КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.901
УДК 004.056

Трофімов Олександр Сергійович
аспірант
Київський столичний університет імені Бориса Грінченка, Київ, Україна

o.trofimov.asp@kubg.edu.ua

МЕТОД КОМБІНОВАНОГО ШИФРУВАННЯ ДАНИХ В ХМАРНИХ СЕРЕДОВИЩАХ

Анотація. Стаття присвячена розробленню методу криптографічного захисту даних у корпоративних хмарних середовищах на засадах концепції Zero Trust з урахуванням вимог до продуктивності, масштабованості та прогнозованості затримок. У вступі обґрунтовано актуальність теми в умовах переходу корпоративних систем до хмарних сервісів, зростання кількості кіберзагроз і потреби поєднати криптографічну стійкість із практичними обмеженнями експлуатації. У розділі аналізу досліджень розглянуто нормативну та наукову базу, що охоплює як міжнародні, так і національні стандарти інформаційної безпеки, підходи Zero Trust, моделі контролю доступу та шифрування. Сформульовано проблему відсутності цілісного методу, який одночасно враховував би модель загроз, розмежування рівнів довіри, керування ключами та часові обмеження високонавантажених систем. У дослідницькій частині показано, що гомоморфне шифрування, попри переваги для обробки зашифрованих даних, не може використовуватися як базовий механізм захисту сховищ через значні обчислювальні накладні витрати. Обґрунтовано доцільність його використання лише як окремого сервісного рівня для спеціалізованих сценаріїв. Основну увагу зосереджено на архітектурних засадах методу: недовірі до інфраструктури провайдера, клієнтському

Ключові слова: криптографічний захист даних; корпоративні хмарні середовища; Zero Trust; керування криптографічними ключами; гомоморфне шифрування.

ВСТУП

В умовах масового переходу корпоративних інформаційних систем від локальних до хмарних середовищ питання забезпечення захищеного зберігання і обробки даних набуває критичного значення. На фоні зростання кількості застосувань подібних технологій, збільшується і кількість загроз, значну частину яких складають цілеспрямовані кібератаки. У відповідь на ці виклики міжнародні та національні стандарти пропонують комплексні підходи до побудови систем управління інформаційною безпекою що базуються на концепції «Повної недовіри» (Zero Trust) як основі сучасних політик захисту.

Криптографічний захист даних у хмарі вимагає балансу між криптографічними гарантами та експлуатаційними вимогами — продуктивністю, прогнозованістю

© О.С. Трофімов, 2025

затримок та дотриманням обмежень на допустиму затримку виконання операцій (SLA). На практиці це означає застосовування механізми, що забезпечують необхідний рівень безпеки, але при цьому не роблять систему непридатною для реальних навантажень.

Постановка проблеми. Хмарні сервіси функціонують в умовах підвищеного навантаження та жорстких вимог до продуктивності, що ускладнює застосування ресурсоємних криптографічних механізмів. Попри наявність нормативних вимог і поширення концепції Zero Trust, залишається відкритим питання розроблення цілісного криптографічного методу, який би поєднував формалізовану модель загроз, розмежування рівнів довіри, керування ключами та узгодження криптографічних механізмів із часовими обмеженнями високонавантажених систем.

Аналіз останніх досліджень і публікацій. Нормативною основою побудови систем захисту інформації в Україні є міжнародні та національні стандарти у сфері інформаційної безпеки. Зокрема ДСТУ ISO/IEC 27001:2023, що визначає вимоги до систем керування інформаційною безпекою та формалізує ризикоорієнтований підхід до впровадження організаційних і технічних заходів захисту [1]. У контексті хмарних обчислень концепція «Повної недовіри», викладена в NIST SP 800-207, пропонує архітектурну модель, у якій жоден компонент інфраструктури не вважається довіреним доки не буде доведено зворотне, а рішення щодо доступу приймаються з урахуванням ідентичності, контексту та політик безпеки [2].

Важливою складовою національного регуляторного поля є стандарти криптографічного захисту — ДСТУ 7624:2014 (алгоритм «Калина») та ДСТУ 7564:2014 (функція гешування «Купина») [3], [4]. Їх використання забезпечує відповідність національним вимогам у сфері криптографії та створює підґрунтя для формування власних криптографічних профілів захисту хмарних сервісів.

Питання забезпечення стійкості гарантоздатних інформаційних систем до сучасних кіберзагроз, зокрема до атак із застосуванням шкідливого програмного забезпечення шифрувального типу, детально розглянуто в роботі [5]. Автори підкреслюють необхідність формалізованих процедур керування ключами, журналювання подій та ізоляції доменів безпеки як базових умов забезпечення відновлюваності та стійкості систем.

Окремі аспекти захисту даних у хмарних середовищах також досліджуються в контексті моделей контролю доступу та управління ідентифікацією. Зокрема, у роботі [6] йдеться про модель безпеки хмарних сервісів на основі механізмів керування ідентифікацією та доступом (IAM), що дозволяє деталізувати політики доступу та підвищити рівень керованості.

У публікаціях [7] проаналізовано загрози, пов’язані з використанням хмарних сервісів, і підкреслено ризики витоку даних та залежності від провайдера.

Дослідження [8] розглядає синтез типових алгоритмів захисту інформації в корпоративних мережах і вказує на необхідність комплексного підходу до інтеграції криптографічних та організаційних механізмів.

У роботі [9] досліджено уразливості шифрування коротких повідомлень у інформаційно-комунікаційних системах. Автори акцентують увагу на ризиках некоректної реалізації криптографічних механізмів та порушеннях при використанні параметрів, що призводить до зниження фактичної криптостійкості систем навіть при застосуванні формально надійних алгоритмів.

Попри значний обсяг публікацій, більшість досліджень або зосереджується на теоретичних аспектах шифрування, або розглядає загальні питання менеджменту

інформаційної безпеки без детальної формалізації криптографічних профілів для різних типів хмарних сховищ. Недостатньо дослідженим залишається питання архітектурного розмежування рівнів застосування криптографії, формалізації контексту автентичності даних і узгодження криптографічних механізмів із часовими обмеженнями в корпоративних хмарних системах.

Мета статті. Метою статті є розроблення та обґрунтування методу криптографічного захисту даних у корпоративних хмарних системах на засадах концепції «Повної недовіри» з урахуванням експлуатаційних обмежень і вимог до продуктивності.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Контекст застосування криптографії в корпоративних хмарних системах

Корпоративні хмарні системи функціонують в умовах високої інтенсивності введення-виведення, жорстких вимог до доступності та прогнозованої затримки, а також необхідності дотримання нормативних вимог щодо захисту інформації [7], [10].

У парадигмі концепції «Повної недовіри» інфраструктура провайдера хмарних сервісів не входить до кола довіри, а отже, криптографічний захист має реалізовуватися таким чином, щоб дані залишалися захищеними незалежно від безпеки транспортного середовища, гіпервізора або систем зберігання [2], [10]. У цьому контексті ключову роль відіграє клієнтське шифрування даних із криптографічно гарантованою цілісністю та контрольованим життєвим циклом ключів [1], [11].

Разом з тим у наукових і прикладних роботах дедалі частіше розглядається можливість застосування гомоморфного шифрування як універсального засобу захисту даних у хмарних обчисленнях [12] – [15]. Це зумовлює необхідність чіткого визначення місця таких схем у загальній архітектурі корпоративних хмарних систем.

Можливості та обмеження гомоморфного шифрування

Гомоморфне шифрування дозволяє виконувати обчислення над зашифрованими даними без розкриття відкритого тексту, що теоретично усуває необхідність довіряти обчислювальному середовищу. Ця властивість робить гомоморфні схеми привабливими для задач приватної аналітики, обробки чутливих даних та делегування обчислень у недовірене середовище [12] – [16].

Водночас практичне застосування повністю гомоморфного шифрування супроводжується суттєвими обмеженнями. Основними з них є значні накладні витрати на обчислення, збільшення обсягів даних та залежність часу виконання операцій від глибини обчислювального кола [12] – [17]. У корпоративних хмарних системах, орієнтованих на інтенсивні операції, такі обмеження є критичними [7], [10]. Сервіси об’єктного, файлового та блочного доступу потребують передбачуваної затримки та високої пропускної здатності, що не відповідає типовим характеристикам повністю гомоморфних схем [16], [17].

Часові обмеження та непридатність повністю гомоморфного шифрування як базового механізму захисту сховищ

Для формального обґрунтування доцільності використання різних криптографічних підходів розглянемо часову модель виконання операцій введення-виведення в корпоративній хмарній системі. Загальний час виконання операції може бути поданий у вигляді формули 1:

$$T_{\text{total}} = T_{\text{I/O}} + T_{\text{crypto}}, \quad (1)$$

де T_{total} — загальний час виконання операції, $T_{\text{I/O}}$ — час виконання операцій зберігання без урахування криптографічної обробки, T_{crypto} — час, витрачений на криптографічні перетворення.

Для забезпечення заданих показників допустимої затримки виконання операцій (SLA), частка часу, що витрачається на криптографічну обробку, обмежується деяким коефіцієнтом $\beta \in (0,1)$ [10], що обчислюється за формулою 2:

$$T_{\text{crypto}} \leq \beta \cdot L_{\text{SLA}}, \quad (2)$$

де L_{SLA} — гранично допустима затримка відповідно до SLA, β — допустима частка криптографічних накладних витрат.

Для режимів автентифікованого симетричного шифрування (AEAD) час криптографічної обробки масштабуються лінійно від розміру повідомлення та добре узгоджуються з встановленими обмеженнями за наявності апаратного прискорення [18, 19]. Натомість для повністю гомоморфних схем час обчислень суттєво перевищує допустимі межі навіть для відносно простих операцій, що робить їх непридатними як базовий механізм захисту даних у сховищах корпоративних хмарних систем.

Таким чином, використання гомоморфного шифрування як основного засобу захисту даних на рівні сховищ суперечить вимогам до продуктивності, масштабованості та прогнозованості затримок.

Місце гомоморфного шифрування в запропонованій архітектурі

З огляду на наведені обмеження, гомоморфне шифрування пропонується розглядати не як альтернативу базовим криптографічним механізмам захисту сховищ, а як допоміжний інструмент для окремих класів задач.

Пропонований метод виходить із таких принципів:

–базовий захист даних у корпоративних хмарних сховищах реалізується за допомогою симетричних режимів автентифікованого шифрування та спеціалізованих режимів для блочного доступу [18], [19];

–криптографічні механізми повинні забезпечувати мінімальні накладні витрати та відповідати часовим обмеженням [10], [18];

–гомоморфне шифрування може застосовуватися як окремий сервісний рівень для задач обробки зашифрованих даних, де допустимі підвищені затримки та обмежена складність обчислень [15], [16].

Таким чином, гомоморфні схеми доцільно використовувати для вибіркових сценаріїв, таких як пакетна аналітична обробка або спеціалізовані обчислювальні сервіси, але не для базових операцій зберігання та доступу до даних.

Архітектурні засади та модель загроз

Запропонований метод базується на архітектурних принципах парадигми концепції «Повної недовіри» та орієнтований на забезпечення конфіденційності, цілісності й актуальності даних незалежно від рівня довіри до інфраструктури провайдера. Метод розглядає криптографічний захист не як сукупність окремих алгоритмів або протоколів, а як цілісну систему узгоджених рішень, адаптованих до реальних умов експлуатації хмарних сховищ.

Архітектурні принципи методу

Базовим принципом побудови методу є недовіра до інфраструктури. Усі компоненти хмарного середовища, включно з мережами, сервісами зберігання, обчислювальними платформами та засобами віртуалізації, розглядаються як потенційно недовірені. Криптографічні гарантії безпеки даних не повинні залежати від коректності реалізації або політик безпеки провайдера. Відповідно, метод реалізує клієнтський криптографічний захист, за якого всі критичні криптографічні перетворення виконуються на стороні клієнта або в довіреному домені керування ключами. Сервіси зберігання та транспортні компоненти оперують виключно зашифрованими даними й автентифікаційними тегами та не мають доступу до відкритого тексту або ключового матеріалу.

Ще одним невід'ємним принципом є обов'язкове поєднання конфіденційності та цілісності даних. Метод орієнтований на використання режимів автентифікованого шифрування або еквівалентних конструкцій, що забезпечують криптографічну перевірку цілісності кожної одиниці даних.

Окрему роль відіграє принцип формалізованого криптографічного контексту. Кожна операція шифрування виконується в чітко визначеному контексті, що включає ідентифікатори ресурсу, версію політики захисту та інші незмінні параметри. Такий підхід забезпечує криптографічну прив'язку даних до їх логічного розташування та стану й унеможливлює «атаки повтору» (повторне використання раніше коректного шифротексту або фрагмента даних), «перестановки» (зміна логічного розташування коректних фрагментів даних без їх модифікації) та «відкату» (підміна актуальної версії даних їх попередньою коректною версією).

Розмежування рівнів застосування криптографії

Метод передбачає чітке логічне розмежування рівнів застосування криптографічних механізмів, що дозволяє уникнути ототожнення транспортного захисту з безпекою даних у стані зберігання.

1) Транспортний рівень

Охоплює механізми захисту каналів зв'язку між клієнтами та компонентами хмарної інфраструктури. Його призначенням є забезпечення конфіденційності й цілісності передавання даних та команд управління, а також зниження ризиків активних мережевих атак.

Водночас транспортний рівень розглядається як допоміжний і не використовується для забезпечення довгострокової криптографічної безпеки даних у сховищі.

2) Рівень сховищ

Є центральним у запропонованій методиці. Саме на цьому рівні реалізуються основні криптографічні гарантії безпеки даних, незалежні від типу транспортного протоколу або конкретної реалізації інфраструктури. Захист на рівні сховищ забезпечує конфіденційність даних у стані зберігання, криптографічно гарантовану цілісність кожної одиниці даних та захист від атак, пов'язаних з маніпуляціями над їх розміщенням і версіями.

3) Рівень реалізації

Охоплює програмні та апаратні засоби, за допомогою яких застосовуються криптографічні механізми, зокрема криптографічні бібліотеки, сервіси керування ключами та апаратні модулі безпеки. У межах метод цей рівень розглядається абстрактно, без прив'язки до конкретних платформ або виробників, з фокусом на вимоги до коректності реалізації, керованості та можливості аудиту.

Модель загроз і припущення безпеки

Модель загроз формується відповідно до парадигми концепції «Повної недовіри» та ґрунтується на припущенні, що всі компоненти хмарної інфраструктури, за винятком клієнтського середовища та довіреного домену керування ключами, є потенційно недовіреними. Такий підхід означає, що криптографічні гарантії конфіденційності, цілісності й актуальності даних не повинні залежати від коректності реалізації, налаштувань або політик безпеки провайдера хмарних сервісів.

До потенційно недовірених компонентів належать мережеві комунікації, сервіси зберігання, обчислювальні середовища провайдера, гіпервізори, а також адміністративний персонал, який не входить до домену безпеки клієнта. Межа довіри проходить між клієнтським середовищем і доменом керування ключами з одного боку та інфраструктурою провайдера — з іншого.

На рисунку 1 відображено логічне розмежування довіреного домену та потенційно недовіреної інфраструктури, позначено межу довіри (Zero Trust Boundary) та показано напрям передавання даних у зашифрованому вигляді через транспортний рівень до сервісів зберігання.

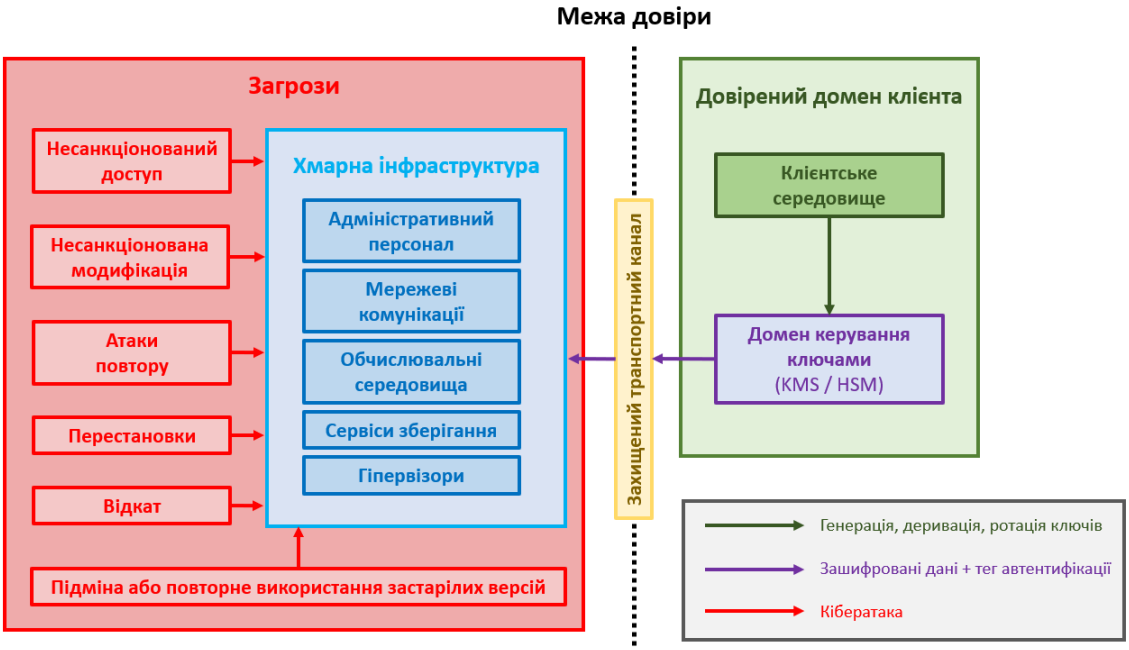

Рис. 1. Модель загроз методу криптографічного захисту даних у корпоративній хмарній системі на засадах концепції «Повної недовіри»

Запропонований метод спрямований на протидію таким класам загроз:

–несанкціонований доступ до даних у сховищі;

–несанкціонована модифікація даних;

–атаки повтору;

–перестановки;

–відкату;

–атаки, пов’язані з підміною або повторним використанням застарілих версій даних.

Криптографічний захист реалізується таким чином, щоб будь-які спроби модифікації, перестановки або повторного використання раніше коректних фрагментів даних виявлялися на рівні перевірки автентичності. Використання захищених транспортних каналів розглядається як додатковий захисний шар, що зменшує ризики активних мережевих атак, однак не є основним механізмом забезпечення довгострокової безпеки даних у стані зберігання.

Криптографічні гарантії методу ґрунтуються на припущенні коректної реалізації обраних алгоритмів і режимів, збереження секретності ключового матеріалу протягом визначеного життєвого циклу та дотримання дисципліни використання криптографічних параметрів, зокрема унікальності значень ініціалізації. Порушення цих припущень розглядається як експлуатаційна або організаційна помилка та потребує окремих процедур реагування.

Захист даних на рівні сховищ

Як вже було визначено, рівень сховищ є центральним у запропонованій методиці, оскільки саме на ньому забезпечуються основні гарантії конфіденційності, цілісності та актуальності даних незалежно від транспортного середовища й конкретної реалізації хмарної інфраструктури. Метод виходить з того, що всі операції шифрування та перевірки цілісності виконуються на стороні клієнта або в довіреному домені керування ключами, тоді як сховища оперують виключно зашифрованими даними.

Залежно від типу доступу до даних (об’єктного, файлового або мережевого блочного) застосовуються різні криптографічні профілі, узгоджені спільними принципами формалізованого контексту автентичності та керованого життєвого циклу ключів.

Захист об’єктних і файлових хмарних сховищ

Об’єктні та файлові хмарні сховища характеризуються логічною адресацією даних, фрагментацією об’єктів і можливістю паралельного доступу. Для цього класу сховищ у методиці пропонується застосування принципу проєктування криптографічного захисту (AEAD-first), відповідно до якого автентифіковане симетричне шифрування (AEAD) використовується як базовий і обов’язковий механізм захисту даних на рівні сховищ. Формально операції шифрування та розшифрування описуються стандартною нотацією AEAD (3):

$$(C, \tau) = \mathrm{AEAD.Enc}_K(\mathrm{nonce}, P, \mathrm{AAD}),$$
$$P = \mathrm{AEAD.Dec}_K(\mathrm{nonce}, C, \mathrm{AAD}) \text{ або } \perp, \quad (3)$$

де C — шифротекст, P — відкритий текст, τ — тег автентичності, K — криптографічний ключ, nonce — унікальне значення ініціалізації, AAD — додаткові автентифіковані дані, $\perp$ — результат відмови у випадку порушення цілісності. $\mathrm{AEAD.Enc}_K$ — операція шифрування в режимі автентифікованого шифрування з додатковими даними з використанням ключа K, в свою чергу, $\mathrm{AEAD.Dec}_K$ — операція

розшифрування з перевіркою автентичності, яка повертає відкритий текст лише у разі успішної перевірки тега автентичності, або значення $\perp$ у випадку її невдачі. Розшифрування виконується лише після успішної перевірки тега автентичності (принцип *verify-then-decrypt*).

Для запобігання атакам повтору, перестановки та відкату використовується формалізований криптографічний контекст, який включається до додаткових автентифікованих даних (AAD). У загальному випадку AAD формується як конкатенація таких компонентів (4):

$$AAD = Tenant \parallel ObjID \parallel ver \parallel idx, \quad (4)$$

де Tenant — ідентифікатор орендаря або домену безпеки, ObjID — ідентифікатор об'єкта або файлу, ver — версія криптографічної політики або даних, idx — індекс фрагмента в межах об'єкта. $\parallel$ — операція конкатенації (кодування полів виконується в канонічному форматі з однозначним визначенням меж).

Унікальність значення nonce забезпечується детермінованим способом на основі ідентифікаторів об'єкта, індексу фрагмента та версії політики. Порушення дисципліни унікальності nonce розглядається як критична експлуатаційна помилка та усувається шляхом ротації ключів або оновлення версії політики.

Захист мережевих блочних сховищ

Мережеві блочні сховища (SAN) надають доступ до даних у вигляді лінійно адресованих секторів фіксованого розміру та не містять вбудованого логічного контексту. Це ускладнює захист від атак перестановки, повтору та відкату секторів, особливо в багатоорендних хмарних середовищах.

У межах методу транспортні протоколи блочного доступу (iSCSI, Fibre Channel, NVMe-oF) розглядаються виключно як механізми доставки операцій читання та запису. Їхні внутрішні засоби захисту не використовуються для забезпечення криптографічної автентичності даних у стані зберігання.

Для SAN у методиці визначено два допустимі криптографічні профілі:

1) Профіль AEAD-на-сектор

Кожен сектор розглядається як окреме повідомлення AEAD, для якого виконується шифрування з прив'язкою до адресації (5):

$$(C_s, \tau_s) = \mathrm{AEAD.Enc}_K(\mathrm{nonce}_s, P_s, \mathrm{AAD}_s), \quad (5)$$

де C_s — шифротекст сектора, τ_s — тег автентичності, nonce_s — унікальне значення ініціалізації, P_s — відкритий текст сектора, AAD_s — контекст автентичності сектора.

AAD формується з урахуванням адресації та версійності даних (6):

$$\mathrm{AAD}_s = \mathrm{DevID} \parallel \mathrm{LBN} \parallel \mathrm{ver}, \quad (6)$$

де DevID — ідентифікатор логічного пристрою або тома, LBN — номер логічного блока, ver — версія криптографічної політики або даних.

Такий підхід забезпечує виявлення будь-яких спроб модифікації, перестановки або повторного використання секторів.

2) Профіль XTS-AES з додатковою автентифікацією

У випадках, коли застосування AEAD-на-сектор є недоцільним (технічно, або з точки зору продуктивності), допускається використання режиму шифрування блочного шифру (AES) (XTS-AES) виключно для забезпечення конфіденційності даних із обов'язковим доповненням механізмом криптографічної автентифікації.

Перевірка цілісності реалізується окремим механізмом автентифікації, обчисленим над шифротекстом і контекстом адресації сектора. Самостійне використання XTS-AES без автентифікації, в межах методу, не допускається.

XTS вводить параметр tweak (похідне значення від номера логічного блока (LBN), номера сектора та позиції в секторі) та шифрує кожен сектор незалежно. Для захисту даних на блочних пристроях використовується два незалежні ключі (AES): перший — для шифрування даних, другий — для обчислення значення tweak. Математично це можна представити у вигляді формули 7:

$$C_i = \mathrm{AES}_{K_1}(P_i \oplus T_i) \oplus T_i, \quad (7)$$

де: C_i — відповідний блок шифротексту, AES_{K_1} — незалежний ключ, P_i — блок відкритого тексту, T_i — tweak (похідний від номера сектора), K_1 — незалежний ключ для шифрування даних.

Така конструкція забезпечує конфіденційність і криптографічну прив’язку до адресації, проте не гарантує цілісності та автентичності даних. Тому в межах методу використання XTS-AES допускається лише за умови додаткового обчислення автентифікаційного коду (код автентифікації повідомлення (MAC) або еквівалентного механізму) над шифротекстом і контекстом адресації сектора. Самостійне застосування XTS-AES без автентифікації не допускається.

Керування ключами та криптографічні профілі

Навіть за використання криптографічно стійких алгоритмів і режимів порушення дисципліни управління ключовим матеріалом призводить до втрати конфіденційності або цілісності даних, а отже — нівелює криптографічні гарантії всієї системи.

Метод розглядає керування ключами як формалізований процес, інтегрований у загальну архітектуру «Повної недовіри» і узгоджений з вимогами стандартів інформаційної безпеки. Криптографічний захист даних не відокремлюється від процедур генерації, зберігання, деривації та ротації ключового матеріалу.

Архітектура керування ключами

У межах методу, ключовий матеріал поділяється на логічні рівні відповідно до їх призначення та експлуатаційних вимог. Кореневі ключі використовуються виключно як базис для деривації та зберігаються в межах довіреного домену керування ключами. Вони ніколи не застосовуються безпосередньо для шифрування даних і не покидають межі сервісів керування ключами або апаратних криптомодулів. Робочі ключі даних застосовуються безпосередньо для операцій шифрування та автентифікації, однак не зберігаються у стійкій пам’яті. Натомість вони детерміновано виводяться з кореневого ключового матеріалу на основі формалізованого контексту. Тимчасові або контекстні ключі можуть використовуватися в межах окремих операцій або обмежених часових інтервалів для зниження ризиків тривалої експлуатації одного ключа.

Для захисту кореневого ключового матеріалу метод передбачає використання сервісів керування ключами (KMS) та/або апаратних модулів безпеки (HSM). Такі компоненти забезпечують контроль доступу до криптографічних операцій, аудит використання ключів, а також підтримку процедур резервування та знищення ключового матеріалу. Вимоги до криптографічних модулів формулюються з

урахуванням гармонізованого національного стандарту ДСТУ ISO/IEC 19790 [20] (або FIPS 140-3 [21]).

Детермінована деривація та ротація ключів

Робочі ключі даних у методиці формуються шляхом детермінованої деривації з використанням стандартизованих криптографічних функцій. Контекст деривації однозначно визначає призначення ключа та включає, зокрема, тип операції, ідентифікатор орендаря або домену безпеки, ідентифікатор ресурсу та версію криптографічної політики [22]. Такий підхід забезпечує криптографічну ізоляцію ключів між різними орендарями, ресурсами та версіями даних без необхідності зберігання великої кількості ключового матеріалу.

Метод передбачає обов'язкову ротацію ключів як засіб зниження ризиків криптографічної компрометації. Ротація може ініціюватись при досягненні встановлених експлуатаційних меж використання ключа, спливу встановленого часовго інтервалу, зміни криптографічної політики або виявлення інциденту безпеки [23]. На практиці ротація реалізується шляхом оновлення контексту деривації або збільшення версії політики, що дозволяє уникнути повторного шифрування всього обсягу даних.

Для режимів автентифікованого шифрування метод вводить поняття експлуатаційних меж використання ключів, які визначають допустимий обсяг даних і кількість криптографічних операцій під одним ключем. Контроль таких меж забезпечує передбачуваність рівня безпеки та уніфікацію політик ротації в довготривалій експлуатації [24], [25].

Криптографічні алгоритми та профілі

Запропонований метод є алгоритмічно нейтральним та визначає не конкретні криптографічні примітиви, а вимоги до їх властивостей і умов застосування. Алгоритми, що використовуються для захисту даних у корпоративних хмарних сховищах, повинні відповідати сучасному рівню криптостійкості, мати формалізований аналіз безпеки та підтримувати реалізацію в сертифікованих криптографічних модулях.

Метод орієнтований на використання симетричних алгоритмів у режимах автентифікованого шифрування або в еквівалентних конструкціях. Для мережевих блочних сховищ допускається застосування спеціалізованих режимів шифрування виключно за умови доповнення механізмами криптографічної автентифікації.

Метод підтримує використання як міжнародно визнаних криптографічних алгоритмів, так і національних стандартів України. Зокрема, у межах національного криптографічного профілю допускається застосування блочного шифру «Калина» відповідно до ДСТУ 7624:2014 [3] та криптографічних геш-функцій і механізмів автентифікації, визначених стандартом ДСТУ 7564:2014 [4]. Використання національних алгоритмів не змінює логіку методу, а лише замінює окремі криптографічні примітиви при збереженні архітектурних принципів захисту.

Алгоритмічна нейтральність методу дозволяє адаптувати його до змін нормативної бази, оновлювати криптографічні примітиви без перегляду архітектури захисту та використовувати різні криптографічні профілі залежно від регуляторних вимог або політики організації.

Структурне узагальнення методу

Узагальнення архітектурних принципів, моделі загроз, криптографічних профілів захисту та механізмів керування ключами, сформульованих у розділі 3, дозволяє подати цілісну структуру запропонованого методу. На рисунку 2 наведено узагальнену модель криптографічного захисту даних у корпоративних хмарних системах, що відображає розмежування рівнів застосування криптографії, межу довіри відповідно до парадигми концепції «Повної недовіри» та використання гомоморфного шифрування.

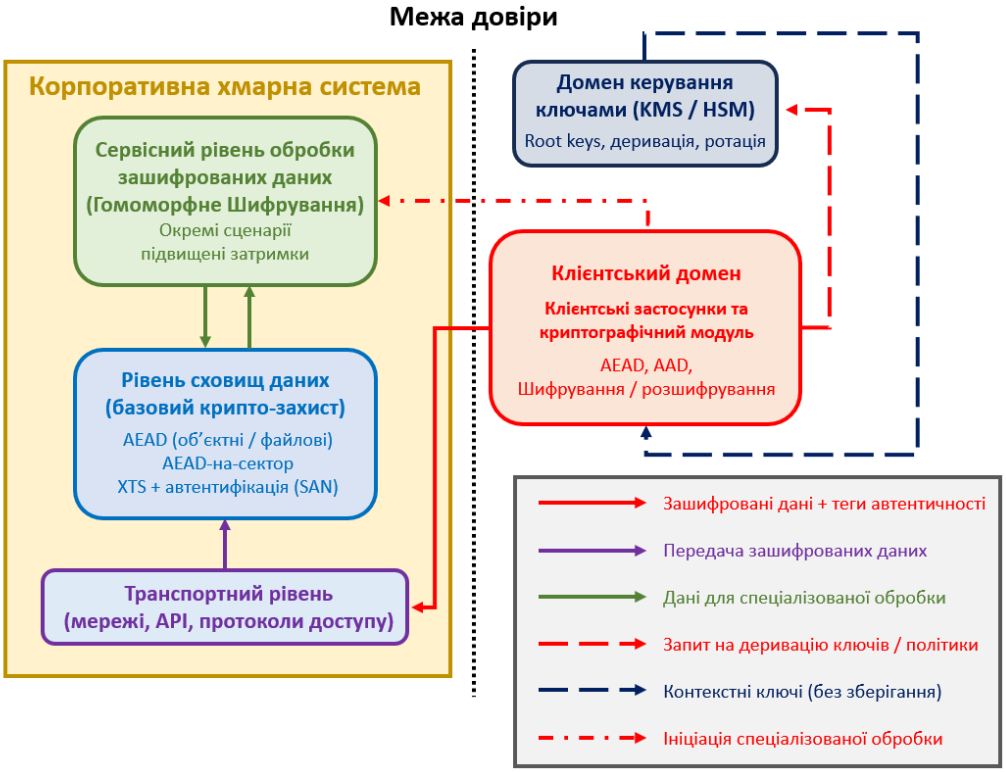

Рис. 2. Структурна модель методу криптографічного захисту даних у корпоративних хмарних системах на засадах Zero Trust

Наведена схема демонструє, що базові криптографічні гарантії конфіденційності та цілісності забезпечуються на рівні сховищ із використанням автентифікованих симетричних механізмів, тоді як домен керування ключами логічно відокремлений від недовіреної інфраструктури провайдера та взаємодіє виключно з клієнтським середовищем. Передавання даних між клієнтом і сховищем здійснюється через транспортний рівень у вже зашифрованому вигляді, що виключає залежність криптографічних гарантій від інфраструктури провайдера.

Гомоморфне шифрування представлено як окремий сервісний рівень, який ініціюється клієнтом для виконання спеціалізованих обчислень над зашифрованими даними, отриманими зі сховища, та повертає результат у зашифрованому вигляді без доступу до ключового матеріалу. Воно не інтегрується в базові операції введення-виведення та не впливає на механізми зберігання.

Таким чином, схема відображає кінцевий результат роботи — архітектурно узгоджений метод криптографічного захисту даних у корпоративних хмарних системах, що забезпечує формалізоване розмежування рівнів довіри, керованість

ключового матеріалу та адаптацію до експлуатаційних обмежень високонавантажених середовищ.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження сформовано архітектурно узгоджений криптографічний метод захисту даних у корпоративних хмарних системах, побудований на засадах концепції «Повної недовіри» та формалізованого криптографічного контексту. Обґрунтовано недоцільність використання лише гомоморфного шифрування як базового механізму захисту сховищ з огляду на часові та експлуатаційні обмеження корпоративних SLA, а також визначено його допустиме місце як окремого сервісного рівня для спеціалізованих сценаріїв обробки зашифрованих даних. Розроблено структурну модель розмежування рівнів застосування криптографії, визначено профілі захисту для об’єктних, файлових і мережевих блочних сховищ та сформульовано вимоги до домену керування ключами, що забезпечують ізоляцію орендарів, контрольований життєвий цикл ключового матеріалу та формалізовану ротацію.

Практичне значення отриманих результатів полягає у можливості застосування запропонованого методу для побудови або модернізації систем криптографічного захисту даних у корпоративних хмарних середовищах з високою інтенсивністю операцій введення-виведення. Метод дозволяє узгодити криптографічні механізми з реальними вимогами до продуктивності, масштабованості та прогнозованості затримок, забезпечуючи при цьому конфіденційність і цілісність даних незалежно від довіри до інфраструктури провайдера. Сформульовані профілі захисту та підходи до детермінованої деривації й ротації ключів можуть бути використані при розробленні внутрішніх політик безпеки організацій, технічних регламентів та архітектурних рішень у сфері корпоративних хмарних сервісів.

Подальші дослідження доцільно зосередити на розширенні моделі загроз із урахуванням апаратних побічних каналів, мікроархітектурних атак і ризиків компрометації клієнтського середовища, а також на інтеграції запропонованого методу з механізмами довіреного виконання та апаратними засобами ізоляції. Перспективним напрямом є також оцінювання впливу постквантових криптографічних примітивів на запропоновані профілі захисту та дослідження можливостей практичного поєднання сервісного гомоморфного шифрування з вимогами до продуктивності корпоративних хмарних систем. Додаткової уваги потребує формалізація процедур аудиту та автоматизованого контролю політик ротації ключів у довготривалій експлуатації.

ПОДЯКА

Автор висловлює щиру подяку Гулаку Геннадію Миколайовичу за консультації з питань криптографії та хмарних середовищ, Складанному Павлу Миколайовичу за цінні поради щодо концепції «Повної недовіри», а також викладачам Кафедри інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка за викладання профільних дисциплін, знання з яких були використані під час дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ержавний стандарт України. (2023). ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги

ержавний стандарт України. (2014). ДСТУ 7624:2014. Інформаційні технології. Криптографічний з

ержавний стандарт України. (2014). ДСТУ 7564:2014. Інформаційні технології. Криптографічний х

улак, Г., Бурячок, В., Складанний, П., & Кузьменко, Л. (2020). Криптовірусологія: загрози безпеці карантоздатних інформаційних систем та заходи протидії вірусам-шифрувальникам. К

ртика, А., & Захарова, Я. (2024). Модель безпеки та контролю доступу до даних у хмарних ервісах на основі механізму identity and access management (IAM). Ukrainian Scientific Journal of

віленкова, А. (2024). Загрози від використання cloud-сервісів у сфері кібербезпеки.

ітов, А., & Кропивницький, Д. (2024). Синтез типових алгоритмів захисту інформації в

ак, Г., Жданова, Ю., Складанний, П., Гулак, Є., & Корнієць, В. (2022). Уразливості шифрування коротких повідомлень у мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Кібербезпека: освіта, наука, техніка, 1(17), 145–158.

ержавний стандарт України. (2017). ДСТУ ISO/IEC 27017:2017. Інформаційні технології. Методи ахисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002,

rds and Technology. (2020). Recommendation for key management: Part 1 – General (NIST Special

as, V., Manzano, M., Bassoli, R., Fitzek, F. H. P., & Aaraj, N. (2022). Survey on fully homomorphic ncryption, theory, and applications. Proceedings of the IEEE, 111(3), 317–345.

ng, Y., Chang, X., Mišić, J., & Mišić, V. B. (2024). Practical solutions in fully homomorphic

illotti, I., Gama, N., Georgieva, M., & Izabachène, M. (2020). TFHE: Fast fully homomorphic

levi, S., & Shoup, V. (2014). Algorithms in HElib. In J. A. Garay & R. Gennaro (Eds.), Advances in

жавний стандарт України. (2022). ДСТУ EN ISO/IEC 19790:2022. Інформаційні технології. Методи захисту. Вимоги безпеки до криптографічних модулів (EN ISO/IEC 19790:2020, IDT;

22. Chen, L. (2022). Recommendation for key derivation using pseudorandom functions (NIST SP 800-108 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-108r1
ker, E., Smid, M., Branstad, D., & Chokhani, S. (2019). Recommendation for Key Management: Part – Best Practices for Key Management Organizations (NIST SP 800-57 Part 2 Rev. 1). National nstitute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt2r1
24. Gueron, S., Langley, A., & Lindell, Y. (2019). AES-GCM-SIV: Nonce misuse-resistant authenticated ncryption (RFC 8452). RFC Editor. https://doi.org/10.17487/RFC8452
25. Cloud Security Alliance. (2023). Key Management Lifecycle Best Practices. Cloud Security Alliance. https://cloudsecurityalliance.org/artifacts/key-management-lifecycle-best-practices

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

Oleksandr Trofimov
Postgraduate student
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0009-0008-5760-7803
o.trofimov.asp@kubg.edu.ua

METHOD FOR COMBINED DATA ENCRYPTION IN CLOUD ENVIRONMENTS

Abstract. The article is devoted to the development of a cryptographic data protection method for corporate cloud environments based on the Zero Trust concept, taking into account the requirements for performance, scalability, and predictable latency. The introduction substantiates the relevance of the topic in the context of the transition of corporate systems to cloud services, the growth of cyber threats, and the need to combine cryptographic strength with practical operational constraints. The section reviewing recent studies examines the regulatory and scientific foundation of the research, covering both international and national information security standards, Zero Trust approaches, access control models, and encryption methods. On this basis, the paper formulates the problem of the absence of an integrated method that would simultaneously consider the threat model, separation of trust levels, key management, and time constraints typical of high-load systems. The research part shows that homomorphic encryption, despite its advantages for processing encrypted data, cannot be used as the basic storage protection mechanism because of substantial computational overhead. Its use is justified only as a separate service layer for specialized scenarios. The main attention is focused on the architectural principles of the method: distrust of the provider infrastructure, client-side execution of critical cryptographic operations, and a formalized cryptographic context. The paper defines protection profiles for object, file, and network block storage. For object and file access, authenticated symmetric encryption with additional authenticated data is proposed. For network block storage, the method specifies sector-level authenticated encryption and XTS-AES only in combination with separate cryptographic authentication. A structured approach to deterministic key derivation, key rotation, and key isolation within a trusted key management domain is also formulated. The conclusions summarize that the proposed method can be used for the design or modernization of corporate information protection systems.

Keywords: cryptographic data protection; corporate cloud environments; Zero Trust; cryptographic key management; homomorphic encryption.

REFERENCES

1. State Standard of Ukraine. (2023). DSTU ISO/IEC 27001:2023. Information security, cybersecurity and privacy protection. Information security management systems. Requirements (ISO/IEC 27001:2022, IDT). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398
2. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
3. State Standard of Ukraine. (2014). DSTU 7624:2014. Information technology. Cryptographic data protection. Symmetric block transformation algorithm “Kalyna”. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=65314
4. State Standard of Ukraine. (2014). DSTU 7564:2014. Information technology. Cryptographic data protection. Hash function “Kupyna”. https://usts.kiev.ua/wp-content/uploads/2020/07/dstu-7564-2014.pdf
5. Hulak, H., Buriachok, V., Skladannyi, P., & Kuzmenko, L. (2020). Cryptovirology: Security threats to guaranteed information systems and measures to combat encryption viruses. Cybersecurity: Education, Science, Technique, 2(10), 6–28. https://doi.org/10.28925/2663-4023.2020.10.628
6. Partyka, A., & Zakharova, Y. (2024). Security model and data access control in cloud services based on the Identity and Access Management (IAM) mechanism. Ukrainian Scientific Journal of Information Security, 30(1), 12–20. https://doi.org/10.18372/2225-5036.30.18575
7. Vavilenkova, A. (2024). Threats from the use of cloud services in cybersecurity. Cybersecurity: Education, Science, Technique, 2(26), 409–416. https://doi.org/10.28925/2663-4023.2024.26.704

8. Shkitov, A., & Kropyvnytskyi, D. (2024). Synthesis of typical information protection algorithms in corporate networks. Management of Development of Complex Systems, (60), 129–135. https://doi.org/10.32347/2412-9933.2024.60.129-135
9. Hulak, H., Zhdanova, Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Vulnerabilities of short message encryption in mobile information and communication systems of critical infrastructure objects. Cybersecurity: Education, Science, Technique, 1(17), 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
10. State Standard of Ukraine. (2017). DSTU ISO/IEC 27017:2017. Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO/IEC 27017:2015, IDT). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=75487
11. National Institute of Standards and Technology. (2020). Recommendation for Key Management: Part 1 – General (NIST Special Publication 800-57 Part 1 Rev. 5). https://doi.org/10.6028/NIST.SP.800-57pt1r5
12. Marcolla, C., Sucasas, V., Manzano, M., Bassoli, R., Fitzek, F. H. P., & Aaraj, N. (2022). Survey on Fully Homomorphic Encryption, Theory, and Applications. Proceedings of the IEEE, 1–38. https://doi.org/10.1109/JPROC.2022.3205665
13. Gong, Y., Chang, X., Mišić, J., Mišić, V. B., & Chang, X. (2024). Practical solutions in fully homomorphic encryption: A survey analyzing existing acceleration methods. Cybersecurity, 7, Article 5. https://doi.org/10.1186/s42400-023-00187-4
14. Junior, M. A., de Oliveira, R. A. R., da Silva, A. A., & de Souza, J. N. (2025). Cloud data privacy protection with homomorphic algorithm: A systematic literature review. Journal of Cloud Computing. https://doi.org/10.1186/s13677-025-00774-5
15. Chillotti, I., Gama, N., Georgieva, M., et al. (2020). TFHE: Fast Fully Homomorphic Encryption over the Torus. Journal of Cryptology, 33, 34–91. https://doi.org/10.1007/s00145-019-09319-x
16. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys, 51(4), 79:1–79:35. https://dl.acm.org/doi/10.1145/3214303
17. Halevi, S., & Shoup, V. (2014). Algorithms in HElib. In J. A. Garay & R. Gennaro (Eds.), Advances in Cryptology – CRYPTO 2014 (Vol. 8616). Springer. https://doi.org/10.1007/978-3-662-44371-2_31
18. McGrew, D., & Viega, J. (2005). The Galois/Counter Mode of Operation (GCM). Submission to NIST Modes of Operation Process. National Institute of Standards and Technology. https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-revised-spec.pdf
19. Gueron, S., Langley, A., & Lindell, Y. (2019). AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption. RFC 8452. https://doi.org/10.17487/RFC8452
20. State Standard of Ukraine. (2022). DSTU EN ISO/IEC 19790:2022. Information technology. Security techniques. Security requirements for cryptographic modules (EN ISO/IEC 19790:2020, IDT; ISO/IEC 19790:2012, including corrected version 2015-12, IDT). https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=100251
21. National Institute of Standards and Technology. (2019). FIPS 140-3:2019. Security Requirements for Cryptographic Modules. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
22. Chen, L. (2022). Recommendation for key derivation using pseudorandom functions (NIST SP 800-108 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-108r1
23. Barker, E., Smid, M., Branstad, D., & Chokhani, S. (2019). Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations (NIST SP 800-57 Part 2 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt2r1
24. Gueron, S., Langley, A., & Lindell, Y. (2019). AES-GCM-SIV: Nonce misuse-resistant authenticated encryption (RFC 8452). RFC Editor. https://doi.org/10.17487/RFC8452
25. Cloud Security Alliance. (2023, December 19). Key Management Lifecycle Best Practices. Cloud Security Alliance. https://cloudsecurityalliance.org/artifacts/key-management-lifecycle-best-practices

(cc) BY-NC-SA
This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.