УДК 004.056.55:004.7 DOI: 10.31673/2412-4338.2026.029112

Складанний Павло Миколайович
кандидат технічних наук, доцент, завідувач кафедри інформаційної
та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Костюк Юлія Володимирівна
доктор філософії, доцент кафедри інформаційної
та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Соколов Володимир Юрійович
кандидат технічних наук, доцент, доцент кафедри інформаційної
та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

Кучаковська Галина Андріївна
кандидат педагогічних наук, старший викладач кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-4555-896X
h.kuchakovska@kubg.edu.ua

МОДЕЛЬ ДИНАМІЧНОГО ВИБОРУ ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ ІНТЕГРАЛЬНОЇ ОЦІНКИ РИЗИКУ ТА ЕФЕКТИВНОСТІ

Анотація. *У статті досліджено проблему забезпечення криптографічної стійкості інформаційно-комунікаційних систем в умовах зростання інтенсивності кіберзагроз та розвитку квантових обчислень, що знижують ефективність класичних криптографічних алгоритмів. Проведено аналіз сучасних підходів до застосування постквантових криптографічних алгоритмів, який показав їх переважно статичний характер використання без урахування динаміки зміни середовища функціонування, рівня ризику та параметрів атак. Обґрунтовано необхідність розроблення адаптивних механізмів вибору криптографічних алгоритмів, здатних забезпечити належний рівень захисту в умовах змінних загроз. Запропоновано модель динамічного вибору постквантових криптографічних алгоритмів на основі інтегральної оцінки ефективності та ризику, що дозволяє враховувати як технічні характеристики алгоритмів (швидкодію, криптостійкість, ресурсоємність), так і поточний стан безпеки системи. У межах моделі введено інтегральний показник ефективності та функцію ризику, яка формується з урахуванням рівня вразливостей, інтенсивності загроз і критичності інформаційних ресурсів. Реалізовано механізм адаптації, що забезпечує автоматичний перегляд та вибір оптимального алгоритму залежно від зміни ризику в реальному часі. Результати дослідження свідчать, що використання запропонованої моделі створює передумови для підвищення рівня криптографічного захисту, забезпечує формалізовану основу для адаптивного управління функціонуванням системи та дозволяє обґрунтовано здійснювати оптимізацію використання обчислювальних ресурсів. Отримані результати підтверджують наукову новизну та практичну доцільність впровадження адаптивних підходів до криптографічного захисту інформаційно-комунікаційних систем.*

Ключові слова: *постквантова криптографія, інформаційно-комунікаційні системи, криптографічний захист, інтегральна оцінка ризику, адаптивна модель, динамічний вибір алгоритмів, кібербезпека.*

Pavlo Skladannyi
PhD, Associate Professor, Head of the Department of
Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Костюк Юлія Володимирівна
PhD, Associate Professor of the Department of
Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

ORCID ID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Volodymyr Sokolov
PhD, Associate Professor, Associate Professor of the Department of
Information and Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-9349-7946
v.sokolov@kubg.edu.ua

Halyna Kuchakovska
PhD, Senior Lecturer of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-4555-896X
h.kuchakovska@kubg.edu.ua

MODEL OF DYNAMIC SELECTION OF POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS IN INFORMATION AND COMMUNICATION SYSTEMS BASED ON INTEGRATED RISK AND EFFICIENCY ASSESSMENT

Abstract. *The article investigates the problem of ensuring cryptographic stability of information and communication systems in the conditions of increasing intensity of cyber threats and development of quantum computing, which reduces the efficiency of classical cryptographic algorithms. An analysis of modern approaches to the application of post-quantum cryptographic algorithms was conducted, which showed their predominantly static nature of use without taking into account the dynamics of changes in the operating environment, risk level and attack parameters. The need to develop adaptive mechanisms for selecting cryptographic algorithms capable of providing an appropriate level of protection in conditions of changing threats was substantiated. A model for dynamic selection of post-quantum cryptographic algorithms based on an integral assessment of efficiency and risk is proposed, which allows taking into account both the technical characteristics of the algorithms (speed, cryptographic stability, resource intensity) and the current state of system security. An integral efficiency indicator and a risk function are introduced within the model, which are formed taking into account the level of vulnerabilities, threat intensity and criticality of information resources. An adaptation mechanism is implemented, which provides automatic review and selection of the optimal algorithm depending on the change in risk in real time. The results of the study indicate that the use of the proposed model creates the prerequisites for increasing the level of cryptographic protection, provides a formalized basis for adaptive management of the system's functioning, and allows for reasonable optimization of the use of computing resources. The results obtained confirm the scientific novelty and practical feasibility of implementing adaptive approaches to cryptographic protection of information and communication systems.*

Keywords: *post-quantum cryptography, information and communication systems, cryptographic protection, integral risk assessment, adaptive model, dynamic algorithm selection, cybersecurity.*

1. Вступ.

Стрімкий розвиток інформаційно-комунікаційних систем, зростання обсягів передавання та оброблення даних, а також підвищення складності кіберзагроз обумовлюють необхідність удосконалення методів забезпечення криптографічного захисту. Особливої актуальності ця проблема набуває в умовах розвитку квантових обчислень, які потенційно здатні порушити стійкість традиційних криптографічних алгоритмів, зокрема тих, що базуються на складності факторизації та дискретного логарифмування [1]. У зв’язку з цим значної уваги набуває впровадження постквантових криптографічних алгоритмів, які забезпечують стійкість до атак із використанням квантових комп’ютерів.

Разом із тим, аналіз існуючих підходів показує, що більшість сучасних систем криптографічного захисту використовують фіксований набір алгоритмів без урахування динаміки змін середовища функціонування, рівня загроз, вразливостей та критичності інформаційних ресурсів [2-3]. Такий підхід знижує ефективність захисту в умовах змінних кіберзагроз і не дозволяє своєчасно адаптувати криптографічні механізми до поточного стану безпеки системи [6]. Відсутність механізмів динамічного вибору криптографічних алгоритмів ускладнює забезпечення балансу між рівнем захисту та витратами обчислювальних ресурсів.

У цьому контексті актуальною науково-прикладною задачею є розроблення моделей та методів адаптивного управління криптографічним захистом інформаційно-комунікаційних систем, які забезпечують динамічний вибір алгоритмів залежно від поточного рівня ризику та умов функціонування [8-9]. Розв’язання цієї задачі безпосередньо пов’язане з підвищенням ефективності систем інформаційної безпеки, забезпеченням їх стійкості до сучасних і перспективних загроз, а також оптимізацією використання ресурсів.

Наукова новизна дослідження полягає у розробленні інтегрованої математичної моделі динамічного вибору постквантових криптографічних алгоритмів, у якій в єдиному контурі прийняття рішень поєднано оцінювання ризику компрометації системи, інтегральну функцію корисності алгоритму, критерій стабільності криптографічної політики та прогнозну умову адаптації. На відміну від існуючих підходів, де продуктивність алгоритмів, ризик і перехід до постквантових засобів розглядаються переважно окремо, запропонована модель забезпечує їх спільне врахування при адаптивному виборі алгоритму в реальному часі.

Теоретичне значення роботи полягає у розвитку методів формалізації процесів вибору криптографічних алгоритмів у складних інформаційно-комунікаційних системах із урахуванням динаміки ризику [8, 13].

Практичне значення отриманих результатів полягає у можливості їх використання для підвищення ефективності систем захисту інформації, зокрема при побудові адаптивних криптографічних підсистем, здатних автоматично реагувати на зміну кіберзагроз і забезпечувати необхідний рівень безпеки з мінімальними витратами ресурсів.

Метою дослідження є розроблення математичної моделі динамічного вибору постквантових криптографічних алгоритмів в інформаційно-комунікаційних системах на основі інтегральної оцінки ефективності та ризику, яка забезпечує адаптивне управління криптографічним захистом залежно від поточного стану безпеки середовища. Для досягнення поставленої мети передбачається формалізація множини доступних криптографічних алгоритмів та критеріїв їх оцінювання, розроблення інтегрального показника ефективності з урахуванням технічних характеристик алгоритмів, побудова моделі оцінювання ризику, що враховує рівень вразливостей, інтенсивність загроз і критичність інформаційних ресурсів, а також визначення механізму адаптації, який забезпечує автоматичний вибір оптимального криптографічного алгоритму в умовах динамічної зміни кіберзагроз. Додатково метою є обґрунтування доцільності застосування запропонованої моделі шляхом аналізу її ефективності та впливу на рівень захищеності інформаційно-комунікаційних систем і використання обчислювальних ресурсів.

2. Аналіз останніх досліджень і публікацій.

Упродовж останніх років проблема переходу до постквантової криптографії активно досліджується як у теоретичному, так і в прикладному аспектах. У роботі [1] узагальнено основні напрями розвитку постквантової криптографії, розглянуто ключові сімейства квантово-стійких алгоритмів та окреслено основні проблеми їх впровадження у сучасні інформаційно-комунікаційні системи. Дослідження [2] акцентує увагу на складності міграції прикладних систем до постквантових алгоритмів, підкреслюючи, що заміна криптографічних примітивів потребує комплексного врахування архітектурних та безпекових аспектів. Подібну проблематику розвинуто у роботі [3, 17], де запропоновано фреймворк переходу до постквантової криптографії на основі аналізу криптографічних залежностей і визначення пріоритетів заміни алгоритмів.

Окремий напрям досліджень становить оцінювання продуктивності постквантових алгоритмів у мережевих протоколах та інформаційно-комунікаційних системах. У праці [4] проведено порівняльний аналіз класичних і постквантових алгоритмів у протоколі TLS 1.3, що дозволило виявити суттєве зростання затримок та обсягів передавання даних при використанні постквантових криптографічних алгоритмів (Post-Quantum Cryptography, PQC). У роботі [5] досліджено можливість застосування постквантових алгоритмів у системах Інтернету речей, зокрема в e-health середовищах, де важливими є як криптографічна стійкість, так і обмежені ресурси пристроїв. Подальший розвиток цього напряму представлено у [6], де запропоновано фреймворк оцінювання ефективності постквантових і гібридних алгоритмів у TLS із урахуванням їх впливу на мережеві характеристики. У дослідженні [7, 23] показано, що для ресурсно-обмежених IoT-пристроїв доцільним є адаптивний підхід до вибору криптографічних алгоритмів залежно від умов функціонування, зокрема затримок, енергоспоживання та типу мережевого інтерфейсу. Додатково у [25, 26] підтверджено, що використання постквантових алгоритмів у TLS 1.3 може істотно впливати на часові характеристики з'єднань і потребує окремого аналізу продуктивності нових криптографічних стандартів.

Важливим напрямом є формування ризик-орієнтованих підходів до впровадження постквантової криптографії. У роботі [8] запропоновано модель оцінювання квантового ризику, яка дозволяє враховувати вплив майбутніх квантових загроз на криптографічну стійкість систем. У дослідженні [9, 15, 19] розглянуто стратегічні аспекти переходу підприємств до постквантових алгоритмів, включаючи часові горизонти, ризики та організаційні виклики. Дані роботи підтверджують необхідність поєднання технічних характеристик криптографічних алгоритмів із оцінюванням ризиків при їх впровадженні.

Разом з тим проведений аналіз показує, що існуючі дослідження переважно зосереджені на окремих аспектах проблеми, таких як огляд алгоритмів [1, 13, 21], питання міграції [2-3, 17] або експериментальне оцінювання їх продуктивності [4, 6-7, 25-26]. Незважаючи на наявність робіт, у яких розглядаються елементи адаптивності або ризик-орієнтованого підходу [7-8, 24], відсутні узагальнені формалізовані моделі, що забезпечують комплексний динамічний вибір постквантових криптографічних алгоритмів в інформаційно-комунікаційних системах. Зокрема, недостатньо дослідженими залишаються питання інтеграції технічних характеристик алгоритмів із поточним рівнем ризику, критичністю інформаційних ресурсів та умовами функціонування системи.

Для узагальнення результатів аналізу літературних джерел та виявлення ключових напрямів розвитку постквантової криптографії доцільно подати основні підходи у вигляді порівняльної табл. 1. Це дозволяє визначити їх переваги, обмеження та виявити відсутність комплексних моделей динамічного вибору алгоритмів з урахуванням ризику та ефективності.

Аналіз наведених у табл. 1 підходів дозволяє виділити основні тенденції розвитку постквантової криптографії. Зокрема, спостерігається перехід від статичних схем використання криптографічних алгоритмів до адаптивних моделей, орієнтованих на умови функціонування системи [7, 24]. Значна увага приділяється інтеграції постквантових алгоритмів у реальні інформаційно-комунікаційні системи, зокрема протоколи TLS та середовища Інтернету речей [4-7, 23], а також урахуванню ресурсних обмежень при їх застосуванні. Водночас активно розвиваються ризик-орієнтовані підходи, що враховують вплив квантових загроз на безпеку систем [8-9, 15]. Окрім цього, сучасні дослідження спрямовані на розвиток концепцій криптографічної гнучкості, використання гібридних схем [6, 11] та впровадження інтелектуальних методів адаптивного вибору

криптографічних алгоритмів. Зазначені тенденції підтверджують доцільність розроблення адаптивних моделей динамічного вибору криптографічних алгоритмів.

Таблиця 1

Порівняльний аналіз підходів до постквантової криптографії

Джерело	Основний внесок	Переваги	Обмеження
[1]	**Огляд напрямів PQC та сімейств алгоритмів**	**Систематизація підходів**	**Відсутність практичних моделей вибору**
[2]	Аналіз складності міграції до PQC	Врахування архітектурних аспектів	Відсутність адаптивності
[3]	Фреймворк переходу до PQC	Формалізація процесу міграції	Не враховано ризики в реальному часі
[4]	Аналіз PQC у TLS 1.3	Практичне оцінювання продуктивності	Не враховано адаптивний вибір
[5]	PQC для IoT (e-health)	Урахування ресурсних обмежень	Обмежена універсальність
[6]	Оцінювання ефективності PQC у TLS	Комплексний аналіз характеристик	Відсутність інтегрального критерію
[7]	Адаптивний вибір для IoT	Урахування середовища	Відсутність формалізованої моделі
[8]	Модель квантового ризику	Урахування загроз	Не інтегровано з характеристиками алгоритмів
[9]	Стратегії переходу підприємств	Організаційний аспект	Відсутність технічної реалізації

Крім того, у більшості існуючих підходів не враховується необхідність динамічної зміни криптографічної політики залежно від змін кіберзагроз, що може призводити до неефективного використання обчислювальних ресурсів або зниження рівня захищеності. Відсутність формалізованих механізмів адаптації та інтегральних критеріїв вибору алгоритмів обмежує можливість створення інтелектуальних систем криптографічного захисту.

У зв'язку з цим у статті вирішується науково-прикладна задача розроблення моделі динамічного вибору постквантових криптографічних алгоритмів в інформаційно-комунікаційних системах на основі інтегральної оцінки ризику та ефективності. Запропонований підхід спрямований на забезпечення адаптивного управління криптографічним захистом, що дозволяє автоматично змінювати використовувані алгоритми залежно від поточного стану системи, рівня загроз і доступних ресурсів, підвищуючи загальний рівень захищеності та ефективність функціонування інформаційно-комунікаційних систем.

3. Результати дослідження.

У сучасних інформаційно-комунікаційних системах забезпечення криптографічного захисту ускладнюється необхідністю одночасного врахування зростаючої інтенсивності кіберзагроз, розвитку квантових обчислень та обмеженості обчислювальних ресурсів [1, 19]. Використання постквантових криптографічних алгоритмів дозволяє підвищити стійкість до перспективних атак, однак їх ефективність значною мірою залежить від умов функціонування системи [26]. У зв'язку з цим виникає необхідність формалізації процесу вибору криптографічних алгоритмів як динамічної задачі, що враховує як технічні характеристики алгоритмів, так і поточний стан безпекового середовища.

Рис. 1 ілюструє архітектуру моделі динамічного вибору постквантових криптографічних алгоритмів, побудовану у вигляді багаторівневої системи. На рівні вхідних даних формується поточний стан системи та визначається множина доступних криптографічних алгоритмів. Далі, на рівні аналізу, виконується оцінювання ризику та обчислюється корисність кожного алгоритму з урахуванням його характеристик і умов функціонування. На рівні прийняття рішень ці показники інтегруються в єдиний критерій, на основі якого здійснюється вибір найбільш доцільного алгоритму. На завершальному рівні реалізації формується підсумкове рішення – обраний криптографічний алгоритм. Запропонована архітектура забезпечує адаптивний вибір алгоритмів залежно від поточного стану системи, рівня загроз і доступних ресурсів.

Запропонований підхід ґрунтується на представленні процесу вибору алгоритму як задачі оптимального керування, у якій рішення приймається на основі інтегрального критерію, що поєднує ефективність алгоритму, ризик компрометації системи та стабільність її функціонування [24]. Така постановка дозволяє перейти від статичних схем застосування криптографії до адаптивної моделі, здатної реагувати на зміну параметрів середовища у реальному часі.

З метою забезпечення формалізованого та обґрунтованого підходу до динамічного вибору криптографічних алгоритмів запропонована модель розглядається як послідовність взаємопов'язаних етапів, що відображають логіку функціонування адаптивної криптографічної підсистеми. На першому етапі здійснюється формування простору станів інформаційно-комунікаційної системи та визначення множини доступних постквантових криптографічних алгоритмів, що дозволяє врахувати як параметри середовища функціонування, так і технічні характеристики засобів захисту [13]. Другий етап передбачає оцінювання ризику компрометації

системи в реальному часі з урахуванням динаміки загроз, вразливостей і навантаження, що забезпечує актуалізацію рівня безпеки в кожен момент часу.

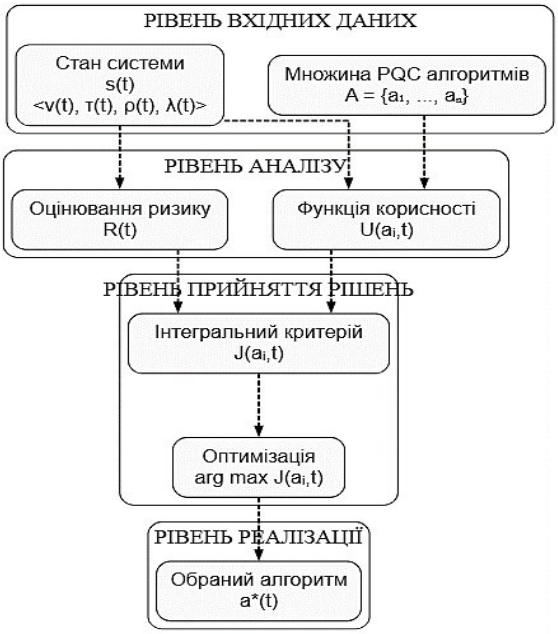

Рис. 1. Архітектура моделі динамічного вибору постквантових криптографічних алгоритмів

На третьому етапі формується інтегральна функція корисності криптографічних алгоритмів, яка узагальнює їх ефективність з урахуванням обчислювальних витрат і продуктивності. Четвертий етап полягає в інтеграції отриманих оцінок ефективності та ризику в єдиний критерій прийняття рішення, що дозволяє формалізувати компроміс між рівнем захисту та витратами ресурсів [8-9]. Завершальний етап передбачає реалізацію оптимізаційної процедури вибору криптографічного алгоритму з урахуванням стабільності функціонування системи та обмеження частоти змін криптографічної політики [24]. Така декомпозиція процесу забезпечує узгодженість між параметрами безпекового середовища, характеристиками алгоритмів і механізмом їх вибору, що є основою для побудови адаптивної моделі криптографічного захисту інформаційно-комунікаційних систем.

Рис. 2 відображає послідовність етапів динамічного вибору криптографічного алгоритму. На основі поточного стану системи виконується паралельне оцінювання ризику та корисності алгоритмів, після чого формується інтегральний критерій, здійснюється вибір алгоритму та перевіряється необхідність адаптації криптографічної політики.

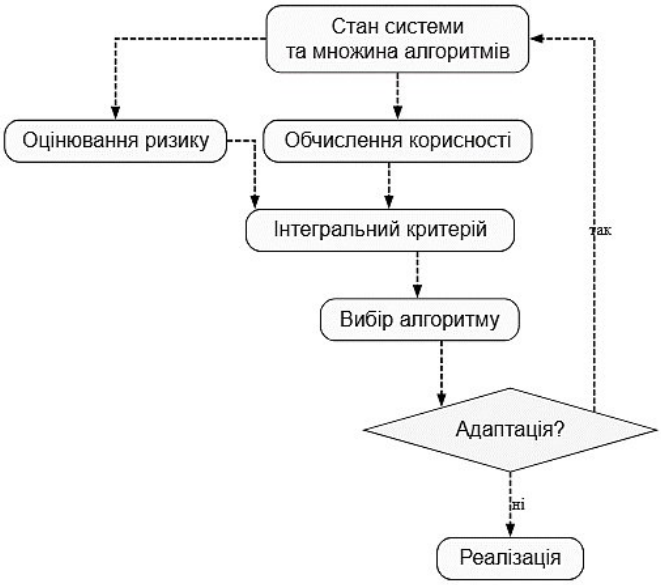

Рис. 2. Структурна схема процесу динамічного вибору криптографічних алгоритмів

Відповідно до поставленої задачі модель динамічного вибору постквантових криптографічних алгоритмів будується як адаптивна багатокритеріальна процедура, у межах якої в єдиному математичному контурі інтегруються поточний стан інформаційно-комунікаційної системи, імовірність компрометації, інтегральна корисність алгоритму, стабільність криптографічної політики та прогнозна умова адаптації. Такий підхід дозволяє формалізувати процес прийняття рішень щодо вибору криптографічного алгоритму в умовах динамічних кіберзагроз.

Формалізація простору станів та криптографічних рішень. Для побудови моделі введемо формалізований опис стану інформаційно-комунікаційної системи у момент часу t. Стан системи визначається вектором:

$$s(t) = \langle v(t), \tau(t), \rho(t), \lambda(t) \rangle, \tag{1}$$

де $v(t)$ характеризує рівень вразливостей системи, $\tau(t)$ – інтенсивність атак, $\rho(t)$ – доступні обчислювальні ресурси, $\lambda(t)$ – рівень навантаження [16]. Такий підхід дозволяє інтегрувати як внутрішні, так і зовнішні фактори, що впливають на безпеку системи.

Введення вектора стану системи $s(t)$ дозволяє перейти від статичного опису середовища до динамічної моделі, у якій кожен компонент прямо впливає на рівень ризику та вибір криптографічного алгоритму. Зокрема, зростання $v(t)$ та $\tau(t)$ підвищує ймовірність компрометації, тоді як параметри $\rho(t)$ і $\lambda(t)$ обмежують можливість використання ресурсоємних алгоритмів.

Обраний склад вектора стану не є довільним. Параметр $v(t)$ відображає структурну схильність системи до компрометації, $\tau(t)$ характеризує зовнішній дестабілізуючий вплив, $\rho(t)$ визначає допустимий клас обчислювально складних алгоритмів, а $\lambda(t)$ відображає експлуатаційне навантаження, яке впливає на допустиму затримку криптографічних операцій [8, 15]. Сукупно ці параметри формують мінімально достатній простір станів для прийняття рішень щодо вибору постквантового алгоритму в умовах динамічної зміни безпекових і ресурсних умов.

Множина доступних постквантових криптографічних алгоритмів задається як:

$$A = [a_1, a_2, \ldots, a_n], \tag{2}$$

де кожен алгоритм a_i описується набором характеристик:

$$x_i = \langle c_i, t_i, r_i, e_i \rangle, \tag{3}$$

де c_i відображає криптографічну стійкість алгоритму, t_i – час виконання, r_i – споживання обчислювальних ресурсів, e_i – енергоспоживання. Таким чином, кожен алгоритм розглядається як багатокритеріальний об'єкт, придатний до порівняння в умовах заданого стану системи. Значення параметрів x_i повинні визначатися з урахуванням конкретного контексту застосування алгоритму в інформаційно-комунікаційній системі. Для магістральних вузлів пріоритетними можуть бути криптостійкість і пропускна здатність, для мобільних або периферійних пристроїв – енергоспоживання та затримка, а для сервісів автентифікації – баланс між швидкістю виконання і стійкістю до перспективних атак. Це забезпечує прикладну придатність моделі до різних класів систем.

Таким чином, задача вибору алгоритму формалізується як відображення:

$$a^*(t) = \Phi(s(t), A), \tag{4}$$

де Φ – функція прийняття рішення, яка залежить від стану системи та характеристик алгоритмів. Саме побудова цієї функції становить основну задачу дослідження.

Модель оцінювання ризику з урахуванням динаміки середовища. Оцінювання ризику є ключовим елементом запропонованої моделі, оскільки саме ризик визначає доцільність застосування того чи іншого алгоритму. У загальному вигляді ризик розглядається як умовна ймовірність компрометації системи:

$$R(t) = P(compromise \mid s(t)), \tag{5}$$

Це означає, що ризик залежить від поточного стану системи, визначеного вектором $s(t)$.

На практиці значення $v(t)$ можуть визначатися на основі результатів сканування вразливостей, $\tau(t)$ – за телеметрією мережевих подій, частотою аномалій або спроб автентифікації, а $\lambda(t)$ – за

поточним рівнем навантаження на обчислювальну інфраструктуру. Коефіцієнти a_1, a_2, a_3 доцільно визначати експертним шляхом, методом аналізу ієрархій або на основі статистичного навчання за історичними даними інцидентів [16]. Такий підхід забезпечує адаптацію моделі до конкретної інформаційно-комунікаційної системи.

Для практичної реалізації використовується логістична функція:

$$R(t) = \frac{1}{1+e^{-(a_1 v(t) + a_2 \tau(t) + a_3 \lambda(t) + a_4 (1-p(t)))}}, \tag{6}$$

яка дозволяє врахувати нелінійний вплив параметрів середовища на ризик [8, 15]. Додавання складової $1 - p(t)$ дозволяє врахувати, що зменшення доступних ресурсів саме по собі підвищує операційний ризик, оскільки обмежує можливість використання криптографічно стійкіших, але ресурсоємних алгоритмів.

Рис. 3 відображає залежність рівня ризику від параметрів середовища з урахуванням різних сценаріїв функціонування системи та зон її станів. По горизонтальній осі відкладено узагальнені параметри середовища, а по вертикальній – рівень ризику. Графік поділено на чотири кольорові області S1–S4, які відповідають різним режимам роботи системи: від нормального стану до критичного. Зі збільшенням значень параметрів середовища спостерігається зростання рівня ризику. На графіку наведено чотири криві, що відповідають сценаріям S1–S4. Вони демонструють різну швидкість зростання ризику: у нормальному режимі ризик зростає повільно, тоді як у критичному – різко досягає високих значень. Пунктирна горизонтальна лінія відображає критичний рівень ризику, перевищення якого свідчить про необхідність адаптації системи. Таким чином, рисунок ілюструє, що вибір криптографічного алгоритму має здійснюватися з урахуванням як поточного рівня ризику, так і сценарію функціонування системи.

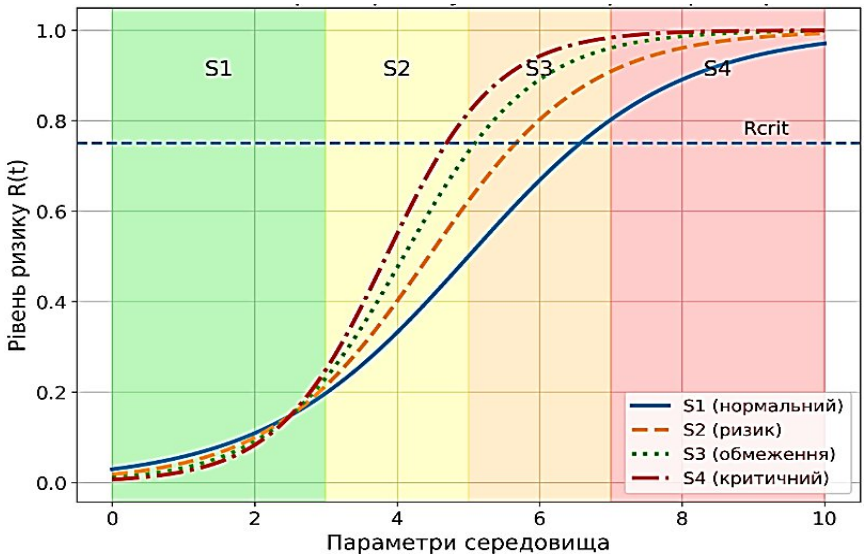

Рис. 3. Залежність рівня ризику $R(t)$ від параметрів середовища з виділенням режимів функціонування S1–S4

Зокрема, навіть незначне зростання інтенсивності атак або кількості вразливостей може призвести до суттєвого підвищення ризику [21-22]. Використання логістичної функції дозволяє інтерпретувати ризик як ймовірність переходу системи в небезпечний стан. При цьому значення $R(t)$ безпосередньо впливає на допустимий клас криптографічних алгоритмів: при високому ризику система повинна віддавати перевагу алгоритмам з максимальною криптостійкістю незалежно від їх ресурсної вартості.

Динаміка зміни ризику описується диференціальним рівнянням:

$$\frac{dR(t)}{dt} = \eta(\tau(t) - \theta R(t)), \tag{7}$$

яке відображає баланс між зростанням загроз та здатністю системи їх компенсувати. Таким чином, модель враховує не лише поточне значення ризику, а й тенденцію його зміни. Урахування похідної $\frac{dR(t)}{dt}$ дозволяє

врахувати не лише поточний стан, а й тенденцію розвитку загроз, що є принципово важливим для побудови проактивних механізмів захисту.

Формування інтегральної функції корисності алгоритмів. Для забезпечення обґрунтованого вибору криптографічного алгоритму вводиться функція корисності, яка узагальнює його переваги та витрати:

$$U(a_i,t) = w_1 c_i - w_2 t_i - w_3 r_i - w_4 e_i, \tag{8}$$

де коефіцієнти w_i визначають вагомість відповідних характеристик. Така форма дозволяє одночасно враховувати як позитивні (стійкість), так і негативні (затримки, ресурси) фактори. Запропонована функція корисності відрізняється від класичних підходів тим, що вона одночасно враховує як криптографічну стійкість алгоритму, так і витрати на його використання. [18, 23, 26] Це дозволяє формалізувати компроміс між безпекою та продуктивністю, що є критичним для інформаційно-комунікаційних систем реального часу.

У практичному застосуванні вагові коефіцієнти w_i, а також параметри $a_1 \dots a_4, k, \sigma, R_{crit}$, визначаються на основі поєднання експертного оцінювання, політики безпеки системи та статистичного аналізу журналів подій [16]. Зокрема, коефіцієнти w_i і $a_1 \dots a_4$ задають відносну важливість криптостійкості, затримки, ресурсоємності та енергоспоживання залежно від класу сервісу, параметр k визначає чутливість стохастичного механізму вибору, σ задає вагу прогнозної складової адаптації, а R_{crit} встановлюється відповідно до допустимого рівня ризику для конкретної інформаційно-комунікаційної системи.

Рис. 4 ілюструє процес формування інтегральної функції корисності криптографічних алгоритмів на основі врахування їх основних характеристик. Зокрема, показано вплив криптостійкості як позитивного фактора, а також витратних параметрів, таких як час виконання, використання ресурсів та енергоспоживання, які мають зростаючий характер. Інтегральна функція корисності формується як узагальнений показник, що відображає компроміс між рівнем захищеності та витратами. Зі збільшенням витрат значення корисності зменшується, що підтверджує необхідність балансування між ефективністю та безпекою. На графіку також позначено точку оптимуму, яка відповідає максимальному значенню корисності та визначає найбільш доцільний вибір криптографічного алгоритму за заданих умов.

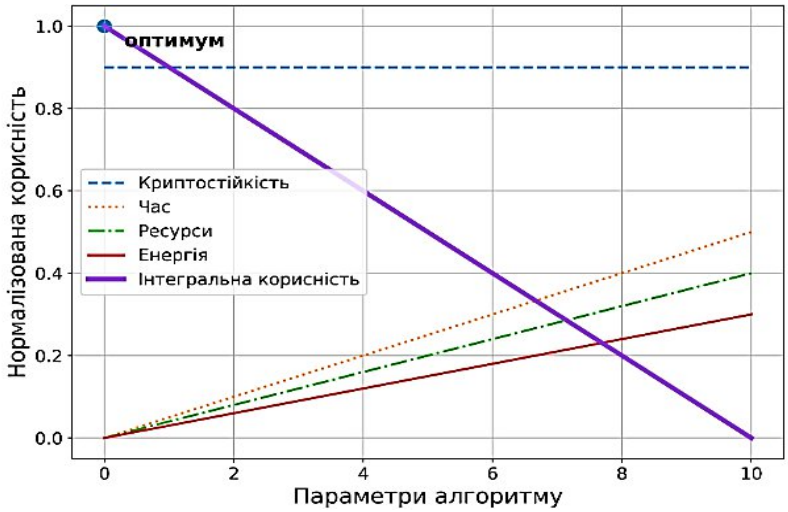

Рис. 4. Формування інтегральної функції корисності криптографічних алгоритмів

Вагові коефіцієнти w_i мають визначатися відповідно до типу захищуваного сервісу та політики безпеки системи. Для критичних інформаційних ресурсів доцільно збільшувати вагу криптостійкості w_1, тоді як для систем реального часу або ресурсно-обмежених вузлів більшої ваги набувають параметри затримки w_2, споживання ресурсів w_3 та енергоспоживання w_4 [14, 23]. Таким чином, функція корисності стає не універсальною абстракцією, а параметризованим інструментом адаптації криптографічної політики.

Для забезпечення порівнюваності значень використовується нормалізація:

$$\tilde{U}(a_i,t) = \frac{U(a_i,t) - U_{min}}{U_{max} - U_{min}}, \tag{9}$$

що переводить функцію корисності у діапазон [0,1]. Це дозволяє інтегрувати її з іншими показниками, зокрема ризиком. Нормалізація функції корисності забезпечує її сумісність із ризиковою складовою моделі, що дозволяє інтегрувати ці показники в єдиний критерій прийняття рішення.

Інтеграція ризику та ефективності у критерії вибору. Ключовим елементом моделі є формування інтегрального критерію, який поєднує ефективність алгоритму та ризик:

$$J\left(a_i,t\right) = \tilde{U}\left(a_i,t\right) \cdot (1 - R(t)) + k \cdot S\left(a_i,t\right), \tag{10}$$

Перший доданок відображає ефективність алгоритму з урахуванням ризику, тоді як другий враховує стабільність системи. Запропонований інтегральний критерій $J\left(a_i,t\right)$ є ключовим елементом моделі, оскільки він забезпечує одночасне врахування ефективності алгоритму, рівня ризику та стабільності системи [22-23]. На відміну від існуючих підходів, у яких ці фактори розглядаються окремо, у запропонованій моделі вони інтегруються в єдину функцію, що дозволяє формалізувати процес прийняття рішень.

Стабільність визначається як:

$$S\left(a_i,t\right) = e^{-D(a_i,a_{prev})}, \tag{11}$$

де $D(a_i,a_{prev})$ – метрика відмінності між алгоритмами за їх часовими, ресурсними та експлуатаційними характеристиками. Введення компоненти стабільності $S\left(a_i,t\right)$ дозволяє уникнути частих змін криптографічних алгоритмів [18, 20], що є важливим для забезпечення безперервності функціонування системи та зменшення накладних витрат.

Як метрику $D(a_i,a_{prev})$ доцільно використовувати зважену відстань між векторами характеристик x_i,x_{prev}, що дозволяє оцінити не символічну, а функціональну різницю між поточним і новим алгоритмом. Це усуває неоднозначність формули стабільності та робить її придатною до практичного застосування.

Оптимізаційна модель вибору алгоритму. Вибір алгоритму формулюється як задача:

$$a^*(t) = arg\,arg\,J\left(a_i,t\right) \ , \tag{12}$$

Це забезпечує вибір алгоритму з максимальною адаптивною ефективністю. Таким чином, вибір алгоритму формалізується як задача багатокритеріальної оптимізації, у якій враховуються як безпекові, так і ресурсні обмеження. Це дозволяє адаптувати криптографічну політику до поточного стану системи.

Перехід між алгоритмами описується:

$$P\left(a_j \to a_i\right) = \frac{e^{J\left(a_i,t\right)}}{\sum_{a^k \quad A} e^{J\left(a_k,t\right)}}, \tag{13}$$

що відповідає стохастичному механізму вибору (softmax) [11-12]. Використання стохастичного механізму вибору дозволяє уникнути різких змін алгоритмів і забезпечує більш плавну адаптацію системи, що є особливо важливим у розподілених інформаційно-комунікаційних системах.

Перед виконанням оптимізаційного вибору доцільно формувати допустиму підмножину алгоритмів $A_{adm}(t) \subseteq A$, яка враховує вимоги сумісності, нормативні обмеження, клас захищуваного сервісу та ресурсні обмеження вузла. У такому разі оптимізаційна процедура виконується не на всій множині A, а лише на множині допустимих рішень, що підвищує практичну коректність моделі.

Умова адаптації системи. Адаптація відбувається при:

$$R(t) + \sigma \frac{dR(t)}{dt} > R_{crit}, \tag{14}$$

де σ враховує швидкість зміни ризику. Це дозволяє системі реагувати на прогноз, а не лише на факт. Запропонована умова адаптації враховує як поточний рівень ризику, так і швидкість його зміни, що дозволяє реалізувати проактивний підхід до захисту [22]. А також означає, що система здатна змінювати криптографічний алгоритм до настання критичного стану, що суттєво підвищує її стійкість до атак.

Отже, сукупність співвідношень (1)–(14) утворює завершену математичну модель динамічного вибору постквантових криптографічних алгоритмів в інформаційно-комунікаційних системах, у якій стан середовища, ризик компрометації, інтегральна корисність алгоритмів, критерій стабільності та механізм адаптації об'єднані в єдиний контур прийняття рішень. Саме така інтеграція забезпечує можливість формування адаптивної криптографічної політики, орієнтованої на підтримання необхідного рівня безпеки за умов змінних кіберзагроз і ресурсних обмежень.

Апробація моделі на основі сценарного аналізу. Для перевірки працездатності запропонованої моделі динамічного вибору постквантових криптографічних алгоритмів проведено її апробацію на основі сценарного аналізу, який дозволяє оцінити поведінку системи в умовах різного рівня ризику та доступних обчислювальних ресурсів [18, 23]. У межах дослідження розглянуто чотири типові сценарії функціонування інформаційно-комунікаційної системи, що відображають характерні режими її роботи.

У сценарії S1 (нормальний режим) система характеризується низьким рівнем вразливостей і незначною інтенсивністю атак при достатньому обсязі обчислювальних ресурсів. У цьому випадку значення ризику $R(t)$ є мінімальним, що призводить до домінування складової ефективності у критерії $J\left(a_i,t\right)$. Як наслідок, модель

обирає алгоритми з високою продуктивністю та помірною криптостійкістю, що забезпечує оптимальне використання ресурсів без надлишкових витрат.

Сценарій S2 (підвищений ризик) відповідає умовам зростання інтенсивності атак або збільшення кількості вразливостей. У цьому випадку значення $R(t)$ зростає, що призводить до зменшення ваги ефективності в інтегральному критерії та зміщення вибору у бік більш стійких постквантових алгоритмів. При цьому модель зберігає баланс між безпекою та ресурсними витратами за рахунок використання нормалізованої функції корисності.

У сценарії S3 (ресурсні обмеження) система функціонує в умовах обмежених обчислювальних ресурсів або високого навантаження, що відображається зменшенням параметра $\rho(t)$ та зростанням $\lambda(t)$. Незважаючи на можливий середній рівень ризику, модель віддає перевагу алгоритмам із меншою ресурсоємністю, що дозволяє забезпечити стабільність функціонування системи. У цьому випадку вирішальну роль відіграє функція корисності $U(a_i,t)$, яка обмежує використання надто складних алгоритмів.

Сценарій S4 (критичний стан) відповідає одночасному зростанню ризику та швидкості його зміни, що визначається умовою $R(t) + \sigma\frac{dR(t)}{dt} > R_{crit}$. У цьому режимі модель переходить до проактивного захисту та обирає найбільш криптостійкі алгоритми незалежно від їх обчислювальної вартості [19, 21]. Це дозволяє мінімізувати ймовірність компрометації системи навіть за рахунок тимчасового зниження продуктивності.

Як видно з табл. 2, вибір криптографічного алгоритму визначається не лише рівнем ризику, але й доступними ресурсами, що підтверджує адаптивний характер запропонованої моделі.

Таблиця 2

Результати сценарного аналізу вибору криптографічних алгоритмів

Сценарій	Рівень ризику R(t)	Ресурси ρ(t)	Домінуючий фактор	Вибір алгоритму
S1 (нормальний)	низький	високі	ефективність	швидкі PQC алгоритми
S2 (ризик)	середній/високий	середні	безпека	більш стійкі алгоритми
S3 (ресурси)	середній	низькі	ресурси	легкі алгоритми
S4 (критичний)	високий	будь-які	ризик	максимально стійкі

Для мінімальної кількісної ілюстрації роботи моделі використано умовні нормалізовані характеристики окремих постквантових алгоритмів. Наведені в табл. 3 значення не є результатом прямого бенчмаркінгу конкретних реалізацій, а використовуються як нормалізована ілюстративна база для демонстрації роботи критерію вибору. За сценарію S1 перевагу отримують алгоритми з кращим співвідношенням продуктивності та стійкості, зокрема ML-KEM або Falcon. У сценарії S2 вибір зміщується до криптографічно стійкіших рішень. У сценарії S3 модель віддає перевагу менш ресурсоємним алгоритмам [12, 14]. У критичному сценарії S4 домінує вимога максимальної стійкості, внаслідок чого доцільним стає вибір Classic McEliece або Falcon залежно від допустимих ресурсних обмежень. Така ілюстрація підтверджує, що запропонований критерій забезпечує різний результат вибору залежно від поєднання ризику та доступних ресурсів.

Таблиця 3

Умовні нормалізовані характеристики алгоритмів для ілюстрації роботи моделі

Алгоритм	c_i криптостійкість	t_i затримка	r_i ресурсоємність	e_i енергоспоживання
ML-KEM	0.88	0.42	0.46	0.44
ML-DSA	0.91	0.57	0.61	0.58
Falcon	0.93	0.49	0.54	0.51
Classic McEliece	0.97	0.78	0.83	0.79

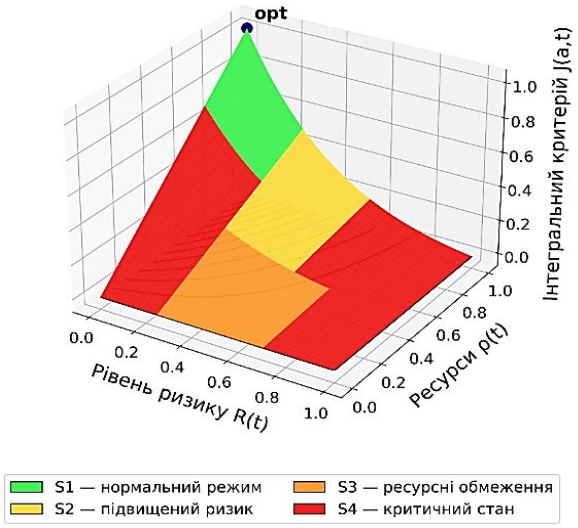

Рис. 5. Нелінійна модель адаптивного вибору постквантового криптографічного алгоритму залежно від рівня ризику та доступних ресурсів

Для візуалізації поведінки запропонованої моделі на рис. 5 представлено тривимірну залежність інтегрального критерію вибору криптографічного алгоритму від рівня ризику та доступних ресурсів системи. Запропонована поверхня має виражений нелінійний характер, що відображає складну взаємодію параметрів середовища. Максимальні значення критерію досягаються в області низького ризику та високих ресурсів, що відповідає оптимальному режиму функціонування системи. Зі зростанням ризику або зменшенням ресурсів спостерігається суттєве зниження значень критерію, що обумовлює зміну пріоритетів вибору криптографічних алгоритмів. Контурні лінії на базовій площині дозволяють додатково ідентифікувати області однакових значень критерію та межі переходу між режимами функціонування системи. Кольорове кодування поверхні відповідає характерним сценаріям S1–S4, що відображають різні режими роботи системи залежно від поєднання рівня ризику та доступних ресурсів.

Отримані результати свідчать, що запропонована модель формалізує механізм адаптивної зміни криптографічної політики залежно від умов функціонування системи, що підтверджує її ефективність для використання в інформаційно-комунікаційних системах із динамічним характером кіберзагроз.

Наведена апробація має характер сценарно-аналітичної валідації математичної моделі та не претендує на повномасштабне експериментальне порівняння реалізацій конкретних постквантових алгоритмів у реальному мережевому середовищі, що визначає напрями подальших досліджень.

Обговорення результатів та переваг підходу. Отримані результати свідчать про доцільність застосування інтегрованого підходу до вибору постквантових криптографічних алгоритмів, який поєднує оцінювання ефективності, рівня ризику та стабільності функціонування системи [22], що узгоджується із сучасними підходами до побудови адаптивних механізмів захисту в інформаційно-комунікаційних системах [10]. На відміну від традиційних підходів, у яких використовується фіксований набір криптографічних алгоритмів, запропонована модель формалізує механізм динамічної адаптації криптографічної політики відповідно до поточного стану інформаційно-комунікаційної системи.

На відміну від праць, орієнтованих переважно на оцінювання продуктивності постквантової криптографії (Post-Quantum Cryptography, PQC) у протоколах TLS або середовищах Інтернету речей, у запропонованій роботі акцент зроблено на формалізованому механізмі вибору криптографічного алгоритму. На відміну від підходів до міграції на постквантові алгоритми, де домінують стратегічні та архітектурні аспекти, у даній статті побудовано математичний критерій оперативного прийняття рішень у реальному часі. Такий підхід дозволяє перейти від статичних схем використання криптографічних засобів до адаптивної моделі, орієнтованої на динамічні умови функціонування системи.

Аналіз сценаріїв S1–S4 показав, що модель демонструє здатність адекватно реагувати на зміну параметрів середовища. У нормальному режимі функціонування (S1) система створює передумови для оптимізації використання ресурсів за рахунок вибору продуктивних алгоритмів, що підтверджує доцільність використання інтегральної функції корисності. У сценарії підвищеного ризику (S2) відбувається зміщення пріоритетів у бік криптографічної стійкості, що демонструє коректність інтеграції ризикової складової у критерій прийняття рішення та узгоджується з підходами до моделювання та управління ризиками інформаційної безпеки на основі когнітивних моделей [27]. У випадку ресурсних обмежень (S3) модель демонструє здатність забезпечувати працездатність системи шляхом вибору менш ресурсоємних алгоритмів, що підтверджує її практичну придатність для використання у гетерогенних середовищах. У критичному стані (S4) реалізується проактивний підхід до захисту, при якому вибір алгоритму визначається не лише поточним рівнем ризику, але й динамікою його зміни.

Важливою перевагою запропонованого підходу є інтеграція різнорідних факторів у єдиному математичному контурі прийняття рішень, що є критично важливим для сучасних інформаційно-комунікаційних систем. Це дозволяє уникнути ситуацій, коли вибір алгоритму базується лише на одному критерії, наприклад, криптостійкості або продуктивності, та формалізувати компроміс між безпекою та ефективністю.

Крім того, використання стохастичного механізму вибору алгоритмів забезпечує плавну адаптацію системи та зменшує ризик нестабільності, пов’язаної з частими змінами криптографічних механізмів [18, 20, 23]. Введення метрики стабільності дозволяє врахувати інерційність системи та створює передумови для зменшення накладних витрат на зміну алгоритмів.

Разом з тим, запропонований підхід має певні обмеження. Зокрема, ефективність моделі залежить від коректності оцінювання параметрів ризику та вагових коефіцієнтів у функції корисності. У реальних умовах це може потребувати використання додаткових методів машинного навчання або адаптивного налаштування параметрів. Подальші дослідження можуть бути спрямовані на автоматизацію процесу визначення вагових коефіцієнтів, розширення множини враховуваних факторів та інтеграцію моделі з системами моніторингу безпеки (SIEM, IDS/IPS).

Отримані результати узгоджуються із загальними підходами до побудови адаптивних механізмів захисту в інформаційно-комунікаційних системах, у яких ефективність забезпечується за рахунок інтеграції різнорідних факторів та динамічної зміни параметрів системи [10].

4. Висновки

У роботі розв'язано науково-прикладну задачу розроблення моделі динамічного вибору постквантових криптографічних алгоритмів в інформаційно-комунікаційних системах на основі інтегральної оцінки ефективності та ризику. Запропонований підхід дозволяє формалізувати процес вибору криптографічних засобів як задачу багатокритеріальної оптимізації, у якій враховуються технічні характеристики алгоритмів, параметри безпекового середовища та динаміка зміни кіберзагроз.

Наукова новизна отриманих результатів полягає у побудові інтегрованої математичної моделі, яка поєднує оцінювання ризику, функцію корисності криптографічних алгоритмів, критерій стабільності та механізм адаптації у єдиному контурі прийняття рішень. На відміну від існуючих підходів, запропонована модель забезпечує динамічну зміну криптографічної політики в реальному часі з урахуванням як поточного стану системи, так і тенденцій розвитку загроз.

Практичне значення отриманих результатів полягає у можливості використання моделі для побудови адаптивних криптографічних підсистем в інформаційно-комунікаційних системах різного призначення, зокрема в розподілених мережах, хмарних середовищах та системах Інтернету речей. Використання запропонованого підходу дозволяє формалізувати підходи до підвищення рівня захищеності інформаційних ресурсів, забезпечує основу для гнучкого управління функціонуванням системи та створює передумови для оптимізації використання обчислювальних ресурсів, забезпечити гнучкість функціонування системи та оптимізувати використання обчислювальних ресурсів.

Результати сценарного аналізу та наведеної кількісної ілюстрації підтвердили працездатність запропонованої моделі та її здатність адаптивно змінювати вибір криптографічних алгоритмів залежно від рівня ризику та доступних ресурсів. Отримані результати підтверджують наукову новизну й практичну доцільність запропонованого підходу на рівні математичної моделі та сценарної апробації і мають аналітико-модельний характер. Подальші дослідження доцільно спрямувати на експериментальну валідацію моделі для конкретних постквантових алгоритмів і мережевих протоколів.

Внесок авторів

Складанний П.М. здійснив концептуалізацію дослідження, сформулював наукову проблему та архітектуру моделі, а також виконав загальне наукове керівництво і редагування рукопису. Костюк Ю.В. розробила математичну модель, включаючи формалізацію простору станів, модель ризику, функцію корисності та оптимізаційний механізм вибору алгоритмів. Соколов В.Ю. виконав аналіз літературних джерел, підготував порівняльний аналіз існуючих підходів та забезпечив інтерпретацію результатів. Кучаковська Г.А. провела сценарну апробацію моделі, підготувала аналітичні таблиці та візуалізацію результатів, а також обґрунтувала практичне значення дослідження. Усі автори брали участь у підготовці тексту статті та погодили її остаточну версію.

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. Cherkaoui Dekkaki, K., Tasic, I., & Cano, M.-D. (2024). Exploring post-quantum cryptography: Review and directions for the transition process. *Technologies, 12*(12), 241. https://doi.org/10.3390/technologies12120241

2. Giron, A. A. (2023). Migrating applications to post-quantum cryptography: Beyond algorithm replacement. In *Proceedings of the 20th International Conference on Security and Cryptography*. https://doi.org/10.5220/0012138800003555

3. Hasan, F., Simpson, L., Rezazadeh Baee, M. A., Islam, C., Rahman, Z., Armstrong, W., Gauravaram, P., & McKague, M. (2024). A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3360412

4. Sosnowski, M., Wiedner, F., Hauser, E., Steger, L., Schoinianakis, D., Gallenmüller, S., & Carle, G. (2023). The performance of post-quantum TLS 1.3. In *Proceedings of the ACM Conference* (pp. 19–27). https://doi.org/10.1145/3624354.3630585

5. Mansoor, K., Afzal, M., Iqbal, W., Abbas, Y., Mussiraliyeva, S., & Chehri, A. (2024). PQCAIE: Post-quantum cryptographic authentication scheme for IoT-based e-health systems. *Internet of Things, 27*, 101228. https://doi.org/10.1016/j.iot.2024.101228

6. Montenegro, J., Rios, R., & López-Cerezo, J. (2025). A performance evaluation framework for post-quantum TLS. *Future Generation Computer Systems, 175*, 108062. https://doi.org/10.1016/j.future.2025.108062

7. Hanna, Y., Bozhko, J., Tonyalı, S., Harrilal-Parchment, R., Cebe, M., & Akkaya, K. (2025). A comprehensive and realistic performance evaluation of post-quantum security for consumer IoT devices. *Internet of Things, 33*, 101650. https://doi.org/10.1016/j.iot.2025.101650

8. Grigaliūnas, Š., & Brūzgienė, R. (2025). Towards a unified quantum risk assessment. *Electronics, 14*(17), 3338. https://doi.org/10.3390/electronics14173338

9. Campbell, R. (2026). Enterprise migration to post-quantum cryptography: Timeline analysis and strategic frameworks. *Computers, 15*(1), 9. https://doi.org/10.3390/computers15010009

10. Skladannyi, P., Kostiuk, Y., Rzaieva, S., Bebeshko, B., & Korshun, N. (2025). Adaptive methods for embedding digital watermarks to protect audio and video images in information and communication systems. In *Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography (CQPC 2025)*. *CEUR Workshop Proceedings, 4016*, 13–31.

11. Zafar, A., & Iqbal, S. S. (2025). Integrating code-based post-quantum cryptography into SSL/TLS protocols through an interoperable hybrid framework. *Discover Computing, 28*, 202. https://doi.org/10.1007/s10791-025-09735-7

12. Kostiuk, Y., Bebeshko, B., Kriuchkova, L., Lytvynov, V., Oksanych, I., Skladannyi, P., & Khorolska, K. (2024). Information protection and data exchange security 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

13. Hasib, S., Rasool, A., Gyanchandani, M., et al. (2026). A structured review of lattice-based attribute-based encryption methods for post-quantum security. *Discover Computing, 29*, 175. https://doi.org/10.1007/s10791-026-09965-3

14. Kostiuk, Y., Bebeshko, B., Hulak, H., Skladannyi, P., Rzaieva, S., & Khorolska, K. (2024). Ensuring cybersecurity and high-speed data transmission in wireless networks. *Information Security, 30*(3), 365–375. https://doi.org/10.18372/2225-5036.30.20357

15. Gupta, A., & Mittal, S. (2026). Post-quantum readiness and cryptographic transition planning for enterprise cloud. *Cybersecurity, 9*, 147. https://doi.org/10.1186/s42400-026-00579-2

16. Skladannyi, P., Kostiuk, Y., Rzaieva, S., Samoilenko, Y., & Savchenko, T. (2025). Development of modular neural networks for detecting different classes of network attacks. *Cybersecurity: Education, Science, Technique, 3*(27), 534–548. https://doi.org/10.28925/2663-4023.2025.27.772

17. Näther, C., Herzinger, D., Gazdag, S.-L., Steghöfer, J.-P., Daum, S., & Loebenberger, D. (2024). Migrating software systems towards post-quantum cryptography: A systematic literature review. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3450306

18. Skladannyi, P., Kostiuk, Y., Mazur, N., & Pitaichuk, M. (2025). Performance analysis of access protocols to cloud computing environments based on universal testing. *Telecommunications and Information Technologies, 1*(86), 61–74. https://doi.org/10.31673/2412-4338.2025.014649

19. Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., & Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature, 605*, 237–243. https://doi.org/10.1038/s41586-022-04623-2

20. Skladannyi, P., Hulak, H., & Kostiuk, Y. (2025). Chaotic number generator with fuzzy control for cryptographic systems with dynamic trust. *Telecommunications and Information Technologies, 4*(89), 137–147. https://doi.org/10.31673/2412-4338.2025.048916

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

22. Kostiuk, Y., Skladannyi, P., Mazur, N., Rzaieva, S., Hnatchenko, D., & Honcharenko, I. (2026). Formal model for adaptive selection of cryptographic parameters for secure communication channels in corporate computer networks based on dynamic trust evaluation. *Cybersecurity: Education, Science, Technique, 4*(32), 20–44. https://doi.org/10.28925/2663-4023.2026.32.1111

23. Liu, T., Ramachandran, G., & Jurdak, R. (2024). Post-quantum cryptography for Internet of Things: A survey on performance and optimization. *arXiv*. https://arxiv.org/abs/2401.17538

24. Skladannyi, P., Kostiuk, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). Model and methodology for forming adaptive security profiles for wireless network protection under dynamic cyber threats. In *Proceedings of the Workshop Cyber Security and Data Protection (CSDP 2025)*. *CEUR Workshop Proceedings, 4042*, 17–36.

25. Kampanakis, P., & Childs-Klein, W. (2024). The impact of data-heavy post-quantum TLS 1.3 on the time-to-last-byte of web connections. https://doi.org/10.14722/madweb.2024.23010

26. Souvatzidaki, K., & Limniotis, K. (2025). Post-quantum key exchange in TLS 1.3: Further analysis of the performance of new cryptographic standards. *Cryptography, 9*(4), 73. https://doi.org/10.3390/cryptography9040073

27. Shevchenko, S., Zhdanova, Y., & Harkushenko, A. (2025). Cognitive approach in information and cybersecurity. *Cybersecurity: Education, Science, Technique, 1*(29), 854–866. https://doi.org/10.28925/2663-4023.2025.29.945

Надійшла до редакції: 13.01.26
Прийнята до друку:12.06.26
Опубліковано:30.06.26