми захисту інформації, включаючи шифрування, багатофакторну автентифікацію, токени безпеки та системи моніторингу аномалій, що уможливило сформувати вимоги до сучасної системи ВІБ.

4. Розроблено логічну та фізичну модель безпечної інтернет-банківські системи на основі розширеної архітектури бази даних та контролю доступу користувачів, що забезпечує контроль, конфіденційність, цілісність та доступність інформації.

5. Удосконалено систему інтернет-банкінгу з використанням блокчейн та хмарних технологій для забезпечення прозорості транзакцій та масштабування й резервування даних, що уможливило підвищити надійність, стійкість до атак та ефективність обробки фінансових операцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авраменко О. М. Інтернет-банкінг: особливості та перспективи розвитку банківській системі України. Економіка: проблеми теорії та практики : зб. наук. пр. Дніпропетровськ : ДНУ, 2010. С. 707-712.

2. Базилевич В. Розвиток фінансового ринку в сучасних умовах. Фінанси України. 2009. № 12. С. 5–12.

3. Банківська система України : становлення і розвиток в умовах глобалізації економічних процесів : монографія / за ред. О.В. Дзюблюка. Тернопіль : Вектор, 2012. 355 с.

4. Блащук-Дев'яткіна Н.З., Петришин Х.Р. ДБО: теоретичні аспекти, сучасний стан та перспективи його розвитку // «Молодий вчений». 2022. № 9 (109). С. 122–128.

5. Боднар О., Паламарчук В., Гаврилов А. Аналіз стану ринку банківських послуг України в умовах пандемії. Modern Economics. 2020. Вип. № 23. С. 13-19.

6. Борисова І.С., Галінська Т.С. Інтернет-банкінг як перспективний напрям розвитку ринку банківських послуг.URL: www.pdaa.edu.ua (дата звернення: 12.12.2021).

7. Вядрова І., Мозговська А., Вядрова В. Розвиток системи дистанційного банківського обслуговування // Банки сучасного та майбутнього. 2022. Вип. 4 (7). С. 7-13.

8. Голда А. А. Методи та засоби забезпечення інформаційної безпеки в системах інтернет-банкінгу: квал. роб. Тернопіль : Терн. нац. техн. у-тет, 2023. 72 с.

9. Гураль В.С., Зубрович Р.Е., Савка Н.Я. Системи контролю показників здоров'я людини // Матеріали XVIII міжнародної науково-практичної конференції «Інформаційні технології та автоматизація – 2025». Одеса, 30-31 жовтня 2025. С.

10. Деменков М. Інтернет-технології в обслуговуванні клієнтів банку. Банківська справа. 2009. №1. С. 58-64.

11. Деркач А. О. Діджиталізація банківського сектору України. Фінансові дослідження. 2016. № 1. С. 69–75.

12. Єсіна О. Г. Інтернет-банкінг в Україні: сучасний стан, проблеми та перспективи розвитку. Вісник соціально-економічних досліджень. 2013. Вип. 1. С. 209-213.

13. Засадна Х. О. Про захист послуг Інтернет-банкінгу. Вісник університету банківської справи національного банку України. 2008. № 3. С. 225-229.

14. Засадний Х.О. Про захист послуг Інтернет-банкінгу. Вісник університету банківської справи національного банку України. 2009. № 12. С. 5–12.

15. Захарченко О.М. Безпека системи дистанційного банківського обслуговування та напрями її забезпечення: веб-сайт. URL: https://core.ac.uk/download/pdf/300237413.pdf (дата звернення 18.05.2025 р.).

16. Зубрович Р.Е., Приходько алгоритм реконструкції зображень на основі глибоких нейромереж // Матеріали III всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Інтелектуальні комп'ютерні системи та мережі. Тернопіль:ЗУНУ, 2025. С. 135-135.

17. Карчева Г. Т., Карчева І. Я. Інноваційні блокчейн-технології як фактор підвищення ефективності фінансової сфери та економіки. Наукові праці НДФІ. 2017. Вип. 4. С. 39-42.

18. Клюско Л. А. Інновації у сфері банківського бізнесу. Збірник наукових праць Університету державної фіскальної служби України. 2019. № 2. С. 109-128.

19. Коробова Г.Г. Банківська справа: навч. посіб. Москва: ИНФРАМ, 2015. 154 с.

20. Коробчук Т. Використання платіжних систем в Інтернеті. Економічні науки. 2008. №5. С.303-309.

21. Костіна Н. І. Банки: сучасні інформаційні технології : навч. посіб. Ірпінь, 2001. 359 с.

22. Костогриз В. Г. Дистанційне обслуговування як перспективна складова системи дистрибуції банківських продуктів. Фінансовий простір. 2011. № 1. С. 33-41.

23. Котуранова Т. В., Вартоха Я. С., Александрова М. О. Інтернет-банкінг в Україні – інноваційний розвиток банківської сфери. Економічний простір. 2019. № 146. С. 43-56.

24. Кулініч О. А., Андросов В. Ю. Інтернет-банкінг в Україні як складова розвитку мережної інфраструктури. Економічна стратегія і перспективи розвитку сфери торгівлі та послуг. Харків: Харк. держ. ун-т харчування та торгівлі. 2011. Вип. 2. С. 421-429.

25. Методичні вказівки до оформлення курсових, звітів про проходження практики, випускних кваліфікаційних робіт для студентів спеціальності «Комп’ютерна інженерія» / І.В. Гураль, Л.О.Дубчак / під ред. О.М. Березького. Тернопіль: ТНЕУ, 2019. 34 с.

26. Методичні рекомендації до виконання кваліфікаційної роботи з освітнього ступеня “Магістр” спеціальності 123 «Комп’ютерна інженерія» Магістерська програма - Комп’ютерна інженерія" / О.М. Березький, Г.М. Мельник / Під ред. Л.О.Дубчак. Тернопіль: ЗУНУ, 2024. 32 с.

27. Міщанин О. М. Інтернет-банкінг в Україні. Молодіжний економічний дайджест. 2014. № 1(1). С. 71-75.

28. Нікіфорова А. О. Вітчизняний та зарубіжний Інтернет-банкінг – стан, проблеми та перспективи розвитку. Регіональна економіка. 2010. № 8. С. 23-26.

29. Руда О.Л. Дистанційне обслуговування в банківській системі інфраструктура ринку. 2020. Випуск 39. С. 353-358.

30. Сербина О. Г. Інтернет-банкінг: українська практика та світовий досвід. Молодий вчений. 2014. № 4(07)(1). С. 122-125.

31. Сербина О. Г., Загузова О. М. Інтернет-банкінг: українська практика та світовий досвід. Молодий вчений. Херсон: Гельветика., 2014. № 4(07)(1). С. 122-125.

32. Страхарчук А.Я. Інформаційні системи і технології в банках: навч. посіб. Київ: Знання. 2010 р. 201 с.

33. Тангієв А.А. Деревецький В.Ю., Гураль В.С. Методи протидії атакам на дистанційний банкінг. Матеріали IX Всеукраїнської науково-практичної конференції молодих вчених «Інформаційні технології – 2024». 16 травня 2024 р., м. Київ, 2024. С. 260-261.

34. Чуб О.О. Розвиток Інтернет-банкінгу в глобальному середовищі. Вісник Української академії банківської справи. 2010. №10.С.10-23.

35. Юденков, Н. Інтернет-технології в банківському бізнесі: перспективи і ризики : навч. посіб. Миколаїв: КНОРУС. 2010. 320 с.

36. Burkovska A., Koval P. Innovative technologies in the banking sector of Ukraine in the period of digitalization // Ukrainian Black Sea Region Agrarian Science. 2023. Vol. 27. No. 1. P. 51-63.

37. Kloba Lev, Kloba Taras Cyber threats of the banking sector in the conditions of the war in Ukraine // Financial and credit activity: problems of theory and practice. 2022. Vol. 5 (46). P. 19-28.

38. MegaMatcher Automated Biometric Identification System: веб-сайт. URL: https://www.neurotechnology.com/megamatcher-abis.html?gad_source=1&gclid=Cj0KCQjw3tCyBhDBARIsAEY0XNllG36QoZQrxilz5KNLlz6s80XikaNrIG4Bi5YjjuZsXyiVQoE9RS8aAoA5EALw_wcB (дата звернення 01.09.2025 р.).