КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1234
УДК 004.056.5:004.056.55

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

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

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

МОДЕЛЬ ЗАСТОСУВАННЯ ДОКАЗІВ З НУЛЬОВИМ РОЗГОЛОШЕННЯМ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОЇ АУТЕНТИФІКАЦІЇ ТА КОНТРОЛЮ ДОСТУПУ В ІНФОРМАЦІЙНО-ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ ПІДПРИЄМСТВА

Анотація. У статті досліджено проблему забезпечення конфіденційності процесів аутентифікації в інформаційно-інтелектуальних системах підприємства в умовах зростання кіберзагроз та підвищених вимог до захисту даних. У вступній частині обґрунтовано актуальність використання сучасних криптографічних підходів, що дозволяють мінімізувати передачу чутливої інформації під час підтвердження автентичності користувача. У розділі аналізу літературних джерел розглянуто підходи до побудови доказів з нульовим розголошенням, які забезпечують можливість підтвердження істинності твердження без розкриття секретних даних, зокрема лаконічні неінтерактивні аргументи знання, прозорі масштабовані аргументи знання та компактні доказові схеми без довіреної ініціалізації. Визначено їх криптографічні властивості, вимоги до моделі довіри, масштабованість і обчислювальні характеристики. У методичній частині запропоновано адаптивну модель аутентифікації, що базується на інтеграції криптографічних доказів із механізмами оцінювання ризику та аналізу контексту доступу. Формалізовано математичну модель прийняття рішень щодо доступу, яка враховує параметри користувача, характеристики середовища та рівень загроз і дозволяє динамічно обирати тип криптографічного доказу залежно від поточного рівня ризику. Розроблено алгоритм аутентифікації, який включає етапи ідентифікації, оцінювання контексту, формування доказу та його перевірки. У розділі результатів проведено порівняльний аналіз ефективності різних типів доказів з нульовим розголошенням у корпоративних інформаційних системах, оцінено їх вплив на продуктивність, рівень захисту та стійкість до атак. Показано, що використання адаптивного підходу дозволяє досягти балансу між криптографічною стійкістю та обчислювальними витратами. У висновках обґрунтовано доцільність впровадження запропонованої моделі як

складової сучасних концепцій безперервної перевірки доступу та підвищення рівня інформаційної безпеки підприємства.

Ключові слова: доказ з нульовим розголошенням; аутентифікація; криптографічні методи; управління доступом; оцінювання ризику; інформаційна безпека; конфіденційність; захист даних.

ВСТУП

Сучасний етап розвитку інформаційно-інтелектуальних систем підприємства характеризується стрімким зростанням обсягів оброблюваних даних, широким впровадженням хмарних технологій, розподілених обчислень і мобільних сервісів, що, у свою чергу, суттєво підвищує вимоги до забезпечення конфіденційності та захисту процесів аутентифікації. Традиційні підходи до підтвердження автентичності користувачів, які базуються на передачі паролів, криптографічних ключів або токенів доступу, залишаються вразливими до широкого спектра атак, зокрема перехоплення, повторного відтворення, підміни та компрометації облікових даних. У контексті сучасних кіберзагроз такі механізми вже не забезпечують належного рівня захисту інформаційних ресурсів підприємства.

Одним із перспективних напрямів підвищення рівня конфіденційності є використання криптографічних методів, що дозволяють здійснювати підтвердження істинності твердження без розкриття секретної інформації [1-2]. До таких методів належать докази з нульовим розголошенням, які набули значного поширення в системах розподілених обчислень, електронних фінансових сервісах та механізмах захисту персональних даних [5]. Використання таких підходів дозволяє усунути необхідність передачі конфіденційних даних у відкритому або навіть зашифрованому вигляді, що істотно знижує ризик їх компрометації.

Під аутентифікацією на основі доказів з нульовим розголошенням в інформаційно-інтелектуальних системах підприємства доцільно розуміти процес підтвердження автентичності користувача або правомірності його доступу до ресурсів системи без передавання чи розкриття секретних даних, на яких ґрунтується перевірка [3, 6-7]. На відміну від традиційних підходів, за яких система отримує пароль, токен, ключ або їх похідні, у такій моделі користувач формує криптографічний доказ знання певного секрету чи виконання заданої умови, а система перевіряє лише коректність цього доказу. У контексті інформаційно-інтелектуальних систем підприємства це дозволяє поєднати конфіденційне підтвердження особи з адаптивним контролем доступу, оцінюванням ризику та аналізом контексту функціонування системи.

Під конфіденційною аутентифікацією в даному дослідженні розуміється такий спосіб підтвердження особи, за якого система встановлює факт правомірності доступу без отримання відкритих або відтворюваних секретних даних користувача.

Аналіз сучасних наукових досліджень свідчить, що значна увага приділяється розробленню ефективних криптографічних схем доказів з нульовим розголошенням, зокрема лаконічних неінтерактивних аргументів знання, прозорих масштабованих аргументів знання та компактних доказових конструкцій без довіреної ініціалізації [1-2, 11]. Водночас більшість існуючих підходів орієнтована на вузькі прикладні області, такі як блокчейн-системи або спеціалізовані протоколи обміну даними, і не враховує специфіку функціонування інформаційно-інтелектуальних систем підприємства, де необхідно поєднувати високий рівень криптографічного захисту з вимогами до продуктивності, адаптивності та управління ризиками.

Незважаючи на значний прогрес у розвитку криптографічних схем доказів з нульовим розголошенням, більшість існуючих рішень характеризується статичністю вибору механізму доказу та орієнтацією на вузькоспеціалізовані середовища. Такий підхід не враховує динамічну змінність ризиків і контексту доступу, що знижує ефективність застосування зазначених методів у складних інформаційно-інтелектуальних системах підприємства та обмежує їх практичну придатність у реальних умовах функціонування.

Особливої актуальності набуває проблема побудови таких механізмів аутентифікації, які б дозволяли не лише забезпечити конфіденційність підтвердження особи, але й адаптувати рівень криптографічного захисту до поточного стану системи, контексту доступу та рівня кіберзагроз [12]. У сучасних умовах статичний вибір криптографічного механізму не забезпечує достатньої ефективності, оскільки не враховує динамічний характер ризиків і змінність середовища функціонування системи.

Наукова новизна отриманих результатів полягає у розробленні адаптивної криптографічної моделі аутентифікації, яка поєднує механізми доказів з нульовим розголошенням із формалізованим оцінюванням ризику та контексту доступу, що дозволяє здійснювати динамічний вибір типу доказу та забезпечує підвищення рівня конфіденційності й стійкості до сучасних кіберзагроз. На відміну від існуючих підходів,

запропонована модель враховує багатофакторний характер ризиків і забезпечує адаптацію криптографічного захисту в реальному часі.

Теоретичне значення роботи полягає у подальшому розвитку методів прикладної криптографії в частині інтеграції доказів з нульовим розголошенням із моделями управління ризиками та контекстно-орієнтованими механізмами контролю доступу, а також у формалізації процесу прийняття рішень щодо вибору криптографічного механізму аутентифікації.

Практичне значення отриманих результатів полягає у можливості використання запропонованої моделі для підвищення рівня захисту корпоративних інформаційно-інтелектуальних систем, зокрема у банківських установах, державних інформаційних ресурсах та розподілених мережах підприємства. Реалізація такого підходу дозволяє зменшити ризик компрометації облікових даних, підвищити ефективність систем контролю доступу та забезпечити відповідність сучасним вимогам інформаційної безпеки.

Постановка проблеми. У межах дослідження під аутентифікацією на основі доказів з нульовим розголошенням розуміється такий механізм перевірки користувача, за якого підтвердження права доступу здійснюється без розкриття секретної автентифікаційної інформації, а рішення щодо доступу може додатково враховувати рівень ризику та контекст функціонування системи.

У сучасних умовах цифровізації діяльності підприємств інформаційно-інтелектуальні системи виступають ключовим середовищем обробки, зберігання та передачі конфіденційних даних, що обумовлює підвищені вимоги до забезпечення їх інформаційної безпеки [10]. Однією з найбільш критичних складових захисту таких систем є процес аутентифікації користувачів, який визначає можливість доступу до інформаційних ресурсів і безпосередньо впливає на рівень захищеності всієї системи.

Традиційні механізми аутентифікації, що базуються на передачі секретних даних, зокрема паролів, ключів або токенів, навіть за умови використання криптографічного захисту каналів зв’язку, залишаються вразливими до сучасних типів атак. До основних загроз належать перехоплення даних, атаки повторного відтворення, компрометація облікових записів, а також використання шкідливого програмного забезпечення для отримання доступу до автентифікаційної інформації [11]. У таких умовах навіть часткове розкриття секретних даних може призвести до порушення конфіденційності та цілісності інформаційних ресурсів підприємства.

Застосування криптографічних методів, що дозволяють підтверджувати автентичність без передачі секретної інформації, відкриває нові можливості для підвищення рівня захисту [13]. Зокрема, використання доказів з нульовим розголошенням дозволяє реалізувати механізми аутентифікації, при яких користувач доводить свою автентичність без розкриття конфіденційних даних [5, 17]. Однак існуючі підходи до використання таких доказів здебільшого орієнтовані на фіксований тип криптографічної схеми та не враховують динамічний характер функціонування інформаційно-інтелектуальних систем підприємства.

У реальних умовах функціонування систем доступу рівень загроз, характеристики користувача, параметри мережевого середовища та поведінкові фактори можуть суттєво змінюватися в часі, що вимагає адаптації механізмів аутентифікації до поточного контексту [12, 16]. Відсутність механізмів динамічного вибору типу криптографічного доказу залежно від рівня ризику призводить до неефективного використання ресурсів системи або недостатнього рівня захисту [14]. З одного боку, застосування надмірно складних криптографічних схем у низькоризикових сценаріях збільшує обчислювальні витрати, а з іншого — використання спрощених механізмів у критичних умовах знижує рівень безпеки.

Таким чином, виникає науково-практична проблема розроблення адаптивного підходу до аутентифікації в інформаційно-інтелектуальних системах підприємства, який забезпечував би вибір криптографічного механізму на основі оцінювання ризику та контексту доступу [12]. Розв’язання цієї проблеми пов’язане з необхідністю інтеграції методів прикладної криптографії, моделей оцінювання ризиків та систем прийняття рішень у єдину формалізовану модель.

Вирішення зазначеної проблеми має важливе значення як для розвитку теоретичних основ побудови захищених систем доступу, так і для практичної реалізації ефективних механізмів захисту інформації в корпоративних, фінансових і державних інформаційних системах, де критичною є вимога забезпечення конфіденційності аутентифікаційних даних і стійкості до сучасних кіберзагроз.

Аналіз останніх досліджень і публікацій. Сучасні дослідження у сфері доказів з нульовим розголошенням спрямовані на розроблення ефективних криптографічних механізмів забезпечення конфіденційності в умовах розподілених та динамічних інформаційних систем. Значна частина робіт присвячена аналізу загальних властивостей таких доказів та їх застосуванню у блокчейн-середовищах. Зокрема, у роботі Diro та ін. проведено системний огляд застосування доказів з нульовим розголошенням у блокчейн-технологіях, де показано їх здатність забезпечувати верифікацію транзакцій без розкриття

конфіденційних даних [1]. Подібні результати наведено також у сучасних оглядових дослідженнях, де підкреслюється важливість таких підходів для побудови приватних і масштабованих систем обробки даних [2].

Окремий напрям досліджень пов'язаний із використанням доказів з нульовим розголошенням у системах аутентифікації. Так, у роботі Wang та ін. запропоновано легковаговий механізм аутентифікації для вбудованих пристроїв Інтернету речей, що дозволяє підтверджувати автентичність без передачі секретних даних [3]. Аналогічно, у дослідженні Zhong та ін. систематизовано підходи до побудови анонімної аутентифікації в середовищах Інтернету речей та визначено основні вимоги до їх безпеки та ефективності [4]. Водночас у цих роботах основний акцент зроблено на конкретних сценаріях застосування без урахування динамічної зміни рівня ризику та контексту доступу.

У більш нових дослідженнях увага приділяється побудові комплексних систем аутентифікації на основі доказів з нульовим розголошенням у поєднанні з технологіями блокчейн. Зокрема, у роботі Zhang та ін. запропоновано метод забезпечення безпечних транзакцій у розподілених обчислювальних середовищах, що використовує криптографічні докази для збереження конфіденційності даних [5]. У дослідженні Zhao та ін. розроблено схему міждоменної аутентифікації, яка забезпечує одночасно анонімність користувача та можливість відкликання доступу [6]. Крім того, у роботі Madine та ін. запропоновано підхід до анонімної аутентифікації користувачів у публічних і приватних блокчейн-системах, що дозволяє досягти високого рівня захисту персональних даних [7].

Паралельно з цим проводяться дослідження ефективності та практичної реалізації таких механізмів. У роботі Ansong та ін. досліджено можливості застосування протоколів доказів з нульовим розголошенням для перевірки ідентифікаційних даних, що підтверджує їх ефективність для зменшення ризику компрометації конфіденційної інформації [8]. Також у сучасних дослідженнях підкреслюється важливість використання таких підходів для забезпечення відповідності вимогам мінімізації даних та захисту приватності у цифрових ідентифікаційних системах [9].

Разом з тим, незважаючи на значну кількість досліджень, більшість існуючих підходів орієнтована на використання фіксованих криптографічних схем і не враховує динамічний характер функціонування інформаційно-інтелектуальних систем підприємства. У наявних роботах відсутні універсальні моделі, які б поєднували механізми доказів з нульовим розголошенням із формалізованим оцінюванням ризику та контексту доступу. Крім того, недостатньо дослідженим залишається питання адаптивного вибору типу криптографічного доказу залежно від поточного рівня загроз і характеристик середовища.

Отже, проведений аналіз літературних джерел показав, що існуючі дослідження формують теоретичну основу для застосування доказів з нульовим розголошенням у задачах аутентифікації та захисту даних, однак не вирішують проблему побудови адаптивних механізмів доступу для інформаційно-інтелектуальних систем підприємства. Саме усунення цієї невирішеної частини загальної проблеми і визначає напрям подальших досліджень, зокрема розроблення адаптивної моделі аутентифікації з урахуванням рівня ризику та контексту доступу.

Мета статті. Метою статті є розроблення адаптивної моделі аутентифікації на основі доказів з нульовим розголошенням для інформаційно-інтелектуальних систем підприємства, яка забезпечує підвищення рівня конфіденційності та стійкості до сучасних кіберзагроз шляхом динамічного вибору криптографічного механізму залежно від рівня ризику, контексту доступу та характеристик середовища функціонування системи [11]. Досягнення поставленої мети передбачає проведення комплексного аналізу сучасних підходів до побудови доказів з нульовим розголошенням і їх застосування в задачах аутентифікації, дослідження особливостей використання криптографічних доказів у інформаційно-інтелектуальних системах підприємства [4, 15], формалізацію моделі прийняття рішень щодо доступу з урахуванням рівня ризику та контекстних параметрів [12, 16], а також розроблення алгоритму адаптивної аутентифікації, що забезпечує вибір оптимального типу доказу залежно від умов функціонування системи. [14] Важливою складовою дослідження є також оцінювання ефективності запропонованого підходу з позицій забезпечення інформаційної безпеки та оптимізації обчислювальних витрат, що дозволяє обґрунтувати доцільність його практичного впровадження у корпоративних інформаційно-інтелектуальних системах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Враховуючи проведений аналіз сучасних підходів до використання доказів з нульовим розголошенням та виявлені обмеження існуючих рішень, пов'язані з відсутністю адаптивності до рівня ризику та контексту доступу, виникає необхідність розроблення узагальненої моделі аутентифікації для інформаційно-інтелектуальних систем підприємства [15, 17, 19]. Така модель повинна забезпечувати не

лише конфіденційність підтвердження автентичності користувача, але й динамічну зміну рівня криптографічного захисту залежно від поточного стану системи.

Запропонований підхід ґрунтується на інтеграції механізмів доказів з нульовим розголошенням із моделями оцінювання ризику та контекстно-орієнтованого доступу [18, 20]. Це дозволяє формалізувати процес прийняття рішення щодо аутентифікації як багатофакторну задачу, в якій вибір криптографічного механізму визначається сукупністю параметрів користувача, середовища та рівня загроз.

У подальшому викладі наведено формалізацію запропонованої моделі, розроблено алгоритмічне забезпечення процесу аутентифікації, а також виконано оцінювання ефективності запропонованого підходу на основі чисельного експерименту.

Формалізація адаптивної моделі аутентифікації

У роботі аутентифікація на основі доказів з нульовим розголошенням розглядається як формалізований процес прийняття рішення щодо доступу, у якому користувач підтверджує свою автентичність за допомогою криптографічного доказу без розкриття секрету [25], а система вибирає рівень захисту залежно від ризику та контексту доступу.

Запропонована модель аутентифікації спрямована на забезпечення конфіденційності доступу до інформаційно-інтелектуальних систем підприємства шляхом використання доказів з нульовим розголошенням у поєднанні з адаптивним механізмом оцінювання ризику. Загальна модель прийняття рішення щодо доступу формалізується як функція:

$$A(t) = f(U, C, R, Z), \tag{1}$$

де $A(t)$ – рішення щодо доступу у момент часу t, U – множина параметрів користувача, C – контекст доступу, R – рівень ризику, Z – тип криптографічного доказу. Дана залежність відображає інтеграцію криптографічних і поведінкових факторів у єдину модель аутентифікації [12, 26]. Для подальшої деталізації моделі необхідно формалізувати складові ризику, оскільки саме вони визначають вибір криптографічного механізму.

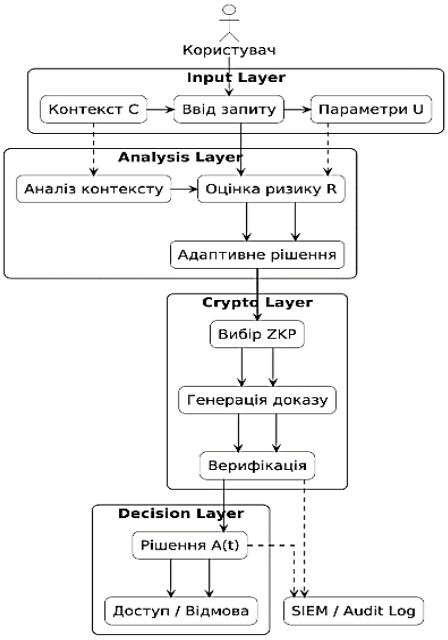

Рис. 1. Архітектура адаптивної моделі аутентифікації на основі доказів з нульовим розголошенням

На рис. 1 подано архітектуру адаптивної моделі аутентифікації на основі доказів з нульовим розголошенням, яка реалізована у вигляді багаторівневої структури. На рівні Input Layer здійснюється формування запиту та збір параметрів користувача U і контексту доступу C. У Analysis Layer виконується оцінювання ризику R та аналіз контексту, на основі яких формується адаптивне рішення щодо рівня захисту. Crypto Layer забезпечує вибір типу криптографічного доказу, його генерацію та верифікацію. На рівні Decision Layer формується рішення $A(t)$ про надання або відмову в доступі. Додатково передбачено журналювання подій у SIEM/Audit Log для подальшого моніторингу та аудиту безпеки.

У запропонованій моделі контроль доступу розглядається як логічне продовження конфіденційної аутентифікації, за якого результат перевірки криптографічного доказу доповнюється оцінюванням ризику

та контексту середовища [11, 19]. Це дозволяє приймати рішення не лише щодо підтвердження особи, але й щодо допустимого рівня доступу до інформаційних ресурсів підприємства.

Запропонована залежність дозволяє розглядати процес аутентифікації як динамічну систему прийняття рішень, у якій кожен із параметрів впливає на рівень довіри до користувача [20]. Особливістю моделі є те, що вона не обмежується лише криптографічною перевіркою, а враховує поведінкові та контекстні характеристики [15, 18]. Це забезпечує можливість підвищення рівня захисту без необхідності передачі додаткових конфіденційних даних. Таким чином, модель виступає узагальненим механізмом інтеграції криптографії та аналізу ризиків у системах доступу.

Модель оцінювання ризику доступу

Рівень ризику визначається як зважена сума окремих факторів, що характеризують стан користувача та середовища:

$$R(t) = \sum_{i=1}^{n} w_i \cdot r_i(t), \tag{2}$$

де $r_i(t)$ – часткові показники ризику (поведінкові аномалії, геолокація, тип пристрою, мережеві параметри), w_i – коефіцієнти їх вагомості. Такий підхід дозволяє врахувати багатофакторну природу кіберзагроз [12, 26]. Нормалізація отриманого значення ризику дозволяє привести його до уніфікованої шкали та забезпечити можливість подальшого використання в алгоритмах прийняття рішень [14]. Такий підхід підвищує чутливість моделі до змін у поведінці користувача та параметрах середовища, що є критично важливим в умовах динамічних кіберзагроз. Отриманий показник ризику використовується як ключовий критерій для адаптивного вибору рівня криптографічного захисту та формування рішення щодо доступу.

З метою уніфікації значення ризику нормалізується до інтервалу [0;1]:

$$R_n(t) = \frac{R(t)}{R_{max}}, \tag{3}$$

де R_{max} – максимально можливе значення ризику. Нормалізований показник $R_n(t)$ використовується для прийняття рішень щодо рівня захисту [16]. Такий підхід забезпечує порівнюваність значень ризику в різних сценаріях функціонування системи та спрощує встановлення порогових рівнів для прийняття рішень. Крім того, використання нормалізованого показника дозволяє підвищити стабільність роботи моделі та адаптивність механізму вибору криптографічного захисту.

На рис. 2 подано алгоритм адаптивної аутентифікації користувача, який починається з введення запиту та збору параметрів користувача і контексту доступу. Далі паралельно виконуються оцінювання рівня ризику та аналіз контексту середовища. На основі отриманого рівня ризику здійснюється адаптивний вибір типу криптографічного доказу. Після цього виконується генерація доказу, контроль контексту та його верифікація. За результатами перевірки формується рішення щодо надання або відмови в доступі, а всі події реєструються у журналі SIEM.

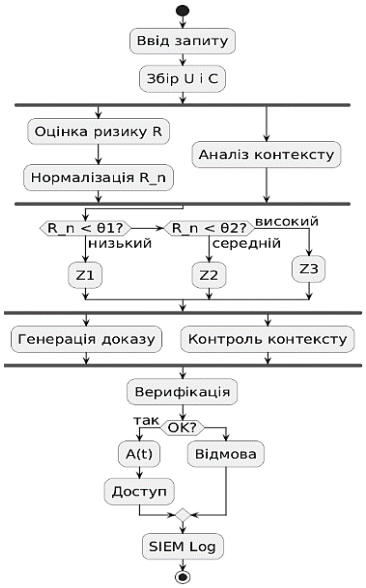

Рис. 2. Алгоритм адаптивної аутентифікації користувача

На рис. 2 подано алгоритм адаптивної аутентифікації користувача, який включає введення даних, збір параметрів користувача і контексту, розрахунок рівня ризику, вибір типу криптографічного доказу, його генерацію, перевірку та прийняття рішення щодо надання або відмови в доступі.

Запропонований підхід до оцінювання ризику дозволяє враховувати не лише статичні параметри користувача, але й динамічні зміни його поведінки та середовища функціонування. Це є критично важливим у сучасних умовах, коли атаки мають адаптивний характер і можуть змінювати свої параметри в реальному часі [21, 23]. Нормалізація ризику забезпечує уніфікацію оцінювання та дозволяє використовувати єдині порогові значення для прийняття рішень. Отриманий показник виступає ключовим елементом у механізмі адаптивного вибору криптографічного доказу.

Формалізація контексту доступу

Контекст доступу визначається як множина параметрів, що описують середовище функціонування системи:

$$C = (c_1, c_2, \dots, c_m), \tag{4}$$

де c_j – окремі контекстні характеристики (час доступу, IP-адреса, тип пристрою, мережеве середовище) [12, 16]. Для оцінювання надійності контексту вводиться функція довіри:

$$T_c = \sum_{j=1}^{m} a_j \cdot c_j, \tag{5}$$

де a_j – коефіцієнти значущості відповідних параметрів. Значення T_c характеризує рівень довіри до поточного середовища доступу і використовується разом із ризиком для прийняття рішення.

Врахування контексту доступу дозволяє підвищити точність оцінювання ризику за рахунок аналізу умов, у яких здійснюється аутентифікація [16]. На відміну від класичних моделей, де враховується лише ідентифікаційна інформація, запропонований підхід дозволяє враховувати зовнішні фактори, що можуть свідчити про потенційні загрози [23]. Це особливо важливо для виявлення аномальних ситуацій, які не пов'язані безпосередньо з компрометацією облікових даних [21]. Таким чином, показник довіри до контексту виступає додатковим параметром стабілізації системи.

Адаптивний вибір криптографічного механізму

Ключовою особливістю запропонованої моделі є динамічний вибір типу доказу залежно від рівня ризику [13, 17]. Формально це описується наступним чином:

$$Z = \begin{cases} Z_1, & R_n < \theta_1 \\ Z_2, & \theta_1 \le R_n < \theta_2, \\ Z_3, & R_n \ge \theta_2 \end{cases} \tag{6}$$

де Z_1, Z_2, Z_3 – різні типи доказів з нульовим розголошенням, що відрізняються за рівнем криптографічної стійкості та обчислювальною складністю, θ_1, θ_2 – порогові значення ризику. Такий підхід дозволяє використовувати менш ресурсоємні схеми при низькому ризику та більш стійкі – при високому. У практичній Z_1, Z_2, Z_3 можуть відповідати криптографічним доказам, що відрізняються за рівнем обчислювальної складності, швидкістю перевірки та стійкістю до атак [25]. Це дозволяє розглядати запропоновану модель як універсальну основу для адаптивного застосування різних класів доказів з нульовим розголошенням у корпоративних системах.

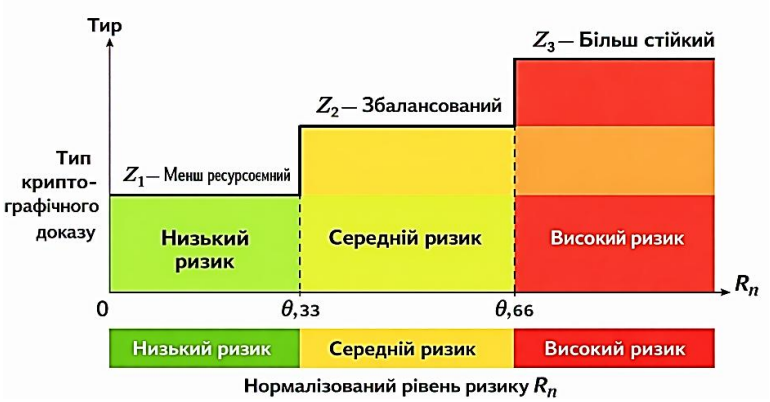

Рис. 3. Залежність вибору типу криптографічного доказу від рівня ризику

Рис. 3 відображає залежність вибору типу криптографічного доказу від рівня ризику та демонструє адаптивний характер запропонованого підходу. Із зростанням рівня ризику система послідовно переходить від використання менш ресурсоємних доказів до більш складних і криптографічно стійких механізмів. У зоні низького ризику застосовується спрощений доказ, що дозволяє мінімізувати обчислювальні витрати та забезпечити високу продуктивність системи. При підвищенні ризику система переходить до збалансованого механізму, який поєднує прийнятний рівень захисту з помірними витратами ресурсів. У разі високого рівня ризику обирається найбільш стійкий криптографічний доказ, що забезпечує максимальний рівень захисту навіть за рахунок збільшення обчислювального навантаження. Таким чином, представлений графік ілюструє логіку динамічного підвищення рівня криптографічного захисту відповідно до зміни умов функціонування системи та рівня загроз, що дозволяє досягти раціонального балансу між безпекою і продуктивністю.

Такий механізм дозволяє забезпечити гнучке управління рівнем криптографічного захисту залежно від умов функціонування системи. У низькоризикових сценаріях це дозволяє зменшити обчислювальні витрати, тоді як у високоризикових – підвищити стійкість до атак [11, 19]. Важливою перевагою є можливість масштабування системи без зміни її архітектури [20]. Таким чином, адаптивність вибору доказу є ключовим фактором підвищення ефективності аутентифікації.

Для оцінювання обчислювальних витрат вводиться функція складності:

$$Comp(Z) = \beta_1 \cdot t_g + \beta_2 \cdot t_v, \tag{7}$$

де t_g – час генерації доказу, t_v – час його перевірки, β_1, β_2 – вагові коефіцієнти. Це дозволяє враховувати продуктивність системи при виборі механізму.

Ймовірнісна модель безпеки аутентифікації

Ймовірність успішної аутентифікації визначається як доповнення до ймовірності атаки:

$$P_{auth} = 1 - P_{attack}, \tag{8}$$

де P_{attack} – ймовірність компрометації процесу аутентифікації. Вона, у свою чергу, залежить від рівня ризику та контексту:

$$P_{attack} = \phi(R_n, T_c), \tag{9}$$

де $\phi(\cdot)$ – функція, що відображає залежність між ризиком, довірою до контексту та ймовірністю атаки. Зі зростанням R_n та зниженням T_c значення P_{attack} зростає.

Використання ймовірнісного підходу дозволяє перейти від детермінованих моделей безпеки до більш гнучких і реалістичних оцінок [20]. Це дає можливість враховувати невизначеність і варіативність поведінки як користувача, так і зловмисника [23]. Отримана залежність може бути використана для прогнозування можливих атак і попередження їх реалізації. Таким чином, модель забезпечує не лише реактивний, але й проактивний захист.

Інтегральна оцінка рівня безпеки

Загальний рівень захищеності системи визначається інтегральним показником:

$$S = \gamma_1 \cdot (1 - R_n) + \gamma_2 \cdot T_c, \tag{10}$$

де γ_1, γ_2 – коефіцієнти вагомості. Формула дозволяє комплексно оцінити безпеку системи з урахуванням ризику та контексту.

Рис. 4 відображає залежність інтегрального показника безпеки від рівня ризику та довіри до контексту доступу у вигляді тривимірної поверхні, що дозволяє комплексно оцінити стан захищеності інформаційно-інтелектуальної системи підприємства. Зі збільшенням рівня ризику значення інтегрального показника безпеки поступово знижується, що обумовлено зростанням ймовірності реалізації кіберзагроз, тоді як підвищення рівня довіри до контексту доступу, навпаки, сприяє зростанню рівня безпеки за рахунок більш сприятливих умов функціонування системи. Найвищі значення інтегрального показника спостерігаються у зоні поєднання низького ризику та високої довіри, де система працює у стабільному та контрольованому середовищі, тоді як мінімальні значення відповідають сценаріям високого ризику та низької довіри, що характеризуються підвищеною вразливістю до атак. Таким чином, представлений графік наочно демонструє взаємозалежність між ризиком, контекстом доступу та рівнем захищеності,

підтверджуючи доцільність використання інтегрального показника для прийняття управлінських рішень у системах аутентифікації та контролю доступу.

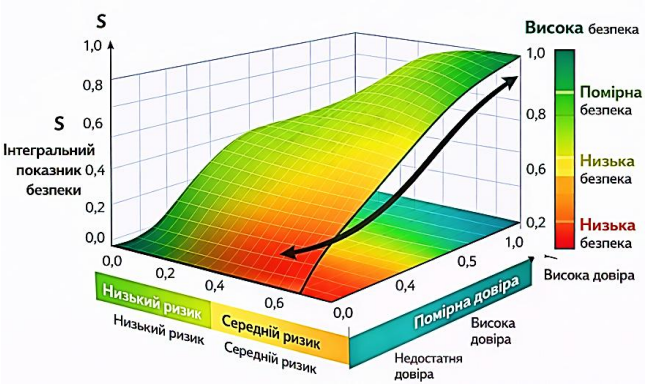

Рис. 4. Залежність інтегрального показника безпеки від рівня ризику та довіри до контексту

Інтегральний показник дозволяє отримати узагальнену оцінку рівня захищеності системи, що є зручним для прийняття управлінських рішень [26]. Він поєднує як ризикові, так і контекстні характеристики, що забезпечує більш повне відображення стану системи. Такий підхід дозволяє швидко оцінити ефективність функціонування механізму аутентифікації [23, 25]. Крім того, він може бути використаний для моніторингу змін у системі в реальному часі.

Оцінка ефективності запропонованої моделі

Ефективність адаптивної моделі визначається через зміну рівня ризику до та після її застосування:

$$E = 1 - \frac{R_{\text{after}}}{R_{before}}, \tag{11}$$

де R_{before} – початковий рівень ризику, R_{after} – ризик після впровадження моделі. Значення E показує відносне зниження ризику.

З урахуванням обчислювальних витрат вводиться узагальнений показник ефективності:

$$E_{total} = \lambda_1 S + \lambda_2 (1 - Comp(Z)), \tag{12}$$

де λ_1, λ_2 – коефіцієнти, що визначають баланс між безпекою та продуктивністю. Це дозволяє оцінити доцільність використання конкретного типу доказу в заданих умовах.

Запропонований показник ефективності дозволяє оцінити не лише рівень безпеки, але й витрати на реалізацію криптографічного механізму. Це є важливим для практичного впровадження системи, оскільки дозволяє враховувати обмеження ресурсів. Баланс між безпекою та продуктивністю є ключовим критерієм для сучасних інформаційних систем [22, 24]. Отриманий показник може використовуватися для оптимізації параметрів системи аутентифікації.

Чисельний експеримент з оцінювання ефективності адаптивної моделі аутентифікації

Для перевірки працездатності запропонованої адаптивної моделі аутентифікації на основі доказів з нульовим розголошенням проведено чисельний експеримент, метою якого є оцінювання впливу рівня ризику та контексту доступу на вибір криптографічного механізму, обчислювальні витрати та загальний рівень безпеки інформаційно-інтелектуальної системи підприємства [24]. Експериментальне дослідження побудовано у вигляді імітаційного моделювання трьох типових сценаріїв доступу: низькоризикового, середньоризикового та високоризикового.

Для побудови експерименту використано нормалізовану шкалу ризику $R_n \in [0; 1]$, показник довіри до контексту $T_c \in [0; 1]$, функцію складності криптографічного доказу $Comp(Z)$, інтегральний показник безпеки S та узагальнений показник ефективності E_{total}. У межах моделі прийнято, що при низькому рівні ризику використовується компактний доказ типу Z_1, при середньому – більш збалансований за безпекою і швидкодією механізм Z_2, а при високому – найбільш стійкий, хоча й більш ресурсоємний механізм Z_3.

Для чисельного моделювання використано порогові значення $\theta_1 = 0{,}35$ та $\theta_2 = 0{,}70$. Це означає, що при $R_n < 0{,}35$ система обирає перший тип доказу, при $0{,}35 \le R_n < 0{,}70$ – другий, а при $R_n \ge 0{,}70$ – третій. Обрані порогові значення визначено на основі узагальнення типових рівнів ризику в корпоративних інформаційних системах та забезпечення рівномірного розподілу сценаріїв за рівнями загроз.

Для інтегральної оцінки рівня безпеки у формулі (10) прийнято вагові коефіцієнти $\gamma_1 = 0{,}6$ і $\gamma_2 = 0{,}4$, що відображає більший вплив ризику порівняно з контекстом доступу. Для узагальненого показника ефективності у формулі (12) використано $\lambda_1 = 0{,}7$ і $\lambda_2 = 0{,}3$, оскільки для системи аутентифікації пріоритетним є рівень безпеки, а не лише швидкодія.

Для оцінювання складності доказу використано спрощену нормалізовану модель, у якій $Comp(Z)$ задається в інтервалі [0;1]: для механізму Z_1 – 0,25, для Z_2 – 0,50, для Z_3 – 0,80. Таке припущення відображає зростання витрат на генерацію та перевірку доказу при переході до більш стійких криптографічних схем.

У першому сценарії розглядався доступ із довіреного середовища, для якого прийнято $R_n = 0{,}22$ та $T_c = 0{,}88$. За правилом (6) система обирає доказ типу Z_1. Інтегральний рівень безпеки, обчислений за формулою (10), становить $S = 0{,}820$, а узагальнений показник ефективності за формулою (12) – $E_{total} = 0{,}799$. Отримані значення свідчать про високу ефективність моделі в умовах низького ризику за рахунок мінімальних обчислювальних витрат.

У другому сценарії, що відповідає середньому рівню ризику ($R_n = 0{,}56$, $T_c = 0{,}63$), система переходить до використання доказу типу Z_2. При цьому інтегральний рівень безпеки становить $S = 0{,}516$, а узагальнений показник ефективності – $E_{total} = 0{,}511$. Це демонструє зниження ефективності порівняно з низькоризиковим сценарієм, однак підтверджує досягнення балансу між рівнем захисту та складністю криптографічного механізму.

Отримане значення є істотно нижчим, що відображає закономірне зростання витрат і зниження загальної ефективності в умовах підвищеного ризику. Однак саме в цьому сценарії система забезпечує максимальний рівень криптографічного захисту, що є виправданим з позиції інформаційної безпеки.

Для високоризикового сценарію ($R_n = 0{,}84$ та $T_c = 0{,}28$) система використовує доказ типу Z_3, що характеризується максимальною криптографічною стійкістю. При цьому інтегральний рівень безпеки становить $S = 0{,}208$, а узагальнений показник ефективності – $E_{total} = 0{,}206$. Незважаючи на зниження ефективності, такий результат є обґрунтованим, оскільки пріоритетним у цьому випадку є забезпечення максимального рівня захисту. Кількісні результати моделювання для кожного сценарію узагальнено в табл. 1.

Таблиця 1

Результати чисельного експерименту для різних сценаріїв доступу

Сценарій	R_n	T_c	Обраний тип доказу	$Comp(Z)$	S	E_{total}
Низькоризиковий доступ	0,22	0,88	Z_1	0,25	0,820	0,799
Середньоризиковий доступ	0,56	0,63	Z_2	0,50	0,516	0,511
Високоризиковий доступ	0,84	0,28	Z_3	0,80	0,208	0,206

Аналіз отриманих результатів показує, що запропонована модель коректно адаптує тип криптографічного доказу до поточного рівня загроз. При низькому ризику система використовує менш ресурсоємний механізм, що забезпечує високу ефективність без надлишкових витрат. При середньому ризику відбувається перехід до більш стійкої схеми, яка знижує загальну ефективність, але підвищує криптографічну надійність. При високому ризику система обирає найбільш захищений механізм, що супроводжується зростанням обчислювальних витрат, однак саме така поведінка є обґрунтованою з точки зору безпечного доступу до критичних ресурсів підприємства.

Рис. 5 демонструє порівняння ефективності адаптивної та статичної моделей аутентифікації за різних рівнів ризику та довіри до контексту. Адаптивна модель у всіх сценаріях забезпечує вищі значення ефективності, особливо в умовах низького ризику, де досягається раціональне використання ресурсів. У міру зростання ризику ефективність знижується для обох моделей, однак адаптивний підхід зберігає перевагу завдяки динамічному вибору більш стійких криптографічних механізмів, що забезпечує кращий баланс між безпекою та продуктивністю.

Рис. 5. Порівняння ефективності адаптивної та статичної моделей аутентифікації

Для додаткового порівняння оцінено запропонований адаптивний підхід відносно статичної схеми, у якій використовується фіксований тип криптографічного доказу незалежно від рівня ризику. Встановлено, що для низькоризикового сценарію узагальнений показник ефективності статичного підходу є нижчим порівняно з адаптивним (0,724 проти 0,799), що свідчить про нераціональне використання обчислювальних ресурсів у безпечних умовах.

Водночас у високоризикових сценаріях статичний підхід не забезпечує достатнього рівня криптографічного захисту, оскільки не передбачає переходу до більш стійких механізмів, що знижує надійність аутентифікації. Це підтверджує, що фіксований вибір криптографічного доказу не відповідає динамічному характеру сучасних кіберзагроз.

Порівняльний аналіз показав, що використання адаптивної моделі дозволяє підвищити ефективність аутентифікації більш ніж на 10% у низькоризикових умовах при одночасному забезпеченні необхідного рівня безпеки в критичних сценаріях. Таким чином, запропонований підхід забезпечує раціональний баланс між конфіденційністю, криптографічною стійкістю та обчислювальною ефективністю, що обґрунтовує доцільність його використання в інформаційно-інтелектуальних системах підприємства.

Отже, результати чисельного експерименту підтвердили, що запропонована адаптивна модель аутентифікації на основі доказів з нульовим розголошенням забезпечує ефективне управління процесом доступу залежно від рівня ризику та контексту середовища. Встановлено, що використання адаптивного підходу дозволяє підвищити ефективність аутентифікації більш ніж на 10% у низькоризикових сценаріях та одночасно забезпечити необхідний рівень криптографічної стійкості у критичних умовах. На відміну від статичних схем, запропонована модель забезпечує динамічну зміну рівня захисту, що дозволяє досягти раціонального балансу між конфіденційністю, безпекою та обчислювальною ефективністю, що обґрунтовує доцільність її використання в інформаційно-інтелектуальних системах підприємства.

Обговорення. Отримані результати свідчать про доцільність використання адаптивного підходу до аутентифікації на основі доказів з нульовим розголошенням у інформаційно-інтелектуальних системах підприємства. На відміну від традиційних моделей, у яких застосовується фіксований криптографічний механізм, запропонована модель забезпечує динамічну зміну рівня захисту залежно від поточного рівня ризику та характеристик контексту доступу. Це дозволяє не лише підвищити рівень конфіденційності, але й оптимізувати використання обчислювальних ресурсів системи.

Порівняння з існуючими підходами показує, що більшість сучасних рішень у сфері аутентифікації на основі доказів з нульовим розголошенням орієнтовані на використання одного типу криптографічного доказу без урахування змінності середовища [23, 25]. Такий підхід є ефективним у статичних або вузькоспеціалізованих системах, проте в умовах динамічних кіберзагроз він не забезпечує необхідного рівня гнучкості. Запропонована модель усуває цей недолік за рахунок інтеграції механізмів оцінювання ризику та контекстно-орієнтованого доступу, що дозволяє адаптувати криптографічний захист у реальному часі.

Особливу увагу слід звернути на отриманий ефект підвищення ефективності аутентифікації у низькоризикових сценаріях. Це свідчить про те, що адаптивний підхід дозволяє уникнути використання надмірно складних криптографічних механізмів там, де це не є необхідним, що зменшує навантаження на систему. Водночас у високоризикових умовах модель забезпечує перехід до більш стійких механізмів, що

підвищує рівень захисту навіть за рахунок збільшення обчислювальних витрат. Таким чином, досягається раціональний компроміс між безпекою та продуктивністю.

Разом з тим, запропонований підхід має певні обмеження. Зокрема, точність оцінювання ризику залежить від якості вхідних даних та правильності визначення вагових коефіцієнтів, що може впливати на вибір криптографічного механізму. Крім того, у роботі використано узагальнену модель оцінювання складності доказів, яка не враховує специфіку конкретних реалізацій криптографічних протоколів [22, 24]. Це може призводити до відхилень між теоретичними та практичними результатами.

Перспективним напрямом подальших досліджень є вдосконалення моделей оцінювання ризику з використанням методів машинного навчання та поведінкового аналізу, що дозволить підвищити точність прийняття рішень. Також доцільним є проведення експериментальних досліджень на реальних корпоративних системах з урахуванням різних типів криптографічних доказів і навантажень. Окремої уваги потребує оптимізація обчислювальних витрат для ресурсно обмежених середовищ, зокрема мобільних і вбудованих систем.

Практична реалізація запропонованого підходу є доцільною в системах доступу до корпоративних сховищ даних, фінансових модулів, сервісів електронного документообігу та аналітичних платформ підприємства, де особливо важливо мінімізувати передачу автентифікаційних секретів. У таких системах адаптивний вибір криптографічного доказу дозволяє одночасно забезпечити конфіденційність доступу та оптимізувати навантаження на обчислювальну інфраструктуру.

Отже, результати дослідження підтверджують, що адаптивна модель аутентифікації на основі доказів з нульовим розголошенням є перспективним напрямом розвитку систем інформаційної безпеки підприємства. Запропонований підхід дозволяє підвищити рівень конфіденційності, забезпечити гнучкість управління доступом та адаптувати механізми захисту до умов функціонування системи, що відповідає сучасним вимогам до кібербезпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті вирішено науково-практичне завдання розроблення адаптивної моделі аутентифікації для інформаційно-інтелектуальних систем підприємства на основі доказів з нульовим розголошенням. Запропонований підхід, на відміну від існуючих рішень, забезпечує динамічний вибір криптографічного механізму залежно від рівня ризику та контексту доступу, що дозволяє підвищити ефективність процесу аутентифікації та рівень конфіденційності передавання даних.

У результаті дослідження сформалізовано модель прийняття рішень щодо доступу, яка інтегрує параметри користувача, характеристики середовища та оцінювання ризику в єдину систему. Розроблено алгоритм адаптивної аутентифікації, що забезпечує гнучке управління рівнем криптографічного захисту без розкриття конфіденційної інформації. Проведений чисельний експеримент підтвердив працездатність запропонованої моделі та показав, що її використання дозволяє підвищити ефективність аутентифікації більш ніж на 10% у низькоризикових сценаріях при одночасному забезпеченні необхідного рівня безпеки у критичних умовах.

Наукова новизна отриманих результатів полягає у поєднанні механізмів доказів з нульовим розголошенням із формалізованим оцінюванням ризику та контексту доступу, що забезпечує адаптивність криптографічного захисту в умовах динамічних кіберзагроз. Практичне значення роботи полягає у можливості застосування запропонованої моделі в корпоративних інформаційно-інтелектуальних системах, де необхідно забезпечити високий рівень захисту при обмежених обчислювальних ресурсах.

До основних переваг запропонованого підходу належать підвищення рівня конфіденційності аутентифікації, зниження ризику компрометації облікових даних, а також забезпечення балансу між криптографічною стійкістю та продуктивністю системи. Разом з тим, ефективність моделі залежить від якості оцінювання ризику та правильності визначення параметрів системи, що обумовлює необхідність подальшого вдосконалення відповідних методів.

Перспективи подальших досліджень пов’язані з розширенням запропонованої моделі за рахунок використання методів машинного навчання для адаптивного оцінювання ризику та поведінкового аналізу користувачів, що дозволить підвищити точність прийняття рішень. Доцільним є також проведення експериментальної апробації моделі в реальних корпоративних системах з урахуванням різних типів навантажень і сценаріїв атак. Окремим напрямом є оптимізація обчислювальних витрат криптографічних доказів для застосування у ресурсно обмежених середовищах, зокрема мобільних і вбудованих системах, а також інтеграція запропонованого підходу з сучасними концепціями безперервної перевірки доступу.

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. Diro, A., Zhou, L., Saini, A., Kaisar, S., & Pham, H. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. Journal of Information Security and Applications, 80, 103678. https://doi.org/10.1016/j.jisa.2023.103678
2. Lavin, R., Liu, X., Mohanty, H., Norman, L., Zaarour, G., & Krishnamachari, B. (2024). A survey on the applications of zero-knowledge proofs. arXiv. https://doi.org/10.48550/arXiv.2408.00243
3. Wang, Z., Huang, J., Miao, K., Lv, X., Chen, Y., Su, B., Liu, L., & Han, M. (2023). Lightweight zero-knowledge authentication scheme for IoT embedded devices. Computer Networks, 236, 110021. https://doi.org/10.1016/j.comnet.2023.110021
4. Zhong, J., He, S., Liu, Z., & Xiong, L. (2025). Lightweight anonymous authentication for IoT: A taxonomy and survey of security frameworks. Sensors, 25(17), 5594. https://doi.org/10.3390/s25175594
5. Zhang, B., Pan, H., Li, K., Xing, Y., Wang, J., Fan, D., & Zhang, W. (2024). A blockchain and zero knowledge proof based data security transaction method in distributed computing. Electronics, 13(21), 4260. https://doi.org/10.3390/electronics13214260
6. Zhao, X., Xia, F., Xia, H., Mao, Y., & Chen, S. (2024). A zero-knowledge-proof-based anonymous and revocable scheme for cross-domain authentication. Electronics, 13(14), 2730. https://doi.org/10.3390/electronics13142730
7. Madine, M., Salah, K., Jayaraman, R., & Yaqoob, I. (2025). Zero-knowledge proofs for anonymous authentication of patients on public and private blockchains. Array, 28, 100590. https://doi.org/10.1016/j.array.2025.100590
8. Ansong, E. D., Osei, S. B., & Adjei, R. A. (2025). Implementation and evaluation of the zero-knowledge protocol for identity card verification. Journal of Cyber Security, 7(1), 533–564. https://doi.org/10.32604/jcs.2025.061821
9. Podda, E., Hölzmer, P., Amard, A., Sedlmeir, J., & Fridgen, G. (2025). The impact of zero-knowledge proofs on data minimisation compliance of digital identity wallets. Internet Policy Review, 14(3). https://doi.org/10.14763/2025.3.2019
10. Kostiuk, Y., Rzaieva, S., Khorolska, K., Mazur, N., & Korshun, N. (2025). Architecture of the software system of confidential access to information resources of computer networks. In Proceedings of the Workshop Cyber Security and Data Protection (CSDP 2025) (Vol. 4042, pp. 37–53).
11. Pathak, A., Al Anbagi, I. S., & Hamilton, H. J. (2024). Blockchain-enhanced zero knowledge proof-based privacy-preserving mutual authentication for IoT networks. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3450313
12. Skladannyi, P., Kostiuk, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). Model and methodology for the formation of adaptive security profiles for the protection of wireless networks in the face of dynamic cyber threats. In Proceedings of the Workshop Cyber Security and Data Protection.
13. Dieye, M., Valiorgue, P., Gelas, J.-P., Diallo, E.-H., Ghodous, P., Biennier, F., & Peyrol, E. (2023). A self-sovereign identity based on zero-knowledge proof and blockchain. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3268768
14. Костюк, Ю., Складанний, П., Мазур, Н., Рзаєва, С., Гнатченко, Д., & Гончаренко, І. (2026). Формальна модель адаптивного вибору криптографічних параметрів захисту каналів у корпоративних комп'ютерних мережах на основі динамічної оцінки довіри. Кібербезпека: освіта, наука, техніка, 4(32), 20–44. https://doi.org/10.28925/2663-4023.2026.32.1111
15. Alabdulatif, A. (2025). Blockchain-based privacy-preserving authentication and access control model for e-health users. Information, 16(3), 219. https://doi.org/10.3390/info16030219
16. Складанний, П., Костюк, Ю., & Рзаєва, С. (2026). Безперервна оцінка доступу в Zero Trust Access Management на основі подієвих сигналів безпеки та динамічного керування сесіями. Математичні машини і системи, 1, 29–46. https://doi.org/10.34121/1028-9763-2026-1-29-46
17. Rupok, M. H. K., & Hasan, K. M. A. (2025). BDIMS: A blockchain based digital identity management system with zero knowledge proof. In Proceedings of the 3rd International Conference on Computing Advancements (ICCA '24) (pp. 607–615). ACM. https://doi.org/10.1145/3723178.3723258
18. Костюк, Ю. В., & Складанний, П. М. (2026). Криптографічна модель довіри до подій безпеки в SIEM для інтелектуального формування мережевих інцидентів. Сучасний захист інформації, 1(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393

19. Ramezan, G., & Meamari, E. (2024). zk-IoT: Securing the Internet of Things with zero-knowledge proofs on blockchain platforms. In Proceedings of IEEE ICBC (pp. 1–7). https://doi.org/10.1109/ICBC59979.2024.10634342
20. 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 MoDaST 2025 (Vol. 4005, pp. 82–96).
21. Shahrouz, J., & Analoui, M. (2023). An anonymous authentication scheme with conditional privacy-preserving for vehicular ad hoc networks based on zero-knowledge proof and blockchain. Ad Hoc Networks, 154, 103349. https://doi.org/10.1016/j.adhoc.2023.103349
22. Skladannyi, P., Kostiuk, Y., Rzaieva, S., Bebeshko, B., & Korshun, N. (2025). Adaptive methods for embedding digital watermarks to protect audio and video images in information and communication systems. In Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography (CQPC 2025) (Vol. 4016, pp. 13–31).
23. Chen, X., Zhang, X., Zhong, S., et al. (2025). Anonymous authentication based on blockchain and zero-knowledge proof for vehicular ad hoc networks. The Journal of Supercomputing, 81, 1416. https://doi.org/10.1007/s11227-025-07912-5
24. Kostiuk, Y., Skladannyi, P., Khorolska, K., Sokolov, V., & Hulak, H. (2025). Application of statistical and neural network algorithms in steganographic synthesis and analysis of hidden information in audio and graphic files. In Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography (CQPC 2025) (Vol. 4016, pp. 45–65).
25. Berrios Moya, J. A., Ayoade, J., & Uddin, M. A. (2025). A zero-knowledge proof-enabled blockchain-based academic record verification system. Sensors, 25(11), 3450. https://doi.org/10.3390/s25113450
26. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., & Korshun, N. (2024). Models and algorithms for analyzing information risks during the security audit of personal data information system. In Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024) (Vol. 3925, pp. 155–171).

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Yuliia Kostiuk
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: 0000-0001-5423-0985
y.kostiuk@kubg.edu.ua

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

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

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

MODEL FOR APPLYING ZERO-KNOWLEDGE PROOFS TO ENSURE CONFIDENTIAL AUTHENTICATION AND ACCESS CONTROL IN ENTERPRISE INFORMATION-INTELLIGENT SYSTEMS

Abstract. The paper investigates the problem of ensuring confidentiality in authentication processes within enterprise information-intelligent systems under increasing cybersecurity threats and growing requirements for data protection. The introduction substantiates the relevance of modern cryptographic approaches that minimize the transmission of sensitive information during user authentication. The literature review analyzes approaches to constructing zero-knowledge proofs, which enable verification of a statement without revealing secret data, including succinct non-interactive arguments of knowledge, transparent scalable arguments of knowledge, and compact proof systems without trusted setup. Their cryptographic properties, trust assumptions, scalability, and computational characteristics are examined. In the methodology section, an adaptive authentication model is proposed, based on the integration of cryptographic proofs with risk assessment mechanisms and contextual access analysis. A formal decision-making model for access control is developed, taking into account user parameters, environmental characteristics, and threat levels, enabling dynamic selection of the proof type depending on the current risk level. An authentication algorithm is designed, including stages of identification, context evaluation, proof generation, and verification. In the results section, a comparative analysis of different types of zero-knowledge proofs in enterprise systems is conducted, evaluating their impact on performance, security level, and resistance to attacks. It is shown that the adaptive approach ensures a balance between cryptographic strength and computational efficiency. The conclusions justify the feasibility of implementing the proposed model as part of modern continuous access verification concepts and as a means of improving enterprise information security.

Keywords: zero-knowledge proof; authentication; cryptographic methods; access control; risk assessment; information security; confidentiality; data protection.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Diro, A., Zhou, L., Saini, A., Kaisar, S., & Pham, H. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. Journal of Information Security and Applications, 80, 103678. https://doi.org/10.1016/j.jisa.2023.103678
2. Lavin, R., Liu, X., Mohanty, H., Norman, L., Zaarour, G., & Krishnamachari, B. (2024). A survey on the applications of zero-knowledge proofs. arXiv. https://doi.org/10.48550/arXiv.2408.00243
3. Wang, Z., Huang, J., Miao, K., Lv, X., Chen, Y., Su, B., Liu, L., & Han, M. (2023). Lightweight zero-knowledge authentication scheme for IoT embedded devices. Computer Networks, 236, 110021. https://doi.org/10.1016/j.comnet.2023.110021
4. Zhong, J., He, S., Liu, Z., & Xiong, L. (2025). Lightweight anonymous authentication for IoT: A taxonomy and survey of security frameworks. Sensors, 25(17), 5594. https://doi.org/10.3390/s25175594
5. Zhang, B., Pan, H., Li, K., Xing, Y., Wang, J., Fan, D., & Zhang, W. (2024). A blockchain and zero knowledge proof based data security transaction method in distributed computing. Electronics, 13(21), 4260. https://doi.org/10.3390/electronics13214260
6. Zhao, X., Xia, F., Xia, H., Mao, Y., & Chen, S. (2024). A zero-knowledge-proof-based anonymous and revocable scheme for cross-domain authentication. Electronics, 13(14), 2730. https://doi.org/10.3390/electronics13142730
7. Madine, M., Salah, K., Jayaraman, R., & Yaqoob, I. (2025). Zero-knowledge proofs for anonymous authentication of patients on public and private blockchains. Array, 28, 100590. https://doi.org/10.1016/j.array.2025.100590
8. Ansong, E. D., Osei, S. B., & Adjei, R. A. (2025). Implementation and evaluation of the zero-knowledge protocol for identity card verification. Journal of Cyber Security, 7(1), 533–564. https://doi.org/10.32604/jcs.2025.061821
9. Podda, E., Hölzmer, P., Amard, A., Sedlmeir, J., & Fridgen, G. (2025). The impact of zero-knowledge proofs on data minimisation compliance of digital identity wallets. Internet Policy Review, 14(3). https://doi.org/10.14763/2025.3.2019
10. Kostiuk, Y., Rzaieva, S., Khorolska, K., Mazur, N., & Korshun, N. (2025). Architecture of the software system of confidential access to information resources of computer networks. In Proceedings of the Workshop Cyber Security and Data Protection (CSDP 2025) (Vol. 4042, pp. 37–53).
11. Pathak, A., Al Anbagi, I. S., & Hamilton, H. J. (2024). Blockchain-enhanced zero knowledge proof-based privacy-preserving mutual authentication for IoT networks. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3450313
12. Skladannyi, P., Kostiuk, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). Model and methodology for the formation of adaptive security profiles for the protection of wireless networks in the face of dynamic cyber threats. In Proceedings of the Workshop Cyber Security and Data Protection.
13. Dieye, M., Valiorgue, P., Gelas, J.-P., Diallo, E.-H., Ghodous, P., Biennier, F., & Peyrol, E. (2023). A self-sovereign identity based on zero-knowledge proof and blockchain. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3268768
14. 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
15. Alabdulatif, A. (2025). Blockchain-based privacy-preserving authentication and access control model for e-health users. Information, 16(3), 219. https://doi.org/10.3390/info16030219
16. 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
17. Rupok, M. H. K., & Hasan, K. M. A. (2025). BDIMS: A blockchain based digital identity management system with zero knowledge proof. In Proceedings of the 3rd International Conference on Computing Advancements (ICCA '24) (pp. 607–615). ACM. https://doi.org/10.1145/3723178.3723258
18. Kostiuk, Y. V., & Skladannyi, P. M. (2026). Cryptographic model of trust in security events in SIEM for intelligent formation of network incidents. *Modern Information Protection, 1*(65), 103–118. https://doi.org/10.31673/2409-7292.2026.011393
19. Ramezan, G., & Meamari, E. (2024). zk-IoT: Securing the Internet of Things with zero-knowledge proofs on blockchain platforms. In Proceedings of IEEE ICBC (pp. 1–7). https://doi.org/10.1109/ICBC59979.2024.10634342

20. 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 MoDaST 2025 (Vol. 4005, pp. 82–96).
21. Shahrouz, J., & Analoui, M. (2023). An anonymous authentication scheme with conditional privacy-preserving for vehicular ad hoc networks based on zero-knowledge proof and blockchain. Ad Hoc Networks, 154, 103349. https://doi.org/10.1016/j.adhoc.2023.103349
22. Skladannyi, P., Kostiuk, Y., Rzaieva, S., Bebeshko, B., & Korshun, N. (2025). Adaptive methods for embedding digital watermarks to protect audio and video images in information and communication systems. In Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography (CQPC 2025) (Vol. 4016, pp. 13–31).
23. Chen, X., Zhang, X., Zhong, S., et al. (2025). Anonymous authentication based on blockchain and zero-knowledge proof for vehicular ad hoc networks. The Journal of Supercomputing, 81, 1416. https://doi.org/10.1007/s11227-025-07912-5
24. Kostiuk, Y., Skladannyi, P., Khorolska, K., Sokolov, V., & Hulak, H. (2025). Application of statistical and neural network algorithms in steganographic synthesis and analysis of hidden information in audio and graphic files. In Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography (CQPC 2025) (Vol. 4016, pp. 45–65).
25. Berrios Moya, J. A., Ayoade, J., & Uddin, M. A. (2025). A zero-knowledge proof-enabled blockchain-based academic record verification system. Sensors, 25(11), 3450. https://doi.org/10.3390/s25113450
26. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., & Korshun, N. (2024). Models and algorithms for analyzing information risks during the security audit of personal data information system. In Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024) (Vol. 3925, pp. 155–171).

Отримано редакцією журналу / Received: 23.02.26
Прорецензовано / Revised: 02.03.26
Схвалено до друку / Accepted: 25.06.26