https://orcid.org/0000-0002-5118-1003
https://orcid.org/0000-0002-7775-6039
https://orcid.org/0000-0001-5423-0985
https://orcid.org/0000-0002-7253-5990
https://orcid.org/0000-0002-9349-7946

УДК 004.056:004.75:004.415

О.С. ЛИТВИН[*], П.М. СКЛАДАННИЙ[*,], Ю.В. КОСТЮК[*], О.Б. ЖИЛЬЦОВ[*], В.Ю. СОКОЛОВ[*]**

МЕТОД АДАПТИВНОГО КЕРУВАННЯ КРИПТОГРАФІЧНИМ ЗАХИСТОМ У КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ ДИНАМІЧНОЇ ОЦІНКИ РИЗИКУ ТА ПОСТКВАНТОВИХ АЛГОРИТМІВ

[*] Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
[**] Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

Анотація. *У статті розглянуто проблему забезпечення адаптивного криптографічного захисту в комп'ютерних мережах за умов зростання кіберзагроз, збільшення кількості атак на інформаційні ресурси та необхідності переходу до постквантових криптографічних алгоритмів. Встановлено, що традиційні підходи до вибору криптографічних механізмів мають статичний характер і недостатньо враховують динаміку ризику, стан мережевої інфраструктури, параметри трафіку та обмеженість ресурсів, що можуть призводити до неефективного використання ресурсів або зниження рівня захисту. Запропоновано метод керування криптографічним захистом, який базується на динамічній оцінці ризику та забезпечує адаптивний вибір криптографічних алгоритмів залежно від стану системи, рівня загроз і вимог до безпеки даних. У межах методу сформовано модель інтегральної оцінки ризику, що враховує інтенсивність загроз, рівень вразливостей, критичність активів та ймовірність реалізації атак. Введено адаптивний показник ефективності криптографічних алгоритмів з урахуванням ризикової складової та витрат обчислювальних ресурсів. Реалізовано механізм динамічного вибору криптографічних рішень, який передбачає застосування класичних, гібридних і постквантових алгоритмів залежно від рівня ризику та стану інформаційного середовища. Особливістю підходу є введення функції інтенсивності криптографічного захисту, що дає змогу формалізувати рівень безпеки як змінну величину в часі та адаптувати параметри захисту до умов функціонування мережі. Показано, що метод підвищує ефективність криптографічного захисту, оптимізує використання ресурсів і забезпечує стійкість інформаційних систем до сучасних і нових кіберзагроз.*

Ключові слова: *криптографічний захист, керування, постквантова криптографія, оцінка ризику, комп'ютерні мережі, інформаційна безпека.*

Abstract. *The article addresses the problem of ensuring adaptive cryptographic protection in computer networks under conditions of increasing cyber threats, a growing number of attacks on information resources, and the need to transition to post-quantum cryptographic algorithms. It is established that traditional approaches to the selection of cryptographic mechanisms are predominantly static and insufficiently consider risk dynamics, the state of network infrastructure, traffic characteristics, and resource constraints, which may result in inefficient resource utilization or a reduced level of information protection. A method for cryptographic protection management based on dynamic risk assessment is proposed. It provides adaptive selection of cryptographic algorithms depending on the current state of the system, threat level, and data security requirements. Within the proposed method, an integrated risk assessment model is developed that takes into account threat intensity, vulnerability level, asset criticality, and the probability of attack realization. An adaptive performance indicator for cryptographic algorithms is introduced, considering both the risk component and computational resource consumption. A mechanism for the dynamic selection of cryptographic solutions is implemented, enabling the use of classical, hybrid, and post-quantum algorithms depending on the risk level and the current state of the information*

ISSN 1028-9763. Математичні машини і системи. 2026. № 3

environment. A distinctive feature of the proposed approach is the introduction of a cryptographic protection intensity function, which enables the formalization of the security level as a time-varying parameter and adapt protection settings to changing network operating conditions. The results demonstrate that the proposed method improves the efficiency of cryptographic protection, optimizes resource utilization, and enhances the resilience of information systems against current and emerging cyber threats.
Keywords: *cryptographic protection, management, post-quantum cryptography, risk assessment, computer networks, information security.*

DOI: 10.34121/1028-9763-2026-3-31-48

1. Вступ

Сучасний розвиток комп'ютерних мереж і інформаційно-інтелектуальних систем супроводжується стрімким зростанням обсягів передавання даних, ускладненням архітектурних рішень та підвищенням рівня кіберзагроз, що зумовлює необхідність забезпечення ефективного криптографічного захисту інформації. Особливої актуальності набуває проблема захисту даних в умовах переходу до постквантових обчислень, які потенційно здатні компрометувати традиційні криптографічні алгоритми [1, 2, 3]. У цьому контексті використання постквантових криптографічних механізмів розглядається як один із ключових напрямів підвищення стійкості інформаційних систем до перспективних атак [4, 5, 6]. Водночас впровадження таких алгоритмів супроводжується значними обчислювальними витратами, що обмежує їх застосування у реальних мережевих середовищах, особливо в умовах обмежених ресурсів.

Аналіз існуючих підходів до забезпечення криптографічного захисту показує, що більшість із них базується на статичних схемах вибору криптографічних механізмів, які не враховують змінність рівня загроз, динаміку вразливостей та контекст функціонування мережі [1, 4]. Це призводить до ситуацій, коли система або використовує надмірно ресурсоємні алгоритми при низькому рівні ризику, або не забезпечує належного рівня захисту в умовах його зростання [7]. Отже, виникає суперечність між необхідністю підвищення рівня криптографічної стійкості та потребою оптимізації використання обчислювальних ресурсів, що визначає актуальність розроблення адаптивних методів керування криптографічним захистом.

Наукова новизна роботи полягає у розробленні методу керування криптографічним захистом у комп'ютерних мережах, який, на відміну від існуючих підходів, забезпечує динамічний вибір криптографічних механізмів на основі інтегральної оцінки поточного та прогнозованого рівня ризику [8, 9]. Запропонований метод передбачає формалізацію ризику як функції інтенсивності загроз, рівня вразливостей і критичності інформаційних активів [10, 11], а також введення адаптивного показника ефективності криптографічних алгоритмів з урахуванням ризикової складової. Додатково впроваджено концепцію інтенсивності криптографічного захисту, що дозволяє описати рівень безпеки як змінну величину в часі та реалізувати механізм адаптивного керування.

На відміну від відомих підходів, у яких оцінювання ризику, вибір криптографічного механізму та ресурсні обмеження аналізуються окремо [12, 13], у запропонованому методі ці складові інтегровано в єдину керувальну модель, що забезпечує динамічний перехід між класичними, гібридними та постквантовими алгоритмами відповідно до поточного й прогнозованого стану кіберсередовища.

Теоретичне значення отриманих результатів полягає у розвитку моделей ризик-орієнтованого управління інформаційною безпекою, зокрема в частині формалізації процесів динамічного вибору криптографічних алгоритмів у комп'ютерних мережах [10, 12–14]. Практичне значення полягає у можливості застосування запропонованого методу для побудови адаптивних систем криптографічного захисту в інформаційно-інтелектуальних системах підприємств, що дозволяє підвищити рівень їх захищеності та ефективність використання ресурсів.

У сучасних комп'ютерних мережах забезпечення ефективного криптографічного захисту інформації ускладнюється зростанням інтенсивності кіберзагроз, динамічністю мережевого середовища та необхідністю переходу до постквантових криптографічних алгоритмів [3, 6]. Розвиток квантових обчислень створює передумови для компрометації традиційних криптографічних механізмів [2], що зумовлює потребу впровадження нових підходів до захисту інформації. Водночас постквантові алгоритми характеризуються підвищеними вимогами до обчислювальних ресурсів [5, 15], що обмежує їх широке застосування у реальних мережевих системах.

Існуючі підходи до організації криптографічного захисту в комп'ютерних мережах переважно базуються на статичному виборі криптографічних алгоритмів [1, 4], який здійснюється на етапі проєктування системи або налаштування її параметрів. Такий підхід не враховує змінність рівня кіберзагроз, стану мережевої інфраструктури, рівня вразливостей та критичності інформаційних ресурсів у процесі функціонування системи [11, 16]. У результаті виникають ситуації, коли використовуються надмірно ресурсоємні криптографічні механізми при низькому рівні загроз, що призводить до неефективного використання ресурсів [7], або, навпаки, застосовуються недостатньо стійкі механізми в умовах підвищеного ризику [12].

Отже, формується суперечність між необхідністю забезпечення високого рівня криптографічної стійкості та потребою оптимізації використання обчислювальних ресурсів мережі [7, 17]. З одного боку, підвищення рівня захисту потребує використання більш складних, зокрема постквантових, алгоритмів [18, 19], а з іншого — обмежені ресурси системи вимагають раціонального їх використання. Додатково ускладнює ситуацію відсутність механізмів, які дозволяють враховувати динаміку змін кіберсередовища та оперативно адаптувати криптографічний захист до поточних умов.

Отже, існує науково-практична проблема розроблення методу адаптивного керування криптографічним захистом у комп'ютерних мережах, який забезпечує вибір криптографічних механізмів залежно від рівня ризику, стану системи та доступних ресурсів [8, 9]. Розв'язання цієї проблеми потребує створення підходу, який дозволяє інтегрувати оцінювання ризику з процесом вибору криптографічних алгоритмів і забезпечує їх динамічну зміну відповідно до умов функціонування мережі.

2. Аналіз останніх досліджень і публікацій

Останнім часом проблема переходу до постквантового криптографічного захисту в мережевих та інформаційних системах набула виразно прикладного характеру: акцент змістився від загальних оглядів постквантових алгоритмів до досліджень міграції, оцінювання продуктивності, енергоспоживання та інтеграції постквантової криптографії (Post-Quantum Cryptography, PQC) у реальні мережеві протоколи [1, 3, 4]. Однією з базових праць у цьому напрямі є дослідження Hasan та співавторів, у якому запропонована структура для міграції до постквантової криптографії з аналізом залежностей між криптографічними активами та використанням підходів до пріоритезації заміни криптосистем [1]. Автори показують, що перехід до PQC є складним багаторівневим процесом, який потребує інвентаризації активів і поетапного планування, однак не пропонують механізму динамічного вибору криптографічних засобів залежно від рівня ризику.

Суттєвим доповненням є систематичний огляд Näther та співавторів, у якому узагальнено підходи до міграції програмних систем до PQC, визначено етапи переходу та типові труднощі впровадження [4]. У роботі підкреслюється відсутність узгоджених методик та практичних механізмів адаптації криптографічного захисту, що підтверджує актуальність подальших досліджень у цьому напрямі.

Окремий напрям становлять дослідження продуктивності постквантових алгоритмів у мережевих протоколах. Так, Sosnowski та співавтори виконали аналіз продуктивності Post-

Quantum TLS 1.3 (Transport Layer Security version 1.3), визначивши вплив постквантових алгоритмів на затримки та обсяг переданих даних [20]. Встановлено, що ефективність таких алгоритмів суттєво залежить від мережевих умов, однак у роботі відсутній механізм адаптивного вибору криптографічних рішень.

У праці Tasopoulos та співавторів досліджено енергоспоживання Post-Quantum TLS 1.3 на ресурсно-обмежених пристроях, де показано значне зростання витрат ресурсів при використанні постквантових алгоритмів [5]. Це підтверджує необхідність урахування ресурсних обмежень при виборі криптографічних механізмів, проте не розв'язує задачу інтеграції цих параметрів з оцінкою ризику.

У роботі Giron та співавторів проаналізовано продуктивність гібридного KEMTLS у різних мережевих середовищах [21]. Отримані результати свідчать про доцільність використання гібридних схем як перехідного етапу до постквантової криптографії, однак питання динамічного керування криптографічним захистом залишаються відкритими.

Подальший розвиток гібридних підходів представлено у дослідженні Astrizi та Custódio, де запропоновано механізм інтеграції постквантових криптографічних механізмів у TLS 1.3 [22]. Незважаючи на практичну значущість результатів, у роботі не розглядається питання адаптивного вибору криптографічних алгоритмів залежно від зміни умов функціонування системи.

У праці Scalise та співавторів виконано аналіз застосування постквантових алгоритмів у мережах 5G/6G, що підтверджує можливість їх інтеграції у сучасні телекомунікаційні системи [6]. Водночас дослідження орієнтоване на конкретні сценарії і не пропонує універсального методу керування криптографічним захистом.

У роботі Montenegro та співавторів запропоновано структуру для оцінювання продуктивності Post-Quantum TLS, що дозволяє порівнювати різні криптографічні конфігурації [23]. Однак цей підхід має оціночний характер і не передбачає автоматизованого прийняття рішень у реальному часі.

Практичні аспекти реалізації постквантової криптографії в бездротових мережах досліджено у роботах Ojetunde та співавторів, де продемонстровано можливість побудови захищених каналів зв'язку з використанням PQC [24]. Незважаючи на підтвердження практичної реалізованості, у роботі відсутній ризик-орієнтований підхід до керування криптографічним захистом.

Отже, проведений аналіз показує, що існуючі дослідження зосереджені на питаннях міграції до постквантової криптографії, оцінювання продуктивності та інтеграції PQC у мережеві протоколи [3, 25]. Водночас невирішеною залишається важлива частина загальної проблеми — відсутність методу керування криптографічним захистом у комп'ютерних мережах, який поєднує динамічну оцінку ризику, врахування ресурсних обмежень та адаптивний вибір між класичними, гібридними та постквантовими алгоритмами. Саме вирішення цієї задачі є предметом даної статті.

Метою статті є розроблення методу адаптивного керування криптографічним захистом у комп'ютерних мережах на основі динамічної оцінки ризику та використання постквантових криптографічних алгоритмів, що забезпечує адаптивний вибір криптографічних механізмів залежно від умов функціонування системи, рівня загроз і ресурсних обмежень.

Для досягнення поставленої мети у роботі було вирішено такі завдання:

• проаналізувати сучасні підходи до забезпечення криптографічного захисту в комп'ютерних мережах та визначити їх обмеження в умовах переходу до постквантової криптографії;

• сформувати підхід до оцінювання рівня ризику з урахуванням інтенсивності загроз, рівня вразливостей і критичності інформаційних активів;

• розробити модель оцінювання ефективності криптографічних алгоритмів з урахуванням ризикової складової та ресурсних обмежень;

• обґрунтувати механізм адаптивного вибору криптографічних рішень, що передбачає використання класичних, гібридних та постквантових алгоритмів залежно від рівня ризику;

• сформувати концепцію динамічного керування рівнем криптографічного захисту в часі; оцінити ефективність запропонованого методу в умовах змінного рівня кіберзагроз.

3. Моделі та метод адаптивного керування криптографічним захистом

У межах дослідження розроблено метод керування криптографічним захистом у комп'ютерних мережах, який орієнтований на адаптивне застосування криптографічних механізмів залежно від поточного та прогнозованого стану кіберсередовища. Основною ідеєю запропонованого підходу є поєднання трьох взаємопов'язаних складових: динамічного оцінювання ризику, оцінювання ефективності криптографічних алгоритмів і механізму вибору такого алгоритму, який у конкретний момент часу забезпечує раціональний баланс між рівнем захищеності та витратами ресурсів [7, 8, 12]. На відміну від статичних схем, у яких криптографічний механізм визначається один раз на етапі налаштування системи, запропонований метод забезпечує динамічний перегляд вибору алгоритму під час функціонування мережі, що узгоджується з підходами адаптивного управління інформаційною безпекою [7, 8, 16] та дає змогу враховувати зміни інтенсивності загроз, стану вразливостей, критичності активів і ресурсних можливостей середовища.

3.1. Модель динамічного оцінювання ризику

Початковим етапом побудови методу є формалізація ризику, оскільки саме ризик виступає базовим керувальним фактором, який визначає доцільність посилення або послаблення криптографічного захисту [11, 12, 13]. У межах даного дослідження ризик розглядається як узагальнена характеристика небезпеки порушення конфіденційності, цілісності або доступності інформації в комп'ютерній мережі. На його значення впливають три ключові параметри: інтенсивність загроз, рівень вразливостей та критичність інформаційних активів. Інтенсивність загроз відображає частоту або силу потенційного негативного впливу з боку атакувального середовища, рівень вразливостей характеризує ступінь відкритості системи до реалізації атак [10, 26], а критичність активів показує важливість відповідних ресурсів для функціонування мережі або підприємства.

З урахуванням зазначених факторів інтегральний ризик у момент часу t пропонується визначати за формулою

$$R(t) = T(t) \cdot V(t) \cdot C(t), \tag{1}$$

де $R(t)$ — інтегральний рівень ризику у момент часу t, $T(t)$ — інтенсивність загроз у момент часу t, $V(t)$ — рівень вразливості системи, $C(t)$ — критичність активів. Формула (1) вводиться для того, щоб відобразити не ізольований, а саме комплексний вплив загрозового середовища на стан безпеки системи. Її мультиплікативний характер означає, що навіть при помірних значеннях окремих складових ризик може різко зростати у випадку їх одночасного підвищення. Наприклад, якщо мережева інфраструктура обробляє критично важливі дані, має високий рівень вразливостей і перебуває під інтенсивним впливом зовнішніх загроз, то загальний ризик набуває великого значення навіть без введення додаткових поправочних коефіцієнтів. Саме тому дана формула використовується як базова модель оцінювання поточного рівня небезпеки.

Оскільки значення окремих складових можуть мати різну шкалу вимірювання, для подальшого використання в алгоритмі керування доцільно перейти до нормованого ризику:

$$R_n(t) = \frac{R(t)}{R_{max}}, \tag{2}$$

де $R_n(t)$ — нормоване значення ризику, R_{max} — максимально можливе або допустиме значення ризику в межах обраної моделі. Формула (2) необхідна для приведення ризику до інтервалу [0;1], що істотно спрощує подальше використання цього показника в моделях адаптивного вибору, функціях інтенсивності захисту та порогових правилах прийняття рішень. Інакше кажучи, ця формула забезпечує уніфікацію масштабу ризику і дозволяє використовувати його як безрозмірний керувальний параметр.

Однак для криптографічного захисту важливий не лише поточний рівень ризику, а й тенденція його зміни. Якщо система спирається виключно на поточне значення ризику, то реагування на атаку може бути запізнілим. Саме тому до моделі вводиться прогнозований ризик:

$$\hat{R}(t + \Delta t) = R_n(t) + \alpha \cdot \frac{dR_n(t)}{dt}, \tag{3}$$

де $\hat{R}(t + \Delta t)$ — прогнозоване значення ризику на наступний інтервал часу, $\frac{dR_n(t)}{dt}$ — швидкість зміни нормованого ризику, α — коефіцієнт прогнозування. Формула (3) використовується для переходу від реактивного до проактивного підходу. Її зміст полягає в тому, що система враховує не тільки факт наявності ризику, а й динаміку його зростання або зниження. Якщо ризик швидко зростає, навіть за ще не критичного поточного значення система може завчасно перейти до більш сильного криптографічного режиму. Надалі саме прогнозований ризик застосовується для визначення рівня інтенсивності захисту та адаптивної ефективності алгоритмів.

3.2. Модель оцінювання ефективності криптографічних алгоритмів

Після оцінювання ризику необхідно визначити, наскільки той чи інший криптографічний алгоритм є доцільним для використання в поточних умовах. У межах цієї статті криптографічний алгоритм розглядається не лише як засіб шифрування або обміну ключами, а як функціональний елемент мережевого захисту, який характеризується сукупністю кількох важливих властивостей [15, 20, 23]. До таких властивостей віднесено криптографічну стійкість, швидкодію, затримку при обробці даних, ресурсоємність, обсяг службового трафіку та придатність до застосування в конкретній мережевій інфраструктурі.

Для узагальнення цих характеристик вводиться базовий показник ефективності алгоритму:

$$E(a_i) = \sum_{k=1}^{m} w_k \cdot e_k(a_i), \tag{4}$$

де $E(a_i)$ — базова інтегральна ефективність i-го криптографічного алгоритму, $e_k(a_i)$ — значення k-го показника для алгоритму a_i, w_k — ваговий коефіцієнт важливості відповідного показника, m — кількість критеріїв оцінювання.

Формула (4) потрібна для багатокритеріального зіставлення алгоритмів, оскільки в реальній мережі неможливо обирати алгоритм лише за одним параметром, наприклад, тільки за криптостійкістю або тільки за швидкодією. Якщо алгоритм має дуже високий рівень стійкості, але водночас спричиняє надмірні затримки або перевантажує ресурсо-обмежені вузли, його застосування не завжди буде оптимальним. Тому дана формула використовується як інструмент інтегрування кількох показників в одну узагальнену оцінку.

Проте базова ефективність сама по собі ще не враховує безпековий контекст. Один і той самий алгоритм може бути доцільним при низькому ризику і недостатнім при високому. Для зв'язування оцінки алгоритму з поточним станом загрозового середовища вводиться адаптивний показник ефективності:

$$E_{ad}(a_i, t) = E(a_i) \cdot (1 - \hat{R}(t + \Delta t)), \quad (5)$$

де $E_{ad}(a_i, t)$ — адаптивна ефективність i-го алгоритму у момент часу t, $\hat{R}(t + \Delta t)$ — прогнозований ризик, визначений за формулою (3). Формула (5) вводиться для того, щоб базова оцінка алгоритму змінювалася залежно від безпекової ситуації. Зі зростанням ризику алгоритми з низьким запасом стійкості або недостатньою придатністю до використання в критичних умовах повинні втрачати пріоритет. Отже, ця формула використовується для узгодження функціональної доцільності алгоритму з поточним рівнем небезпеки.

Оскільки застосування постквантових і гібридних механізмів часто супроводжується додатковими витратами обчислювальних ресурсів, до моделі доцільно додати ресурсну складову:

$$E_{res}(a_i, t) = E_{ad}(a_i, t) \cdot \frac{Res(t)}{Res_{max}}, \quad (6)$$

де $E_{res}(a_i, t)$ — адаптивна ефективність алгоритму з урахуванням ресурсного фактора, $Res(t)$ — доступний обсяг ресурсів системи у момент часу t, Res_{max} — максимальний або еталонний рівень доступних ресурсів. Формула (6) використовується для того, щоб процес вибору криптографічного механізму не був відірваний від реальних технічних можливостей мережі. Якщо ресурсів недостатньо, навіть високостійкий алгоритм може бути непридатним до широкого застосування на окремих вузлах. Отже, ця формула дозволяє перейти від абстрактної безпекової переваги до практичної реалізованості алгоритму в конкретних умовах функціонування системи [5, 15].

3.3. Функція інтенсивності криптографічного захисту

Наступним кроком є формалізація не просто вибору окремого алгоритму, а загального рівня криптографічного впливу, який система повинна підтримувати в поточний момент часу. Для цього вводиться поняття інтенсивності криптографічного захисту [25, 27]. Під інтенсивністю в даному випадку розуміється узагальнений рівень жорсткості або сили криптографічного режиму, який повинна застосовувати мережа залежно від стану ризику.

Загальна функціональна залежність інтенсивності від прогнозованого ризику задається так:

$$U(t) = f(\hat{R}(t + \Delta t)), \quad (7)$$

де $U(t) \in [0;1]$ — інтенсивність криптографічного захисту, $f(\hat{R}(t + \Delta t))$ — функція, яка відображає зв'язок між ризиком і рівнем захисту. Формула (7) є концептуальною. Вона не задає конкретного виду функції, але вводить принцип: що вищий прогнозований ризик, то вищою має бути інтенсивність криптографічного захисту. Ця формула потрібна для логічного переходу від оцінки ризику до формування керувального сигналу, який надалі визначатиме клас рішення.

$$U(t) = \hat{R}(t + \Delta t)^{\beta}, \quad (8)$$

де β — параметр чутливості системи до зміни ризику. Формула (8) використовується для гнучкого налаштування реакції системи. Якщо $\beta > 1$, то система слабше реагує на низькі

значення ризику і різко підсилює захист лише у зоні високих ризиків. Якщо $0 < \beta < 1$, система стає чутливішою вже на ранніх етапах зростання ризику. Це дозволяє адаптувати характер керування до різних типів мережевого середовища: корпоративного, критичного, ресурсно-обмеженого або високонавантаженого.

Отже, функція інтенсивності використовується далі як проміжна керувальна змінна, яка перетворює безперервну зміну ризику в керовану реакцію системи у вигляді переходу між режимами криптографічного захисту. Дана залежність забезпечує можливість адаптивного регулювання інтенсивності криптографічного захисту відповідно до прогнозованої динаміки зміни рівня ризику в інформаційно-комунікаційній системі.

На рис. 1 представлено залежність інтенсивності криптографічного захисту $U(t)$ від прогнозованого рівня ризику $\hat{R}(t+\Delta t)$ для різних значень параметра чутливості β. Показано, що при $\beta = 0,5$ система характеризується підвищеною чутливістю до змін ризику, при $\beta = 1$ залежність є лінійною, а при $\beta = 2$ спостерігається консервативна реакція з різким зростанням інтенсивності захисту в зоні високих ризиків.

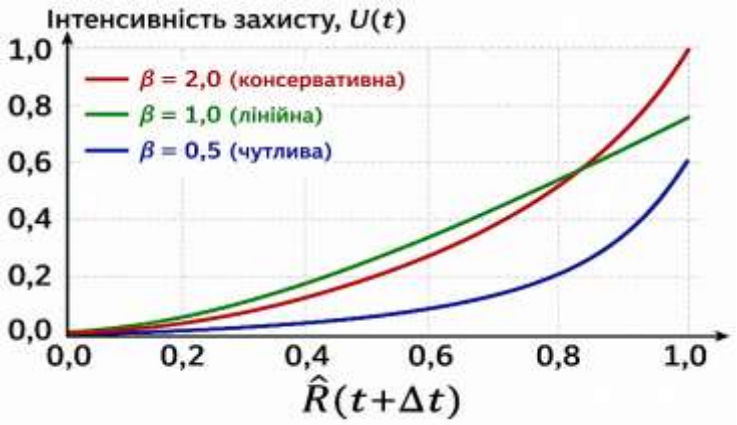

Рисунок 1 — Залежність інтенсивності криптографічного захисту від прогнозованого рівня ризику для різних значень параметра β

Це демонструє можливість адаптивного налаштування механізму криптографічного захисту залежно від умов функціонування системи.

3.4. Механізм вибору криптографічного алгоритму

Після того, як обчислено прогнозований ризик, визначено адаптивну ефективність алгоритмів і сформовано рівень інтенсивності захисту, необхідно перейти до процедури вибору конкретного криптографічного рішення. У статті пропонується розглядати множину доступних алгоритмів як сукупність класичних, гібридних і постквантових механізмів, кожен з яких може бути доцільним за певного значення ризику та обсягу доступних ресурсів.

Оптимальний криптографічний алгоритм пропонується визначати за критерієм максимуму ресурсно-адаптивної ефективності:

$$a^*(t) = \underset{a_i \in A}{arg\,max}\, E_{res}(a_i, t), \tag{9}$$

де $a^*(t)$ — оптимальний алгоритм у момент часу t, A — множина доступних криптографічних алгоритмів, $E_{res}(a_i, t)$ — ефективність алгоритму з урахуванням ризику і ресурсних можливостей. Формула (9) використовується як основне правило. Вона означає, що в кожний момент часу система обирає не просто найстійкіший або найшвидший алгоритм, а той,

який за сукупністю критеріїв і з урахуванням ризику є найбільш доцільним. У цьому і полягає ключова відмінність запропонованого методу від статичних підходів.

Однак для практичного впровадження часто доцільно не працювати з безперервними значеннями інтенсивності безпосередньо, а переводити їх у скінченну множину типових керувальних рішень. Саме для цього вводиться дискретизація інтенсивності захисту:

$$D(t) = \begin{cases} d_1, & \theta \le U(t) < \theta_1, \\ d_2, & \theta_1 \le U(t) < \theta_2, \\ d_3, & \theta_2 \le U(t) < \theta_3, \\ d_4, & \theta_3 \le U(t) \le 1, \end{cases} \tag{10}$$

де $D(t)$ — кінцеве керувальне рішення, d_1 — застосування класичних криптографічних алгоритмів, d_2 — посилений режим класичних алгоритмів або використання більш стійких конфігурацій, d_3 —застосування гібридних схем, d_4 — використання постквантових алгоритмів, θ_1, θ_2, θ_3 — порогові значення інтенсивності.

Формула (10) потрібна для перетворення теоретичної моделі в практично реалізований механізм прийняття рішень. Саме вона дозволяє системі переводити безперервний показник $U(t)$ у чітке управлінське правило: залишити поточний режим, посилити класичний захист, перейти до гібридного режиму або активувати постквантові механізми. Надалі ця формула використовується як основа реалізації програмного або політико-орієнтованого модуля керування криптографічним захистом.

3.5. Узагальнена модель керування криптографічним захистом

На завершальному етапі всі введені компоненти об’єднуються в єдину модель стану системи керування. Для цього пропонується описувати поточний стан механізму криптографічного захисту у вигляді вектора

$$S(t) = \left\langle \hat{R}(t + \Delta t), U(t), a^*(t), D(t) \right\rangle, \tag{11}$$

де $S(t)$ — узагальнений стан системи керування криптографічним захистом, $\hat{R}(t + \Delta t)$ — прогнозований ризик, $U(t)$ — інтенсивність криптографічного захисту, $a^*(t)$ — оптимальний алгоритм, $D(t)$ — дискретне керувальне рішення.

Формула (11) завершує побудову методу, оскільки інтегрує всі попередні результати в єдину логічну конструкцію. Вона показує, що система керування криптографічним захистом не зводиться лише до вибору конкретного алгоритму, а включає прогнозування ризику, формування інтенсивності реакції, оптимізаційний вибір засобу захисту та кінцеве управлінське рішення. Інакше кажучи, дана формула використовується як компактне представлення всього методу і може бути покладена в основу програмної реалізації, імітаційного моделювання або подальшої формалізації у вигляді автоматизованої системи підтримки прийняття рішень.

Отже, сформований механізм вибору криптографічного алгоритму забезпечує узгоджене функціонування всіх компонентів методу, включаючи оцінювання ризику, визначення інтенсивності захисту, оптимізаційний вибір алгоритму та формування кінцевого керувального рішення [7, 12]. Запропонований підхід дозволяє реалізувати адаптивне керування криптографічним захистом у режимі реального часу, забезпечуючи баланс між рівнем безпеки та витратами обчислювальних ресурсів [16, 17]. Це створює основу для побудови

інтелектуальних систем захисту, здатних ефективно реагувати на змінність кіберсередовища та забезпечувати стійкість комп'ютерних мереж до сучасних і перспективних загроз.

3.6. Обґрунтування отриманих наукових результатів

Отримані в роботі наукові результати полягають у тому, що запропоновано цілісний метод керування криптографічним захистом у комп'ютерних мережах, який поєднує ризик-орієнтоване оцінювання стану середовища з адаптивним вибором криптографічних алгоритмів. Наукова новизна підходу проявляється, по-перше, у введенні прогнозованого ризику як основи для керування криптографічним режимом, по-друге, у побудові адаптивної ефективності алгоритму, що поєднує властивості криптографічного механізму з ризиковим контекстом і ресурсними обмеженнями, а по-третє, у введенні функції інтенсивності криптографічного захисту як проміжної керувальної змінної між оцінкою ризику і конкретним рішенням щодо вибору механізму.

Практична значущість отриманих результатів полягає в тому, що розроблений метод дозволяє підвищити гнучкість криптографічного захисту в мережі. За низького рівня ризику система не перевантажується надмірно складними алгоритмами, а за зростання загроз своєчасно переходить до гібридних або постквантових механізмів. Це створює передумови для побудови адаптивної системи захисту, здатної ефективно реагувати на змінність кіберсередовища без необґрунтованого перевитрачання мережевих і обчислювальних ресурсів.

3.7. Функція інтегрального критерію вибору криптографічного алгоритму

Незважаючи на те, що у попередніх підрозділах було сформовано підхід до оцінювання ефективності криптографічних алгоритмів з урахуванням ризику та ресурсних обмежень, для забезпечення більш формалізованого та обґрунтованого процесу вибору доцільно перейти до використання узагальненого критерію оптимізації. Такий критерій повинен одночасно враховувати якісні характеристики алгоритму, рівень загрозового середовища та витрати, пов'язані з його застосуванням.

З цією метою вводиться інтегральна функція критерію вибору криптографічного алгоритму:

$$J(a_i, t) = \lambda_1 \cdot E(a_i) + \lambda_2 \cdot E(1 - \hat{R}(t + \Delta t)) - \lambda_3 \cdot Cost(a_i), \qquad (12)$$

де $J(a_i, t)$ — інтегральний критерій ефективності вибору алгоритму a_i у момент часу t, $E(a_i)$ — базова ефективність алгоритму, $\hat{R}(t + \Delta t)$ — прогнозований рівень ризику, $Cost(a_i)$ — витрати ресурсів на реалізацію алгоритму, $\lambda_1, \lambda_2, \lambda_3$ — вагові коефіцієнти, що визначають важливість відповідних складових.

Формула (12) вводиться для узгодження трьох ключових аспектів функціонування системи: ефективності криптографічного механізму, рівня ризику та витрат ресурсів [13]. На відміну від попередніх підходів, де ці параметри враховувалися окремо, дана формула забезпечує їх інтеграцію в єдину функцію оптимізації. Це дозволяє здійснювати більш точний вибір алгоритму, орієнтований не лише на максимізацію безпеки, але й на досягнення балансу між захищеністю та продуктивністю.

Складова $\lambda_1 \cdot E(a_i)$ відображає внесок базових характеристик алгоритму, як-то криптостійкість і швидкодія. Компонента $\lambda_2 \cdot E(1 - \hat{R}(t + \Delta t))$ забезпечує адаптацію до поточного рівня загроз: зі зростанням ризику її вплив зменшується, що стимулює вибір більш стійких алгоритмів. Від'ємна складова $\lambda_3 \cdot Cost(a_i)$ обмежує вибір надмірно ресурсоємних алгоритмів, що особливо важливо для систем з обмеженими ресурсами.

Отже, формула (12) використовується як основа для формування задачі оптимального вибору криптографічного алгоритму. Вона дозволяє перейти від евристичних правил до формалізованого критерію прийняття рішень, що підвищує обґрунтованість і відтворюваність результатів.

На рис. 2 представлено архітектуру методу керування криптографічним захистом у комп'ютерних мережах, яка поєднує процеси моніторингу кіберзагроз, оцінювання ризику, визначення інтенсивності захисту та адаптивного вибору криптографічних алгоритмів. Модель враховує інтенсивність загроз, рівень вразливостей і критичність інформаційних активів, а також обмеження обчислювальних ресурсів. Це забезпечує динамічний вибір між класичними, гібридними та постквантовими алгоритмами з урахуванням поточного стану системи. Запропонована архітектура реалізує замкнений контур керування, в якому результати оцінювання ризику безпосередньо впливають на вибір криптографічного механізму та рівень захисту.

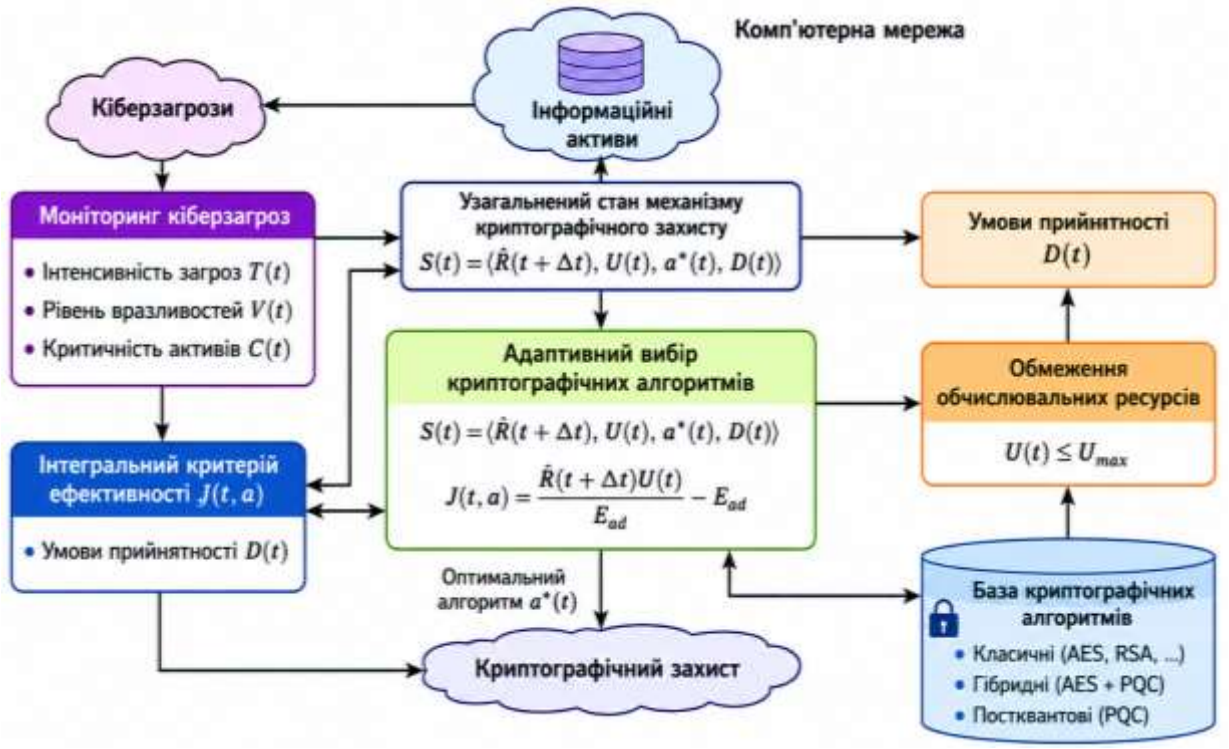

Рисунок 2 — Архітектура методу керування криптографічним захистом у комп'ютерних мережах

На основі введеного критерію оптимальний алгоритм визначається як

$$a^*(t) = \arg\max_{a_i \in A} J(a_i, t), \tag{13}$$

що означає вибір алгоритму, який забезпечує максимальне значення інтегрального критерію ефективності. Формула (13) використовується для реалізації процедури оптимального вибору криптографічного алгоритму на основі інтегрального критерію ефективності. Її застосування забезпечує автоматизоване прийняття рішення щодо вибору такого алгоритму, який за поточних умов функціонування системи забезпечує найкраще співвідношення між рівнем захищеності, прогнозованим ризиком та витратами обчислювальних ресурсів. Отже, дана формула є основою механізму адаптивного керування криптографічним захистом.

3.8. Модель обмежень на допустимі криптографічні рішення

У реальних умовах функціонування комп'ютерних мереж вибір криптографічного алгоритму обмежується не лише критеріями ефективності, а й технічними та ресурсними обмеженнями системи [5, 15]. До таких обмежень належать обчислювальні можливості вузлів, пропускна здатність каналів зв'язку, допустимі затримки обробки даних, а також енергетичні характеристики пристроїв [3, 24]. Особливо це актуально для середовищ з обмеженими ресурсами, як-то вбудовані системи або бездротові мережі.

З метою врахування зазначених обмежень вводиться множина допустимих криптографічних алгоритмів:

$$A_{adm}(t) = \{a_i \in A \mid Cost(a_i) \le Res(t)\}, \tag{14}$$

де $A_{adm}(t)$ — множина допустимих алгоритмів у момент часу t, $Cost(a_i)$ — витрати ресурсів для реалізації алгоритму a_i, $Res(t)$ — доступний обсяг ресурсів системи у момент часу t.

Формула (14) вводиться для відсікання алгоритмів, застосування яких є неможливим або недоцільним у поточних умовах. Наприклад, використання постквантових алгоритмів у системах із обмеженою обчислювальною потужністю може призводити до суттєвого зниження продуктивності або збільшення затримок передачі даних. У таких випадках алгоритми, що перевищують допустимий рівень ресурсоспоживання, виключаються з подальшого розгляду.

Отже, множина $A_{adm}(t)$ формує обмежений простір допустимих рішень, у межах якого здійснюється оптимізація. Це дозволяє враховувати реальні умови функціонування системи та забезпечує практичну реалізованість запропонованого методу.

З урахуванням введених обмежень задача вибору оптимального криптографічного алгоритму набуває вигляду

$$a^*(t) = \underset{a_i \in A_{adm}(t)}{arg\,max}\, J(a_i, t), \tag{15}$$

що означає вибір найефективнішого алгоритму серед тих, які задовольняють ресурсні обмеження системи.

Отже, введення обмежень на допустимі рішення дозволяє підвищити адекватність моделі та забезпечити її застосовність у реальних комп'ютерних мережах. У поєднанні з інтегральним критерієм ефективності це формує повноцінний механізм адаптивного керування криптографічним захистом, який враховує як рівень кіберзагроз, так і технічні можливості системи.

Імітаційне моделювання виконувалося для трьох типових сценаріїв функціонування комп'ютерної мережі, які відповідають низькому, середньому та високому рівням кіберризику. У межах кожного сценарію задавалися значення інтенсивності загроз, рівня вразливостей, критичності активів і доступних ресурсів системи, на основі яких обчислювалися нормований та прогнозований ризики, адаптивна ефективність криптографічних алгоритмів і значення інтегрального критерію вибору. Порівняння здійснювалося між статичним підходом, за якого алгоритм обирається наперед і не змінюється під час функціонування системи, та запропонованим адаптивним методом, який динамічно змінює криптографічне рішення залежно від зміни безпекового середовища.

Результати імітаційного моделювання показали, що запропонований метод забезпечує підвищення інтегрального показника ефективності криптографічного захисту в межах 15–18 % порівняно зі статичними підходами залежно від сценарію функціонування мережі. Кожний сценарій моделювання виконувався серією з $N = 20$ повторних запусків із варіюванням параметрів загрозового середовища та доступних ресурсів системи. Оцінювання

здійснювалося за інтегральним показником ефективності, що враховує рівень захищеності, затримку обробки даних та ресурсні витрати. Отримані результати наведено у табл. 1.

Таблиця 1 — Результати оцінювання ефективності запропонованого методу

Сценарій	Рівень ризику	Обраний алгоритм	Затримка (ms)	E_{stat}	E_{ad}	Приріст (%)	N
S1	Низький	AES	10	0,78	0,90	+15,4	20
S2	Середній	Hybrid	18	0,74	0,87	+17,6	20
S3	Високий	PQC	35	0,70	0,82	+17,1	20

У табл. 1 позначення E_{stat} відповідає інтегральному показнику ефективності за статичного підходу, тоді як E_{ad} характеризує ефективність запропонованого адаптивного методу з урахуванням динаміки ризику та ресурсних обмежень; позначення N відповідає кількості повторних запусків імітаційного моделювання для кожного сценарію.

Узагальнення результатів показало, що середній приріст інтегрального показника ефективності криптографічного захисту становив близько 16,7 %, при мінімальному значенні 15,4 % та максимальному — 17,6 % залежно від сценарію функціонування мережі. Отримані результати свідчать про стабільну тенденцію до підвищення ефективності адаптивного підходу порівняно зі статичними схемами вибору криптографічних алгоритмів.

Аналіз результатів, наведених у табл. 1, показує, що запропонований метод забезпечує стабільне підвищення ефективності криптографічного захисту у всіх розглянутих сценаріях. Найбільший приріст спостерігається в умовах середнього та високого рівнів ризику (сценарії S2–S3), де застосування адаптивного підходу дозволяє своєчасно переходити до більш стійких криптографічних механізмів.

На рис. 3 наведено порівняння інтегрального показника ефективності для статичного та адаптивного підходів у сценаріях S1–S3. Графік демонструє стабільне перевищення значень E_{ad} над E_{stat} у всіх розглянутих сценаріях, що свідчить про підвищення ефективності адаптивного підходу, особливо в умовах середнього та високого рівнів кіберризику. Отримані результати узгоджуються з даними табл. 1 та підтверджують доцільність використання динамічного вибору криптографічних алгоритмів залежно від стану безпекового середовища.

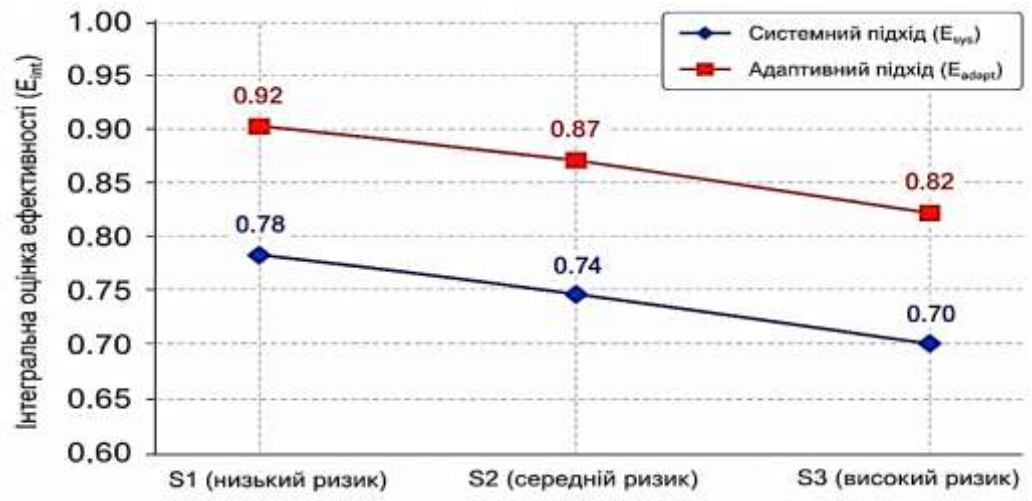

Рисунок 3 — Порівняння інтегрального показника ефективності для статичного та адаптивного підходів у сценаріях S1–S3

На рис. 4 наведено приклад урахування ресурсних обмежень під час вибору криптографічних алгоритмів у комп'ютерній мережі. Показано співвідношення між витратами ресурсів для реалізації класичних, гібридних і постквантових криптографічних механізмів та доступним обсягом ресурсів системи $Res(t)$. Заштрихована область відповідає алгоритмам, витрати яких перевищують допустимий рівень ресурсів системи. Це демонструє необхідність урахування ресурсного фактора під час адаптивного вибору криптографічних механізмів.

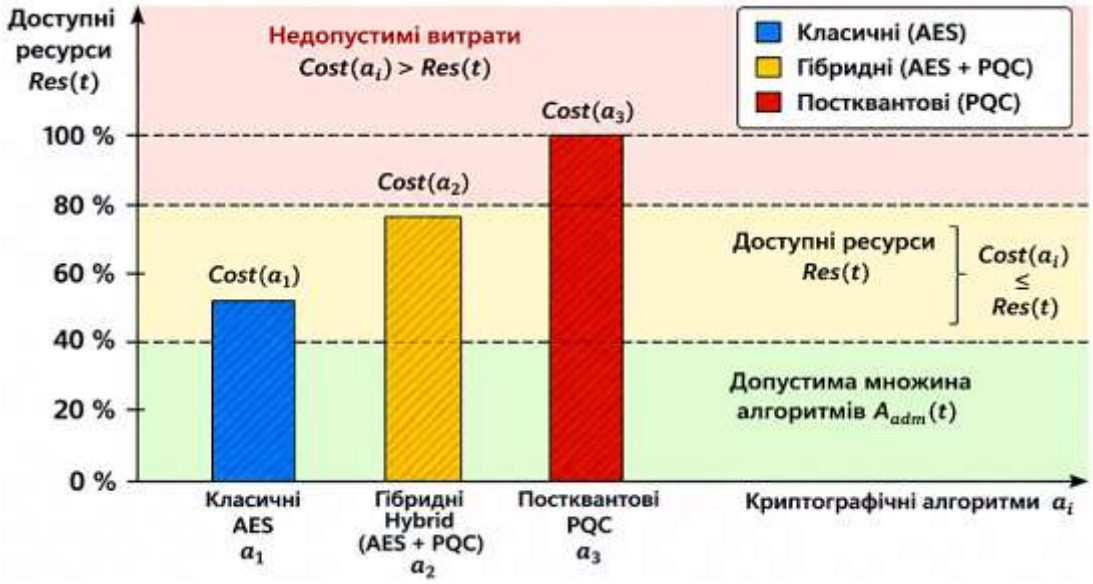

Рисунок 4 — Урахування ресурсних обмежень під час вибору криптографічних алгоритмів

Отже, результати моделювання свідчать про доцільність використання адаптивного вибору криптографічних алгоритмів залежно від поточного стану безпекового середовища та доступних ресурсів системи.

4. Обговорення

Отримані результати дослідження демонструють тенденцію до підвищення ефективності застосування адаптивного підходу до керування криптографічним захистом у комп'ютерних мережах, який базується на інтеграції динамічного оцінювання ризику та механізмі вибору криптографічних алгоритмів. На відміну від традиційних підходів, що передбачають використання фіксованого набору криптографічних засобів, запропонований метод забезпечує гнучке реагування на зміну умов функціонування системи, зокрема на зростання інтенсивності кіберзагроз, появу нових вразливостей та зміну критичності інформаційних активів.

На відміну від підходів [1, 4–6, 20–24], які орієнтовані переважно на оцінювання продуктивності або інтеграцію постквантових алгоритмів у мережеві протоколи, запропонований метод забезпечує інтеграцію трьох складових: динамічної оцінки ризику, ресурсно-орієнтованого обмеження та адаптивного вибору криптографічних алгоритмів у режимі реального часу, що узгоджується з сучасними концепціями адаптивного та контекстно-орієнтованого управління інформаційною безпекою [13, 16].

Однією з ключових переваг запропонованого підходу є використання прогнозованого рівня ризику як керувального параметра. Це дозволяє перейти від реактивного до проактивного управління криптографічним захистом, коли система не лише реагує на вже реалізовані загрози, а й враховує тенденції їх розвитку. У результаті підвищується своєчасність переходу до більш стійких криптографічних механізмів, зокрема постквантових алгоритмів, що є критично важливим в умовах динамічного кіберсередовища.

Важливим результатом є також формалізація інтегрального критерію вибору криптографічного алгоритму, який враховує не лише його криптографічну ефективність, але й рівень ризику та витрати ресурсів. Це дозволяє уникнути крайнощів, характерних для існуючих підходів, коли система або використовує надмірно складні алгоритми незалежно від рівня загроз, або, навпаки, застосовує недостатньо стійкі механізми в критичних умовах. Запропонований критерій забезпечує збалансований вибір, орієнтований на максимізацію ефективності захисту при допустимих витратах ресурсів.

На особливу увагу заслуговує введення функції інтенсивності криптографічного захисту, яка виступає проміжною ланкою між оцінкою ризику та конкретним управлінським рішенням. Такий підхід дозволяє перейти від жорстких порогових правил до більш гнучкого механізму керування, що узгоджується з використанням нечітких та адаптивних механізмів у криптографічних системах із динамічною довірою [25]. Це забезпечує підвищення стабільності системи та зменшення ймовірності різких змін у режимах її функціонування.

Порівняння запропонованого методу з існуючими дослідженнями у сфері постквантової криптографії показує, що більшість сучасних робіт зосереджена на оцінюванні продуктивності та порівняльному аналізі криптографічних алгоритмів, зокрема постквантових підписних схем [28], або їх інтеграції у мережеві протоколи, як-от TLS 1.3 чи 5G/6G інфраструктури. Водночас у них відсутній системний підхід до керування криптографічним захистом як динамічним процесом, що враховує змінність загрозового середовища. На відміну від таких підходів, запропонована модель дозволяє інтегрувати оцінювання ризику, аналіз ефективності та механізм прийняття рішень у єдину систему.

Результати дослідження також показують, що використання множини допустимих криптографічних рішень з урахуванням ресурсних обмежень дозволяє забезпечити практичну реалізованість методу. Це є важливим для застосування у середовищах з обмеженими ресурсами, зокрема в безпроводових мережах і мобільних середовищах, де особливості обміну ключами та автентифікації додатково впливають на вибір криптографічних механізмів [29]. Отже, запропонований підхід дозволяє адаптувати криптографічний захист не лише до рівня загроз, але й до технічних можливостей системи.

Загалом отримані результати свідчать про те, що запропонований метод формує нову концепцію керування криптографічним захистом у комп'ютерних мережах, яка базується на принципах адаптивності, ризик-орієнтованості та інтеграції постквантових криптографічних механізмів. Це дозволяє підвищити рівень захищеності інформаційних систем, забезпечити ефективне використання ресурсів та створити передумови для подальшого розвитку інтелектуальних систем захисту інформації.

Разом із тим запропонований метод має певні обмеження. Зокрема, у поданій версії дослідження оцінювання ефективності виконано на основі імітаційного моделювання з використанням узагальнених сценаріїв кіберзагроз, без прив'язки до конкретної виробничої мережевої інфраструктури та без урахування повного спектра прикладних параметрів реалізації постквантових алгоритмів у різних протоколах. Крім того, вагові коефіцієнти критеріїв ефективності та порогові значення інтенсивності захисту вимагають подальшого налаштування для конкретних класів мережевих систем. Це визначає доцільність наступного етапу досліджень, пов'язаного з експериментальною верифікацією моделі в реальному середовищі.

5. Висновки та перспективи подальших досліджень

У роботі вирішено актуальну науково-практичну задачу розроблення методу керування криптографічним захистом у комп'ютерних мережах на основі динамічної оцінки ризику та використання постквантових криптографічних алгоритмів. Запропонований підхід, на відміну

від існуючих, забезпечує адаптивний вибір криптографічних механізмів залежно від поточного та прогнозованого стану кіберсередовища, що дозволяє враховувати змінність інтенсивності загроз, рівня вразливостей і критичності інформаційних активів.

У межах дослідження розроблено математичну модель інтегрального оцінювання ризику, яка формує основу для прийняття рішень щодо рівня криптографічного захисту. Введення нормованого та прогнозованого ризиків дозволило перейти від статичного до динамічного аналізу безпекового стану системи. Запропоновано модель оцінювання ефективності криптографічних алгоритмів, яка враховує їх криптостійкість, продуктивність і ресурсоємність, а також адаптивний показник ефективності, що інтегрує вплив ризику на доцільність використання алгоритмів.

Розроблено механізм керування криптографічним захистом, який базується на використанні функції інтенсивності захисту та інтегрального критерію вибору криптографічного алгоритму. Це дозволило сформувати формалізовану задачу оптимізації, у межах якої здійснюється вибір найбільш ефективного алгоритму з урахуванням обмежень на доступні ресурси. Запропонований підхід забезпечує можливість динамічного переходу між класичними, гібридними та постквантовими криптографічними механізмами залежно від рівня ризику.

Отримані результати підтверджують наукову новизну запропонованого методу, яка полягає у поєднанні ризик-орієнтованого підходу з адаптивним вибором криптографічних алгоритмів, а також у введенні функції інтенсивності криптографічного захисту як керувальної змінної. Практична значущість дослідження полягає у можливості застосування методу для побудови адаптивних систем захисту інформації в комп’ютерних мережах підприємства, що дозволяє підвищити рівень захищеності та ефективність використання обчислювальних ресурсів.

Перспективи подальших досліджень полягають у розширенні запропонованої моделі шляхом інтеграції методів машинного навчання для прогнозування кіберзагроз та автоматизованого налаштування параметрів системи керування, зокрема вагових коефіцієнтів і порогових значень. Доцільним є також дослідження можливості впровадження запропонованого методу в середовищах з обмеженими ресурсами, як-от IoT-мережі та мобільні системи, а також проведення експериментального моделювання в реальних мережевих інфраструктурах. Подальший розвиток підходу може бути пов’язаний із побудовою інтелектуальних систем підтримки прийняття рішень у сфері керування криптографічним захистом та інтеграцією із сучасними архітектурами кібербезпеки, зокрема концепцією Zero Trust.

Отримані результати підтверджують наукову новизну та практичну значущість запропонованого методу, що дозволяє рекомендувати його для впровадження в сучасних інформаційно-інтелектуальних системах підприємства в умовах переходу до постквантової криптографії.

Дослідження проведено 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).

СПИСОК ДЖЕРЕЛ

1. Hasan K.F., Simpson L.R., Rezazadeh Baee M., Islam C., Rahman Z., Armstrong W., Gauravaram P., McKague M. A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies. *IEEE Access*. 2023. Vol. 12. P. 23427–23450.

2. Yesina M., Ostrianska Y.V., Gorbenko I.D. Status report on the third round of the NIST post-quantum cryptography standardization process. *Radiotekhnika*. 2022. P. 75–86. DOI: https://doi.org/10.30837/rt.2022.3.210.05.

3. Liu T., Ramachandran G.S., Jurdak R. Post-quantum cryptography for Internet of Things: A survey on performance and optimization. *arXiv*. 2024. URL: https://arxiv.org/abs/2401.17538 (дата звернення: 19.06.2026).
4. Näther C., Herzinger D., Gazdag S., Steghöfer J., Daum S., Loebenberger D. Migrating software systems toward post-quantum cryptography: A systematic literature review. *IEEE Access*. 2024. Vol. 12. P. 132107–132126.
5. Tasopoulos G., Dimopoulos C., Fournaris A., Zhao R.K., Sakzad A., Steinfeld R. Energy consumption evaluation of post-quantum TLS 1.3 for resource-constrained embedded devices. P. 366–374. DOI: https://doi.org/10.1145/3587135.3592821.
6. Scalise P., Garcia R., Boeding M., Hempel M., Sharif H. An applied analysis of securing 5G/6G core networks with post-quantum key encapsulation methods. *Electronics*. 2024. Vol. 13, N 21. Article 4258. DOI: https://doi.org/10.3390/electronics13214258.
7. Härting R.-C., Bueechl J., Anderlohr P., Betz L. The impact of effective risk management on the cyber performance of enterprises. *Procedia Computer Science*. 2025. Vol. 270. P. 4343–4352. DOI: https://doi.org/10.1016/j.procs.2025.09.559.
8. Костюк Ю., Складанний П., Мазур Н., Рзаєва С., Гнатченко Д., Гончаренко І. Формальна модель адаптивного вибору криптографічних параметрів захисту каналів у корпоративних комп'ютерних мережах на основі динамічної оцінки довіри. *Кібербезпека: освіта, наука, техніка*. 2026. Т. 4, № 32. С. 20–44. DOI: https://doi.org/10.28925/2663-4023.2026.32.1111.
9. Костюк Ю., Складанний П. Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. *Сучасний захист інформації*. 2026. Т. 1, № 65. С. 103–118. DOI: https://doi.org/10.31673/2409-7292.2026.011393.
10. Костюк Ю., Хорольська К., Бебешко Б., Довженко Н., Коршун Н., Пазинін А. Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. *Кібербезпека: освіта, наука, техніка*. 2025. Т. 4, № 28. С. 633–655. DOI: https://doi.org/10.28925/2663-4023.2025.28.857.
11. Довженко Н., Іваніченко Є., Костюк Ю. Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IoT-компонентами на основі графових моделей. *Кібербезпека: освіта, наука, техніка*. 2025. Т. 1, № 29. С. 762–776. DOI: https://doi.org/10.28925/2663-4023.2025.29.938.
12. Carannante M., Mazzoccoli A. An analytical review of cyber risk management by insurance companies: A mathematical perspective. *Risks*. 2025. Vol. 13, N 8. Article 144. DOI: https://doi.org/10.3390/risks13080144.
13. Mizrak F. Integrating cybersecurity risk management into strategic management: A comprehensive literature review. *Research Journal of Business and Management*. 2023. Vol. 10, N 3. P. 98–108. DOI: https://doi.org/10.17261/Pressacademia.2023.1807.
14. Костюк Ю., Бебешко Б., Гулак Г., Складанний П., Рзаєва С., Хорольська К. Забезпечення кібербезпеки та швидкодії передачі даних у безпровідних мережах. *Безпека інформації*. 2024. Т. 30, № 3. С. 365–375. DOI: https://doi.org/10.18372/2225-5036.30.20357.
15. Demir E., Bilgin B. E., Onbasli M. Performance analysis and industry deployment of post-quantum cryptography algorithms. 2025. DOI: https://doi.org/10.48550/arXiv.2503.1295.
16. Pise A.A., Singh S., Hemachandran K., Gadilkar S., Esther Z.B., Pise G.S., Imuede J. Adapting to evolving cyber threat landscapes with dynamic security protocol management in large-scale IoT sensor networks. *International Journal of Wireless & Ad Hoc Communication*. 2023. Vol. 7, N 2. P. 25–40.
17. Ashley C., Preiksaitis M. Strategic cybersecurity risk management practices for information in small and medium enterprises. *Business Management Research and Applications*. 2022. Vol. 1, N 2. P. 109–157.
18. Khan Q., Purification S., Chang S.-Y. Post-quantum key exchange and subscriber identity encryption in 5G using ML-KEM (Kyber). *Information*. 2025. Vol. 16, N. 7. Article 617. DOI: https://doi.org/10.3390/info16070617.
19. Pablos J.I., Vasco M.I. Secure post-quantum group key exchange: Implementing a solution based on Kyber. *IET Communications*. 2023. Vol. 17. P. 758–773. DOI: https://doi.org/10.1049/cmu2.12561.
20. Sosnowski M., Wiedner F., Hauser E., Steger L., Schoinianakis D., Gallenmüller S., Carle G. The performance of post-quantum TLS 1.3. P. 19–27. DOI: https://doi.org/10.1145/3624354.3630585.
21. Giron A.A., do Nascimento J.P.A., Custódio R., Perin L.P., Mateu V. Post-quantum hybrid KEMTLS performance in simulated and real network environments / Aly A., Tibouchi M. (eds.). *Progress in*

Cryptology — LATINCRYPT 2023. Vol. 14168. Cham: Springer, 2023. DOI: https://doi.org/10.1007/978-3-031-44469-2_15.
22. Astrizi T.L., Custódio R. Seamless transition to post-quantum TLS 1.3: A hybrid approach using identity-based encryption. *Sensors*. 2024. Vol. 24, N 22. Article 7300. DOI: https://doi.org/10.3390/s24227300.
23. Montenegro J., Rios R., López-Cerezo J. A performance evaluation framework for post-quantum TLS. *Future Generation Computer Systems*. 2025. Vol. 175. Article 108062. DOI: https://doi.org/10.1016/j.future.2025.108062.
24. Ojetunde B., Kurihara T., Yano K., Sakano T., Yokoyama H. A practical implementation of post-quantum cryptography for secure wireless communication. *Network*. 2025. Vol. 5, N 2. Article 20. DOI: https://doi.org/10.3390/network5020020.
25. Складанний П.М., Гулак Г.М., Костюк Ю.В. Генератор хаотичних чисел із нечітким керуванням для криптографічних систем із динамічною довірою. *Телекомунікаційні та інформаційні технології*. 2025. Т. 4, № 89. С. 137–147. DOI: https://doi.org/10.31673/2412-4338.2025.048916.
26. Костюк Ю., Складанний П., Рзаєва С., Мазур Н., Черевик В., Аносов А. Особливості реалізації мережевих атак через TCP/IP-протоколи. *Кібербезпека: освіта, наука, техніка*. 2025. Т. 1, № 29. С. 571–597. DOI: https://doi.org/10.28925/2663-4023.2025.29.915.
27. Складанний П., Костюк Ю., Рзаєва С. Безперервна оцінка доступу в Zero Trust Access Management на основі подієвих сигналів безпеки та динамічного керування сесіями. *Математичні машини і системи*. 2026. № 1. С. 29–46. DOI: https://doi.org/10.34121/1028-9763-2026-1-29-46.
28. Raavi M., Wuthier S., Chandramouli P., Balytskyi Y., Zhou X., Chang S.-Y. Security comparisons and performance analyses of post-quantum signature algorithms. *Applied Cryptography and Network Security*. Vol. 12727. Cham: Springer, 2021. DOI: https://doi.org/10.1007/978-3-030-78375-4_17.
29. Костюк Ю., Бебешко Б., Крючкова Л., Литвинов В., Оксанич І., Складанний П., Хорольська К. Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. *Кібербезпека: освіта, наука, техніка*. 2024. Т. 1, № 25. С. 229–252. DOI: https://doi.org/10.28925/2663-4023.2024.25.229252.

Стаття надійшла до редакції 12.06.2026 / прийнята до друку 13.08.2026