КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1339
УДК 004.056.55:004.8

Гулак Геннадій Миколайович
доктор технічних наук, професор
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID:0000-0001-9131-9233
h.hulak@kubg.edu.ua

Трофімов Олександр Сергійович
аспірант
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID:0009-0008-5760-7803
o.trofimov.asp@kubg.edu.ua

ФОРМУВАННЯ ТА ВДОСКОНАЛЕННЯ ПОЛІТИКИ УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ НА ОСНОВІ КОНЦЕПЦІЇ GROUNDED AI

Анотація. Статтю присвячено дослідженню проблем формування та вдосконалення політики управління криптографічними ключами в сучасних інформаційно-комунікаційних системах на основі концепції Grounded AI, яка забезпечує прийняття рішень із використанням перевірених даних, контекстної інформації та механізмів пояснюваності. Показано, що традиційні політики керування ключами, засновані на статичних правилах і фіксованих часових інтервалах ротації, не забезпечують необхідного рівня адаптивності в умовах динамічної зміни стану інформаційного середовища, характеристик користувачів, ресурсів і кіберзагроз. Розглянуто особливості застосування концепції Grounded AI для підтримки процесів генерації, розподілу, зберігання, використання, оновлення, відкликання та знищення криптографічних ключів із урахуванням поточного контексту функціонування системи. Досліджено фактори, що впливають на вибір політики управління ключами, зокрема рівень ризику, критичність інформаційних ресурсів, довіру до суб'єктів взаємодії, характеристики середовища виконання та вимоги нормативних документів. Запропоновано підхід до формування адаптивної політики управління криптографічними ключами, у якому рішення щодо життєвого циклу ключів приймаються на основі інтегрованого аналізу контекстних параметрів, оцінювання ризиків і результатів роботи моделей Grounded AI з можливістю обґрунтування прийнятих рішень. Розроблено концептуальну модель взаємодії компонентів політики, що поєднує модулі моніторингу, оцінювання контексту, аналізу ризиків, формування рекомендацій, пояснення рішень і реалізації керуючих дій. У заключному розділі обґрунтовано переваги запропонованого підходу, які полягають у підвищенні адаптивності, керованості, прозорості та обґрунтованості процесів управління криптографічними ключами, зменшенні ймовірності компрометації ключового матеріалу та підвищенні ефективності функціонування систем криптографічного захисту інформації. За результатами сценарного оцінювання точність прийняття рішень підвищено з 91,8 до 98,4 %, середній час формування керуючої дії зменшено з 214 до 132 мс, а інтегральну ефективність підвищено з 89,6 до 98,1 % порівняно зі статичною політикою.

Ключові слова: Grounded AI; управління криптографічними ключами; політика управління ключами; життєвий цикл криптографічних ключів; інформаційна безпека; кібербезпека; адаптивне управління; пояснюваний штучний інтелект.

ВСТУП

Стрімке зростання кількості кіберзагроз, розвиток хмарних обчислень, розподілених інформаційних систем, Інтернету речей, квантово-стійких криптографічних алгоритмів та технологій штучного інтелекту суттєво підвищують вимоги до ефективності управління криптографічними ключами [1-6, 16, 23-24]. Від правильності формування політики генерації, розподілу, зберігання, використання, ротації, відкликання та знищення криптографічних ключів безпосередньо залежать конфіденційність, цілісність, автентичність і доступність інформаційних ресурсів [21]. Водночас більшість існуючих

політик управління ключами ґрунтується на статичних правилах, попередньо визначених часових інтервалах ротації або фіксованих вимогах нормативних документів, що не дозволяє оперативно враховувати зміну контексту функціонування системи, рівня ризику, характеристик користувачів, стану інфраструктури та поточних кіберзагроз [9, 15, 17].

Одним із перспективних напрямів вирішення зазначеної проблеми є використання концепції Grounded AI, яка забезпечує прийняття рішень на основі перевірених джерел інформації, актуального контексту, фактів предметної області та механізмів пояснюваності [7-8, 10, 18, 20]. На відміну від традиційних моделей штучного інтелекту, Grounded AI дозволяє формувати рекомендації, що базуються не лише на результатах машинного навчання, а й на достовірних даних, політиках безпеки, нормативних вимогах та знаннях експертів [19, 22]. Це створює передумови для побудови адаптивної політики управління криптографічними ключами, здатної автоматично змінювати параметри життєвого циклу ключового матеріалу відповідно до поточного стану інформаційної системи.

Наукова новизна дослідження полягає у запропонованому підході до формування та вдосконалення політики управління криптографічними ключами на основі концепції Grounded AI, який інтегрує контекстну інформацію, оцінювання кіберризиків, правила політик безпеки та механізми пояснюваного штучного інтелекту для підтримки прийняття обґрунтованих рішень щодо життєвого циклу криптографічних ключів.

Теоретичне значення роботи полягає у розвитку наукових підходів до адаптивного управління криптографічними ключами шляхом поєднання концепції Grounded AI, контекстно-орієнтованого аналізу, ризик-орієнтованого управління та пояснюваного штучного інтелекту, що розширює методологічні засади побудови сучасних систем криптографічного захисту інформації.

Практичне значення одержаних результатів полягає у можливості використання запропонованого підходу під час розроблення та модернізації систем управління криптографічними ключами в корпоративних, хмарних, державних і критичних інформаційних системах для автоматизованого вибору політик ротації, відкликання, повторної генерації та контролю використання ключів залежно від поточного рівня ризику, контексту функціонування та вимог інформаційної безпеки.

Постановка проблеми. Ефективність криптографічного захисту інформації значною мірою визначається політикою управління криптографічними ключами, яка охоплює процеси їх генерації, розподілу, зберігання, використання, ротації, відкликання та знищення [11, 16]. В умовах динамічної зміни кіберзагроз, розвитку хмарних технологій, розподілених обчислень і сервісів штучного інтелекту традиційні статичні політики управління ключами не забезпечують достатньої адаптивності та своєчасного реагування на зміну контексту функціонування інформаційних систем [9, 22-23]. Це призводить до підвищення ризику компрометації ключового матеріалу, зниження ефективності механізмів криптографічного захисту та ускладнює виконання сучасних вимог інформаційної безпеки [3-5, 21, 24]. У зв'язку з цим актуальним науково-практичним завданням є розроблення адаптивної політики управління криптографічними ключами на основі концепції Grounded AI, яка забезпечує прийняття обґрунтованих рішень із використанням перевірених даних, контекстної інформації та механізмів пояснюваного штучного інтелекту [10].

Аналіз останніх досліджень і публікацій. Проблема застосування штучного інтелекту для підвищення ефективності криптографічного захисту та управління безпекою інформаційних систем активно досліджується у сучасних наукових працях. Водночас більшість наявних підходів зосереджена на вдосконаленні окремих криптографічних механізмів, виявленні кіберзагроз або оцінюванні ризиків, тоді як питання формування цілісної адаптивної політики управління криптографічними ключами залишається недостатньо розробленим.

У праці H. Taherdoost, T.-V. Le та K. Slimani [1] систематизовано основні напрями інтеграції криптографічних технологій і штучного інтелекту. Авторами визначено можливості використання інтелектуальних методів для оптимізації криптографічних алгоритмів, виявлення атак, аналізу вразливостей і підвищення ефективності захисту даних. Водночас дослідження має переважно оглядовий характер і не містить формалізованого підходу до адаптивного управління життєвим циклом криптографічних ключів.

P. Radanliev [2] досліджує взаємозв’язок між штучним інтелектом і квантовою криптографією. Показано, що алгоритми штучного інтелекту можуть застосовуватися для оптимізації процесів квантового розподілу ключів, аналізу параметрів каналів зв’язку та підвищення ефективності формування ключового матеріалу. Проте питання контекстно залежного вибору політик генерації, ротації, відкликання та знищення ключів у роботі окремо не розглядається.

G. Feretzakis, K. Papaspyridis, A. Gkoulalas-Divanis та V. S. Verykios [3] проаналізували технології збереження конфіденційності під час використання генеративного штучного інтелекту та великих мовних моделей. До таких технологій віднесено диференційну приватність, федеративне навчання,

гомоморфне шифрування та захищені багатосторонні обчислення. Дослідження підтверджує важливість поєднання інтелектуальних технологій із криптографічними засобами захисту, однак не визначає механізмів автоматичного формування та вдосконалення політик управління ключами на основі перевірених контекстних даних.

У роботі M. Elkhodr [4] запропоновано інтегровану систему забезпечення безпеки та конфіденційності Інтернету речей, що поєднує штучний інтелект, блокчейн і квантово-стійку криптографію. Штучний інтелект використовується для аналізу загроз, координації захисних механізмів і підтримки прийняття рішень. Водночас управління криптографічними ключами розглядається лише як складова загальної архітектури, а правила адаптивного управління окремими етапами життєвого циклу ключів не формалізовано.

A. Pallakonda та співавтори [5] розробили систему кіберзахисту промислових систем керування, яка інтегрує методи штучного інтелекту для виявлення атак із криптографічними механізмами захисту конфіденційності. Запропонований підхід спрямований на підвищення кіберстійкості промислової інфраструктури, однак основну увагу в ньому приділено виявленню вторгнень і захисту даних, а не формуванню адаптивної політики управління криптографічними ключами.

T. Swetha, U. Kumaran, V. P. Meena та I. A. Hameed [6] узагальнили можливості застосування штучного інтелекту для виявлення аномалій, поведінкового аналізу, прогнозування загроз та адаптивного реагування на кіберінциденти. Авторами наголошено, що традиційні засоби кіберзахисту недостатньо пристосовані до динамічної зміни характеристик атак. Проте в роботі не запропоновано моделі зв’язку між результатами інтелектуального аналізу та керуючими рішеннями щодо генерації, використання, ротації або відкликання криптографічних ключів.

S. Islam, N. Basheer, S. Papastergiou та співавтори [7] запропонували інтелектуальну систему динамічного управління кіберризиками, яка враховує контекст цифрової інфраструктури, характеристики активів, залежності між компонентами та наявні вразливості. Для забезпечення пояснюваності рішень авторами використано методи SHAP і LIME. Це дослідження створює важливе теоретичне підґрунтя для контекстного та пояснюваного управління безпекою, однак його результати безпосередньо не поширено на процеси управління криптографічними ключами.

L. Ofusori, T. Bokaba та S. Mhlongo [8] систематизували підходи до використання пояснюваного штучного інтелекту в кібербезпеці та обґрунтували необхідність забезпечення прозорості, інтерпретованості й підзвітності автоматизованих рішень. Авторами визначено обмеження сучасних XAI-рішень, пов’язані з якістю початкових даних, складністю інтерпретації моделей і можливістю їх застосування у режимі реального часу. Водночас у роботі не розглянуто формування рішень на основі спільного використання моделей штучного інтелекту, нормативних правил, експертних знань і перевірених контекстних даних.

Отже, аналіз останніх досліджень засвідчив, що сучасні наукові праці охоплюють використання штучного інтелекту у криптографії, квантовому розподілі ключів, забезпеченні конфіденційності, виявленні кіберзагроз, динамічному оцінюванні ризиків і поясненні автоматизованих рішень [12-14, 17-18, 20]. Проте раніше невирішеною частиною загальної проблеми залишається розроблення цілісного підходу до формування та безперервного вдосконалення політики управління криптографічними ключами, який поєднував би перевірені дані, контекст функціонування інформаційної системи, оцінки кіберризику, нормативні вимоги, експертні знання та пояснювані результати моделей штучного інтелекту. Недостатньо дослідженими залишаються також механізми обґрунтованого визначення строку дії ключів, ініціювання їх позапланової ротації, відкликання, повторної генерації та знищення [9-11, 15-19, 22]. Розв’язання зазначених завдань у статті пропонується здійснити на основі концепції Grounded AI.

Мета статті. Метою статті є розроблення адаптивного підходу до формування та вдосконалення політики управління криптографічними ключами на основі концепції Grounded AI, який забезпечує інтелектуальне прийняття рішень щодо управління життєвим циклом криптографічних ключів з урахуванням контексту функціонування інформаційної системи, рівня кіберризику, вимог політик безпеки та використання перевірених даних і механізмів пояснюваного штучного інтелекту.

Для досягнення поставленої мети у статті вирішуються такі завдання:

– проаналізувати сучасні підходи до управління криптографічними ключами та визначити їх основні обмеження;
– дослідити можливості застосування концепції Grounded AI для підтримки процесів управління життєвим циклом криптографічних ключів;
– визначити фактори, що впливають на формування адаптивної політики управління криптографічними ключами;
– розробити підхід до формування та вдосконалення політики управління криптографічними ключами на основі інтегрованого аналізу контексту, кіберризиків і перевірених даних;

– запропонувати концептуальну модель адаптивного управління криптографічними ключами з використанням механізмів пояснюваного штучного інтелекту;
– обґрунтувати переваги запропонованого підходу для підвищення ефективності та безпеки управління криптографічними ключами в сучасних інформаційно-комунікаційних системах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для реалізації інтелектуального управління життєвим циклом криптографічних ключів необхідно сформувати адаптивну політику, здатну враховувати поточний контекст функціонування інформаційної системи, рівень кіберризику та достовірність рішень, сформованих засобами штучного інтелекту [5-8, 23]. З цією метою запропоновано підхід до формування адаптивної політики управління криптографічними ключами на основі концепції Grounded AI.

Формування адаптивної політики управління криптографічними ключами на основі Grounded AI. Формування політики управління криптографічними ключами передбачає визначення правил їх генерації, розподілу, зберігання, використання, ротації, відкликання та знищення [15-16, 21]. Традиційні політики здебільшого ґрунтуються на попередньо встановлених строках дії ключів і статичних правилах реагування, що обмежує їх ефективність за динамічної зміни кіберзагроз, контексту доступу та стану інформаційної системи [22-23]. Для усунення зазначеного недоліку запропоновано формувати адаптивну політику управління криптографічними ключами на основі концепції Grounded AI.

Grounded AI у межах дослідження розглядається як підхід до прийняття інтелектуальних рішень, за якого результати моделей штучного інтелекту узгоджуються з перевіреними даними, нормативними вимогами, експертними правилами та поточним контекстом функціонування системи [10, 18, 20]. Це дає змогу зменшити ризик необґрунтованих рішень і забезпечити пояснюваність керуючих дій щодо життєвого циклу криптографічних ключів.

Джерелами обґрунтування рішень Grounded AI є актуальна телеметрія інформаційної системи, журнали операцій із ключами, результати виявлення аномалій, чинні політики інформаційної безпеки, нормативні вимоги та верифіковані експертні правила. [9, 13, 17] Для кожної рекомендації зберігаються її джерело, час актуалізації, контекст застосування та рівень достовірності. Рекомендація допускається до виконання лише за умови достатньої повноти даних, відсутності суперечностей із нормативними правилами та перевищення встановленого порогу обґрунтованості G_{min}. У протилежному випадку рішення передається адміністратору безпеки або виконується безпечна дія за замовчуванням.

Модель формування адаптивної політики подамо у вигляді:

$$P_K(t) = \langle C(t), R(t), G(t), \Omega_K(t), U_K(t) \rangle \tag{1}$$

де $P_K(t)$ – адаптивна політика управління криптографічними ключами в момент часу t, $C(t)$ – контекст функціонування інформаційної системи, $R(t)$ – поточний рівень кіберризику, $G(t)$ – рівень обґрунтованості рішення Grounded AI, $\Omega_K(t)$ – множина допустимих операцій із ключами, $U_K(t)$ – керуюче рішення щодо життєвого циклу ключа.

Для узагальнення результатів сценарного оцінювання використовується інтегральний показник ефективності, який враховує всі нормовані критерії оцінювання. Контекст функціонування системи формується на основі нормалізованих параметрів:

$$C(t) = \sum_{i=1}^{n} w_i x_i(t), \quad \sum_{i=1}^{n} w_i = 1, \quad w_i \geq 0 \tag{2}$$

де $x_i(t)$ – нормалізоване значення і-го контекстного параметра, w_i – його ваговий коефіцієнт, n – кількість параметрів. До таких параметрів належать критичність інформаційного ресурсу, рівень довіри до користувача або пристрою, місце та час доступу, стан мережі, інтенсивність аномальної активності, строк використання ключа та історія операцій із ним.

Для інтегрального оцінювання поточного рівня кіберризику запропоновано використовувати показник:

$$R(t) = \eta_1 A_n(t) + \eta_2 V(t) + \eta_3 C_r(t), \quad \eta_1 + \eta_2 + \eta_3 = 1 \tag{3}$$

де $A_n(t)$ – нормалізований рівень аномальної активності, $V(t)$ – рівень вразливості, $C_r(t)$ – критичність інформаційного ресурсу, η_i – вагові коефіцієнти. Значення складових нормуються в інтервалі [0;1], причому збільшення кожної складової відповідає зростанню кіберризику. Показник $R(t)$

використовується для визначення необхідності зміни чинної політики управління криптографічними ключами.

Обґрунтованість рекомендації Grounded AI визначається на основі достовірності вхідних даних, пояснюваності рішення, його відповідності експертним знанням і нормативним вимогам:

$$G(t) = \lambda_1 D_v(t) + \lambda_2 E_x(t) + \lambda_3 K_e(t) + \lambda_4 N_r(t), \quad \sum_{j=1}^{4} \lambda_j = 1 \tag{4}$$

де $D_v(t)$ – достовірність вхідних даних, $E_x(t)$ – пояснюваність рішення моделі, $K_e(t)$ – відповідність експертним знанням і правилам безпеки, $N_r(t)$ – відповідність нормативним вимогам, λ_j – вагові коефіцієнти. Значення $G(t)$ характеризує рівень обґрунтованості сформованої рекомендації: що вищим є цей показник, то більшою є допустимість її використання для автоматичного формування керуючої дії.

Рис. 1 відображає структурну схему формування адаптивної політики управління криптографічними ключами на основі Grounded AI. Схема охоплює етапи формування контексту, оцінювання кіберризику, інтелектуального аналізу, перевірки нормативних вимог, формування політики та прийняття керуючих рішень із подальшим виконанням операцій над криптографічними ключами і зворотним зв'язком для актуалізації знань та вдосконалення політики.

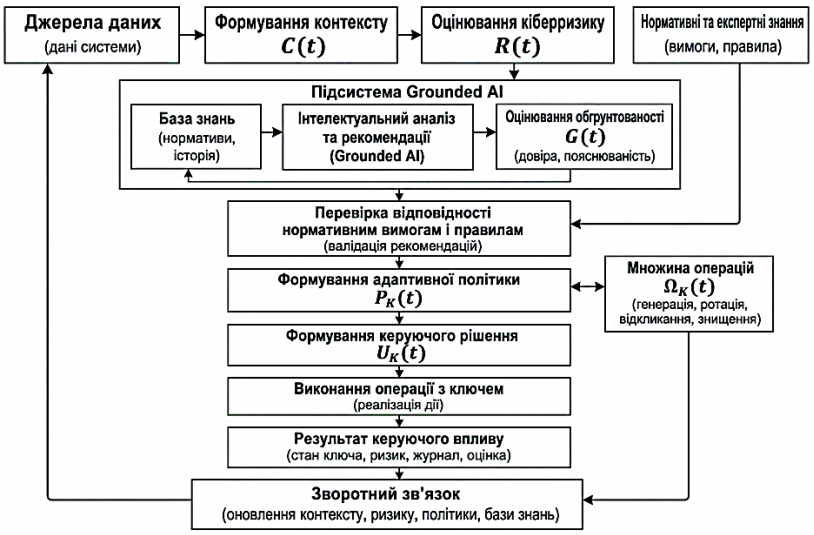

Рис. 1. Структурна схема формування адаптивної політики управління криптографічними ключами на основі Grounded AI

Керуюче рішення може передбачати збереження поточного ключа, планову або позапланову ротацію, призупинення використання, відкликання, повторну генерацію чи знищення ключового матеріалу [15-16, 21]. На відміну від статичної політики, запропонована модель враховує одночасну зміну контексту, кіберризику та достовірності інтелектуального рішення. Науковий результат полягає у формалізації адаптивної політики як замкненого контуру управління, в якому рішення Grounded AI перевіряються на відповідність фактичним даним, експертним знанням і нормативним вимогам перед їх застосуванням до криптографічних ключів.

Модель оцінювання контексту та рівня довіри.

Одним із ключових етапів формування адаптивної політики управління криптографічними ключами є оцінювання поточного контексту функціонування інформаційної системи та рівня довіри до сформованого рішення [13, 17]. На відміну від традиційних підходів, які враховують лише окремі характеристики користувача або пристрою, запропонована модель інтегрує параметри середовища функціонування, стану криптографічного ключа, рівня кіберризику, достовірності вхідних даних і пояснюваності результатів Grounded AI [10, 18-19]. Це забезпечує більш обґрунтований вибір керуючої дії щодо життєвого циклу криптографічного ключа.

Контекст функціонування інформаційної системи описується вектором:

$$\mathbf{C}(t) = \langle U_u(t), D_d(t), N_e(t), C_r(t), S_K(t), A_n(t) \rangle \tag{5}$$

де $C(t)$ – вектор контексту, $U_u(t)$ – довіра до користувача, $D_d(t)$ – довіра до пристрою, $N_e(t)$ – стан мережевого середовища, $C_r(t)$ – критичність інформаційного ресурсу, $S_K(t)$ – стан криптографічного ключа, $A_n(t)$ – аномальна активність.

Для інтегрального оцінювання контексту запропоновано використовувати вираз:

$$Q_C(t) = \sum_{i=1}^{6} \omega_i c_i(t), \quad \sum_{i=1}^{6} \omega_i = 1, \quad \omega_i \geq 0, \tag{6}$$

де $Q_C(t)$ – інтегральний показник контексту, $c_i(t)$ – нормалізоване значення відповідного параметра контексту, ω_i – ваговий коефіцієнт параметра. Вагові коефіцієнти визначаються експертним шляхом або можуть адаптивно змінюватися залежно від класу інформаційної системи та рівня її критичності.

Рівень довіри до рішення Grounded AI визначається як:

$$T(t) = \alpha Q_C(t) + \beta D_v(t) + \gamma E_x(t) + \delta P_r(t), \quad \alpha + \beta + \gamma + \delta = 1 \tag{7}$$

де $T(t)$ – інтегральний рівень довіри, $Q_C(t)$ – інтегральна оцінка контексту, $D_v(t)$ – показник достовірності вхідних даних, $E_x(t)$ – показник пояснюваності рішення Grounded AI, $P_r(t)$ – рівень відповідності рішення нормативним вимогам і політикам безпеки, $\alpha, \beta, \gamma, \delta$ – вагові коефіцієнти.

Чим більшим є значення $T(t)$, тим вищою є обґрунтованість автоматичного виконання операцій генерації, ротації, відкликання або знищення криптографічних ключів. Якщо значення показника є нижчим за встановлений поріг, сформоване рішення передається на додаткову перевірку або потребує підтвердження адміністратора безпеки.

Запропонована модель забезпечує комплексне оцінювання контексту та рівня довіри шляхом інтеграції технічних, поведінкових, мережевих і нормативних факторів. На відміну від існуючих підходів, вона дозволяє використовувати результати Grounded AI лише після перевірки їх достовірності, пояснюваності та відповідності політикам безпеки, що підвищує обґрунтованість прийняття рішень щодо управління криптографічними ключами.

Метод прийняття рішень щодо життєвого циклу криптографічних ключів.

Запропонована модель оцінювання контексту та рівня довіри є основою адаптивного керування життєвим циклом криптографічних ключів. На відміну від традиційних політик, у яких операції генерації, ротації та відкликання виконуються за фіксованими часовими інтервалами, запропонований метод враховує поточний контекст функціонування інформаційної системи, рівень кіберризику, стан криптографічного ключа та достовірність сформованого рішення Grounded AI [10, 15-16, 18]. Це забезпечує своєчасну зміну політики управління ключами відповідно до поточної ситуації.

Перед агрегуванням усі параметри контексту приводяться до єдиної орієнтації: значення 1 відповідає найбільш сприятливому та довіреному стану, а значення 0 – критичному або недовіреному. Для негативно орієнтованих показників, зокрема аномальної активності та мережевого ризику, використовується інверсне нормування [9, 17, 23]. Для визначення необхідності виконання керуючої дії вводиться інтегральний показник пріоритетності:

$$I_K(t) = \alpha R(t) + \beta\big(1 - Q_C(t)\big) + \gamma\big(1 - T(t)\big), \quad \alpha + \beta + \gamma = 1 \tag{8}$$

де $I_K(t)$ – інтегральний показник пріоритетності зміни життєвого циклу ключа, $R(t)$ – рівень кіберризику, $Q_C(t)$ – інтегральна оцінка контексту, $T(t)$ – рівень довіри до рішення Grounded AI, α, β, γ – вагові коефіцієнти. Чим більше значення $I_K(t)$, тим вищою є необхідність зміни поточної політики управління криптографічними ключами та виконання відповідної керуючої дії. Якщо значення показника перевищує порогове I_{min}, система переходить до вибору оптимальної операції над ключем, інакше поточна політика залишається без змін.

Для кожної допустимої операції над криптографічним ключем визначається функція ефективності:

$$F_i(t) = \mu_1 S_i(t) + \mu_2 T(t) + \mu_3 Q_C(t) - \mu_4 C_i(t), \quad \sum_{j=1}^{4} \mu_j = 1 \tag{9}$$

де $F_i(t)$ – інтегральна ефективність і-ї операції, $S_i(t)$ – очікуване підвищення рівня захищеності після виконання операції, $T(t)$ – рівень довіри, $Q_C(t)$ – інтегральна оцінка контексту, $C_i(t)$ – витрати на виконання відповідної операції, μ_j – вагові коефіцієнти. Чим більше значення $F_i(t)$, тим доцільнішим є

виконання відповідної операції з урахуванням очікуваного рівня захищеності, поточного контексту, довіри та пов'язаних витрат. Оптимальною вважається операція, для якої значення $F_i(t)$ є максимальним, після чого вона виконується та її результат використовується для оновлення бази знань Grounded AI.

Оптимальна операція вибирається за правилом:

$$u^*(t) = \begin{cases} u_{keep}, & I_K(t) < I_{min}, \\ arg \max\limits_{u_i \in \Omega_K(t)} F_i(t), & I_K(t) \geq I_{min}, \end{cases} \quad (10)$$

де $u^*(t)$ – оптимальна керуюча дія, $\Omega_K(t)$ – множина допустимих операцій над криптографічним ключем, I_{min} – порогове значення інтегрального показника, після перевищення якого виконується зміна поточної політики. Залежно від етапу життєвого циклу множина $\Omega_K(t)$ також може включати вибір способу безпечного розподілу ключа, зміну сховища або рівня захисту ключового матеріалу, обмеження області його використання, призначення строку дії, резервне копіювання, відновлення та контроль доступу. Допустимість таких операцій визначається типом ключа, його призначенням, критичністю захищуваного ресурсу та нормативними вимогами.

Множина допустимих операцій включає: генерацію нового ключа; продовження використання поточного ключа; ротацію ключа; тимчасове блокування; відкликання ключа; знищення ключового матеріалу.

Якщо значення $I_K(t)$ не перевищує порогового рівня, система продовжує використання поточного ключа. У разі перевищення порогу формується множина можливих керуючих дій, для кожної з яких обчислюється показник ефективності $F_i(t)$. Остаточне рішення приймається шляхом вибору альтернативи з максимальним значенням цього показника.

Алгоритм роботи методу:

1. Збір і перевірка контекстних даних про користувача, пристрій, мережу та криптографічний ключ.
2. Формування контексту та обчислення показників $Q_C(t), T(t), I_K(t)$.
3. Оцінювання кіберризику та перевірка умови $I_K(t) \geq I_{min}$.
4. Якщо умова не виконується, політика залишається без змін.
5. Якщо умова виконується, формується множина допустимих операцій, для яких обчислюється функція ефективності $F_i(t)$.
6. Виконується операція з максимальним значенням $F_i(t)$, а результат використовується для оновлення бази знань Grounded AI.

На рис. 2 наведено алгоритм прийняття рішень щодо управління криптографічними ключами на основі концепції Grounded AI. Алгоритм передбачає послідовне формування контексту, оцінювання довіри та кіберризику, визначення доцільності зміни політики, вибір оптимальної операції над ключем і оновлення бази знань Grounded AI за результатами виконаної керуючої дії.

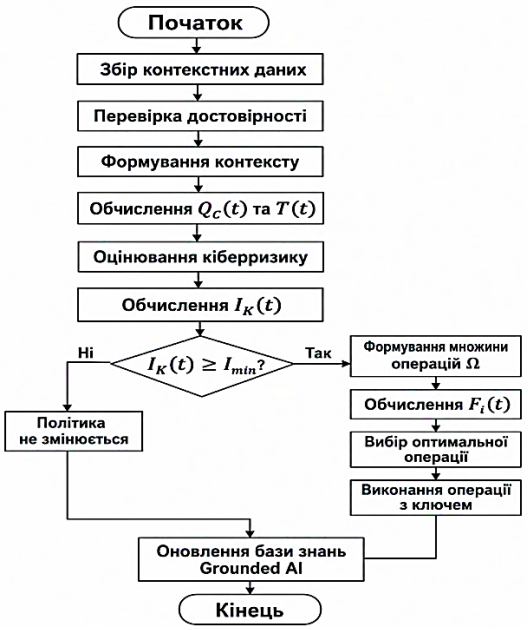

Рис. 2. Блок-схема методу прийняття рішень щодо життєвого циклу криптографічних ключів

Вдосконалення адаптивної політики здійснюється за результатами виконання керуючих дій та оцінювання їх фактичної результативності [9, 13, 19]. Після генерації, ротації, блокування, відкликання або знищення ключа система повторно визначає рівень кіберризику, стан ключового матеріалу та якість функціонування системи управління ключами [16, 21-22]. Результат керуючої дії вважається позитивним, якщо після її виконання зменшується залишковий ризик, не порушуються нормативні обмеження та зберігається допустимий рівень операційних витрат.

Для оцінювання фактичної результативності виконаної операції використовується приріст інтегральної якості стану системи:

$$\Delta Q_i(t) = Q_S^{after}(t) - Q_S^{before}(t) \tag{11}$$

де $Q_S^{after}(t)$ та $Q_S^{before}(t)$ – інтегральні оцінки стану системи відповідно до і після виконання і-ї операції. Якщо $\Delta Q_i(t) > 0$, виконана дія визнається результативною, а відповідний контекст і рішення зберігаються в базі перевірених знань Grounded AI. Якщо дія не забезпечила очікуваного покращення або спричинила порушення встановлених обмежень, її пріоритет зменшується, а політика підлягає коригуванню. Додавання нових правил до бази знань здійснюється лише після автоматичної перевірки їх несуперечності та, для критичних інформаційних систем, підтвердження адміністратором безпеки. Таким чином, зворотний зв'язок забезпечує не лише накопичення результатів, а й контрольоване вдосконалення політики управління криптографічними ключами.

Запропонований метод відрізняється від традиційних підходів тим, що рішення щодо генерації, ротації, блокування або відкликання криптографічного ключа приймається не за наперед визначеним регламентом, а на основі комплексного оцінювання контексту, рівня довіри, кіберризику та прогнозованої ефективності кожної альтернативної дії. Це забезпечує адаптивне керування життєвим циклом криптографічних ключів і підвищує стійкість інформаційної системи до сучасних кіберзагроз.

Результати сценарного оцінювання традиційного та запропонованого підходів. Для перевірки результативності запропонованого підходу сформовано множину сценаріїв функціонування системи управління криптографічними ключами, які охоплювали штатне використання ключів, зміну контексту доступу, наближення строку їх дії до граничного значення, зменшення довіри до користувача або пристрою, аномальну активність, зростання кіберризику, потенційну компрометацію ключового матеріалу та порушення нормативних вимог [15-17, 19, 23].

Для кожного сценарію визначалося еталонне рішення щодо продовження використання, генерації, ротації, блокування, відкликання або знищення ключа на основі політик інформаційної безпеки, нормативних вимог і експертного оцінювання [9, 20-22]. Запропонований підхід порівнювався з традиційною політикою, що використовувала фіксовані інтервали ротації та статичні правила реагування.

Під час оцінювання визначалися точність і час прийняття рішень, своєчасність ротації ключів, виявлення потенційної компрометації та відповідність нормативним правилам [12, 18]. Кожний сценарій виконувався 30 разів за однакових початкових умов, після чого обчислювалися середні значення показників.

Ефективність запропонованого підходу оцінювали шляхом порівняльного аналізу з традиційною політикою управління криптографічними ключами за показниками рівня безпеки, оперативності прийняття рішень і якості управління ключами.

Таблиця 1

Порівняння традиційного та запропонованого підходів

Показник	Традиційний підхід	Запропонований підхід
Точність прийняття рішень, %	91,8	98,4
Частка хибних рішень, %	8,2	1,6
Середній час прийняття рішення, мс	214	132
Частка своєчасної ротації ключів, %	84,5	97,3
Виявлення потенційної компрометації, %	87,1	98,0
Відповідність політикам безпеки, %	92,4	99,2
Інтегральна ефективність, %	89,6	98,1

Для наочного відображення переваг запропонованого підходу порівняння основних нормованих показників наведено на рис. 3.

Рис. 3. Порівняння результативності традиційного та запропонованого підходів до управління криптографічними ключами

Як видно з рис. 3, запропонований підхід забезпечує покращення всіх оцінюваних показників, причому найбільший приріст досягнуто за своєчасністю ротації ключів і виявленням потенційної компрометації.

Для оцінювання стійкості підходів до ускладнення умов функціонування досліджено зміну точності прийняття рішень за різних рівнів кіберризику. Отримані залежності наведено на рис. 4.

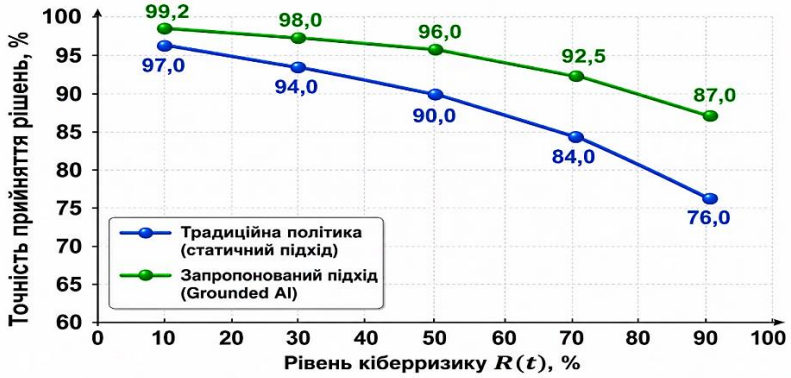

Рис. 4. Залежність точності прийняття рішень від рівня кіберризику

Аналіз залежностей показує, що зі зростанням рівня кіберризику точність обох підходів знижується, однак запропонована політика на основі Grounded AI забезпечує повільніше погіршення показника завдяки врахуванню актуального контексту, перевірених знань і нормативних обмежень.

Для узагальненого оцінювання результативності використовується інтегральний показник ефективності:

$$E = \sum_{i=1}^{m} w_i Q_i, \quad \sum_{i=1}^{m} w_i = 1, \tag{12}$$

де E – інтегральна ефективність запропонованого підходу, Q_i – нормалізоване значення і-го показника ефективності, w_i – ваговий коефіцієнт відповідного показника, m – кількість оцінюваних показників. Для показників, максимізація яких є бажаною, нормування здійснюється відношенням фактичного значення до еталонного значення, а для витратних показників, зокрема часу прийняття рішення та частки хибних рішень, використовується інверсне нормування. Вагові коефіцієнти визначаються експертно й залишаються однаковими для всіх порівнюваних підходів.

Отримані результати свідчать, що використання Grounded AI підвищує ефективність управління життєвим циклом криптографічних ключів. Найбільше покращення спостерігається за точністю прийняття рішень, своєчасністю ротації ключів і виявленням потенційної компрометації [12, 15-17, 23]. Водночас середній час формування керуючої дії зменшується приблизно на 38 %, що є важливим для систем реального часу.

Підвищення інтегральної ефективності зумовлене врахуванням рівня кіберризику, контексту функціонування системи, довіри до рішення Grounded AI та відповідності рекомендацій чинним політикам безпеки [18-20]. Використання механізмів перевірки достовірності даних і пояснюваності

рішень зменшує кількість хибних спрацювань та необґрунтованих операцій із криптографічними ключами.

Основними перевагами запропонованого підходу є адаптивне керування життєвим циклом криптографічних ключів з урахуванням контексту функціонування системи, інтеграція оцінювання кіберризику, рівня довіри та пояснюваності Grounded AI в єдину модель прийняття рішень, підвищення точності визначення необхідності генерації, ротації чи відкликання ключів, скорочення часу формування керуючих рішень, зменшення кількості хибних операцій і ризику компрометації ключового матеріалу, а також забезпечення відповідності вимогам політик інформаційної безпеки та нормативних документів. Таким чином, результати дослідження підтверджують, що запропонований підхід забезпечує ефективніше, адаптивніше й більш обґрунтоване управління життєвим циклом криптографічних ключів порівняно зі статичними політиками ротації та відкликання ключів.

Обговорення. Отримані результати підтверджують, що інтеграція контекстної інформації, оцінювання кіберризику, рівня довіри та механізмів Grounded AI забезпечує більш обґрунтоване прийняття рішень щодо життєвого циклу криптографічних ключів порівняно зі статичними політиками [7-10, 17-20]. Водночас ефективність запропонованого підходу залежить від повноти й достовірності вхідних даних, якості бази знань Grounded AI та правильності налаштування вагових коефіцієнтів [15-16, 22-23]. Тому результати доцільно розглядати як основу для подальшої експериментальної перевірки на реальних інформаційних системах.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі запропоновано адаптивний підхід до формування та вдосконалення політики управління криптографічними ключами на основі концепції Grounded AI, який забезпечує прийняття обґрунтованих керуючих рішень з урахуванням контексту функціонування системи, рівня кіберризику та перевірених знань. Результати сценарного оцінювання підтвердили доцільність використання запропонованого підходу порівняно зі статичною політикою управління ключами.

Перспективи подальших досліджень пов'язані з експериментальною перевіркою підходу в реальних інформаційно-комунікаційних системах, автоматизованим налаштуванням параметрів моделі, розширенням бази знань Grounded AI та інтеграцією запропонованого методу із сучасними системами керування криптографічними ключами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Taherdoost, H., Le, T.-V., & Slimani, K. (2025). Cryptographic techniques in artificial intelligence security: A bibliometric review. *Cryptography, 9*(1), Article 17. https://doi.org/10.3390/cryptography9010017
2. Radanliev, P. (2024). Artificial intelligence and quantum cryptography. *Journal of Analytical Science and Technology, 15*, Article 4. https://doi.org/10.1186/s40543-024-00416-6
3. Feretzakis, G., Papaspyridis, K., Gkoulalas-Divanis, A., & Verykios, V. S. (2024). Privacy-preserving techniques in generative AI and large language models: A narrative review. *Information, 15*(11), Article 697. https://doi.org/10.3390/info15110697
4. Elkhodr, M. (2025). An AI-driven framework for integrated security and privacy in Internet of Things using quantum-resistant blockchain. *Future Internet, 17*(6), Article 246. https://doi.org/10.3390/fi17060246
5. Pallakonda, A., Kaliyannan, K., Sumathi, R. L., Raj, R. D. A., Yanamala, R. M. R., Napoli, C., & Randieri, C. (2025). AI-driven attack detection and cryptographic privacy protection for cyber-resilient industrial control systems. *IoT, 6*(3), Article 56. https://doi.org/10.3390/iot6030056
6. Swetha, T., Kumaran, U., Meena, V. P., et al. (2025). Leveraging AI for enhanced cybersecurity: A comprehensive review. *Discover Applied Sciences, 7*, Article 584. https://doi.org/10.1007/s42452-025-06773-0
7. Islam, S., Basheer, N., Papastergiou, S., et al. (2025). Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. *Journal of Reliable Intelligent Environments, 11*, Article 12. https://doi.org/10.1007/s40860-025-00253-3
8. Ofusori, L., Bokaba, T., & Mhlongo, S. (2025). Explainability and interpretability of artificial intelligence use in cybersecurity. *Discover Computing, 28*, Article 241. https://doi.org/10.1007/s10791-025-09760-6
9. Kostiuk, Y., Skladannyi, P., Mazur, N., Rzaieva, S., Hnatchenko, D., & Honcharenko, I. (2026). Formal model of adaptive selection of cryptographic parameters for channel protection in corporate computer

networks based on dynamic trust assessment. *Cybersecurity: Education, Science, Technique, 4*(32), 20–44. https://doi.org/10.28925/2663-4023.2026.32.1111

10. Schneider, J. (2024). Explainable generative AI (GenXAI): A survey, conceptualization, and research agenda. *Artificial Intelligence Review, 57*, Article 289. https://doi.org/10.1007/s10462-024-10916-x
11. Skladannyi, P. M., Hulak, H. M., & Kostiuk, Y. V. (2025). Chaotic number generator with fuzzy control for cryptographic systems with dynamic trust. *Telecommunication and Information Technologies, 4*(89), 137–147. https://doi.org/10.31673/2412-4338.2025.048916
12. Krishnan, D., Singh, S., & Sugumaran, V. (2025). Explainable AI for zero-day attack detection in IoT networks using attention fusion model. *Discover Internet of Things, 5*, Article 83. https://doi.org/10.1007/s43926-025-00184-8
13. Kostiuk, Y. V., & Skladannyi, P. M. (2026). Cryptographic model of trust in security events in SIEM for intelligent formation of network incidents. *Modern Information Security, 1*(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393
14. Kaur, N., & Gupta, L. (2025). Securing the 6G-IoT environment: A framework for enhancing transparency in artificial intelligence decision-making through explainable artificial intelligence. *Sensors, 25*(3), Article 854. https://doi.org/10.3390/s25030854
15. Skladannyi, P. M., Kostiuk, Y. V., Sokolov, V. Y., & Kuchakovska, H. A. (2026). Model for dynamic selection of post-quantum cryptographic algorithms in information and communication systems based on integrated risk and efficiency assessment. *Telecommunication and Information Technologies, 2*, 16–29. https://doi.org/10.31673/2412-4338.2026.029112
16. Dervisevic, E., Tankovic, A., Fazel, E., Kompella, R., Fazio, P., Voznak, M., & Mehic, M. (2025). Quantum key distribution networks-Key management: A survey. *ACM Computing Surveys, 57*(10), Article 257, 1–36. https://doi.org/10.1145/3730575
17. Skladannyi, P., Kostiuk, Y., & Rzaieva, S. (2026). Continuous access evaluation in Zero Trust Access Management based on event-driven security signals and dynamic session management. *Mathematical Machines and Systems, 1*, 29-46. https://doi.org/10.34121/1028-9763-2026-1-29-46
18. Velmurugan, M., Ouyang, C., Xu, Y., Sindhgatta, R., Wickramanayake, B., & Moreira, C. (2025). Developing guidelines for functionally grounded evaluation of explainable artificial intelligence using tabular data. *Engineering Applications of Artificial Intelligence, 141*, Article 109772. https://doi.org/10.1016/j.engappai.2024.109772
19. Skladannyi, P., & Kostiuk, Y. (2026). Mathematical model of continuous authentication based on dynamic trust in Zero Trust architecture (ZTNA). *Information Technology and Security, 14*(1), 125–138. https://doi.org/10.20535/2411-1031.2026.14.1.365482
20. Rajabi, E., & Etminani, K. (2024). Knowledge-graph-based explainable AI: A systematic review. *Journal of Information Science, 50*(4), 1019-1029. https://doi.org/10.1177/01655515221112844
21. 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 with authentication and key exchange protocols. *Cybersecurity: Education, Science, Technique, 1*(25), 229-252. https://doi.org/10.28925/2663-4023.2024.25.229252
22. Gilliard, E., & Liu, J. (2026). CALIS: AI-driven context-aware encryption for SDN-enabled smart-home IoT. *Journal of King Saud University – Computer and Information Sciences*. Advance online publication. https://doi.org/10.1007/s44443-025-00404-9
23. Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems, 67*, 6969-7055. https://doi.org/10.1007/s10115-025-02429-y
24. Singh, P., Pranav, P., & Dutta, S. (2025). A GA-GAN approach for next-generation cryptographic security with a focus on quantum-resistant cryptography. *Discover Computing, 28*, Article 82. https://doi.org/10.1007/s10791-025-09594-2

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

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

FORMATION AND IMPROVEMENT OF A CRYPTOGRAPHIC KEY MANAGEMENT POLICY BASED ON THE GROUNDED AI CONCEPT

Abstract. The article is devoted to investigating the problems of forming and improving cryptographic key management policies in modern information and communication systems based on the Grounded AI concept, which supports decision-making through the use of verified data, contextual information, and explainability mechanisms. It is shown that traditional key management policies based on static rules and fixed key rotation intervals do not provide the required level of adaptability under dynamically changing conditions of the information environment, user characteristics, resources, and cyber threats. The specific features of applying the Grounded AI concept to support the generation, distribution, storage, use, renewal, revocation, and destruction of cryptographic keys are considered with due regard to the current operational context of the system. The factors influencing the selection of a key management policy are investigated, including the level of risk, the criticality of information resources, trust in interacting entities, execution environment characteristics, and regulatory requirements. An approach to forming an adaptive cryptographic key management policy is proposed, in which decisions concerning the key life cycle are made on the basis of an integrated analysis of contextual parameters, risk assessment, and the outputs of Grounded AI models, with the possibility of providing justification for the decisions made. A conceptual model of interaction among policy components has been developed, combining modules for monitoring, context assessment, risk analysis, recommendation generation, decision explanation, and implementation of control actions. The concluding section substantiates the advantages of the proposed approach, which include increasing the adaptability, controllability, transparency, and validity of cryptographic key management processes, reducing the probability of key material compromise, and improving the operational efficiency of cryptographic information protection systems. According to the scenario-based evaluation results, decision-making accuracy increased from 91.8% to 98.4%, the average time required to generate a control action decreased from 214 to 132 ms, and overall efficiency increased from 89.6% to 98.1% compared with a static policy.

Keywords: Grounded AI; cryptographic key management; key management policy; cryptographic key life cycle; information security; cybersecurity; adaptive management; explainable artificial intelligence.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Taherdoost, H., Le, T.-V., & Slimani, K. (2025). Cryptographic techniques in artificial intelligence security: A bibliometric review. *Cryptography*, *9*(1), Article 17. https://doi.org/10.3390/cryptography9010017
2. Radanliev, P. (2024). Artificial intelligence and quantum cryptography. *Journal of Analytical Science and Technology*, *15*, Article 4. https://doi.org/10.1186/s40543-024-00416-6
3. Feretzakis, G., Papaspyridis, K., Gkoulalas-Divanis, A., & Verykios, V. S. (2024). Privacy-preserving techniques in generative AI and large language models: A narrative review. *Information, 15*(11), Article 697. https://doi.org/10.3390/info15110697
4. Elkhodr, M. (2025). An AI-driven framework for integrated security and privacy in Internet of Things using quantum-resistant blockchain. *Future Internet, 17*(6), Article 246. https://doi.org/10.3390/fi17060246
5. Pallakonda, A., Kaliyannan, K., Sumathi, R. L., Raj, R. D. A., Yanamala, R. M. R., Napoli, C., & Randieri, C. (2025). AI-driven attack detection and cryptographic privacy protection for cyber-resilient industrial control systems. *IoT, 6*(3), Article 56. https://doi.org/10.3390/iot6030056

6. Swetha, T., Kumaran, U., Meena, V. P., et al. (2025). Leveraging AI for enhanced cybersecurity: A comprehensive review. *Discover Applied Sciences, 7*, Article 584. https://doi.org/10.1007/s42452-025-06773-0
7. Islam, S., Basheer, N., Papastergiou, S., et al. (2025). Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. *Journal of Reliable Intelligent Environments, 11*, Article 12. https://doi.org/10.1007/s40860-025-00253-3
8. Ofusori, L., Bokaba, T., & Mhlongo, S. (2025). Explainability and interpretability of artificial intelligence use in cybersecurity. *Discover Computing, 28*, Article 241. https://doi.org/10.1007/s10791-025-09760-6
9. Kostiuk, Y., Skladannyi, P., Mazur, N., Rzaieva, S., Hnatchenko, D., & Honcharenko, I. (2026). Formal model of adaptive selection of cryptographic parameters for channel protection in corporate computer networks based on dynamic trust assessment. *Cybersecurity: Education, Science, Technique, 4*(32), 20–44. https://doi.org/10.28925/2663-4023.2026.32.1111
10. Schneider, J. (2024). Explainable generative AI (GenXAI): A survey, conceptualization, and research agenda. *Artificial Intelligence Review, 57*, Article 289. https://doi.org/10.1007/s10462-024-10916-x
11. Skladannyi, P. M., Hulak, H. M., & Kostiuk, Y. V. (2025). Chaotic number generator with fuzzy control for cryptographic systems with dynamic trust. *Telecommunication and Information Technologies, 4*(89), 137–147. https://doi.org/10.31673/2412-4338.2025.048916
12. Krishnan, D., Singh, S., & Sugumaran, V. (2025). Explainable AI for zero-day attack detection in IoT networks using attention fusion model. *Discover Internet of Things, 5*, Article 83. https://doi.org/10.1007/s43926-025-00184-8
13. Kostiuk, Y. V., & Skladannyi, P. M. (2026). Cryptographic model of trust in security events in SIEM for intelligent formation of network incidents. *Modern Information Security, 1*(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393
14. Kaur, N., & Gupta, L. (2025). Securing the 6G-IoT environment: A framework for enhancing transparency in artificial intelligence decision-making through explainable artificial intelligence. *Sensors, 25*(3), Article 854. https://doi.org/10.3390/s25030854
15. Skladannyi, P. M., Kostiuk, Y. V., Sokolov, V. Y., & Kuchakovska, H. A. (2026). Model for dynamic selection of post-quantum cryptographic algorithms in information and communication systems based on integrated risk and efficiency assessment. *Telecommunication and Information Technologies, 2*, 16–29. https://doi.org/10.31673/2412-4338.2026.029112
16. Dervisevic, E., Tankovic, A., Fazel, E., Kompella, R., Fazio, P., Voznak, M., & Mehic, M. (2025). Quantum key distribution networks-Key management: A survey. *ACM Computing Surveys, 57*(10), Article 257, 1–36. https://doi.org/10.1145/3730575
17. Skladannyi, P., Kostiuk, Y., & Rzaieva, S. (2026). Continuous access evaluation in Zero Trust Access Management based on event-driven security signals and dynamic session management. *Mathematical Machines and Systems, 1*, 29-46. https://doi.org/10.34121/1028-9763-2026-1-29-46
18. Velmurugan, M., Ouyang, C., Xu, Y., Sindhgatta, R., Wickramanayake, B., & Moreira, C. (2025). Developing guidelines for functionally grounded evaluation of explainable artificial intelligence using tabular data. *Engineering Applications of Artificial Intelligence, 141*, Article 109772. https://doi.org/10.1016/j.engappai.2024.109772
19. Skladannyi, P., & Kostiuk, Y. (2026). Mathematical model of continuous authentication based on dynamic trust in Zero Trust architecture (ZTNA). *Information Technology and Security, 14*(1), 125–138. https://doi.org/10.20535/2411-1031.2026.14.1.365482
20. Rajabi, E., & Etminani, K. (2024). Knowledge-graph-based explainable AI: A systematic review. *Journal of Information Science, 50*(4), 1019-1029. https://doi.org/10.1177/01655515221112844
21. 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 with authentication and key exchange protocols. *Cybersecurity: Education, Science, Technique, 1*(25), 229-252. https://doi.org/10.28925/2663-4023.2024.25.229252
22. Gilliard, E., & Liu, J. (2026). CALIS: AI-driven context-aware encryption for SDN-enabled smart-home IoT. *Journal of King Saud University – Computer and Information Sciences*. Advance online publication. https://doi.org/10.1007/s44443-025-00404-9
23. Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems, 67*, 6969-7055. https://doi.org/10.1007/s10115-025-02429-y

24. Singh, P., Pranav, P., & Dutta, S. (2025). A GA-GAN approach for next-generation cryptographic security with a focus on quantum-resistant cryptography. *Discover Computing, 28*, Article 82. https://doi.org/10.1007/s10791-025-09594-2

Отримано редакцією журналу / Received: 07.02.26
Прорецензовано / Revised: 20.02.26
Схвалено до друку / Accepted: 24.09.26