КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1335
УДК 004.056.55:004.738.5:004.75

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

Рзаєва Світлана Леонідівна
кандидат технічних наук, доцент,
доцент кафедри кафедри комп'ютерних наук
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-7589-2045
s.rzaieva@kubg.edu.ua

Мазур Наталія Петрівна
кандидат педагогічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0001-7671-8287
n.mazur@kubg.edu.ua

Хорольська Карина Вікторівна
PhD in Computer Science
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0003-3270-4494
karynakhorolska@gmail.com

Бебешко Богдан Тарасович
PhD in Computer Science
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0001-6599-0808
b.bebeshko@kubg.edu.ua

Гнатченко Дмитро Дмитрович
PhD in Computer Science,
старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, м. Київ, Україна
ORCID: 0000-0002-6584-4525
hnatchenko@knute.edu.ua

МОДЕЛЬ КОГНІТИВНОЇ БАГАТОСТОРОННЬОЇ АВТОРИЗАЦІЇ КРИТИЧНИХ КРИПТОГРАФІЧНИХ ОПЕРАЦІЙ У КОРПОРАТИВНИХ ХМАРНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Анотація. Статтю присвячено розробленню моделі когнітивної багатосторонньої авторизації критичних криптографічних операцій у корпоративних хмарних інформаційних системах, спрямованої на підвищення рівня захищеності криптографічних сервісів, достовірності прийняття рішень щодо виконання критичних операцій та зменшення ризику компрометації криптографічних ключів. Досліджено сучасні підходи до багатосторонньої авторизації, порогової криптографії, контекстно-орієнтованого контролю доступу, концепції Zero Trust і методів підтримки прийняття рішень у розподілених інтелектуальних системах. Встановлено, що існуючі механізми багатосторонньої авторизації переважно використовують статичні правила підтвердження криптографічних операцій і недостатньо враховують зміну контексту функціонування, рівень довіри до суб'єктів, критичність

операції, поточний кіберризик та взаємозалежність факторів, які впливають на безпеку корпоративного хмарного середовища. Запропоновано модель когнітивної багатосторонньої авторизації, що ґрунтується на інтеграції когнітивного моделювання, контекстного оцінювання, розподіленого інтелектуального аналізу та адаптивного визначення необхідного рівня колективного підтвердження критичних криптографічних операцій. Розроблено модель прийняття рішень, яка формує вимоги до багатосторонньої авторизації на основі комплексного оцінювання критичності операції, рівня довіри, кіберризику, характеристик інформаційного ресурсу та поточного стану корпоративного хмарного середовища. Проведено структурно-функціональне оцінювання запропонованої моделі, результати якого показали її здатність адаптивно змінювати склад авторизаторів, поріг підтвердження та тип керуючого рішення відповідно до зміни контексту, довіри, критичності операції й прогнозованого кіберризику. Практичне значення отриманих результатів полягає у можливості використання запропонованої моделі під час побудови захищених корпоративних хмарних інформаційних систем, сервісів керування криптографічними ключами та інфраструктур підтримки критичних криптографічних операцій.

Ключові слова: когнітивна модель; багатостороння авторизація; корпоративні хмарні інформаційні системи; критичні криптографічні операції; розподілені інтелектуальні системи; підтримка прийняття рішень; криптографічні ключі; Zero Trust.

ВСТУП

Стрімке поширення корпоративних хмарних інформаційних систем зумовило суттєве зростання кількості критичних криптографічних операцій, пов'язаних із генерацією, розподілом, ротацією, відкликанням і використанням криптографічних ключів, підписанням цифрових документів, керуванням сертифікатами та доступом до криптографічних сервісів [1-2, 16, 22]. Компрометація таких операцій може призвести до порушення конфіденційності, цілісності та доступності корпоративних інформаційних ресурсів, що безпосередньо впливає на безпеку бізнес-процесів і стійкість функціонування хмарної інфраструктури [11, 13, 20]. У сучасних умовах традиційні механізми автентифікації та авторизації вже не забезпечують належного рівня захисту, оскільки здебільшого базуються на статичних політиках доступу, які не враховують динамічні зміни контексту функціонування, рівень довіри до суб'єктів, поточний кіберризик і критичність виконуваної криптографічної операції [3-9].

Концепція Zero Trust передбачає безперервну перевірку суб'єктів, пристроїв і середовища виконання операцій [21, 25-26], однак більшість існуючих механізмів багатосторонньої авторизації реалізує фіксовані схеми підтвердження типу k із n, у яких кількість учасників, необхідних для виконання критичної криптографічної операції, визначається заздалегідь і не змінюється залежно від поточної ситуації [18-19, 24]. Такий підхід не враховує взаємний вплив факторів довіри, поведінкових характеристик користувачів, критичності інформаційного ресурсу, результатів моніторингу кіберзагроз та інших контекстних параметрів, що істотно знижує адаптивність системи захисту.

Одним із перспективних напрямів розв'язання зазначеної проблеми є використання когнітивного моделювання та розподілених інтелектуальних систем підтримки прийняття рішень [10, 12, 14-15]. Когнітивні моделі дають змогу формалізувати причинно-наслідкові зв'язки між факторами, що характеризують стан корпоративного хмарного середовища, а розподілені інтелектуальні агенти забезпечують незалежне оцінювання довіри, ризику, контексту та критичності операції з подальшим агрегуванням результатів для формування обґрунтованого рішення щодо можливості її виконання [17, 23, 27]. Це створює передумови для переходу від статичних схем багатосторонньої авторизації до адаптивних моделей, здатних змінювати вимоги до колективного підтвердження відповідно до поточної ситуації.

Наукова новизна роботи полягає у розробленні моделі когнітивної багатосторонньої авторизації критичних криптографічних операцій у корпоративних хмарних інформаційних системах, яка, на відміну від існуючих підходів, інтегрує когнітивне моделювання, контекстне оцінювання, аналіз рівня довіри, оцінювання кіберризику та розподілене інтелектуальне прийняття рішень для адаптивного визначення необхідного рівня колективної авторизації.

Теоретичне значення дослідження полягає у розвитку моделей підтримки прийняття рішень щодо виконання критичних криптографічних операцій шляхом формалізації взаємозв'язків між контекстом функціонування, рівнем довіри, критичністю операції та кіберризиком у межах єдиної когнітивної моделі.

Практичне значення полягає у можливості застосування запропонованої моделі під час побудови корпоративних хмарних інформаційних систем, центрів керування криптографічними ключами, інфраструктур відкритих ключів, сервісів цифрового підпису та інших криптографічних сервісів, де необхідно забезпечити адаптивну багатосторонню авторизацію критичних операцій, підвищити стійкість до несанкціонованого доступу та зменшити ризик компрометації криптографічних активів.

Постановка проблеми. Корпоративні хмарні інформаційні системи забезпечують виконання великої кількості критичних криптографічних операцій, пов'язаних із керуванням криптографічними ключами, цифровим підписом, шифруванням та контролем доступу [16, 18, 22]. Більшість сучасних механізмів багатосторонньої авторизації використовує статичні схеми підтвердження, які не враховують поточний контекст функціонування, рівень довіри до учасників, критичність операції та кіберризик [11, 19-21, 25-26]. Це знижує ефективність захисту корпоративних хмарних сервісів в умовах динамічної зміни середовища.

У зв'язку з цим актуальним науково-практичним завданням є розроблення моделі когнітивної багатосторонньої авторизації критичних криптографічних операцій, яка забезпечує адаптивне прийняття рішень на основі комплексного оцінювання контексту, рівня довіри, кіберризику та критичності операції для підвищення захищеності корпоративних хмарних інформаційних систем [10, 14, 27].

Аналіз останніх досліджень і публікацій. Сучасні дослідження у сфері захисту корпоративних хмарних інформаційних систем зосереджені переважно на розвитку порогової криптографії, динамічного контролю доступу, механізмів оцінювання довіри та практичної реалізації принципів Zero Trust. Багатостороння авторизація в таких системах розглядається як засіб розподілу криптографічних повноважень між кількома суб’єктами, усунення одноосібного контролю над критичними операціями та зниження ризику єдиної точки відмови.

Питання адаптивного виконання порогових криптографічних операцій розглянуто у праці Y. Tong та співавторів [1]. Авторами запропоновано адаптивно захищену, подільну та стійку схему порогового розшифрування з перевіркою підпису, у якій криптографічна операція виконується за участю не менше ніж (t) із (n) учасників. Запропонована схема забезпечує стійкість до компрометації окремих сторін, публічну перевірюваність результату та надійність порогового виконання. Водночас її адаптивність пов’язана переважно з моделлю криптографічного противника і не передбачає динамічного визначення складу авторизаторів або порога підтвердження залежно від контексту, довіри та поточного кіберризику.

Квантово стійкий напрям багатостороннього керування криптографічними ключами розвинено P. S. Renisha та B. Rudra [2]. Запропонований авторами механізм ґрунтується на бездилерному розподіленому генеруванні ключів і застосуванні CRYSTALS–Kyber, що дає змогу усунути залежність від єдиного довіреного центру та розподілити криптографічні повноваження між учасниками. Разом із тим у цій схемі не формалізовано оцінювання поведінки суб’єктів, контексту виконання операції, її критичності та рівня кіберризику.

Динамічний контроль доступу до хмарних ресурсів на основі Zero Trust запропоновано R. Wang, C. Li, K. Zhang та співавторами [3]. У розробленій моделі рівень довіри до користувача коригується з урахуванням його поведінки, а алгоритм Deep Q-Network використовується для адаптивної зміни порогових значень. Такий підхід підвищує гнучкість політик доступу, однак орієнтований переважно на індивідуальну авторизацію та не охоплює колективне підтвердження критичних криптографічних операцій.

Інший підхід до формування авторизаційного рішення представлено E. Jeong і D. Yang [4]. Розроблена ними модель ґрунтується на кількісному показнику довіри, який обчислюється за атрибутами користувача та результатами моніторингу його активності. Проведене оцінювання підтвердило можливість використання інтегрального рівня довіри для динамічного контролю доступу. Проте ця модель не передбачає узгодження рішень кількох незалежних учасників і не визначає адаптивної кількості необхідних підтверджень.

Поєднання атрибутивного керування доступом із динамічним оцінюванням довіри досліджено Y. Mao та співавторами [5]. Запропонована модель враховує як позитивні характеристики довіри, так і негативні ризикові фактори, завдяки чому підвищується контекстна обґрунтованість рішень щодо доступу до хмарних ресурсів. Водночас основним об’єктом аналізу залишається окремий запит користувача, а взаємозалежність рішень кількох уповноважених сторін не розглядається.

Децентралізований механізм Zero Trust із використанням блокчейну та функціонального шифрування розроблено S. Nie та співавторами [6]. Інтеграція блокчейну, смартконтрактів, репутаційного оцінювання та шифрування за внутрішнім добутком забезпечує прозорість, автоматизацію і незмінність рішень щодо доступу. Однак запропонований механізм не містить когнітивної моделі причинно-наслідкових зв’язків між довірою, контекстом, критичністю операції та поточним рівнем кіберризику.

Адаптивне керування політиками Zero Trust у мережах 5G досліджено A. K. Alnaim [7]. У запропонованій системі засоби контролю змінюються відповідно до стану середовища, поведінки суб'єктів і виявлених загроз. Результати дослідження підтверджують доцільність динамічного перегляду політик безпеки, однак не визначають процедури багатостороннього прийняття рішень щодо виконання криптографічних операцій і не враховують розподілу криптографічних повноважень.

Архітектурні аспекти побудови та перевірки систем безпеки відповідно до принципів Zero Trust розглянуто S. Lee, J.-H. Huh і H. Woo [8]. Запропонована архітектура забезпечує послідовну перевірку суб'єктів, контроль доступу та верифікацію захисних механізмів. Водночас у ній не передбачено адаптивного формування групи авторизаторів, оцінювання їхньої сукупної довіри та визначення динамічного порога підтвердження критичної операції.

Практичні складові впровадження Zero Trust систематизовано F. Santucci та співавторами [9]. До ключових елементів авторами віднесено керування ідентичністю, контроль доступу, безперервний моніторинг, захист даних, сегментацію та оцінювання ризиків. Отримані результати підтверджують необхідність комплексного врахування організаційних і технічних факторів під час побудови корпоративних систем захисту. Проте в роботі не запропоновано формалізованої моделі колективного прийняття рішень щодо критичних криптографічних операцій.

Отже, проаналізовані дослідження окремо розв'язують завдання порогового виконання криптографічних операцій, розподіленого генерування ключів, динамічного оцінювання довіри, контекстного контролю доступу та реалізації принципів Zero Trust [1-12, 16, 18, 25-26]. Водночас раніше невирішеною частиною загальної проблеми залишається розроблення єдиної моделі, яка поєднує багатосторонню авторизацію з когнітивним аналізом причинно-наслідкових зв'язків між контекстом функціонування, рівнем довіри до кожного учасника, критичністю криптографічної операції та поточним кіберризиком [20-24, 27]. Недостатньо дослідженими також є адаптивне формування складу авторизаторів, визначення необхідної кількості підтверджень і вибір остаточного рішення щодо дозволу, додаткової перевірки або блокування критичної криптографічної операції. Розв'язанню зазначених завдань присвячене дослідження.

Мета статті. Метою статті є розробка моделі когнітивної багатосторонньої авторизації критичних криптографічних операцій у корпоративних хмарних інформаційних системах, яка забезпечує адаптивне прийняття рішень на основі комплексного оцінювання контексту функціонування, рівня довіри, кіберризику та критичності операцій для підвищення рівня захищеності корпоративних криптографічних сервісів.

Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

– проаналізувати сучасні підходи до багатосторонньої авторизації критичних криптографічних операцій у корпоративних хмарних інформаційних системах та визначити їх основні недоліки;
– сформувати систему факторів, що впливають на прийняття рішень щодо виконання критичних криптографічних операцій;
– розробити модель когнітивної багатосторонньої авторизації на основі комплексного оцінювання контексту, рівня довіри, кіберризику та критичності операцій;
– розробити алгоритм прийняття рішень щодо адаптивної багатосторонньої авторизації критичних криптографічних операцій;
– провести структурно-функціональне оцінювання запропонованої моделі та визначити ефективність її використання у корпоративних хмарних інформаційних системах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У межах дослідження розроблено комплекс взаємопов'язаних моделей, що формалізують повний цикл когнітивної багатосторонньої авторизації критичних криптографічних операцій. Запропонований підхід охоплює формування контексту авторизації, динамічне оцінювання довіри, визначення критичності операції, прогнозування кіберризику, побудову причинно-наслідкової когнітивної моделі, адаптивний вибір складу авторизаторів і порога підтвердження, а також прийняття остаточного рішення щодо виконання операції.

Формалізація простору багатосторонньої авторизації.

Запропонована модель ґрунтується на розгляді процесу багатосторонньої авторизації як єдиного когнітивного простору взаємодії користувачів, криптографічних операцій, ключів, контексту функціонування та політик безпеки [14-15, 23]. На відміну від існуючих підходів, у яких зазначені компоненти розглядаються ізольовано, запропонована модель інтегрує їх у спільний математичний простір прийняття рішень [17, 24]. Це дає змогу формувати адаптивне рішення щодо виконання

критичної криптографічної операції залежно від поточного стану системи, рівня довіри до учасників, контекстних характеристик та рівня кіберризику.

Формально простір багатосторонньої авторизації визначимо як:

$$\Omega_{Auth} = \langle U, O, K, C, P, T, R, D \rangle \quad (1)$$

де $U = \{u_1, u_2, \dots, u_n\}$ – множина уповноважених користувачів, $O = \{o_1, o_2, \dots, o_m\}$ – множина критичних криптографічних операцій, $K = \{k_1, k_2, \dots, k_s\}$ – множина криптографічних ключів, C – множина контекстних параметрів, P – множина політик безпеки, T – множина показників довіри, R – множина оцінок кіберризику, D – множина можливих авторизаційних рішень.

Кожна криптографічна операція характеризується власним інформаційним описом:

$$o_i = \langle K_i, L_i, S_i, \tau_i \rangle \quad (2)$$

де K_i – криптографічний ключ, що використовується під час виконання операції, L_i – рівень критичності операції, S_i – множина необхідних повноважень, τ_i – допустимий часовий інтервал виконання.

Для кожного користувача формується когнітивний профіль:

$$o_i = \langle K_i, L_i, S_i, \tau_i \rangle \quad (3)$$

де A_j – атрибути користувача, T_j – поточний рівень довіри, B_j – поведінкові характеристики, H_j – історія виконання критичних криптографічних операцій.

Контекст функціонування системи визначається множиною взаємопов'язаних параметрів:

$$C = \langle C_t, C_l, C_d, C_n, C_s, C_a \rangle \quad (4)$$

де C_t – часовий контекст, C_l – просторовий контекст, C_d – характеристики пристрою, C_n – мережевий стан, C_s – поточний стан системи, C_a – активність користувачів.

Для забезпечення універсальності моделі всі параметри переводяться до безрозмірної шкали:

$$\hat{x}_i = \begin{cases} \dfrac{x_i - x_i^{min}}{x_i^{max} - x_i^{min}} & \text{якщо зростання показника покращує стан системи,} \\ 1 - \dfrac{x_i - x_i^{min}}{x_i^{max} - x_i^{min}} & \text{якщо зростання показника погіршує стан системи.} \end{cases} \quad (5)$$

Такий спосіб нормування забезпечує єдину орієнтацію показників: значення, наближене до одиниці, відповідає сприятливому або безпечному стану, а значення, наближене до нуля, — несприятливому або небезпечному стану.

Таким чином, запропонована формалізація створює єдиний математичний простір, у межах якого всі сутності процесу багатосторонньої авторизації описуються уніфіковано та можуть одночасно враховуватися під час прийняття рішення [14-15, 23-24]. На відміну від існуючих моделей, вона забезпечує інтеграцію характеристик користувачів, криптографічних операцій, ключів, політик безпеки та контексту функціонування в єдину систему, що є теоретичною основою для подальшої побудови когнітивної моделі оцінювання довіри, прогнозування кіберризику та адаптивного визначення складу авторизаторів.

На рис. 1 наведено загальну структуру запропонованої моделі, яка відображає послідовність оброблення запиту на виконання критичної криптографічної операції: від формування контексту, оцінювання довіри, визначення критичності та прогнозування кіберризику до когнітивного аналізу, адаптивного вибору складу авторизаторів, визначення порога підтвердження й прийняття остаточного рішення [19-21]. Передбачено механізм зворотного зв'язку, що забезпечує безперервне оновлення оцінок довіри, ризику та параметрів моделі відповідно до результатів виконання операцій.

Рис. 1. Структурно-функціональна модель когнітивної багатосторонньої авторизації

Модель когнітивного контексту авторизації.

Одним із ключових недоліків існуючих систем багатосторонньої авторизації є прийняття рішення на основі обмеженої кількості незалежних параметрів, що не відображають реального стану корпоративного хмарного середовища [20, 25-26]. Для усунення цього недоліку запропоновано модель когнітивного контексту авторизації, яка інтегрує різнорідні характеристики користувача, інформаційної системи та зовнішнього середовища в єдиний інформаційний простір прийняття рішень [10, 12, 14-16]. На відміну від традиційних моделей, запропонований підхід не лише накопичує контекстні дані, а й формує їхню узгоджену когнітивну інтерпретацію з урахуванням взаємного впливу окремих факторів.

Когнітивний контекст визначимо у вигляді багатовимірного вектора:

$$C(t) = \langle C_B, C_L, C_T, C_D, C_N, C_S, C_H, C_R, C_E, C_A \rangle \tag{6}$$

де C_B – поведінковий контекст користувача, C_L – просторове розташування, C_T – часові характеристики, C_D – параметри пристрою, C_N – стан мережевого середовища, C_S – поточний рівень інформаційної безпеки, C_H – історія попередніх криптографічних операцій, C_R – рівень актуальних кіберзагроз, C_E – характеристики середовища виконання, C_A – активність інших учасників багатосторонньої авторизації.

Оскільки окремі складові мають різну важливість для різних криптографічних операцій, інтегральний когнітивний контекст визначається як:

$$Q_C^0(t) = \sum_{i=1}^{m} \omega_i(t)\widehat{C}_\iota(t), \quad \sum_{i=1}^{m} \omega_i(t) = 1 \tag{7}$$

де $Q_C^0(t)$ – первинна інтегральна оцінка контексту без урахування когнітивних взаємовпливів, $\widehat{C}_\iota(t)$ – нормоване значення i-го контекстного параметра, $\omega_i(t)$ – його адаптивна вага, що автоматично змінюється залежно від типу криптографічної операції, політики безпеки та поточного стану системи.

Для врахування взаємозалежності контекстних факторів вводиться матриця когнітивних взаємовпливів:

$$\mathbf{M}_C = [m_{ij}], \quad m_{ij} \in [-1; 1] \tag{8}$$

де m_{ij} характеризує силу позитивного або негативного впливу j-го контекстного параметра на i-й. Це дозволяє враховувати причинно-наслідкові зв'язки між окремими характеристиками, наприклад між нетиповим місцем входу, новим пристроєм, підвищеним мережевим ризиком та аномальною поведінкою користувача.

Спочатку ввести вектор нормованого контексту:

$$\hat{\mathbf{C}}(t) = \left[\hat{C}_1(t), \ldots, \hat{C}_m(t)\right]^T \tag{9}$$

Остаточне когнітивне представлення контексту визначається як:

$$\hat{\mathbf{C}}^*(t) = f_C(M_C\hat{\mathbf{C}}(t)) \tag{10}$$

де $\hat{\boldsymbol{C}}^*(t)$ – скоригований вектор контекстних оцінок, отриманий з урахуванням причинно-наслідкових взаємовпливів, $f(\cdot)$ – функція нормування, яка приводить компоненти вектора до інтервалу [0;1].

Інтегральну оцінка:

$$Q_C(t) = \omega^T(t)\hat{\boldsymbol{C}}^*(t), \ \sum_{i=1}^{m}\omega_i(t) = 1 \tag{11}$$

Таким чином, запропонована модель вперше формалізує когнітивний контекст багатосторонньої авторизації як інтегровану багатовимірну систему взаємопов'язаних параметрів, у якій рішення формується на основі комплексного аналізу поведінки користувачів, характеристик середовища, стану мережі, історії виконання операцій та актуального рівня кіберзагроз. Це створює математичну основу для подальшого адаптивного оцінювання довіри учасників і прогнозування ризику виконання критичних криптографічних операцій.

Модель довіри учасників.

Однією з основних причин компрометації критичних криптографічних операцій є використання статичних моделей довіри, у яких рівень довіри визначається лише під час первинної автентифікації та практично не змінюється в процесі роботи [11, 25-26]. Запропоновано модель динамічного оцінювання довіри, яка враховує не тільки поточний стан користувача, а й накопичений досвід його взаємодії із системою [17, 19, 21]. Завдяки цьому довіра розглядається як еволюційний показник, що безперервно оновлюється відповідно до історії виконаних дій, зміни контексту та результатів попередніх авторизацій.

Для кожного учасника формується функція довіри:

$$T_i(t) = \alpha T_i(t-1) + (1-\alpha)\Phi_i(t), \quad 0 \le \alpha \le 1 \tag{12}$$

де $T_i(t-1)$ – попередній рівень довіри, $\Phi_i(t)$ – інтегральна оцінка поточної поведінки користувача, α – коефіцієнт пам'яті, який визначає вплив попереднього досвіду на нову оцінку.

Поточна поведінкова оцінка визначається як:

$$\Phi_i(t) = \lambda_1 A_i(t) + \lambda_2 B_i(t) + \lambda_3 H_i(t) + \lambda_4 Q_C(t) - \lambda_5 R_{sys}(t-1), \quad \sum_{j=1}^{5}\lambda_j = 1 \tag{13}$$

де A_i(t) – відповідність атрибутів користувача політикам безпеки, B_i(t) – оцінка поведінкової активності, $H_i(t)$ – історична надійність виконання криптографічних операцій, $Q_C(t)$ – інтегральний когнітивний контекст, $R_{sys}(t-1)$ – відома на момент оцінювання довіри системна оцінка ризику, сформована за результатами попереднього циклу моніторингу.

Для врахування стабільності поведінки вводиться коефіцієнт когнітивної узгодженості:

$$S_i(t) = 1 - \frac{1}{N}\sum_{k=1}^{N}|T_i(k) - \overline{T_i}| \tag{14}$$

де $\overline{T_i}$ – середній рівень довіри користувача за останні N сеансів. Чим меншими є коливання довіри, тим вищою вважається стабільність поведінки учасника.

Остаточний рівень довіри визначається як:

$$T_i^*(t) = \beta T_i(t) + (1-\beta)S_i(t), \quad 0 \le \beta \le 1 \tag{15}$$

де $T_i^*(t)$ є інтегральною оцінкою довіри, яка одночасно враховує поточну поведінку користувача та її довгострокову стабільність.

Таким чином, запропонована модель уперше поєднує механізм накопичення історичного досвіду, адаптивне оновлення рівня довіри та оцінювання стабільності поведінки учасників у межах єдиного

математичного підходу. На відміну від статичних моделей, вона забезпечує безперервне коригування рівня довіри відповідно до зміни когнітивного контексту, що створює основу для подальшого адаптивного визначення складу авторизаторів та прийняття обґрунтованого рішення щодо виконання критичної криптографічної операції.

Модель оцінювання критичності криптографічної операції.

У більшості сучасних систем рішення про авторизацію приймається переважно на основі характеристик користувача, тоді як сама криптографічна операція вважається однаково важливою незалежно від її призначення [16, 18, 20]. Такий підхід не враховує, що компрометація різних операцій призводить до принципово різних наслідків для корпоративної інформаційної системи [13, 22]. У зв'язку з цим запропоновано модель оцінювання критичності криптографічної операції, у якій об'єктом аналізу виступає не лише суб'єкт доступу, а й сама операція, її роль у бізнес-процесі, можливі наслідки компрометації та залежність від інших криптографічних сервісів.

Кожна криптографічна операція описується вектором критичних характеристик:

$$O_i = \langle C_i, I_i, E_i, D_i, F_i \rangle \tag{16}$$

де C_i – рівень конфіденційності інформації, I_i – вплив операції на цілісність даних, E_i – рівень впливу на безперервність функціонування системи, D_i – ступінь залежності інших сервісів від результату операції, F_i – потенційні фінансові або організаційні наслідки її компрометації.

Інтегральна оцінка критичності визначається як:

$$L_i = \sum_{k=1}^{5} y_k \hat{O}_{ik}, \quad \sum_{k=1}^{5} y_k = 1 \tag{17}$$

де $\hat{O}_{ik}$ – нормоване значення k-го показника, y_k – його ваговий коефіцієнт.

Для врахування поточного стану корпоративного середовища вводиться адаптивний коефіцієнт контекстної чутливості:

$$\eta_i(t) = 1 + \delta[1 - Q_C(t)]R_i^0(t), \ \ \delta > 0, \tag{18}$$

де $Q_C(t)$ – інтегральний когнітивний контекст авторизації, $R_i^0(t)$ – базова оцінка ризику операції, сформована на основі її типу, класу криптографічного ключа, відомих уразливостей і чинної політики безпеки до виконання прогнозного оцінювання, δ – коефіцієнт масштабування.

Тоді остаточна оцінка критичності криптографічної операції визначається як:

$$L_i^*(t) = \min\{1, L_i\eta_i(t)\} \tag{19}$$

де $L_i^*(t)$ характеризує реальну критичність операції в конкретний момент часу з урахуванням зміни контексту функціонування та поточної кіберзагрози.

Для подальшого прийняття рішення формується множина рівнів критичності:

$$\Psi = \begin{cases} \Psi_1, & L_i^* < \theta_1, \\ \Psi_2, & \theta_1 \le L_i^* < \theta_2, \\ \Psi_3, & \theta_2 \le L_i^* < \theta_3, \\ \Psi_4, & L_i^* \ge \theta_3, \end{cases} \tag{20}$$

де $\Psi_1, \Psi_2, \Psi_3, \Psi_4$ відповідають низькому, середньому, високому та критичному рівням важливості криптографічної операції.

Таким чином, запропонована модель уперше формалізує оцінювання критичності як властивість самої криптографічної операції, а не лише суб'єкта доступу. На відміну від традиційних підходів, критичність визначається комплексно з урахуванням потенційних наслідків компрометації, взаємозалежності криптографічних сервісів, поточного когнітивного контексту та рівня кіберризику. Отримана інтегральна оцінка використовується надалі для адаптивного визначення необхідної кількості авторизаторів, рівня довіри та процедури підтвердження виконання критичної криптографічної операції.

Модель прогнозування кіберризику.

Традиційні механізми авторизації здебільшого оцінюють небезпеку після виявлення порушення або вже під час виконання криптографічної операції [11]. Для критичних операцій такий реактивний підхід є недостатнім, оскільки навіть короткочасне використання скомпрометованого ключа може

спричинити незворотні наслідки [22]. Тому запропоновано модель випереджального прогнозування кіберризику, яка оцінює ймовірність небезпечного результату до запуску операції та дає змогу змінити склад авторизаторів, підвищити поріг підтвердження або заблокувати виконання.

Для операції o_i у момент часу t формується вектор ризикових ознак:

$$\mathbf{X}_{R,i}(t) = \langle Q_C(t), L_i^*(t), \bar{T}_A(t), A_i(t), V_i(t), H_i(t), \Theta(t) \rangle \tag{21}$$

де $Q_C(t)$ – оцінка когнітивного контексту, $L_i^*(t)$ – критичність операції, $\bar{T}_A(t)$ – сукупна довіра до потенційних авторизаторів, $A_i(t)$ – рівень поведінкової аномальності, $V_i(t)$ – уразливість залучених криптографічних ресурсів, $H_i(t)$ – історична частота інцидентів для операцій відповідного типу, $\Theta(t)$ – інтенсивність актуальних кіберзагроз.

Прогнозовану ймовірність компрометації операції визначимо логістичною функцією:

$$P_i^{comp}(t + \Delta t) = \frac{1}{1 + exp\left[-\left(b_0 + \sum_{j=1}^{m} b_j X_{R,ij}(t)\right)\right]} \tag{22}$$

де b_0, b_j – параметри прогнозної моделі, Δt – часовий горизонт, що охоплює період від формування запиту до завершення операції.

Оскільки однакова ймовірність компрометації може мати різні наслідки для різних криптографічних дій, прогнозований ризик визначається як добуток ймовірності небезпечної події та очікуваних втрат:

$$R_i^{pr}(t + \Delta t) = P_i^{comp}(t + \Delta t) L_i^*(t) [1 - \bar{T}_A(t)] L_i^{loss} \tag{23}$$

де L_i^{loss} – нормована оцінка можливих фінансових, репутаційних, правових та інформаційних втрат унаслідок компрометації операції.

Для врахування тенденції розвитку загроз вводиться випереджальна поправка:

$$R_i^*(t + \Delta t) = \text{clip}_{[0,1]} \left[R_i^{pr}(t + \Delta t) + k \frac{R_i(t) - R_i(t - \Delta t)}{\Delta t} \right] \tag{24}$$

де $\text{clip}_{[0,1]}$ – оператор обмеження значення інтервалом [0;1], k – коефіцієнт чутливості до швидкості зміни ризику. Завдяки цьому небезпечною вважається не лише ситуація з високим поточним ризиком, а й стан із його стрімким зростанням.

Результат прогнозування подається у вигляді дискретного рівня:

$$\Lambda_i = \begin{cases} \Lambda_{low}, & R_i^* < r_1, \\ \Lambda_{medium}, & r_1 \le R_i^* < r_2, \\ \Lambda_{high}, & r_2 \le R_i^* < r_3, \\ \Lambda_{critical}, & R_i^* \ge r_3, \end{cases} \tag{25}$$

де r_1, r_2, r_3 – адаптивні пороги ризику, встановлені політикою безпеки корпоративної хмарної інформаційної системи.

Таким чином, запропонована модель переносить оцінювання ризику з реактивного на випереджальний рівень. Вона прогнозує не лише ймовірність атаки, а саме небезпеку виконання конкретної криптографічної операції з урахуванням її критичності, довіри до авторизаторів, контексту, вразливостей і динаміки загроз. Отриманий прогноз є основою для адаптивного визначення складу учасників, порога багатостороннього підтвердження та остаточного рішення щодо дозволу, додаткової перевірки, відкладення або блокування операції.

Когнітивна причинно-наслідкова модель.

Ефективність багатосторонньої авторизації визначається не окремими характеристиками користувача чи криптографічної операції, а їх взаємозалежністю [17, 19, 21]. На практиці зміна одного параметра спричиняє каскадні зміни інших: погіршення контексту знижує рівень довіри, збільшення ризику підвищує критичність операції, а висока критичність потребує більш суворої процедури підтвердження [24]. Для формалізації таких взаємозв'язків запропоновано когнітивну причинно-наслідкову модель, яка подає процес авторизації як орієнтований зважений граф взаємного впливу ключових факторів.

Когнітивний граф визначимо як:

$$G_C = \langle V, E, W \rangle \tag{26}$$

де V – множина когнітивних вершин, $E \subseteq V \times V$ – множина причинно-наслідкових зв'язків, $W = [w_{ij}]$ – матриця вагових коефіцієнтів впливу.

Множина вершин формується як:

$$V = \{Q_C, T, L, R, A, t, D\} \tag{27}$$

де Q_C – когнітивний контекст, T – інтегральний рівень довіри, L – критичність криптографічної операції, R – прогнозований кіберризик, A – склад учасників багатосторонньої авторизації, t – необхідний поріг підтвердження, D – кінцеве рішення щодо виконання операції.

Стан когнітивного графа оновлюється відповідно до співвідношення:

$$\mathbf{V}(t+1) = f(W\mathbf{V}(t) + \mathbf{U}(t)) \tag{28}$$

де $\mathbf{V}(t)$ – вектор станів вершин, W – матриця взаємного впливу, $\mathbf{U}(t)$ – вектор зовнішніх впливів (нові загрози, зміна політики безпеки, оновлення контексту); $f(\cdot)$ – нелінійна функція нормалізації.

Для кількісного оцінювання узгодженості всіх факторів вводиться інтегральний когнітивний показник:

$$K_{Cog}(t) = \sum_{i=1}^{n}\sum_{j=1}^{n} w_{ij}\, v_i(t) v_j(t) \tag{29}$$

де $v_i(t)$ – поточний стан і-ї вершини графа. Отриманий показник $K_{Cog}(t)$ характеризує узгодженість причинно-наслідкових зв'язків між контекстом, довірою, критичністю операції, прогнозованим кіберризиком, складом авторизаторів і необхідним порогом підтвердження. Надалі він використовується як одна зі складових багатокритеріальної моделі прийняття рішення.

На основі отриманого показника визначається готовність системи до виконання криптографічної операції

$$\Gamma(t) = \mu_1 T(t) + \mu_2 Q_C(t) + \mu_3[1 - R(t)] + \mu_4[1 - L(t)] + \mu_5 K_{Cog}(t), \quad \sum_{i=1}^{5} \mu_i = 1 \tag{30}$$

Чим більшим є значення $\Gamma(t)$, тим вищою є узгодженість когнітивного стану системи та безпечність виконання криптографічної операції.

На рис. 2 наведено когнітивну карту взаємозв'язків між основними складовими процесу багатосторонньої авторизації критичних криптографічних операцій. Карта відображає причинно-наслідковий вплив когнітивного контексту, рівня довіри, критичності операції та прогнозованого кіберризику на адаптивне визначення складу авторизаторів, порога підтвердження та формування остаточного рішення щодо виконання криптографічної операції. Позитивні та негативні зв'язки характеризують напрям і силу взаємного впливу між факторами, що забезпечує пояснюване прийняття рішень у запропонованій моделі.

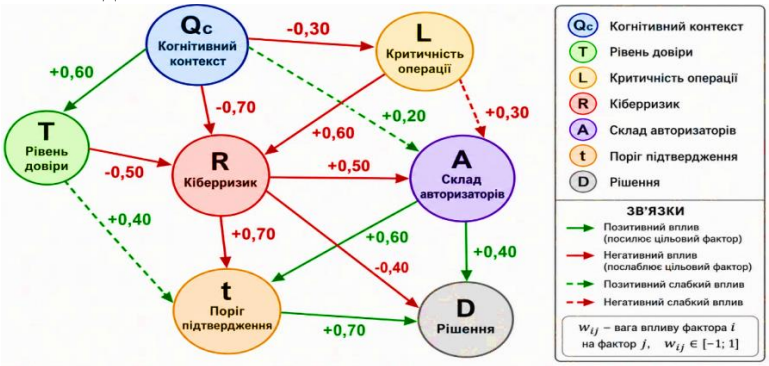

Рис. 2. Когнітивна карта причинно-наслідкових зв'язків

Таким чином, запропонована когнітивна причинно-наслідкова модель вперше об'єднує контекст, довіру, критичність, прогнозований ризик і процедуру багатосторонньої авторизації в єдину математичну систему взаємозалежних факторів. На відміну від традиційних моделей, вона враховує не лише значення окремих показників, а й причинно-наслідковий характер їх взаємного впливу, що забезпечує пояснюване, адаптивне та обґрунтоване прийняття рішень щодо виконання критичних криптографічних операцій.

Модель адаптивного визначення складу авторизаторів.

У традиційних схемах багатосторонньої авторизації склад учасників задається наперед і залишається незмінним незалежно від критичності операції, поточного ризику та рівня довіри [18]. Такий підхід створює дві протилежні проблеми: залучення надмірної кількості осіб збільшує затримку, тоді як фіксований склад може містити учасників із недостатньою довірою або спільною зоною компрометації [20-21, 24]. Для усунення цього обмеження запропоновано модель, яка автоматично формує склад авторизаторів для кожної операції.

Для потенційного авторизатора u_j визначається вектор придатності:

$$\mathbf{Z}_{ij}(t) = \langle T_j^*(t), P_{ij}(t), E_{ij}(t), Q_{C,j}(t), A_j(t), D_{ij}(t), V_j(t) \rangle \tag{31}$$

де $T_j^*(t)$ – динамічний рівень довіри, $P_{ij}(t)$ – відповідність повноважень вимогам операції, $E_{ij}(t)$ – компетентність щодо її виконання, $Q_{C,j}(t)$ – контекстна узгодженість, $A_j(t)$ – доступність учасника, $D_{ij}(t)$ – організаційна незалежність від інших авторизаторів, $V_j(t)$ – оцінка вразливості його облікового запису та пристрою.

Інтегральна придатність учасника визначається як:

$$S_{ij}(t) = \alpha_1 T_j^*(t) + \alpha_2 P_{ij}(t) + \alpha_3 E_{ij}(t) + \alpha_4 Q_{C,j}(t) + \alpha_5 A_j(t) + \alpha_6 D_{ij}(t) - \alpha_7 V_j(t), \tag{32}$$

причому $\sum_{k=1}^{7} \alpha_k = 1$.

Для виключення формально придатних, але небезпечних учасників вводиться функція допустимості:

$$G_{ij}(t) = \begin{cases} 1, & T_j^*(t) \geq T_{min}^i, \quad P_{ij} = 1, \ V_j(t) \leq V_{max}^i, \\ 0, & \text{інакше} \end{cases} \tag{33}$$

де T_{min}^i та V_{max}^i залежать від критичності й прогнозованого ризику операції.

Оптимальний склад авторизаторів визначається як:

$$A_i^*(t) = \arg\max_{A \subseteq U} \left[\sum_{u_j \in A} G_{ij}(t) S_{ij}(t) - \lambda C_A(A) - \mu K_A(A) \right] \tag{34}$$

за умов

$$|A| \geq t_i^{min}, \ \ \mathrm{Cov}_i(A) \geq P_{min}^i, \ \ \mathrm{div}(A) \geq d_{min} \tag{35}$$

де t_i^{min} – мінімально допустима кількість учасників для операції o_i, $\mathrm{Cov}_i(A)$ – рівень покриття сформованою групою повноважень, необхідних для виконання операції, P_{min}^i – мінімально допустимий рівень покриття повноважень, $C_A(A)$ – часові й обчислювальні витрати на залучення групи, $K_A(A)$ – ризик змови або спільної компрометації, $\mathrm{div}(A)$ – функціональна й організаційна різноманітність складу.

Таким чином, система обирає не просто доступних користувачів із необхідними ролями, а мінімально достатню та водночас стійку до компрометації групу. Зі зростанням критичності або ризику підвищуються вимоги до довіри, компетентності, незалежності та різноманітності авторизаторів; за нормального контексту склад автоматично скорочується без зниження рівня захищеності. Запропонована модель перетворює багатосторонню авторизацію з фіксованої організаційної процедури на контекстно-керований механізм формування колективної довіри.

Модель адаптивного визначення порога підтвердження.

У класичних порогових схемах кількість підтверджень задається наперед як $t = const$, унаслідок чого однакові вимоги застосовуються як за штатних умов, так і за підвищеного рівня кіберризику [18]. Такий підхід може створювати надлишкові часові витрати для операцій низької критичності або, навпаки, не забезпечувати достатнього рівня захисту під час виконання критичних операцій [20-21]. Для

усунення цього обмеження запропоновано адаптивне визначення порога підтвердження залежно від критичності операції, прогнозованого кіберризику, когнітивного контексту та довіри до обраного складу авторизаторів.

Базовий рівень необхідності посилення авторизації визначимо як:

$$H_i(t) = \rho_1 L_i^*(t) + \rho_2 R_i^*(t) + \rho_3[1 - Q_C(t)] + \rho_4\left[1 - \bar{T}_{A_i^*}(t)\right], \ \sum_{j=1}^{4} \rho_j = 1 \tag{36}$$

де $L_i^*(t)$ – контекстно скоригована критичність операції, $R_i^*(t)$ – прогнозований кіберризик, $Q_C(t)$ – інтегральна оцінка когнітивного контексту, $\bar{T}_{A_i^*}(t)$ – сукупна довіра до обраного складу авторизаторів, ρ_j – вагові коефіцієнти.

Адаптивний поріг підтвердження визначається як:

$$t_i^*(t) = \min\{|A_i^*(t)|, t_i^{min} + round\left[\left(t_i^{max} - t_i^{min}\right)H_i(t)\right]\} \tag{37}$$

де t_i^{min} і t_i^{max} – мінімально та максимально допустима кількість підтверджень для операції o_i, $|A_i^*|$ – кількість учасників в адаптивно сформованій групі авторизаторів, $round(\cdot)$ – оператор округлення до найближчого цілого числа. Для забезпечення виконуваності процедури багатосторонньої авторизації має виконуватися умова:

$$t_i^{min} \le t_i^*(t) \le |A_i^*| \le n_i \tag{38}$$

де n_i – загальна кількість доступних і допустимих авторизаторів для операції o_i.

Після визначення адаптивного порога виконується перевірка достатності сформованої групи авторизаторів. Якщо $|A_i^*(t)| \ge t_i^*$, система переходить до процедури збирання підтверджень. Якщо сформований склад не забезпечує необхідного порога, модель повторно формує розширену групу авторизаторів. За неможливості залучити достатню кількість допустимих і незалежних учасників операція відкладається або забороняється.

За сприятливого контексту, низького ризику та високої сукупної довіри значення $H_i(t)$ зменшується, тому поріг наближається до t_i^{min}. Зі зростанням критичності операції, погіршенням контексту, зниженням довіри або підвищенням прогнозованого ризику поріг автоматично збільшується до t_i^{max}. Якщо необхідний поріг перевищує кількість допустимих і доступних учасників, операція не може бути негайно виконана та передається на додаткову перевірку, відкладається або блокується.

Таким чином, запропонована модель замінює статичне співвідношення $t = const$ функціональною залежністю:

$$t_i^*(t) = f\left(Q_C(t), R_i^*(t), L_i^*(t), \bar{T}_{A_i^*}(t), P\right) \tag{39}$$

що забезпечує адаптивне узгодження рівня колективного підтвердження з фактичним станом корпоративної хмарної інформаційної системи.

Після формування складу авторизаторів і визначення адаптивного порога виконується збирання часткових підтверджень. Результат багатосторонньої авторизації визначається як:

$$\Psi_{A,i}(t) = \begin{cases} 1, & n_i^{conf}(t) \ge t_i^*(t), \\ 0, & n_i^{conf}(t) < t_i^*(t), \end{cases} \tag{40}$$

де $n_i^{conf}(t)$ – кількість отриманих дійсних підтверджень операції oio_ioi. Значення $\Psi_{A,i}(t) = 1$ означає досягнення необхідного порога, а $\Psi_{A,i}(t) = 0$ – недостатність підтверджень.

Багатокритеріальна модель прийняття рішення.

Заключним етапом когнітивної багатосторонньої авторизації є інтегрування всіх отриманих оцінок у єдине керуюче рішення [10, 12, 14]. На відміну від традиційних схем, де рішення залежить від виконання окремої умови або досягнення фіксованого порога, запропонована модель враховує взаємний вплив когнітивного контексту, довіри, критичності операції, прогнозованого ризику та результатів колективної авторизації [17, 19]. Це забезпечує прийняття рішення на основі сукупної оцінки стану системи.

Вектор прийняття рішення визначимо як:

$$\mathbf{Y}(t) = \langle Q_C(t), \bar{T}_A(t), L_i^*(t), R_i^*(t), K_{Cog}(t), \Psi_A(t) \rangle \tag{41}$$

де $Q_C(t)$ – когнітивний контекст, $\bar{T}_A(t)$ – інтегральна довіра до складу авторизаторів, $L_i^*(t)$ – критичність операції, $R_i^*(t)$ – прогнозований кіберризик, $K_{Cog}(t)$ – когнітивна узгодженість системи, $\Psi_A(t)$ – результат процедури багатосторонньої авторизації.

Інтегральний показник готовності до виконання операції визначається як:

$$F_D(t) = \gamma_1 Q_C(t) + \gamma_2 \bar{T}_A(t) + \gamma_3 K_{Cog}(t) + \gamma_4 \Psi_A(t) - \gamma_5 L_i^*(t) - \gamma_6 R_i^*(t) \tag{42}$$

причому $\sum_{j=1}^{6} \gamma_j = 1,\ \gamma_j \geq 0$.

Чим більшим є значення $F_D(t)$, тим вищою є впевненість у безпечному виконанні криптографічної операції.

Перед застосуванням інтегрального критерію перевіряються обов'язкові умови безпеки. Операція забороняється незалежно від значення $F_D(t)$, якщо прогнозований ризик досяг критичного рівня, підтверджено компрометацію хоча б одного обов'язкового учасника, порушено критичну політику безпеки або когнітивний контекст є недопустимим: $D_i(t) = D_4$, якщо $R_i^*(t) \geq r_3 \ \vee\ I_i^{comp}(t) = 1 \vee Q_C(t) < Q_C^{crit} \vee P_C^{\text{viol}}(t) = 1$, де $I_i^{comp}(t)$ – індикатор підтвердженої компрометації; Q_C^{crit} – критично допустимий рівень контексту; $P_C^{\text{viol}}(t)$ – індикатор порушення обов'язкової політики безпеки.

Остаточне рішення визначається правилом:

$$D_i(t) = \begin{cases} D_1, & F_D(t) \geq \delta_1, \\ D_2, & \delta_2 \leq F_D(t) < \delta_1, \\ D_3, & \delta_3 \leq F_D(t) < \delta_2, \\ D_4, & F_D(t) \geq \delta_3, \end{cases} \qquad \delta_1 > \delta_2 > \delta_3, \tag{43}$$

де D_1 – дозволити виконання операції, D_2 – вимагати додаткової авторизації або підвищити поріг підтвердження, D_3 – відкласти виконання до нормалізації контексту або появи необхідних авторизаторів, D_4 – заборонити виконання операції.

Рішення про додаткову авторизацію означає повторне формування складу $A_i^*(t)$ та збільшення порога $t_i^*(t)$. Відкладення застосовується, якщо виконання операції потенційно допустиме, але поточний контекст, доступність авторизаторів або рівень ризику не дають змоги безпечно завершити процедуру. Заборона формується у разі критичного ризику, недопустимого контексту, виявлення компрометації або невиконання обов'язкових політик безпеки.

Таким чином, запропонована багатокритеріальна модель перетворює процес авторизації із простого контролю виконання порогових умов на задачу інтегрального оцінювання когнітивного стану системи. Отримане рішення є результатом комплексного аналізу взаємозалежних факторів безпеки та забезпечує адаптивне керування виконанням критичних криптографічних операцій.

Алгоритм когнітивної багатосторонньої авторизації.

Запропоновані математичні моделі утворюють єдиний замкнений цикл когнітивної багатосторонньої авторизації, у якому кожний наступний етап використовує результати попереднього [21, 23-24]. На відміну від класичних схем порогової криптографії, запропонований алгоритм виконує не лише перевірку достатньої кількості підтверджень, а й адаптивно формує склад авторизаторів, визначає необхідний поріг підтвердження, прогнозує ризик виконання операції та приймає пояснюване рішення з урахуванням поточного когнітивного стану системи.

Загальна модель функціонування системи описується оператором:

$$\mathcal{F}_{Auth} : (O_i, U, K, C, P) \to (A_i^*, t_i^*, D_i) \tag{44}$$

де O_i – запит на виконання i-ї критичної криптографічної операції, U – множина потенційних авторизаторів, K – множина криптографічних ключів та їхніх параметрів, C – поточний контекст функціонування, P – множина політик безпеки, $A_i^*(t)$ – адаптивно сформований склад авторизаторів, $t_i^*(t)$ – необхідний поріг підтвердження, $D_i(t)$ – остаточне рішення щодо виконання операції.

Послідовність оброблення визначається рекурентною залежністю:

$$\hat{\mathbf{C}}(t) \to Q_C(t) \to T_j^*(t) \to L_j^*(t) \to R_j^*(t + \Delta t) \to K_{Cog}(t) \to A_j^*(t) \to t_j^*(t) \to \Psi_{A,i}(t) \to F_{D,i}(t) \to D_i(t) \tag{45}$$

де послідовно виконуються оцінювання когнітивного контексту, довіри, критичності операції, прогнозування ризику, формування когнітивного графа, автоматичний вибір складу авторизаторів, адаптивне визначення порога підтвердження, інтегральне оцінювання та прийняття рішення.

Загальна ефективність функціонування системи визначається як:

$$E_{Auth} = \varsigma_1 Q_{dec} + \varsigma_2 Q_{sec} + \varsigma_3 Q_{adapt} + \varsigma_4 Q_{avail} - \varsigma_5 Q_{time} - \varsigma_6 Q_{cost}, \quad \sum_{j=1}^{6} \varsigma_j = 1, \tag{46}$$

де Q_{dec} – точність авторизаційних рішень, Q_{sec} – рівень блокування небезпечних операцій, Q_{adapt} – відповідність вибраного порога поточному ризику, Q_{avail} – частка легітимних операцій, виконаних без необґрунтованого блокування, Q_{time} – нормовані часові витрати, Q_{cost} – нормовані обчислювальні й організаційні витрати, ς_j – вагові коефіцієнти відповідних етапів.

Сукупність розроблених моделей утворює інтегровану математичну модель когнітивної багатосторонньої авторизації:

$$\mathcal{M}_{Auth} = \{\mathcal{M}_C, \mathcal{M}_T, \mathcal{M}_L, \mathcal{M}_R, \mathcal{M}_{Cog}, \mathcal{M}_A, \mathcal{M}_t, \mathcal{M}_D, \mathcal{M}_{FB}\} \tag{47}$$

де $\mathcal{M}_C$ – модель когнітивного контексту, $\mathcal{M}_T$ – модель довіри, $\mathcal{M}_L$ – модель критичності, $\mathcal{M}_R$ – модель прогнозування ризику, $\mathcal{M}_{Cog}$ – когнітивна причинно-наслідкова модель, $\mathcal{M}_A$ – модель формування складу авторизаторів, $\mathcal{M}_t$ – модель адаптивного порога, $\mathcal{M}_D$ – модель прийняття рішення, $\mathcal{M}_{FB}$ – модель зворотного зв’язку.

$$S(t+1) = \mathcal{M}_{FB}\left(\mathbf{S}(t), D_i(t), Z_i^{exec}(t), I_i^{sec}(t)\right) \tag{48}$$

де Z_i^{exec} – фактичний результат виконання операції, $I_i^{sec}(t)$ – інформація про виявлені інциденти або відхилення.

Таким чином, запропонований алгоритм формалізує повний цикл прийняття рішень під час виконання критичних криптографічних операцій – від аналізу контексту до видачі кінцевого рішення. Наукова новизна алгоритму полягає в інтеграції когнітивного контексту, динамічної довіри, оцінювання критичності, прогнозування кіберризику, адаптивного формування складу авторизаторів і автоматичного визначення порога підтвердження в єдину математичну модель функціонування корпоративної хмарної системи, що забезпечує пояснюване, адаптивне та ризик-орієнтоване керування критичними криптографічними операціями.

Структурно-функціональне оцінювання запропонованої моделі.

Структурно-функціональне оцінювання запропонованої моделі проведено з метою перевірки повноти її структури, логічної узгодженості компонентів, адаптивності процедури багатосторонньої авторизації та коректності формування рішень за різних умов функціонування корпоративної хмарної інформаційної системи. На першому етапі оцінено функціональну відповідність основних компонентів моделі їх призначенню. Результати наведено в табл. 1.

Таблиця 1

Функціональна відповідність компонентів запропонованої моделі

Компонент моделі	Основне призначення
Модель контексту	Оцінювання поточного стану середовища функціонування
Модель довіри	Визначення рівня довіри до потенційних авторизаторів
Модель критичності	Оцінювання важливості криптографічної операції
Модель прогнозування ризику	Прогнозування ймовірності компрометації операції
Модель вибору авторизаторів	Формування складу учасників багатосторонньої авторизації
Модель адаптивного порога	Визначення необхідної кількості підтверджень
Модель прийняття рішення	Формування остаточного рішення щодо виконання операції
Механізм зворотного зв'язку	Оновлення параметрів моделі за результатами виконання операцій

Як видно з табл. 1, запропонована модель охоплює всі основні етапи когнітивної багатосторонньої авторизації – від аналізу контексту до формування остаточного рішення та оновлення параметрів системи. Це підтверджує функціональну повноту та логічну узгодженість її компонентів.

Для оцінювання адаптивності моделі розглянуто типові сценарії функціонування, які відображають як штатні режими роботи, так і ситуації зі зміною контексту, рівня довіри та прогнозованого кіберризику. Очікувані реакції моделі наведено в табл. 2.

Таблиця 2

Сценарії структурно-функціонального оцінювання запропонованої моделі

Сценарій	Контекст	Довіра	Ризик	Очікувана реакція
Штатна операція	високий	висока	низький	мінімальний поріг, дозволити
Критична ротація ключа	високий	висока	середній	збільшений поріг
Новий пристрій	знижений	середня	середній	додаткова авторизація
Аномальна поведінка	низький	низька	високий	відкласти або заборонити
Компрометація учасника	критичний	низька	критичний	виключити учасника, заборонити
Недоступність частини авторизаторів	допустимий	висока	низький	сформувати альтернативний склад

Структурно-функціональне оцінювання підтвердило, що запропонована модель забезпечує узгоджену взаємодію всіх функціональних компонентів та адаптивно змінює склад авторизаторів, поріг підтвердження і тип рішення відповідно до поточного контексту, рівня довіри, критичності операції та прогнозованого кіберризику. Це свідчить про функціональну повноту моделі, логічну узгодженість її компонентів і придатність до використання для багатосторонньої авторизації критичних криптографічних операцій у корпоративних хмарних інформаційних системах.

Обговорення. Запропонована модель відрізняється від існуючих підходів тим, що поєднує когнітивне моделювання, контекстне оцінювання, аналіз рівня довіри, прогнозування кіберризику та багатокритеріальне прийняття рішень у межах єдиного математичного підходу [10, 12, 14-15, 17]. На відміну від традиційних схем багатосторонньої авторизації, вона забезпечує адаптивне формування складу авторизаторів, автоматичне визначення порога підтвердження та пояснюване прийняття рішень відповідно до поточного стану корпоративного хмарного середовища [19, 21]. Це дає змогу підвищити гнучкість і обґрунтованість процедури авторизації без створення надлишкових вимог за штатних умов функціонування.

Отримані результати підтверджують доцільність інтеграції когнітивного моделювання, контекстного оцінювання, аналізу довіри та прогнозування кіберризику в єдину модель багатосторонньої авторизації критичних криптографічних операцій [23-24, 27]. На відміну від існуючих підходів, що використовують фіксований склад учасників і статичний поріг підтвердження, запропонована модель адаптивно формує склад авторизаторів та визначає необхідний рівень колективного підтвердження залежно від поточного контексту функціонування, рівня довіри, критичності операції та прогнозованого кіберризику [19-21]. Це дає змогу підвищити обґрунтованість прийняття рішень, зменшити ймовірність виконання небезпечних криптографічних операцій і водночас уникнути необґрунтованого ускладнення процедури авторизації за штатних умов. Запропонований підхід також забезпечує пояснюваність процесу прийняття рішень завдяки використанню когнітивної причинно-наслідкової моделі, що є важливою перевагою під час реалізації корпоративних хмарних криптографічних сервісів відповідно до принципів Zero Trust.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розроблено модель когнітивної багатосторонньої авторизації критичних криптографічних операцій у корпоративних хмарних інформаційних системах, яка інтегрує моделі когнітивного контексту, динамічного оцінювання довіри, оцінювання критичності операції, прогнозування кіберризику, адаптивного формування складу авторизаторів, визначення порога підтвердження та багатокритеріального прийняття рішень у межах єдиного математичного підходу. На відміну від відомих моделей, запропонований підхід забезпечує адаптивне керування процедурою багатосторонньої авторизації відповідно до поточного стану корпоративного хмарного середовища та взаємозалежності ключових факторів безпеки. Проведене структурно-функціональне оцінювання підтвердило функціональну повноту моделі, логічну узгодженість її компонентів і здатність формувати обґрунтовані рішення за різних сценаріїв функціонування.

Перспективи подальших досліджень полягають у розробленні програмної реалізації запропонованої моделі, експериментальному оцінюванні її ефективності в корпоративних хмарних

середовищах, інтеграції з пороговими постквантовими криптографічними протоколами та дослідженні можливостей використання методів машинного навчання для автоматичного налаштування вагових коефіцієнтів когнітивної моделі.

Дослідження проведено в рамках реалізації науково-дослідної теми "Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури (реєстраційний номер 0122U200483 від 06.07.2022).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tong, Y., Li, S., Wang, Z., et al. (2025). Adaptively secure, splittable, and robust threshold unsigncryption. *Cybersecurity*, *8*, Article 57. https://doi.org/10.1186/s42400-024-00344-3
2. Renisha, P. S., & Rudra, B. (2025). Quantum-safe threshold cryptography for decentralized group key management via dealerless DKG (CRYSTALS-Kyber). *Mathematics*, *13*(21), Article 3429. https://doi.org/10.3390/math13213429
3. Wang, R., Li, C., Zhang, K., et al. (2025). Zero-trust based dynamic access control for cloud computing. *Cybersecurity*, *8*, Article 12. https://doi.org/10.1186/s42400-024-00320-x
4. Jeong, E., & Yang, D. (2025). A trust score-based access control model for Zero Trust architecture: Design, sensitivity analysis, and real-world performance evaluation. *Applied Sciences*, *15*(17), Article 9551. https://doi.org/10.3390/app15179551
5. Mao, Y., Fu, W., Zhao, Y., Yuan, Z., Sun, Z., & Zhao, Y. (2025). A Zero-Trust access control model based on attribute and dynamic trust evaluation for cloud environments. *Symmetry*, *17*(12), Article 2059. https://doi.org/10.3390/sym17122059
6. Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-Trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment. *Sensors*, *25*(2), Article 550. https://doi.org/10.3390/s25020550
7. Alnaim, A. K. (2025). Adaptive Zero Trust policy management framework in 5G networks. *Mathematics*, *13*(9), Article 1501. https://doi.org/10.3390/math13091501
8. Lee, S., Huh, J.-H., & Woo, H. (2025). Security system design and verification for Zero Trust architecture. *Electronics*, *14*(4), Article 643. https://doi.org/10.3390/electronics14040643
9. Santucci, F., Oliva, G., Gonnella, M. T., Briga, M. E., Leanza, M., Massenzi, M., Faramondi, L., & Setola, R. (2025). Implementing Zero Trust: Expert insights on key security pillars and prioritization in digital transformation. *Information*, *16*(8), Article 667. https://doi.org/10.3390/info16080667
10. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2024). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. In *Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024)* (CEUR Workshop Proceedings, Vol. 3925, pp. 249-264). CEUR-WS.org.
11. Ma, Y.-W., & Chiu, P.-H. (2025). A novel risk-based access control engine in Zero Trust architecture for IoT network. *International Journal of Information Security*, *24*. https://doi.org/10.1007/s10207-025-01030-2
12. Kostiuk, Y., Skladannyi, P., Sokolov, V., & Vorokhob, M. (2025). Models and technologies of cognitive agents for decision-making with integration of artificial intelligence. In *Proceedings of the Modern Data Science Technologies Doctoral Consortium (MoDaST 2025)* (CEUR Workshop Proceedings, Vol. 4005, pp. 82-96). CEUR-WS.org.
13. Escaleira, P., Cunha, V. A., Barraca, J. P., et al. (2025). A systematic review on security mechanisms for serverless computing. *Cluster Computing*, *28*, Article 465. https://doi.org/10.1007/s10586-025-05371-4
14. Kostiuk, Y. (2025). Multi-agent system for detecting and counteracting attacks on the enterprise information system. In *Insider threats and security in corporations* (pp. 205-232). https://doi.org/10.36690/ITSC-205-232
15. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Petrenko, T. (2024). Fuzzy cognitive maps as a visualization tool for incident response scenarios in security systems. *Cybersecurity: Education, Science, Technique*, *2*(26), 417-429. https://doi.org/10.28925/2663-4023.2024.26.707
16. Musa, N. S., Murugan, T., N., N. A., et al. (2025). Research study on securing the cloud: Utilizing conventional and blockchain-based access control mechanisms. *Journal of Cloud Computing*, *14*, Article 88. https://doi.org/10.1186/s13677-025-00803-3
17. Kostiuk, Y., Skladannyi, P., Mazur, N., Rzaieva, S., Hnatchenko, D., & Honcharenko, I. (2026). Formal model of adaptive selection of cryptographic parameters for protecting communication channels 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

18. Wang, Y., Li, B., Wu, J., et al. (2025). An efficient multi-party signature for securing blockchain wallet. *Peer-to-Peer Networking and Applications, 18*, Article 137. https://doi.org/10.1007/s12083-025-01958-1
19. Skladannyi, P., Kostiuk, Y., & Rzaieva, S. (2026). Continuous access evaluation in Zero Trust access management based on security event signals and dynamic session management. *Mathematical Machines and Systems, 1*, 29-46. https://doi.org/10.34121/1028-9763-2026-1-29-46
20. Lilhore, U. K., Simaiya, S., Alroobaea, R., et al. (2025). SmartTrust: A hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust architecture. *Journal of Cloud Computing, 14*, Article 35. https://doi.org/10.1186/s13677-025-00764-7
21. Kostiuk, Y. V., Skladannyi, P. M., & Hnatchenko, D. D. (2026). Risk-adaptive authorization in Zero Trust with dynamic trust and security tokens. *Problems in Programming, 1*, 66-81. https://doi.org/10.15407/pp2026.01.066
22. Alatawi, M. N. (2025). Blockchain-driven smart contracts for advanced authorization and authentication in cloud security. *Electronics, 14*(15), Article 3104. https://doi.org/10.3390/electronics14153104
23. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In *Cybersecurity Providing in Information and Telecommunication Systems II 2024* (CEUR Workshop Proceedings, Vol. 3826, pp. 356-362). CEUR-WS.org.
24. Kostiuk, Y. V., & Skladannyi, P. M. (2026). Cryptographic trust model for security events in SIEM systems for intelligent generation of network incidents. *Modern Information Protection, 1*(65), 103-118. https://doi.org/10.31673/2409-7292.2026.011393
25. Li, Z., Du, X., Wu, X., et al. (2025). Gatac: Research on microservice access control techniques based on trust assessment and game analysis. *Cybersecurity, 8*, Article 122. https://doi.org/10.1186/s42400-025-00520-z
26. Paya, A., Vicente-García, J., & Gómez, A. (2025). Enhancing software-defined perimeters with integrated identity solutions and threat detection for robust Zero Trust security. *International Journal of Information Security, 24*, Article 178. https://doi.org/10.1007/s10207-025-01099-9
27. Calzarossa, M. C., Giudici, P., & Zieni, R. (2025). An assessment framework for explainable AI with applications to cybersecurity. *Artificial Intelligence Review, 58*, Article 150. https://doi.org/10.1007/s10462-025-11141-w

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

Yuliia Kostiuk
PhD in Computer Science, Associate Professor,
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

Rzaeva Svitlana
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-7589-2045
s.rzaieva@kubg.edu.ua

Nataliia Mazur
PhD, Associate Professor
Associate Professor of the Department of Information and
Cyber Securitynamed after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0001-7671-8287
n.mazur@kubg.edu.ua

Karyna Khorolska
PhD in Computer Science
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buryachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0003-3270-4494
k.khorolska@kubg.edu.ua

Bohdan Bebeshko
PhD in Computer Science
Associate Professor of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0001-6599-0808
b.bebeshko@kubg.edu.ua

Dmytro Hnatchenko
PhD in Computer Science,
Senior Lecturer at the Department of Software Engineering and Cybersecurity
State University of Trade and Economic, Kyiv, Ukraine
ORCID: 0000-0002-6584-4525
hnatchenko@knute.edu.ua

COGNITIVE MULTI-PARTY AUTHORIZATION MODEL FOR CRITICAL CRYPTOGRAPHIC OPERATIONS IN CORPORATE CLOUD INFORMATION SYSTEMS

Abstract. This paper presents the development of a cognitive multi-party authorization model for critical cryptographic operations in corporate cloud information systems aimed at enhancing the security of cryptographic services, improving the reliability of decision-making for critical cryptographic operations, and reducing the risk of cryptographic key compromise. Current approaches to multi-party authorization, threshold cryptography, context-aware access control, the Zero Trust concept, and decision support methods for distributed intelligent systems are analyzed. The study demonstrates that existing multi-party authorization mechanisms primarily rely on static approval rules for cryptographic operations and insufficiently account for changes in the operational context, the trust level of participating entities, the criticality of the requested

operation, the current cyber risk, and the interdependencies among security-related factors within corporate cloud environments.

A cognitive multi-party authorization model is proposed based on the integration of cognitive modeling, contextual assessment, distributed intelligent analytics, and adaptive determination of the required level of collective approval for critical cryptographic operations. A decision-making model is developed that dynamically establishes authorization requirements through the comprehensive assessment of operation criticality, trust level, cyber risk, information resource characteristics, and the current state of the corporate cloud environment. Structural and functional evaluation of the proposed model demonstrates its capability to adaptively modify the composition of authorizing participants, the authorization threshold, and the decision type in response to changes in operational context, trust level, operation criticality, and predicted cyber risk. The practical significance of the proposed model lies in its applicability to the design and implementation of secure corporate cloud information systems, cryptographic key management services, and infrastructures supporting critical cryptographic operations.

Keywords: cognitive model; multi-party authorization; corporate cloud information systems; critical cryptographic operations; distributed intelligent systems; decision support; cryptographic keys; Zero Trust.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Tong, Y., Li, S., Wang, Z., et al. (2025). Adaptively secure, splittable, and robust threshold unsigncryption. *Cybersecurity*, *8*, Article 57. https://doi.org/10.1186/s42400-024-00344-3
2. Renisha, P. S., & Rudra, B. (2025). Quantum-safe threshold cryptography for decentralized group key management via dealerless DKG (CRYSTALS-Kyber). *Mathematics, 13*(21), Article 3429. https://doi.org/10.3390/math13213429
3. Wang, R., Li, C., Zhang, K., et al. (2025). Zero-trust based dynamic access control for cloud computing. *Cybersecurity*, *8*, Article 12. https://doi.org/10.1186/s42400-024-00320-x
4. Jeong, E., & Yang, D. (2025). A trust score-based access control model for Zero Trust architecture: Design, sensitivity analysis, and real-world performance evaluation. *Applied Sciences, 15*(17), Article 9551. https://doi.org/10.3390/app15179551
5. Mao, Y., Fu, W., Zhao, Y., Yuan, Z., Sun, Z., & Zhao, Y. (2025). A Zero-Trust access control model based on attribute and dynamic trust evaluation for cloud environments. *Symmetry*, *17*(12), Article 2059. https://doi.org/10.3390/sym17122059
6. Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-Trust access control mechanism based on blockchain and inner-product encryption in the Internet of Things in a 6G environment. *Sensors, 25*(2), Article 550. https://doi.org/10.3390/s25020550
7. Alnaim, A. K. (2025). Adaptive Zero Trust policy management framework in 5G networks. *Mathematics, 13*(9), Article 1501. https://doi.org/10.3390/math13091501
8. Lee, S., Huh, J.-H., & Woo, H. (2025). Security system design and verification for Zero Trust architecture. *Electronics*, *14*(4), Article 643. https://doi.org/10.3390/electronics14040643
9. Santucci, F., Oliva, G., Gonnella, M. T., Briga, M. E., Leanza, M., Massenzi, M., Faramondi, L., & Setola, R. (2025). Implementing Zero Trust: Expert insights on key security pillars and prioritization in digital transformation. *Information*, *16*(8), Article 667. https://doi.org/10.3390/info16080667
10. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2024). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. In *Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024)* (CEUR Workshop Proceedings, Vol. 3925, pp. 249-264). CEUR-WS.org.
11. Ma, Y.-W., & Chiu, P.-H. (2025). A novel risk-based access control engine in Zero Trust architecture for IoT network. *International Journal of Information Security, 24*. https://doi.org/10.1007/s10207-025-01030-2
12. Kostiuk, Y., Skladannyi, P., Sokolov, V., & Vorokhob, M. (2025). Models and technologies of cognitive agents for decision-making with integration of artificial intelligence. In *Proceedings of the Modern Data Science Technologies Doctoral Consortium (MoDaST 2025)* (CEUR Workshop Proceedings, Vol. 4005, pp. 82-96). CEUR-WS.org.
13. Escaleira, P., Cunha, V. A., Barraca, J. P., et al. (2025). A systematic review on security mechanisms for serverless computing. *Cluster Computing, 28*, Article 465. https://doi.org/10.1007/s10586-025-05371-4

14. Kostiuk, Y. (2025). Multi-agent system for detecting and counteracting attacks on the enterprise information system. In *Insider threats and security in corporations* (pp. 205-232). https://doi.org/10.36690/ITSC-205-232
15. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Petrenko, T. (2024). Fuzzy cognitive maps as a visualization tool for incident response scenarios in security systems. *Cybersecurity: Education, Science, Technique, 2*(26), 417-429. https://doi.org/10.28925/2663-4023.2024.26.707
16. Musa, N. S., Murugan, T., N., N. A., et al. (2025). Research study on securing the cloud: Utilizing conventional and blockchain-based access control mechanisms. *Journal of Cloud Computing, 14*, Article 88. https://doi.org/10.1186/s13677-025-00803-3
17. Kostiuk, Y., Skladannyi, P., Mazur, N., Rzaieva, S., Hnatchenko, D., & Honcharenko, I. (2026). Formal model of adaptive selection of cryptographic parameters for protecting communication channels 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
18. Wang, Y., Li, B., Wu, J., et al. (2025). An efficient multi-party signature for securing blockchain wallet. *Peer-to-Peer Networking and Applications, 18*, Article 137. https://doi.org/10.1007/s12083-025-01958-1
19. Skladannyi, P., Kostiuk, Y., & Rzaieva, S. (2026). Continuous access evaluation in Zero Trust access management based on security event signals and dynamic session management. *Mathematical Machines and Systems, 1*, 29-46. https://doi.org/10.34121/1028-9763-2026-1-29-46
20. Lilhore, U. K., Simaiya, S., Alroobaea, R., et al. (2025). SmartTrust: A hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust architecture. *Journal of Cloud Computing, 14*, Article 35. https://doi.org/10.1186/s13677-025-00764-7
21. Kostiuk, Y. V., Skladannyi, P. M., & Hnatchenko, D. D. (2026). Risk-adaptive authorization in Zero Trust with dynamic trust and security tokens. *Problems in Programming, 1*, 66-81. https://doi.org/10.15407/pp2026.01.066
22. Alatawi, M. N. (2025). Blockchain-driven smart contracts for advanced authorization and authentication in cloud security. *Electronics, 14*(15), Article 3104. https://doi.org/10.3390/electronics14153104
23. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In *Cybersecurity Providing in Information and Telecommunication Systems II 2024* (CEUR Workshop Proceedings, Vol. 3826, pp. 356-362). CEUR-WS.org.
24. Kostiuk, Y. V., & Skladannyi, P. M. (2026). Cryptographic trust model for security events in SIEM systems for intelligent generation of network incidents. *Modern Information Protection, 1*(65), 103-118. https://doi.org/10.31673/2409-7292.2026.011393
25. Li, Z., Du, X., Wu, X., et al. (2025). Gatac: Research on microservice access control techniques based on trust assessment and game analysis. *Cybersecurity, 8*, Article 122. https://doi.org/10.1186/s42400-025-00520-z
26. Paya, A., Vicente-García, J., & Gómez, A. (2025). Enhancing software-defined perimeters with integrated identity solutions and threat detection for robust Zero Trust security. *International Journal of Information Security, 24*, Article 178. https://doi.org/10.1007/s10207-025-01099-9
27. Calzarossa, M. C., Giudici, P., & Zieni, R. (2025). An assessment framework for explainable AI with applications to cybersecurity. *Artificial Intelligence Review, 58*, Article 150. https://doi.org/10.1007/s10462-025-11141-w

Отримано редакцією журналу / Received: 27.01.26
Прорецензовано / Revised: 06.02.26
Схвалено до друку / Accepted: 24.09.26