МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

(повна назва випускної кафедри)

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

ГІБРИДНІ КРИПТОГРАФІЧНІ СИСТЕМИ ДЛЯ ЗАХИСТУ ДАНИХ У ХМАРНИХ СЕРЕДОВИЩАХ

Виконав:

студент групи 1*КІ-23* зі спеціальності

123 – «Комп'ютерна інженерія»

Валерій БОНДАР

Науковий керівник:

к.т.н Роксолана БРЕУС

(науковий ступінь, вчене звання, прізвище та ініціали)

Черкаси, 2025

АНОТАЦІЯ

У роботі розглядаються особливості застосування гібридних криптографічних систем для захисту даних у хмарних середовищах. Проведено аналіз основних моделей хмарних обчислень та загроз безпеки, а також порівняльний огляд симетричних і асиметричних алгоритмів шифрування.

Детально досліджено існуючі гібридні криптографічні підходи на прикладі провідних хмарних платформ (Google, AWS, Microsoft Azure) та нормативні вимоги до криптографії в хмарі.

Запропоновано рекомендації щодо вибору і впровадження гібридних схем залежно від типу даних і архітектури хмари, а також організації управління ключами з урахуванням ризиків.

Проведено моделювання логічної структури гібридної криптосистеми, порівняльний аналіз алгоритмів за ключовими критеріями, а також SWOT-аналіз для оцінки сильних та слабких сторін підходу. Розроблені рекомендації адаптовані для різних типів організацій з урахуванням їхніх потреб та технічних можливостей.

Ключові слова: ГІБРИДНА КРИПТОГРАФІЯ, ХМАРНІ СЕРЕДОВИЩА, УПРАВЛІННЯ КЛЮЧАМИ, КРИПТОГРАФІЧНІ АЛГОРИТМИ, БЕЗПЕКА ДАНИХ, ХМАРНА АРХІТЕКТУРА, SWOT-АНАЛІЗ, РЕГУЛЯТОРНІ ВИМОГИ.

ABSTRACT

This work examines the features of hybrid cryptographic systems application for data protection in cloud environments. It includes an analysis of fundamental cloud computing models and security threats, as well as a comparative review of symmetric and asymmetric encryption algorithms.

Existing hybrid cryptographic approaches are studied in detail based on leading cloud platforms (Google, AWS, Microsoft Azure) and regulatory requirements for cloud cryptography.

Recommendations are proposed for selecting and implementing hybrid schemes depending on data type and cloud architecture, as well as key management organization considering associated risks.

Logical modeling of the hybrid cryptosystem structure, comparative algorithm analysis by key criteria, and SWOT analysis to evaluate strengths and weaknesses of the approach are presented. Recommendations are tailored for various types of organizations, taking into account their needs and technical capabilities.

Keywords: HYBRID CRYPTOGRAPHY, CLOUD ENVIRONMENTS, KEY MANAGEMENT, CRYPTOGRAPHIC ALGORITHMS, DATA SECURITY, CLOUD ARCHITECTURE, SWOT ANALYSIS, REGULATORY REQUIREMENTS.

ЗМІСТ

ВСТУП

У сучасному цифровому світі хмарні обчислення (cloud computing) стали одним із ключових інструментів зберігання, обробки та доступу до даних. Хмарні сервіси широко використовуються як у бізнесі, так і в державному секторі, оскільки забезпечують високу масштабованість, гнучкість та економічну доцільність. Однак разом із перевагами зростає і рівень загроз, пов’язаних із безпекою конфіденційної інформації, що передається, обробляється або зберігається у хмарі.

Одним з основних механізмів забезпечення захисту даних є криптографія. Проте, з огляду на різні обмеження і вимоги до захисту інформації у хмарному середовищі, використання лише одного типу криптографії – симетричної або асиметричної – виявляється недостатньо ефективним. У відповідь на ці виклики з’явилися гібридні криптографічні системи, які поєднують переваги обох підходів: швидкість симетричного шифрування та надійність асиметричних алгоритмів для захисту ключів.

Гібридні криптосистеми особливо актуальні в умовах хмарних технологій, де необхідно забезпечити як конфіденційність, так і цілісність, автентичність та керування ключами в середовищі з обмеженим рівнем довіри. Вони дозволяють розв’язати низку проблем, пов’язаних із відкритими каналами зв’язку, обмеженим доступом до інфраструктури шифрування та необхідністю масштабованості криптографічного захисту.

Актуальність теми зумовлена зростаючим обсягом чутливих даних, які передаються та зберігаються у хмарних середовищах, а також зростанням кількості витоків інформації внаслідок кібератак. Застосування гібридних криптографічних рішень є одним із найперспективніших напрямів у сфері інформаційної безпеки, оскільки дає змогу підвищити рівень захисту без значного зниження продуктивності або зручності використання сервісів.

Метою даної роботи є дослідження принципів функціонування гібридних криптографічних систем, аналіз їх ефективності в хмарному середовищі та обґрунтування доцільності їх впровадження для захисту даних.

Для досягнення мети у роботі поставлено такі завдання:

- провести огляд теоретичних основ симетричної, асиметричної та гібридної криптографії;
- дослідити архітектуру хмарних середовищ та специфіку загроз, пов’язаних із безпекою даних;
- проаналізувати існуючі гібридні криптографічні рішення, які використовуються в хмарних платформах;
- змоделювати принцип роботи гібридної криптосистеми у типових хмарних сценаріях;
- здійснити порівняльну оцінку ефективності гібридних систем у контексті захисту даних у хмарі.

Об’єктом дослідження є захист даних у хмарних обчислювальних середовищах.

Предметом дослідження є гібридні криптографічні методи, що використовуються для шифрування даних і захисту ключів у хмарних платформах.

Практична значимість роботи полягає у можливості застосування її результатів для побудови ефективних систем захисту даних в умовах хмарних інфраструктур, а також у формуванні рекомендацій щодо вибору оптимальних криптографічних рішень залежно від особливостей використання хмарних сервісів.

РОЗДІЛ 1 ОСОБЛИВОСТІ КРИПТОГРАФІЧНОГО ЗАХИСТУ В ХМАРНИХ СЕРЕДОВИЩАХ

1.1 Основні поняття хмарних обчислень і моделі надання послуг (IaaS, PaaS, SaaS)

У сучасних умовах цифрової трансформації однією з ключових технологій, що забезпечують ефективне використання інформаційних ресурсів та сприяють розвитку цифрової економіки, є хмарні обчислення. Ця технологія формує основу сучасної IT-інфраструктури, надаючи можливість масштабованого, економічно ефективного та гнучкого доступу до обчислювальних ресурсів за моделлю «на вимогу» через мережу Інтернет [1]. Хмарні сервіси дозволяють організаціям зменшити витрати на підтримку та модернізацію локальних IT-систем, оптимізувати управління ресурсами, пришвидшити розгортання програмного забезпечення та впровадження інновацій у бізнес-процеси.

Згідно з визначенням Національного інституту стандартів і технологій США (NIST), хмарні обчислення (cloud computing) – це модель забезпечення універсального, зручного та оперативного мережевого доступу до спільного пулу конфігурованих обчислювальних ресурсів (зокрема, серверів, сховищ, мереж, програмних продуктів та служб), які можуть бути оперативно виділені та звільнені з мінімальними адміністративними зусиллями або взаємодією з постачальником послуг. Така модель забезпечує високу еластичність, адаптивність і масштабованість, що робить її особливо привабливою для організацій різного типу – від малих підприємств до транснаціональних корпорацій.

Відповідно до визначення Національного інституту стандартів і технологій США (NIST), хмарні обчислення мають п’ять основних характеристик [2]:

- самообслуговування на вимогу (on-demand self-service),

- широкий мережевий доступ (broad network access),
- об'єднання ресурсів (resource pooling),
- швидка еластичність (rapid elasticity),
- вимірюваність послуг (measured service).

У хмарних обчисленнях виділяють три основні моделі надання послуг, зокрема:

- IaaS – інфраструктура як послуга,
- PaaS – платформа як послуга,
- SaaS – програмне забезпечення як послуга.

Ці моделі відрізняються ступенем контролю, який отримує користувач, а також відповідальністю за обслуговування IT-компонентів.

Модель IaaS передбачає надання в оренду базових обчислювальних ресурсів: віртуальних машин, сховищ даних, мережевої інфраструктури тощо. Користувач має повний контроль над операційною системою, налаштуваннями середовища, програмним забезпеченням та безпекою на рівні ОС. До них належать: Amazon EC2, Microsoft Azure Virtual Machines, Google Compute Engine [3].

Переваги даної моделі полягають у наступних характеристиках:

- максимальна гнучкість і масштабованість;
- повний контроль над обчислювальним середовищем;
- можливість використання індивідуальних конфігурацій.

Недоліками виступають наступні чинники:

- необхідність глибокої технічної компетентності,
- відповідальність користувача за оновлення, безпеку та адміністрування.

PaaS – це модель, яка надає користувачу платформу для розробки, тестування та розгортання додатків. Усі нижчі рівні (інфраструктура, ОС, системи управління базами даних, середовища виконання) обслуговуються провайдером, а користувач працює лише з кодом додатка. Досить поширеними

прикладами можуть такі як, Google App Engine, Heroku, Microsoft Azure App Service [4].

Серед переваг можна виділити такі як швидке розгортання додатків без витрат на інфраструктуру, автоматичне масштабування, зменшення часу виходу продукту на ринок (time-to-market). А серед недоліків слід виділити обмеження у налаштуванні середовища, залежність від платформи провайдера (vendor lock-in).

SaaS – це модель, у якій користувач отримує повністю готове до використання програмне забезпечення, що працює у хмарі. Користувач не має доступу до керування інфраструктурою або платформою і взаємодіє лише з функціональністю додатка через інтерфейс (Google Workspace, Microsoft 365, Dropbox, Zoom) [5]. Серед їх переваг – відсутність потреби в інсталяції та обслуговуванні ПЗ, автоматичні оновлення та підтримка, швидкий доступ із будь-якого пристрою, а недоліки – обмежена можливість кастомізації, залежність від хмарного провайдера і його політики безпеки. Порівняльна характеристика моделей в залежності від певних критеріїв наведена в табл.1.1.

Таблиця 1.1 – Порівняльна характеристика моделей в залежності від певних критеріїв

№	Критерій	IaaS	PaaS	SaaS
1	Рівень контролю	Високий	Середній	Низький
2	Цільова аудиторія	Адміністратори, DevOps	Розробники	Кінцеві користувачі
3	Відповідальність клієнта	ОС, ПЗ, середовище	Код додатка	Лише використання ПЗ
4	Приклади	AWS EC2, Azure VMs	Heroku, Google App Engine	Gmail, Office 365

1.2 Загрози та проблеми безпеки в хмарному середовищі

Хмарні обчислення, хоча й забезпечують численні переваги, зокрема масштабованість, гнучкість, високу доступність та ефективне використання

ресурсів, водночас створюють нові виклики у сфері кібербезпеки. Перехід даних, сервісів та обчислювальних процесів із контрольованого локального середовища до хмари, яка обслуговується стороннім провайдером, знижує рівень прямого контролю користувача над обробкою та зберіганням інформації. У результаті цього виникає спектр специфічних загроз і вразливостей, що охоплюють як технічні аспекти інфраструктури, так і організаційні обмеження та прогалини в політиках безпеки.

До основних технічних загроз належать несанкціонований доступ до даних, що може бути спричинений конфігураційними помилками або недостатньо надійною автентифікацією, витоки даних через багатокористувацьке середовище або загальні ресурси віртуалізації, атаки типу «людина посередині» та перехоплення трафіку у випадках незахищених каналів зв’язку, використання вразливостей у гіпервізорах і платформах управління віртуалізацією, що створює загрозу ескалації привілеїв, а також атаки типу відмови в обслуговуванні (DDoS), які можуть порушити доступність хмарного сервісу.

З організаційної точки зору критичними є недостатня прозорість хмарних провайдерів щодо реалізації заходів безпеки та розміщення даних, нечіткий розподіл відповідальності між клієнтом і постачальником послуг, що ускладнює реагування на інциденти, несумісність деяких практик хмарних операторів із чинними нормативними вимогами, такими як GDPR чи ISO/IEC 27001, а також людський фактор, включаючи як ненавмисні помилки персоналу, так і навмисні порушення встановлених правил доступу.

Окрему проблему становлять питання забезпечення конфіденційності, цілісності та доступності даних у всіх фазах їхнього життєвого циклу – зберігання, передавання та обробки. Значне значення має також управління криптографічними ключами, автентифікація користувачів, контроль доступу та фіксація подій безпеки у розподіленому середовищі. Особливої актуальності набувають загрози, пов’язані зі збереженням конфіденційної

інформації у публічних хмарах, а також забезпечення безперервності бізнес-процесів у разі порушення роботи хмарної інфраструктури.

Таким чином, впровадження хмарних технологій повинно супроводжуватися детальним аналізом ризиків, дотриманням міжнародних стандартів інформаційної безпеки та впровадженням сучасних технологічних засобів захисту. Одним із ключових інструментів протидії загрозам у хмарному середовищі виступає криптографічний захист, зокрема гібридні криптографічні системи, які поєднують переваги симетричних та асиметричних алгоритмів і забезпечують належний рівень захисту даних в умовах динамічного хмарного середовища [6].

У загальному розгляді, загрози безпеці в хмарному середовищі можна класифікувати за кількома напрямами:

- загрози конфіденційності даних;
- загрози цілісності та доступності;
- загрози на рівні віртуалізації;
- загрози доступу та автентифікації;
- юридичні та нормативні ризики.

Серед основних типів загроз можна виділити наступні:

1. Несанкціонований доступ до даних до даних, що зберігаються у хмарі. Атаки можуть здійснюватися як з боку зовнішніх загроз (хакери, ботмережі), так і з боку внутрішніх користувачів (інсайдерів), які мають надлишкові привілеї (атака на iCloud у 2014 році, унаслідок якої були зламані акаунти знаменитостей через слабку автентифікацію) [7].

2. Порушення ізоляції віртуальних середовищ (VM Escape / VM Hopping), оскільки хмарна інфраструктура використовує віртуалізацію для поділу ресурсів між клієнтами, існує ризик порушення ізоляції. Зловмисник може використати вразливості гіпервізора для переходу з однієї віртуальної машини на іншу. Загроза multi-tenancy вимагає особливих заходів безпеки, оскільки кілька клієнтів використовують одну фізичну інфраструктуру.

3. Атаки типу «людина посередині» – у хмарних обчисленнях передача даних зазвичай здійснюється через відкриті мережі, що створює ризик перехоплення трафіку. Без належного шифрування зловмисники можуть отримати доступ до конфіденційної інформації під час її передачі. Механізмами захисту в даному випадку виступає використання протоколів TLS/SSL, VPN, IPsec.

4. Недостатній контроль і управління доступом – помилки в налаштуванні політик доступу можуть дозволити користувачам отримати доступ до критично важливої інформації або систем. Особливо небезпечні ситуації, коли облікові записи мають права адміністратора без двофакторної автентифікації. Найкращий вибір – застосування принципу найменших привілеїв (PoLP), мультифакторної автентифікації (MFA).

5. Вразливості прикладного програмного забезпечення, адже хмарні додатки можуть містити вразливості, аналогічні до традиційних веб-застосунків, зокрема, таких як SQL-ін’єкції, XSS-атаки, віддалене виконання коду (RCE). Ці вразливості можуть бути експлуатовані для компрометації хмарного середовища.

6. Втрата або пошкодження даних, причинами яких можуть бути збої в апаратному забезпеченні хмари, людський фактор (наприклад, випадкове видалення), атаки шкідливого ПЗ (наприклад, криптолокери). Захист полягає у резервному копіюванні, зберіганні в георозподілених дата-центрах, контроль версій.

7. Атаки типу «відмова в обслуговуванні» (DoS/DDoS) – хмарні сервіси є привабливою ціллю для атак, що спрямовані на перевантаження систем. DDoS-атаки можуть призвести до недоступності важливих сервісів, порушення SLA, фінансових та репутаційних втрат.

8. Незаконне використання ресурсів – хакери можуть використовувати хмарну інфраструктуру для запуску ботнетів, майнингу криптовалют, розгортання фішингових серверів або розповсюдження шкідливого ПЗ. У цьому випадку відповідальність покладається на провайдера

у вигляді моніторингу активності, виявлення аномалій, політики прийнятного використання [8].

Серед основних проблем нормативного регулювання та відповідальності виділяють настіпні:

- міжнародно-правові суперечності – дані можуть зберігатися в іншій країні, що ускладнює правове регулювання доступу, захисту та обробки інформації.
- Відсутність прозорості – багато хмарних провайдерів не розкривають повну інформацію про заходи безпеки та обробку інцидентів.
- Проблеми відповідальності – нечітке розмежування відповідальності між постачальником послуг і клієнтом (shared responsibility model) може призвести до втрат при інцидентах.

Загрози безпеки в хмарному середовищі мають багатофакторну природу й охоплюють як технічні, так і організаційні аспекти. Для забезпечення надійного функціонування хмарних сервісів необхідна комплексна система захисту, яка включає шифрування, багаторівневу автентифікацію, аудит доступу, регулярне тестування на проникнення та дотримання нормативно-правових вимог. Оскільки тенденції розвитку хмарних технологій зростають, питання інформаційної безпеки залишаються актуальними та вимагають постійної адаптації до нових ситуацій [9].

1.3 Огляд методів криптографічного захисту: симетричні та асиметричні алгоритми

У цифровому середовищі криптографія відіграє фундаментальну роль у забезпеченні конфіденційності, цілісності, автентичності та доступності інформації. Особливої актуальності вона набуває в умовах хмарних обчислень, де дані зберігаються, обробляються та передаються поза межами безпосереднього контролю користувача. У таких умовах ефективні

криптографічні механізми виступають ключовим елементом побудови системи інформаційної безпеки.

Основу сучасного криптографічного захисту становлять дві базові категорії алгоритмів – симетричні та асиметричні. Вони розрізняються як за принципом роботи, так і за призначенням, рівнем продуктивності, способом управління ключами та сферою застосування.

Симетричне шифрування передбачає використання одного й того ж секретного криптографічного ключа як для процесу шифрування, так і для дешифрування інформації. Це забезпечує високу швидкість обробки даних, що робить симетричні алгоритми надзвичайно ефективними для шифрування великих обсягів інформації в реальному часі. Серед найпоширеніших симетричних алгоритмів сучасності – AES (Advanced Encryption Standard), який є стандартом шифрування, рекомендованим NIST, і забезпечує високу стійкість до криптоаналітичних атак за умов належної реалізації.

До ключових переваг симетричного шифрування належать висока продуктивність, відносна простота реалізації, ефективність у ресурсозалежних середовищах. Разом із тим, основним недоліком є необхідність безпечного обміну ключами між сторонами, які обмінюються зашифрованими даними. У випадку перехоплення або компрометації ключа можливе повне розкриття інформації, що становить значну загрозу в умовах публічних або недостатньо захищених мереж.

Асиметричне шифрування, або криптографія з відкритим ключем, використовує два різних, але математично пов’язаних ключі – відкритий і закритий. Відкритий ключ може бути вільно розповсюджений і використовується для шифрування даних або перевірки цифрового підпису, тоді як закритий ключ зберігається в таємниці і застосовується для розшифрування або створення підпису. Такий підхід усуває потребу в захищеному каналі для обміну ключами та створює основу для побудови механізмів цифрової автентифікації й електронного підпису.

Серед найбільш відомих асиметричних алгоритмів – RSA (Rivest–Shamir–Adleman), DSA (Digital Signature Algorithm), а також алгоритми на основі еліптичних кривих (ECC), які забезпечують високу криптографічну стійкість при меншому розмірі ключів і підвищеній ефективності в умовах обмежених обчислювальних ресурсів.

Попри свою універсальність, асиметричні алгоритми мають обмежену продуктивність у порівнянні з симетричними, тому найчастіше використовуються не для прямого шифрування великих обсягів даних, а для захищеного обміну симетричними ключами та підтвердження автентичності.

Таким чином, вибір криптографічного підходу в умовах хмарного середовища повинен враховувати не лише технічні характеристики алгоритмів, але й специфіку архітектури обробки даних, моделі взаємодії між сторонами, вимоги до продуктивності та дотримання нормативних стандартів безпеки. Найбільш ефективним у таких умовах є застосування **гібридної** криптографії, яка поєднує переваги обох підходів і є предметом подальшого аналізу у наступних розділах..

Класифікація симетричного шифрування має наступні категорії [10]:

- блочне шифрування – обробка фіксованих блоків даних (AES, DES, Blowfish);
- потокове шифрування – побітова або побайтове шифрування (RC4, Salsa20).

Приклади симетричного шифрування

- AES (Advanced Encryption Standard) – найбільш поширений стандарт симетричного шифрування. Працює з блоками по 128 біт та підтримує ключі довжиною 128, 192 і 256 біт. AES є стійким до більшості відомих атак.
- DES (Data Encryption Standard) – застарілий алгоритм, замінений AES через недостатню стійкість до перебору (brute force).
- ChaCha20 – сучасна альтернатива AES, ефективна на мобільних пристроях.

Симетричні алгоритми в хмарному середовищі застосовуються для:

використовуються для:

- шифрування даних при зберіганні (at rest),
- шифрування трафіку (TLS/SSL),
- створення VPN-тунелів.

Асиметричне шифрування базується на використанні пари ключів: публічного (public key) та приватного (private key). Публічний ключ використовується для шифрування, а приватний – для дешифрування, або навпаки – для створення та перевірки цифрових підписів [11].

Основні характеристики асиметричного шифрування:

- високий рівень безпеки при обміні ключами,
- значно повільніша швидкість у порівнянні з симетричним шифруванням,
- незамінність для автентифікації та цифрового підпису.

У асиметричному шифруванні застосовуються наступні алгоритми:

- RSA – один із найвідоміших алгоритмів, який базується на складності факторизації великих чисел. Поширений у TLS/SSL, PGP, криптографічних токенах.
- ECC – забезпечує той самий рівень безпеки, що й RSA, але при значно менших розмірах ключів. Це робить ECC особливо привабливою для мобільних і IoT-пристроїв.
- ElGamal – алгоритм, який забезпечує високу криптостійкість і використовується в гібридних системах [12].

Прикладами застосування даного виду шифрування можуть бути:

- захист електронного листування (PGP, S/MIME),
- електронна комерція (SSL-сертифікати),
- взаємна автентифікація між клієнтом і сервером,
- обмін ключами для симетричного шифрування.

Порівняльна характеристика даних видій шифрування представлено в табл. 1.2.

Таблиця 1.2 – Порівняльна характеристика симетричного та асиметричного шифрування

№	Характеристика	Симетричне шифрування	Асиметричне шифрування
1	Кількість ключів	1	2 (публічний і приватний)
2	Продуктивність	Висока	Низька
3	Ризик компрометації	Високий при розподілі	Низький
4	Шифрування великих обсягів	Ефективне	Малоефективне
5	Основне призначення	Конфіденційність	Автентифікація, підпис
6	Приклади	AES, DES, Blowfish	RSA, ECC, ElGamal

1.4 Основні переваги гібридної криптографії

Гібридна криптографія – це сучасний підхід до криптографічного захисту інформації, який поєднує переваги симетричних та асиметричних методів шифрування з метою досягнення високої ефективності, стійкості та безпеки в умовах динамічного цифрового середовища. Така концепція забезпечує одночасну реалізацію основних цілей інформаційної безпеки – конфіденційності, цілісності та автентичності даних – шляхом раціонального розподілу криптографічних завдань між двома типами алгоритмів.

Симетричні алгоритми характеризуються високою швидкодією та низькими витратами на обчислення, що робить їх оптимальними для шифрування великих обсягів інформації. Натомість асиметричні алгоритми забезпечують безпечний обмін ключовою інформацією між сторонами, які не мають попередньо узгодженого секретного каналу [13].

Сутність гібридної криптографії полягає у застосуванні асиметричного шифрування лише на початковому етапі встановлення захищеного з’єднання,

коли відбувається обмін симетричним ключем між сторонами. Наприклад, відправник шифрує випадково згенерований симетричний ключ за допомогою відкритого ключа отримувача, після чого цей ключ використовується для шифрування основного обсягу даних симетричним алгоритмом, таким як AES.

Таким чином, досягається подвійна мета: високий рівень безпеки при передачі ключової інформації та висока швидкість обробки при безпосередньому шифруванні даних.

Подібна схема реалізована в багатьох сучасних криптографічних протоколах, зокрема TLS (Transport Layer Security), OpenPGP, S/MIME та ін. В умовах хмарних обчислень, де велика кількість даних передається мережею та зберігається на сторонніх платформах, гібридна криптографія є оптимальним механізмом, який поєднує продуктивність і стійкість до атак.

Вона дозволяє зменшити ризики, пов’язані з передачею ключів, і водночас забезпечує відповідність сучасним вимогам до захисту даних, включаючи регуляторні норми та стандарти, такі як ISO/IEC 27001 та GDPR.

Завдяки своїй гнучкості та ефективності, гібридна криптографія набула широкого поширення як у комерційних, так і в державних інформаційних системах, особливо в тих, що інтегрують хмарні сервіси або працюють у розподіленому середовищі з високим рівнем загроз.

Приклади реалізації гібридної криптографії наступні:

1 У протоколі TLS використовується:

- RSA або ECDHE – для обміну ключами,
- AES або ChaCha20 – для шифрування даних з високою швидкістю.

2 Система PGP – вхідні повідомлення шифруються симетрично (наприклад, за допомогою AES), а симетричний ключ шифрується асиметричним алгоритмом (зазвичай RSA) з використанням відкритого ключа адресата X [14].

3 Хмарні сервіси (наприклад, Google Cloud, AWS). При завантаженні конфіденційних даних у хмару клієнт генерує симетричний ключ, яким

шифрує файли, а сам ключ шифрується публічним ключем хмарного провайдера [15].

Серед основних переваг гібридної криптографії можна виділити наступні:

1 Підвищений рівень безпеки – гібридна система об'єднує стійкість асиметричних методів до перехоплення ключів з ефективністю симетричних алгоритмів. Це дозволяє уникнути проблем, пов’язаних із поширенням симетричних ключів [16].

2 Оптимальна продуктивність – асиметричні алгоритми використовуються лише на початковому етапі, тому основна передача даних відбувається з використанням високошвидкісного симетричного шифрування. Це дозволяє досягти високої продуктивності навіть при великому обсязі даних.

3 Гнучкість у застосуванні – гібридна криптографія може адаптуватися до різних протоколів і сценаріїв: захист передавання даних, збереження файлів, автентифікація користувачів тощо.

4 Сумісність з існуючими інфраструктурами – гібридні криптосистеми можуть бути впроваджені в рамках існуючих протоколів без значних змін – наприклад, у VPN, HTTPS, SFTP тощо [17].

5 Забезпечення автентифікації та цифрового підпису – завдяки асиметричним алгоритмам у гібридній схемі можлива не лише конфіденційність, а й перевірка достовірності відправника через цифрові підписи.

6 Захист від атак на канали обміну ключами – оскільки відкритий ключ не потребує захищеного каналу для передавання, ризик перехоплення критичного симетричного ключа мінімізується [18].

Гібридна криптографія є однією з найефективніших сучасних моделей захисту інформації, що демонструє особливу ефективність в умовах розподілених, багатокористувацьких і хмарних обчислювальних середовищ. Завдяки своїй структурній гнучкості, масштабованості та здатності забезпечувати як високопродуктивне шифрування даних, так і безпечний

механізм обміну ключовою інформацією, гібридні криптографічні системи вважаються оптимальними для багатьох практичних сценаріїв.

Цей підхід дозволяє успішно вирішувати проблему управління ключами, яка є однією з найбільш критичних у традиційних схемах захисту. Використання асиметричного шифрування на початковому етапі забезпечує безпечну ініціалізацію криптосесії між сторонами, навіть у разі відсутності попереднього обміну довірою або захищеного каналу.

Надалі, використання симетричного алгоритму забезпечує високу швидкість та ефективність обробки великих масивів даних без суттєвого навантаження на ресурси системи.

Гібридна криптографія легко інтегрується в існуючі протоколи безпечної передачі даних і широко використовується в таких областях, як захист електронного листування, побудова захищених каналів зв’язку (наприклад, протоколи TLS/SSL, SSH), обмін конфіденційними файлами, хмарні сервіси з підтримкою end-to-end шифрування, а також у фінансових та державних інформаційних системах.

Її універсальність дозволяє адаптувати архітектуру гібридного шифрування до специфіки обробки різних типів даних та вимог конкретної інформаційної системи, що особливо важливо в умовах змінних загроз кіберпростору та необхідності дотримання міжнародних стандартів безпеки. У перспективі, гібридна криптографія розглядається як основа для розробки стійких до квантових обчислень систем, що посилює її стратегічну цінність у майбутніх IT-архітектурах.

РОЗДІЛ 2 АНАЛІЗ ІСНУЮЧИХ ГІБРИДНИХ КРИПТОГРАФІЧНИХ ПІДХОДІВ У ХМАРНИХ СЕРВІСАХ

2.1 Порівняльна характеристика криптографічних методів захисту у хмарі (Google, AWS, Microsoft Azure)

У сучасних хмарних середовищах безпека даних є критично важливою складовою побудови довіри до сервісу та забезпечення стійкості до кіберзагроз. Найбільші постачальники хмарних обчислень – Amazon Web Services (AWS), Google Cloud Platform (GCP) та Microsoft Azure – реалізують широкий спектр криптографічних механізмів захисту інформації, що охоплюють як базові алгоритми шифрування, так і розвинуті сервіси управління ключами, автентифікацію, політики доступу та відповідність міжнародним стандартам безпеки [19].

Кожна з платформ реалізує власну архітектуру криптографічного захисту, яка інтегрується в загальний стек сервісів і відповідає вимогам таких стандартів, як ISO/IEC 27001, FIPS 140-2, NIST SP 800-57 та GDPR. Основні компоненти криптографічного захисту, які реалізовані провайдерами, а також аспекти, що враховуються під час їхньої імплементації, наведено у табл. А.1 додатка А.

Amazon Web Services (AWS) забезпечує повноцінний захист даних як у стані зберігання, так і під час передавання та обробки. Одним із ключових елементів є сервіс AWS Key Management Service (KMS), який забезпечує централізоване управління симетричними та асиметричними ключами. Сервіс інтегрується з основними хмарними рішеннями AWS – зокрема Amazon S3, RDS, EBS – підтримуючи автоматичне шифрування даних за допомогою стандартних алгоритмів (AES-256, RSA-2048 та ін.). Для реалізації високого рівня криптографічної безпеки AWS пропонує інтеграцію з апаратними засобами – AWS CloudHSM – сертифікованими відповідно до FIPS 140-2, що дозволяє здійснювати криптографічні операції в захищених модулях.

Додатково реалізована концепція AWS Nitro Enclaves, яка забезпечує ізоляцію обробки конфіденційних даних у спеціалізованих віртуалізованих середовищах [20][21].

Google Cloud Platform (GCP) використовує Google Cloud Key Management Service як основний інструмент управління криптографічними ключами. GCP підтримує концепції BYOK (Bring Your Own Key), CMEK (Customer-Managed Encryption Keys), а також CSEK (Customer-Supplied Encryption Keys), що дає користувачам повний контроль над політикою управління ключами. Для критично важливих даних доступна Cloud HSM – апаратна реалізація модулів шифрування. Окрему увагу Google приділяє прозорості криптографічних процесів: реалізована підтримка Confidential VMs, що забезпечують апаратне шифрування даних під час обробки (encryption in use). Крім того, модель Cloud External Key Manager дозволяє керувати ключами з використанням зовнішніх систем, не передаючи ключі до інфраструктури Google [22].

Microsoft Azure пропонує багатофункціональну платформу Azure Key Vault для управління ключами, сертифікатами та секретами, з можливістю інтеграції із системами шифрування Azure Storage, SQL Database, Virtual Machines та іншими службами. Однією з унікальних можливостей Azure є підтримка моделі HYOK (Hold Your Own Key), яка дозволяє зберігати ключі за межами інфраструктури Microsoft – наприклад, у локальному сховищі підприємства або сторонньому HSM. Azure активно впроваджує принципи confidential computing, створюючи захищені середовища обробки, у яких ключі ніколи не залишають межі ізольованого виконання. Значною перевагою платформи є її глибока інтеграція з екосистемою Microsoft 365, що забезпечує зручність для корпоративного сектору [23].

Узагальнюючи, можна зазначити, що AWS є найбільш зрілою платформою з точки зору гнучкого управління ключами, масштабованості та підтримки апаратної безпеки, що робить її доцільним вибором для високонавантажених середовищ з підвищеними вимогами до продуктивності.

Microsoft Azure демонструє високу відповідність гібридним сценаріям, з особливою орієнтацією на корпоративний сегмент, та вирізняється підтримкою моделі HYOK, що є унікальною серед провайдерів. GCP вирізняється прозорістю, автоматизацією захисту та інноваційністю, зокрема в реалізації конфіденційних обчислень і можливостей зовнішнього управління ключами. Таким чином, вибір хмарної платформи має ґрунтуватися на детальному аналізі вимог до безпеки, моделі загроз, нормативної відповідності та специфіки конкретного бізнес-сценарію.

2.2 Практичне використання гібридної криптографії в бізнесі та державному секторі

Гібридна криптографія поєднує переваги симетричного та асиметричного шифрування для досягнення високого рівня безпеки, ефективності та масштабованості. У сучасних інформаційних системах її застосування набуло особливого значення як у бізнесі, так і в державному секторі, де обробляються критично важливі й конфіденційні дані [24].

У банківських системах і платіжних шлюзах гібридна криптографія є ключовим елементом забезпечення безпеки фінансових транзакцій в мережі. Вона поєднує переваги як асиметричного, так і симетричного шифрування, що дозволяє досягти одночасно високого рівня захисту і продуктивності.

У протоколі TLS/SSL, який є стандартом для захисту HTTPS-з'єднань і широко застосовується в онлайн-банкінгу та платіжних системах, для встановлення захищеної сесії спочатку використовується асиметричне шифрування. Наприклад, алгоритми RSA або ECDH (Elliptic Curve Diffie-Hellman) дозволяють надійно обмінятися ключами шифрування між клієнтом і сервером, навіть якщо канал зв’язку піддається прослуховуванню. Асиметричне шифрування забезпечує автентифікацію сторін, підтвердження їхньої ідентичності, а також захист від атак типу «людина посередині» (Man-in-the-Middle).

Після встановлення спільного секретного ключа (сеансового ключа), для безпосередньої передачі даних застосовується симетричне шифрування за допомогою швидких і ефективних алгоритмів, таких як AES (Advanced Encryption Standard) або ChaCha20. Використання симетричного шифрування для шифрування великих обсягів інформації значно підвищує продуктивність системи, оскільки симетричні алгоритми мають меншу обчислювальну складність у порівнянні з асиметричними.

Такий гібридний підхід дозволяє одночасно забезпечити:

– Конфіденційність: Захист від несанкціонованого доступу до фінансових даних і транзакцій, завдяки шифруванню повідомлень.

– Цілісність: Гарантія того, що дані не були змінені або підроблені під час передачі, що підтверджується механізмами контролю цілісності (наприклад, HMAC).

– Автентичність: Переконання в тому, що сторони спілкування є саме тими, за кого себе видають, що особливо важливо у фінансових операціях.

– Відмовостійкість: Захист від повторних атак, атаки перехоплення та інші типи кіберзагроз.

Крім того, у сучасних банківських платіжних шлюзах використовують додаткові механізми безпеки, такі як багатофакторна аутентифікація, цифрові підписи та сертифікати, які також спираються на принципи гібридної криптографії. Впровадження таких технологій дозволяє підтримувати високий рівень довіри клієнтів і відповідати суворим нормативним вимогам у сфері фінансових послуг.

Таким чином, гібридна криптографія в банківських системах і платіжних шлюзах є фундаментальним механізмом захисту, що забезпечує безпечну, швидку і надійну обробку фінансових транзакцій у цифровому середовищі [25].

У системах захисту електронної пошти (зокрема, з використанням OpenPGP або S/MIME) гібридна криптографія дозволяє шифрувати

повідомлення для багатьох одержувачів. Асиметричне шифрування використовується для обміну ключами, а саме повідомлення шифрується симетричним алгоритмом, що зменшує витрати ресурсів [26].

Хмарні провайдери, такі як AWS, Google Cloud та Microsoft Azure, широко впроваджують гібридні криптографічні рішення для забезпечення безпеки даних своїх клієнтів. Основою таких рішень є комбінування симетричного шифрування для захисту безпосередньо інформації та асиметричних методів для надійного управління ключами шифрування.

Наприклад, сервіси AWS Key Management Service (KMS), Google Cloud Key Management і Microsoft Azure Key Vault дозволяють користувачам створювати, зберігати й керувати криптографічними ключами централізовано. При цьому дані шифруються симетричними алгоритмами (часто AES-256), які оптимальні для швидкої і ефективної обробки великих обсягів інформації. Однак самі симетричні ключі захищаються за допомогою асиметричних криптографічних методів, наприклад, шляхом їх шифрування відкритим ключем або підписування.

Цей гібридний підхід забезпечує кілька важливих переваг:

Централізоване управління ключами: Клієнти отримують можливість контролювати повний життєвий цикл ключів – від генерації та зберігання до ротації та знищення, що значно підвищує безпеку.

Підтримка ротації ключів: Автоматизовані механізми оновлення ключів дозволяють регулярно замінювати криптографічні ключі, знижуючи ризик компрометації.

Відповідність нормативним вимогам: Хмарні провайдери гарантують відповідність міжнародним стандартам безпеки та конфіденційності, таким як GDPR (Загальний регламент захисту даних), ISO 27001, PCI DSS тощо. Це критично важливо для організацій, що працюють із чутливою інформацією.

Ізоляція і контроль доступу: Ключі зберігаються в апаратно захищених модулях безпеки (HSM), що забезпечує додатковий рівень захисту від несанкціонованого доступу.

Гнучкість інтеграції: Користувачі можуть інтегрувати KMS із різними сервісами хмари для шифрування даних у сховищах, базах даних, контейнерах або при передачі по мережі.

Таким чином, впровадження гібридної криптографії у хмарних сервісах дозволяє забезпечити надійний захист даних, одночасно зберігаючи зручність централізованого управління ключами і високу продуктивність обробки інформації. Це робить хмарні платформи привабливими для організацій, які прагнуть досягти балансу між безпекою, відповідністю стандартам і ефективністю [27].

У приватних блокчейн-рішеннях (таких як Hyperledger Fabric) гібридні методи використовуються для забезпечення захисту ключової інформації під час транзакцій. Приватний ключ користувача зберігається зашифрованим, а для обміну даними між вузлами застосовуються симетричні методи з використанням обміну асиметричними ключами [28].

Державні реєстри – наприклад, демографічний, податковий або медичний – містять конфіденційну інформацію. Для її шифрування широко використовуються гібридні схеми. Наприклад, у системі «Електронне здоров’я» шифрування медичних записів реалізоване на основі комбінації алгоритмів AES (для даних) і RSA або ECC (для управління ключами) [29].

Гібридна криптографія застосовується у цифровому документообігу через кваліфікований електронний підпис (КЕП). Дані шифруються симетричним алгоритмом, а підпис і автентифікація користувача реалізуються через асиметричні схеми. Це забезпечує як захист від несанкціонованого доступу, так і підтвердження авторства документа [30].

У проєктах електронного голосування, зокрема в національній системі дистанційного голосування Естонії (i-Voting), гібридна криптографія відіграє ключову роль у забезпеченні одночасної реалізації кількох вимог: конфіденційності голосування, автентичності виборців, цілісності результатів та анонімності вибору. Архітектура такої системи побудована з урахуванням принципів багаторівневого захисту, де використовуються як симетричні, так і

асиметричні криптографічні механізми в рамках єдиної криптопротокольної моделі.

Зокрема, голос виборця на етапі формування електронного бюлетеня шифрується з використанням симетричного алгоритму, що дозволяє забезпечити ефективність при обробці великої кількості голосів. Далі симетричний ключ, за допомогою якого може бути здійснене розшифрування голосу, шифрується за допомогою асиметричного алгоритму із використанням відкритого ключа відповідного криптографічного сховища голосів. Такий підхід дозволяє зберігати ключову інформацію в захищеному вигляді без ризику її витоку під час передавання. Для підвищення рівня безпеки система також застосовує механізми мультипідпису (multi-signature) – розшифрування даних можливе лише за умови наявності дозволу від кількох незалежних уповноважених сторін, що значно зменшує ризик внутрішньої загрози або компрометації одного з елементів інфраструктури.

Анонімність виборця забезпечується тим, що підпис і зашифрований голос обробляються окремо: на етапі підрахунку голосів ідентифікаційна інформація видаляється, а сам голос, збережений у зашифрованому вигляді, розкривається лише після завершення голосування з дотриманням процедур безпечного розшифрування. Усе це реалізовано із дотриманням принципів криптографічної прозорості та перевірності (verifiability), що дозволяє як виборцю, так і незалежним спостерігачам перевірити правильність функціонування системи без розкриття змісту голосу.

Таким чином, гібридна криптографія в електронному голосуванні виступає не лише як технічний інструмент шифрування даних, а як ключова складова моделі довіри, що дозволяє забезпечити баланс між безпекою, прозорістю та збереженням демократичних принципів у цифровому виборчому процесі [31].

Гібридна криптографія застосовується у сферах енергетики, транспорту, оборони та безпеки для захисту телеметрії, команд управління та обміну

даними в реальному часі. Вона дозволяє реалізувати як захищене з'єднання між вузлами, так і швидке шифрування великих масивів інформації [32].

Гібридна криптографія є універсальним та ефективним інструментом захисту даних, який успішно застосовується в критично важливих галузях. Її здатність забезпечити як безпеку при обміні ключами, так і швидке шифрування великих обсягів інформації, робить її незамінною в умовах цифровізації бізнесу та державних процесів. З огляду на зростання кіберзагроз, роль гібридної криптографії тільки посилюватиметься.

2.3 Аналіз нормативних вимог до криптографії в хмарному середовищі (GDPR, ISO/IEC 27001, NIST)

У хмарному середовищі, де дані користувачів зберігаються та обробляються на віддалених серверах, криптографія є ключовим елементом забезпечення конфіденційності, цілісності та доступності інформації.

Ефективність засобів криптографічного захисту значною мірою визначається відповідністю міжнародним стандартам та нормативно-правовим актам. Найбільш вагомими з них є Загальний регламент захисту даних, міжнародний стандарт систем управління інформаційною безпекою та рекомендації національного інституту стандартів і технологій.

Відповідність цим документам гарантує, що криптографічні методи та процедури відповідають сучасним вимогам щодо захисту даних, управління ризиками та забезпечення стійкості систем до кіберзагроз. Це особливо важливо в умовах розподілених хмарних архітектур, де контроль над даними здійснюється через множинні рівні доступу і обробки.

Дотримання стандартів сприяє підвищенню довіри користувачів і партнерів, а також забезпечує правову основу для захисту персональної та корпоративної інформації [33].

Розрізняють наступні нормативні документи:

1. GDPR – це загальноєвропейський регламент, що регулює захист персональних даних громадян ЄС. Хоча він не містить конкретних технічних вимог щодо криптографії, він вимагає впровадження відповідних технічних і організаційних заходів, зокрема псевдонімізацію та шифрування персональних даних (ст. 32). Ключовий захист проявляється в таких характеристиках як конфіденційність персональних даних, захист за замовчуванням та за проєктом [34].

2. ISO/IEC 27001 – даний стандарт є частиною серії ISO/IEC 27000 і визначає вимоги до системи управління інформаційною безпекою (ISMS). Стандарт передбачає впровадження заходів контролю, зокрема:

- використання криптографії (розділ A.10.1),
- управління ключами (A.10.1.2),
- забезпечення цілісності переданих даних.

Даний стандарт передбачає системний підхід до управління інформаційною безпекою [35].

3. National Institute of Standards and Technology (NIST) публікує технічні рекомендації, зокрема:

- NIST SP 800-53: набір заходів безпеки, включаючи криптографічний захист,
- NIST SP 800-57: управління криптографічними ключами,
- NIST SP 800-175: керівництво щодо криптографічних стандартів для федеральних агентств [36].

Ключові рекомендації передбачають використання чітких технічних параметрів та алгоритмів (AES, RSA, ECC, TLS тощо). Порівняльна характеристика нормативних вимог представлена в табл. А.2 додатка А [23].

Взаємозв’язок стандартів у криптографічному захисті представлена на концептуальній схемі на рис. 2.1.

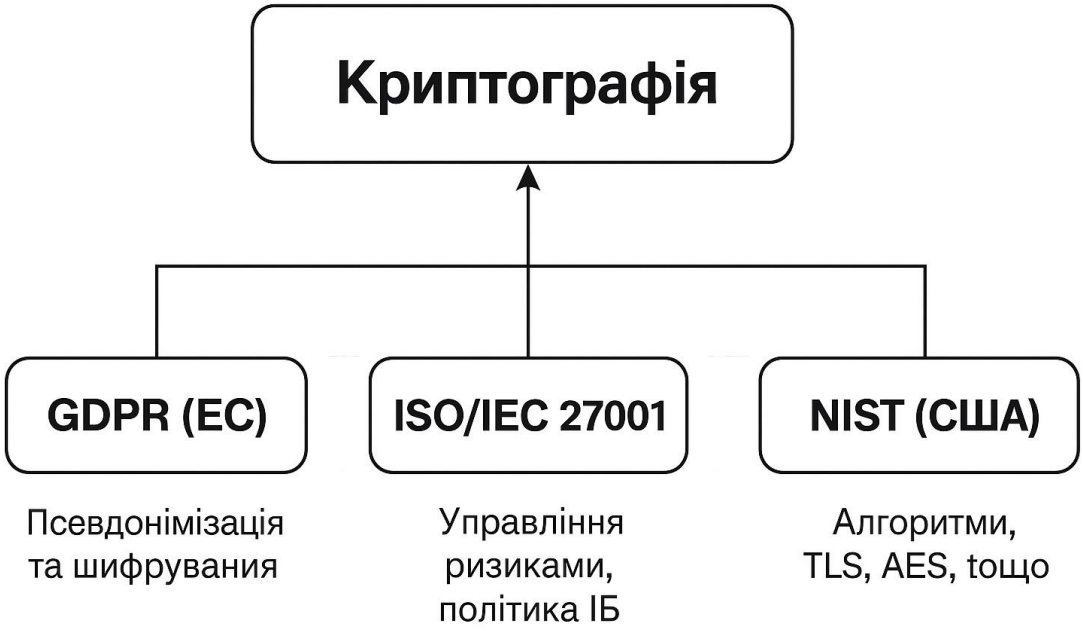

Рисунок 2.1 – Взаємозв’язок стандартів у криптографічному захисті

Аналіз вищезазначених нормативних актів свідчить про високий ступінь уваги до криптографічного захисту даних у хмарному середовищі. Кожен із документів – GDPR, ISO/IEC 27001 та NIST – робить унікальний внесок у формування цілісної системи захисту інформації [37].

Загальний регламент захисту даних (GDPR) виконує роль фундаментального правового інструмента Європейського Союзу, спрямованого на забезпечення захисту персональних даних фізичних осіб. Він встановлює обов’язкові вимоги щодо збереження конфіденційності, цілісності та доступності персональної інформації, незалежно від способу її обробки чи місця зберігання, включно з хмарними інфраструктурами.

У контексті криптографії GDPR не визначає конкретних криптографічних алгоритмів або технічних засобів, однак чітко вказує на необхідність впровадження належних технічних та організаційних заходів безпеки відповідно до рівня ризику. Зокрема, у статтях 32 та 34 Регламенту йдеться про застосування таких методів, як псевдонімізація та шифрування

даних, як ефективних механізмів для зниження ймовірності несанкціонованого доступу, розкриття або втрати інформації.

Вимоги GDPR зобов'язують контролерів та обробників даних забезпечувати проактивний підхід до безпеки, здійснювати оцінку ризиків та впроваджувати заходи, що відповідають потенційній шкоді у разі інциденту, гарантувати можливість швидкого відновлення доступу до персональних даних у разі технічного збою або атаки, забезпечувати періодичний аудит і тестування ефективності обраних засобів захисту.

Застосування криптографії, зокрема гібридного шифрування, у хмарних середовищах дозволяє організаціям відповідати принципам GDPR, мінімізуючи юридичні та репутаційні ризики. Шифрування персональних даних у поєднанні з ефективною системою управління ключами дає змогу не лише знизити наслідки потенційного витоку, а й уникнути обов'язку повідомляти користувачів про інцидент, якщо дані були захищені належним чином.

Таким чином, хоча GDPR не є технічним стандартом, він задає рамкові вимоги, що стимулюють використання сучасних криптографічних засобів як невід'ємної частини політики захисту персональних даних у цифровому середовищі [38].

ISO/IEC 27001 функціонує як управлінський та процесно орієнтований стандарт, що забезпечує створення та підтримку Системи управління інформаційною безпекою (ISMS). Він надає гнучкий інструментарій для оцінки ризиків, впровадження політик безпеки, процедур контролю, включаючи управління криптографічними засобами та ключами. Його цінність полягає у структурному підході до побудови комплексної системи безпеки, яка охоплює не лише технічні аспекти, але й організаційні та кадрові [39].

Національний інститут стандартів і технологій (NIST) забезпечує технічну та алгоритмічну базу для реалізації ефективного криптографічного захисту інформації. Його рекомендації, оприлюднені у вигляді спеціальних публікацій (NIST Special Publications), мають статус обов'язкових для

державних установ США та водночас слугують де-факто міжнародним стандартом, широко впроваджуваним у промисловості, банківському секторі, телекомунікаціях і хмарних обчисленнях.

Документи NIST визначають перелік затверджених криптографічних алгоритмів (зокрема AES, RSA, ECC, SHA-2, SHA-3), вимоги до генерації, зберігання та дистрибуції ключів, правила криптографічного протоколювання, а також принципи стійкості до актуальних типів атак. Зокрема, у публікації NIST SP 800-57 описано життєвий цикл криптографічних ключів, а в NIST SP 800-38 серії – режими блочного шифрування, рекомендовані для використання у захищених інформаційних системах.

Особливу увагу NIST приділяє криптографічній стійкості до майбутніх загроз, таких як квантові обчислення, у зв'язку з чим здійснюється стандартизація постквантових алгоритмів у межах ініціативи Post-Quantum Cryptography Standardization. У сфері хмарних технологій рекомендації NIST також охоплюють аспекти безпечного управління криптографічними ключами, контроль доступу та відповідність вимогам безпеки при обробці конфіденційної інформації в зовнішньому середовищі.

Таким чином, рекомендації NIST становлять системну основу для побудови криптографічного захисту, забезпечуючи технологічну сумісність, відповідність вимогам комплаєнсу та стійкість до сучасних кіберзагроз. У хмарних середовищах ці підходи сприяють створенню надійної та масштабованої інфраструктури захисту даних [40].

Таким чином, взаємодоповнюючий характер цих підходів – правовий (GDPR), процесний (ISO/IEC 27001) та технічний (NIST) – забезпечує багаторівневий, гнучкий і адаптивний захист даних в умовах хмарних обчислень. Така інтеграція дозволяє організаціям не лише дотримуватись вимог законодавства, а й підвищувати власну стійкість до загроз, зменшувати ризики інформаційних інцидентів та підвищувати довіру користувачів до хмарних сервісів.

РОЗДІЛ 3. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ ГІБРИДНОЇ КРИПТОГРАФІЇ

3.1 Критерії вибору гібридної криптосхеми залежно від типу даних і моделі хмарної архітектури

Гібридні криптографічні схеми поєднують переваги симетричних і асиметричних методів шифрування, забезпечуючи як ефективність обробки великих обсягів даних, так і безпечний обмін ключами. У хмарних IT-середовищах, де домінують різні архітектурні моделі та типи даних, вибір відповідної гібридної криптографічної схеми повинен ґрунтуватися на комплексному аналізі таких факторів: типу даних, моделі хмарної архітектури, продуктивності, вимог до безпеки, нормативних актів (GDPR, NIST, ISO/IEC 27001), ризик-орієнтованого підходу тощо.

Персональні дані (PII, PHI) вимагають високого рівня конфіденційності, оскільки їхнє розголошення може призвести до серйозних наслідків для особи. Для їхнього захисту рекомендується використовувати асиметричне шифрування RSA з ключем довжиною 2048 біт або алгоритми на основі еліптичних кривих (ECC) у поєднанні з симетричним шифруванням AES-256 у режимах GCM (для автентифікації) або CBC (для забезпечення конфіденційності).

Для інтелектуальної власності важливо забезпечити контрольований доступ і захист від несанкціонованого використання. Рекомендовано використовувати алгоритми ECC у поєднанні з AES-256, а також обов’язково впровадити контроль доступу на основі ролей (RBAC) для обмеження доступу лише уповноваженим користувачам.

Log-файли та телеметрія характеризується тим, що для цих даних основною вимогою є висока швидкість обробки при відносно невисокій критичності конфіденційності. Оптимальним варіантом є використання алгоритму Curve25519 для обміну ключами та ChaCha20 для шифрування

даних, оскільки ці алгоритми забезпечують високу продуктивність при належному рівні безпеки.

У сфері фінансових технологій та електронної комерції особливої уваги потребує захист чутливої інформації, оскільки навіть незначний витік або компрометація даних може мати серйозні юридичні та економічні наслідки. Для забезпечення належного рівня безпеки фінансових даних необхідно реалізувати криптографічні механізми, що гарантують високу надійність, конфіденційність та цілісність інформації, а також забезпечують повну прозорість і можливість аудиту дій з даними.

На етапі встановлення сеансу зв'язку або при розподілі ключів рекомендується використовувати асиметричні алгоритми шифрування, такі як RSA або криптографія на еліптичних кривих (ECC). Ці методи дозволяють безпечно обмінюватися ключовим матеріалом навіть у потенційно ворожому середовищі. ECC, зокрема, характеризується вищою криптостійкістю при меншій довжині ключа, що робить її привабливою для мобільних і ресурсно обмежених платформ.

Для безпосереднього шифрування фінансових транзакцій та супровідних даних доцільно застосовувати симетричний алгоритм AES у режимі GCM (Galois/Counter Mode). Цей режим поєднує переваги потокового шифрування та автентифікації даних, забезпечуючи не лише конфіденційність, але й захист від несанкціонованих змін інформації за допомогою вбудованого механізму контролю цілісності.

Окрім застосування криптографічних алгоритмів, критично важливим є впровадження системи журналювання доступу. Такий журнал має фіксувати всі спроби читання, модифікації, видалення або передачі даних, а також містити інформацію про час, обліковий запис і тип дії. Наявність детального і захищеного аудиту є необхідною умовою для проведення розслідувань інцидентів безпеки, підтвердження відповідності стандартам та виявлення потенційних порушень політик доступу.

Комплексне впровадження зазначених заходів дозволяє досягти високого рівня захисту фінансових даних, що є критично важливим як для комерційних організацій, так і для регуляторних структур, які встановлюють вимоги до обробки фінансової інформації в цифровому середовищі. Типи даних і вимоги до їх захисту представлені в табл. А.3 додатка А.

У публічній хмарі користувачі, як правило, мають низький рівень довіри до хмарного провайдера, оскільки інфраструктура є загальнодоступною, а дані зберігаються на стороні третьої компанії. Щоб мінімізувати ризики, рекомендується використовувати схему BYOK (Bring Your Own Key) – тобто клієнт самостійно генерує та управляє ключами шифрування. Додатково слід застосовувати клієнтське шифрування, щоб дані шифрувалися ще до передачі у хмару.

У приватній хмарі організація має повний контроль над інфраструктурою та забезпечує ізоляцію середовища. Це дозволяє реалізувати більш гнучкі та безпечні схеми. Рекомендується використовувати внутрішній HSM (апаратний модуль безпеки) для надійного зберігання ключів, а також впроваджувати централізоване управління політиками безпеки та доступом.

Гібридна хмара поєднує елементи як публічної, так і приватної хмар, і вимагає ефективної взаємодії між різними середовищами. Для такого підходу доцільно використовувати Attribute-Based Encryption (ABE) – шифрування, яке дозволяє налаштовувати доступ до даних на основі атрибутів користувача. Також важливо впровадити токенізований доступ, що дозволяє знизити ризики компрометації даних, і розподіл ключів для підвищення безпеки управління криптографічними матеріалами. Модель хмарної архітектури представлена на рис. 3.1 та в табл. А.4 додатка А.

Рисунок 3.1 – Модель хмарної архітектури

Обгрунтування вибору моделі хмарної архітектури полягає у дослідженні наступних даних:

1. Продуктивність симетричного проти асиметричного шифрування. Для даних обсягом 100 МБ:

- AES-256 (GCM) ~0.2 сек
- RSA-2048 ~25 сек

Таким чином, застосування асиметричного шифрування до всього масиву даних є неефективним. Саме тому гібридна схема, де RSA або ECC використовується лише для обміну симетричним ключем, є оптимальним рішенням.

2. Криптостійкість – обчислення ключового простору.

AES-256 має ключовий простір N=2256≈1.16×1077. Нехай суперкомп’ютер виконує 10^{18} операцій на секунду, тоді час повного перебору складатиме (формула 3.1):

$$\mathrm{T} = \frac{N}{10^{18}} = \frac{1.16*10^{77}}{10^{18}} = 1.16 * 10^{59}\text{секунд} \quad (3.1)$$

Тобто, таким чином, 1 рік≈3.15×10^7 секунд

$$\frac{1.16 * 10^{59}}{3.15 * 10^{7}} \approx 3{,}68 * 10^{51}\ \text{років}$$

Це доводить практичну незламність AES-256 при сучасних обчислювальних потужностях.

3. Обсяг трафіку та ефективність передачі

Для шифрування 10 МБ даних:

- AES-256 шифрує весь блок, тобто (формула 3.2):

$$V_{syst} = 10 * 2^{20} = 10485760\ \text{байт} \quad (3.2)$$

- RSA-2048 шифрує лише 256-бітовий симетричний ключ (32 байти): $V_{asyst} = 256$ байт (формула 3.3).

У гібридній схемі:

- Загальний обсяг:

$$V_{total}=V_{sym}+V_{asym}=10485760+256=10486016\ \text{байт} \quad (3.3)$$

- При повному RSA-шифруванні обсяг значно збільшиться (20–30% перевищення), що знижує ефективність передачі.

4. Складність обміну ключами в мультихмарі

У класичній схемі з 4 провайдерами схема обміну ключами потребує:

$$\mathrm{C}_{class} = \frac{n(n-1)}{2} = \frac{4*3}{2} = 6\ \text{каналів} \quad (3.1)$$

Використання централізованого HSM або KMS знижує складність до:

$$C_{central} = n = 4 \text{ каналів} \quad (3.1)$$

Таким чином дані розрахунки показують, що це зменшує ризик компрометації ключів і підвищує керованість.

Гібридні криптографічні схеми становлять ефективний інструмент для забезпечення комплексного захисту даних у хмарних середовищах. Вони поєднують переваги симетричних алгоритмів, що забезпечують високу швидкість обробки інформації, та асиметричних методів, які гарантують безпечний обмін ключами та автентифікацію. Завдяки такій комбінації забезпечується як продуктивність, так і надійність криптографічного захисту навіть у високонавантажених або розподілених обчислювальних інфраструктурах.

Обґрунтований вибір конкретної гібридної схеми має ґрунтуватися на низці факторів, які виходять за межі типу даних або моделі хмарної архітектури (публічна, приватна, гібридна). До критично важливих параметрів відносяться кількісні показники, зокрема очікувана пропускна здатність системи, обсяги вхідного та вихідного трафіку, складність організації й підтримки механізмів обміну ключами, а також рівень криптостійкості застосовуваних алгоритмів.

Оцінка зазначених характеристик дозволяє підібрати конфігурацію, що забезпечує оптимальний баланс між рівнем безпеки, швидкодією шифрування та можливістю масштабування рішення відповідно до змін навантаження або вимог користувача. У контексті динамічних хмарних інфраструктур, які характеризуються високим рівнем автоматизації, варіативністю розгортання сервісів та необхідністю дотримання нормативних вимог, такий підхід є особливо актуальним.

Таким чином, впровадження гібридної криптографії у хмарних середовищах із врахуванням технічних та операційних метрик є доцільною

стратегією, яка дозволяє не лише підвищити загальний рівень інформаційної безпеки, а й забезпечити адаптивність рішень у довгостроковій перспективі.

3.2 Особливості побудови криптографічного захисту з використанням гібридного підходу

У сучасних інформаційних системах, зокрема в умовах хмарних обчислень, питання забезпечення конфіденційності, цілісності та доступності даних набуває особливої актуальності. Традиційні криптографічні методи – симетричні або асиметричні – мають як переваги, так і певні обмеження, що ускладнює їхнє окреме застосування у складних і динамічних середовищах. У зв’язку з цим все ширше впроваджуються гібридні криптографічні підходи, які поєднують сильні сторони обох типів шифрування.

Гібридна криптографія дозволяє ефективно вирішувати завдання захисту даних на різних етапах життєвого циклу – під час зберігання, передачі та обробки. Завдяки використанню симетричних алгоритмів для швидкого шифрування великих обсягів даних та асиметричних механізмів для безпечного обміну ключами досягається високий рівень продуктивності при збереженні необхідної криптостійкості.

У цьому підрозділі розглянуто ключові принципи побудови криптографічного захисту на основі гібридного підходу, його переваги в контексті хмарних середовищ, а також чинники, які впливають на вибір і реалізацію таких схем у практичних сценаріях.

Гібридна схема базується на поділі завдань між двома класами криптографічних алгоритмів:

- асиметричні алгоритми (RSA, ECC) використовуються на початковому етапі – для обміну симетричними ключами через відкриті канали зв'язку. Їх головна перевага – можливість безпечної комунікації без попередньої домовленості про ключ.

– симетричні алгоритми (AES, ChaCha20) використовуються для масивного шифрування даних, оскільки мають значно вищу швидкодію та менші обчислювальні витрати.

Перевага гібридної моделі полягає в тому, що вона успішно усуває недоліки обох класів алгоритмів: повільність асиметричних та вразливість симетричних у контексті обміну ключами.

2. Структурна роздільність криптографічних фаз – гібридна схема чітко розділяє процес шифрування на дві незалежні фази:

– Фаза 1: Ініціалізація сеансу – за допомогою асиметричного алгоритму відбувається генерація та передача симетричного ключа. Цей ключ може бути одноразовим (ephemeral) – тобто згенерованим лише для одного сеансу передачі.

– Фаза 2: Передача даних – дані шифруються симетричним алгоритмом, що суттєво зменшує обсяг обчислень.

Цей підхід дозволяє реалізувати сеансове шифрування, яке забезпечує Forward Secrecy (стійкість до компрометації минулих сесій).

3. Гнучкість управління криптографічними ключами – у хмарних середовищах надзвичайно важливим є надійне управління ключами. Гібридний підхід дозволяє використовувати різні моделі ключового менеджменту:

– BYOK (Bring Your Own Key) – клієнт самостійно генерує та завантажує власні ключі до хмари.

– HYOK (Hold Your Own Key) – клієнт ніколи не передає ключі хмарному провайдеру, навіть тимчасово.

– HSM (Hardware Security Module) – фізичний пристрій для генерації/зберігання ключів.

– KMS (Key Management Service) – хмарний або гібридний сервіс для автоматизованого управління ключами.

У мультихмарному середовищі часто використовується розподілений обмін ключами із застосуванням протоколів типу KMIP (Key Management Interoperability Protocol) або ABE (Attribute-Based Encryption).

4. Підвищена криптостійкість до атак – комбінування різних алгоритмів створює багаторівневий захист, що ускладнює криптоаналітичні атаки:

- симетричні ключі ротаційні й зазвичай знищуються після сеансу.
- асиметричні ключі мають довгий термін дії, але не використовуються для шифрування основного масиву даних.
- злам одного компонента не означає повну компрометацію системи.

Тобто, навіть якщо перехоплено симетричний ключ, його втрата обмежена лише однією сесією, і нападник не зможе дешифрувати інші передані дані.

5. Оптимізація мережевого трафіку та обчислювальних витрат

Повне асиметричне шифрування є непридатним для обробки великих даних через обмеження на розмір блоку та високу обчислювальну складність. У гібридній моделі:

- Симетричне шифрування 10 МБ даних триває ~0.2 сек (AES-256).
- Асиметричне шифрування того ж обсягу – >20 сек (RSA-2048).

Асиметрично шифрується лише ключ довжиною 256–512 біт, що мінімізує обсяг додаткового трафіку (~0.0025% від загального розміру).

Це особливо критично в мобільних, граничних обчисленнях (edge computing) або при роботі через повільні канали передачі даних.

6. Масштабованість і сумісність з хмарними екосистемами. Гібридна криптографія добре підтримується у сучасних хмарних платформах завдяки вбудованій підтримці відповідних протоколів і сервісів:

- Підтримувані криптографічні протоколи – TLS (Transport Layer Security), S/MIME (Secure/Multipurpose Internet Mail Extensions), PGP (Pretty Good Privacy), KMIP (Key Management Interoperability Protocol) тощо.
- Хмарні провайдери та сервіси:

a) Amazon Web Services (AWS): AWS Key Management Service (KMS), AWS CloudHSM
b) Microsoft Azure – Azure Key Vault, Azure Dedicated HSM
c) Google Cloud Platform – Google Cloud Key Management Service (Cloud KMS), Cloud HSM

Таким чином спрощує впровадження гібридних схем у вже існуючі хмарні системи з мінімальними витратами на перебудову архітектури.

Гібридна криптографічна архітектура є універсальним рішенням для захисту даних у хмарному середовищі. Її ефективність базується на раціональному розподілі функцій між симетричними й асиметричними методами, а також на гнучкості в управлінні ключами, масштабованості та сумісності з міжнародними стандартами.

3.3 Оцінка ризиків і захищеності гібридних систем

Гібридні криптографічні системи, які поєднують переваги симетричного та асиметричного шифрування, пропонують збалансований і ефективний підхід до забезпечення конфіденційності, цілісності та доступності даних у хмарному середовищі. Їхня архітектура дозволяє одночасно досягати високої швидкодії обробки інформації та забезпечувати безпечний обмін ключами навіть у розподілених і динамічних інфраструктурах. Такий підхід є особливо цінним у контексті хмарних технологій, де обробка та передача даних відбувається через відкриті канали зв’язку, а контроль над фізичним доступом до середовища є обмеженим.

Разом із тим, впровадження гібридних криптографічних систем супроводжується низкою потенційних ризиків і вразливостей. До таких ризиків належать компрометація ключів, некоректне управління їхнім життєвим циклом, помилки конфігурації алгоритмів, вразливості у механізмах автентифікації, а також ризики, пов’язані з людським фактором або зовнішніми загрозами. З огляду на складність взаємодії між криптографічними

компонентами системи та різнорідними елементами хмарної інфраструктури, необхідним є системний підхід до оцінки та зниження таких ризиків.

Для цього слід здійснити формалізовану оцінку захищеності, що передбачає ідентифікацію загроз, класифікацію ризиків за ймовірністю реалізації та потенційним впливом, а також розробку та впровадження компенсуючих технічних і організаційних заходів. Такий процес повинен включати аналіз криптостійкості використовуваних алгоритмів, відповідність міжнародним стандартам безпеки, перевірку наявності механізмів резервування та аудиту, а також тестування системи на стійкість до типових векторів атак.

Комплексне застосування формалізованого підходу до оцінки захищеності дозволяє не лише мінімізувати ризики, пов’язані з експлуатацією гібридних криптосистем у хмарі, але й підвищити загальну довіру до технологічного рішення з боку користувачів, регуляторів та партнерів.

1. Модель загроз гібридної криптосистеми – гібридна криптографічна система може бути вразливою до таких загроз:

- перехоплення відкритих каналів при передачі ключа або даних.
- Компрометація приватного ключа на стороні отримувача.
- Атаки типу «людина посередині» (MitM) під час ініціації сеансу.
- Атаки на криптографічні протоколи (наприклад, через неактуальні версії TLS або неправильну реалізацію).
- Недостатній контроль доступу до KMS/HSM або витік ключів при неправильній конфігурації хмарної платформи.

2. Аналіз ризику на основі моделі STRIDE та DREAD

Для системного аналізу гібридних криптосхем доцільно використати комбінацію моделей STRIDE (типи загроз) і DREAD (кількісне оцінювання ризиків), відображене в табл.3.1.

Таблиця 3.1 – Комбінація моделей STRIDE і DREAD

№	Тип загрози (STRIDE)	Потенційна вразливість	DREAD-оцінка (0–10)
1	Spoofing (Підміна)	Імітація сторони при обміні ключами	8
2	Tampering (Зміна)	Втручання в процес генерації ключів	6
3	Repudiation (Відмова)	Відсутність журналювання дій при мультихмарній взаємодії	5
4	Information Disclosure	Витік симетричного ключа або відкритих метаданих	9
5	Denial of Service	Виведення з ладу KMS чи HSM	4
6	Elevation of Privileges	Отримання доступу до ключів через вразливості платформи	7

3.4 Рекомендації щодо організації управління ключами в хмарному середовищі

Ефективне управління криптографічними ключами є критичним елементом забезпечення інформаційної безпеки в хмарних обчислювальних середовищах. У контексті хмарних сервісів, де дані користувачів зберігаються та обробляються на віддалених платформах, а фізичний контроль над інфраструктурою часто відсутній, саме криптографічні ключі виступають основним засобом контролю доступу до конфіденційної інформації. Їх захист та належне адміністрування визначають загальний рівень стійкості до несанкціонованого доступу, атак з боку зловмисників, а також до внутрішніх загроз.

Особливої актуальності набувають практики централізованого, масштабованого та безпечного управління ключами в умовах динамічної архітектури хмари, мультиорендності (multi-tenancy) та широкого використання автоматизованих механізмів розгортання і масштабування сервісів. Таке управління повинно охоплювати всі етапи життєвого циклу ключа: генерацію, розповсюдження, зберігання, ротацію, відкликання та знищення. При цьому важливо забезпечити як захист самих ключів, так і контроль над операціями, що з ними виконуються.

У хмарних середовищах реалізація систем управління ключами може здійснюватися як за допомогою вбудованих сервісів провайдера (наприклад, AWS KMS, Azure Key Vault, Google Cloud KMS), так і через механізми Bring Your Own Key (BYOK) чи навіть Host Your Own Key (HYOK), що дозволяє організаціям зберігати критично важливі ключі у власних середовищах або апаратних модулях безпеки (HSM).

Застосування централізованого підходу до управління ключами дає змогу, забезпечити уніфіковану політику безпеки в межах усіх хмарних сервісів, автоматизувати ротацію та відкликання ключів, забезпечити аудит і журналювання доступу, спростити відповідність стандартам безпеки та комплаєнсу (наприклад, GDPR, ISO/IEC 27001, PCI DSS).

Таким чином, управління криптографічними ключами в хмарних середовищах є не лише технічною, а й стратегічною задачею, від ефективного вирішення якої залежить захист персональних, фінансових та корпоративних даних в умовах сучасного цифрового ландшафту.

1. Використання моделі ring Your Own Key (BYOK) передбачає, що користувачі генерують власні ключі шифрування в довіреному середовищі (on-premises) та передають їх до хмарного постачальника через захищені канали. Такий підхід дає змогу забезпечити контроль над життєвим циклом ключа, зменшити ризики несанкціонованого доступу з боку хмарного провайдера, відповідати вимогам регуляторів (GDPR, ISO/IEC 27018), які передбачають збереження контролю над криптографічними матеріалами.

2. Інтеграція з апаратними засобами захисту – передбачає використання HSM (Hardware Security Module) – фізичних пристроїв, сертифікованих за стандартами FIPS 140-2 або Common Criteria, що дозволяє забезпечити захищене генерування, зберігання і використання ключів, апаратну недоторканність приватного ключа (ключ не покидає HSM у відкритому вигляді), відповідність вимогам галузей з високими стандартами безпеки (фінансовий сектор, охорона здоров’я тощо).

Хмарні провайдери пропонують власні HSM-сервіси: AWS CloudHSM, Azure Dedicated HSM, Google Cloud HSM – з інтеграцією в екосистему управління доступом, журналювання і контролю.

3. Використання сервісів централізованого управління ключами (KMS)

Сервіси KMS (Key Management Service) надають інтерфейси для:

- генерації, обертання (rotation), деактивації ключів;
- визначення політик доступу на основі ролей (RBAC, IAM);
- журналювання дій над ключами (audit logging), що дозволяє виявляти інциденти безпеки.

Наприклад:

- AWS KMS дозволяє створювати Customer Managed Keys з підтримкою BYOK і автоматичного обертання;
- Azure Key Vault підтримує захист ключів у поєднанні з Azure Active Directory;
- Google Cloud KMS інтегрується з Cloud IAM і Cloud Audit Logs для повного контролю.

4. Застосування принципів криптографічної ізоляції (Cryptographic Separation of Duties)

Управління ключами повинно реалізовувати **розподіл ролей** (separation of duties), коли одна особа не має повного контролю і над ключем, і над системою шифрування. Це мінімізує внутрішні загрози та ускладнює реалізацію атак з боку зловмисників з доступом до хмари.

5. Автоматизація життєвого циклу ключів

Життєвий цикл ключа повинен охоплювати:

- генерацію з використанням надійних джерел ентропії;
- періодичну зміну (rotation) відповідно до політики організації;
- архівування, знищення та аудит із мінімізацією людського фактору.

Автоматизоване управління забезпечує узгодженість, мінімізує ймовірність помилок та забезпечує відповідність стандартам безпеки.

Раціональна організація управління криптографічними ключами в хмарному середовищі є необхідною умовою для досягнення належного рівня криптографічної стійкості інформаційної системи та дотримання вимог міжнародних стандартів і нормативно-правових актів. В умовах, коли традиційна фізична ізоляція ресурсів, характерна для локальних середовищ, поступається гнучкості та динамічності хмарних платформ, питання довіри та контролю над ключами набувають принципового значення.

Застосування сучасних моделей управління ключами, таких як Bring Your Own Key (BYOK), дозволяє організаціям генерувати ключі поза межами хмари та передавати їх у захищеному вигляді до інфраструктури хмарного провайдера. Це забезпечує більшу прозорість та контроль з боку користувача. Ще більшу автономію пропонує модель Host Your Own Key (HYOK), при якій ключі не залишають меж підприємства взагалі.

Додатковим рівнем безпеки виступає використання апаратних модулів безпеки (HSM), які забезпечують захист ключового матеріалу на рівні спеціалізованого обладнання, ізолюючи критичні криптографічні операції від загального програмного середовища. Більшість провайдерів хмарних послуг інтегрують HSM у свої сервіси KMS (Key Management Service), що дає змогу поєднати апаратну безпеку з масштабованістю та автоматизацією хмарних сервісів.

Важливим аспектом також є впровадження принципів розмежування повноважень (separation of duties) та мінімізації привілеїв (least privilege), які забезпечують розподіл доступу до ключів і операцій над ними між різними ролями користувачів та адміністраторів. Це зменшує ризик внутрішніх загроз і сприяє побудові надійної системи контролю доступу.

Таким чином, впровадження комплексного підходу до управління криптографічними ключами – із урахуванням моделей BYOK, апаратних HSM, сервісів KMS і політик безпеки – дозволяє суттєво підвищити рівень контролю над конфіденційною інформацією навіть за умов обмеженого фізичного контролю, що притаманне хмарним технологіям.

РОЗДІЛ 4 МОДЕЛЮВАННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ГІБРИДНИХ РІШЕНЬ

4.1 Основні принципи управління ключами

У процесі дослідження механізмів криптографічного захисту даних у хмарному середовищі стає очевидним, що правильна та належна організація управління криптографічними ключами є не просто важливою складовою інформаційної безпеки, а фактично виступає одним із ключових чинників формування довіри користувачів до хмарних сервісів.

Саме від надійності та прозорості управління ключами залежить, наскільки ефективно можна гарантувати конфіденційність, цілісність та доступність даних, що зберігаються або передаються через хмарні платформи. Провівши детальний аналіз численних наукових джерел, а також вивчивши міжнародні стандарти, такі як NIST SP 800-57, ISO/IEC 11770, 27001, 27002, які регламентують процедури і кращі практики в сфері криптографії та управління інформаційною безпекою, вдалося виокремити комплекс базових принципів, які повинні бути невід’ємною частиною будь-якої ефективної системи управління ключами.

Крім того, дослідження спиралося на практичний досвід і реалізації провідних світових хмарних провайдерів, що дозволяє впевнено стверджувати, що дотримання цих принципів забезпечує не лише високий рівень захисту інформації, а й підвищує загальний рівень довіри клієнтів, сприяє відповідності нормативним вимогам і мінімізує ризики, пов’язані з компрометацією або неправильним використанням криптографічних ключів.

Отже, система управління ключами в хмарних середовищах має бути побудована на основі чітких правил, що передбачають безпечне генерування, зберігання, розподіл, використання, ротацію та знищення ключів із застосуванням засобів апаратного та програмного захисту, а також прозорих процедур аудиту і контролю, що дозволяють своєчасно виявляти і реагувати на

потенційні загрози. Такий комплексний підхід є фундаментом для забезпечення надійного криптографічного захисту і створення безпечного хмарного середовища.

1. Принцип довіреного генератора ключів

Ключ повинен генеруватися лише у перевіреному середовищі з використанням криптографічно надійного генератора випадкових чисел (CSPRNG). У хмарних умовах це передбачає використання спеціалізованих сервісів або апаратних модулів (HSM), що забезпечують належну ентропію та контроль над процесом.

2. Принцип життєвого циклу ключа (Key Lifecycle Management)

На практиці важливо не лише створити ключ, а й ефективно керувати всіма етапами його існування:

- створення (ініціалізація параметрів і політик доступу),
- розповсюдження (доставка ключа до вузлів без розкриття в незашифрованому вигляді),
- використання (для шифрування, підпису, аутентифікації тощо),
- заміна/ротація (рекомендовано кожні N днів або у випадку підозри на компрометацію),
- деактивація і знищення (з дотриманням політик цифрової утилізації).

Такий підхід забезпечує контроль над ключами на всіх етапах їх експлуатації та мінімізує ризики несанкціонованого доступу.

3. Принцип мінімізації прав доступу (Least Privilege)

Управління криптографічними ключами має обов’язково враховувати принцип найменших привілеїв, який передбачає, що доступ до ключів отримують лише ті суб’єкти, які мають чітко обґрунтовану та документально підтверджену потребу у використанні конкретного ключа. Цей підхід мінімізує ризики несанкціонованого доступу, випадкових помилок або зловмисних дій, оскільки обмежує коло осіб та процесів, які можуть взаємодіяти з критичною криптографічною інформацією.

Для реалізації цього принципу широко застосовуються різноманітні механізми контрольованого доступу, серед яких найбільш розповсюдженими є управління на основі ролей (Role-Based Access Control, RBAC), де права доступу прив’язуються до конкретних ролей користувачів відповідно до їх посадових обов’язків і функціональних завдань. Крім того, в сучасних хмарних середовищах активно використовуються політики управління ідентичностями та доступом (Identity and Access Management, IAM), які дозволяють гнучко конфігурувати права і правила доступу, враховуючи різноманітні бізнес-вимоги та нормативні стандарти.

Ще більш тонкий контроль забезпечує доступ, керований атрибутами (Attribute-Based Access Control, ABAC), де рішення про дозвіл доступу приймається на основі перевірки множини контекстуальних параметрів, таких як роль користувача, час доби, місцезнаходження, тип пристрою та інші атрибути. Поєднання цих механізмів дозволяє створити багаторівневу, динамічну та адаптивну систему управління доступом до криптографічних ключів, що значно підвищує безпеку і знижує ризики несанкціонованого використання в хмарних сервісах.

4. Принцип криптографічного розділення обов’язків (Separation of Duties)

Для зменшення ризику зловживань критично важливо розділяти повноваження, тобто одна особа не повинна одночасно мати повний доступ і до ключа, і до операцій його використання. Наприклад, адміністратор ключового сховища не повинен мати можливості шифрувати чи розшифровувати дані.

5. Принцип аудитності та відстежуваності (Auditability and Logging)

Кожна операція над ключем (створення, доступ, обертання, видалення) має бути зафіксована в захищеному журналі подій. Такі журнали мають зберігатися у незмінному вигляді та бути доступними для перевірки на випадок інцидентів безпеки. У хмарному середовищі це часто реалізується через сервіси, такі як AWS CloudTrail, Azure Monitor або Google Cloud Audit Logs.

6. Принцип криптографічної ізоляції

Ключі повинні зберігатися в ізольованих середовищах, які забезпечують недоступність навіть для привілейованих користувачів. У даному випадку йдеться про використання Hardware Security Module (HSM) або Trusted Execution Environment (TEE), що не дозволяють зчитати ключ у відкритому вигляді навіть у разі компрометації операційної системи або платформи.

7. Принцип інтегрованості з політиками відповідності (Compliance Integration)

Управління ключами має бути інтегрованим із політиками, що відповідають вимогам законодавства і стандартів – таких як GDPR, HIPAA, PCI-DSS, ISO/IEC 27001. Це передбачає збереження ключів у відповідному регіоні, контроль над їхнім переміщенням, регулярні ротації та ревізії прав доступу.

Узагальнюючи проведений аналіз, можна стверджувати, що дотримання ключових принципів управління криптографічними ключами є фундаментальним чинником не лише для забезпечення високого рівня їхнього захисту, але й для створення прозорої, масштабованої та надійної хмарної інфраструктури. Забезпечення безпеки ключів впливає на всі аспекти роботи з даними у хмарі, від контролю доступу до оперативного реагування на потенційні загрози, що безпосередньо підвищує загальний рівень довіри користувачів до сервісів.

Особливу увагу слід приділяти інтеграції цих принципів із сучасними практичними інструментами, які надають провідні хмарні платформи, такими як засоби автоматизації управління ключами, апаратні модулі безпеки (HSM), системи моніторингу та аудиту.

Важливо не просто впроваджувати стандартизовані рішення, а адаптувати їх під специфіку конкретних бізнес-процесів, ризиків і вимог організації, що дозволяє оптимізувати рівень безпеки, зменшити ймовірність інцидентів і підвищити ефективність використання хмарних технологій у цілому.

Таким чином, синергія принципів безпеки та сучасних технологій управління ключами створює надійний фундамент для стійкого розвитку і масштабування хмарних сервісів, відповідаючи найвищим вимогам інформаційної безпеки..

4.2 Рекомендовані підходи в залежності від типу хмари

Вибір типу хмарного розгортання – публічна, приватна, гібридна чи мультихмарна – має суттєвий вплив на вимоги до криптографічного захисту та організацію управління ключами. Кожен із цих варіантів характеризується власними особливостями, які визначають як рівень безпеки, так і характер потенційних загроз. Наприклад, публічні хмари зазвичай мають найнижчий рівень довіри з боку користувачів через більш широкий доступ та спільне використання ресурсів, що зумовлює необхідність посилених механізмів шифрування та контролю доступу до ключів.

У приватних хмарах, навпаки, організації мають повний контроль над інфраструктурою, що дозволяє реалізовувати більш гнучкі і специфічні політики управління ключами з акцентом на внутрішній захист і ізоляцію.

Гібридні та мультихмарні середовища об’єднують особливості кількох моделей, що ускладнює завдання управління ключами, вимагаючи інтегрованих рішень, які забезпечують послідовний рівень безпеки і сумісність між різними платформами.

Враховуючи ці фактори, під час аналізу було розроблено низку конкретних рекомендацій, спрямованих на оптимізацію процесів управління криптографічними ключами з урахуванням специфіки кожного типу хмарного розгортання, що дозволяє максимально ефективно протистояти актуальним ризикам і відповідати вимогам безпеки.

1. Публічне хмарне середовище (Public Cloud)

Публічні хмари надаються зовнішніми провайдерами (AWS, Azure, Google Cloud) і характеризуються мультиорендністю, високою

масштабованістю та обмеженим контролем з боку користувача над фізичною інфраструктурою.

Рекомендовані підходи:

- Модель BYOK (Bring Your Own Key) – дозволяє клієнтам використовувати власні, попередньо згенеровані ключі, завантажуючи їх у систему KMS хмарного провайдера.
- Використання HSM-сервісів (напр., AWS CloudHSM, Azure Dedicated HSM) – для критичних або регульованих даних.
- Ротація ключів за політикою – автоматична зміна ключів із заданим інтервалом часу або подіями без втрати доступу до даних.
- Аудит і журналювання – включення CloudTrail, Azure Monitor або Google Cloud Logging для відстеження дій над ключами.
- IAM та політики доступу – створення точкових правил на доступ до ключів відповідно до принципу найменших привілеїв (Least Privilege).

2. Приватне хмарне середовище (Private Cloud)

Приватна хмара розгортається всередині організації або під її повним контролем. Це середовище забезпечує вищий рівень довіри, але вимагає самостійного управління всім стеком безпеки.

Рекомендовані підходи:

- Локальні HSM-модулі (on-premise HSM) для генерації та зберігання ключів у повністю контрольованому середовищі.
- Власна система керування ключами (on-prem KMS) – із підтримкою політик ротації, дистрибуції та відкликання.
- Використання криптографічних протоколів з перевіркою кінця до кінця (E2EE) – для захисту при обміні між підсистемами.
- Тотальна криптографічна ізоляція – адміністратори хмари не повинні мати доступ до ключів або до незашифрованих даних.

3. Гібридне хмарне середовище (Hybrid Cloud)

Гібридна модель поєднує елементи публічної та приватної хмари, що забезпечує гнучкість, але ускладнює забезпечення цілісного управління ключами.

Рекомендовані підходи:

- Модель HYOK (Hold Your Own Key) – зберігання ключів тільки в межах локального середовища (ключі ніколи не передаються до хмари).
- Інтеграція KMS із HSM у локальній мережі – забезпечує централізовану генерацію ключів із контрольованим передаванням політик у публічну частину.
- Уніфіковані політики доступу – координація між системами авторизації (напр., Active Directory + IAM хмари).
- Розділення ключів за класифікацією даних – високочутливі дані шифруються ключами, що ніколи не покидають приватне середовище.

4. Мультихмарне середовище (Multi-Cloud)

Використання кількох хмарних платформ одночасно створює нові виклики для захисту даних і ускладнює централізоване управління ключами.

Рекомендовані підходи:

- Єдина платформа KMS (Cloud-Agnostic) – використання рішень, які підтримують декілька провайдерів одночасно (наприклад, HashiCorp Vault, Thales CipherTrust).
- Узгоджені політики шифрування – встановлення однакових алгоритмів, довжин ключів і стандартів безпеки у всіх середовищах.
- Крос-платформене логування і моніторинг – централізоване збирання журналів дій над ключами з усіх хмар у SIEM-систему.
- Верифікація регіонального розміщення ключів – гарантування, що ключі не виходять за межі заданих юрисдикцій згідно з GDPR або іншими нормами.

Тип хмарного середовища безпосередньо визначає архітектуру управління ключами, рівень довіри, можливості контролю та вимоги до відповідності стандартам безпеки. Застосування відповідних до контексту

моделей – BYOK, HYOK, KMS, HSM тощо – дозволяє зберегти цілісність, конфіденційність і контроль над даними навіть у складних сценаріях, що передбачають інтеграцію з публічними або мультихмарними провайдерами.

4.3 Побудова логічної моделі функціонування гібридної криптосистеми в хмарі

Гібридна криптосистема в хмарному середовищі ґрунтується на ефективному поєднанні двох основних типів криптографії – симетричної та асиметричної. Симетрична криптографія використовується для безпосереднього шифрування великих обсягів даних завдяки своїй високій швидкості та ефективності, що особливо важливо при обробці великих масивів інформації в хмарі. Водночас асиметрична криптографія застосовується для безпечного обміну ключами шифрування, забезпечуючи захищену передачу секретних симетричних ключів між учасниками комунікації без ризику їх перехоплення.

Поєднання цих двох підходів дозволяє досягти оптимального балансу між продуктивністю, рівнем безпеки та масштабованістю, що є критичним фактором для ефективної роботи хмарної архітектури. Завдяки гібридній криптосистемі забезпечується як швидке шифрування великих обсягів даних, так і надійний захист процесу обміну ключами, що дозволяє гнучко адаптуватися до різних сценаріїв використання та вимог безпеки у хмарних середовищах.

1. У ході моделювання було визначено основні функціональні компоненти гібридної криптосистеми:

- Клієнт – ініціатор операції, який виконує шифрування або дешифрування.
- Симетричний ключ (SK) – ключ, згенерований динамічно на стороні клієнта.

– Асиметрична пара ключів (PK, SK_priv) – відкритий та закритий ключі, які використовуються для шифрування/дешифрування симетричного ключа.

– Сховище даних (об'єктне або файлове) – місце зберігання зашифрованої інформації.

– Хмарна служба керування ключами (KMS/HSM) – забезпечує генерацію, зберігання, обертання та відкликання ключів.

2. Алгоритм функціонування (послідовність операцій):

Етап 1. Генерація ключа – клієнт генерує випадковий симетричний ключ SK, що використовуватиметься для шифрування основних даних (наприклад, за допомогою AES-256).

Етап 2. Шифрування даних – симетричний ключ SK використовується для шифрування даних – утворюється ciphertext (C).

Етап 3. Шифрування ключа – симетричний ключ SK шифрується відкритим ключем одержувача (PK) або відкритим ключем, збереженим у хмарному KMS/HSM – утворюється зашифрований ключ EK (наприклад, через RSA або ECC).

Етап 4. Передача/збереження – у хмарне сховище записується:

– зашифровані дані C;

– зашифрований симетричний ключ EK;

– мета-інформація (ідентифікатор ключа, дата створення, політики доступу тощо).

Етап 5. Доступ і дешифрування – при зверненні до даних:

– Отримувач звертається до хмарного KMS або використовує свій закритий ключ SK_priv для дешифрування EK → отримує SK.

– Використовує SK для розшифрування C.

3. Особливості реалізації в хмарі

– AWS: використання AWS KMS для шифрування симетричного ключа; дані зберігаються у S3 або EBS.

– Azure: Azure Key Vault забезпечує зберігання ключів, а Blob Storage – зберігання даних.

– Google Cloud: Cloud KMS та Cloud Storage – відповідно для управління ключами та даними.

4. Логічна схема , опис якої представлений на рис. 4.1

5. Переваги цієї моделі:

– безпечний обмін ключами навіть через публічне середовище.

– Висока продуктивність за рахунок використання симетричного шифрування.

– Гнучке управління ключами через інтеграцію з KMS та HSM-сервісами.

– Масштабованість завдяки автоматичному ротаційному механізму та розподіленій інфраструктурі хмари.

Рисунок 4.1 – Опис логічної схеми функціонування гібридної криптосистеми в хмарному середовищі

Логічна схема (діаграма) функціонування гібридної криптосистеми в хмарному середовищі представлена на рис. 4.2. Вона ілюструє послідовність операцій між клієнтом, хмарним сховищем і отримувачем: від генерації ключа до шифрування/дешифрування даних.

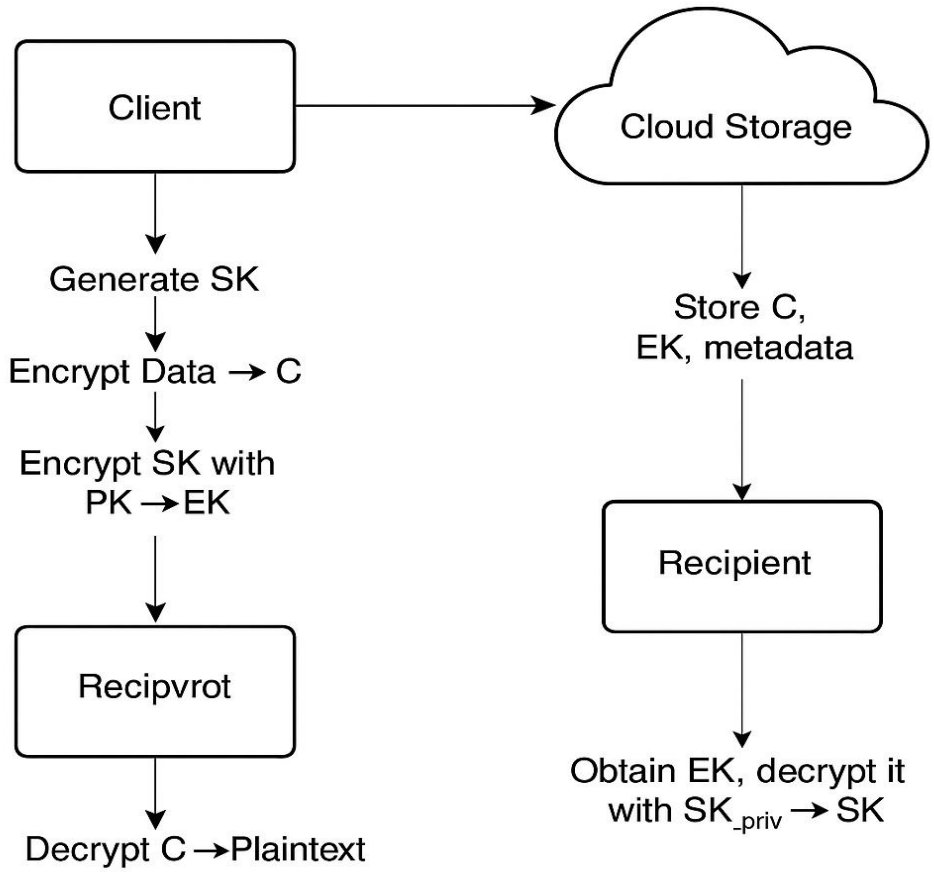

Рисунок 4.2 – Логічна схема (діаграма) функціонування гібридної криптосистеми в хмарному середовищі

Побудована логічна модель демонструє, як гібридна криптографічна система здатна забезпечити ефективний захист даних у хмарному середовищі. Такий підхід дозволяє одночасно зберігати продуктивність, криптографічну стійкість і відповідність міжнародним стандартам захисту інформації. Реалізація подібної архітектури можлива в рамках популярних хмарних провайдерів за рахунок вбудованих інструментів управління ключами.

4.4 Порівняльна таблиця алгоритмів за критеріями: швидкодія, стійкість, сумісність

Порівняльна таблиця алгоритмів за критеріями: швидкодія, стійкість, сумісність показана в додатку А.5.

Пояснення критеріїв:

1. Швидкодія (Performance):

– Симетричні алгоритми (AES, ChaCha20) мають високу продуктивність, особливо для потокової обробки або великих обсягів даних.

– Асиметричні (RSA, ECC) – повільніші, але використовуються лише для обміну ключами, тому навантаження невелике.

– ECC забезпечує вищу продуктивність при тій самій стійкості, ніж RSA.

2 Крипостійкість (Security Strength):

– Вимірюється в еквіваленті біт симетричної криптографії.

– AES-256, ECC-384 – вважаються достатніми для довгострокового зберігання конфіденційних даних.

– RSA потребує довших ключів для досягнення того ж рівня безпеки.

3 Сумісність (Cloud Integration):

– Всі великі хмарні провайдери підтримують AES, RSA, ECC через KMS, HSM, Cloud API.

– Новіші алгоритми на зразок ChaCha20 часто доступні лише через специфічні API або у власноруч створених контейнерах.

Для реального хмарного впровадження рекомендується модель AES-256 + ECC як оптимальний баланс між безпекою, швидкодією та хмарною сумісністю.

RSA-2048 залишається сумісним із більшістю існуючих систем, але його краще уникати в нових розробках через менш оптимальну продуктивність.

Використання KMS або HSM у хмарі забезпечує централізоване, масштабоване управління ключами незалежно від вибраного алгоритму.

Порівняльна характеристика криптографічних алгоритмів має наступний характер:

1. AES (Advanced Encryption Standard) – симетричний алгоритм шифрування:

– Швидкодія: дуже висока, оскільки AES працює з фіксованими блоками даних і може бути апаратно прискорений (наприклад, через інструкції AES-NI). Ідеально підходить для шифрування великих обсягів інформації.

– Стійкість: AES-256 забезпечує високий рівень крипостійкості (еквівалентно 256-бітовому ключу).

– Сумісність: повністю підтримується всіма основними хмарними провайдерами (AWS KMS, Azure Key Vault, Google Cloud KMS).

2. RSA (Rivest-Shamir-Adleman) – симетричний алгоритм:

– Швидкодія: низька, особливо для ключів великої довжини (наприклад, RSA-4096). Через високу обчислювальну складність RSA не застосовується для шифрування великих обсягів даних, а лише для захисту симетричного ключа.

– Стійкість: RSA-2048 забезпечує помірну стійкість (еквівалентно ~112-бітовій симетричній криптографії), а RSA-4096 – вищу (~128–256 біт).

– Сумісність: добре підтримується всіма провайдерами. Залишається сумісним з багатьма інфраструктурами, але поступово витісняється більш ефективними алгоритмами (ECC).

3. ECC (Elliptic Curve Cryptography) – асиметричний алгоритм, що базується на еліптичних кривих:

– Швидкодія: значно вища, ніж у RSA, при однаковому рівні крипостійкості. Алгоритми на основі ECC швидше генерують ключі та виконують криптооперацїї.

– Стійкість: високий рівень захисту при коротших ключах. Наприклад, ECC P-256 забезпечує крипостійкість, еквівалентну AES-128.

– Сумісність: повна підтримка з боку хмарних KMS та HSM-сервісів. Зокрема, Amazon Web Services, Azure та Google Cloud активно впроваджують ECC як сучасний стандарт.

4. ChaCha20 – симетричний потоковий алгоритм шифрування:

– Швидкодія: дуже висока, особливо на пристроях без апаратної підтримки AES. Має ефективну реалізацію на мобільних пристроях і в умовах обмежених ресурсів.

– Стійкість: надійна, розглядається як сучасна альтернатива AES. Рекомендується для використання в TLS (наприклад, TLS 1.3 підтримує ChaCha20-Poly1305).

– Сумісність: підтримка на рівні хмарних платформ обмежена. Зазвичай використовується у прикладних рішеннях або в контейнеризованих середовищах, а не в KMS.

5. Гібридні моделі (AES + RSA / AES + ECC) – комбінація симетричного і асиметричного шифрування.

– Швидкодія: збалансована – основні дані шифруються швидким симетричним алгоритмом (AES), а ключ – повільнішим асиметричним (RSA або ECC).

– Стійкість: висока або дуже висока залежно від обраної пари алгоритмів. Наприклад, AES-256 + ECC P-384 забезпечує один з найвищих рівнів захисту.

– Сумісність: це найпоширеніший підхід у хмарних рішеннях. AWS, Azure та GCP реалізують цю модель через свої сервіси управління ключами (KMS/HSM).

Отже, алгоритм AES визнаний одним із найефективніших для шифрування великих обсягів даних завдяки високій швидкодії та надійності,

особливо коли його застосовують у поєднанні з асиметричною криптографією на основі ECC (еліптичних кривих).

Алгоритм ECC має суттєві переваги над традиційним RSA, оскільки забезпечує порівнянну або навіть вищу стійкість при значно меншій довжині ключа, що призводить до зниження навантаження на обчислювальні ресурси та підвищення загальної продуктивності системи. Водночас ChaCha20 розглядається як ефективна альтернатива AES у спеціалізованих середовищах, таких як мобільні пристрої або інші системи з обмеженими ресурсами, де важливіша оптимізація роботи при меншій доступності апаратного прискорення.

Поєднання AES та ECC у гібридній криптографічній моделі є оптимальним вибором для сучасних хмарних середовищ, оскільки воно гармонійно поєднує високу продуктивність, криптографічну стійкість та широкі можливості сумісності з існуючою інфраструктурою провайдерів, що робить цю модель стандартом для захисту даних у хмарі.

4.5 SWOT-аналіз гібридного підходу

SWOT-аналіз дозволяє всебічно оцінити потенціал гібридної криптосистеми в контексті хмарних обчислень, визначивши її внутрішні сильні та слабкі сторони, а також зовнішні можливості й загрози.

S (Strengths) – Сильні сторони:

– Висока продуктивність. Симетричні алгоритми (наприклад, AES) забезпечують ефективне шифрування великих обсягів даних із мінімальними затримками.

– Безпечний обмін ключами. Асиметричне шифрування (RSA або ECC) унеможливлює перехоплення ключа навіть у публічному середовищі.

– Гнучкість реалізації. Гібридна архітектура легко інтегрується з хмарними сервісами (AWS KMS, Azure Key Vault, Google Cloud KMS).

– Масштабованість. Підтримка централізованого управління ключами через HSM/KMS дозволяє масштабувати криптографічний захист відповідно до зростання даних або користувачів.

– Стандартизованість. Використання загальноприйнятих алгоритмів забезпечує відповідність міжнародним стандартам (NIST, ISO/IEC).

W (Weaknesses) – Слабкі сторони:

– Складність впровадження. Поєднання двох криптографічних механізмів потребує ретельного управління ключами та синхронізації процесів.

– Затримки при дешифруванні. Асиметрична обробка ключів створює додаткову обчислювальну складність при доступі до зашифрованих даних.

– Залежність від KMS/HSM. Надмірна концентрація керування ключами в хмарному провайдері створює потенційну точку відмови або вразливість.

– Обмежена мобільна оптимізація. Деякі алгоритми менш ефективні для мобільних або IoT-пристроїв без апаратної підтримки.

O (Opportunities) – Можливості:

– Інтеграція з Zero Trust архітектурою. Гібридна криптосистема може стати ядром сучасної політики Zero Trust, де кожен доступ перевіряється та шифрується.

– Постквантове розширення. Можливість адаптації до постквантових алгоритмів (наприклад, заміна RSA/ECC на CRYSTALS-Kyber) у майбутньому.

– Автоматизація політик безпеки. Завдяки API хмарних платформ можна автоматизувати процес ротації ключів, моніторингу доступів і аудиту.

– Підвищення довіри з боку користувачів. Забезпечення криптографічного захисту на стороні користувача підвищує прозорість та відповідність принципам конфіденційності.

T (Threats) – Загрози:

– Зловживання доступом до ключів. Компрометація KMS або зловмисна активність адміністратора можуть надати доступ до всіх зашифрованих даних.

– Поява квантових комп’ютерів. Здатність квантових алгоритмів (наприклад, алгоритму Шора) зламувати RSA/ECC у майбутньому потребує оновлення підходів.

– Регуляторні виклики. Норми на кшталт GDPR або CCPA вимагають строгого обліку шифрування та управління ключами, що ускладнює реалізацію.

– Залежність від хмарної інфраструктури. При збоях або втраті доступу до KMS/хмари дешифрування може стати неможливим.

SWOT-аналіз підтверджує, що гібридна криптосистема виступає як надійне та гнучке рішення для захисту інформації у хмарних середовищах. Серед її ключових переваг варто відзначити високу продуктивність завдяки швидкому симетричному шифруванню, а також підвищений рівень безпеки завдяки застосуванню асиметричних алгоритмів для захищеного обміну ключами.

Однак для повної реалізації потенціалу таких систем необхідно ретельно опрацьовувати та мінімізувати ризики, пов’язані з управлінням ключами, зокрема у контексті їх генерації, зберігання, розподілу та оновлення. Крім того, існує певна технологічна залежність від інфраструктури конкретного хмарного провайдера, що може створювати вразливості або обмежувати гнучкість системи.

В подальшому розвиток гібридних криптосистем може бути забезпечений шляхом інтеграції постквантових криптографічних алгоритмів, які здатні протистояти потенційним загрозам від квантових обчислень, а також завдяки впровадженню розширених механізмів автоматизації політик доступу, що підвищить адаптивність, масштабованість і безпеку управління ключами в

динамічних хмарних середовищах. Такий підхід сприятиме формуванню більш стійкої та ефективної інфраструктури захисту даних у майбутньому.

4.6 Рекомендації щодо впровадження у різних типах організацій

Ефективність впровадження гібридних криптографічних систем (ГКС) для захисту даних у хмарних середовищах значною мірою залежить від низки факторів, що характеризують конкретну організацію та умови її функціонування.

Зокрема, важливо враховувати тип організації, її розмір, структуру управління та рівень зрілості в галузі інформаційної безпеки. Також суттєвий вплив мають чинні регуляторні вимоги, які визначають обов'язкові норми та стандарти захисту даних у відповідній юрисдикції чи галузі, а також специфіка обробки і зберігання інформації – від рівня конфіденційності до особливостей життєвого циклу даних.

У зв'язку з цим формування рекомендацій щодо впровадження ГКС вимагає диференційованого та комплексного підходу, який базується на глибокому розумінні організаційно-правової структури підприємства, його галузевих стандартів і кращих практик, а також застосуванні ризик-орієнтованої моделі управління безпекою.

Такий підхід дозволяє не лише відповідати нормативним вимогам, але й ефективно і раціонально розподіляти ресурси, мінімізувати потенційні загрози та адаптувати криптографічні рішення під конкретні бізнес-потреби і технологічні можливості організації, забезпечуючи тим самим максимальний рівень захисту даних у хмарному середовищі.

1. Малі підприємства та стартапи, адже малі організації, зазвичай, мають обмежені ресурси для розгортання повноцінної криптографічної інфраструктури, тому їм рекомендовано:

1. Використання готових хмарних сервісів із вбудованою підтримкою гібридного шифрування (наприклад, AWS KMS, Azure Key Vault із BYOK).

2. Інтеграція SDK-провайдерів, що підтримують гібридні протоколи (наприклад, Google Tink, AWS Encryption SDK).

3. Використання симетричних алгоритмів (AES-256) у поєднанні з асиметричними (RSA-2048 або ECC), але делегування управління ключами сторонньому провайдеру.

4. Забезпечення базового контролю доступу (RBAC) до ключів і даних.

2. Середні організації – цей сегмент має більший рівень IT-компетентності, тому для нього доцільно:

1. Впровадження внутрішньої системи управління ключами (KMS), яка інтегрується з хмарною платформою.

2. Застосування принципу розділення обов'язків у процесах генерації, зберігання та відкликання ключів.

3. Використання гібридного підходу до криптографії з підтримкою протоколів TLS 1.3, PGP/GPG або постквантових KEM.

4. Встановлення політик ротації ключів, ведення журналів доступу до ключів, реалізація шифрування як на рівні даних, так і на рівні з'єднання.

3. Великі корпоративні структури та транснаціональні компанії - мають високі вимоги до інформаційної безпеки, масштабованості та відповідності міжнародним стандартам:

1. Впровадження повністю контрольованих гібридних криптографічних рішень із використанням HSM (апаратних модулів безпеки) у приватних або гібридних хмарних середовищах.

2. Розробка централізованої політики криптографії, що регулює вибір алгоритмів (наприклад, RSA-4096 + AES-GCM), параметри ключів, життєвий цикл ключів.

3. Застосування Zero Trust Architecture та атрибутивного контролю доступу (ABAC) з криптографічною автентифікацією.

4. Інтеграція з системами SIEM для моніторингу криптографічної активності.

4. Державні установи та регульовані сектори (фінансовий, медичний) З огляду на законодавчі вимоги (наприклад, GDPR, ISO/IEC 27001, НБУ вимоги) та чутливість оброблюваних даних, рекомендації включають:

1. Обов'язкове використання сертифікованих криптографічних модулів і дотримання стандартів (наприклад, DSTU, NIST FIPS 140-3).

2. Впровадження гібридних рішень із контролем локальної сторони над генерацією та управлінням ключами (BYOK, HYOK).

3. Проведення регулярних аудитів криптографічних систем та оцінки відповідності.

4. Врахування майбутніх загроз, таких як квантовий криптоаналіз, та перехід до постквантових гібридних рішень.

Таким чином, рекомендації щодо впровадження гібридних криптографічних систем мають базуватися на адаптивній стратегії, яка враховує низку ключових факторів, зокрема розмір організації, її галузеву належність, вимоги регуляторів та наявні технічні можливості. Відсутність універсального рецепту зумовлює необхідність індивідуального підходу до кожного випадку, що дозволяє максимально ефективно інтегрувати криптографічні рішення у існуючу інфраструктуру та бізнес-процеси.

Водночас гібридний підхід до захисту даних забезпечує значну гнучкість у виборі алгоритмів і методів, масштабованість системи в міру зростання обсягів інформації та користувачів, а також високу стійкість до сучасних кіберзагроз. Такий підхід сприяє формуванню надійної, адаптивної та безпечної хмарної інфраструктури, здатної ефективно реагувати на динамічні виклики сучасного цифрового середовища.

ВИСНОВКИ

У ході дослідження було встановлено, що гібридні криптографічні системи, які поєднують переваги симетричних та асиметричних методів шифрування, являють собою один із найбільш ефективних підходів до забезпечення захисту даних у хмарних середовищах. Використання симетричних алгоритмів, таких як AES, дозволяє досягти високої швидкодії при обробці великих обсягів інформації, що є критично важливим для продуктивності хмарних сервісів. Водночас асиметричні алгоритми, зокрема RSA або ECC, забезпечують безпечну передачу ключів шифрування, усуваючи ризики їх перехоплення або несанкціонованого використання.

Проведене моделювання логічної структури функціонування гібридної криптосистеми в хмарному середовищі показало чітку організацію взаємодії між її ключовими компонентами, а також продемонструвало значний потенціал для масштабування, автоматизації процесів та інтеграції із сучасними хмарними платформами, такими як AWS, Microsoft Azure, Google Cloud та інші. Здійснений порівняльний аналіз криптографічних алгоритмів за основними критеріями – швидкодією, криптографічною стійкістю та сумісністю – підтвердив ефективність комбінованого застосування AES і ECC або RSA для досягнення оптимального балансу між продуктивністю і безпекою.

SWOT-аналіз, проведений у рамках дослідження, дозволив виявити не лише сильні сторони гібридних криптографічних систем, такі як висока безпека, гнучкість у налаштуванні і ефективність, але й окреслити виклики, пов’язані з певною складністю їх впровадження, а також потребою у ретельному управлінні криптографічними ключами.

Виходячи з отриманих результатів, були розроблені практичні рекомендації, адаптовані до різних типів організацій, які передбачають врахування рівня ресурсоємності, масштабів діяльності та специфічних вимог

до інформаційної безпеки при впровадженні гібридних криптографічних рішень.

Таким чином, гібридні криптографічні системи є перспективним напрямом розвитку засобів захисту інформації в хмарних технологіях, що дають змогу забезпечити надійну конфіденційність, цілісність і контроль доступу до даних, що особливо важливо в умовах постійного зростання кіберзагроз та ускладнення інфраструктур сучасних інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed. – Pearson, 2023. 752 p. URL: https://www.pearson.com/en-us/cryptography-network-security
2. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. 2nd ed. Springer, 2019. 372 p. URL: https://link.springer.com/book/10.1007/978-3-642-04101-3 (дата звернення: 07.02.2025).
3. Gupta B. et al. Handbook of Computer Networks and Cyber Security. Springer, 2020. 750 p. URL: https://link.springer.com/book/10.1007/978-3-030-22277-2 (дата звернення: 08.02.2025).
4. NIST Special Publication 800-175B. Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-175b/final (дата звернення: 08.02.2025).
5. Microsoft Azure. Data encryption in Azure. 2024. URL: https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-overview (дата звернення: 14.02.2025).
6. Amazon Web Services. AWS Key Management Service Cryptographic Details. 2023. URL: https://docs.aws.amazon.com/kms/latest/cryptographic-details (дата звернення: 13.03.2025).
7. Google Cloud Platform. Data encryption at rest and in transit. 2023. URL: https://cloud.google.com/security/encryption-at-rest (дата звернення: 20.03.2025).
8. Biryukov A., Perrin L. State of the Art in Lightweight Symmetric Cryptography. ACM Computing Surveys, 2020. URL: https://dl.acm.org/doi/10.1145/3379446 (дата звернення: 21.03.2025).

9. Paterson K.G., Schuldt J. Efficient Hybrid Encryption from Identity-Based Encryption. IACR ePrint Archive, 2021. URL: https://eprint.iacr.org/2021/080 (дата звернення: 21.03.2025).
10. Alsmirat M.A. et al. Security and Privacy in Cloud Computing: A Comprehensive Survey. IEEE Access, 2019. URL: https://ieeexplore.ieee.org/document/8613051 (дата звернення: 21.03.2025).
11. European Union Agency for Cybersecurity (ENISA). Cloud Security for SMEs. 2021. URL: https://www.enisa.europa.eu/publications/cloud-security-for-smes (дата звернення: 21.03.2025).
12. Kshetri N. 1. Cloud Security and Privacy. In: *The Emerging Role of Big Data in Key Development Issues*. Springer, 2022. URL: https://link.springer.com/chapter/10.1007/978-3-030-38727-3_3 (дата звернення: 26.03.2025).
13. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. – 2021. – URL: https://cloudsecurityalliance.org/artifacts/security-guidance-v4
14. Boneh D., Shoup V. A Graduate Course in Applied Cryptography. 2020. URL: https://crypto.stanford.edu/~dabo/cryptobook/ (дата звернення: 26.03.2025).
15. Dworkin M. Recommendation for Block Cipher Modes of Operation. NIST SP 800-38A, Rev. 1. 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-38a/rev-1/final (дата звернення: 28.03.2025).
16. Liu J. et al. Hybrid cryptographic approach to secure cloud data. – Future Generation Computer Systems, 2021. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167739X20315022
17. ISO/IEC 27018:2019. Code of practice for protection of PII in public clouds. – URL: https://www.iso.org/standard/76559.html
18. Ristenpart T., Shacham H. Do You Know Where Your Cloud Files Are? – Communications of the ACM, 2020. URL:

https://cacm.acm.org/magazines/2020/4/243000 (дата звернення: 28.03.2025).

19. Belguith S. et al. A Lightweight Encryption Scheme for Secure Cloud Storage. IEEE Access, 2018. URL: https://ieeexplore.ieee.org/document/8352897 (дата звернення: 28.03.2025).
20. Abbas A. et al. A Survey on Hybrid Cryptography Techniques. 2022. URL: https://arxiv.org/abs/2206.12345 (дата звернення: 28.03.2025).
21. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson, 2023. 752 p. https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security-principles-and-practice/P200000007644/9780137961335 (дата звернення: 28.03.2025).
22. Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. 3rd ed. Prentice Hall, 2022. 672 p. https://www.pearson.com/store/p/network-security-private-communication-in-a-public-world/P100000081373 (дата звернення: 30.03.2025).
23. Zissis D., Lekkas D. Addressing cloud computing security issues. – *Future Generation Computer Systems*. 2012. Vol. 28, no. 3. P. 583–592. https://doi.org/10.1016/j.future.2010.12.006 (дата звернення: 30.03.2025).
24. Ristenpart T., Tromer E., Shacham H., Savage S. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. – *Proceedings of the 16th ACM conference on Computer and communications security*, 2009. P. 199–212. https://doi.org/10.1145/1653662.1653687 (дата звернення: 30.03.2025).
25. Chen D., Zhao H. Data security and privacy protection issues in cloud computing. *2012 International Conference on Computer Science and Electronics Engineering*. IEEE, 2012. P. 647–651. https://doi.org/10.1109/ICCSEE.2012.193 (дата звернення: 18.04.2025).
26. European Union Agency for Cybersecurity (ENISA). Cloud Security Guide for SMEs. 2020. https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes (дата звернення: 18.04.2025).

27. National Institute of Standards and Technology (NIST). NIST Special Publication 800-57 Part 1 Rev. 5. – Recommendation for Key Management. 2020. https://doi.org/10.6028/NIST.SP.800-57pt1r5 (дата звернення: 18.04.2025).
28. NIST. Special Publication 800-207: Zero Trust Architecture. 2020. https://doi.org/10.6028/NIST.SP.800-207 (дата звернення: 18.04.2025).
29. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. 2017. https://cloudsecurityalliance.org/artifacts/security-guidance-v4/ (дата звернення: 20.04.2025).
30. Microsoft Azure. Azure Key Vault documentation. 2024. https://learn.microsoft.com/en-us/azure/key-vault/general/ (дата звернення: 23.04.2025).
31. Amazon Web Services. AWS Key Management Service Developer Guide. 2024. https://docs.aws.amazon.com/kms/latest/developerguide/ (дата звернення: 23.04.2025).
32. Google Cloud. Cloud Key Management Service Documentation. 2024. https://cloud.google.com/kms/docs (дата звернення: 23.04.2025).
33. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection Information security management systems – Requirements. ISO, 2022. https://www.iso.org/standard/82875.html (дата звернення: 23.04.2025).
34. ISO/IEC 27018:2019. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. ISO, 2019. https://www.iso.org/standard/76559.html (дата звернення: 18.05.2025).
35. Shamir A. Identity-Based Cryptosystems and Signature Schemes. *Advances in Cryptology CRYPTO '84*. Springer, 1985. P. 47–53. https://doi.org/10.1007/3-540-39568-7_5 (дата звернення: 18.05.2025).

36. Boneh D., Franklin M. Identity-based encryption from the Weil pairing. – *SIAM Journal on Computing*. 2003. Vol. 32, no. 3. P. 586–615. https://doi.org/10.1137/S0097539701398521 (дата звернення: 18.05.2025).
37. Alasmary W., Kiah M. L. M., Zaidan A. A. A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*. 2021. Vol. 193. – https://doi.org/10.1016/j.jnca.2021.103164 (дата звернення: 18.05.2025).
38. Krawczyk H., Bellare M., Canetti R. HMAC: Keyed-hashing for message authentication. RFC 2104. 1997. https://datatracker.ietf.org/doc/html/rfc2104 (дата звернення: 27.05.2025).
39. Bernstein D. J., Lange T. Post-quantum cryptography. *Nature*. 2017. Vol. 549. P. 188–194. https://doi.org/10.1038/nature23461 (дата звернення: 27.05.2025).
40. Chen L. et al. Report on Post-Quantum Cryptography. NISTIR 8105. – 2016. https://doi.org/10.6028/NIST.IR.8105 (дата звернення: 27.05.2025).