НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут телекомунікаційних систем

Кафедра інформаційних технологій в телекомунікаціях

До захисту допущено:

В.О. завідувача кафедри

_____ Валерій ПРАВИЛО

«_____»_____2026 р.

ДИПЛОМНА РОБОТА

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інформаційно-комунікаційні технології»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Підхід до підвищення стійкості криптографічного захисту в банківських мережах»

Виконала: здобувачка вищої освіти 4 курсу, групи ТІ-22

Менська Юлія Вікторівна _____

Науковий керівник: професор кафедри ІТТ НН ІТС,

доктор технічних наук, доцент

Астраханцев Андрій Анатолійович _____

Рецензент: професор кафедри ТК НН ІТС,

доктор технічних наук, доцент

Нестеренко Микола Миколайович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Здобувачка вищої освіти _____

Київ – 2026 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут телекомунікаційних систем
Кафедра інформаційних технологій в телекомунікаціях

Рівень вищої освіти – перший (бакалаврський)
Освітньо-професійна програма «Інформаційно-комунікаційні технології»
спеціальності 172 Телекомунікації та радіотехніка

ЗАТВЕРДЖУЮ

В.О. завідувача кафедри

_____ Валерій ПРАВИЛО
«_____»_____2026 р.

ЗАВДАННЯ

на дипломну роботу студентці

Менській Юлії Вікторівні

1. Тема дипломної роботи: Підхід до підвищення стійкості криптографічного захисту в банківських мережах, науковий керівник роботи професор кафедри ІТТ НН ІТС, доктор технічних наук, доцент Астраханцев Андрій Анатолійович – затверджені наказом по університету від 26.05.2026 р. №1912-с.

2. Строк подання студентом дипломної роботи 06.06.2026 р.

3. Об’єкт дослідження: Процес криптографічного захисту інформації в мережах банківських установ в умовах зростання кіберзагроз та появи постквантових методів криптоаналізу.

4. Вихідні дані до роботи: криптографічні алгоритми шифрування та цифрового підпису, постквантові криптографічні алгоритми, методи криптоаналізу, методи завадостійкого кодування, сучасні підходи до підвищення стійкості криптографічного захисту інформації в банківських мережах, а також наукові публікації, стандарти та нормативні документи у сфері криптографічного захисту інформації.

5. Перелік завдань, які потрібно розробити: Провести аналіз сучасних загроз інформаційній безпеці телекомунікаційних мереж банківських установ та визначити вимоги до їх криптографічного захисту.

Здійснити порівняльний аналіз алгоритмів шифрування за критеріями криптографічної стійкості та складності реалізації.

Дослідити можливість інтеграції елементів завадостійкого кодування як додаткового рівня захисту цілісності даних у складі існуючих криптографічних схем.

Обґрунтувати доцільність застосування постквантових алгоритмів для захисту каналу обміну ключами в банківських мережах.

Створити підхід до підвищення стійкості криптографічного захисту та оцінити його ефективність за показниками криптографічної стійкості, обчислювальної складності, стійкості до квантових атак і можливості адаптації до потенційних кіберзагроз.

6. Перелік ілюстративного матеріалу: презентація – 19 слайдів, 6 таблиць, 16 рисунків.

7. Дата видачі завдання: 05.10.2025 р.

Календарний план

№з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Узгодження організаційних питань з науковим керівником	05.10.25 - 06.10.25	Виконано
2	Узгодження теми роботи та початок роботи над першим розділом	06.10.25 - 09.10.25	Виконано
3	Робота над першим, другим та третім розділами	09.10.25 - 06.01.26	Виконано
4	Робота над четвертим розділом. Розробка власного підходу	06.01.26 - 26.04.24	Виконано
5	Оформлення дипломної роботи	26.04.26 - 30.04.26	Виконано
6	Підготовка презентації до захисту	30.04.26 - 16.05.26	Виконано

Здобувачка вищої освіти _____ Юлія МЕНСЬКА

Науковий керівник роботи _____ Андрій АСТРАХАНЦЕВ

РЕФЕРАТ

Дипломна робота «Підхід до підвищення стійкості криптографічного захисту в банківських мережах» містить 84 сторінок тексту, 19 рисунків та 6 таблиць, а також використовує 57 літературних джерел.

Актуальність теми. Забезпечення стійкого криптографічного захисту інформації в банківських мережах є одним із ключових завдань сучасних телекомунікаційних систем, оскільки банківський сектор належить до об’єктів критичної інформаційної інфраструктури. Зростання кількості кіберзагроз, збільшення обсягів електронних фінансових операцій та розвиток методів криптоаналізу висувають підвищені вимоги до ефективності існуючих криптографічних засобів захисту. Додатковим викликом є розвиток постквантових обчислень, який створює потенційну загрозу для сучасних алгоритмів шифрування та обумовлює необхідність пошуку підходів до підвищення стійкості криптографічного захисту без повної модернізації банківської інфраструктури.

Метою роботи є підвищення стійкості криптографічного захисту інформації в банківських телекомунікаційних мережах до сучасних та постквантових загроз шляхом створення підходу до поетапного нарощування рівня захисту існуючих криптографічних схем.

Об’єктом дослідження процес криптографічного захисту інформації в мережах банківських установ в умовах зростання кіберзагроз та появи постквантових методів криптоаналізу.

Предметом дослідження є стійкість існуючих криптографічних схем захисту банківських мереж та властивості підходу до її підвищення шляхом інтеграції елементів завадостійкого кодування і постквантових алгоритмів.

Методи дослідження. Для досягнення поставленої мети використано системний аналіз, порівняльний аналіз, методи аналітичної оцінки

криптографічної стійкості, теорії ймовірностей та оцінювання обчислювальної складності алгоритмів. Системний аналіз застосовано для дослідження сучасних загроз інформаційній безпеці банківських мереж та визначення вимог до криптографічного захисту. Порівняльний аналіз використано для оцінювання характеристик симетричних, асиметричних і постквантових алгоритмів за критеріями стійкості та складності реалізації. Методи аналітичної оцінки криптографічної стійкості, теорії ймовірностей та оцінювання обчислювальної складності застосовано для кількісного аналізу характеристик алгоритмів та оцінювання ефективності запропонованого підходу.

Запропонований підхід забезпечує можливість поетапного підвищення стійкості криптографічного захисту та адаптації банківських телекомунікаційних систем до сучасних і перспективних кіберзагроз без необхідності повної заміни існуючої криптографічної інфраструктури.

Ключові слова: БАНКІВСЬКІ МЕРЕЖІ, КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, АЛГОРИТМИ ШИФРУВАННЯ, ПОСТКВАНТОВА КРИПТОГРАФІЯ, ЗАВАДОСТІЙКЕ КОДУВАННЯ, КРИПТОАНАЛІЗ, ЦИФРОВИЙ ПІДПИС, ОБМІН КЛЮЧАМИ, КІБЕРБЕЗПЕКА.

ABSTRACT

The master's thesis «An approach to enhancing the robustness of cryptographic security in banking networks» contains 84 pages, 19 figures, and 6 tables and 57 references sources.

Relevance of the topic. Ensuring robust cryptographic protection of information in banking networks is one of the key challenges of modern telecommunication systems, as the banking sector belongs to the category of critical information infrastructure. The increasing number of cyber threats, the growing volume of electronic financial transactions, and the continuous advancement of cryptanalytic methods impose heightened requirements on the efficiency of existing cryptographic protection mechanisms. An additional challenge is the emergence of post-quantum computing, which poses a potential threat to contemporary encryption algorithms and necessitates the development of approaches aimed at enhancing the resilience of cryptographic protection without a complete overhaul of banking infrastructure.

The aim of the study is to improve the robustness of cryptographic information protection in banking telecommunication networks against modern and post-quantum threats by developing an approach for the incremental strengthening of existing cryptographic schemes.

The object of research is the process of cryptographic protection of information in banking networks under conditions of increasing cyber threats and the emergence of post-quantum cryptanalytic methods.

The subject of research is the resilience of existing cryptographic schemes used in banking networks and the properties of an approach for enhancing this resilience through the integration of error-correcting coding elements and post-quantum algorithms.

Research methods. To achieve the stated objective, system analysis, comparative analysis, methods of analytical evaluation of cryptographic strength, probability theory, and computational complexity analysis were employed. System analysis was applied to study contemporary threats to information security in banking networks and to define requirements for cryptographic protection. Comparative analysis was used to evaluate the characteristics of symmetric, asymmetric, and post-quantum algorithms according to criteria of resistance and implementation complexity. Methods of analytical assessment of cryptographic strength, probability theory, and computational complexity analysis were applied for the quantitative evaluation of algorithmic properties and the effectiveness of the proposed approach.

The proposed approach enables a gradual enhancement of cryptographic protection resilience and supports the adaptation of banking telecommunication systems to both current and emerging cyber threats without requiring a complete replacement of the existing cryptographic infrastructure.

Keywords: BANKING NETWORKS, CRYPTOGRAPHIC INFORMATION PROTECTION, ENCRYPTION ALGORITHMS, POST-QUANTUM CRYPTOGRAPHY, ERROR-CORRECTING CODING, CRYPTANALYSIS, DIGITAL SIGNATURE, KEY EXCHANGE, CYBERSECURITY.

ЗМІСТ

СПИСОК ТЕРМІНІВ І СКОРОЧЕНЬ 10
ВСТУП 11
РОЗДІЛ 1
ПРИНЦИПИ ПОБУДОВИ ТА ЗАХИСТУ МЕРЕЖ В БАНКІВСЬКИХ УСТАНОВАХ 14
1.1 Нормативно-правова база забезпечення інформаційної безпеки банківських установ України 15
1.2 Загальні принципи організації захисту інформації в банківських установах 16
1.2.1 Фізичний захист об'єктів банківської інфраструктури 17
1.2.2 Організаційні заходи забезпечення інформаційної безпеки 20
1.2.3 Технічні засоби захисту в банківських мережах 21
1.2.4 Безпека банківських комп'ютерних мереж та каналів передачі даних 23
1.2.5 Криптографічні засоби захисту інформації 24
1.3 Вимоги до криптографічного захисту в банківських системах 25
1.4 Висновки до першого розділу 28
РОЗДІЛ 2
ОГЛЯД ІСНУЮЧИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ТА МЕТОДІВ АТАК 29
2.1 Класифікація та аналіз класичних атак на криптографічні алгоритми і канали передачі даних 29
2.2 Характеристики та оцінка криптографічної стійкості алгоритмів 31
2.3 Симетричні алгоритми шифрування 34
2.4 Асиметричні алгоритми шифрування 42
2.5 Гібридні алгоритми шифрування та криптографічні схеми в телекомунікаційних протоколах захисту 46

2.6 Висновки до другого розділу 49

РОЗДІЛ 3

ПОРІВНЯЛЬНИЙ АНАЛІЗ ХАРАКТЕРИСТИК АЛГОРИТМІВ ШИФРУВАННЯ ТА ЦИФРОВОГО ПІДПИСУ 51

3.1 Недоліки та обмеження існуючих підходів 51

3.2 Порівняльний аналіз симетричних алгоритмів шифрування 54

3.3 Порівняльний аналіз алгоритмів цифрового підпису та забезпечення цілісності даних 58

3.4 Висновки до третього розділу 60

РОЗДІЛ 4

АНАЛІЗ ПОСТКВАНТОВИХ АЛГОРИТМІВ ШИФРУВАННЯ І ПІДХОДІВ ДО ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ 62

4.1 Обґрунтування необхідності застосування постквантових алгоритмів 62

4.2 Огляд та класифікація основних постквантових алгоритмів 65

4.3 Порівняльний аналіз сучасних та постквантових алгоритмів шифрування 67

4.4 Пропозиції щодо підвищенню стійкості алгоритмів шифрування в банківських системах 72

4.5 Підхід до поетапного вдосконалення криптографічного захисту в банківських мережах 74

4.6 Висновки до четвертого розділу 78

ЗАГАЛЬНІ ВИСНОВКИ 80

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 83

СПИСОК ТЕРМІНІВ І СКОРОЧЕНЬ

NIST	National Institute of Standards and Technology
НБУ	Національний банк України
DORA	Digital Operational Resilience Act (Закон про цифрову операційну стійкість)
DMZ	Demilitarized Zone
AAA	Authentication, Authorization, Accounting
КЗІ	Криптографічний захист інформації
E2EE	End-to-End Encryption (Наскрізне шифрування)
PKI	Public Key Infrastructure (Інфраструктура відкритих ключів)
MAC	Media Access Control
VPN	Віртуальна приватна мережа
VLAN	Virtual Local Area Network (Віртуальна локальна мережа)
ДССЗЗІ	Державна служба спеціального зв'язку та захисту інформації
HSM	Hardware Security Module (Апаратні модулі безпеки)
SP-мережі	Substitution-Permutation network
DES	Data Encryption Standard
IDEA	International Data Encryption Algorithm
AES	Advanced Encryption Standard
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography (Криптографія на еліптичних кривих)
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDH	Elliptic Curve Diffie–Hellman (Протокол Діффі-Хеллмана на еліптичних кривих)
ECDSA	Elliptic Curve Digital Signature Algorithm (Алгоритм цифрового підпису на еліптичних кривих)
OSI	Open Systems Interconnection (Мережева модель OSI)
HKDF	HMAC-based Key Derivation Function
KEM	Key Encapsulation Mechanism (Механізм інкапсуляції ключа)

ВСТУП

«Безпека – це процес, а не продукт. Продукти забезпечують певний рівень захисту, але єдиний спосіб ефективно вести бізнес у небезпечному світі – це впровадити процеси, які враховують властиву продуктам вразливість» [1]. Ці слова належать Брюсу Шнайєру – одному з найвідоміших американських криптографів та експертів у сфері комп'ютерної безпеки. Незважаючи на те, що дана теза була сформульована ще наприкінці 1990-х років, вона не втратила своєї актуальності й сьогодні.

Історія криптографії демонструє, що алгоритми, які вважалися надійними та стійкими протягом десятиліть, з часом втрачали свою ефективність через зростання обчислювальних можливостей і появу нових методів атак. Те, що забезпечує належний рівень захисту сьогодні, у майбутньому може виявитися недостатнім, зокрема в умовах розвитку квантових обчислень, здатних поставити під загрозу значну частину сучасних криптографічних механізмів. Особливо актуальною ця проблема є для банківських мереж, у яких криптографічний захист є одним із ключових елементів забезпечення конфіденційності, цілісності та автентичності інформації.

Додатковим викликом для сучасних криптографічних систем є розвиток квантових обчислень. У 2024 році NIST фіналізував перші постквантові стандарти ML-KEM, ML-DSA та SLH-DSA (на основі CRYSTALS-Kyber, CRYSTALS-Dilithium і SPHINCS+), що підтверджує актуальність підготовки до майбутніх загроз для існуючих схем шифрування [2]. За таких умов особливої важливості набуває пошук підходів до поетапного підвищення стійкості криптографічного захисту, здатних забезпечити адаптацію банківських систем до сучасних та перспективних кіберзагроз.

У відповідь на ці загрози міжнародна банківська спільнота вже розпочала практичні кроки з впровадження постквантового захисту. Зокрема,

у 2023 році в рамках Project Leap, було створено квантово-безпечний канал зв'язку для тестових платежів із використанням квантового розподілу ключів [3]. JPMorgan Chase побудував квантово-захищену мережу Q-CAN на 100 Гбіт/с у Сінгапурі, продемонструвавши можливість інтеграції постквантової криптографії в існуючу інфраструктуру [4].

У зв’язку з цим актуальним науково-практичним завданням є розроблення підходів до поетапного підвищення стійкості криптографічного захисту, які дозволяють адаптувати існуючі системи безпеки до сучасних та перспективних загроз без необхідності їх повної заміни.

Метою дипломної роботи є підвищення стійкості криптографічного захисту інформації в банківських мережах шляхом інтеграції елементів завадостійкого кодування та постквантових криптографічних алгоритмів у складі існуючих схем шифрування.

Об'єктом дослідження є процес забезпечення криптографічного захисту інформації в телекомунікаційних мережах банківських установ в умовах зростання кіберзагроз і розвитку постквантових методів криптоаналізу.

Предметом дослідження є стійкість існуючих криптографічних схем захисту банківських мереж та властивості підходу до її підвищення шляхом інтеграції елементів завадостійкого кодування і постквантових алгоритмів.

Методи дослідження. Для вирішення поставлених завдань використано комплекс загальнонаукових і спеціальних методів дослідження, зокрема системний аналіз, порівняльний аналіз, методи аналітичної оцінки криптографічної стійкості, теорії ймовірностей та оцінювання обчислювальної складності алгоритмів. Системний аналіз застосовано для дослідження сучасних загроз інформаційній безпеці банківських мереж та визначення вимог до криптографічного захисту. Порівняльний аналіз використано для оцінювання характеристик симетричних, асиметричних і постквантових алгоритмів за критеріями стійкості та складності реалізації. Методи аналітичної оцінки криптографічної стійкості, теорії ймовірностей та

оцінювання обчислювальної складності застосовано для кількісного аналізу характеристик алгоритмів і дослідження ефективності запропонованого підходу.

У результаті дослідження проведено порівняльний аналіз сучасних криптографічних алгоритмів та визначено їх обмеження в умовах сучасних кіберзагроз. Обґрунтовано доцільність використання елементів завадостійкого кодування та постквантових алгоритмів як додаткових рівнів захисту. Запропонований підхід забезпечує підвищення стійкості криптографічних схем з урахуванням вимог безпеки, обчислювальної складності та адаптивності до перспективних кіберзагроз без необхідності повної заміни існуючої криптографічної інфраструктури.

Елементом новизни є запропонований підхід до підвищення стійкості криптографічного захисту в банківських мережах, який передбачає інтеграцію елементів завадостійкого кодування та постквантових криптографічних алгоритмів у складі існуючих схем шифрування незалежно від типу базового криптографічного алгоритму.

Практичне значення роботи полягає у можливості використання запропонованого підходу для поетапного підвищення рівня криптографічного захисту банківських телекомунікаційних систем шляхом впровадження додаткових рівнів захисту без необхідності повної заміни існуючих криптографічних засобів.

Дипломна робота має 84 сторінок тексту, 19 рисунків та 6 таблиць, а також використовує 57 літературних джерел.

РОЗДІЛ 1
ПРИНЦИПИ ПОБУДОВИ ТА ЗАХИСТУ МЕРЕЖ В БАНКІВСЬКИХ УСТАНОВАХ

Сучасний етап розвитку фінансового сектору України характеризується активною цифровізацією банківських послуг, впровадженням новітніх інформаційно-комунікаційних технологій та постійним зростанням обсягів електронних фінансових операцій.

За даними Національного банку України, у 2025 році частка безготівкових операцій у загальному обсязі карткових транзакцій досягла 95,5%, що становить понад 9 мільярдів операцій на суму 4,68 трильйона гривень [5]. Така концентрація фінансових процесів у цифровому середовищі висуває підвищені вимоги до надійності та захищеності банківських телекомунікаційних мереж.

Одночасно зі зростанням обсягів цифрових транзакцій підвищується інтенсивність кіберзагроз. За даними CERT-UA, у 2025 році кількість зареєстрованих кіберінцидентів зросла на 37,4% порівняно з попереднім роком, а фінансовий сектор залишається одним із пріоритетних об'єктів атак зловмисників [6].

За таких умов комп'ютерні мережі банківських установ стають критично важливими елементами інформаційної інфраструктури, компрометація яких може призвести до значних фінансових втрат, порушення безперервності банківських послуг та зниження довіри користувачів.

Забезпечення належного рівня захисту банківських інформаційно-комунікаційних систем є комплексним завданням, що охоплює нормативно-правові, організаційні, технічні та криптографічні аспекти безпеки. Тому для розуміння особливостей побудови криптографічного захисту в банківських мережах доцільно розглянути чинну нормативно-правову базу, основні

принципи організації захисту інформації та вимоги, що висуваються до сучасних банківських телекомунікаційних систем.

1.1 Нормативно-правова база забезпечення інформаційної безпеки банківських установ України

Нормативно-правова база головним чином включає закони України, постанови й положення НБУ, а також міжнародні стандарти, інтегровані у національне правове поле. Останні роки ознаменувалися суттєвим реформуванням цієї сфери, відбулися відмови від застарілих галузевих стандартів на користь динамічної системи регулювання, адаптованої до умов воєнного стану та європейського регламенту DORA [7]. Україна наразі активно імплементує ці норми в національне законодавство в межах євроінтеграційних зобов'язань, щоб синхронізувати український фінансовий ринок з європейським.

Наразі, фундамент правового регулювання становлять наступні базові закони України:

- **«Про Національний банк України»**, що визначає повноваження регулятора щодо встановлення обов'язкових вимог із захисту інформації [8];
- **«Про захист інформації в інформаційно-комунікаційних системах»,** який встановлює правові основи захисту державних та фінансових інформаційних ресурсів [9];
- **«Про основні засади забезпечення кібербезпеки України»** [10].

На виконання цих законів НБУ розробив та впровадив тріаду ключових нормативно-правових актів, які безпосередньо регламентують принципи функціонування мереж сучасних банків:

1. Постанова Правління НБУ №95 від 28.09.2017, яка затвердила «Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» [11]. Цей документ є фундаментальним

наступником скасованої Постанови №474. Він визначає обов'язкові мінімальні вимоги до архітектури мереж, системи криптографічного захисту, автентифікації користувачів, а також зобов'язує банки впроваджувати ризик-орієнтований підхід під час проєктування інформаційних систем.

2. Постанова Правління НБУ №178 від 12.08.2022, якою введено в дію «Положення про організацію кіберзахисту в банківській системі України» [12]. Документ з'явився як відповідь на виклики повномасштабної війни та фокусується на забезпеченні безперервності бізнесу фінансових установ. Постанова №178 висуває жорсткі технічні вимоги до захисту об'єктів критичної інформаційної інфраструктури банків, регламентує правила резервного копіювання даних, сегментації корпоративних мереж, а також взаємодії банків із Центром кіберзахисту НБУ.

3. Постанова Правління НБУ №143 від 09.12.2025, яка затвердила «Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг» [13]. Цей документ закріпив підхід «cyber compliance by design» (безпека на етапі проєктування). Постанова уніфікувала вимоги кібербезпеки для всього фінансового ринку, поширивши суворі стандарти захисту банківського рівня на небанківський сектор, як страхові компанії, кредитні спілки тощо.

Окрім національних положень, банки також спираються на міжнародну серію стандартів ISO/IEC 27001 [14] та ISO/IEC 27002 [15], які визначають найкращі світові практики побудови систем управління інформаційною безпекою.

Така гармонізована нормативна база створює чіткий правовий фундамент для захисту банківських мереж і безпосередньо визначає загальні принципи організації захисту інформації в установах.

1.2 Загальні принципи організації захисту інформації в банківських установах

Система захисту банківської установи є багаторівневою і охоплює взаємопов'язані фізичні, організаційні, технічні та криптографічні заходи. Для мінімізації як зовнішніх, так і внутрішніх ризиків безпека інформаційних технологій реалізується через ефективне управління процесами, дотримання нормативних вимог та забезпечення безперервності діяльності банку. Фундаментом для побудови такої системи є класична тріада інформаційної безпеки [16], яка визначає три ключові цілі захисту фінансових даних: конфіденційність банківської таємниці, цілісність транзакцій та постійну доступність сервісів для клієнтів (рис. 1.1) [17].

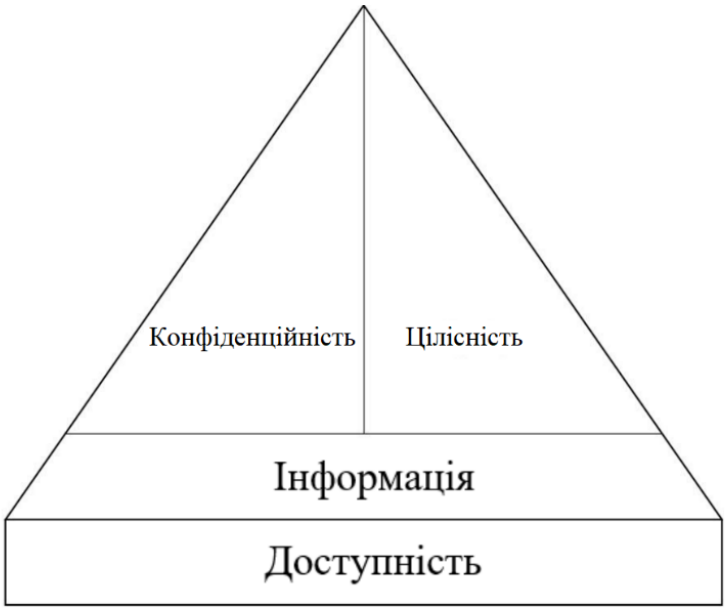

Рисунок 1.1 – Модифікована тріада CIA

Сучасні положення Національного банку України вимагають від фінансових установ відмови від формального підходу до безпеки та практичного забезпечення зазначених цілей. Відповідно до чинних регуляторних вимог, побудова стійких мереж передбачає обов'язкове впровадження комплексу різнохарактерних заходів, які детально розглядаються через призму конкретних видів захисту.

1.2.1 Фізичний захист об'єктів банківської інфраструктури

Фізичний захист є першим і базовим рівнем системи безпеки банківської установи, що забезпечує унеможливлення несанкціонованого фізичного доступу до інформаційних ресурсів та телекомунікаційної інфраструктури. Основним завданням фізичного захисту банку є запобігання та протидія загрозам фізичного характеру. Такі загрози створюють пряму небезпеку для життя людей, цілісності майна та стабільної роботи фінансової установи.

У системі безпеки банківської діяльності фізичні загрози поділяють на такі категорії:

- **Посягання на життя та свободу людей:** викрадення (або загрози викрадення) співробітників банку, членів їхніх сімей та близьких родичів, а також умисні вбивства, що супроводжуються насильством або катуванням.
- **Розбійні напади та грабежі:** силові напади на відділення чи інкасаторів з метою протиправного заволодіння грошовими коштами, цінностями та конфіденційними документами.
- **Нищення матеріальних активів:** умисне пошкодження або знищення рухомого й нерухомого майна банку, а також особистої власності його працівників.
- **Терористичні акти:** скоєння злочинів у формі вибухів, підпалів, застосування або загрози застосування вибухових пристроїв, хімічних, біологічних чи отруйних речовин.
- **Захоплення заручників та об'єктів:** незаконне утримання людей, а також захоплення чи блокування адміністративних будівель і транспортних засобів банку [18].

Протидія цим ризикам вимагає комплексного підходу, що поєднує роботу фізичної охорони, використання технічних засобів безпеки та чітке дотримання персоналом інструкцій.

Периметральний захист забезпечує контроль навколо серверних приміщень, центрів обробки даних та телекомунікаційних вузлів банку. Він поєднує капітальні інженерні бар'єри та цілодобове відеоспостереження з обов'язковим збереженням відеоархіву.

Контроль доступу до приміщень реалізується через системи контролю та управління доступом із багатофакторною автентифікацією за допомогою карток, PIN-кодів та біометрії. Серверні кімнати належать до зон обмеженого доступу, де кожне переміщення персоналу автоматично фіксується в електронних журналах.

Стабільність інфраструктури підтримують системи охоронної, пожежної та тривожної сигналізації, підключені через захищені кабельні мережі та шлейфи. Для запобігання знеструмленню обладнання впроваджуються системи безперебійного живлення, а координація охорони здійснюється через оперативний зв'язок.

З погляду розміщення апаратного забезпечення, окремим елементом захисту є організація DMZ [19]. Вона реалізується як фізично ізольований сегмент мережі або окремий майданчик для розміщення публічних сервісів, таких як веб-портали, поштові шлюзи та API-інтерфейси [19, 20]. Таке архітектурне рішення забезпечує відокремлення ресурсів, доступних з мережі Інтернет, від критичних компонентів внутрішньої банківської інфраструктури та автоматизованої банківської системи [19–21]. Структуру цієї зони продемонстровано на схемі (рис. 1.2).

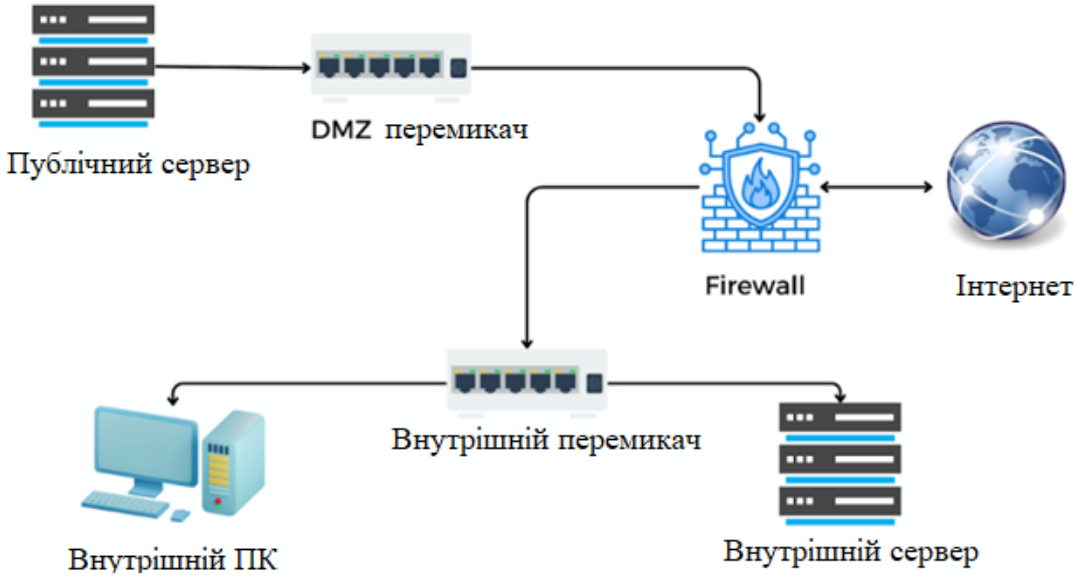

Рисунок 1.2 – Структура DMZ

1.2.2 Організаційні заходи забезпечення інформаційної безпеки

Згідно зі стандартом ISO/IEC 27001 [14], реалізація організаційних заходів інформаційної безпеки банків передбачає розроблення комплексної політики Системи управління інформаційною безпекою [22], чіткий розподіл ролей та обов'язків, а також проведення регулярного внутрішнього аудиту. Практичне впровадження цих вимог включає створення регламентів роботи з конфіденційною інформацією, процедур реагування на інциденти та планів забезпечення безперервності бізнесу.

Організаційне регулювання повсякденної діяльності установи базується на суворому контролі процедур надання доступу до банківських мереж, де права кожного користувача обмежуються виключно його посадовими обов'язками за принципом мінімальних привілеїв. Іншим критично важливим процесом є систематичне ознайомлення персоналу з вимогами безпеки через регулярне навчання та інструктажі. Оскільки людський фактор залишається одним із ключових методів компрометації систем, підвищення обізнаності працівників виступає головним

інструментом протидії внутрішнім загрозам – як навмисним зловживанням, так і випадковим технологічним помилкам співробітників [23].

Відповідно, у структурі банку обов'язково передбачаються посади відповідальних працівників з інформаційної безпеки та адміністрування засобів захисту. До їхніх безпосередніх обов'язків належить постійний моніторинг дій персоналу та аналіз потенційних вразливостей інформаційних систем.

1.2.3 Технічні засоби захисту в банківських мережах

Відповідно до нормативних документів у сфері технічного захисту інформації, захист інформаційних ресурсів передбачає реалізацію комплексу програмних, апаратних та організаційних заходів, спрямованих на запобігання несанкціонованому доступу до інформації та порушенню штатного режиму функціонування інформаційних систем [24].

Технічні заходи передбачають розгортання комплексу програмних та апаратних засобів для захисту кінцевих точок, серверів та інформаційних ресурсів банку (рис. 1.3). Головною метою цих засобів є недопущення несанкціонованого керування вузлами системи та запобігання внутрішнім компрометаціям [25].

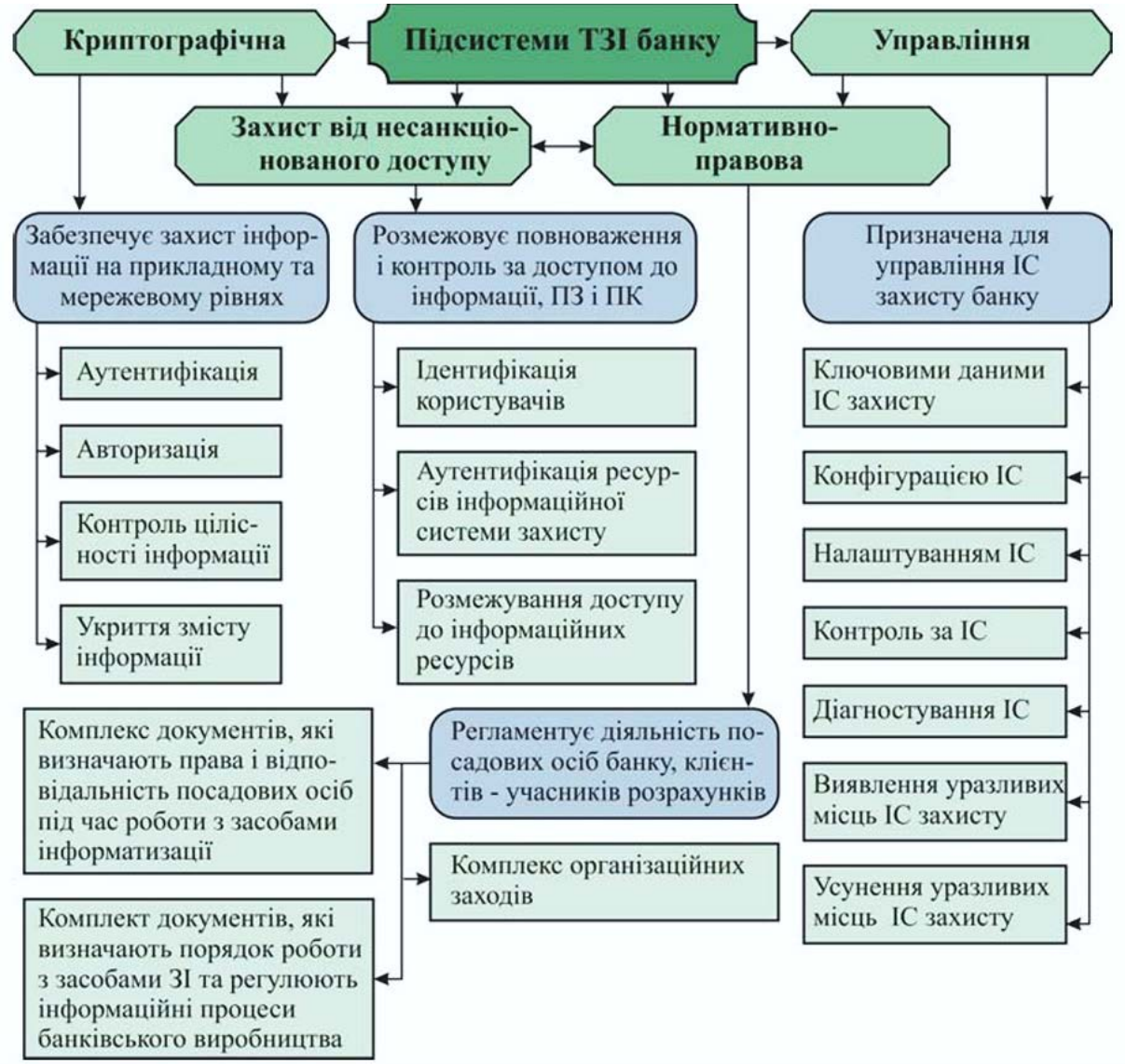

Рисунок 1.3 – Структура системи технічного захисту інформації банку

Базовим рівнем технічного захисту є використання антивірусних комплексів корпоративного класу та систем виявлення і реагування на кінцевих точках, які блокують шкідливе програмне забезпечення та аналізують поведінку процесів у реальному часі. Для ідентифікації користувачів впроваджуються системи MFA (рис. 1.4), які значно знижують ризик компрометації облікових записів навіть у випадку викрадення паролів [26].

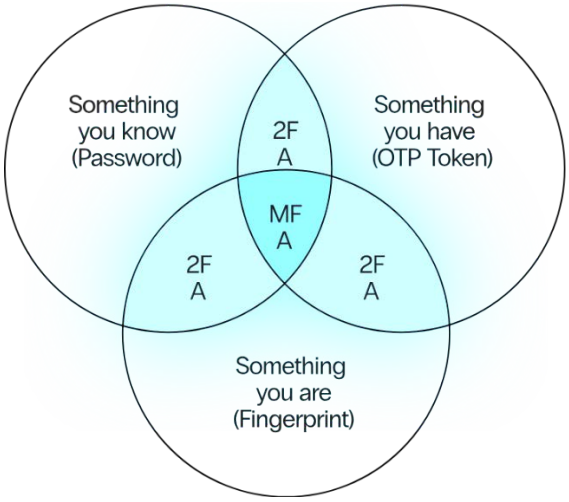

Рисунок 1.4 – Фактори MFA

Захист банківської таємниці та конфіденційних даних від внутрішніх витоків забезпечують системи запобігання витоку інформації [15], які контролюють рух документів через корпоративну пошту, зовнішні носії та хмарні сервіси. Усі події безпеки, що генеруються цими засобами, централізовано збираються та аналізуються системами управління інформацією та подіями безпеки, що дозволяє адміністраторам оперативно виявляти аномалії згідно з регламентами.

1.2.4 Безпека банківських комп'ютерних мереж та каналів передачі даних

Банківська комп'ютерна мережа є складною телекомунікаційною системою, що об'єднує центральний офіс, філії, банкомати, термінали самообслуговування та зовнішні платіжні системи. Захист каналів передачі даних є критично важливим завданням, оскільки перехоплення або модифікація фінансових транзакцій у каналі може призвести до значних фінансових та репутаційних втрат.

Для захисту каналів передачі даних застосовуються VPN на основі протоколу IPSec, що забезпечують конфіденційність та цілісність трафіку

між вузлами банківської мережі. Протокол TLS використовується для захисту з'єднань між клієнтами та банківськими веб-сервісами. Архітектура AAA на основі протоколу Kerberos забезпечує централізовану автентифікацію та авторизацію користувачів у межах банківської мережі.

Сегментація мережі на ізольовані VLAN-зони (рис. 1.5) дозволяє обмежити поширення атаки у разі компрометації одного із сегментів та мінімізувати поверхню атаки на критичні банківські системи [27].

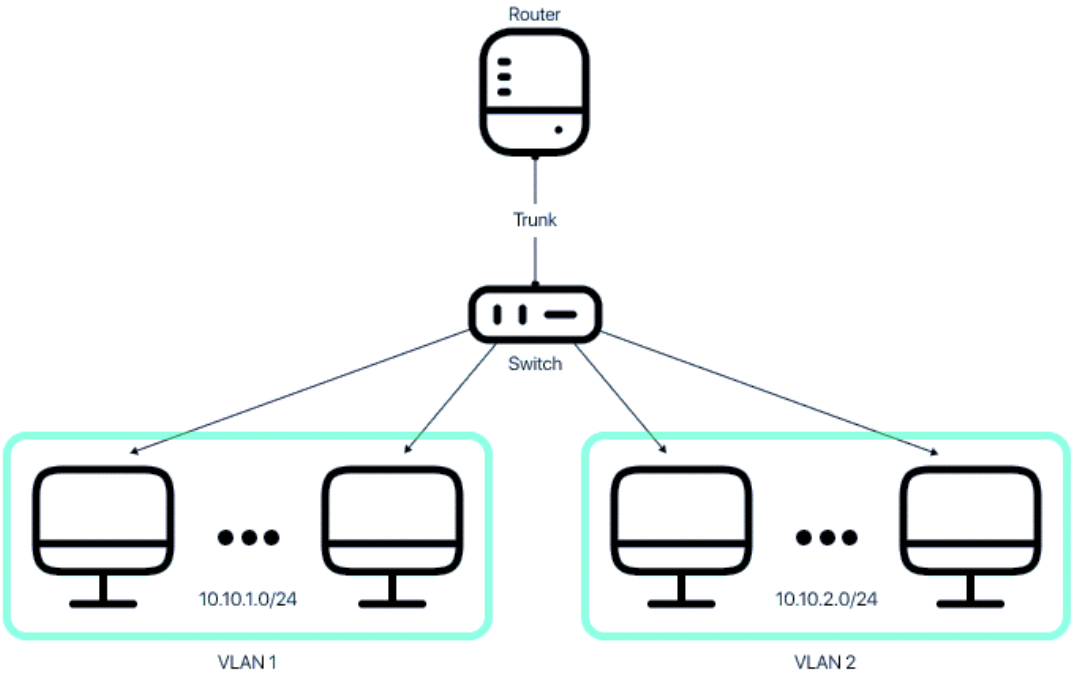

Рисунок 1.5 – Приклад VLAN

1.2.5 Криптографічні засоби захисту інформації

Криптографічні методи захисту інформації – це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. Криптографічний метод захисту є найнадійнішим методом захисту, оскільки охороняється безпосередньо сама інформація, а не доступ до неї.

У банківських системах криптографічні засоби застосовуються для забезпечення трьох ключових властивостей інформаційної безпеки:

конфіденційності, цілісності та автентичності даних. Симетричні алгоритми шифрування використовуються для захисту масивів даних та транзакційного трафіку, асиметричні – для захищеного обміну ключами та формування цифрового підпису.

Національний банк України застосовує апаратно-програмні засоби криптографічного захисту інформації, зокрема модулі генерації ключів, призначені для генерації ключових пар у складі програмно-апаратних комплексів банків [28]. HSM забезпечують захищене зберігання та використання криптографічних ключів і є обов'язковим елементом PKI банківських установ.

Організаційні, технічні та криптографічні заходи утворюють єдину систему захисту інформації в платіжній системі, вимоги до якої встановлені законодавством України.

1.3 Вимоги до криптографічного захисту в банківських системах

В умовах функціонування сучасних розподілених інформаційно-комунікаційних мереж фінансових установ КЗІ виступає базовим та найбільш надійним інструментом забезпечення конфіденційності, цілісності, автентичності та неспростовності даних, що циркулюють у банківських телекомунікаційних системах. Специфіка захисту банківського трафіку полягає в необхідності протидії широкому спектру кіберзагроз – від перехоплення пакетів даних та модифікації фінансових повідомлень під час їх транзиту («людина посередині» або MitM-атаки) до спроб несанкціонованого доступу до технологічних сегментів мережі.

Теоретико-методологічний базис та практична реалізація підсистем КЗІ в банківському секторі України чітко регламентуються нормативно-правовими актами Національного банку України, державними стандартами, а також вимогами адміністрації ДССЗЗІ. Відповідно до базових вимог чинного

регулятора, зокрема Постанови Правління НБУ №95 [11], будь-яка банківська телекомунікаційна система, яка здійснює обробку, збереження або передачу конфіденційної інформації та банківської таємниці, повинна використовувати засоби КЗІ, що мають чинний експертний висновок за результатами державної експертизи у сфері КЗІ.

Система криптографічного захисту банківських телекомунікацій базується на поєднанні двох основних технологічних підходів: симетричного шифрування та асиметричного шифрування (PKI).

Перший застосовується для високошвидкісного захисту великих масивів інформації, а саме канального та пакетного шифрування трафіку. Фінансові установи зобов'язані використовувати стійкі алгоритми, сертифіковані на національному рівні або визнані міжнародні стандарти для організації VPN між Головним офісом, резервними дата-центрами та мережею філій.

Другий інтегрується в телекомунікаційні системи для забезпечення процедур суворої автентифікації користувачів та мережевих вузлів, розподілу ключів шифрування, а також генерації та перевірки кваліфікованого електронного підпису. НБУ висуває жорсткі вимоги до стійкості асиметричних алгоритмів, що мінімізує ризики компрометації ключів шляхом математичного підбору чи факторизації.

Організація криптографічного захисту безпосередньо на рівні мережевої архітектури банку передбачає обов'язкове виконання низки архітектурних та експлуатаційних вимог:

- **End-to-End Encryption**. Увесь платіжний трафік, інформація про стан рахунків клієнтів та операційні дані повинні шифруватися безпосередньо на кінцевому терміналі (клієнтському або внутрішньобанківському) перед відправленням у мережевий канал та дешифруватися виключно на легітимному вузлі-одержувачі. Проходження відкритого банківського трафіку через проміжні телекомунікаційні вузли чи маршрутизатори загального користування категорично заборонено;

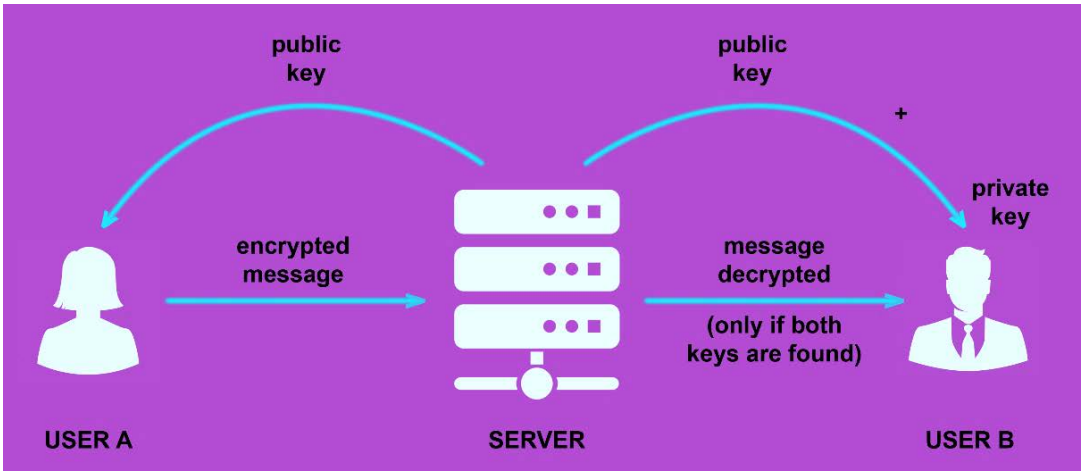

Рисунок 1.6 – Схема архітектури E2EE

- **Захист мережевих протоколів адміністрування**. Доступ інженерно-технічного персоналу до налаштування мережевого обладнання, як маршрутизатори, комутатори, міжмережеві екрани, має здійснюватися виключно за допомогою криптографічно захищених протоколів (SSH версії 2, TLS 1.3, HTTPS) [29]. Використання незахищених протоколів у банківських телекомунікаційних системах розцінюється як критична вразливість;
- **Строгий життєвий цикл криптографічних ключів**. Ключова система є найбільш уразливим елементом КЗІ. Регуляторні вимоги НБУ зобов'язують банки забезпечити повну автоматизацію процесів генерації, розподілу, ротації, резервування та гарантованого знищення криптографічних ключів. Для генерації та зберігання майстер-ключів та ключів вищого рівня банки повинні розгортати спеціалізовані HSM, що мають фізичний захист від розкриття.

Окремим важливим аспектом є забезпечення стійкості КЗІ в умовах розвитку хмарних технологій та віддаленого доступу співробітників банку. При побудові криптографічного захисту для віддалених підключень телекомунікаційна система банку повинна функціонувати відповідно до концепції Zero Trust, за якою жоден користувач або пристрій не вважається довіреним за замовчуванням незалежно від його розташування у мережі [30].

Це передбачає обов'язкове використання двосторонньої автентифікації (Mutual TLS / mTLS) та створення ізольованих криптографічних тунелів окремо для кожного сеансу зв'язку з обов'язковим динамічним контролем цілісності кінцевої робочої станції.

1.4 Висновки до першого розділу

Отже, вимоги до криптографічного захисту в банківських телекомунікаційних системах України формуються на перетині нормативно-правових, технічних та організаційних чинників. Застосування сертифікованих алгоритмів шифрування, апаратних засобів захисту ключової інформації та механізмів наскрізного шифрування створює необхідне підґрунтя для зниження ризиків витоку даних і забезпечення належного рівня стійкості мережевої інфраструктури банківської установи до актуальних кіберзагроз.

Проведений огляд законодавчо-нормативної бази дозволяє сформувати цілісне уявлення про обов'язкові та рекомендовані вимоги до криптографічного захисту в банківському секторі. Отримані результати враховано в подальших частинах роботи під час аналізу алгоритмів шифрування та розробки підходу до підвищення стійкості криптографічного захисту.

РОЗДІЛ 2
ОГЛЯД ІСНУЮЧИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ТА МЕТОДІВ АТАК

Побудова ефективної системи криптографічного захисту банківських мереж потребує ґрунтовного знання як наявних загроз, так і доступних інструментів протидії. Перш ніж перейти до вибору конкретних алгоритмів шифрування для практичного застосування, необхідне розуміння, яким чином зловмисники можуть атакувати, за якими критеріями оцінюється стійкість криптографічних механізмів та які саме алгоритми сьогодні формують арсенал засобів захисту інформації.

В цьому розділі здійснюється огляд основних класів атак на криптографічні системи, визначення кількісних критеріїв оцінки стійкості та огляд принципів побудови сучасних алгоритмів шифрування. Отримані теоретичні відомості стануть фундаментом для проведення подальшого порівняльного аналізу.

2.1 Класифікація та аналіз класичних атак на криптографічні алгоритми і канали передачі даних

Атаки на криптографічні алгоритми та захищені канали передачі даних доцільно класифікувати за декількома незалежними критеріями, кожен з яких відображає окремий аспект загрози. Розгляд атак доцільно зробити із трьох позицій: з боку атакованої системи, з боку зловмисника та з боку спостерігача [1].

З позиції атакованої системи атаки класифікуються за типом використовуваної вразливості. Найбільш поширеними категоріями є:

- Атаки на реалізацію криптографічних алгоритмів (side-channel attacks), які експлуатують фізичні витоки інформації під час виконання обчислень – час виконання операцій, енергоспоживання,

електромагнітне випромінювання – і дозволяють відновити секретний ключ без математичного зламу алгоритму;

- Атаки на протоколи обміну, зокрема атака «людина посередині» (Man-in-the-Middle), коли зловмисник непомітно вклинюється в комунікацію між двома сторонами та перехоплює або модифікує повідомлення;
- Математичні атаки, спрямовані на використання структурних особливостей шифру – диференціальний та лінійний криптоаналіз, атаки на основі підібраного відкритого тексту або шифротексту.

З позиції зловмисника атаки класифікуються за кінцевою метою, що визначає характер загрози для банківської установи. Виділяють такі основні цілі:

- Порушення доступності, зокрема відмова в обслуговуванні (Denial-of-Service, DoS), коли зловмисник перевантажує сервер або канал зв'язку, унеможливлюючи обробку легітимних транзакцій;
- Порушення конфіденційності – копіювання інформації, що передається, включаючи реквізити платежів, персональні дані клієнтів та сеансові ключі; особливу небезпеку становить модель «harvest now, decrypt later», за якої перехоплені дані зберігаються до появи потужніших обчислювальних засобів;
- Порушення цілісності та автентичності – підміна платіжних доручень або модифікація сум транзакцій під час передачі;
- Отримання прав суперкористувача в системі, що надає зловмиснику повний контроль над банківським сервером і можливість відключити або скомпрометувати всі механізми захисту.

З позиції спостерігача атаки класифікуються за ознаками, що дозволяють виявити факт вторгнення. До таких індикаторів належать:

- Аномалії в журналах реєстрації подій: нехарактерна кількість невдалих спроб автентифікації, спроби доступу в неробочий час, звернення до нестандартних портів або служб;

- Мережеві аномалії: різке зростання обсягу трафіку, поява пакетів із некоректними контрольними сумами, численні спроби підключення до закритих портів;
- Ознаки атак повторного відтворення (replay attack) – дублювання ідентифікаторів сеансів або часових міток у перехоплених пакетах.

Отже, комплексна класифікація атак формує основу для розробки системи захисту банківських мереж, де кожен рівень протидіє загрозам певного типу. При цьому слід враховувати, що реальний зловмисник рідко обмежується одним вектором атаки, натомість застосовує комбіновані методи, експлуатуючи найслабшу ланку системи.

2.2 Характеристики та оцінка криптографічної стійкості алгоритмів

Об'єктивне порівняння криптографічних алгоритмів неможливе без формалізованих критеріїв, які дозволяють кількісно оцінити їхню стійкість, продуктивність та надійність. У даному підрозділі наведено основні розрахункові співвідношення, що використовуються в роботі для оцінювання алгоритмів симетричного шифрування, асиметричних схем та механізмів забезпечення цілісності даних.

Час зламу методом грубої сили. Одним із фундаментальних показників криптографічної стійкості є прогнозований час, необхідний зловмиснику для повного перебору всіх можливих варіантів ключа. Цей показник розраховується за формулою:

$$t_б = \frac{N_B}{\gamma \cdot K} \cdot P_T,$$

де $N_в$ – загальна кількість варіантів ключа (простір ключів), яка для алгоритму з довжиною ключа n біт становить $2n$; γ – продуктивність криптографічної системи зловмисника, що вимірюється в операціях за секунду (для сучасних високопродуктивних обчислювальних кластерів

приймається γ= 10^{10}опер/с); $K = 3{,}1 \cdot 10^7$ – кількість секунд в одному році, яка використовується для переведення результату в роки; P_T – ймовірність, з якою необхідно виконати криптоаналіз (зазвичай приймається $P_T = 1$ для гарантованого зламу або $P_T = 0{,}5$ для оцінки середнього часу).

Практичне застосування цієї формули дозволяє оцінити, наприклад, що для алгоритму DES із 56-бітним ключем ($N_в = 256 \approx 7{,}2 \cdot 1016$ $N_в = 256 \approx 7{,}2 \cdot 1016$) час зламу при $P_T = 1$ становить:

$$t_б = \frac{2^{56}}{10^{10} \cdot 3{,}1 \cdot 10^7} \approx 0{,}23 \text{ року},$$

тобто менше трьох місяців. Натомість для AES-256 ($N_в = 2^{256} \approx 1{,}16 \cdot 10^{77}$) аналогічний розрахунок дає $t_б \approx 3{,}7 \cdot 10^{59}$ років, що на багато порядків перевищує вік Всесвіту. Такі обчислення є основою для віднесення алгоритмів до категорій «застарілий» або «актуальний» у порівняльних таблицях.

Робоча характеристика криптографічної стійкості. Для комплексної оцінки стійкості, яка враховує не лише довжину ключа, а й статистичні властивості джерела ключів та особливості захищеного тексту, використовується робоча характеристика l0*l*0, що обчислюється за формулою:

$$l_0 = \frac{H(K)}{\chi},$$

де *H(K)* – ентропія джерела ключів, яка для ідеального випадкового джерела збігається з довжиною ключа в бітах; χ – надмірність тексту, що характеризує ступінь передбачуваності символів у повідомленні (для природних мов значення χ лежить у межах від 0,2 до 0,5, для зашифрованих даних наближається до 1).

Фізичний зміст показника l_0 полягає в тому, що він визначає мінімальну складність успішної атаки в бітах. Наприклад, для алгоритму Rijndael-256 при *H(K)* = 256 біт та $\chi = 0{,}45$ робоча характеристика становить l_0 == 256/0,45 ≈ 568 біт. Цей показник є більш інформативним, ніж

проста довжина ключа, оскільки враховує реальні умови експлуатації криптографічної системи.

Імовірність обману для алгоритмів забезпечення цілісності. Для оцінки надійності алгоритмів цифрового підпису та хеш-функцій застосовується показник імовірності обману $P_{\text{обм}}$, який визначає ймовірність того, що зловмисник зможе підібрати інше повідомлення з тим самим значенням хеш-функції (створити колізію). Розрахунок виконується за формулою:

$$P_{\text{обм}} = 2^{lm}/2^{lm+ls},$$

де l_m – довжина повідомлення в бітах; l_s – довжина підпису (хеш-значення) в бітах. Після спрощення вираз зводиться до:

$$P_{обм} = 1/2^{ls}.$$

Таким чином, імовірність обману обернено пропорційна до потужності простору можливих хеш-значень. Для алгоритму SHA-1 із довжиною хешу 160 біт маємо $P_{\text{обм}} = 2^{-160} \approx 6{,}8 \cdot 10^{-49}$. Для вітчизняного стандарту «Калина» в режимі MAC із довжиною хешу 256 біт цей показник становить $P_{обм} = 2^{-256} \approx 10^{-78}$, що на десятки порядків краще. Ці значення використовуються в таблиці 3.3 для порівняння алгоритмів забезпечення цілісності.

Обчислювальна складність реалізації. Окрім суто криптографічних показників, важливим критерієм вибору алгоритму є його обчислювальна складність, яка визначає кількість елементарних операцій, необхідних для обробки одного блоку даних. Цей показник безпосередньо впливає на продуктивність системи в цілому. Для різних алгоритмів складність може відрізнятися на порядки, при виборі алгоритму для банківських систем необхідно знаходити компроміс між стійкістю та складністю, оскільки надмірна ресурсоємність може призвести до неприйнятних затримок при обробці фінансових транзакцій у реальному часі.

Узагальнюючи, можна зробити висновок, що система з чотирьох кількісних показників – часу зламу грубою силою $t_б$, робочої характеристики стійкості l_0, імовірності обману $P_{обм}$ та обчислювальної складності реалізації

– створює достатню базу для об'єктивного порівняльного аналізу криптографічних алгоритмів, який буде проведено згодом в роботі.

Застосування цих показників дозволяє уникнути суб'єктивних суджень і оперувати точними кількісними оцінками, що є необхідною умовою для прийняття обґрунтованих рішень у сфері захисту банківських мереж.

2.3 Симетричні алгоритми шифрування

Симетричні алгоритми шифрування становлять значну частку криптографічного захисту інформації в сучасних телекомунікаційних системах завдяки поєднанню високої швидкодії та надійності [31]. Їхній фундаментальний принцип полягає у використанні одного й того самого секретного ключа як для шифрування, так і для розшифрування даних. За способом обробки інформації симетричні шифри поділяються на блокові, що оперують фіксованими блоками даних, і потокові, які обробляють дані побитово або побайтово. У банківських мережах найбільшого поширення набули блокові шифри, оскільки вони забезпечують високий рівень криптографічної стійкості, ефективно підтримують захист великих обсягів транзакційних даних та широко інтегровані у сучасні протоколи безпечного обміну інформацією [32, 33].

Більшість сучасних блокових шифрів будуються на основі двох архітектурних підходів: збалансованої мережі Фейстеля та SP-мережі [34]. У мережі Фейстеля блок даних ділиться на дві половини, після чого виконується серія раундів, у кожному з яких одна половина модифікується за допомогою функції від іншої половини та раундового ключа. Така структура є оборотною навіть тоді, коли сама функція необоротна, що спрощує реалізацію. За цим принципом побудовано алгоритми DES, ГОСТ 28147-89, Blowfish та Twofish. SP-мережа передбачає чергування шарів підстановки (S-блоків) і перестановки, що забезпечує швидке розсіювання та перемішування бітів. Цей підхід використовується в алгоритмах Rijndael (AES) та «Калина»,

які демонструють високу продуктивність як на програмному, так і на апаратному рівні.

Алгоритм DES (рис. 2.1), прийнятий як федеральний стандарт США у 1977 році, став першим широко розповсюдженим симетричним шифром.

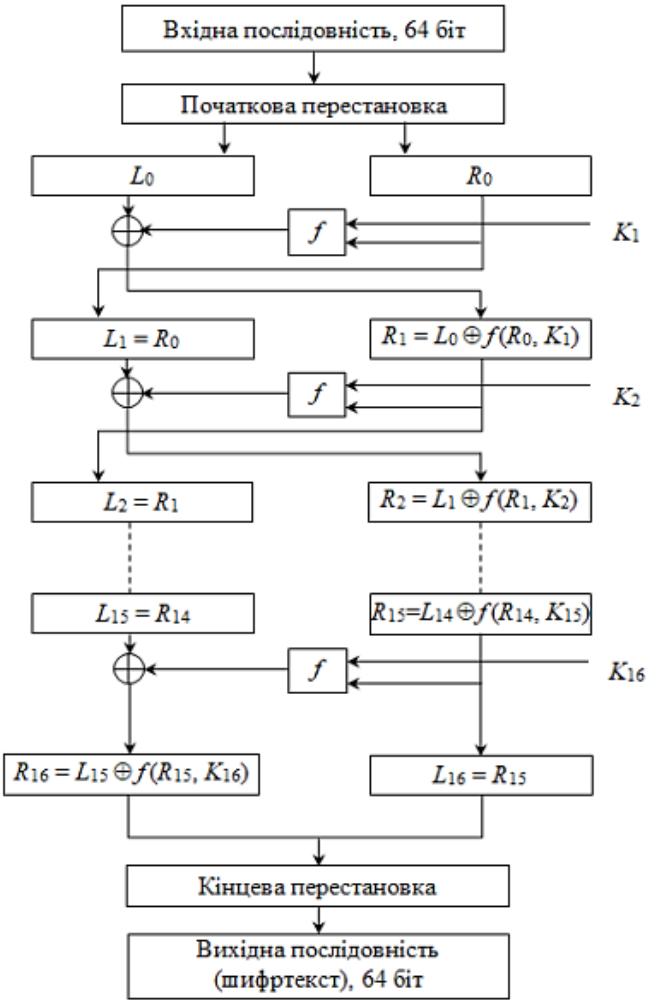

Рисунок 2.1 – Схема алгоритму DES

Він оперує 64-бітними блоками даних і використовує 56-бітний ключ. Структура DES базується на збалансованій мережі Фейстеля з 16 раундами перетворень. Основним недоліком алгоритму є мала довжина ключа, що робить його вразливим до атак повного перебору: вже на початку 2000-х років демонструвався злам DES менш ніж за 24 години. Для подолання цього обмеження було розроблено варіант 3DES (Triple DES), який тричі застосовує операцію DES із двома або трьома різними ключами, що збільшує

ефективну довжину ключа до 112 або 168 біт. Однак потрійне виконання призводить до значного зниження продуктивності, а розмір блоку залишається 64 біти, що вже не відповідає сучасним вимогам безпеки при великих обсягах даних.

Алгоритм IDEA (рис. 2.2) (International Data Encryption Algorithm), розроблений у 1991 році, став одним із перших шифрів, які запропонували 128-бітний ключ. Він оперує 64-бітними блоками та виконує 8 раундів перетворень, використовуючи операції додавання, множення та XOR у різних алгебраїчних групах. Цей підхід забезпечує високий рівень захисту від диференціального криптоаналізу. IDEA тривалий час використовувався в протоколах електронної пошти та VPN, однак через обмеження розміру блоку та патентні обмеження поступився більш сучасним рішенням.

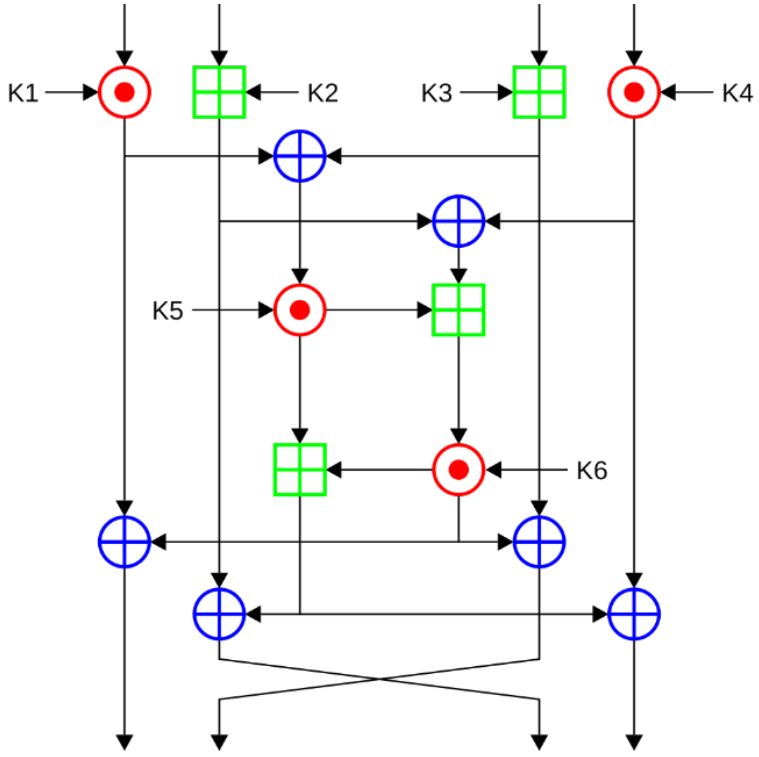

Рисунок 2.2 – Схема алгоритму IDEA

Алгоритм Rijndael (рис. 2.3), розроблений у 2001 році був прийнятий NIST як стандарт AES. Це блоковий шифр із SP-мережевою архітектурою, який підтримує довжину ключа 128, 192 або 256 біт при фіксованому розмірі блоку 128 біт. Кількість раундів залежить від довжини ключа: 10 для 128-

бітного, 12 для 192-бітного, 14 для 256-бітного. Кожен раунд складається з чотирьох операцій: підстановка байтів (SubBytes), зсув рядків (ShiftRows), перемішування стовпців (MixColumns) і додавання раундового ключа (AddRoundKey). Завдяки ефективній реалізації на різноманітних платформах та апаратній підтримці через інструкції AES-NI, Rijndael став де-факто стандартом для захисту банківських транзакцій у всьому світі.

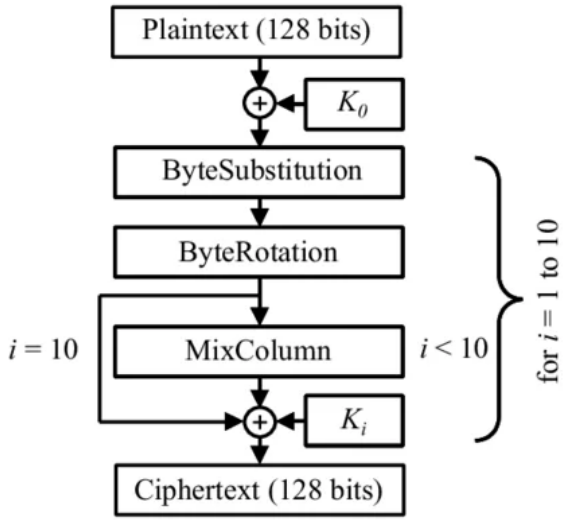

Рисунок 2.3 – Структура алгоритму шифрування Rijndael

Алгоритм RC6 (рис. 2.4), був розроблений у 1998 році, він успадкував архітектуру RC5, але зі збільшеним розміром блоку до 128 біт і підтримкою ключів до 256 біт. RC6 використовує мережу Фейстеля з 20 раундами, в яких активно застосовуються циклічні зсуви, залежні від даних, що ускладнює криптоаналіз. RC6 певний час використовувався в комерційних продуктах, хоча згодом був визнаний застарілим через виявлені структурні вразливості.

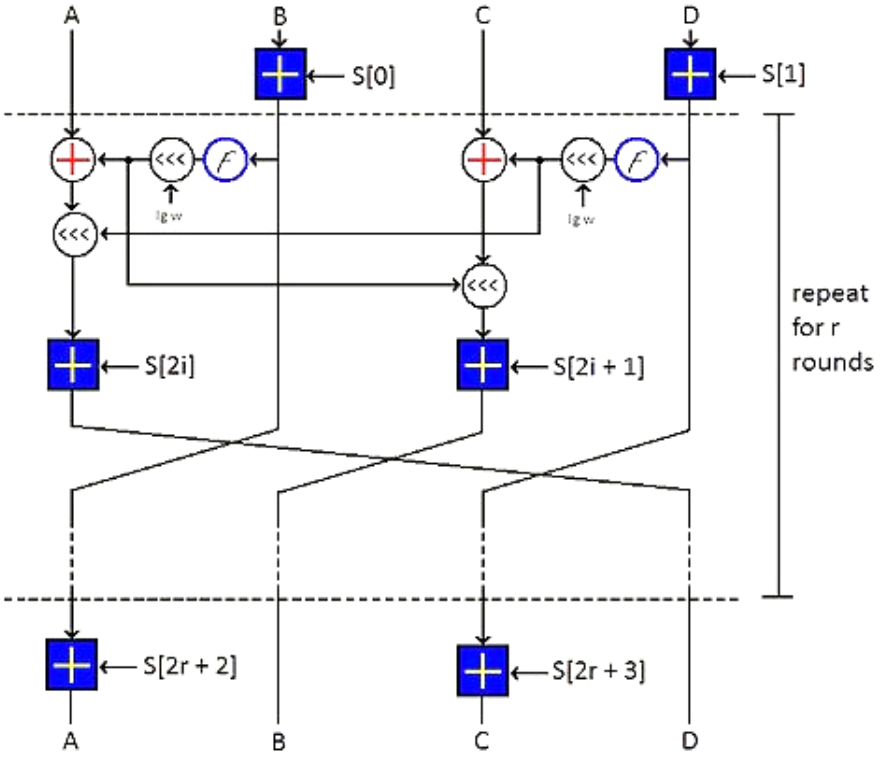

Рисунок 2.4 – Схема алгоритму RC6

Алгоритм Blowfish (рис. 2.5), створений у 1993 році, є блоковим шифром із мережею Фейстеля, який оперує 64-бітними блоками та підтримує ключі змінної довжини від 32 до 448 біт. Особливістю Blowfish є використання ключезалежних S-блоків, які генеруються динамічно на основі секретного ключа. Кількість раундів становить 16. Завдяки вільній ліцензії та простоті реалізації Blowfish набув значного поширення, однак розмір блоку 64 біти та відомі атаки на скорочену версію обмежують його застосування в сучасних системах.

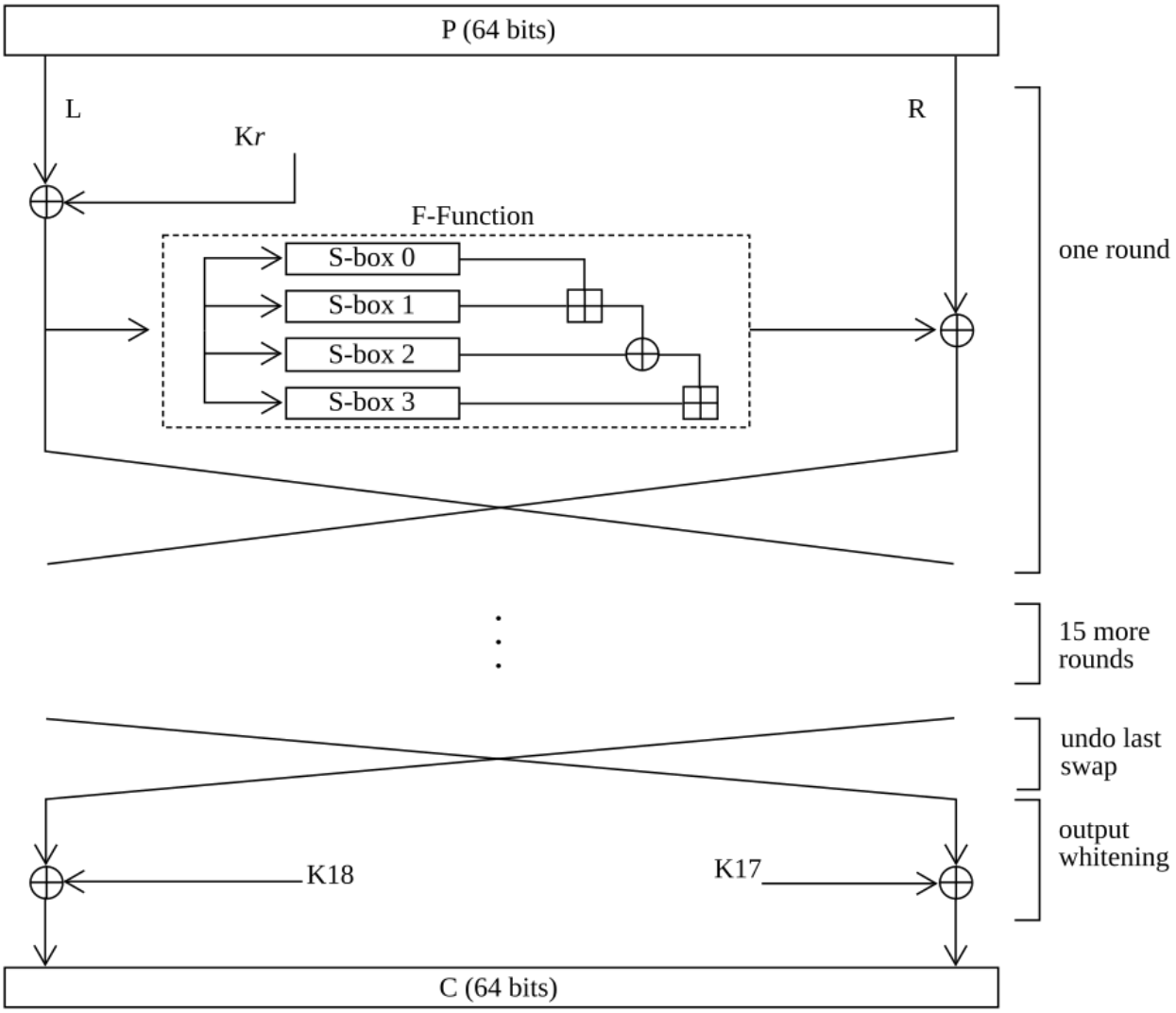

Рисунок 2.5 – Діаграма алгоритму Blowfish

Алгоритм Twofish (рис. 2.6), розроблений у 1998 році і став одним із фіналістів конкурсу AES. Він оперує 128-бітними блоками, підтримує ключі довжиною 128, 192 або 256 біт і виконує 16 раундів. Архітектура Twofish є модифікованою мережею Фейстеля з використанням ключезалежних S-блоків та операції множення в полі Галуа. Порівняно з Blowfish, Twofish забезпечує кращу продуктивність на сучасних процесорах і вищий рівень стійкості, однак не набув такого широкого поширення, як AES.

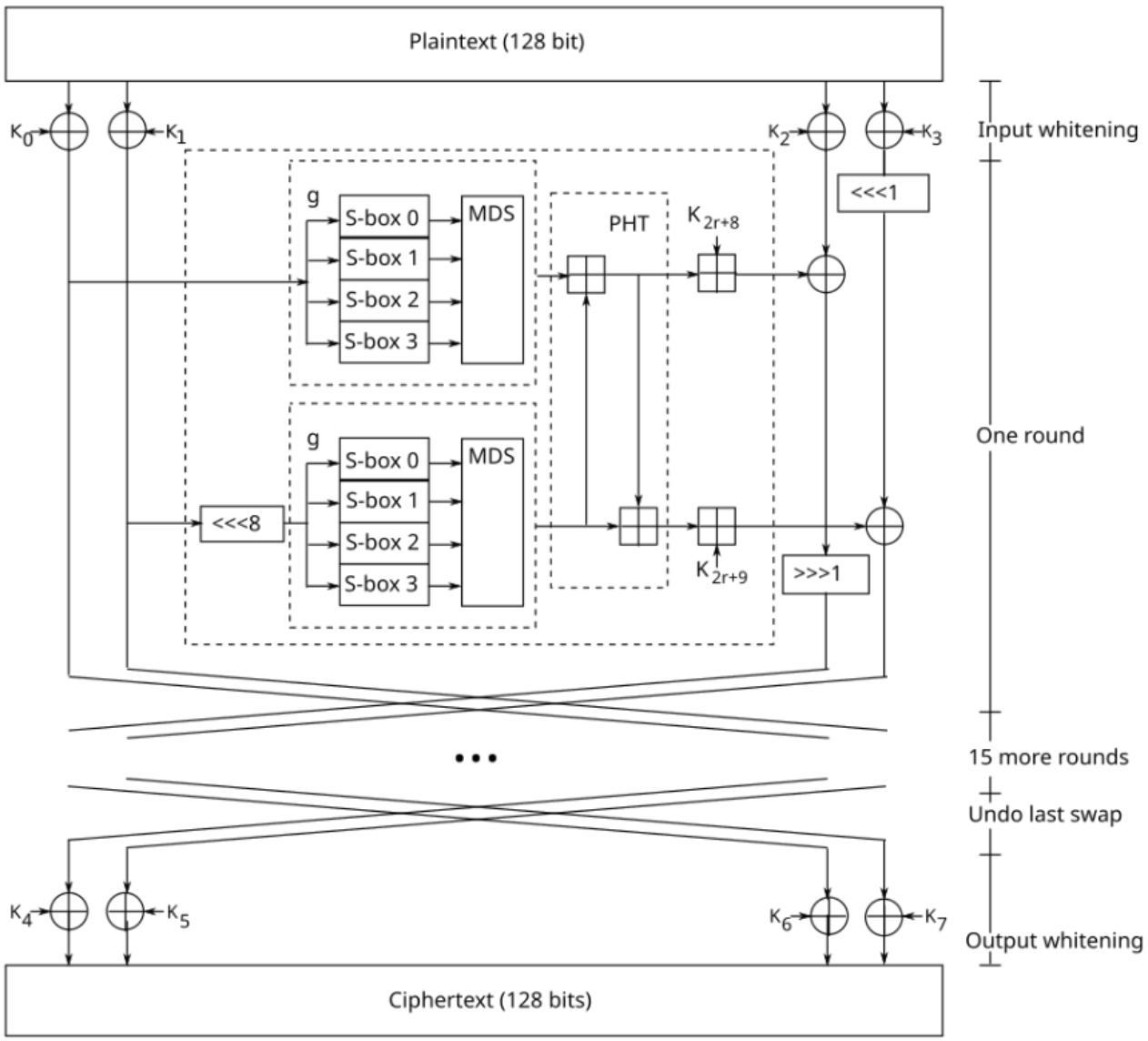

Рисунок 2.6 – Діаграма алгоритму Twofish

Алгоритм ГОСТ 28147-89 (рис. 2.7) був розроблений у 1989 році як державний стандарт симетричного шифрування СРСР. Він використовує 256-бітний ключ і оперує 64-бітними блоками даних. Архітектура алгоритму базується на мережі Фейстеля з 32 раундами, що є значно більшою кількістю порівняно з аналогами. У кожному раунді використовується вісім S-блоків, які в різних реалізаціях можуть бути різними, що забезпечує додаткову гнучкість. Однак через обмеження розміру блоку 64 біти та вік стандарту, ГОСТ 28147-89 наразі вважається застарілим.

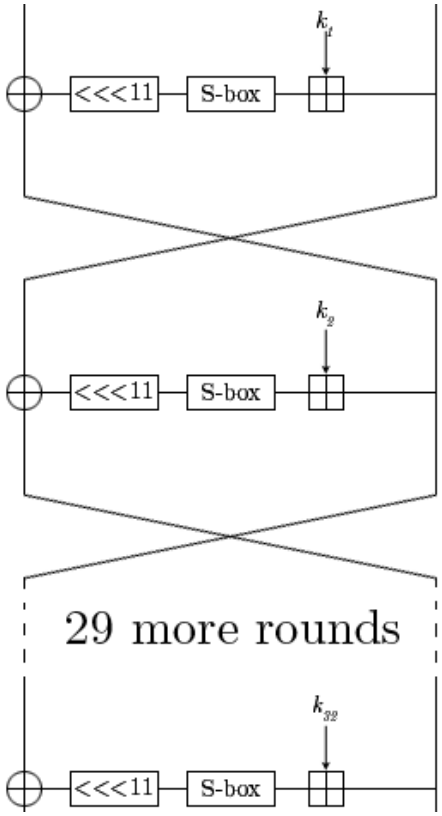

Рисунок 2.7 – Схема алгоритму ГОСТ 28147-89

Алгоритм «Калина» ДСТУ 7693:2014 (рис. 2.8), є українським національним стандартом блокового симетричного шифрування, прийнятим у 2014 році.

Він підтримує довжину блоку та ключа 128, 256 або 512 біт, що дозволяє гнучко налаштовувати рівень безпеки відповідно до вимог конкретного застосування. Кількість раундів залежить від розміру блоку: 10 раундів для 128 біт, 14 для 256 біт, 18 для 512 біт. В основі Калини лежить SP-мережа з використанням чотирьох типів S-блоків та операцій зсуву рядків і перемішування стовпців у скінченному полі GF(2^8).

Варіант Калина-256 із 256-бітним ключем забезпечує робочу характеристику стійкості 1 $\cdot 2^{256}$, але з 2^{568} біт, що є меншою обчислювальною складністю реалізації (104 000 операцій на блок проти 176 000 у Rijndael-256).

Активне використання «Калини» для захисту державних інформаційних систем робить цей алгоритм актуальним і для банків, що діють у правовому полі України [35].

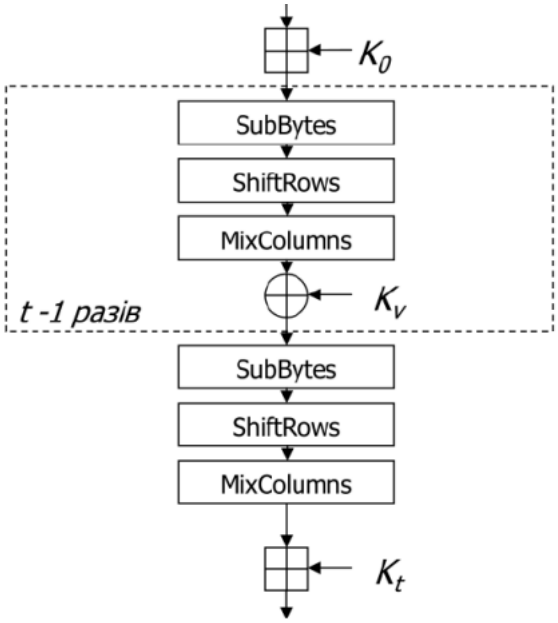

Рисунок 2.8 – Алгоритм шифрування «Калина»

Завершуючи огляд, слід відзначити загальну тенденцію переходу до блокових шифрів із розміром блоку 128 біт і більше та довжиною ключа не менше 256 біт [36]. Це зумовлено як зростанням обчислювальних можливостей зловмисників, так і необхідністю обробки великих обсягів даних у високошвидкісних банківських мережах. Проведений огляд створює теоретичне підґрунтя для порівняльного аналізу стійкості та продуктивності цих алгоритмів.

2.4 Асиметричні алгоритми шифрування

Асиметрична криптографія базується на використанні пари математично пов'язаних ключів, що складається з відкритого та закритого ключа.

Цей підхід усуває потребу в попередньому обміні конфіденційною інформацією й дозволяє ефективно вирішувати три ключові завдання інформаційної безпеки:

- Забезпечення конфіденційності шляхом шифрування даних на базі відкритого ключа одержувача;
- Безпечний обмін даними для встановлення спільного сеансового ключа через незахищені канали зв'язку;
- Цілісність та автентифікація джерела повідомлень із гарантією неможливості відмови від авторства через механізм цифрового підпису.

Сучасні банківські протоколи, зокрема TLS/SSL, на яких базується захист онлайн-банкінгу та міжбанківських комунікацій, значною мірою спираються на асиметричні алгоритми для початкового встановлення захищеного з'єднання.

Криптографічна стійкість асиметричних систем ґрунтується на обчислювальній складності певних математичних задач, для яких на сьогодні не існує ефективних алгоритмів розв'язання класичними комп'ютерами. Залежно від типу покладеної в основу математичної проблеми розрізняють три основні родини асиметричних алгоритмів: системи на основі факторизації великих цілих чисел, системи на основі дискретного логарифмування в скінченних полях та системи на основі еліптичних кривих.

Найвідомішим представником першої родини є алгоритм RSA (рис. 2.9), названий за ініціалами його творців Рівеста, Шаміра та Адлемана, які опублікували його у 1978 році. Безпека RSA базується на складності розкладання великого складеного числа на два прості множники. Для генерації ключів обираються два випадкові прості числа, з їх добутку формується модуль, а відкритий і закритий ключі пов'язуються через функцію Ейлера. Довжина ключа в RSA визначається розміром модуля; на сьогодні мінімально рекомендованою є довжина 2048 біт, що забезпечує приблизно 112-бітний рівень безпеки [37].

Алгоритм може використовуватися як безпосередньо для шифрування, так і для формування цифрового підпису. Попри широке розповсюдження в банківських системах, зокрема в протоколах TLS, RSA має суттєвий недолік

– значну обчислювальну складність операцій, особливо під час генерації ключів, що спонукає до пошуку більш ефективних альтернатив.

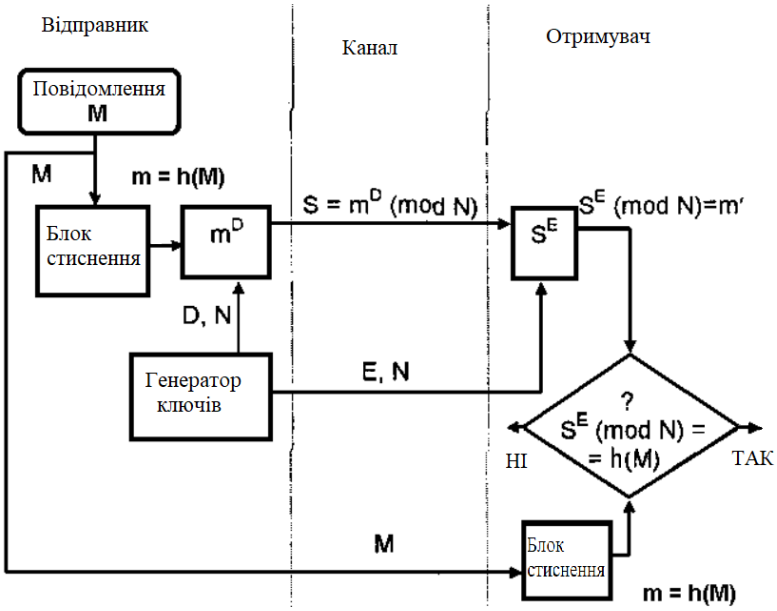

Рисунок 2.9 – Узагальнена схема цифрового підпису RSA

Друга родина, алгоритми на основі дискретного логарифмування, представлена насамперед схемою цифрового підпису DSA, стандартизованою NIST у 1991 році. На відміну від RSA, DSA призначений виключно для підпису, а не для шифрування. Його стійкість ґрунтується на складності обчислення дискретного логарифма в мультиплікативній групі простого скінченного поля. Алгоритм використовує пару ключів, де закритий ключ є випадковим числом, а відкритий обчислюється шляхом піднесення генератора до степеня закритого ключа за модулем великого простого числа. Для забезпечення прийнятного рівня безпеки DSA потребує довжини ключа не менше 2048 біт.

Найбільш сучасною та ефективною родиною асиметричних алгоритмів є криптографія на еліптичних кривих, запропонована у 1985 році. Математичний апарат ECC базується на властивостях групи точок еліптичної кривої над скінченним полем, де операція додавання точок є аналогом множення в класичних системах, а задача дискретного логарифмування на еліптичній кривій є значно складнішою за класичний дискретний логарифм/

Головна перевага ECC полягає в тому, що еквівалентний рівень безпеки досягається при значно меншій довжині ключа: наприклад, 256-бітний ключ на еліптичній кривій забезпечує приблизно такий самий захист, як 3072-бітний ключ RSA. Це зменшує обчислювальне навантаження, обсяг пам'яті для зберігання ключів та розмір службових даних, що є критичним для мобільних банківських застосунків і платіжних терміналів [38].

На практиці в банківських системах найчастіше використовуються два протоколи на основі еліптичних кривих: ECDH (рис. 2.10) для обміну ключами та ECDSA для цифрового підпису [39]. ECDH дозволяє двом сторонам виробити спільний секретний ключ, обмінюючись лише відкритими ключами незахищеним каналом. Кожна сторона генерує випадковий закритий ключ і обчислює відповідний відкритий ключ як добуток базової точки кривої на закритий ключ. Після взаємного обміну публічними ключами кожна сторона виконує операцію множення отриманого відкритого ключа на власний закритий, у результаті чого формується ідентичний для обох сторін спільний пароль.

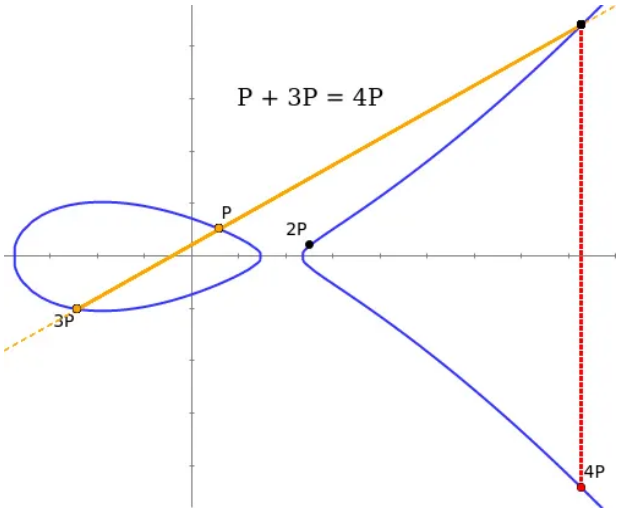

Рисунок 2.10 – Приклад еліптичної кривої та операції додавання точок, математична основа алгоритму ECDH

Алгоритм ECDSA, у свою чергу, реалізує механізм цифрового підпису: відправник обчислює хеш-повідомлення, підписує його своїм закритим ключем, а отримувач перевіряє підпис за допомогою відкритого ключа

відправника. Обидва алгоритми стандартизовані NIST і широко застосовуються в протоколах TLS версії 1.3, які є основою захисту сучасних банківських онлайн-сервісів [40, 41].

Окрему категорію становлять алгоритми цифрового підпису, які забезпечують цілісність, автентифікацію та неспростовність транзакцій. Спільним для всіх схем цифрового підпису є використання хеш-функції для стиснення повідомлення до фіксованого дайджесту, який потім підписується закритим ключем. Отож, загальна стійкість схеми підпису залежить як від надійності асиметричного алгоритму, так і від криптографічної якості використовуваної хеш-функції. Якщо хеш-функція вразлива до колізій, зловмисник може підібрати два різні повідомлення з однаковим підписом, що повністю компрометує механізм. В сучасних банківських системах спостерігається відмова від застарілих хеш-функцій MD5 і SHA-1 на користь SHA-2, SHA-3 та національних стандартів, таких як «Калина» в режимі MAC.

Видно, що асиметричні алгоритми відіграють критичну роль у побудові захищених банківських комунікацій, вирішуючи задачу безпечного обміну ключами та автентифікації транзакцій без необхідності попереднього розповсюдження секретних ключів. Водночас практика показала, що безпосереднє застосування асиметричного шифрування до великих обсягів даних є неефективним через високу обчислювальну складність. Вона зумовила появу гібридних криптографічних схем, в яких асиметричні алгоритми використовуються лише для обміну сеансовим ключем, а основний потік даних шифрується швидкодіючими симетричними шифрами.

2.5 Гібридні алгоритми шифрування та криптографічні схеми в телекомунікаційних протоколах захисту

Гібридні криптографічні схеми є сучасним підходом до забезпечення захисту інформації в телекомунікаційних системах та поєднують переваги

асиметричних і симетричних алгоритмів шифрування. Їх використання обумовлене необхідністю одночасного досягнення високого рівня криптографічної стійкості та ефективності обробки даних. У таких схемах асиметричні алгоритми застосовуються для автентифікації сторін та узгодження ключового матеріалу, тоді як симетричні алгоритми використовуються для безпосереднього шифрування інформаційного потоку. Завдяки такому розподілу функцій вдається усунути основний недолік асиметричної криптографії – високу обчислювальну складність, зберігаючи при цьому переваги безпечного обміну ключами через відкриті канали зв’язку.

Принцип функціонування гібридної схеми передбачає виконання двох послідовних етапів. На етапі встановлення з’єднання сторони здійснюють узгодження криптографічних параметрів і формують спільний ключовий матеріал за допомогою алгоритмів асиметричної криптографії. Найбільш поширеним механізмом для реалізації цього процесу є протокол Діффі-Хеллмана на еліптичних кривих (ECDH, Elliptic Curve Diffie-Hellman), який дозволяє сформувати спільне значення ключового матеріалу через незахищений канал зв’язку без передавання конфіденційної інформації. Надалі на основі отриманих параметрів генеруються сеансові ключі, які використовуються симетричними алгоритмами для захисту даних.

Практична реалізація такого підходу найбільш повно представлена в протоколі TLS 1.3 який є актуальним стандартом захисту мережевих з’єднань [42]. На відміну від попередніх версій протоколу, TLS 1.3 підтримує лише ефемерні механізми обміну ключами на основі (EC)DHE, що забезпечують властивість forward secrecy. Під час процедури handshake сторони обмінюються відкритими параметрами, виконують обчислення спільного ключового матеріалу та за допомогою функції HKDF формують набір незалежних сеансових ключів для шифрування та автентифікації повідомлень.

Для захисту трафіку в TLS 1.3 використовуються виключно алгоритми автентифікованого шифрування, серед яких основними є AES-128-GCM, AES-256-GCM та ChaCha20-Poly1305. Такі алгоритми забезпечують не лише конфіденційність інформації, але й контроль її цілісності та автентичності в межах єдиного криптографічного механізму.

Ще одним прикладом використання гібридної криптографії є протокол IPsec, який реалізує захист інформації на мережевому рівні моделі OSI. У цьому випадку узгодження параметрів безпеки та формування ключового матеріалу здійснюється за допомогою протоколу IKEv2, який підтримує як класичні алгоритми Діффі-Хеллмана, так і їх реалізації на еліптичних кривих. Після завершення процедури обміну ключами передавання даних здійснюється із застосуванням симетричних алгоритмів шифрування, переважно сімейства AES. Підхід забезпечує високий рівень захисту мережевого трафіку при збереженні прийнятної продуктивності навіть у великих корпоративних мережах.

Перспективним напрямом розвитку гібридних криптографічних схем є інтеграція постквантових алгоритмів обміну ключами. Актуальність цього напряму пов’язана з потенційною загрозою з боку квантових комп’ютерів, які теоретично здатні порушити криптографічну стійкість сучасних алгоритмів асиметричної криптографії. У гібридних постквантових схемах ключовий матеріал формується шляхом комбінування результатів, отриманих від класичного алгоритму обміну ключами, наприклад ECDH, та постквантового механізму інкапсуляції ключів, зокрема CRYSTALS-Kyber [43, 44]. Такий підхід забезпечує збереження криптографічної стійкості навіть у разі компрометації одного з компонентів схеми. Саме тому інтеграція постквантових алгоритмів у протоколи TLS та IPsec розглядається міжнародними організаціями стандартизації як один із пріоритетних напрямів розвитку телекомунікаційної безпеки.

2.6 Висновки до другого розділу

Гібридні криптографічні схеми є основою сучасних протоколів захисту інформації, оскільки дозволяють поєднати безпечне узгодження ключового матеріалу з ефективним симетричним шифруванням даних. Подальший розвиток таких схем пов’язаний із впровадженням постквантових криптографічних алгоритмів, що має забезпечити необхідний рівень захисту телекомунікаційних систем в умовах розвитку нових обчислювальних технологій.

У даному розділі було розглянуто теоретичні засади криптографічного захисту інформації в банківських телекомунікаційних мережах, зокрема основні типи криптографічних атак, критерії оцінювання криптографічної стійкості та принципи функціонування сучасних алгоритмів шифрування. Увагу приділено симетричним, асиметричним і гібридним криптографічним алгоритмам, які становлять основу сучасних засобів захисту інформації.

Узагальнена схема наведена на рисунку 2.11, де представлено класифікацію основних алгоритмів шифрування, досліджених у роботі. Отримані результати формують теоретичну основу для подальшого аналізу їхніх характеристик, порівняння криптографічної стійкості та оцінювання перспектив використання в умовах розвитку постквантових обчислювальних технологій.

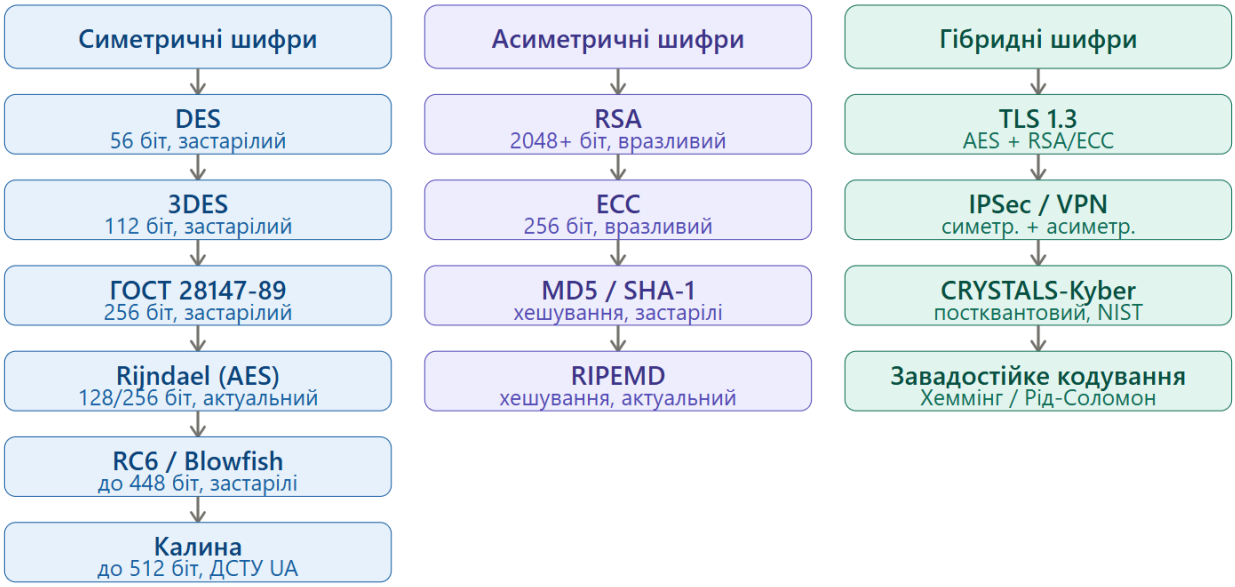

Рис. 2.11 – Криптографічні алгоритми захисту інформації

РОЗДІЛ 3
ПОРІВНЯЛЬНИЙ АНАЛІЗ ХАРАКТЕРИСТИК АЛГОРИТМІВ ШИФРУВАННЯ ТА ЦИФРОВОГО ПІДПИСУ

У попередньому розділі було розглянуто теоретичні основи побудови симетричних, асиметричних та гібридних криптографічних схем, а також основні класи атак на них. Проте теоретичного опису недостатньо для прийняття обґрунтованого рішення щодо вибору конкретних алгоритмів для побудови захищеної банківської телекомунікаційної системи. Необхідно кількісно оцінити, наскільки існуючі алгоритми відповідають сучасним вимогам із криптографічної стійкості, цілісності даних та обчислювальної ефективності.

Метою даного розділу є проведення порівняльного аналізу характеристик найпоширеніших алгоритмів шифрування та цифрового підпису за визначеними критеріями. Аналіз виконується у три етапи: спочатку виявляються системні недоліки та обмеження існуючих підходів в умовах сучасних загроз, потім проводиться безпосереднє порівняння алгоритмів симетричного шифрування за показниками криптографічної стійкості та складності реалізації, і нарешті аналізуються алгоритми забезпечення цілісності та цифрового підпису. Результати цього розділу стануть основою для формулювання вимог до вдосконаленої криптографічної схеми, яка розроблятиметься далі.

3.1 Недоліки та обмеження існуючих підходів

Незважаючи на значний прогрес у галузі криптографічного захисту інформації, практика експлуатації банківських телекомунікаційних систем виявляє низку системних недоліків та обмежень, притаманних багатьом існуючим підходам. Ці обмеження охоплюють чотири ключові напрями: недостатню довжину ключа та застарілість алгоритмів, неадекватність оцінки

стійкості в умовах нових типів атак, обмеження механізмів забезпечення цілісності даних, а також проблему адаптивності до перспективних загроз, зокрема квантового криптоаналізу.

Передусім слід відзначити, що значна частина алгоритмів, які досі використовуються в окремих банківських системах, була розроблена в 1970-1990-х роках і вже не відповідає сучасним вимогам безпеки. Як зазначається у звіті NIST, алгоритми з довжиною ключа менше 128 біт не рекомендуються для використання в системах із високими вимогами до безпеки після 2020 року.

Наступним суттєвим обмеженням є те, що класичне поняття криптографічної стійкості часто зводиться лише до оцінки складності атаки грубої сили, яка визначається довжиною ключа. Проте сучасні методи криптоаналізу, такі як диференціальний, лінійний та атаки на реалізацію, дозволяють суттєво знизити ефективну стійкість алгоритму. Наприклад, для алгоритму RC6 з 256-бітним ключем складність диференціального криптоаналізу оцінюється як 2^{21} межу 2^{2} порядки нижчою за номінальну, і цей фактор необхідно враховувати при виборі алгоритмів для банківських систем.

Не менш важливою проблемою є обмеженість традиційних механізмів забезпечення цілісності даних. Алгоритми хешування MD5 та SHA-1, які тривалий час використовувалися для контролю цілісності фінансових повідомлень, на сьогодні є повністю скомпрометованими. Для MD5 ймовірність успішної колізійної атаки становить $2{,}9 \cdot 10^{-39}$, а для $6{,}8 \cdot 10^{-49}$, практична колізія для SHA-1 була публічно продемонстрована дослідниками з Google та CWI Amsterdam у 2017 році в рамках проекту SHAttered [45]. Хоча сучасні алгоритми, такі як SHA-3 та вітчизняний стандарт «Калина» в режимі MAC, забезпечують значно кращі показники з імовірністю обману до 10^{-78}, що все ще вважається прийнятним обмеженням

виявляти пошкодження або модифікацію даних, але не виправляти їх. В умовах активних атак на канали передачі даних, коли зловмисник цілеспрямовано спотворює пакети, самого лише виявлення недостатньо – потрібні механізми відновлення втраченої інформації.

Зрештою, найбільш критичним обмеженням існуючих підходів є їхня принципова вразливість до атак із використанням квантових обчислень. Алгоритм Шора, розроблений ще в 1994 році, теоретично дозволяє за поліноміальний час зламати всі асиметричні криптосистеми, що базуються на факторизації цілих чисел або дискретному логарифмуванні в групі точок еліптичної криптографії [46]. Як зазначається у звіті NIST IR 8105 «Report on Post-Quantum Cryptography», поява квантового комп'ютера достатньої потужності поставить під загрозу практично всі сучасні протоколи обміну ключами, включно з тими, що використовуються в банківських TLS/SSL-з'єднаннях [47]. Хоча симетричні алгоритми, зокрема AES та «Калина», вважаються відносно стійкими до квантових атак, оскільки алгоритм Ґровера дає лише квадратичне прискорення перебору, компрометація каналу обміну ключами нівелює весь захист, адже зловмисник отримує сеансові ключі у відкритому вигляді.

Проведений аналіз виявляє чотири ключові проблеми, які мають бути вирішені при розробці вдосконаленого підходу до криптографічного захисту:

- Необхідність вибору алгоритмів із достатньою довжиною ключа та доведеною стійкістю до диференціального криптоаналізу;
- Потреба у механізмах не лише виявлення, а й виправлення пошкоджених даних;
- Необхідність захисту каналу обміну ключами від квантових атак;
- Забезпечення прийнятного рівня обчислювальної складності для практичного впровадження в банківських мережах.

Зазначені вимоги будуть покладені в основу порівняльного аналізу в наступних підрозділах та формування вдосконаленого підходу.

3.2 Порівняльний аналіз симетричних алгоритмів шифрування

Виявлені раніше обмеження існуючих підходів обумовлюють необхідність проведення кількісного порівняльного аналізу сучасних алгоритмів симетричного шифрування. Метою такого аналізу є визначення алгоритму або групи алгоритмів, які можуть бути обрані як базова схема для подальшого вдосконалення. Для забезпечення об'єктивності оцінювання необхідно визначити чіткі критерії, що враховують як безпекові, так і практичні аспекти застосування алгоритмів у банківських телекомунікаційних мережах.

Першим і найважливішим критерієм є криптографічна стійкість алгоритму, яка кількісно виражається через робочу характеристику l_{p}, що визначає мінімальну складність успішної атаки в бітах. Цей показник інтегрує в собі як стійкість до атаки грубої сили, так і стійкість до відомих методів криптоаналізу, зокрема диференціального та лінійного.

Другим критерієм виступає часова складність реалізації алгоритму, яка вимірюється в кількості елементарних операцій, необхідних для обробки одного блоку даних, і безпосередньо впливає на продуктивність системи в цілому.

Третім критерієм є довжина ключа, оскільки вона визначає не лише стійкість до перебору, а й відповідність сучасним нормативним вимогам. Додатково враховується статус алгоритму з точки зору актуальності та наявності відомих вразливостей.

У таблиці 3.1 наведено результати розрахунку показників криптографічної стійкості для основних алгоритмів симетричного шифрування, включно з вітчизняними стандартами.

Таблиця 3.1 – Результати оцінки складності реалізації алгоритмів обміну ключами

Алгоритм	Довжина ключа, біт	Nk (груба сила)	Nопер (диф. криптоаналіз)	tб (груба сила), років	tб (диф. криптоаналіз), років	l_0 біт	Статус
DES	56	2^{56}	2^{47}	0,23	$3\cdot10^{-3}$	124	Застарілий
Rijndael	128	2^{128}	2^{72}	$1{,}1\cdot10^{21}$	$1{,}5\cdot10^{4}$	284	Актуальний
Rijndael	256	2^{256}	2^{215}	$3{,}7\cdot10^{59}$	–	568	Актуальний
ГОСТ 28147-89	256	2^{256}	–	$3{,}7\cdot10^{59}$	–	568	Застарілий
RC6	128	2^{128}	2^{122}	$1{,}1\cdot10^{21}$	$1{,}71\cdot10^{19}$	284	Застарілий
RC6	192	2^{192}	2^{160}	$2{,}02\cdot10^{4}$	$4{,}7\cdot10^{3}$ □	426	Застарілий
RC6	256	2^{256}	2^{215}	$3{,}7\cdot10^{59}$	$1{,}7\cdot10^{47}$	568	Застарілий
Blowfish	32	2^{32}	–	$1{,}4\cdot10^{-9}$	–	71	Застарілий
Blowfish	448	2^{4}	–	$2{,}35\cdot10^{117}$	–	995	Застарілий
«Купина» (ДСТУ 7624)	256	2^{256}	$\sim2^{215}$	$\sim3{,}7\cdot10^{5}$	–	568	UA стандарт
«Купина» (ДСТУ 7624)	512	2^{51}	$\sim2^{450}$	$\sim10^{154}$	–	1136	UA стандарт
«Калина» (ДСТУ 7693)	256	2^{256}	$\sim2^{215}$	$\sim3{,}7\cdot10^{5}$	–	568	UA стандарт
«Калина» (ДСТУ 7693)	512	2^{51}	$\sim2^{450}$	$\sim10^{154}$	–	1136	UA стандарт

Аналіз даних таблиці 3.1 дозволяє зробити кілька важливих висновків. Алгоритм DES із робочою характеристикою l_0 = 124 біт та часом зламу менше однієї доби є абсолютно непридатним для сучасних банківських систем. Алгоритм RC6, попри формально високу стійкість до грубої сили, демонструє суттєве зниження ефективної стійкості при диференціальному

криптоаналізі: для 256-бітної версії $N_{опер}$ становить 2 [21]
нижче за теоретичну межу. Алгоритм Blowfish із 32-бітним ключем має l_{σ}= 71 біт, що є критично низьким показником, а його 448-бітна версія, хоча й демонструє формально високу стійкість, визнана застарілою через структурні недоліки. Алгоритм ГОСТ 28147-89 також вважається застарілим і не рекомендований для нових впроваджень. Так, серед актуальних алгоритмів найкращі показники демонструють Rijndael з довжиною ключа 256 біт та вітчизняні стандарти «Калина» і «Купина» з аналогічною довжиною ключа, для яких l_{σ}= 568 біт, а для 512-бітних версій цей показник сягає 1136 біт.

Хоча криптографічна стійкість є необхідною, але не достатньою умовою для вибору алгоритму. Не менш важливим критерієм є обчислювальна складність реалізації, яка визначає швидкодію алгоритму та його придатність для обробки великих обсягів фінансових транзакцій у реальному часі. У таблиці 3.2 представлено результати оцінки складності реалізації досліджуваних алгоритмів.

Таблиця 3.2 – Оцінка складності реалізації алгоритмів симетричного шифрування

Алгоритм	Розмір блоку, біт	Довжина ключа, біт	Складність (операцій на блок)	Підсумкова складність	Покоління
3DES	64	112	2076·Nd	132 864	Застарілий
IDEA	192	192	216·Nd + 92	41 564	Застарілий
Rijndael 128	128	128	688·Nd + 188	88 252	Актуальний
Rijndael 256	256	256	688·Nd + 188	176 316	Актуальний
Twofish	192	192	312·Nd + 1404	61 308	Актуальний
ГОСТ 28147-89	256	256	384·Nd + 32	98 336	Застарілий
Калина-256	256	256	544·Nd + 288	104 000	UA стандарт

Дані таблиці 3.2 свідчать, що найнижчу складність реалізації серед актуальних алгоритмів має Twofish, однак він поступається за показником криптографічної стійкості, оскільки максимальна довжина його ключа становить 192 біти, що не відповідає визначеній у підрозділі 3.1 вимозі щодо мінімальної довжини ключа 256 біт. Алгоритм 3DES демонструє найвищу складність (132 864 операцій) при найменшому розмірі блоку (64 біт), що робить його неефективним для сучасних високошвидкісних мереж. Вітчизняний стандарт Калина-256 має дещо вищу складність (104 000 операцій) порівняно з Rijndael-128 (88 252), проте забезпечує вдвічі більшу довжину ключа та відповідно кращу стійкість. Розширена версія Rijndael-256 із підсумковою складністю 176 316 операцій є закономірно більш ресурсоємною, що є платою за суттєве підвищення рівня безпеки.

Проведений порівняльний аналіз за сукупністю критеріїв дозволяє визначити групу алгоритмів, які є найбільш придатними для використання як базові в банківських телекомунікаційних системах. Алгоритм Rijndael-256 забезпечує найкращий баланс між стійкістю ($l_{о}$ = 568 біт) та прийнятною складністю реалізації (176 316 операцій). Вітчизняний стандарт Калина-256 є обґрунтованою альтернативою, особливо в контексті вимог нормативно-правової бази України щодо використання національних криптографічних стандартів у державних та банківських установах, і демонструє співмірні показники ($l_{о}$ = 568 біт, складність 104 000 операцій). Саме ці алгоритми будуть розглядатися як базові схеми при розробці вдосконаленого підходу до криптографічного захисту, а їхні кількісні характеристики стануть еталонними значеннями для оцінки ефективності. При цьому питання забезпечення цілісності даних та автентифікації, які не охоплюються симетричним шифруванням, потребують окремого аналізу і будуть розглянуті в наступному підрозділі.

3.3 Порівняльний аналіз алгоритмів цифрового підпису та забезпечення цілісності даних

Як було встановлено в підрозділі 3.1, забезпечення цілісності даних є однією з ключових вимог до криптографічного захисту банківських телекомунікаційних мереж, а традиційні алгоритми хешування мають суттєві обмеження, пов'язані з неможливістю виправлення пошкоджених даних. У даному підрозділі проводиться порівняльний аналіз сучасних алгоритмів цифрового підпису та хеш-функцій, які використовуються для контролю цілісності та автентифікації повідомлень у банківських системах. Метою аналізу є визначення алгоритмів, що забезпечують найкращі показники за критерієм ймовірності обману, а також виявлення їхніх функціональних обмежень, які мають бути подолані в рамках запропонованого вдосконаленого підходу.

Ключовим критерієм оцінки алгоритмів забезпечення цілісності є ймовірність обману – імовірність того, що зловмисник зможе підібрати інше повідомлення з тим самим значенням хеш-функції, тобто створити колізію. Цей показник визначає рівень довіри до того, що отримане повідомлення не було модифіковане в процесі передачі каналами зв'язку. Додатковими критеріями виступають довжина вихідного хеш-значення, яка впливає на обсяг службової інформації, та статус алгоритму з точки зору стійкості до відомих атак. У таблиці 3.3 наведено результати порівняльного аналізу основних алгоритмів хешування та цифрового підпису.

Таблиця 3.3 – Порівняльний аналіз алгоритмів забезпечення цілісності даних

Алгоритм	Ймовірність обману	Статус
MD5	$2{,}9 \cdot 10^{-39}$	Скомпрометований
SHA-1	$6{,}8 \cdot 10^{-49}$	Застарілий
RIPEMD	$6{,}8 \cdot 10^{-49}$	Актуальний

«Калина» (як MAC)	$>10^{-78}$	Держстандарт UA
SHA-3 / SHAKE	$>10^{-49}$	Постквантово стійкий

Аналіз даних таблиці 3.3 виявляє чітку ієрархію алгоритмів за рівнем надійності. Алгоритм MD5 із імовірністю обману $2{,}9 \cdot 10^{-39}$ Е повністю скомпрометованим ще з 2008 року, коли дослідники продемонстрували можливість створення колізій за частки секунди на стандартному обладнанні. Алгоритм SHA-1 із показником $6{,}8 \cdot 10^{-49}$ визнаний застарілим після практичної демонстрації колізії в рамках проекту SHAttered у 2017 році, і з 2020 року його використання не рекомендується в системах із високими вимогами до безпеки. Алгоритм RIPEMD забезпечує співмірний із SHA-1 рівень стійкості, однак не набув широкого поширення в банківському секторі через меншу кількість незалежних досліджень його криптографічної стійкості.

Найкращі показники демонструють алгоритми нового покоління. Вітчизняний стандарт «Калина» в режимі використання як MAC забезпечує ймовірність обману понад 10^{-78}, показники SHA-1 та RIPEMD. Алгоритм SHA-3 із імовірністю обману понад 10^{-49} є статус постквантово стійкого, оскільки його структура на основі губчастої конструкції не вразлива до відомих квантових атак, зокрема до алгоритму Гровера в повному обсязі.

Попри суттєвий прогрес у підвищенні ймовірності обману, принциповим обмеженням усіх розглянутих алгоритмів залишається те, що вони виконують лише функцію виявлення пошкоджень або модифікації даних. Жоден із них не здатен самостійно відновити втрачену чи спотворену інформацію. У банківських телекомунікаційних мережах, де втрата навіть одного пакету фінансової транзакції може призвести до значних наслідків, необхідність повторної передачі даних після виявлення помилки створює додаткове навантаження на канали зв'язку та збільшує затримку обробки.

Таке обмеження обґрунтовує доцільність інтеграції завадостійкого кодування як додаткового рівня захисту, здатного не лише виявляти, а й виправляти помилки в межах визначеної коригувальної здатності коду.

3.4 Висновки до третього розділу

Проведений у даному розділі порівняльний аналіз характеристик алгоритмів шифрування та забезпечення цілісності даних дозволяє сформулювати такі основні результати. Виявлено чотири системні обмеження існуючих підходів до криптографічного захисту банківських мереж: застарілість алгоритмів із недостатньою довжиною ключа, неадекватність оцінки стійкості до сучасних методів криптоаналізу, обмеженість механізмів забезпечення цілісності даних лише функцією виявлення помилок та незахищеність каналу обміну ключами від квантових атак. Ці обмеження формують перелік вимог, яким має відповідати вдосконалений підхід.

За результатами аналізу алгоритмів симетричного шифрування встановлено, що найкращий баланс між криптографічною стійкістю та обчислювальною складністю забезпечують алгоритми Rijndael-256 (l_{σ} = 568 біт, складність 176 316 операцій) та Калина-256 (l_{σ} = 568 біт, складність 104 000 операцій). Аналіз алгоритмів забезпечення цілісності показав, що найкращі показники ймовірності обману демонструють SHA-3 та «Калина» в режимі MAC, однак усі вони обмежені лише виявленням пошкоджень. Це обґрунтовує необхідність доповнення криптографічної схеми механізмами завадостійкого кодування для забезпечення можливості виправлення помилок.

Отримані в цьому розділі кількісні показники (l_{σ} = 568 біт, складність реалізації від 104 000 до 176 000 операцій, ймовірність обману до 10^{-78}) становитимуть еталонну базу для оцінювання ефективності запропонованого

вдосконаленого підходу, який розроблятиметься з урахуванням необхідності захисту від постквантових загроз.

РОЗДІЛ 4
АНАЛІЗ ПОСТКВАНТОВИХ АЛГОРИТМІВ ШИФРУВАННЯ І ПІДХОДІВ ДО ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ

Проведений у попередньому розділі порівняльний аналіз дозволив визначити базові алгоритми симетричного шифрування (Rijndael-256 та Калина-256), які забезпечують найкращий баланс між криптографічною стійкістю та обчислювальною складністю, а також виявив принципове обмеження, притаманне всім розглянутим схемам – незахищеність каналу обміну ключами від квантових атак. Це обмеження має критичне значення, оскільки компрометація сеансового ключа повністю нівелює стійкість симетричного шифру незалежно від його теоретичної надійності.

Метою даного розділу є дослідження постквантових криптографічних алгоритмів як засобу подолання виявлених обмежень та формування підходу до поетапного підвищення стійкості криптографічного захисту банківських телекомунікаційних мереж.

4.1 Обґрунтування необхідності застосування постквантових алгоритмів

Розвиток квантових обчислень створює принципово новий клас загроз для криптографічних систем, що протягом десятиліть вважалися безумовно надійними. На відміну від класичних комп'ютерів, які оперують бітами в стані 0 або 1, квантові комп'ютери використовують кубіти, здатні перебувати в суперпозиції, що забезпечує експоненційне прискорення для розв'язання задач факторизації великих цілих чисел та обчислення дискретного логарифма. На цих математичних проблемах базується стійкість практично всіх сучасних асиметричних криптосистем, включаючи RSA, ECDH та ECDSA. Алгоритм Шора, теоретично дозволяє за поліноміальний час зламати всі ці системи на квантовому комп'ютері достатньої потужності.

Хоча такий комп'ютер наразі не створений, останні рекомендації NIST вказують, що до 2030 року шифрування зі 112-бітним рівнем безпеки має бути визнане застарілим, а до 2035 року навіть 128-бітний рівень безпеки повинен бути заборонений для використання в критичних системах [48].

Для банківського сектору квантова загроза має особливий вимір, передусім через довготривалу цінність фінансових даних. На відміну від повсякденного листування, яке втрачає актуальність за кілька днів, банківські транзакції, кредитні історії та персональна інформація клієнтів зберігають конфіденційність протягом десятиліть. Це робить цілком реальною модель атаки «harvest now, decrypt later» («збирай зараз, розшифровуй пізніше»), за якої зловмисник перехоплює та накопичує зашифрований трафік сьогодні, розраховуючи розшифрувати його після появи потужного квантового комп'ютера [49]. Усвідомлення цієї загрози змушує фінансові установи діяти превентивно, не чекаючи моменту, коли квантовий злам стане технічно можливим.

Як показав проведений аналіз, симетричні алгоритми, зокрема Rijndael-256 та Калина-256, демонструють високу стійкість із робочою характеристикою $l = 568$ біт. Алгоритм Гровера, що є основним квантовим інструментом для атаки на симетричні шифри, забезпечує лише квадратичне прискорення перебору ключа, тобто зменшує ефективну стійкість 256-бітного ключа до 128 біт, що все ще є прийнятним рівнем безпеки.

Однак ця стійкість повністю нівелюється, якщо зловмисник отримує сеансовий ключ через компрометацію асиметричної схеми обміну ключами, вразливої до алгоритму Шора. Як наслідок, першочерговим завданням при переході до постквантової криптографії є захист саме каналу обміну ключами, тоді як симетричні шифри можуть бути збережені в якості базового рівня.

Додатковим свідченням актуальності проблеми є активна фаза стандартизації постквантових алгоритмів на міжнародному рівні. У серпні 2024 року NIST офіційно затвердив перші три стандарти: FIPS-203 на основі

CRYSTALS-Kyber для обміну ключами, FIPS-204 на основі CRYSTALS-Dilithium та FIPS-205 на основі SPHINCS+ для цифрового підпису [50-52]. Паралельно ETSI у березні 2025 року опублікував гібридний стандарт обміну ключами TS 104 015, що поєднує постквантову криптографію на ґратках із класичним шифруванням [53]. Не менш важливим є регуляторний тиск: GDPR вимагає «відповідних технічних заходів» для постійної конфіденційності персональних даних, а DORA, що набирає чинності в ЄС із січня 2025 року, зобов'язує фінансові організації ідентифікувати нові ІКТ-загрози, включно з квантовими, та впроваджувати відповідні заходи захисту [54, 55].

Окремо слід відзначити гетерогенність банківської інфраструктури, де співіснують сучасні хмарні сервіси, традиційні банкоматні мережі, платіжні термінали та системи міжбанківських розрахунків. Така різнорідність унеможливлює одномоментну заміну всіх криптографічних алгоритмів і вимагає поетапного підходу, що передбачає не повну відмову від існуючих рішень, а їх доповнення постквантовими механізмами в найбільш уразливих ланках, передусім у каналі обміну ключами.

Підсумовуючи, необхідність застосування постквантових алгоритмів у банківських системах обумовлюється сукупністю технічних, часових, регуляторних та практичних чинників. Технічно критичною є вразливість асиметричних схем обміну ключами до алгоритму Шора. Часовий чинник пов'язаний із довготривалою цінністю фінансових даних, що робить реальною загрозу атаки за моделлю «harvest now, decrypt later». Регуляторний тиск проявляється через затверджені стандарти NIST FIPS 203-205, гібридний стандарт ETSI TS 104 015 та вимоги GDPR і DORA.

Практичний досвід провідних банків свідчить, що постквантова криптографія вже перейшла з теоретичної площини в інженерну. У наступному підрозділі буде проведено огляд та класифікацію основних постквантових алгоритмів, що дозволить обрати найбільш придатні для інтеграції в банківські телекомунікаційні мережі.

4.2 Огляд та класифікація основних постквантових алгоритмів

Стрімкий розвиток квантових обчислень стимулював масштабні дослідження в галузі криптографії, результатом яких стала поява цілої низки алгоритмів, стійких до атак як класичними, так і квантовими комп'ютерами. У 2016 році NIST ініціював відкритий конкурс зі стандартизації постквантових криптографічних алгоритмів, який завершився у 2024 році затвердженням перших стандартів. Усі подані на конкурс алгоритми базуються на математичних задачах, для яких на сьогодні невідомо ефективних квантових алгоритмів розв'язання. За типом математичного апарату, покладеного в основу, постквантові алгоритми поділяються на чотири основні родини: алгоритми на ґратках, алгоритми на кодах, алгоритми на основі хеш-функцій та багатовимірні алгоритми. Кожна з цих родин має свої особливості, переваги та обмеження, які визначають сферу їх потенційного застосування.

Алгоритми на ґратках (lattice-based cryptography) становлять найбільш численну та опрацьовану родину постквантових алгоритмів. Їхня стійкість базується на складності розв'язання задач теорії ґраток, зокрема задачі навчання з помилками (Learning With Errors, LWE) та її варіантів на модулях (Module-LWE). Характерною особливістю цих алгоритмів є відносно невеликий розмір ключів та висока швидкість виконання операцій, що робить їх привабливими для практичного впровадження. Найвідомішим представником цієї родини є алгоритм CRYSTALS-Kyber, який у серпні 2024 року був стандартизований NIST як FIPS-203 для KEM. Алгоритм Kyber забезпечує обмін сеансовими ключами між сторонами із рівнем безпеки, еквівалентним AES-192. Для цифрового підпису в межах цієї ж родини був стандартизований алгоритм CRYSTALS-Dilithium (FIPS-204), який також

базується на задачах теорії ґраток і забезпечує прийнятний баланс між розміром підпису та швидкодією.

Другу велику родину становлять алгоритми на кодах (code-based cryptography), стійкість яких ґрунтується на складності декодування випадкового лінійного коду – задачі, що залишається нерозв'язною за поліноміальний час уже понад 40 років. Класичним представником цієї родини є криптосистема Мак-Еліса, запропонована ще у 1978 році. Сучасні варіанти цієї схеми, зокрема алгоритм Classic McEliece, який дійшов до фінального раунду конкурсу NIST, використовують коди Гоппи з відкритим ключем великого розміру, що є їхнім основним недоліком. Попри це, алгоритми на кодах мають найдовшу історію криптоаналізу серед усіх постквантових кандидатів, що забезпечує високий рівень довіри до їх стійкості.

Третя родина – алгоритми на основі хеш-функцій (hash-based cryptography). Використовує криптографічну стійкість хеш-функцій, таких як SHA-2 або SHA-3, для побудови схем цифрового підпису. Принцип їх дії базується на деревах Меркла та одноразових підписах Лемпорта. Головною перевагою цих алгоритмів є те, що їхня безпека повністю залежить від стійкості базової хеш-функції, яка добре вивчена. Водночас вони генерують підписи значно більшого розміру порівняно з алгоритмами на ґратках. Представником цієї родини, стандартизованим NIST як FIPS-205, є алгоритм SPHINCS+ – схема підпису без збереження стану, що забезпечує високий рівень безпеки ціною збільшеного розміру вихідних даних.

Четверта родина – багатовимірні алгоритми (multivariate cryptography). Будується на складності розв'язання систем багатовимірних поліноміальних рівнянь над скінченними полями. Ці алгоритми забезпечують високу швидкість операцій, однак поступаються іншим родинам за розміром ключів та кількістю успішних атак, яким піддалися окремі кандидати під час конкурсу NIST. Деякі представники цієї родини, зокрема Rainbow та GeMSS,

дійшли до фінального раунду конкурсу, однак не увійшли до першої хвилі стандартів через виявлені вразливості.

Окремим напрямком, який не входить до жодної з чотирьох класичних родин, але набуває практичного значення, є гібридні схеми, що поєднують класичні та постквантові алгоритми. Такий підхід був закріплений у стандарті ETSI TS 104 015, опублікованому в березні 2025 року. Стандарт визначає механізм гібридного обміну ключами, за якого сеансовий ключ формується шляхом комбінування результатів роботи класичної схеми (наприклад, ECDH) та постквантової (наприклад, Kyber). Підхід забезпечує захист «в глибину»: навіть якщо одна зі схем буде зламана в майбутньому, інша продовжить забезпечувати конфіденційність. Цей принцип є особливо актуальним для банківських систем, де ціна компрометації даних є надзвичайно високою, а перехід на нові алгоритми має відбуватися поступово, без порушення безперервності бізнес-процесів.

Проведений огляд дозволяє зробити висновок, що на сьогодні сформовано достатню теоретичну та практичну базу для початку міграції банківських криптографічних систем на постквантові алгоритми. Наявність затверджених міжнародних стандартів, різноманіття математичних підходів та активна фаза пілотних впроваджень у фінансовому секторі створюють передумови для обґрунтованого вибору конкретних алгоритмів, які можуть бути інтегровані в існуючу інфраструктуру. У наступному підрозділі буде проведено порівняльний аналіз класичних алгоритмів, відібраних у Розділі 3, із постквантовими алгоритмами, розглянутими вище, за сукупністю критеріїв стійкості та продуктивності, що дозволить визначити оптимальну комбінацію для побудови вдосконаленої схеми захисту.

4.3 Порівняльний аналіз сучасних та постквантових алгоритмів шифрування

Проведений раніше аналіз дозволив виокремити два алгоритми симетричного шифрування – Rijndael-256 та Калина-256, які демонструють найкращий баланс між криптографічною стійкістю та обчислювальною складністю реалізації. Водночас було обґрунтовано, що навіть ці алгоритми не забезпечують повноцінного захисту в умовах перспективних квантових загроз, оскільки канал обміну ключами, побудований на класичних асиметричних схемах, залишається вразливим до атаки Шора.

У даному підрозділі проводиться комплексний порівняльний аналіз відібраних класичних алгоритмів та постквантових алгоритмів, розглянутих у підрозділі 4.2, за розширеною системою критеріїв, що включає класичну стійкість, постквантову стійкість, обчислювальну складність, функціональні можливості щодо забезпечення цілісності даних та практичну готовність до впровадження в банківських системах.

Метою даного аналізу є не просто констатація переваг і недоліків окремих алгоритмів, а формування доказової бази для обґрунтування структурии підходу, який має поєднати сильні сторони різних типів алгоритмів і забезпечити адаптивне нарощування рівня захисту залежно від актуальних загроз.

Для забезпечення об'єктивності оцінювання визначено шість ключових критеріїв:

1. Класична криптографічна стійкість, яка вимірюється робочою характеристикою l_{α} (біт) та визначає мінімальну складність успішної атаки з використанням класичних обчислювальних засобів.
2. Постквантова стійкість, що характеризує здатність алгоритму протистояти атакам із застосуванням квантових комп'ютерів, зокрема алгоритмів Шора та Гровера.
3. Обчислювальна складність реалізації, яка вимірюється в кількості елементарних операцій на блок даних і безпосередньо впливає на продуктивність системи.

4. Можливість забезпечення цілісності даних із функцією виправлення помилок, що є особливо актуальним в умовах активних атак на канали передачі.
5. Статус стандартизації, який визначає готовність алгоритму до практичного впровадження в банківських системах з урахуванням вимог регуляторів.
6. Оцінка накладних витрат, що включає збільшення розміру пакетів та додаткові затримки при виконанні криптографічних операцій.

У таблиці 4.1 наведено узагальнені характеристики двох алгоритмів симетричного шифрування, відібраних за результатами аналізу в минулому розділі, а також класичної схеми обміну ключами ECDH, яка наразі використовується в більшості банківських TLS/SSL-з'єднань.

Таблиця 4.1 – Характеристики відібраних класичних алгоритмів

Алгоритм	Тип	l ₀, бі	Складність реалізації	Постквантова стійкість	Статус
Rijndael-256	Симетричне шифрування	568	176 316	Часткова (ключ 128 біт після Гровера)	Актуальний
Калина-256 (ДСТУ 7693)	Симетричне шифрування	568	104 000	Часткова (ключ 128 біт після Гровера)	UA стандарт
ECDH P-256	Обмін ключами	128	~50 000	Відсутня (злам алгоритмом Шора)	Актуальний, потребує заміни

Дані таблиці 4.1 підтверджують, що обидва симетричні алгоритми забезпечують високий рівень класичної стійкості, проте їхня постквантова стійкість є лише частковою. Алгоритм Гровера теоретично знижує ефективну

довжину ключа з 256 до 128 біт, що залишається прийнятним рівнем, однак це не компенсує повної вразливості схеми обміну ключами ECDH до алгоритму Шора. Виходячи з цього навіть при використанні Rijndael-256 або Калини-256 загальна стійкість системи визначається найслабшою ланкою – обміном ключами.

Порівняння постквантових алгоритмів обміну ключами. У таблиці 4.2 наведено характеристики основних постквантових алгоритмів, призначених для захисту каналу обміну ключами, які були розглянуті раніше.

Таблиця 4.2 – Характеристики постквантових алгоритмів обміну ключами

Алгоритм	Математична основа	Рівень безпеки NIST	Розмір відкритого ключа, байт	Розмір шифротексту, байт	Час інкапсуляції, мс	Статус стандартизації
CRYSTALS-Kyber-768	Ґратки (Module-LWE)	3 (екв. AES-192)	1 184	1 088	~0,10	FIPS-203 (2024)
CRYSTALS-Kyber-1024	Ґратки (Module-LWE)	5 (екв. AES-256)	1 568	1 568	~0,14	FIPS-203 (2024)
Classic McEliece	Коди (Гоппа)	5	1 048 576	188	~0,05	Фіналіст NIST

Аналіз таблиці 4.2 показує, що алгоритм Kyber має суттєві практичні переваги для банківських застосувань. Попри те, що Classic McEliece демонструє менший час інкапсуляції та найдовшу історію криптоаналізу, розмір його відкритого ключа є неприйнятним для більшості банківських телекомунікаційних протоколів, де кожен байт службової інформації впливає на загальну пропускну здатність. Kyber-768 забезпечує третій рівень безпеки за класифікацією NIST, що відповідає стійкості AES-192 і є достатнім для захисту фінансових даних з тривалим терміном конфіденційності. Алгоритм є оптимальним балансом між рівнем захисту та розміром ключів і

шифротексту, що є критичним критерієм для інтеграції в існуючу телекомунікаційну інфраструктуру банківських мереж без суттєвого збільшення трафіку службових даних.

Як можна бачити з рис. 4.1, алгоритми серії ML-KEM демонструють суттєво вищу продуктивність порівняно з класичними аналогами. Зокрема, ML-KEM-768, обраний у даній роботі, виконує інкапсуляцію за ~0,10 мс, що є цілком порівнянним з операціями ECDH і не створює критичного навантаження на банківську телекомунікаційну інфраструктуру.

Classic McEliece показано для контрасту – він забезпечує найвищу стійкість, але час генерації ключа складає десятки секунд, що виключає його з практичного застосування в банківських системах. Шкала логарифмічна, бо інакше McEliece унеможливлює порівняння інших алгоритмів [56].

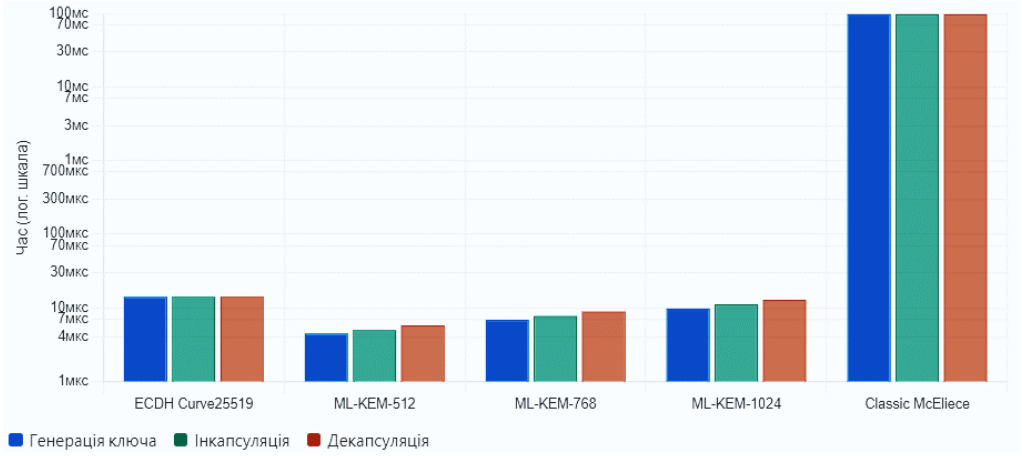

Рисунок 4.1 – Продуктивність алгоритмів обміну ключами

На рис. 4.2 наведено порівняння класичної та постквантової стійкості алгоритмів згідно з класифікацією NIST PQC. Класичні алгоритми RSA та ECDH мають нульову постквантову стійкість, що підтверджує їх вразливість до алгоритму Шора. Рівні безпеки ML-KEM відповідають стійкості AES-128, AES-192 та AES-256 для параметрів 512, 768 та 1024 відповідно. Таким чином, інтеграція Kyber-768 у запропонований підхід забезпечує перехід від нульової до 192-бітної постквантової стійкості каналу обміну ключами – без зміни симетричного шифру [57].

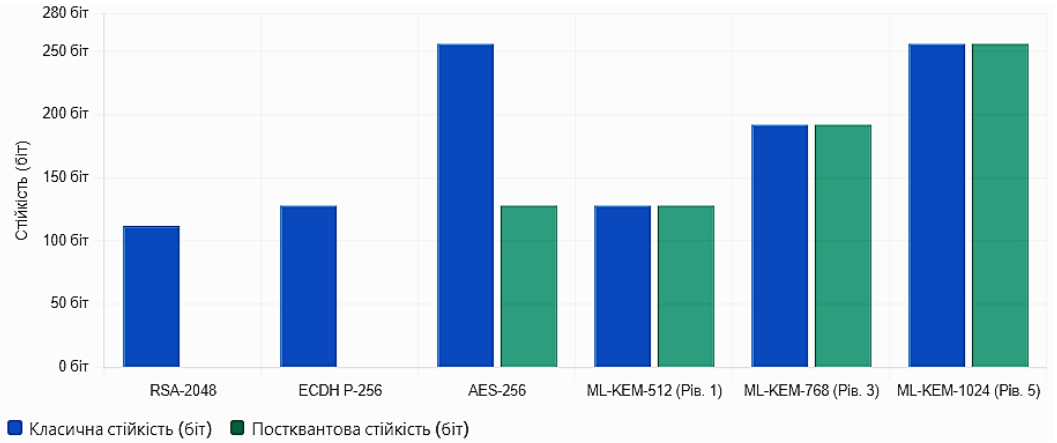

Рисунок 4.2 – Рівні постквантової стійкості алгоритмів

4.4 Пропозиції щодо підвищенню стійкості алгоритмів шифрування в банківських системах

Метою даної роботи є розробка підходу до поетапного підвищення стійкості, який поєднує симетричне шифрування, постквантовий обмін ключами та завадостійке кодування, тому абсолютно доцільно також провести порівняння не тільки окремих алгоритмів, а цілісних комбінованих схем. У таблиці 4.3 представлено порівняльний аналіз трьох конфігурацій: базової схеми, що використовується сьогодні; гібридної схеми з постквантовим обміном ключами; та запропонованої схеми з додаванням завадостійкого кодування.

Базова схема, що використовує ECDH для обміну ключами, має критичну вразливість до квантових атак. Попри те, що симетричне шифрування AES-256 забезпечує $l_o = 568$ біт, компрометація ECDH алгоритмом Шора повністю нівелює цю стійкість. Крім того, механізм забезпечення цілісності на основі SHA-3 виконує лише функцію виявлення пошкоджень, що змушує до повторної передачі даних у разі їх спотворення.

Гібридна схема з інтеграцією Kyber-768 закриває квантову вразливість каналу обміну ключами, при цьому обчислювальна складність навіть дещо знижується порівняно з базовою схемою завдяки ефективнішій реалізації операцій на ґратках. Однак ця схема все ще не вирішує проблему виправлення пошкоджених даних.

Запропонована схема, яка додатково інтегрує завадостійке кодування (код Ріда-Соломона), забезпечує не лише виявлення, а й гарантоване виправлення помилок, що є критично важливим для банківських систем в умовах активних атак на канали передачі. При цьому збільшення обчислювальної складності на приблизно 15 000 операцій порівняно з гібридною схемою та накладні витрати близько 19,3% є прийнятною ціною за суттєве підвищення надійності. Час встановлення сеансу зростає до 1,5 мс, що залишається в межах допустимих значень для банківських транзакцій, де критичний поріг затримки становить 100-200 мс.

Таблиця 4.3 – Комплексне порівняння комбінованих криптографічних схем

Критерій	Базова схема (AES-256 + ECDH + SHA-3)	Гібридна схема (AES-256 + Kyber-768 + SHA-3)	Запропонована схема (AES-256 + Kyber-768 + RS + SHA-3)
Класична стійкість (l_0)	568 біт (AES) / 128 біт (ECDH)	568 біт (AES) + постквантова (Kyber)	568 біт (AES) + постквантова (Kyber)
Постквантова стійкість обміну ключами	Відсутня (злам Шором)	Присутня (стійкість на ґратках)	Присутня (стійкість на ґратках)
Ефективна довжина ключа після Гровера	128 біт (AES)	128 біт (AES) + постквантовий захист	128 біт (AES) + постквантовий захист
Цілісність даних	Виявлення помилок (SHA-3), без виправлення	Виявлення помилок (SHA-3), без виправлення	Виявлення (SHA-3) + виправлення до 16 байт на блок (RS)
Обчислювальна складність	~226 000	~206 000	~221 000
Накладні витрати (overhead)	0% (базова точка відліку)	~5% (більший розмір ключів Kyber)	~14,3% (RS) + ~5% (Kyber) ≈ 19,3%

Час встановлення сеансу	~1,0 мс	~1,2 мс	~1,5 мс
Готовність до стандартизації	Поточна	NIST FIPS-203 (2024)	NIST FIPS-203 + додатковий рівень
Адаптивність до нових загроз	Низька	Середня (можливість заміни Kyber)	Висока (модульна архітектура)

Принципово важливою характеристикою запропонованої схеми є її модульна архітектура, яка забезпечує адаптивність до нових загроз. Кожен компонент схеми (симетричний шифр, механізм обміну ключами, алгоритм забезпечення цілісності, завадостійкий код) може бути незалежно замінений на більш сучасний без порушення загальної структури. Це дозволяє реалізувати поетапне нарощування рівня захисту: від базової схеми через гібридну до повної конфігурації із завадостійким кодуванням, а в перспективі замінити окремі компоненти на ще більш досконалі алгоритми в міру їх стандартизації.

Кількісні оцінки підтверджують, що запропонований підхід забезпечує підвищення стійкості криптографічного захисту одночасно за трьома напрямами: усунення квантової вразливості каналу обміну ключами, додавання функції виправлення помилок та збереження прийнятної продуктивності.

4.5 Підхід до поетапного вдосконалення криптографічного захисту в банківських мережах

Результати порівняльного аналізу, проведеного в попередньому підрозділі, засвідчили, що жоден окремо взятий алгоритм не здатен задовольнити весь комплекс вимог до криптографічного захисту банківських мереж в умовах сучасних і перспективних загроз. Симетричні шифри, такі як Rijndael-256 та Калина-256, забезпечують високу класичну стійкість, однак

вимагають захищеного каналу обміну ключами, вразливого до квантових атак. Постквантові алгоритми на кшталт Kyber закривають цю вразливість, проте не вирішують проблему цілісності даних під час активних атак на канал передачі. Нарешті, класичні механізми хешування лише виявляють пошкодження, але не виправляють їх. Зазначене протиріччя зумовлює потребу в новому підході, який не зводився б до вибору одного «найкращого» алгоритму, а пропонував би архітектурне рішення, здатне об'єднати сильні сторони різних типів криптографічних механізмів у єдиній адаптивній системі.

Пропонований підхід ґрунтується на трьох ключових принципах: модульності, багаторівневості та криптографічної гнучкості. Модульність означає, що система криптографічного захисту розглядається як сукупність незалежних функціональних блоків: симетричного шифрування, обміну ключами, контролю цілісності та завадостійкого кодування, кожен із яких може бути замінений або модернізований без порушення функціонування решти системи. Багаторівневість передбачає, що ці блоки утворюють ієрархію захисту, де компрометація одного рівня не призводить до повної втрати безпеки. Криптографічна гнучкість забезпечує можливість швидкої заміни будь-якого алгоритму в разі виявлення вразливостей або появи нових стандартів без зупинки банківських сервісів.

Архітектурно підхід реалізується у вигляді трьох послідовних рівнів захисту, які можуть бути впроваджені поетапно, без необхідності одномоментної заміни всієї криптографічної інфраструктури:

1. **Базовий рівень**. Відповідає поточному стану банківських систем і включає симетричне шифрування (AES-256 або Калина-256) у поєднанні з класичним обміном ключами на еліптичних кривих (ECDH) та хеш-функцією для контролю цілісності. Цей рівень забезпечує достатню стійкість проти класичних атак, однак є вразливим до квантового криптоаналізу в частині обміну ключами та не здатен виправляти пошкоджені дані.

2. **Гібридний рівень.** Передбачає заміну або доповнення класичного обміну ключами постквантовим алгоритмом. При цьому симетричний шифр залишається незмінним, що є принципово важливим: модернізація торкається лише найуразливішої ланки, не вимагаючи перебудови всієї системи. Як показав аналіз у підрозділі 4.3, інтеграція Kyber-768 забезпечує постквантову стійкість каналу обміну ключами без збільшення обчислювального навантаження порівняно з базовою схемою. Технічно це реалізується шляхом використання гібридного обміну ключами: сеансовий ключ формується як результат комбінування (наприклад, через конкатенацію та хешування) секретних ключів, отриманих від класичного ECDH та постквантового Kyber. Такий підхід гарантує, що навіть у разі компрометації одного з алгоритмів у майбутньому другий продовжить забезпечувати конфіденційність.
3. **Повний рівень**. Цей рівень додатково інтегрує завадостійке кодування як засіб не лише виявлення, а й виправлення помилок, спричинених атаками на канал передачі або технічними збоями. Використання коду Ріда-Соломона, дозволяє гарантовано виправляти до 16 байтових помилок на кожні 223 байти корисних даних. Він може бути впроваджений незалежно від двох попередніх, залежно від конкретних вимог до надійності каналу та допустимих накладних витрат.

Для кількісної оцінки практичної прийнятності запропонованого підходу на рисунку 4.3 наведено залежність накладних витрат від розміру корисного навантаження для трьох схем: базової (AES-GCM), гібридної (AES + ML-KEM-768) та повної (AES + ML-KEM-768 + RS(255,223)). Як видно з графіка, для малих пакетів (64–256 байт) повна схема з кодом Ріда-Соломона дає 16–18% overhead, однак вже від 1 КБ він знижується нижче 15%, а від 4 КБ – нижче 14,5%, що є цілком прийнятним для банківських транзакційних даних.

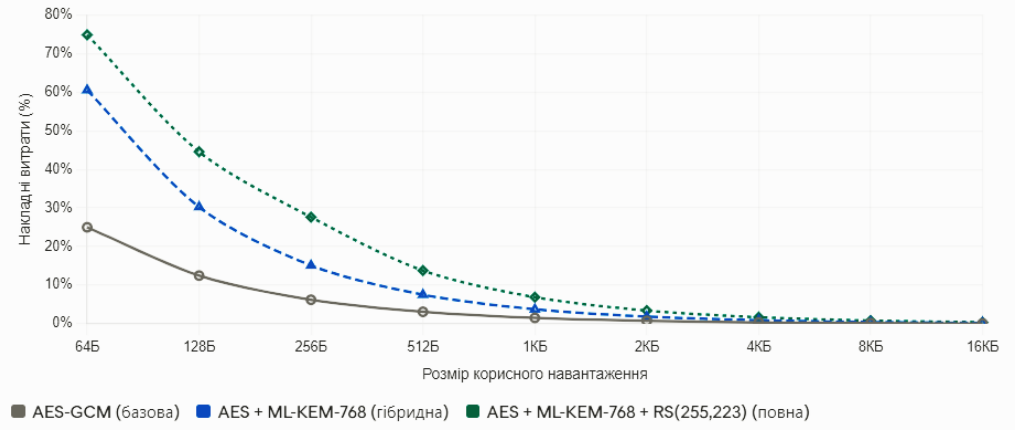

Рисунок 4.3 – Залежність накладних витрат від розміру корисного навантаження

Отже, збільшення накладних витрат є керованим і прогнозованим, а не критичним обмеженням, що підтверджує практичну реалізованість поетапного підходу без суттєвого погіршення продуктивності банківської телекомунікаційної мережі.

Важливо підкреслити, що запропонований підхід не прив'язаний до конкретного постквантового алгоритму. Хоча в якості прикладу в роботі розглянуто Kyber-768 як стандартизований NIST алгоритм, модульна архітектура дозволяє замінити його на будь-який інший механізм інкапсуляції ключа, що відповідає визначеному інтерфейсу. Це може бути як інший алгоритм на ґратках, так і алгоритм з іншої математичної родини, наприклад, на кодах або на основі хеш-функцій, щойно він отримає відповідний статус стандартизації та підтвердить прийнятні показники продуктивності.

Практична реалізація підходу в банківській інфраструктурі може відбуватися шляхом поступового оновлення криптографічних бібліотек на серверах, у VPN-шлюзах та на клієнтських пристроях. На першому етапі достатньо додати підтримку гібридного обміну ключами в TLS-з'єднаннях, що вже передбачено сучасними версіями криптографічних бібліотек з відкритим кодом. На другому етапі вмикається завадостійке кодування для найбільш критичних каналів, таких як міжбанківські розрахунки або зв'язок із центральним банком. Усі зміни є зворотно сумісними: системи, які ще не

пройшли модернізацію, продовжують працювати за класичними схемами, тоді як оновлені вузли використовують посилений захист.

Таким чином, запропонований підхід забезпечує принципово новий рівень захищеності банківської мережі при прийнятних витратах на модернізацію: overhead не перевищує 19% навіть для найменших пакетів і знижується до 14,5% для типового банківського трафіку, а збільшення часу встановлення сеансу до 1,5 мс є несуттєвим в контексті допустимих затримок 100–200 мс. Водночас система отримує дві властивості, яких не має жодна з існуючих схем окремо: стійкість до квантового криптоаналізу в частині обміну ключами та здатність виправляти пошкоджені пакети без повторної передачі.

4.6 Висновки до четвертого розділу

У розділі проведено комплексний аналіз продуктивності та стійкості класичних і постквантових криптографічних алгоритмів для банківських телекомунікаційних мереж. Головним підсумком стало обґрунтування модульного підходу до поетапного підвищення захисту.

Аналіз продуктивності (рис. 4.1) показав, що алгоритми серії ML -KEM тоді як Classic McEliece через час генерації ключа в десятки секунд є непридатним для банківських систем. Оцінка постквантової стійкості (рис. 4.2) засвідчила, що RSA та ECDH мають нульовий захист проти квантових атак, натомість ML -KEM AES -192 таAES-256.

Порівняння комбінованих схем (табл. 4.3) показало, що базова схема з ECDH є вразливою до алгоритму Шора, гібридна схема з Kyber -768 у цю проблему, а запропонована схема з додаванням коду Ріда -Соло дозволяє не лише виявляти, а й виправляти помилки. Накладні витрати близько 19% та зростання часу встановлення сеансу до 1,5 мс є прийнятними,

оскільки критичний поріг затримки для банківських транзакцій становить 100 -200 мс

Розроблений підхід ґрунтується на трьох принципах: модульності, багаторівневості та криптографічної гнучкості. Аналіз залежності накладних витрат від розміру пакета (рис. 4.3) показав, що для пакетів від 1 КБ вони становлять менше 15%, що робить схему практично придатною.

Запропонований підхід забезпечує адаптивне нарощування рівня криптографічного захисту банківських телекомунікаційних мереж шляхом поетапної інтеграції постквантового обміну ключами та завадостійкого кодування в існуючі схеми симетричного шифрування, а модульна архітектура гарантує довготривалу актуальність рішення в умовах постійної еволюції кіберзагроз і криптографічних стандартів.

ЗАГАЛЬНІ ВИСНОВКИ

У дипломній роботі розв'язано актуальне науково-практичне завдання підвищення стійкості криптографічного захисту інформації в банківських мережах в умовах зростання інтенсивності кіберзагроз та розвитку постквантових методів криптоаналізу.

У першому розділі виконано аналіз нормативно-правової бази забезпечення інформаційної безпеки банківських установ України, розглянуто загальні принципи організації захисту інформації та визначено вимоги до криптографічного захисту в банківських телекомунікаційних системах. Встановлено, що вимоги до криптографічного захисту формуються на перетині нормативно-правових, технічних та організаційних чинників, а застосування сертифікованих алгоритмів шифрування, апаратних засобів захисту ключової інформації та механізмів наскрізного шифрування створює необхідне підґрунтя для зниження ризиків витоку даних і забезпечення належного рівня стійкості мережевої інфраструктури банківської установи до актуальних кіберзагроз.

У другому розділі розглянуто теоретичні засади криптографічного захисту інформації в банківських телекомунікаційних мережах. Систематизовано класифікацію атак на криптографічні системи за типом вразливості, кінцевою метою зловмисника та ознаками виявлення. Визначено формальні критерії оцінки криптографічної стійкості, розглянуто принципи побудови симетричних, асиметричних і гібридних шифрів, які становлять основу сучасних засобів захисту інформації. Встановлено, що гібридні криптографічні схеми, реалізовані в протоколах TLS та IPsec, є основним практичним механізмом захисту банківських комунікацій, а подальший розвиток таких схем пов'язаний із впровадженням постквантових криптографічних алгоритмів.

У третьому розділі проведено порівняльний аналіз характеристик алгоритмів шифрування та забезпечення цілісності даних. Виявлено чотири системні обмеження існуючих підходів до криптографічного захисту банківських мереж: застарілість алгоритмів із недостатньою довжиною ключа, неадекватність оцінки стійкості до сучасних методів криптоаналізу, обмеженість механізмів забезпечення цілісності даних лише функцією виявлення помилок та незахищеність каналу обміну ключами від квантових атак. За результатами аналізу симетричних алгоритмів встановлено, що найкращий баланс між криптографічною стійкістю та обчислювальною складністю забезпечують Rijndael-256 та Калина-256. Аналіз алгоритмів забезпечення цілісності показав, що найкращі показники ймовірності обману демонструють SHA-3 та «Калина» в режимі MAC, однак усі вони обмежені лише виявленням пошкоджень, що обґрунтовує доцільність доповнення криптографічної схеми механізмами завадостійкого кодування.

У четвертому розділі проведено комплексний аналіз продуктивності та стійкості класичних і постквантових криптографічних алгоритмів для банківських телекомунікаційних мереж. Аналіз продуктивності показав, що алгоритми серії ML-KEM суттєво перевищують класичні аналоги за швидкістю операцій, тоді як Classic McEliece через значний час генерації ключа виявився непридатним для банківських систем. Оцінка постквантової стійкості засвідчила, що RSA та ECDH не мають захисту проти квантових атак, натомість ML-KEM забезпечує рівні безпеки, еквівалентні AES-128, AES-192 та AES-256. Порівняння комбінованих схем показало, що базова схема з ECDH є вразливою до алгоритму Шора, гібридна схема з Kyber-768 усуває цю проблему, а запропонована схема з додаванням коду Ріда-Соломона дозволяє не лише виявляти, а й виправляти помилки. Розроблений підхід ґрунтується на трьох принципах: модульності, багаторівневості та криптографічної гнучкості, і передбачає три послідовні рівні впровадження: базовий (AES-256 + ECDH + SHA-3), гібридний (AES-256 + Kyber-768 + SHA-3) та повний (AES-256 + Kyber-768 + RS + SHA-3). Оцінка ефективності

показала, що перехід від базової до повної схеми супроводжується збільшенням часу встановлення сеансу з 1,0 до 1,5 мс та накладними витратами близько 19%, що є цілком прийнятним для банківських застосувань, де типовий поріг допустимої затримки становить 100-200 мс.

У результаті виконання роботи досягнуто поставленої мети – підвищення стійкості криптографічного захисту інформації в банківських телекомунікаційних мережах до сучасних та постквантових загроз шляхом створення підходу до поетапного нарощування рівня захисту існуючих криптографічних схем. Практичне значення отриманих результатів полягає в можливості безпосереднього застосування запропонованого підходу для поетапної модернізації криптографічного захисту в діючих банківських мережах без зупинки бізнес-процесів. Отримані кількісні оцінки продуктивності дозволяють обґрунтовано планувати бюджет модернізації та визначати пріоритетність оновлення окремих компонентів інфраструктури. Модульна структура підходу забезпечує його відповідність принципу криптографічної гнучкості, що є обов'язковою вимогою сучасних регуляторних стандартів, зокрема DORA та рекомендацій NIST.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Schneier B. Crypto-Gram Newsletter, May 15, 2000 [Електронний ресурс]. – Режим доступу: https://www.schneier.com/crypto-gram/archives/2000/0515.html
2. National Institute of Standards and Technology (NIST). NIST Releases First 3 Finalized Post-Quantum Encryption Standards [Електронний ресурс]. – Режим доступу: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
3. HSBC Holdings plc. HSBC explores the application of quantum-secure technology for buying and selling tokenised physical gold [Електронний ресурс]. – Режим доступу: https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-explores-the-application-of-quantum-secure-technology-for-buying-and-selling-tokenised-physical-gold
4. JPMorgan Chase & Co. JPMorgan and partners demonstrate a quantum-secure 100 Gbps network in Singapore [Електронний ресурс]. – Режим доступу: https://www.jpmorgan.com/technology/technology-blog/qcna-singapore-quantum-network
5. Національний банк України. Операції з платіжними картками у 2025 році: більшість – безготівкові. 2025. URL: https://bank.gov.ua/ua/news/all/operatsiyi-z-platijnimi-kartkami-u-2025-rotsi-bilshist--bezgotivkovi
6. Юридична газета. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: якими були атаки. 2025. URL: https://yur-gazeta.com/golovna/certua-u-2025-roci-opracyuvala-mayzhe-6000-kiberincidentiv-yaki-buli-ataki.html
7. European Parliament and Council of the European Union. Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). Official Journal of the European Union. 2022. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

8. Про Національний банк України : Закон України від 20.05.1999 № 679-XIV // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/679-14
9. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80
10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19
11. Національний банк України. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова Правління НБУ від 28.09.2017 № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17
12. Національний банк України. Про затвердження Положення про організацію кіберзахисту в банківській системі України : Постанова Правління НБУ від 12.08.2022 № 178. URL: https://zakon.rada.gov.ua/laws/show/v0178500-22
13. Національний банк України. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг : Постанова Правління НБУ від 09.12.2025 № 143. URL: https://bank.gov.ua/ua/legislation/Resolution_09122025_143
14. International Organization for Standardization. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva : ISO, 2022. URL: https://www.iso.org/standard/27001
15. International Organization for Standardization. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information

security controls. Geneva : ISO, 2022. URL: https://www.iso.org/standard/27002

16. International Organization for Standardization. ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary. Geneva : ISO, 2018. URL: https://www.iso.org/standard/73906.html
17. Qadir, S. and Quadri, S. (2016) Information Availability: An Insight into the Most Important Attribute of Information Security. Journal of Information Security, 7, 185-194. doi: 10.4236/jis.2016.73014.
18. Васильчак С. В., Жидяк О. Р. Економічна безпека банку та інструменти її забезпечення. Науковий вісник НЛТУ України. 2015. Т. 25, № 12. С. 222–227. URL: https://nv.nltu.edu.ua
19. Scarfone K., Hoffman P. Guidelines on Firewalls and Firewall Policy. NIST Special Publication 800-41 Revision 1. National Institute of Standards and Technology, 2009. URL: https://doi.org/10.6028/NIST.SP.800-41r1
20. Wack J., Cutler K., Pole J. Guidelines on Firewalls and Firewall Policy. NIST Special Publication 800-41. National Institute of Standards and Technology, 2002.
21. Rushadi S. Konsep Keamanan Jaringan Komputer dengan Infrastruktur Demilitarized Zone. 2018. URL: https://www.researchgate.net/publication/328130248_Konsep_Keamanan_Jaringan_Komputer_dengan_Infrastruktur_Demilitarized_Zone
22. Державна служба спеціального зв'язку та захисту інформації України. Система управління інформаційною безпекою (СУІБ). URL: https://cip.gov.ua/ua/news/sistema-upravlinnya-informaciinoyu-bezpekoyu-suib
23. European Union Agency for Cybersecurity (ENISA). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. Athens : ENISA, 2021. URL: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

24. Про затвердження Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи : Постанова Національного банку України; Правила від 04.07.2007 № 243 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/z0955-07
25. Грицюк П. Ю., Грицюк Ю. І. Особливості захисту електронних платіжних систем у мережі Інтернет. Науковий вісник НЛТУ України. 2013. Вип. 23.10. С. 314–331.
26. Ometov A., Bezzateev S., Mäkinen J., Andreev S., Mikkonen T., Koucheryavy Y. Multi-Factor Authentication: A Survey. Cryptography. 2018. Vol. 2, no. 1. Article 1. URL: https://doi.org/10.3390/cryptography2010001
27. National Institute of Standards and Technology. SP 800-125B. Secure Virtual Network Configuration for Virtual Machine (VM) Protection. Gaithersburg : NIST, 2020. URL: https://doi.org/10.6028/NIST.SP.800-125B
28. Про затвердження Положення про використання електронного підпису та електронної печатки : Постанова Національного банку України; Положення, Стандарт від 20.12.2023 № 172 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/v0172500-23
29. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Internet Engineering Task Force, 2018. URL: https://doi.org/10.17487/RFC8446
30. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg : National Institute of Standards and Technology, 2020. URL: https://doi.org/10.6028/NIST.SP.800-207
31. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. Boca Raton : CRC Press, 1996.
32. Daemen J., Rijmen V. The Design of Rijndael: AES – The Advanced Encryption Standard. Berlin : Springer, 2002. URL: https://doi.org/10.1007/978-3-662-04722-4

33. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Harlow : Pearson, 2023.
34. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Berlin : Springer, 2010.
35. Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем : Постанова Кабінету Міністрів України; Вимоги від 29.03.2006 № 373 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/373-2006-%D0%BF
36. Barker E. Recommendation for Key Management. NIST Special Publication 800-57 Part 1 Rev. 5. Gaithersburg : NIST, 2020. URL: https://doi.org/10.6028/NIST.SP.800-57pt1r5
37. European Union Agency for Cybersecurity (ENISA). ECCG Agreed Cryptographic Mechanisms, Version 2 [Електронний ресурс]. – Brussels: ENISA, 2023. – Режим доступу: https://certification.enisa.europa.eu/document/download/a845662b-aee0-484e-9191-890c4cfa7aaa_en.
38. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. New York : Springer, 2004. URL: https://doi.org/10.1007/b97644
39. Theefipe. SecureComm: A Deep Dive into Dynamic Key Exchange, End-to-End Encryption and ML-Powered Intrusion Detection. Medium, 2024.
40. Barker E., Chen L., Roginsky A., Vassilev A., Davis R. Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. NIST Special Publication 800-56A Rev. 3. Gaithersburg : National Institute of Standards and Technology, 2018. URL: https://doi.org/10.6028/NIST.SP.800-56Ar3
41. National Institute of Standards and Technology. Digital Signature Standard (DSS). FIPS PUB 186-5. Gaithersburg : NIST, 2023. URL: https://doi.org/10.6028/NIST.FIPS.186-5

42. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Internet Engineering Task Force (IETF), 2018. 160 p.
43. National Institute of Standards and Technology. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). Gaithersburg : NIST, 2024. URL: https://doi.org/10.6028/NIST.FIPS.203
44. National Institute of Standards and Technology. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). Gaithersburg : NIST, 2024. URL: https://doi.org/10.6028/NIST.FIPS.203
45. Stevens M., Bursztein E., Karpman P., Albertini A., Markov Y. The First Collision for Full SHA-1. In: Advances in Cryptology – CRYPTO 2017. Lecture Notes in Computer Science. Vol. 10401. Cham : Springer, 2017. P. 570–596. URL: https://doi.org/10.1007/978-3-319-63688-7_19
46. Shor P. W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS). Santa Fe, New Mexico, 1994. P. 124–134. URL: https://doi.org/10.1109/SFCS.1994.365700
47. Chen L., Jordan S., Liu Y.-K., Moody D., Peralta R., Perlner R., Smith-Tone D. Report on Post-Quantum Cryptography. NIST Interagency Report 8105. Gaithersburg : National Institute of Standards and Technology, 2016. URL: https://doi.org/10.6028/NIST.IR.8105
48. National Institute of Standards and Technology. Transition to Post-Quantum Cryptography Standards. NIST, 2024. URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
49. European Telecommunications Standards Institute (ETSI). Quantum-Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges. ETSI White Paper No. 8. 2015. URL: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

50. National Institute of Standards and Technology. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). Gaithersburg : NIST, 2024. URL: https://doi.org/10.6028/NIST.FIPS.203
51. National Institute of Standards and Technology. FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA). Gaithersburg : NIST, 2024. URL: https://doi.org/10.6028/NIST.FIPS.204
52. National Institute of Standards and Technology. FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA). Gaithersburg : NIST, 2024. URL: https://doi.org/10.6028/NIST.FIPS.205
53. European Telecommunications Standards Institute. ETSI TS 104 015 V1.1.1. Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies. Sophia Antipolis : ETSI, 2025.
54. European Parliament and the Council of the European Union. Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
55. European Parliament and the Council of the European Union. Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector (DORA). Official Journal of the European Union. 2022. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj
56. Open Quantum Safe. ML-KEM. Open Quantum Safe Project. 2025. URL: https://openquantumsafe.org/liboqs/algorithms/kem/ml-kem.html
57. Calomel.org. AES-NI SSL Performance Study. 2024. URL: https://calomel.org/aesni_ssl_performance.html