

Гулак Геннадій Миколайович

доктор технічних наук, професор

професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID ID: 0000-0001-9131-9233

h.hulak@kubg.edu.ua

Трофімов Олександр Сергійович

аспірант

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID ID: 0009-0008-5760-7803

o.trofimov.asp@kubg.edu.ua

МЕТОД КОМБІНОВАНОГО КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ У КОРПОРАТИВНИХ ХМАРНИХ ОБЧИСЛЕННЯХ

Анотація. Статтю присвячено розробленню методу комбінованого криптографічного захисту даних у корпоративних хмарних обчисленнях, спрямованого на підвищення конфіденційності, цілісності, автентичності та доступності інформаційних ресурсів в умовах динамічної зміни середовища функціонування. Проведено аналіз сучасних методів криптографічного захисту корпоративних хмарних обчислень, визначено їх переваги, недоліки та особливості практичного застосування. Встановлено, що використання окремих механізмів шифрування, керування криптографічними ключами і контролю доступу не забезпечує необхідної узгодженості між рівнем захищеності, продуктивністю та адаптивністю системи. Розглянуто особливості функціонування корпоративних хмарних середовищ, багатокористувацької архітектури, розподіленого зберігання даних, контекстного контролю доступу та концепції повної недовіри, що визначають вимоги до побудови сучасних засобів криптографічного захисту. Запропоновано метод комбінованого криптографічного захисту даних, який поєднує симетричне й асиметричне шифрування, адаптивне керування криптографічними ключами, контекстно орієнтований вибір режимів шифрування та оцінювання ризику компрометації. Описано структуру методу, послідовність виконання його етапів і механізм вибору криптографічних параметрів відповідно до характеристик інформаційних ресурсів, рівня довіри до користувача та поточного стану хмарного середовища. Проведено структурно-функціональне та сценарне оцінювання запропонованого методу порівняно зі статичним і традиційним гібридним підходами. За результатами структурно-функціонального та сценарного оцінювання встановлено, що запропонований метод, на відміну від розглянутих аналогів, забезпечує контекстний вибір криптографічного профілю, дострокову ротацію ключів, контроль актуальності криптографічного контейнера та адаптивне реагування на зміну рівня кіберризiku. Практичне значення полягає у можливості використання методу під час побудови захищених корпоративних хмарних сервісів.

Ключові слова: корпоративні хмарні обчислення, криптографічний захист, комбінований метод, симетричне шифрування, асиметричне шифрування, криптографічні ключі, контекстно-орієнтований захист, оцінювання ризику, конфіденційність, цілісність даних.

Hennadii Hulak

doctor of technical sciences, professor

professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok

Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

ORCID ID: 0000-0001-9131-9233

h.hulak@kubg.edu.ua

Oleksandr Trofimov

Postgraduate student

Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

ORCID: 0009-0008-5760-7803

o.trofimov.asp@kubg.edu.ua

METHOD OF COMBINED CRYPTOGRAPHIC DATA PROTECTION IN CORPORATE CLOUD COMPUTING

Abstract. This paper presents a method of combined cryptographic data protection for corporate cloud computing aimed at improving the confidentiality, integrity, authenticity, and availability of information resources under dynamically changing operating conditions. A comprehensive analysis of contemporary cryptographic protection methods for corporate cloud environments was conducted, identifying their advantages, limitations, and practical application characteristics. The analysis demonstrated that the independent application of encryption, cryptographic key management, and access control mechanisms does not provide an appropriate balance between security, system performance, and adaptability. The specific characteristics of corporate cloud

© 2026 Гулак Г.М., Трофімов О.С. Цей матеріал ліцензовано за умовами CC BY 4.0.

<https://creativecommons.org/licenses/by/4.0/>

environments, including multi-tenant architectures, distributed data storage, context-aware access control, and the Zero Trust concept, were examined to determine the requirements for modern cryptographic protection mechanisms. A combined cryptographic data protection method is proposed that integrates symmetric and asymmetric encryption, adaptive cryptographic key management, context-aware selection of encryption modes, and compromise risk assessment. The structure of the proposed method, the sequence of its operational stages, and the mechanism for selecting cryptographic parameters according to information resource characteristics, user trust level, and the current state of the cloud environment are described. A structural-functional and scenario-based evaluation of the proposed method was performed in comparison with static and conventional hybrid approaches. The evaluation results demonstrate that, unlike existing approaches, the proposed method provides context-aware cryptographic profile selection, proactive key rotation, cryptographic container validity verification, and adaptive response to changes in cyber risk. The practical significance of the proposed method lies in its applicability to the design and deployment of secure corporate cloud services.

Keywords: corporate cloud computing; cryptographic protection; combined cryptographic method; symmetric encryption; asymmetric encryption; cryptographic keys; context-aware security; risk assessment; confidentiality; data integrity.

1. Вступ

Сучасні корпоративні хмарні обчислення є основою функціонування інформаційних систем підприємств, однак зростання кількості кіберзагроз, розподілений характер оброблення даних і багатокористувацька архітектура висувають підвищені вимоги до забезпечення конфіденційності, цілісності, автентичності та доступності інформаційних ресурсів [1, 7-8, 14]. Існуючі криптографічні рішення переважно реалізують шифрування, керування ключами та контроль доступу як окремі процеси, що ускладнює адаптацію системи захисту до зміни контексту функціонування та збільшує обчислювальні витрати [2, 6, 12-13]. Це зумовлює актуальність розроблення комбінованих методів криптографічного захисту, здатних інтегрувати декілька механізмів безпеки в єдину адаптивну систему.

Наукова новизна роботи полягає у розробленні методу комбінованого криптографічного захисту даних у корпоративних хмарних обчисленнях, який поєднує симетричне й асиметричне шифрування, адаптивне керування криптографічними ключами та контекстно-орієнтований вибір параметрів криптографічного захисту залежно від рівня ризику й характеристик інформаційних ресурсів.

Теоретичне значення полягає у розвитку методичних засад побудови комбінованих криптографічних механізмів захисту корпоративних хмарних середовищ на основі інтеграції криптографічних алгоритмів, керування ключами та контекстного аналізу.

Практичне значення полягає у можливості використання запропонованого методу під час проектування та модернізації корпоративних хмарних систем для підвищення ефективності захисту даних, створення передумов для зменшення криптографічних накладних витрат і забезпечення адаптивного реагування на зміну умов функціонування та рівня кіберзагроз.

2. Постановка проблеми

Стрімкий розвиток корпоративних хмарних обчислень зумовив широке використання розподілених середовищ для зберігання, оброблення та передавання критично важливих даних [5, 8, 11]. Водночас централізація інформаційних ресурсів, багатокористувацька архітектура, віддалений доступ і постійне зростання кількості кіберзагроз підвищують ризик несанкціонованого доступу, компрометації криптографічних ключів, порушення конфіденційності та цілісності інформації [6-7, 16, 18]. Існуючі підходи до криптографічного захисту здебільшого реалізують шифрування, керування ключами, автентифікацію та контроль доступу як окремі незалежні механізми, що ускладнює їх узгоджене функціонування, збільшує обчислювальні витрати та знижує ефективність захисту в умовах динамічної зміни контексту функціонування корпоративного хмарного середовища [20].

У зв'язку з цим актуальним науково-практичним завданням є розроблення методу комбінованого криптографічного захисту даних, який забезпечуватиме інтеграцію сучасних криптографічних механізмів, адаптивне керування параметрами захисту відповідно до поточного рівня ризику та ефективне використання обчислювальних ресурсів корпоративної хмарної інфраструктури [19, 21, 23]. Розв'язання цієї проблеми сприятиме підвищенню рівня захищеності корпоративних даних, стійкості хмарних сервісів до сучасних кіберзагроз і ефективності функціонування корпоративних інформаційних систем.

3. Аналіз останніх досліджень і публікацій

Проблема криптографічного захисту даних у корпоративних хмарних середовищах досліджується за напрямками забезпечення конфіденційності й цілісності інформації, захисту криптографічних ключів, розмежування доступу, упровадження архітектури повної недовіри та підготовки криптографічних систем до квантових загроз.

Mishra K. N. та Mishra A. запропонували багаторівневу схему кодування даних у хмарних сховищах, доповнену одноразовою авторизацією користувача [1]. Поєднання декількох процедур перетворення ускладнює відновлення початкових даних неавторизованою стороною та підвищує рівень їх конфіденційності. Водночас запропонований підхід орієнтований переважно на захист даних під час зберігання та не передбачає адаптивного вибору криптографічних механізмів залежно від критичності ресурсу, рівня ризику й поточного стану корпоративної хмарної інфраструктури.

Kim C. та Kim S. розробили масштабовану схему шифрування файлів для хмарних систем, яка інтегрує класичну і постквантову криптографію, квантовий розподіл ключів та симетричне шифрування [2]. Така інтеграція спрямована на забезпечення стійкості хмарних систем до перспективних квантових атак. Однак реалізація рішення потребує складної розподіленої інфраструктури, а питання адаптивного вибору режимів захисту відповідно до продуктивності, вартості обчислень і поточного кіберризiku залишається недостатньо формалізованим.

Dakić V. та Regvart D. дослідили особливості впровадження архітектури повної недовіри у хмарному середовищі Microsoft Azure для організацій середнього розміру [3]. Автори обґрунтували необхідність постійної перевірки користувачів, пристроїв, запитів і контексту доступу, а також визначили організаційні й технічні умови переходу до відповідної архітектури. Проте дослідження зосереджене переважно на контролі доступу та конфігурації хмарної інфраструктури й не містить формалізованого механізму узгодженого вибору алгоритмів шифрування, параметрів криптографічної стійкості та політик керування ключами.

Nie S. та Wan W. запропонували механізм контролю доступу, що поєднує концепцію повної недовіри, блокчейн і шифрування внутрішнього добутку [4]. Рішення забезпечує перевірюваність операцій, децентралізоване зберігання відомостей про доступ і деталізоване розмежування повноважень. Водночас метод орієнтований переважно на Інтернет речей у мережах шостого покоління та не враховує специфіки корпоративних хмарних систем, зокрема вимог до продуктивності, рівня обслуговування і диференційованого захисту різних категорій даних.

Velmurugan S. та співавтори розробили схему вибіркового поширення даних у хмарному середовищі на основі атрибутного шифрування, повторного шифрування через посередника та децентралізованого керування довірою [5]. Запропонований підхід забезпечує вибіркоче надання доступу, перевірюваність операцій і зменшення витрат, пов'язаних із керуванням ключами. Однак у ньому не передбачено узгодженого застосування симетричного й асиметричного шифрування залежно від обсягу, критичності, місця зберігання та режиму використання корпоративних даних.

Huang J. та Yi J. запропонували схему захищеного керування ключами хмарного сховища на основі блокчейну, цифрових двійників, розподілу секрету та рандомізованих конвергентних ключів [6]. Застосування блокчейну забезпечує незмінність і простежуваність операцій, а розподіл ключа на фрагменти підвищує надійність його зберігання та відновлення. Разом із тим рішення орієнтоване передусім на керування ключами та захищене усунення дублювання даних і не охоплює комплексного вибору криптографічних режимів під час зберігання, передавання й оброблення інформації.

Goswami P. та співавтори систематизували стратегії забезпечення цілісності даних на рівні хмарного сховища, класифікували загрози, моделі аудиту, механізми перевірки та пов'язані з ними накладні витрати [7]. Автори показали необхідність одночасного врахування безпеки, продуктивності та вартості перевірки цілісності. Проте в роботі не запропоновано єдиного методу, який інтегрував би контроль цілісності, шифрування, автентифікацію, керування ключами та контекстне оцінювання ризику.

Pathak M., Mishra K. N. та Singh S. P. здійснили комплексний аналіз загроз безпеці та конфіденційності даних у системах хмарного Інтернету речей [8]. Авторами розглянуто блокчейн, машинне навчання, периферійні й туманні обчислення та криптографічні механізми як засоби протидії атакам. У роботі наголошено на необхідності вдосконалення протоколів наскрізного захисту даних, однак не визначено механізму спільного вибору алгоритмів шифрування, способів розподілу ключів і параметрів захисту відповідно до поточного стану корпоративного хмарного середовища.

Ajala O. A. та Daraojimba A. I. розглянули вплив квантових обчислень на сучасні методи криптографічного захисту [9]. Автори проаналізували загрози для поширених асиметричних алгоритмів, можливості постквантової криптографії та квантового розподілу ключів, а також перспективи поєднання класичних і квантово стійких механізмів. Водночас дослідження має оглядовий характер і не пропонує прикладного методу інтеграції таких механізмів у корпоративну хмарну інфраструктуру з урахуванням її продуктивності та поточного рівня ризику.

Отже, проаналізовані дослідження охоплюють багаторівневе кодування даних [1], поєднання симетричного й асиметричного шифрування [2, 10], постквантові криптографічні механізми та квантовий розподіл ключів [15, 26], атрибутно-орієнтоване шифрування [4], блокчейн-орієнтовані механізми захисту [13, 26], архітектуру повної недовіри [3, 19, 21], контроль цілісності хмарних даних [7], а також розподілене керування криптографічними ключами й довірою [5, 6, 20]. Окремі праці також розглядають гомоморфне шифрування для забезпечення конфіденційності даних під час їх оброблення у хмарі [11], рольове керування доступом до багаторівневих сховищ [18] та адаптивне керування інформаційною безпекою у хмарно-орієнтованих системах [23]. Проте зазначені засоби переважно застосовуються окремо або орієнтуються на вузькі сценарії захисту, що не забезпечує комплексного узгодження криптографічних механізмів, політик доступу, керування ключами та ресурсних обмежень корпоративного хмарного середовища [8, 12–14].

Раніше не вирішеною частиною загальної проблеми є відсутність цілісного методу комбінованого криптографічного захисту даних у корпоративних хмарних обчисленнях, який узгоджено поєднує симетричне й асиметричне шифрування, захист цілісності, керування криптографічними ключами та контекстно-орієнтований вибір параметрів захисту з урахуванням критичності даних, рівня довіри, поточного кіберризiku, продуктивності та обчислювальних обмежень хмарної інфраструктури.

4. Мета і задачі дослідження

Метою дослідження є розроблення методу комбінованого криптографічного захисту даних у корпоративних хмарних обчисленнях, який забезпечує інтеграцію симетричного й асиметричного шифрування, адаптивне керування криптографічними ключами та контекстно-орієнтований вибір параметрів захисту для підвищення конфіденційності, цілісності, автентичності й ефективності використання обчислювальних ресурсів корпоративного хмарного середовища.

Для досягнення поставленої мети необхідно вирішити такі **задачі**:

- проаналізувати сучасні методи криптографічного захисту даних у корпоративних хмарних обчисленнях та визначити їх переваги й обмеження;
- дослідити особливості функціонування корпоративних хмарних середовищ, що впливають на вибір механізмів криптографічного захисту;
- розробити метод комбінованого криптографічного захисту даних на основі інтеграції симетричного й асиметричного шифрування, адаптивного керування криптографічними ключами та контекстно-орієнтованого вибору параметрів захисту;
- описати структуру та основні етапи функціонування запропонованого методу;
- здійснити структурно-функціональне та сценарне оцінювання запропонованого методу порівняно зі статичним і традиційним гібридним підходами до криптографічного захисту корпоративних хмарних обчислень.

5. Результати дослідження

Запропонований метод призначений для узгодженого застосування симетричних та асиметричних криптографічних механізмів у корпоративному хмарному середовищі. Метод охоплює класифікацію інформаційного ресурсу, оцінювання контексту та ризику, формування криптографічного профілю, генерування і захист сеансового ключа, автентифіковане шифрування даних, перевірку їх цілісності та адаптивне оновлення параметрів захисту. Поєднання симетричних і асиметричних механізмів дає змогу використовувати переваги швидкого шифрування значних обсягів даних та захищеного керування криптографічними ключами. Вибір параметрів захисту здійснюється з урахуванням критичності інформаційного ресурсу, умов його використання та поточного рівня кіберризiku. Сформований криптографічний профіль визначає необхідні параметри шифрування, правила використання сеансового ключа та умови його оновлення. У разі зміни контексту функціонування або підвищення рівня ризику передбачається повторне оцінювання параметрів захисту та, за необхідності, їх адаптивна зміна. Такий підхід забезпечує цілісне функціонування криптографічних механізмів і створює можливість адаптації рівня захисту до поточного стану корпоративного хмарного середовища.

5.1. Структура методу комбінованого криптографічного захисту

Запропонований метод реалізує криптографічний захист на двох взаємопов'язаних рівнях. На рівні даних застосовується швидке симетричне автентифіковане шифрування, а на рівні керування ключами — асиметричний механізм захисту та передавання сеансового ключа [11]. Такий поділ забезпечує високу швидкодію під час оброблення значних обсягів корпоративних даних і водночас унеможливорює передавання сеансового ключа у відкритому вигляді [15].

Передбачається, що порушник може перехоплювати, повторно передавати, модифікувати або підміняти дані, намагатися отримати несанкціонований доступ до хмарного сховища та використовувати скомпрометовані облікові дані [4, 17, 19, 21]. Довіреними вважаються криптографічний модуль і захищене сховище кореневих ключів. Атаки через повну компрометацію довіреного криптографічного модуля виходять за межі цього дослідження.

Метод включає такі етапи: ідентифікацію та класифікацію інформаційного ресурсу; збирання контекстних параметрів; оцінювання необхідного рівня захисту; вибір криптографічного профілю; генерування сеансового симетричного ключа; автентифіковане шифрування даних; асиметричний захист сеансового ключа; передавання або зберігання криптографічного контейнера; перевірку автентичності й цілісності; оновлення профілю за зміни контексту або рівня ризику.

На першому етапі інформаційний ресурс класифікується за рівнем критичності, вимогами до конфіденційності, цілісності та доступності [7-9, 14]. Далі формується множина контекстних параметрів, що характеризують поточний стан корпоративного хмарного середовища [17, 21, 23]. На основі отриманих характеристик визначається необхідний рівень криптографічного захисту, після чого автоматично формується відповідний криптографічний профіль, генерується сеансовий ключ, виконується шифрування даних та перевірка їх автентичності і цілісності [20, 25].

Структурно-функціональну схему запропонованого методу комбінованого криптографічного захисту даних у корпоративних хмарних обчисленнях наведено на рис. 1.

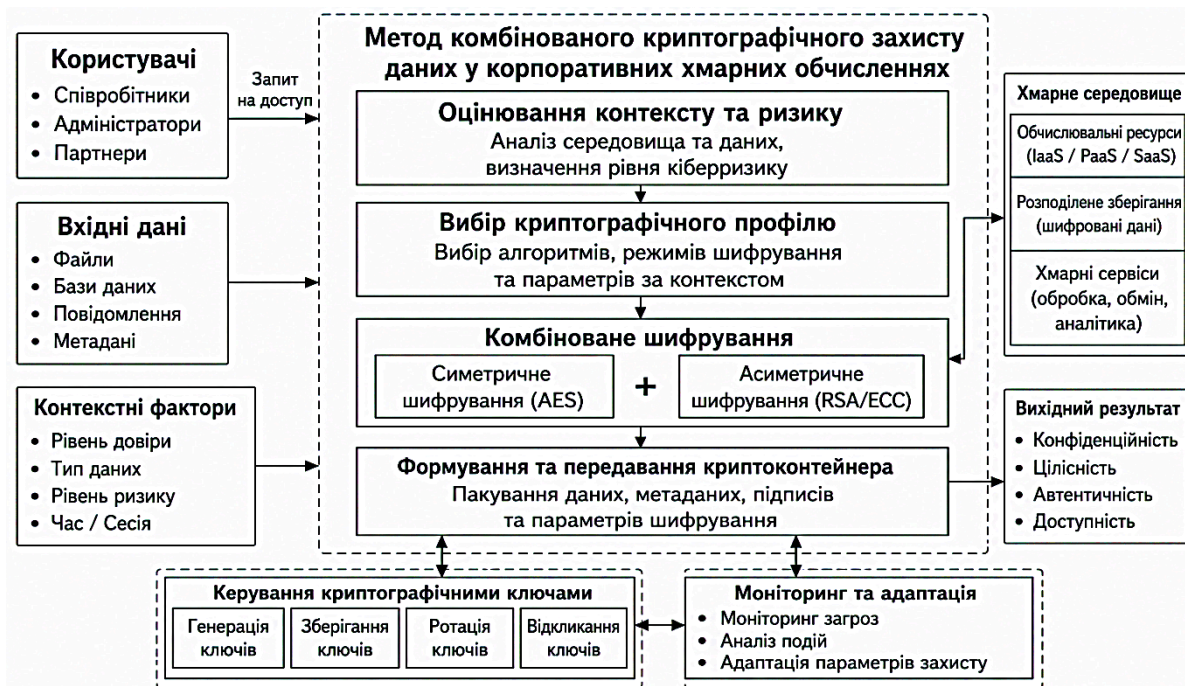


Рис. 1. Структурно-функціональна схема методу комбінованого криптографічного захисту даних у корпоративних хмарних обчисленнях

Як видно з рис. 1, метод реалізує послідовний перехід від аналізу контексту та вибору криптографічного профілю до комбінованого шифрування, формування криптографічного контейнера, керування життєвим циклом ключів і адаптивного моніторингу. Така структура забезпечує узгоджене досягнення конфіденційності, цілісності, автентичності та доступності даних у корпоративному хмарному середовищі.

5.2. Формування контексту та необхідного рівня захисту

Запропонований метод ґрунтується на інтеграції симетричного та асиметричного шифрування, адаптивному керуванні криптографічними ключами та контекстному виборі параметрів захисту [22]. На відміну від традиційних підходів, параметри криптографічного захисту визначаються не лише політикою безпеки, а й поточним станом корпоративного хмарного середовища [17, 19].

Нехай стан інформаційного ресурсу визначається вектором:

$$X_r(t) = \langle c_r, i_r, a_r, v_r, \tau_u(t), \rho(t), l(t) \rangle, \quad (1)$$

де c_r, i_r, a_r – нормовані вимоги до конфіденційності, цілісності та доступності ресурсу r , v_r – номер актуальної версії криптографічного контейнера, $\tau_u(t)$ – рівень довіри до користувача, $\rho(t)$ – поточний кіберризик, $l(t)$ – рівень навантаження на хмарну інфраструктуру. Усі параметри нормуються на інтервалі $[0;1]$.

Необхідний рівень криптографічного захисту інформаційного ресурсу визначається як:

$$q_r(t) = \alpha_1 c_r + \alpha_2 i_r + \alpha_3 v_r + \alpha_4 \rho(t) + \alpha_5 (1 - \tau_u(t)), \quad \sum_{j=1}^5 \alpha_j = 1, \quad (2)$$

де $q_r(t) \in [0;1]$ – необхідний рівень криптографічного захисту ресурсу. Чим вищі критичність і ризик та чим нижча довіра до користувача, тим сильніший профіль має бути застосований. Отримане значення $q_r(t)$ використовується для автоматичного вибору криптографічного профілю. Зі збільшенням критичності інформаційного ресурсу, рівня кіберризiku або зниженням довіри до користувача система переходить до профілів із вищою криптографічною стійкістю, коротшим строком використання ключів та більш жорсткими процедурами автентифікації.

Параметри доступності a_r та навантаження $l(t)$ не включаються безпосередньо до показника необхідного рівня криптографічного захисту, оскільки характеризують не вимоги до криптографічної стійкості, а експлуатаційні обмеження вибору профілю. Вони враховуються під час формування множини допустимих профілів $A(t)$ через обмеження на час оброблення, пропускну здатність і допустимі ресурсні витрати.

5.3. Адаптивний вибір криптографічного профілю

Для кожного допустимого криптографічного профілю оцінюються рівень криптографічної стійкості, відповідність поточним вимогам захисту, час оброблення та ресурсні витрати. Функція доцільності застосування i -го профілю визначається як:

$$F_i(t) = w_1 s_i + w_2 m_i(t) + w_3 p_i - w_4 \hat{T}_i - w_5 \hat{C}_i, \quad \sum_{j=1}^5 w_j = 1, \quad (3)$$

де s_i – нормований рівень криптографічної стійкості i -го профілю, $m_i(t)$ – ступінь відповідності профілю необхідному рівню захисту $q_r(t)$, p_i – повнота забезпечення конфіденційності, цілісності й автентичності, $\hat{T}_i$ – нормований час криптографічного оброблення, $\hat{C}_i$ – нормовані обчислювальні витрати, w_j – вагові коефіцієнти.

Значення $m_i(t)$ визначається шляхом зіставлення рівня криптографічної стійкості профілю s_i з необхідним рівнем захисту $q_r(t)$. Значення показника наближається до одиниці, якщо профіль забезпечує необхідний рівень захисту без невиправданого збільшення часу та ресурсних витрат. Профілі, рівень стійкості яких є нижчим за $q_r(t)$, не включаються до множини допустимих профілів $A(t)$.

Оптимальний криптографічний профіль визначається як:

$$\Omega^*(t) = \arg \arg F_i, \quad (4)$$

де $A(t)$ – множина профілів, які підтримуються корпоративною хмарною інфраструктурою, відповідають установленим вимогам криптографічної стійкості та не перевищують допустимого часу оброблення.

Обраний криптографічний профіль подається як:

$$\Omega_i = \langle E_i^s, E_i^a, k_i, H_i, \theta_i, \pi_i \rangle, \quad (5)$$

де E_i^s – симетричний алгоритм автентифікованого шифрування, E_i^a – асиметричний механізм захисту сеансового ключа, k_i – довжина ключа, H_i – додатковий механізм хешування, цифрового підпису або контролю цілісності службових метаданих, який застосовується за вимогами обраного профілю, θ_i – допустимий строк використання сеансового ключа, π_i – політика ротації, відкликання, відновлення та знищення ключів.

Залежно від значення $q_r(t)$ можуть застосовуватися базовий, підвищений або критичний профілі. Базовий профіль призначений для некритичних внутрішніх даних за низького ризику; підвищений – для конфіденційних корпоративних ресурсів; критичний – для особливо важливих даних, високого ризику або зниженого рівня довіри до користувача. Профілі відрізняються строком дії ключів, частотою їх ротації, параметрами асиметричного захисту та кількістю додаткових перевірок.

Для однозначного вибору профілю задаються два порогові значення q_1 і q_2 , де $0 < q_1 < q_2 < 1$. Базовий профіль застосовується за $q_r(t) < q_1$, підвищений — за $q_1 \leq q_r(t) < q_2$, а критичний — за $q_r(t) \geq q_2$. Значення порогів установлюються політикою безпеки корпоративної хмарної системи з урахуванням категорій оброблюваної інформації та прийнятного рівня ризику.

5.4. Формування та захист сеансового ключа

Для забезпечення високої швидкодії в кожній криптографічній сесії формується окремий симетричний ключ, що обмежує наслідки його можливої компрометації та унеможливорює повторне використання в різних контекстах. Оскільки передавання сеансового ключа відкритими каналами не допускається, він захищається асиметричним криптографічним механізмом.

Сеансовий ключ визначається як:

$$K_s = KDF(K_0, ID_r || ID_u || t || n), \quad (6)$$

де K_s – сеансовий симетричний ключ, K_0 – початковий секретний матеріал, ID_r – ідентифікатор інформаційного ресурсу, ID_u – ідентифікатор користувача або сервісу, t – мітка часу, n – криптографічно стійке випадкове одноразове значення, KDF – функція формування ключа, символ $\parallel$ означає конкатенацію. Значення n має бути унікальним для кожної криптографічної сесії, а початковий секретний матеріал K_0 зберігається виключно в захищеному модулі керування ключами корпоративної хмарної інфраструктури.

Після формування ключа виконується симетричне автентифіковане шифрування:

$$(C_r, T_r) = AEAD.Enc_{K_s}(N_r, D_r, AAD_r), \quad (7)$$

де D_r – відкриті дані інформаційного ресурсу, C_r – шифротекст, T_r – тег автентичності, N_r – унікальне одноразове значення операції шифрування, AAD_r – додаткові автентифіковані дані, що містять ідентифікатор ресурсу, категорію критичності, мітку часу та ідентифікатор криптографічного профілю. Тег T_r використовується для виявлення модифікації шифротексту та службових атрибутів. Зміна будь-якого захищеного елемента спричиняє відхилення ресурсу під час розшифрування.

Після цього сеансовий ключ захищається асиметричним механізмом:

$$W_r = Enc_{PK_d}^a(K_s \parallel ID_r \parallel t), \quad (8)$$

де W_r – асиметрично захищена оболонка сеансового ключа, PK_d – відкритий ключ дозволеного одержувача або хмарного сервісу, $Enc_{PK_d}^a$ – асиметричне шифрування відкритим ключем одержувача. ID_r і t забезпечують криптографічне зв'язування ключа з конкретним ресурсом і часовим контекстом. Використання асиметричного механізму лише для захисту короткого сеансового ключа, а симетричного — для шифрування основного масиву даних дає змогу поєднати високу продуктивність симетричної криптографії із захищеним розподілом ключів.

У межах запропонованого методу передбачено застосування симетричного автентифікованого шифрування даних та асиметричного захисту сеансового ключа. Для традиційного гібридного і запропонованого підходів передбачається використання однакових криптографічних алгоритмів, тому їх відмінність полягає у контекстному виборі профілю, зміні строку використання ключа, виконанні додаткових перевірок і достроковій ротації ключового матеріалу.

5.5. Формування і перевірка криптографічного контейнера

Результати шифрування даних і захисту сеансового ключа об'єднуються у криптографічний контейнер:

$$Z_r = \langle C_r, T_r, W_r, N_r, AAD_r, ID_r, v_r \rangle, \quad (9)$$

де Z_r – криптографічний контейнер ресурсу, ID_r – ідентифікатор застосованого профілю, v_r – номер актуальної версії криптографічного контейнера. Зберігання номера версії та мітки часу у складі автентифікованих атрибутів запобігає повторному відтворенню попередньої версії ресурсу.

Під час отримання контейнера дозволений суб'єкт за допомогою закритого ключ SK_d розшифровує оболонку W_r та відновлює сеансовий ключ K_s і перевіряє відповідність ідентифікатора ресурсу, чинність ключа, актуальність часових і версійних параметрів, відповідність криптографічного профілю та тег автентичності. Результат перевірки й розшифрування визначається як:

$$D_r' = \{AEAD.Dec_{K_s}(N_r, C_r, T_r, AAD_r) V_K = 1 \wedge V_t = 1 \wedge V_\Omega = 1 \wedge V_T = 1, \perp, \text{інакше}, (10)$$

де V_K – ознака чинності сеансового ключа, V_t – ознака актуальності часових і версійних параметрів, V_T – результат перевірки тега автентичності, V_Ω – ознака відповідності криптографічного профілю встановленій політиці, $\perp$ – відхилення ресурсу.

У разі негативного результату хоча б однієї перевірки дані не передаються користувачеві, подія реєструється в журналі безпеки, а ключ або криптографічний профіль підлягає повторній перевірці.

5.6. Адаптивне керування криптографічними ключами

Керування криптографічними ключами охоплює їх генерування, захищене зберігання, використання, ротацію, відкликання, відновлення та знищення. Планова ротація виконується після завершення допустимого строку θ_r , установленого криптографічним профілем. Дострокова ротація ініціюється у разі зростання кіберризиків, зниження довіри до користувача, зміни критичності інформаційного ресурсу, перевищення допустимої кількості криптографічних операцій або виявлення ознак компрометації.

За зміни контексту формується оновлений вектор $X_r(t)$, повторно обчислюється значення $q_r(t)$ та визначається новий профіль $\Omega^*(t)$. Якщо новий профіль відрізняється від поточного, система генерує новий сеансовий ключ і припиняє використання попереднього. Відкликані або прострочені ключі не можуть використовуватися для нових операцій, а доступ до архівних ресурсів здійснюється лише через контрольовану процедуру відновлення ключа.

Підтримання доступності інформаційних ресурсів забезпечується обмеженням допустимого часу криптографічного оброблення під час формування множини $A(t)$, резервним захищеним зберіганням ключових

матеріалів і контрольованою процедурою відновлення ключів. Це запобігає вибору надмірно ресурсомісткого профілю та зменшує ризик недоступності даних через втрату або пошкодження окремого ключового компонента.

5.7. Структурно-функціональне та сценарне оцінювання запропонованого методу

Для подальшого кількісного оцінювання запропонованого методу враховуються частка успішно захищених операцій, пропускна здатність, час криптографічного оброблення та ресурсні витрати. Інтегральна ефективність визначається як:

$$\eta = \lambda_1 P_{sec} + \lambda_2 \hat{V} - \lambda_3 \hat{T} - \lambda_4 \hat{C}, \quad \sum_{j=1}^4 \lambda_j = 1 \quad (11)$$

де P_{sec} – частка операцій, для яких виконано всі встановлені вимоги безпеки, $\hat{V}$ – нормована пропускна здатність, $\hat{T}$ – нормований час криптографічного оброблення, $\hat{C}$ – нормовані витрати процесорного часу та оперативної пам'яті, λ_j – вагові коефіцієнти.

Перед агрегуванням усі показники нормуються на інтервалі $[0;1]$. Для показників-стимуляторів P_{sec} і $\hat{V}$ більше значення відповідає кращому результату, тоді як для показників-дестимуляторів $\hat{T}$ і $\hat{C}$ більше значення відображає погіршення ефективності. Вагові коефіцієнти визначаються відповідно до пріоритетів корпоративної політики безпеки та залишаються однаковими для всіх порівнюваних методів.

Після програмної реалізації значення інтегральної ефективності може використовуватися для порівняння криптографічних профілів і визначення необхідності повторного оцінювання контексту, зміни профілю або ротації сеансового ключа.

Запропонований інтегральний показник призначений для подальшого кількісного порівняння методів після їх програмної реалізації. У цій роботі оцінювання зосереджено на структурно-функціональній повноті запропонованого методу та його функціонуванні в типових сценаріях.

Для оцінювання повноти реалізації запропонованого методу виконано його структурно-функціональне порівняння зі статичним і традиційним гібридним підходами. Статичний метод використовує фіксований криптографічний профіль, тоді як традиційний гібридний підхід поєднує симетричне шифрування з асиметричним захистом сеансового ключа, але не підтримує контекстний вибір профілю та адаптивне керування життєвим циклом ключів.

Структурно-функціональне оцінювання виконано за такими ознаками: використання симетричних і асиметричних криптографічних механізмів, автентифіковане шифрування, урахування критичності ресурсу, рівня довіри, кіберризiku та навантаження хмарної інфраструктури, контекстний вибір криптографічного профілю, керування життєвим циклом ключів, перевірка чинності ключів і криптографічного контейнера, протидія модифікації та повторному відтворенню даних, а також адаптивна зміна параметрів захисту.

Порівняння здійснено для прийнятих у дослідженні базових реалізацій статичного та традиційного гібридного методів. Їх характеристики визначено відповідно до сформованої моделі порівняння та однакових початкових вимог до криптографічного захисту. Результати структурно-функціонального порівняння наведено в табл. 1.

Таблиця 1

Структурно-функціональне порівняння методів криптографічного захисту

Функціональна характеристика	Статичний метод	Традиційний гібридний метод	Запропонований метод
Симетричне шифрування даних	Використовується один фіксований алгоритм	Використовується симетричний алгоритм	Використовується симетричний алгоритм відповідно до вибраного криптографічного профілю
Захист сеансового ключа	Не передбачений	Реалізується асиметричним алгоритмом	Реалізується асиметричним алгоритмом відповідно до вибраного профілю
Автентифіковане шифрування	Реалізується лише частково	Реалізується	Реалізується із захистом службових атрибутів
Урахування критичності інформаційного ресурсу	Не враховується	Не враховується	Враховується під час вибору криптографічного профілю
Урахування рівня довіри до користувача	Не враховується	Не враховується	Враховується під час формування контексту
Урахування поточного кіберризiku	Не враховується	Не враховується	Враховується під час визначення рівня криптографічного захисту

Урахування навантаження хмарної інфраструктури	Не враховується	Не враховується	Враховується під час вибору допустимого профілю
Контекстний вибір криптографічного профілю	Відсутній	Відсутній	Реалізується автоматично
Строк використання сеансового ключа	Фіксований	Фіксований	Визначається відповідно до обраного профілю
Планова ротація ключів	Передбачена	Передбачена	Передбачена
Дострокова ротація ключів	Не виконується	Не виконується	Виконується за зміни контексту або кіберризик
Перевірка чинності криптографічного ключа	Часткова	Повна	Повна
Перевірка актуальності криптографічного контейнера	Не виконується	Часткова	Повна
Контроль часових параметрів	Не виконується	Частковий	Повний
Захист від модифікації шифротексту	Частковий	Повний	Повний
Захист від модифікації службових атрибутів	Не реалізований	Частково реалізований	Повністю реалізований
Захист від повторного відтворення попередньої версії	Не реалізований	Частково реалізований	Повністю реалізований
Адаптивна зміна параметрів захисту	Не виконується	Не виконується	Виконується автоматично

Формулювання в таблиці характеризують ступінь реалізації відповідної функції. Відсутність або невиконання означає, що функція не підтримується; часткова реалізація — виконання окремих процедур без повного контролю або контекстної адаптації; повна реалізація — підтримку функції в межах усіх визначених умов функціонування.

Результати структурно-функціонального порівняння свідчать, що статичний метод забезпечує лише базові криптографічні перетворення без урахування критичності ресурсу, рівня довіри, кіберризик та навантаження хмарної інфраструктури. Традиційний гібридний підхід поєднує симетричне шифрування з асиметричним захистом сеансового ключа, проте не підтримує контекстний вибір криптографічного профілю. На відміну від них, запропонований метод забезпечує контекстний вибір профілю, адаптивне керування життєвим циклом ключів, перевірку актуальності криптографічного контейнера та автоматичне реагування на зміну умов функціонування.

Для сценарного оцінювання сформовано три типові умови функціонування корпоративного хмарного середовища. Сценарій S1 відповідає обробленню некритичних даних за низького кіберризик та високого рівня довіри, що зумовлює використання базового криптографічного профілю і планову ротацію ключів. Сценарій S2 описує оброблення конфіденційних ресурсів за середнього кіберризик та зниження рівня довіри, за яких застосовується підвищений криптографічний профіль, скорочується строк використання ключа й посилюється перевірка криптографічного контейнера. Сценарій S3 характеризується високим кіберризиком, обробленням критичних даних або порушенням цілісності чи актуальності контейнера. У цьому разі застосовується критичний криптографічний профіль, виконується дострокова ротація ключа, а ресурс відхиляється за порушення хоча б однієї умови автентичності, цілісності чи актуальності.

Результати сценарного оцінювання наведено в табл. 2.

Таблиця 2

Сценарне оцінювання функціонування запропонованого методу

Характеристика	Сценарій S1	Сценарій S2	Сценарій S3
Тип інформаційного ресурсу	Некритичні внутрішні дані	Конфіденційні корпоративні дані	Критичні корпоративні дані
Рівень кіберризик	Низький	Середній	Високий
Рівень довіри до користувача	Високий	Середній	Низький
Навантаження хмарної інфраструктури	Нормальне	Підвищене	Високе
Обраний криптографічний профіль	Базовий	Підвищений	Критичний
Строк використання сеансового ключа	Стандартний	Скорочений	Мінімально допустимий
Ротація ключа	Планова	Планова або дострокова	Дострокова

Перевірка криптографічного контейнера	Стандартна	Розширена	Максимально повна
Перевірка часових і версійних параметрів	Виконується	Виконується	Виконується
Реакція на модифікацію шифротексту	Ресурс відхиляється	Ресурс відхиляється	Ресурс відхиляється, інцидент реєструється
Реакція на модифікацію службових атрибутів	Ресурс відхиляється	Ресурс відхиляється	Ресурс відхиляється, виконується додаткова перевірка
Реакція на використання простроченого ключа	Операція відхиляється	Операція відхиляється	Операція відхиляється та виконується дострокова ротація ключа
Реакція на повторне відтворення попередньої версії контейнера	Попередня версія відхиляється	Попередня версія відхиляється	Попередня версія відхиляється, подія реєструється
Підсумковий результат	Доступ надається після успішної перевірки	Доступ надається із застосуванням посиленого захисту	Небезпечна операція блокується

Структурно-функціональне та сценарне оцінювання показало, що зі зростанням критичності інформаційного ресурсу, рівня кіберризиків та зниженням довіри до користувача запропонований метод забезпечує послідовний перехід між криптографічними профілями, скорочує строк використання сеансового ключа, посилює перевірку криптографічного контейнера та автоматично виконує дострокову ротацію ключового матеріалу.

У разі порушення цілісності шифротексту чи автентифікованих атрибутів, невідповідності версії контейнера, використання простроченого ключа або повторного відтворення попередньої версії контейнера операція відхиляється, подія реєструється в журналі безпеки, а за високого рівня ризику виконується дострокова ротація ключового матеріалу.

Отже, запропонований метод забезпечує контекстно-орієнтоване узгодження параметрів шифрування, контролю цілісності та керування ключами, що підтверджує повноту реалізації його функціональних можливостей, логічну узгодженість етапів і доцільність застосування для захисту інформаційних ресурсів корпоративних хмарних обчислень.

Отримані результати свідчать, що запропонований метод розширює можливості традиційного гібридного криптографічного захисту завдяки контекстно-орієнтованому вибору криптографічного профілю, адаптивному керуванню життєвим циклом ключів і перевірці актуальності криптографічного контейнера [19, 21-22, 24]. На відміну від статичного та традиційного гібридного підходів, параметри захисту визначаються з урахуванням критичності ресурсу, рівня довіри до користувача, поточного кіберризиків та обмежень хмарної інфраструктури.

Сценарне оцінювання підтвердило послідовну зміну базового, підвищеного та критичного профілів відповідно до умов функціонування. За виявлення порушень цілісності, використання простроченого ключа або повторного відтворення попередньої версії контейнера операція відхиляється, а за високого ризику виконується дострокова ротація ключового матеріалу. Обмеженням дослідження є відсутність програмної реалізації та кількісного експериментального порівняння продуктивності запропонованого методу.

6. Висновки і перспективи подальших досліджень

Розроблено метод комбінованого криптографічного захисту даних у корпоративних хмарних обчисленнях, який поєднує симетричне автентифіковане шифрування, асиметричний захист сеансового ключа, контекстний вибір криптографічного профілю та адаптивне керування ключами. Формалізовано оцінювання необхідного рівня захисту, вибір допустимого профілю, формування сеансового ключа, криптографічного контейнера та процедуру його перевірки.

Структурно-функціональне та сценарне оцінювання підтвердило повноту реалізації заявлених функцій, логічну узгодженість етапів і коректність реагування методу на зміну критичності ресурсу, рівня довіри та кіберризиків. Запропонований метод забезпечує адаптивне узгодження параметрів шифрування, контролю цілісності й керування ключами з поточним станом корпоративного хмарного середовища.

Перспективи подальших досліджень полягають у програмній реалізації методу, обґрунтуванні вагових коефіцієнтів і порогів вибору профілів, а також експериментальному порівнянні методів за пропускну здатністю, часом криптографічного оброблення, ресурсними витратами та часткою операцій, виконаних із дотриманням установлених вимог безпеки.

Подяка, джерела фінансування

Дослідження здійснено в рамках реалізації науково-дослідної теми "Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки

програмно-технічних комплексів управління критичної інфраструктури (реєстраційний номер 0122U200483 від 06.07.2022).

Декларація про штучний інтелект

Під час підготовки цієї роботи автори використовували програму штучного інтелекту Grammarly Pro для виправлення граматики тексту та систему Strike Plagiarism для пошуку можливих проявів плагіату. Після використання цих інструментів автори переглянули та відредагували зміст за потреби і несуть повну відповідальність за зміст публікації.

Конфлікт інтересів

Автори заявляють про відсутність конфлікту інтересів та підтверджують, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Mishra, K. N., Lal, R. K., Barwal, P. N., & Mishra, A. (2025). Advancing data privacy in cloud storage: A novel multi-layer encoding framework. *Applied Sciences*, 15(13), Article 7485. <https://doi.org/10.3390/app15137485>
2. Kim, C., Kim, S., Sohn, K., Son, Y., Kumar, M., & Kim, S. (2025). Secure and scalable file encryption for cloud systems via distributed integration of quantum and classical cryptography. *Applied Sciences*, 15(14), Article 7782. <https://doi.org/10.3390/app15147782>
3. Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2025). Analysis of Azure Zero Trust architecture implementation for mid-size organizations. *Journal of Cybersecurity and Privacy*, 5(1), Article 2. <https://doi.org/10.3390/jcp5010002>
4. Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment. *Sensors*, 25(2), Article 550. <https://doi.org/10.3390/s25020550>
5. Velmurugan, S., Prakash, M., Neelakandan, S., et al. (2024). Provably secure data selective sharing scheme with cloud-based decentralized trust management systems. *Journal of Cloud Computing*, 13, Article 86. <https://doi.org/10.1186/s13677-024-00634-8>
6. Huang, J., & Yi, J. (2024). The key security management scheme of cloud storage based on blockchain and digital twins. *Journal of Cloud Computing*, 13, Article 15. <https://doi.org/10.1186/s13677-023-00587-4>
7. Goswami, P., Faujdar, N., Debnath, S., et al. (2024). Investigation on storage level data integrity strategies in cloud computing: Classification, security obstructions, challenges and vulnerability. *Journal of Cloud Computing*, 13, Article 45. <https://doi.org/10.1186/s13677-024-00605-z>
8. Pathak, M., Mishra, K. N., & Singh, S. P. (2024). Securing data and preserving privacy in cloud IoT-based technologies: An analysis of assessing threats and developing effective safeguards. *Artificial Intelligence Review*, 57, Article 269. <https://doi.org/10.1007/s10462-024-10908-x>
9. Ajala, O. A., Arinze, C. A., Ofodile, O. C., Okoye, C. C., & Daraojimba, A. I. (2024). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. *Magna Scientia Advanced Research and Reviews*, 10(1), 321–329.
10. Kostiuk, Y., Bebesko, B., Kriuchkova, L., Lytvynov, V., Oksanych, I., Skladannyi, P., & Khorolska, K. (2024). Information protection and secure data exchange in wireless mobile networks using authentication and key exchange protocols. *Cybersecurity: Education, Science, Technique*, 1(25), 229–252. <https://doi.org/10.28925/2663-4023.2024.25.229252>
11. Junior, M. A., Appiahene, P., Appiah, O., et al. (2025). Cloud data privacy protection with homomorphic algorithm: A systematic literature review. *Journal of Cloud Computing*, 14, Article 84. <https://doi.org/10.1186/s13677-025-00774-5>
12. Skladannyi, P. M., Kostiuk, Y. V., Mazur, N. P., & Pitaichuk, M. A. (2025). Performance evaluation and characteristics of access protocols for cloud computing environments based on universal testing. *Telecommunication and Information Technologies*, (1)(86), 61–74. <https://doi.org/10.31673/2412-4338.2025.014649>
13. Musa, N. S., Murugan, T., N., N. A., et al. (2025). Research study on securing the cloud: Utilizing conventional and blockchain-based access control mechanisms. *Journal of Cloud Computing*, 14, Article 88. <https://doi.org/10.1186/s13677-025-00803-3>
14. Kostiuk, Y., Khorolska, K., Bebesko, B., Dovzhenko, N., Korshun, N., & Pazynin, A. (2025). Software tools for ensuring information security against hidden threats in cloud computing infrastructure. *Cybersecurity: Education, Science, Technique*, 4(28), 633–655. <https://doi.org/10.28925/2663-4023.2025.28.857>
15. Farooq, S., Altaf, A., Iqbal, F., Bautista Thompson, E., Ramírez-Vargas, D. L., Díez, I. D. L. T., & Ashraf, I. (2023). Resilience optimization of post-quantum cryptography key encapsulation algorithms. *Sensors*, 23(12), Article 5379.
16. Skladannyi, P. M., Mashkina, I. V., Rzaieva, S. L., & Kostiuk, Y. V. (2025). GDPR-based methods for securing data repositories against information leakage and cyber threats. *Telecommunication and Information Technologies*, (2), 59–76. <https://doi.org/10.31673/2412-4338.2025.027860>
17. N'goran, R., Tetchueng, J. L., Pandry, G., Kermarrec, Y., & Asseu, O. (2022). Trust assessment model based on a Zero Trust strategy in a community cloud environment. *Engineering*, 14(11), 479–496.
18. Rzaieva, S. L., Skladannyi, P. M., Mashkina, I. V., & Kostiuk, Y. V. (2025). Role-based access control (RBAC) implementation model for a multi-level data warehouse architecture. *Modern Information Protection*, 3(63), 137–149. <https://doi.org/10.31673/2409-7292.2025.031671>
19. Wang, R., Li, C., Zhang, K., et al. (2025). Zero-trust based dynamic access control for cloud computing. *Cybersecurity*, 8, Article 12. <https://doi.org/10.1186/s42400-024-00320-x>
20. Skladannyi, P. M., Hulak, H. M., & Kostiuk, Y. V. (2025). Chaotic number generator with fuzzy control for cryptographic systems with dynamic trust. *Telecommunication and Information Technologies*, (4)(89), 137–147. <https://doi.org/10.31673/2412-4338.2025.048916>

21. Liu, C., Tan, R., Wu, Y., et al. (2024). Dissecting Zero Trust: Research landscape and its implementation in IoT. *Cybersecurity*, 7, Article 20. <https://doi.org/10.1186/s42400-024-00212-0>
22. Taherdoost, H., Le, T.-V., & Slimani, K. (2025). Cryptographic techniques in artificial intelligence security: A bibliometric review. *Cryptography*, 9(1), Article 17. <https://doi.org/10.3390/cryptography9010017>
23. Rzaieva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*, 31(1), 23–36. <https://doi.org/10.18372/2225-5036.31.20634>
24. Sen, S. (2026). Artificial intelligence and cryptography in data security. In *2026 IEEE World AI IoT Congress (AIoT)* (pp. 877–886). IEEE. <https://doi.org/10.1109/AIIoT68874.2026.11569582>
25. Kostiuk, Y., Rzaieva, S., Khorolska, K., Mazur, N., & Korshun, N. (2025). Architecture of the software system of confidential access to information resources of computer networks. In *Proceedings of the Workshop on Cyber Security and Data Protection (CSDP 2025)* (Vol. 4042, pp. 37–53). CEUR Workshop Proceedings.
26. Elkhodr, M. (2025). An AI-driven framework for integrated security and privacy in Internet of Things using quantum-resistant blockchain. *Future Internet*, 17(6), Article 246. <https://doi.org/10.3390/fi17060246>

References

1. Mishra, K. N., Lal, R. K., Barwal, P. N., & Mishra, A. (2025). Advancing data privacy in cloud storage: A novel multi-layer encoding framework. *Applied Sciences*, 15(13), Article 7485. <https://doi.org/10.3390/app15137485>
2. Kim, C., Kim, S., Sohn, K., Son, Y., Kumar, M., & Kim, S. (2025). Secure and scalable file encryption for cloud systems via distributed integration of quantum and classical cryptography. *Applied Sciences*, 15(14), Article 7782. <https://doi.org/10.3390/app15147782>
3. Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2025). Analysis of Azure Zero Trust architecture implementation for mid-size organizations. *Journal of Cybersecurity and Privacy*, 5(1), Article 2. <https://doi.org/10.3390/jcp5010002>
4. Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment. *Sensors*, 25(2), Article 550. <https://doi.org/10.3390/s25020550>
5. Velmurugan, S., Prakash, M., Neelakandan, S., et al. (2024). Provably secure data selective sharing scheme with cloud-based decentralized trust management systems. *Journal of Cloud Computing*, 13, Article 86. <https://doi.org/10.1186/s13677-024-00634-8>
6. Huang, J., & Yi, J. (2024). The key security management scheme of cloud storage based on blockchain and digital twins. *Journal of Cloud Computing*, 13, Article 15. <https://doi.org/10.1186/s13677-023-00587-4>
7. Goswami, P., Faujdar, N., Debnath, S., et al. (2024). Investigation on storage level data integrity strategies in cloud computing: Classification, security obstructions, challenges and vulnerability. *Journal of Cloud Computing*, 13, Article 45. <https://doi.org/10.1186/s13677-024-00605-z>
8. Pathak, M., Mishra, K. N., & Singh, S. P. (2024). Securing data and preserving privacy in cloud IoT-based technologies: An analysis of assessing threats and developing effective safeguards. *Artificial Intelligence Review*, 57, Article 269. <https://doi.org/10.1007/s10462-024-10908-x>
9. Ajala, O. A., Arinze, C. A., Ofodile, O. C., Okoye, C. C., & Daraojimba, A. I. (2024). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. *Magna Scientia Advanced Research and Reviews*, 10(1), 321–329.
10. Kostiuk, Y., Bebeshko, B., Kriuchkova, L., Lytvynov, V., Oksanych, I., Skladannyi, P., & Khorolska, K. (2024). Information protection and secure data exchange in wireless mobile networks using authentication and key exchange protocols. *Cybersecurity: Education, Science, Technique*, 1(25), 229–252. <https://doi.org/10.28925/2663-4023.2024.25.229252>
11. Junior, M. A., Appiahene, P., Appiah, O., et al. (2025). Cloud data privacy protection with homomorphic algorithm: A systematic literature review. *Journal of Cloud Computing*, 14, Article 84. <https://doi.org/10.1186/s13677-025-00774-5>
12. Skladannyi, P. M., Kostiuk, Y. V., Mazur, N. P., & Pitaichuk, M. A. (2025). Performance evaluation and characteristics of access protocols for cloud computing environments based on universal testing. *Telecommunication and Information Technologies*, (1)(86), 61–74. <https://doi.org/10.31673/2412-4338.2025.014649>
13. Musa, N. S., Murugan, T. N., N. A., et al. (2025). Research study on securing the cloud: Utilizing conventional and blockchain-based access control mechanisms. *Journal of Cloud Computing*, 14, Article 88. <https://doi.org/10.1186/s13677-025-00803-3>
14. Kostiuk, Y., Khorolska, K., Bebeshko, B., Dovzhenko, N., Korshun, N., & Pazynin, A. (2025). Software tools for ensuring information security against hidden threats in cloud computing infrastructure. *Cybersecurity: Education, Science, Technique*, 4(28), 633–655. <https://doi.org/10.28925/2663-4023.2025.28.857>
15. Farooq, S., Altaf, A., Iqbal, F., Bautista Thompson, E., Ramírez-Vargas, D. L., Díez, I. D. L. T., & Ashraf, I. (2023). Resilience optimization of post-quantum cryptography key encapsulation algorithms. *Sensors*, 23(12), Article 5379.
16. Skladannyi, P. M., Mashkina, I. V., Rzaieva, S. L., & Kostiuk, Y. V. (2025). GDPR-based methods for securing data repositories against information leakage and cyber threats. *Telecommunication and Information Technologies*, (2), 59–76. <https://doi.org/10.31673/2412-4338.2025.027860>
17. N'goran, R., Tetchueng, J. L., Pandry, G., Kermarrec, Y., & Asseu, O. (2022). Trust assessment model based on a Zero Trust strategy in a community cloud environment. *Engineering*, 14(11), 479–496.
18. Rzaieva, S. L., Skladannyi, P. M., Mashkina, I. V., & Kostiuk, Y. V. (2025). Role-based access control (RBAC) implementation model for a multi-level data warehouse architecture. *Modern Information Protection*, 3(63), 137–149. <https://doi.org/10.31673/2409-7292.2025.031671>
19. Wang, R., Li, C., Zhang, K., et al. (2025). Zero-trust based dynamic access control for cloud computing. *Cybersecurity*, 8, Article 12. <https://doi.org/10.1186/s42400-024-00320-x>
20. Skladannyi, P. M., Hulak, H. M., & Kostiuk, Y. V. (2025). Chaotic number generator with fuzzy control for cryptographic systems with dynamic trust. *Telecommunication and Information Technologies*, (4)(89), 137–147. <https://doi.org/10.31673/2412-4338.2025.048916>

21. Liu, C., Tan, R., Wu, Y., et al. (2024). Dissecting Zero Trust: Research landscape and its implementation in IoT. *Cybersecurity*, 7, Article 20. <https://doi.org/10.1186/s42400-024-00212-0>
22. Taherdoost, H., Le, T.-V., & Slimani, K. (2025). Cryptographic techniques in artificial intelligence security: A bibliometric review. *Cryptography*, 9(1), Article 17. <https://doi.org/10.3390/cryptography9010017>
23. Rzaieva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*, 31(1), 23–36. <https://doi.org/10.18372/2225-5036.31.20634>
24. Sen, S. (2026). Artificial intelligence and cryptography in data security. In *2026 IEEE World AI IoT Congress (AIIoT)* (pp. 877–886). IEEE. <https://doi.org/10.1109/AIIoT68874.2026.11569582>
25. Kostiuk, Y., Rzaieva, S., Khorolska, K., Mazur, N., & Korshun, N. (2025). Architecture of the software system of confidential access to information resources of computer networks. In *Proceedings of the Workshop on Cyber Security and Data Protection (CSDP 2025)* (Vol. 4042, pp. 37–53). CEUR Workshop Proceedings.
26. Elkhodr, M. (2025). An AI-driven framework for integrated security and privacy in Internet of Things using quantum-resistant blockchain. *Future Internet*, 17(6), Article 246. <https://doi.org/10.3390/fi17060246>

Надійшла до редакції: 14.05.2026

Прийнята до друку: 15.09.2026

Опубліковано: 30.09.2026