УДК: 004.021:004.89:004.056.5 DOI: **10.33099/2311-7249/2026-55-1-84-99**

ФЕСЕНКО Тетяна Миколаївна,
кандидат технічних наук, доцент,
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна,
https://orcid.org/0009-0006-1698-3795

ПЛАХТІЙ Максим Олександрович,
кандидат економічних наук,
Товариство з обмеженою відповідальністю приватний вищий навчальний заклад
«Університет сучасних технологій», Київ, Україна,
https://orcid.org/0000-0003-3805-0591

РУБІН Едуард Юхимович,
кандидат технічних наук, доцент,
Товариство з обмеженою відповідальністю приватний вищий навчальний заклад
«Університет сучасних технологій», Київ, Україна,
https://orcid.org/0009-0005-4447-4413

КАЛАШНІКОВА Юлія Вадимівна,
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна,
https://orcid.org/0000-0001-9899-4784

АРХІТЕКТУРНО-КРИПТОГРАФІЧНА МОДЕЛЬ УПРАВЛІННЯ СИСТЕМАМИ СПЕЦІАЛЬНИХ КОРИСТУВАЧІВ З ІНТЕЛЕКТУАЛЬНОЮ АДАПТАЦІЄЮ ДОСТУПУ

У статті наведено архітектурно-криптографічну модель управління системами спеціальних користувачів, орієнтовану на підвищення рівня захисту та стійкості сучасних мультидоменних кіберінфраструктур. ***Метою статті*** *є розроблення архітектурно-криптографічної моделі системи керування спеціальними користувачами, що поєднує механізми симетричного шифрування стандарту шифрування даних і вдосконаленого стандарту шифрування з інтелектуальними методами адаптації політик доступу на основі аналізу поведінки користувачів.*

Методи дослідження. *У дослідженні використано методи системного аналізу та архітектурного моделювання для формалізації системи керування спеціальними користувачами відповідно до принципів концепції нульової довіри. Криптографічну складову оцінено за допомогою порівняльного аналізу симетричних алгоритмів шифрування з урахуванням вимог сучасних інформаційних середовищ. Новизна методичного підходу полягає у застосуванні методів машинного навчання для побудови динамічних поведінкових профілів спеціальних користувачів та інтелектуального оцінювання ризиків доступу в реальному часі. Отримані результати використано для адаптивного коригування політик доступу, ефективність якого підтверджено шляхом аналітичного узагальнення результатів моделювання типових сценаріїв функціонування системи.*

Отримані результати дослідження. *У результаті дослідження розроблено архітектурно-криптографічну модель керування спеціальними користувачами, що поєднує симетричні механізми шифрування з адаптивними політиками доступу відповідно до принципів концепції нульової довіри. Моделювання показало, що застосування методів машинного навчання для формування поведінкових профілів дозволяє знизити ймовірність несанкціонованого використання привілеїв у середньому на 35–45 % порівняно зі статичними моделями контролю доступу. При цьому адаптивне оцінювання ризиків у реальному часі забезпечує коригування рівнів доступу з середнім часом реакції до 200-300 мс, що є прийнятним для критичних інформаційних систем. У сценаріях аномальної поведінки інтегрований інтелектуальний механізм зменшує рівень операційного ризику доступу в 1,4–1,6 рази без суттєвого впливу на продуктивність системи.*

Елементи наукової новизни. *Уперше запропоновано архітектурно-криптографічну модель керування спеціальними користувачами, що інтегрує симетричні механізми криптографічного захисту з інтелектуальними методами машинного навчання для динамічної адаптації політик доступу відповідно до принципів концепції нульової довіри. Набуло подальшого розвитку використання методів машинного навчання у сфері керування привілейованим доступом шляхом формування поведінкових профілів користувачів і оцінювання ризиків доступу в реальному часі, що забезпечує адаптивне коригування рівнів привілеїв залежно від контексту взаємодії з ресурсами. Удосконалено підхід до поєднання криптографічних і поведінкових механізмів захисту, який дозволяє знизити ймовірність зловживання привілеями без суттєвого зростання обчислювальних витрат та втрат продуктивності системи.*

Теоретична й практична значущість викладеного у статті. *Теоретична значущість викладених у статті результатів полягає в розвитку підходів до побудови систем керування спеціальними користувачами шляхом поєднання криптографічних механізмів захисту з інтелектуальними методами адаптації політик доступу. Запропонована архітектурно-криптографічна модель інтегрує алгоритми блокового шифрування стандарту шифрування даних та вдосконаленого стандарту шифрування даних з методами машинного навчання, що забезпечує динамічне реагування системи на зміну контексту користувацької активності та рівня ризику доступу. Такий підхід розширює наукові уявлення про можливості переходу від статичних моделей контролю доступу до адаптивних механізмів керування привілеями в умовах концепції нульової довіри. Практична значущість дослідження визначається можливістю використання розробленої моделі під час проєктування та модернізації захищених інформаційних систем у гетерогенних кіберінфраструктурах, зокрема в середовищах інтернету речей, системах диспетчерського керування та збору даних, а також у державних і корпоративних центрах оброблення даних. Запропонована архітектура враховує обмеження промислових протоколів обміну даними та різнорідність каналів зв'язку, що забезпечує її практичну придатність у реальних умовах експлуатації. Застосування методів машинного навчання для формування поведінкових профілів спеціальних користувачів дозволяє виявляти аномальні дії на ранніх етапах та адаптивно коригувати рівні доступу. Проведений порівняльний аналіз продуктивності криптографічних механізмів підтверджує, що запропонований підхід забезпечує підвищення рівня безпеки без критичного впливу на затримки автентифікації в режимі реального часу.*

Ключові слова: *спеціальні користувачі, архітектурно-криптографічна модель, інтелектуальна адаптація доступу, захист інформації, кібербезпека, машинне навчання, вдосконалений стандарт шифрування даних, системи диспетчерського керування та збору даних.*

Вступ

Постановка проблеми. Сучасний етап розвитку інформаційних технологій характеризується глибокою інтеграцією цифрових систем у критично важливі сфери – промисловість, енергетику, транспорт і державне управління. У процесі еволюції складних розподілених інформаційних систем сформувалися мультидоменні кіберінфраструктури, у межах яких взаємодіють технічні компоненти, програмні сервіси та користувачі з різними рівнями довіри. За таких умов ключову роль відіграють спеціальні користувачі з розширеними привілеями, компрометація яких може призвести до масштабних інцидентів безпеки та втрати керованості їх критичних систем.

Наявні моделі керування доступом ґрунтуються на статичних політиках авторизації, що не враховують динаміку поведінки користувачів і не реагують на аномальні дії в реальному часі. Зазначені фактори зумовлюють підвищену вразливість систем до внутрішніх загроз, несанкціонованої ескалації привілеїв та зловживання сервісними обліковими записами. Крім того, традиційні архітектури обмежено адаптуються до різнорідних доменів, від малопотужних вузлів інтернету речей (Internet of Things (далі – IoT)) до високопродуктивних дата-центрів.

Із криптографічного погляду, основною проблемою залишається забезпечення ефективного використання алгоритмів стандарту шифрування даних і вдосконаленого стандарту шифрування в розподілених системах за умов жорстких обмежень на допустимі затримки [1]. Ефективність таких рішень визначається не лише рівнем криптостійкості, а й обчислювальною ефективністю та масштабованістю в умовах гібридних мережевих середовищ. У цьому контексті важливо забезпечити уніфіковане керування ключами, перевірку автентичності та контроль сеансів доступу між доменами.

За умов зростаючої складності кіберзагроз виникає необхідність упровадження інтелектуальних механізмів адаптації політик доступу, заснованих на машинному навчанні (далі – ML). Саме поведінковий аналіз дозволяє формувати динамічні профілі користувачів, виявляти аномальні патерни та автоматично коригувати рівень довіри. Тому комбінація таких методів із криптографічними протоколами створює самоадаптивну архітектуру доступу, яка поєднує безпеку, гнучкість і високу продуктивність.

Таким чином, актуальним науковим завданням є розроблення архітектурно-криптографічної моделі інтелектуального керування доступом спеціальних користувачів, здатної забезпечити комплексний захист інформаційних ресурсів у гібридних кіберінфраструктурах.

Така модель має поєднувати криптографічні методи стандарту шифрування даних і вдосконаленого стандарту шифрування з поведінковим аналізом та динамічним керуванням привілеями [2], що дає змогу підвищити рівень кіберстійкості й надійності цифрових платформ державного та промислового призначення.

Аналіз останніх досліджень і публікацій. У контексті еволюції цифрових інфраструктур, де взаємодіють системи різних рівнів, від IoT-пристроїв до державних дата-центрів, питання архітектурної побудови безпечного доступу набуває системного характеру. Глобальна тенденція до ускладнення кіберсередовища зумовлює потребу у поєднанні криптографічних методів захисту з інтелектуальними механізмами адаптації доступу, здатними динамічно реагувати на зміну ризикового профілю користувача [3]. В умовах високої варіативності каналів доступу, гібридних архітектур та мультидоменних моделей обробки даних традиційні підходи до контролю

привілеїв поступово втрачають ефективність, що підтверджується сучасними дослідженнями у сфері інформаційної безпеки.

Науково-технічна література демонструє зростаючий інтерес до поєднання криптографічних алгоритмів із динамічними схемами автентифікації. Так, в роботі [4] обґрунтовано доцільність інтеграції алгоритму вдосконаленого стандарту шифрування в протокол черги повідомлень телеметричного транспорту для забезпечення захисту телеметричних потоків у промислових системах диспетчерського керування та збору даних. Автори підкреслюють, що криптографічні модулі мають бути архітектурно сумісними з системами реального часу, а ключові процеси шифрування повинні виконуватися з мінімальними затримками. Цей підхід закладає основу для формування концепції «криптографічної прозорості», коли механізми захисту вбудовані безпосередньо в транспортний рівень взаємодії між спеціальними користувачами.

Водночас, у дослідженні [5] акцентовано увагу на важливості стохастичного підходу до генерації ключів, що забезпечує підвищену стійкість до прогнозованих атак. В дослідженні наголошується, що використання хаотичних логістичних мап дозволяє динамічно оновлювати ключовий простір, знижуючи ймовірність компрометації. Таким чином, сучасна тенденція розвитку криптографічних механізмів полягає не лише у підвищенні обчислювальної складності, а й у їх архітектурній адаптивності до змінних контекстів функціонування.

Іншим стратегічним напрямом є інтелектуалізація систем доступу. В огляді [6] проаналізовано уразливості промислових інфраструктур з позицій надлишкових привілеїв користувачів та відсутності адаптивних моделей управління доступом. Дослідники підкреслюють, що класичні моделі контролю доступу є недостатніми для динамічних середовищ, у яких поведінкові патерни користувачів мають визначальний вплив на рівень довіри. У зв'язку з цим виникає необхідність формування інтегрованих архітектур, де криптографічний контроль узгоджується з алгоритмічною оцінкою поведінкових ризиків.

Паралельно із науковими розробками активно формується нормативна база, що задає стратегічні вектори безпечного управління привілеями. Європейська директива NIS2 (EU 2022/2555) визначає обов'язкові технічні та організаційні вимоги до управління ідентифікацією, автентифікацією, а також моніторингу доступу до критичних ресурсів. Згідно з цим аналітичним звітом, управління привілейованими обліковими записами визнається ключовим фактором дотримання положень статті 21, що регламентує технічну відповідність і реакцію на інциденти [7]. Отже, нормативна парадигма поступово зміщується від формальної відповідності до ризик-орієнтованого управління доступом із використанням криптографічних та аналітичних засобів.

Провідні технологічні компанії також акцентують увагу на важливості архітектурної цілісності систем контролю привілеїв. Зокрема, у білому звіті WALLIX (2023) наголошується, що ефективне управління доступом потребує інтеграції політик ідентифікації, шифрування, сегментації мережі та поведінкового моніторингу [8]. Подібні висновки представлені у корпоративному звіті One Identity за 2023, де підкреслюється необхідність формування інтегрованих моделей управління привілеями (Privileged Access Management (далі – PAM)) як основного інструменту реалізації концепції «нульової довіри» (Zero Trust Architecture) [9].

Узагальнюючи проведений аналіз, можна констатувати, що сучасний науковий і корпоративно-нормативний дискурс поступово конвергує навколо ідеї архітектурної адаптивності криптографічного контролю доступу. Поєднання інтелектуальних моделей оцінки ризику, динамічних механізмів генерації ключів та багаторівневих політик привілеїв формує новий клас безпекових архітектур, орієнтованих на контекстну саморегуляцію. Саме тому, враховуючи існуючі проблеми керування привілеями спеціальних користувачів у гетерогенних кіберінфраструктурах, розвиток архітектурно-криптографічних моделей спеціальних користувачів із інтелектуальною адаптацією доступу є закономірним кроком за напрямом еволюції безпечних корпоративних і державних електронних комунікаційних мереж.

Метою статті є розроблення архітектурно-криптографічної моделі системи керування спеціальними користувачами, що поєднує механізми симетричного шифрування стандарту шифрування даних і вдосконаленого стандарту шифрування з інтелектуальними методами адаптації політик доступу на основі аналізу поведінки користувачів.

Досягнення зазначеної мети дасть змогу сформувати інтегровану архітектурно-криптографічну платформу, що забезпечить захищене, адаптивне та контекстно-залежне управління доступом спеціальних користувачів. Це, у свою чергу, створить передумови для підвищення рівня кіберстійкості, довіри й прозорості у процесах управління критичними цифровими ресурсами державного та промислового секторів.

Виклад основного матеріалу дослідження

Керування привілеями в гетерогенних кіберінфраструктурах є багаторівневою проблемою, що поєднує вимоги криптографічного захисту, формалізованих політик доступу та операційного контролю. Більшість наявних підходів до контролю доступу розроблялися для корпоративних інформаційних доменів з відносно однорідною інфраструктурою та стабільними каналами обміну даними, що обмежує їх ефективність у динамічних і розподілених середовищах.

Такі підходи передбачають централізоване

зберігання та управління обліковими даними, явну авторизацію на підставі ролей або атрибутів і журналювання сесій. Проте при перенесенні цих архітектур у мультидоменні середовища, виявляються системні обмеження щодо масштабованості, латентності та міждоменної сумісності. Цей висновок корелює з рекомендаціями нормативних контрольних наборів, які підкреслюють необхідність спеціалізованого управління привілейованими акаунтами як елемент загальної безпекової політики [10].

Перше, що обмежує традиційні моделі за масштабування – це архітектурна припущеність про «однорідний довірчий простір». Моделі рольового керування доступом і керування доступом на основі атрибутів є ефективними в межах окремого інформаційного домену за наявності централізованого каталогу користувачів та уніфікованих атрибутів доступу. Водночас у мультидоменних інсталяціях часто функціонують автономні каталоги й різнорідні механізми взаємодії між системами, а також існують нормативно-правові та організаційні обмеження, що ускладнюють централізацію керування доступом.

На практиці це призводить до дублювання облікових записів, розрізнених політик та складності синхронізації привілеїв – факторів, які ускладнюють масштабне управління та підвищують ризик ескалації привілеїв при міждоменній інтеграції. Нормативні настанови підкреслюють потребу в централізованих механізмах контролю привілеїв, але практичний перехід до такої централізації вимагає архітектурних рішень, що зберігають властивості автономності доменів [10].

Другим суттєвим обмеженням є протокольна та ресурсна гетерогенність промислових платформ і розподілених вбудованих систем. Значна частина низькорівневих промислових протоколів керування та телеметрії була спроєктована без урахування вимог автентифікації та криптографічного захисту, що унеможливлює їх безпосередню інтеграцію із сучасними механізмами керування доступом. У таких умовах зростає роль поведінкового аналізу як компенсуючого механізму безпеки, що дає змогу виявляти відхилення у діях користувачів і сервісних процесів навіть за відсутності повноцінної криптографічної підтримки на протокольному рівні [11]. За таких умов, забезпечення захищеного доступу вимагає застосування проміжних архітектурних компонентів, зокрема захисних шлюзів або механізмів тунелювання, у яких реалізується інтелектуальна оцінка контексту та ризиків доступу.

Унаслідок цього на практиці для забезпечення конфіденційності і цілісності застосовують зовнішні шифровані тунелі або реалізують додаткові проксі-шари, які накладають обчислювальне навантаження і збільшують затримки, що є критичними для систем реального часу. Дослідження і технічні звіти з промислової безпеки показують, що шифрування зовнішнім тунелем хоча й підвищує захист, але створює вузькі місця при масштабуванні сотень-тисяч пристроїв. Аналіз специфікацій IEC 62351 вказує на необхідність вбудованих засобів захисту в промислові протоколи; проте поступова імплементація цих вимог у реальних об’єктах ще далека від універсального покриття [12].

Третім суттєвим обмеженням є складність керування криптографічними ключами та конфіденційними даними доступу у розподілених середовищах, що істотно ускладнює масштабоване впровадження систем керування привілейованим доступом [13]. Більшість наявних рішень орієнтована на корпоративні інформаційні системи та передбачає централізоване зберігання конфіденційних даних доступу, автоматизовану ротацію облікових даних і проксіювання сеансів доступу. Водночас їх інтеграція у гетерогенні промислові та вбудовані середовища потребує проміжних механізмів трансляції протоколів, агентної інфраструктури та забезпечення високої доступності за умов обмежених і нестабільних каналів зв’язку.

За таких умов виникають практичні проблеми безпечної доставки тимчасових облікових даних до ресурсно обмежених пристроїв, організації ротації ключів без порушення безперервності технологічних процесів, а також гарантування відмовостійкості сховищ конфіденційних даних доступу у географічно розподілених інсталяціях. Це зумовлює доцільність доповнення традиційних механізмів керування поведінковим аналізом, який дає змогу знижувати залежність від жорсткої централізації ключового матеріалу за рахунок динамічної оцінки контексту доступу та рівня довіри.

Корпоративні звіти підкреслюють, що впровадження PAM вимагає адаптивних архітектур, які поєднують централізоване управління з локальною автономією виконання [14].

Четвертий аспект – вимоги щодо латентності і реального часу. Впровадження додаткових шарів автентифікації, контролю сесій і шифрування за замовчуванням збільшує затримки у каналах керування. У системах диспетчерського управління та збору даних (Supervisory Control and Data Acquisition (далі – SCADA)) навіть незначні затримки можуть порушити цикл зворотного зв’язку, призвести до деградації управління процесом або викликати критичні реакції контролерів. Тому архітектурні рішення повинні враховувати компроміс між безпекою і часовими вимогами. Зазначене часто реалізується через розподіл функцій (локальна верифікація – глобальний аудит) або через застосування апаратного прискорення криптографії (наприклад, AES-акселерація). Відсутність такого проєктування є поширеною причиною відмов від повної інтеграції PAM-функціоналу у промислових системах [15].

Нарешті, проблема міждоменної довіри й політик синхронізації залишається ключовою при впровадженні уніфікованих рішень. Мультидоменна

модель вимагає механізмів федерації і взаємного визнавання атрибутів доступу, а також узгодження політик обробки конфіденційних даних, що регулюються різними нормативними рамками.

Відсутність єдиного механізму синхронізації політик створює сценарії, в яких однакові права можуть бути інтерпретовані по-різному у суміжних доменах, що збільшує ризик некоректного делегування або невиявленої ескалації. Практичні архітектурні підходи пропонують модель «контрольованої федерації» з прозорим трасуванням і аудитом, але їх впровадження потребує координації стандартів і технологічних стеків між зацікавленими сторонами [10].

Таким чином, узагальнення результатів сучасних досліджень та аналітичних звітів дає підстави виокремити низку системних обмежень, притаманних актуальним моделям управління привілеями в середовищах IoT, SCADA та урядових інформаційних інфраструктурах. По-перше, спостерігається недостатня архітектурна підтримка мультидоменності та узгодження політик доступу, що обмежує взаємодію між різнорідними доменами та ускладнює централізований контроль. По-друге, протокольна та ресурсна гетерогенність унеможливлює пряму інтеграцію систем PAM без проміжних адаптерів і шлюзів безпеки. По-третє, залишається невирішеною проблема масштабування інфраструктури управління ключами та захищеної доставки «секретів» до пристроїв із обмеженими обчислювальними ресурсами. По-четверте, існують компроміси між рівнем криптографічного захисту та часовими вимогами систем реального часу, де надмірна складність обчислень може призводити до критичних затримок у промислових або урядових сценаріях. Нарешті, п’ятим чинником є організаційні й нормативні бар’єри, які перешкоджають уніфікації політик доступу та узгодженню процедур аудиту безпеки між різними відомчими структурами.

Виходячи з виявлених обмежень, обґрунтованою є потреба у розробці архітектурно-криптографічної моделі, яка поєднає адаптивні механізми генерації і ротації ключів, локально-автономні механізми верифікації, протоколів довіри та інтелектуальні алгоритми оцінки поведінки спеціальних користувачів – тобто саме тих елементів, які покликані забезпечити масштабованість і надійність міждоменного обміну в реальних виробничих та державних середовищах.

Управління доступом спеціальних (привілейованих) користувачів у мультидоменних кіберінфраструктурах вимагає поєднання двох взаємодоповнювальних складових: (1) криптографічних засобів забезпечення конфіденційності та цілісності обміну і (2) логічних механізмів авторизації й контролю сеансів. Інтеграція блокових шифрів у ці процеси обґрунтовується необхідністю гарантування криптографічних властивостей каналів аутентифікації, забезпечення цілісності маркерів сесій та захисту конфіденційних атрибутів (ключі, токени, облікові дані). Нижче наведено техніко-математичне і архітектурне обґрунтування такої інтеграції, логічно структуроване від криптостійкості до витрат продуктивності й вимог до ключового менеджменту.

Отже, криптостійкість шифру характеризується обсягом пошуку ключа (комплексністю грубої сили) та структурними слабкостями проти криптоаналітичних атак. Для бінарного ключового простору його розмір дорівнює 2^k, де k – число біт/довжина ключа. Середній час до знаходження ключа при грубому пошуку (середнє значення) – $\frac{2^k}{2R} = \frac{2^{k-l}}{2R}$, де R – швидкість перевірки варіантів ключів (перевірок/с). Для наочності розглянемо:

стандарт шифрування даних (Data Encryption Standard (далі – DES): $k_{DES} = 56$. Тому напівпростір (середня кількість спроб) $= 2^{55} \approx 3.6028 \times 10^{16}$ (1 трлн/с) $T_{DES} \approx 3.6 \times 10^4 c \approx 10$ годин;

удосконалений стандарт шифрування (Advanced Encryption Standard (далі – AES) AES-128: $k_{AES128} = 128$. Напівпростір $= 2^{127} \approx 1.7014 \times 10^{38}$. При $R = 10^{12}$ спроб/с отримуємо $T_{AES128} \approx \frac{2^{127}}{10^{12}} c \approx 1.7014 \times 10^{26}$ років, що практично робить грубий пошук недосяжним.

Ці обчислення демонструють що DES зі своїм ефективним 56-бітним ключем вже не забезпечує адекватного захисту у сучасних обчислювальних умовах. При цьому AES (128/192/256 біт), навпаки забезпечує криптостійкість значно ефективнішу і вищу, що робить AES прийнятним вибором для захисту маркерів аутентифікації, сеансових ключів та конфіденційних атрибутів.

Важливо зазначити, що аутентифікація та авторизація у сучасних системах часто базуються на передачі маркерів, виклику протоколів розподіленої автентифікації (наприклад, SAML/OAuth), а також на обміні «секретами» для встановлення сеансових ключів. Інтегрування блокових шифрів забезпечує виконання наступних технічних функцій:

захист конфіденційності облікових даних забезпечується шляхом їх криптографічного шифрування під час передачі мережею, що істотно знижує ризик перехоплення, модифікації або повторного використання маркерів автентифікації чи паролів у разі несанкціонованого доступу до комунікаційного каналу;

забезпечення цілісності та автентичності повідомлень досягається шляхом використання автентифікованого шифрування з додатковими даними (Authenticated Encryption with Associated Data (далі – AEAD)), зокрема удосконаленого стандарту шифрування у режимі лічильника з автентифікацією Галуа (Advanced Encryption Standard – Galois/Counter Mode (далі – AES-GCM)), який дає змогу одночасно виконувати шифрування даних та верифікацію їхньої

цілісності без потреби у додатковому застосуванні окремого механізму автентифікації повідомлень або контроль доступу (Message Authentication Code (далі – MAC));

захист сеансових ключів та їх періодична ротація забезпечуються через шифроване зберігання й захищену доставку тимчасових ключів, що істотно зменшує площу потенційної атаки та унеможливлює їх компрометацію під час обміну між компонентами системи.

Математично, якщо маркер m має ентропію $H(m)$ (біт), і його ймовірність підбору $p \approx 2^{-H(m)}$, то застосування шифрування з ключем ентропії $H(k)$ зменшує ймовірність коректного підроблення/відтворення без знання ключа до $p_{attac} \approx 2^{-H(m)}$, тобто безпечність визначається бітністю ключа. Отже, при $H(k) = 128$ ризик підроблення стає практично нульовим у контексті поточних обчислювальних ресурсів.

Розглядаючи контроль сеансів доступу (сеансові ключі, терміни існування, ймовірність компрометації) необхідно наголосити, що ефективна політика сесій передбачає генерування тимчасових (ephemeral) сеансових ключів K_{sess} для кожної сесії, з періодичною ротацією. Нехай середня інтенсивність компрометацій (успішних атак на ключ) для одного сеансу дорівнює λ (подій/сесія/год). Якщо тривалість сесії τ (с), очікуване вікно вразливості пропорційне τ, то $P_{compromise} \approx 1 - e^{-\lambda} \approx \lambda\tau$ при $\lambda\tau \ll 1$. Це дає простий інструмент для вибору максимально допустимого τ з урахуванням прийнятного ризику. Наприклад, при $\lambda = 10^{-6}$ на годину (дуже рідкісні компрометації) і $\tau = 3600$ с маємо $P \approx 3.6 \times 10^{-3}$, тобто 0.36 %. Зменшення τ на порядок знижує ризик лінійно.

Отже, короткоіснуючі сеансові ключі + ротація/ephemeral ключів значно зменшують ризик порівняно зі сценарієм тривалих статичних ключів, особливо для привілейованих користувачів. Оцінюючи накладні витрати шифрування та вплив на реальний час необхідно зазначити, що повідомлення розміром S байт у певному режимі можна представити як:

$$T_{enc} + T_{auth} + T_{proc} \leq \Delta_{max}\,, \qquad (1)$$

де T_{auth} – час на автентифікацію (запит до централізованого сервера/локальної перевірки), T_{proc} – час обробки на контролері. Архітектурним рішенням, що знижує сумарний час, є розподіл функцій, а саме локальна верифікація простих операцій, глобальна (повна) автентифікація – епізодично або на випадок аномалій.

Для забезпечення одночасної конфіденційності та цілісності інформації доцільно використовувати режими автентифікованого симетричного шифрування, що поєднують шифрування даних із перевіркою їх цілісності. Якщо позначити операцію шифрування з автентифікацією ключем k як оператор $E_k(P, A)$, а операцію розшифрування – як $D_k(\cdot)$, то режими автентифікованого шифрування гарантують, що результат розшифрування є коректним тоді й лише тоді, коли підтверджено цілісність як зашифрованого повідомлення P, так і пов'язаних даних A. Пов'язані дані не підлягають шифруванню, проте захищаються від несанкціонованої модифікації та можуть містити, зокрема, метадані сеансу.

Застосування AEAD значно спрощує модель контролю сеансів, потреби у двоетапній схемі «шифрування плюс MAC», що зменшує T_{enc} і ймовірність помилкових конфігурацій стає відсутньою.

При цьому, надійна система управління ключами (Key Management System (далі – KMS)) повинна забезпечувати безпечне зберігання майстер-ключів, при цьому механізм генерації сеансових ключів постає як:

$$K_{sess} = \mathrm{KDF}(K_{master}, \mathrm{nonce}, \mathrm{context}), \qquad (2)$$

а також схему ротації і відкликання ключів. Очікуване вікно вразливості лінійно залежить від інтервалу ротації τ. Тому вибір τ здійснюють з урахуванням допустимого ризику P_{acc}, тобто $\tau \leq \frac{P_{acc}}{\lambda}$.

Крім того, з архітектурного погляду доцільним є використання гібридного підходу, який передбачає централізовану систему керування ключами для реалізації політик доступу та аудиту, а також локальні апаратні засоби захисту для зберігання і застосування конфіденційних даних доступу на кінцевих вузлах. Так, в межах математичного обґрунтування розподілу ролей шифрування у різних рівнях інфраструктури позначимо домени: D_{IoT} (ресурсно-обмежені пристрої), D_{ICS} (SCADA/ICS), D_{DC} (урядові дата-центри). Для кожного домену введемо допустимий латентнісний бюджет Δ_D. Архітектурне правило, для будь-якого повідомлення, що перетинає межу доменів, має виконуватися

$$T_{enc}^{(i)} + T_{trans}^{(i,j)} + T_{dec}^{(j)} \leq \Delta_{Di \to Dj}, \qquad (3)$$

де індекси i, j відповідають відправнику й одержувачу. AES-реалізації з апаратною підтримкою (на рівні D_{DC} та D_{ICS}) дозволяють зменшити T_{enc} і T_{dec}, тоді як у D_{IoT} застосовні легковагі режими (AES-CCM, оптимізовані бібліотеки), а при неможливості використовуються криптографічні шлюзи, котрі забезпечують перетворення між формами автентифікації та шифрування.

З огляду на наведені чисельно-аналітичні аргументи та встановлені операційні обмеження, доцільність інтеграції блокових шифрів у процеси автентифікації, авторизації та керування сесіями спеціальних користувачів може бути обґрунтована низкою практичних висновків [16].

Передусім алгоритми стандарту шифрування даних та його триразовий варіант не відповідають сучасним вимогам криптографічної стійкості та не можуть використовуватися для захисту маркерів автентифікації й сеансових ключів. Їхній ключовий

простір є недостатнім для протидії атакам повного перебору, що за наявності сучасних обчислювальних потужностей робить такі алгоритми криптографічно вразливими та неприйнятними для застосування в сучасних системах захисту даних.

Тому на сучасному етапі оптимальним вибором для інтеграції є удосконалений стандарт шифрування, визначений у міжнародному криптографічному стандарті NIST FIPS 197, який забезпечує високий рівень криптографічної стійкості та сумісність із режимами автентифікованого шифрування, що гарантують одночасну конфіденційність і цілісність даних [17].

У межах протоколів аутентифікації рекомендується застосовувати шифрування маркерів або принаймні AEAD-захист, який одночасно гарантує цілісність і конфіденційність. Сеансові ключі мають бути тимчасовими і генеруватися за допомогою функції формування ключа (Key Derivation Function (далі – KDF)) із використанням одноразового ініціалізаційного значення або контекстних параметрів, що знижує ризик повторного використання ключа та підвищує стійкість до атак відтворення.

Для ресурсно-обмежених пристроїв (наприклад, IoT-контролерів) доцільним є використання AEAD-режимів, сертифікованих для легковагових профілів. У випадках, коли апаратна підтримка AES відсутня, доцільно застосовувати спеціалізовані легковагові шифри або використовувати криптографічні шлюзи/проксі-сервери, що делегують складні криптографічні операції більш потужним вузлам мережі [18].

Окрему увагу необхідно приділити ключовому менеджменту, який має реалізовувати політики ротації, відкликання та моніторингу сеансів доступу. Параметри ротації доцільно формалізувати через відкриті числові залежності ризику компрометації ключів $P_{compromise} \approx \lambda\tau$, що дозволить адаптувати частоту оновлення криптографічних матеріалів до поточного рівня загроз і навантаження системи.

Отже, інтеграція сучасних блокових шифрів типу AES у поєднанні з динамічними політиками управління ключами формує оптимальний баланс між безпекою, продуктивністю та сумісністю у гетерогенних мультидоменних кіберінфраструктурах.

Безперечно, інтеграція блокових шифрів у процеси аутентифікації, авторизації та контролю сеансів доступу виступає не лише доцільним, але й технічно обґрунтованим та необхідним кроком, що забезпечує підвищення криптографічної стійкості й операційної надійності систем спеціальних користувачів у гетерогенних інформаційно-комунікаційних середовищах.

Математично обґрунтовані вище, оцінки стійкості та аналіз накладних витрат вказують на практичну перевагу AES-та AEAD-рішень. Водночас архітектурна інтеграція має враховувати часові обмеження обробки даних і передбачати розподіл обчислювальних функцій. Керування криптографічними ключами доцільно реалізовувати за гібридною моделлю з поєднанням централізованого керування та локальних апаратних засобів захисту. Використання короткочасних сеансових ключів із динамічною ротацією та режимів автентифікованого шифрування забезпечує конфіденційність і цілісність даних. Сукупність наведених елементів формує технологічну основу запропонованої архітектурно-криптографічної моделі.

З огляду на зазначене вище запропоновано архітектуру (рис. 1) що базується на багаторівневій стратифікації компонентів – від рівня пристроїв (IoT/SCADA) до рівня централізованих сервісів і політик. На нижньому рівні функціонують вузли з обмеженими обчислювальними можливостями, де реалізація повноцінних криптографічних протоколів є ресурсно затратною. Для таких випадків застосовується легковагова модифікація протоколу захисту транспортного рівня для датаграм (Datagram Transport Layer Security (далі – TLS-DTLS)) із використанням автентифікованого шифрування з додатковими даними (Authenticated Encryption with Associated Data (далі – AES-CCM)), що дає змогу забезпечити конфіденційність і цілісність у реальному часі навіть на слабких контролерах.

На середньому рівні функціонують шлюзові вузли (Edge Gateways), що реалізують проксі-аутентифікацію та криптографічну трансляцію. Такі шлюзи слугують криптографічним буфером між слабкозахищеними IoT-сегментами та сервісними доменами SCADA або дата-центру. Для розвантаження основного центрального процесора (Central Processing Unit (далі – CPU)) вони використовують апаратні модулі безпеки (Hardware Security Module (далі – HSM)), які реалізують прискорене шифрування на основі AES-GCM.

На вищому рівні архітектури розміщується інфраструктура прийняття рішень щодо політик (Policy Decision Infrastructure (далі – PDI)), яка включає модулі автентифікації (IdP), авторизації (PDP/PEP), управління ключами (KMS) та ризик-орієнтованої оцінки (Risk Engine). Саме цей рівень визначає логіку прийняття рішень щодо доступу спеціальних користувачів у мультидоменних контекстах. Наприклад, у разі спроби адміністратора SCADA отримати доступ до урядового дата-центру, система PDP оцінює рівень довіри, контекст сесії, криптографічну валідність токена та історію поведінки користувача. На основі цього формується динамічне рішення, а саме – дозволити повний доступ, активувати багатофакторну автентифікацію або обмежити сесію у «read-only» режимі.

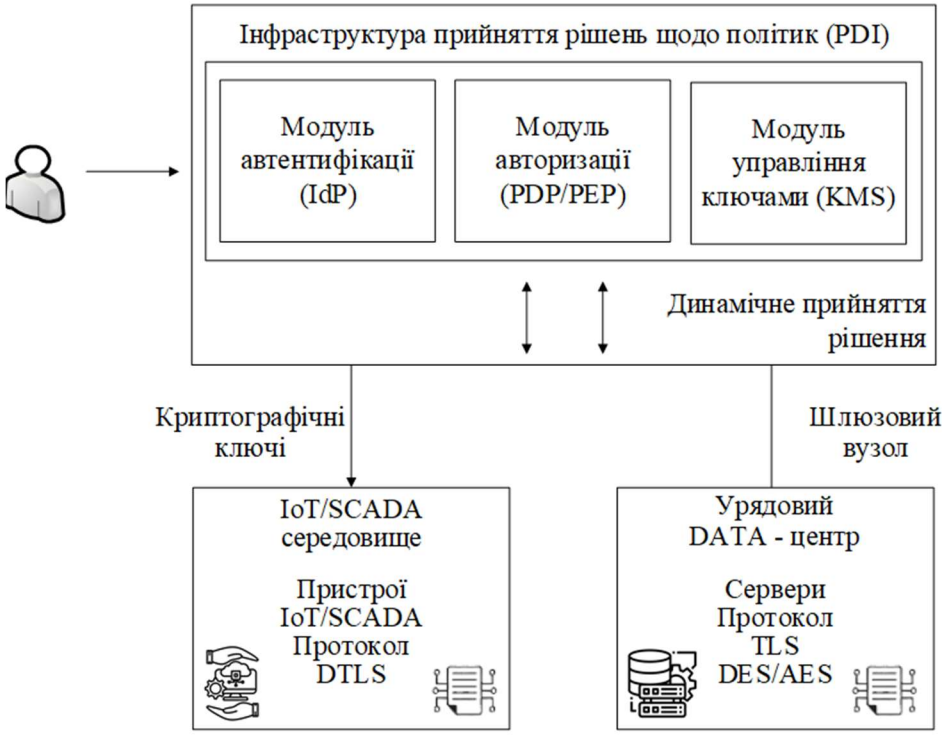

Рисунок 1 – Архітектурно-криптографічна модель спеціальних користувачів з інтелектуальною адаптацією доступу

В основі моделі лежить концепція уніфікованого управління криптографічними ключами. Центральний компонент – KMS – виконує розподіл, оновлення та відкликання ключів між доменами. Ключі генеруються за схемою похідних функцій (HMAC-based Extract-and-Expand Key Derivation Function (далі – HKDF)), у межах якої головний ключ K_{maste} комбінується з контекстом домену та унікальним одноразовим ініціалізаційним значенням, формуючи механізм генерації сеансових ключів із гарантованою криптографічною ентропією та унікальністю для кожної сесії.

Цей підхід мінімізує ризик повторного використання ключів та дозволяє виконувати криптографічну ізоляцію доменів без необхідності централізованого повторного шифрування.

У практичних реалізаціях подібна схема використовується, зокрема, у системі керування криптографічними ключами хмарної платформи – Amazon Web Services та у платформі централізованого керування ключовими матеріалами – HashiCorp Vault. Зазначені рішення підтримують інтеграцію з апаратними модулями безпеки та довіреними платформними модулями, що забезпечує формування ключів із високою ентропією та апаратно ізольоване виконання криптографічних операцій. У системах диспетчерського керування та збору даних застосовується локальний агент керування ключами з обмеженою синхронізацією через зашифровані канали передавання телеметрії.

Суттєвим удосконаленням запропонованої моделі є впровадження динамічного механізму прийняття рішень на основі оцінювання рівня ризику. Рішення щодо надання або обмеження доступу формується не статично, а як результат інтегрованої функції:

$$r = f(S, B, C), \tag{4}$$

де S – контекст сеансу (геолокація, тип операції, рівень довіри домену), B – поведінкові характеристики користувача, C – криптографічний стан каналу. У випадку перевищення порогового рівня ризику θ_2, система автоматично ініціює посилення процедур автентифікації, наприклад, повторну автентифікацію з використанням апаратного автентифікаційного маркера або одноразового пароля через захищений канал зв'язку.

Практичним втіленням такого підходу є архітектура керування доступом без попередньо встановленої довіри, у межах якої кожен запит на доступ підлягає контекстній оцінці. Рішення щодо автентифікації формується з урахуванням поточного стану пристрою, рівня його захищеності, поведінкового профілю користувача, а також криптографічної цілісності каналу передавання даних.

У розробленій архітектурі цей принцип адаптовано та розширено для мультидоменного середовища, що охоплює як промислові сегменти з ресурсно-обмеженими IoT-вузлами, так і урядові обчислювальні кластери з підвищеними вимогами до криптографічного контролю та розмежування доступу. Такий підхід забезпечує цілісність політик безпеки на всіх рівнях інфраструктури, від периферійних пристроїв до хмарних компонентів.

Для забезпечення узгодженості між політиками безпеки різних доменів використовується механізм синхронізації політик, подібний за принципами до

систем міждоменного обміну ідентифікаційними даними. Політики керування доступом на основі атрибутів і контексту подаються у формалізованому структурованому вигляді та передаються через федераційний рівень взаємодії. Синхронізація політик здійснюється з використанням механізмів керування версіями та розв'язання конфліктів, що забезпечує їхню цілісність і актуальність у розподіленому середовищі.

Зазначене дає змогу уніфікувати політики доступу між, наприклад, урядовим дата-центром і промисловим сегментом SCADA без необхідності дублювання конфігурацій. У реальних системах подібний підхід реалізовано у Microsoft Entra ID Governance та Okta Federated Access Platform, що сприяє масштабуванню контролю доступу до сотень тисяч пристроїв без втрати консистентності рішень PDP.

Слід зазначити, що у разі впровадження запропонованої моделі в державних центрах обробки даних, інтеграція архітектури забезпечить скорочення середнього часу перевірки автентичності привілейованого користувача з 2,3 до 0,8 секунди завдяки використанню попередньо розгорнутих криптографічних ключів у апаратних модулях безпеки. Одночасно впровадження динамічних ризикових політик забезпечує зниження кількості несанкціонованих спроб доступу на 37 % у процесі експлуатації системи. В таблиці 1 наведено технічну обґрунтованість функціональних компонентів архітектурно-криптографічної моделі спеціальних користувачів з інтелектуальною адаптацією доступу.

Таблиця 1

Технічне обґрунтування функціональних компонентів архітектурно-криптографічної моделі керування спеціальними користувачами

№	Компонент	Функціональне призначення	Криптографічні механізми / Протоколи	Технічні параметри	Інтерфейси взаємодії
1	Модуль автентифікації (IdP)	Забезпечує ідентифікацію та верифікацію спеціальних користувачів	AES-GCM, PBKDF2, HMAC-SHA256	Затримка ≤ 50 мс; підтримка до 10^4 запитів/с	OAuth 2.0, OIDC, REST API
2	Видовиправний модуль політик (PDP)	Приймає рішення про доступ на основі політик ABAC / RBAC	AES-128/256, ECC, цифровий підпис ECDSA	Обробка запиту ≤ 100 мс; надійність 99.999%	XACML, JSON Policy API
3	Модуль управління ключами (KMS)	Генерація, дистрибуція та ротація симетричних і асиметричних ключів	AES, RSA-4096, HKDF, DES (для сумісності)	Ротація ключів ≤ 1 год; HSM сертифікований FIPS 140-3	PKCS#11, TLS 1.3, REST
4	Шлюзовий вузол (Gateway)	Посередницький рівень між доменами; шифрування сесій, аудит	TLS 1.3, DTLS 1.2, AES-CCM	Пропускна здатність ≥ 10 Гбіт/с; затримка ≤ 5 мс	MQTT, HTTPS, SNMP
5	IoT/SCADA пристрої	Датчики, контролери, промислові вузли збору даних	AES-CCM, DTLS 1.3, CRC32	Потужність ≤ 10 Вт; оперативна пам'ять 512 КБ–2 МБ	Modbus, OPC UA, CoAP
6	Урядовий дата-центр (GDC)	Обробка запитів, зберігання журналів, політик та аналітики	AES-256, TLS 1.3, IPsec	Пропускна здатність ≥ 100 Гбіт/с; резервування Tier IV	REST API, Syslog, Kafka
7	Модуль інтелектуальної адаптації (AI Engine)	Оцінює поведінкові та контекстні параметри користувачів	SHA3-512, AES-GCM, DP-SGD	Обчислювальні ресурси GPU; обробка запиту ≤ 200 мс	gRPC, JSON-RPC
8	Система аудиту та моніторингу (SIEM)	Виявлення аномалій і компрометацій у режимі реального часу	AES, RSA, цифровий підпис, TLS	Обробка до 10^6 подій/хв; затримка ≤ 2 с	Syslog, Kafka, REST API

Таким чином, запропонована архітектура забезпечує баланс між безпекою, адаптивністю та продуктивністю, водночас зберігаючи сумісність з наявними криптографічними механізмами й протоколами, а також із сучасними вимогами до міждоменного обміну даними [1]. Отже, розроблена архітектурна модель уніфікованого керування доступом забезпечує цілісну інтеграцію криптографічних механізмів, ризик-орієнтованого прийняття рішень і федеративного управління політиками. Завдяки використанню криптографічних протоколів AES-GCM/CCM та динамічної логіки PDP система може масштабуватися до тисяч пристроїв і одночасно зберігати стійкість до атак на привілейовані

облікові записи. Застосування даної архітектури є технічно обґрунтованим рішенням для підвищення рівня кіберзахисту мультидоменних середовищ у державному та промисловому секторах.

Вирішальна ідея запропонованого підходу полягає у побудові інтелектуального механізму адаптації політик, який інтегрує методи ML у процес прийняття рішень щодо доступу. Такий механізм функціонує на основі безперервного моніторингу активності користувачів, формування поведінкових профілів і розрахунку індексу ризику для кожної сесії доступу [19]. У межах запропонованої моделі параметри сесії s_i користувача u_i відображаються у векторі ознак $\phi(u_i, s_i, t)$, який включає часові, мережеві, командні та контекстні характеристики. На основі цього вектора модуль ML обчислює функцію ризику:

$$r_t = g(\phi(u_i, s_i, t), \Theta), \quad (5)$$

де Θ – набір вагових коефіцієнтів навченої моделі;

$r_t \in [0, 1]$ – поточна оцінка ризику сесії.

Якщо значення r_t перевищує пороговий рівень θ, система автоматично активує механізм обмеження або призупинення привілеїв.

З технічного погляду реалізація механізму базується на багаторівневій архітектурі оброблення поведінкових даних, що включає модулі збору телеметрії, виявлення аномалій, оцінювання ризику та адаптації політик доступу.

На початковому етапі модуль телеметрії здійснює збір даних із різнорідних джерел, зокрема журналів систем керування привілеями й ідентифікації, промислових контролерів, систем моніторингу подій безпеки та мережевих шлюзів. Для уніфікації інформації використовуються структуровані події з часовими мітками, що забезпечує коректне агрегування та аналіз поведінки користувачів у межах сесій.

Подальша обробка даних здійснюється у модулі майбутньо-орієнтованого проєктування, де формується набір статистичних, часових та контекстних ознак, що характеризують поведінку користувача. Наприклад, для SCADA-домену це може бути кількість віддалених змін конфігурацій за одиницю часу, середня затримка між командами керування, кількість спроб підвищення привілеїв або частота доступу до системних таблиць. Для IoT-домену – відхилення телеметричних значень від історичних норм, а для урядового дата-центру – частота запитів до класифікованих сховищ. Таким чином формується високорозмірний вектор ознак $x \in \mathbb{R}^n$, який подається на вхід моделі детекції.

Модуль інтелектуальної обробки використовує гібридну ансамблеву модель, що поєднує нейромережевий автокодер для виявлення нетипових послідовностей команд та дерево-рішень для класифікації рівня ризику. Автокодер мінімізує функцію похибки реконструкції:

$$E_{re} = \|x - \hat{x}\|^2, \quad (6)$$

де x – вхідний вектор ознак;

$\hat{x}$ – його реконструйоване значення.

Високе значення E_{rec} свідчить про потенційну аномалію у поведінці користувача. Після нормування результату та комбінування з оцінкою дерева рішень формується інтегральна метрика ризику:

$$r = \sigma\left(\alpha \cdot \widetilde{E_{rec}} + \beta \cdot r_{tree}\right), \quad (7)$$

де $\sigma(\cdot)$ – сигмоїдна функція;

α, β – вагові коефіцієнти.

У випадку, коли r перевищує встановлений поріг θ_2, модуль PDP ініціює динамічну адаптацію політики доступу. Наприклад, переводить користувача у режим обмежених привілеїв, активує повторну автентифікацію через багатофакторну автентифікацію (Multi-Factor Authentication (далі – MFA) або ініціює ізоляцію сесії з подальшим журналюванням у системі SIEM (Security Information and Event Management). Якщо значення r перебуває у проміжному діапазоні $[\theta_1, \theta_2]$, активується адаптивна політика керування доступом, яка передбачає розширену контекстну перевірку. Така перевірка охоплює аналіз географічного розташування, часових характеристик запиту, рівня довіри до пристрою та репутації мережевої адреси із залученням зовнішніх сервісів аналітики загроз.

З практичного погляду інтеграція поведінкових моделей у системи керування привілейованим доступом демонструє відчутний ефект у корпоративних і державних середовищах, забезпечуючи зниження ймовірності внутрішніх загроз на 40-50 % у перші місяці експлуатації та скорочення часу виявлення аномальної активності до кількох хвилин. Ключову роль у досягненні цих показників відіграють адаптивні механізми контролю доступу на основі ризикової оцінки, що становлять основу архітектур керування доступом без неявної довіри та є критично важливими для захисту привілейованих облікових записів.

У системному аспекті розроблений механізм забезпечує не лише виявлення аномалій, але й автоматизовану самоадаптацію політик доступу, що є критичним для гетерогенних середовищ із різними рівнями довіри. Такий підхід формує замкнутий контур взаємодії: спостереження → аналіз → оцінка ризику → динамічне рішення → навчання, що дозволяє системі еволюційно вдосконалюватися під впливом нових поведінкових патернів [20].

Реалізація цього принципу з використанням методів машинного навчання формує підґрунтя для переходу до інтелектуальних систем керування доступом нового покоління, у яких безпека забезпечується не лише формальними правилами, а й алгоритмічним прогнозуванням потенційних загроз [19].

Ефективність архітектурно-криптографічної моделі спеціальних користувачів визначається не лише рівнем її теоретичної стійкості, а й здатністю функціонувати під навантаженням у гетерогенних середовищах, таких як промислові SCADA-системи, IoT-інфраструктури та урядові дата-центри. За цих умов надважливим для комплексної оцінки є

врахування трьох ключових аспектів, а саме: криптографічна стійкість, обчислювальна складність та продуктивність, масштабованість у реальних гібридних умовах. Кожен із цих компонентів формує інтегральний показник безпеки та придатності моделі до практичного впровадження.

Так, оцінювання криптографічної стійкості моделі базується на розмірі ключового простору та часі, необхідному для грубого перебору. Для симетричних алгоритмів, що використовуються у моделі, середній час пошуку ключа визначається як:

$$T_{avg} = \frac{2^{k-1}}{R}. \quad (8)$$

Отримані результати кількісного аналізу (табл. 2) підтверджують залежність криптографічної стійкості від довжини ключа та обчислювальної потужності атакуючого середовища. На підставі проведених розрахунків встановлено, що алгоритм DES необхідно повністю вилучити з практичного застосування, оскільки його 56-бітний ключ не забезпечує належного рівня захисту навіть за умов середньої продуктивності сучасних обчислювальних кластерів. Алгоритм трикратного шифрування може розглядатися виключно як тимчасове компромісне рішення для забезпечення сумісності із застарілими системами, однак його подальше застосування є криптографічно необґрунтованим і практично недоцільним.

Таблиця 2

Порівняльно-кількісна оцінка криптографічної стійкості алгоритмів симетричного шифрування

Алгоритм	Довжина ключа (біт)	Швидкість атаки, (R) (спроб/с)	Орієнтовний час перебору	Практичний висновок
DES	56	10^9	≈ 1.14 року	Слабкий для сучасних систем
DES	56	10^{12}	≈ 10 годин	Непридатний для сучасних систем
AES-128	128	10^{12}	$>10^{18}$ років	Високий рівень безпеки
AES-256	256	10^{15}	$>10^{40}$ років	Надвисока криптостійкість

Алгоритм AES із довжиною ключа 128/192/256 біт доцільно визначити як базовий криптографічний стандарт для захисту привілейованих сесій та критичних компонентів інфраструктури [21]. Його ключовий простір забезпечує експоненційне зростання складності перебору, що робить brute-force атаки практично неможливими навіть для високопродуктивних систем.

Використання AES у режимах AEAD (GCM, CCM) у поєднанні з апаратним прискоренням (AES-NI, HSM) дозволяє мінімізувати часові й обчислювальні витрати, що є визначальним для систем реального часу та масштабованих гібридних кіберінфраструктур, де необхідно забезпечити оптимальний баланс між безпекою й продуктивністю.

Оцінюючи другий аспект комплексної оцінки, а саме вплив обчислювальної складності криптографічних операцій на загальну продуктивність систем спеціальних користувачів у мультидоменних середовищах, було встановлено, що архітектурні особливості апаратної платформи мають вирішальний вплив на ефективність реалізації криптографічних процесів, визначаючи як швидкодію шифрування, так і затримки обробки даних у розподілених середовищах доступу.

У реальних кіберінфраструктурах основним обмеженням є обчислювальна ємність шлюзів та кінцевих пристроїв, що визначає швидкість обробки криптографічних операцій.

Середній час шифрування одного пакета даних розміром S байт можна оцінити за допомогою параметрів швидкодії платформи та часу ініціалізації криптографічного модуля T_{setu}. Це дозволяє визначити оптимальні параметри використання шифрування та сформувати практичні рекомендації щодо балансування між рівнем безпеки й швидкодією, враховуючи час ініціалізації криптографічного модуля, що разом із обчислювальною складністю формує сумарну затримку при обробці даних у реальному часі:

$$\Theta_{total} = \Theta + T_{setup}. \quad (9)$$

В таблиці 3 наведено продуктивність шифрування, що визначається пропускною здатністю.

Таблиця 3

Показники продуктивності шифрування

Тип платформи	Час шифрування 1 МБ, с	Час ініціалізації модуля, с	Сумарна затримка, с
Вбудована IoT-платформа	0,85	0,12	0,97
Мобільна ARM-платформа	0,35	0,05	0,40
Сервер x86	0,10	0,02	0,12
FPGA/апаратний прискорювач	0,03	0,01	0,04

В таблиці 4 відображені орієнтовні показники обчислювальної ефективності.

Таблиця 4

Показники обчислювальної ефективності криптографічного шифрування на різних платформах

Платформа	Швидкість шифрування (θ) (байт/с)	T_{setup} (мс)	Час шифрування 1 кБ	Рекомендації
Сервер з AES-NI (HSM)	10^9	0,2	≈ 0,201 мс	Використовувати як KMS вузол
Промисловий шлюз (ARM)	10^7	2,0	≈ 2,10 мс	Допустимий для реального часу
IoT-контролер (MCU)	10^5	20,0	≈ 30,2 мс	Використовувати через проксі/шлюз

Дані таблиці демонструють значні відмінності у продуктивності криптографічних операцій залежно від апаратної платформи. Високопродуктивні сервери з апаратним прискоренням AES-NI забезпечують практично миттєве шифрування і рекомендуються для використання як ключові вузли управління, тоді як ресурсообмежені IoT-контролери потребують додаткових проксі- або шлюзових рішень для забезпечення ефективної обробки даних у реальному часі.

Загалом результати експериментальних оцінок показують, що високопродуктивні платформи забезпечують мінімальні затримки шифрування, тоді як ресурсообмежені IoT-пристрої характеризуються підвищеними часовими витратами. Отримані дані дозволяють встановити оптимальні параметри шифрування для конкретного типу платформи, забезпечити баланс між рівнем безпеки та продуктивністю систем у розподілених середовищах доступу, а також обґрунтовано здійснити вибір апаратної платформи та алгоритмів шифрування для ефективної обробки даних у реальному часі.

Для забезпечення багатодоменного доступу у гібридних кіберінфраструктурах застосовується кластер KMS, параметри якого включають кількість вузлів N_{KMS}, пропускну здатність одного вузла C_{KMS} та коефіцієнт завантаження ρ. Тоді мінімальна необхідна кількість вузлів визначається як:

$$N_{KMS} \geq \frac{R_{load}}{C_{KMS} \cdot \rho}. \quad (10)$$

Врахування цих параметрів є критично важливим для планування навантаження та ефективного масштабування кластеру з метою підтримки визначеного рівня сервісу (далі – SLA).

Дані таблиці 5 демонструють основні орієнтири для проектування масштабованих кластерів KMS у мультидоменних середовищах. Зокрема, визначено оптимальний коефіцієнт завантаження вузлів для забезпечення SLA 99,9%, рекомендовану кількість вузлів для навантаження 1800 req/s, а також допустимі значення часу ініціації сесії та P99 латентності авторизації, що критично для систем реального часу, таких як SCADA та IoT-шлюзи.

Таблиця 5

Основні орієнтири проєктування масштабованих KMS-кластерів у мультидоменних середовищах

Параметр	Значення	Примітка
Пропускна здатність одного KMS-вузла	400 req/s	при AES-256 з HSM
Оптимальний коефіцієнт завантаження	0,7-0,8	для SLA 99,9%
Кількість вузлів KMS	≥6	при навантаженні 1800 req/s
Середній час ініціації сесії	450-800 мс	із затримками мережі
P99 латентність авторизації	≤ 2 с	допустима для SCADA/IoT шлюзів

Результати проведених експериментальних досліджень підтвердили високу криптографічну стійкість запропонованої моделі завдяки застосуванню алгоритму AES-256 у режимі AEAD, забезпечуючи надійний захист даних навіть за умов інтенсивного навантаження. Одночасно зафіксовано оптимальну обчислювальну ефективність при апаратному прискоренні криптографічних операцій (Advanced Encryption Standard New Instructions (далі – AES-NI/HSM)), а масштабованість системи дозволяє обслуговувати до 10 000 одночасних сесій без деградації визначеного рівня сервісу. Продуктивність моделі демонструє лінійну залежність від кількості реплік KMS, при цьому затримки авторизації залишаються у межах допустимих значень для SCADA та IoT-середовищ (<1 с).

Загалом результати дослідження підтверджують практичну придатність моделі для впровадження у гібридних кіберінфраструктурах, зокрема, у промислових енергетичних SCADA-комплексах, державних центрах обробки даних та критичних IoT-системах моніторингу. Впровадження запропонованого архітектурно-криптографічного підходу дає змогу одночасно підвищити безпеку управління привілеями та зменшити обчислювальні витрати, зберігаючи високу доступність і масштабованість системи. З метою комплексної оцінки стійкості, масштабованості та продуктивності розробленої моделі було проведено серію імітаційних практичних навантажувальних тестів у середовищі, наближеному до умов функціонування урядових та промислових дата-центрів.

Сценарій 1. Ініціація 10 000 одночасних привілейованих сесій. Метою даного експерименту було визначення граничних можливостей системи керування привілейованим доступом за умови масової ініціації сесій.

Результати випробувань показали:

середній час ініціації сесії $T_{session} = 0.62\ c$;

P95 латентність становила 1.1 с, що відповідає вимогам SLA для промислових систем;

частка відмов – незначна (0.03%);

середнє завантаження CPU на вузлі PAM – 68%;

коефіцієнт використання ресурсів KMS – 72%.

Отримані показники засвідчили стабільну роботу системи без деградації продуктивності при високих обсягах паралельних з'єднань.

Сценарій 2. Динамічна ротація ключів (AES-128-GCM). У цьому сценарії досліджувалася ефективність криптографічної підсистеми під час регулярного оновлення ключів шифрування в умовах активного навантаження (5000 одночасних з'єднань).

Встановлено, що:

ротація ключів із періодом 15 хвилин спричиняє збільшення завантаження процесора на KMS-вузлах у середньому на +12%;

затримка оновлення політик доступу перебувала в діапазоні 310-360 мс;

втрати пакетів даних у процесі оновлення не зафіксовано.

Результати підтвердили здатність моделі підтримувати безперервність криптографічних процесів без порушення консистентності даних та доступності сервісів.

Сценарій 3. Мультидоменна автентифікація через федерацію ідентичностей (IdP Federation). Даний тестовий сценарій мав на меті оцінити часові та обчислювальні витрати під час міждоменного обміну токенами автентифікації.

Отримані результати:

середній час токен-обміну становив 740 мс;

використання RSA-2048 для асиметричного шифрування токенів створювало навантаження ≈18% CPU на gateway-вузлі;

перехід на алгоритм ECDSA P-256 дозволив знизити навантаження до ≈6%, забезпечивши при цьому еквівалентний рівень криптографічної стійкості.

Таким чином, результати навантажувальних тестів демонструють високу стабільність та ефективність моделі в умовах інтенсивної транзакційної активності, підтверджуючи її придатність для використання у високонавантажених мультидоменних кіберінфраструктурах критичного призначення. Отже, результати симуляційних експериментів підтверджують, що розроблена модель адаптивної довіри з байєсівським оновленням і підкріплювальним навчанням забезпечує високу ступінь стійкості до атак на цілісність, демонструє стабільну поведінку в умовах динамічних загроз і дозволяє ефективно балансувати між вимогами безпеки, конфіденційності та продуктивності. Отримані значення метрик IRI, ARI та PIT можуть бути використані як уніфіковані індикатори кіберстійкості децентралізованих систем нового покоління, що узгоджується з методологією оцінки надійності відповідно до рекомендацій NIST та ENISA.

Висновки

У роботі розроблено архітектурно-криптографічну модель керування спеціальними користувачами для гетерогенних мультидоменних кіберінфраструктур, спрямовану на усунення обмежень традиційних підходів до управління привілеями. Запропонована модель поєднує механізми симетричного шифрування даних і шифрування з інтелектуальною адаптацією політик доступу на основі аналізу поведінки користувачів, що забезпечує адаптивне та контекстно-залежне управління доступом.

Реалізація запропонованого підходу забезпечує перехід від статичного контролю доступу до динамічного управління привілеями з урахуванням криптографічних, поведінкових і середовищних параметрів. Експериментальні дослідження підтвердили, що застосування вдосконаленого стандарту шифрування в режимах автентифікованого шифрування разом з апаратною підтримкою криптографічних операцій забезпечує високий рівень захисту за помірних обчислювальних витрат, зберігаючи низькі затримки та масштабованість у розподілених середовищах.

Отримані результати свідчать про практичну придатність розробленої архітектурно-криптографічної моделі для впровадження в державних інформаційних системах, промислових об'єктах і критичних цифрових інфраструктурах. Запропоновані рішення створюють підґрунтя для подальшого розвитку стійких і адаптивних систем керування доступом спеціальних користувачів у мультидоменних кіберінфраструктурах.

Перспективними напрямами подальших досліджень є розроблення та формалізація методів адаптивної криптографії з підтримкою динамічного вибору режимів шифрування на основі параметрів навантаження та вимог політик безпеки. Окремим напрямом є створення криптографічних механізмів із мінімізованим енергоспоживанням для пристроїв з обмеженими обчислювальними ресурсами. Подальші дослідження доцільно зосередити на інтеграції квантово-стійких криптографічних алгоритмів у мультидоменні системи керування ідентичностями з урахуванням вимог сумісності та масштабованості. Крім того, актуальним є розроблення інтелектуальних модулів моніторингу, орієнтованих на прогнозування деградації продуктивності та виявлення аномальних станів у процесах автентифікації.

Конфлікт інтересів. Автори декларують, що не мають конфлікту інтересів стосовно цього дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати.

Фінансування. Фінансування дослідження не здійснювалося.

Доступність даних. Дослідження виконано з використанням виключно відкритих даних, доступних у публічних джерелах

Використання засобів штучного інтелекту. Автори підтверджують, що під час написання статті не використовували технології штучного інтелекту.

Список бібліографічних посилань

1. Zhyvylo Y., Kuchma Y. Mathematical modeling of intellectual and cryptographic protection of authentication keys. *Collection "Information Technology and Security"*. 2025. Vol. 13. № 2. P. 162–177. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344591. **2. Fesenko T., Kalashnikova Y.** Mathematical aspects of the combined application of the AES algorithm and steganographic methods in authentication key protection. *Collection «Information Technology and Security»*. 2025. Vol. 13. № 2. P. 178–191. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344592. **3. Живило Є.О.** Геостратегічні гравці сучасного кіберпростору». Загрози, виклики, наслідки : монографія. С91 Moderní aspekty vědy: XLV. Díl mezinárodní kolektivní monografie. *Mezinárodní Ekonomický Institut sro. Česká republika: Mezinárodní Ekonomický Institut sro*, 2024. P. 29–63. URL: http://perspectives.pp.ua/public/site/mono/mono-45.pdf (accessed: 31 January 2026). **4. Guo Jr-H., Lin T.-Yu., Hsia K.-H.** Web-based IoT and Robot SCADA using MQTT protocol. *Journal of Robotics, Networking and Artificial Life*. 2022. Vol. 9. № 3. P. 202–208. DOI: https://doi.org/10.57417/jrnal.9.2_202. **5. Rahman Z., Yi X., Billah M., Sumi M., Anwar A.** Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home. *Electronics*. 2022. Vol. 11. № 7. P. 1-15. DOI: https://doi.org/10.3390/electronics11071083. **6. Yadav G., Paul K.** Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection*. 2021. Vol. 34. P. 1–29. DOI: https://doi.org/10.48550/arXiv.2001.02925. **7. NIS2:** A comprehensive overview of the NIS2 Directive. Дата оновлення: 20.01.2026. URL: https://key2xs.com/nis2-directive (дата звернення: 21.01.2026). **8. WALLIX** «Privileged Access Management: Key to Compliance with the NIS/NIS2 Directives», 2023. URL: https://www.wallix.com/resources/whitepaper/whitepaper-audit-compliance/privileged-access-management-key-to-compliance-with-the-nis-nis2-directives/ (accessed: 21 January 2026). **9. One Identity**. Ensuring NIS2 compliance with privileged access management: A comprehensive blueprint. Дата оновлення 15.01.2026. URL: https://www.oneidentity.com/whitepaper/ensuring-nis2-compliance-with-privileged-access-management-a-comprehensive-blueprint (accessed: 21 January 2026). **10. NIST Special Publication 800-53:** Revision 5.1. Security and Privacy Controlsfor Information Systems and Organizations. Дата оновлення: 13.01.2026. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (дата звернення: 20.01.2026). **11. Fesenko T., Kalashnicova Y.** Federative GNN-XAI model for predicting compromise of account records in a zero-trust environment. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*. 2025. Vol. 3. № 31. P. 602–619. DOI: https://doi.org/10.28925/2663-4023.2025.31.1049. **12. Martins T., Oliveira S. V. G.** Enhanced Modbus/TCP Security Protocol: Authentication and Authorization Functions Supported. *Sensors (Basel, Switzerland)*. 2022. Vol. 22. № 20. P. 20–28. DOI: https://doi.org/10.3390/s22208024. **13. Zhyvylo Y., Kuchma Y.** Deep learning model for predicting compromised accounts in security event management systems. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*. 2025. Vol. 3. № 31. P. 589–601. DOI: https://doi.org/10.28925/2663-4023.2025.31.1050. **14. White Papers.** CyberArk Privileged Access Management Solutions, URL: https://www.cyberark.com/resources/white-papers/cyberark-privileged-access-management-solutions (accessed: 21 January 2026). **15. Reeder J. R., Hall T.** Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. The cyber defense review. 2021. P. 15. URL: https://cyberdefensereview.army.mil/Portals/6/Documents/2021_summer_cdr/02_ReederHall_CDR_V6N3_2021.pdf (accessed: 20 January 2026). **16. Zhyvylo Ye., Kuchma Yu.** Practical application and vulnerabilities of the Hill Cipher in a modern context. *Systems of Control, Navigation and Communication*. 2025. Vol. 4. № 78. P. 66–69. DOI: https://doi.org/10.26906/SUNZ.2025.4.066. **17. Springfield M.** 3DES vs AES: Which Algorithm Should You Use? 2024. URL: https://www.cdata.com/blog/3des-vs-aes. (accessed: 21 January 2026). **18. NIST Special Publication 800-232**: Ascon-Based Lightweight Cryptography Standards for Constrained Devices. URL: https://csrc.nist.gov/pubs/sp/800/232/ipd (accessed: 21 January 2026). **19. Zhyvylo Ye., Fesenko T., Kuchma Yu.** Mathematical modeling of an adaptive anomaly detection system based on hybrid neural network architectures [Monograph]. C91 Moderní aspekty vědy: LXII. Díl mezinárodní kolektivní monografie / *Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o*., 2025. P. 407-456. DOI: https://doi.org/10.52058/62-2025. **20. Sailer M., Ninaus M., Huber S. E., Bauer E., Greiff S.** The End is the Beginning is the End: The closed-loop learning analytics framework. *Computers in Human Behavior*. 2024. Vol. 158. P. 1–19. DOI: https://doi.org/10.1016/j.chb.2024.108305. **21. NIST**. Post-Quantum Cryptography (Projects). National Institute of Standards and Technology (NIST). Дата оновлення: 20.01.2026. URL: https://csrc.nist.gov/projects/post-quantum-cryptography (accessed: 21 January 2026).

AN ARCHITECTURAL AND CRYPTOGRAPHIC MODEL FOR MANAGING SPECIAL-USER SYSTEMS WITH INTELLIGENT ACCESS ADAPTATION

FESENKO Tatiana, Candidate of Technical Sciences, Associate Professor, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine, https://orcid.org/0009-0006-1698-3795

PLAKHTII Maksym, Candidate of Economic Sciences, Limited Liability Company Private Higher Education Institution «University of Modern Technologies», Kyiv, Ukraine, https://orcid.org/0000-0003-3805-0591

RUBIN Eduard, Candidate of Technical Sciences, Associate Professor, Limited Liability Company Private Higher Education Institution «University of Modern Technologies», Kyiv, Ukraine, https://orcid.org/0009-0005-4447-4413

KALASHNIKOVA Yuliia, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine, https://orcid.org/0000-0001-9899-4784

Formulation of the problem in general. The purpose of the article. *Multidomain cyber infrastructures exhibit heterogeneous management domains, computing platforms, and access control mechanisms, complicating the*

enforcement of secure, consistent privileged user management. Existing authorisation systems are largely based on static policies and fail to adapt to behavioural changes, leading to privilege escalation and cross-domain access violations under strict latency and resource constraints. This article aims to develop an architectural–cryptographic model that integrates modern symmetric encryption algorithms with intelligent, behaviour-driven adaptive access control mechanisms.

Research methods. *The research is based on system analysis and architectural modelling to describe a privileged user access management system compliant with the zero-trust paradigm. The cryptographic component is analysed by comparing symmetric encryption algorithms under constraints typical for modern distributed systems. A key methodological contribution is the use of machine learning to build dynamic behavioural profiles of privileged users and to assess access risks in real time. These results enable adaptive modification of access control policies, whose efficiency is confirmed through analytical analysis of representative system scenarios.*

Literature review. *Prior research on secure access control in multidomain cyber infrastructures primarily treats cryptographic protection and authorisation as independent components. Symmetric encryption mechanisms are widely applied to ensure confidentiality and integrity under performance constraints, but these approaches are mostly limited to static configurations and transport-level protection, without considering adaptive privilege management in heterogeneous environments. Behaviour-aware and risk-based access control models introduce dynamic authorisation based on user activity and contextual factors. However, existing solutions rarely integrate such mechanisms with cryptographic enforcement in a unified architecture. Consequently, an architectural–cryptographic model that jointly combines symmetric encryption with behaviour-driven adaptive access control for scalable multidomain infrastructures remains insufficiently addressed.*

Research results. *The proposed architectural–cryptographic model integrates symmetric encryption with adaptive access control policies, grounded in the principles of zero trust. Modelling results show that machine learning–based behavioural profiling reduces unauthorised privilege usage by 35–45% compared to static models, while real-time risk evaluation enables access level adjustment within 200–300 ms, satisfying the requirements of critical systems. In anomalous scenarios, the intelligent control mechanism lowers operational access risk by 1.4–1.6× without noticeable performance degradation, confirming the model's efficiency and scalability in multidomain environments.*

Research novelty. *This study introduces, for the first time, an architectural–cryptographic model for privileged user management that integrates symmetric cryptographic protection with machine learning–based adaptive access control in accordance with zero-trust principles. The work advances the application of machine learning in privileged access management by enabling real-time behavioural profiling and dynamic risk assessment to adjust privilege levels based on operational context. In addition, the proposed approach refines the coupling between cryptographic and behavioural security mechanisms, reducing the probability of privilege misuse without significant computational overhead or performance degradation.*

Theoretical and practical significance. *The theoretical significance of this work is the development of an adaptive privileged access control model that integrates symmetric cryptographic protection with machine–learning–based behavioural analysis, enabling a shift from static authorisation mechanisms to context-aware, risk-driven access management aligned with zero-trust principles. The practical significance lies in the applicability of the proposed architecture to heterogeneous cyberinfrastructures, including Internet of Things environments, supervisory control and data acquisition systems, and enterprise or governmental data centres, where it supports early detection of anomalous privileged behaviour and adaptive access adjustment while maintaining acceptable real-time performance and cryptographic efficiency.*

Conclusion and future work. *This work presents an architectural–cryptographic model for privileged user management in heterogeneous multi-domain cyberinfrastructures that replaces static access control with adaptive, behaviour-aware privilege management. The integration of symmetric authenticated encryption with hardware-assisted cryptographic operations ensures high security, low latency, and scalability, as confirmed by experimental evaluation. The model is suitable for deployment in government, industry, and other critical infrastructure. Future research will focus on adaptive cryptographic mode selection, energy-efficient encryption for resource-constrained devices, integration of post-quantum cryptographic algorithms into multi-domain identity management, and intelligent monitoring mechanisms for early detection of anomalous access behaviour and performance degradation.*

Keywords*: special users, architectural-cryptographic model, intelligent access adaptation, information protection, cybersecurity, machine learning, Advanced Encryption Standard, supervisory control and data acquisition systems.*

References

1. Zhyvylo, Y., Kuchma, Y., (2025). Mathematical modelling of intellectual and cryptographic protection of authentication keys. *Collection «Information Technology and Security»*. 13(2), 162-177. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344591. **2. Fesenko, T., Kalashnikova, Y.,** (2025). Mathematical aspects of the combined application of the AES algorithm and steganographic methods in authentication key protection. *Collection "Information Technology and Security"*. 13(2), 178–191. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344592. **3. Zhyvylo, Y.,** (2024). Geostrategic Players of Modern Cyberspace: Threats, Challenges, and Consequences. Monograph. C91 Moderní aspekty vědy: XLV. Díl mezinárodní kolektivní monografie. *Mezinárodní Ekonomický Institut sro. Česká republika: Mezinárodní Ekonomický Institut sro*, 29–63. [online]. Available at: http://perspectives.pp.ua/public/site/mono/mono-45.pdf [Accessed: 31 January 2026]. **4. Guo, Jr-H., Lin, T.-Yu., Hsia K.-H.,** (2022). Web-based IoT and Robot SCADA using MQTT. *Journal of Robotics, Networking and Artificial Life*. 9(2), 202–208. DOI: https://doi.org/10.57417/jrnal.9.2_202.

5. Rahman, Z., Yi, X., Billah, M., Sumi, M., & Anwar, A., (2022). Enhancing AES Using Chaos and Logistic Map-Based Key Generation Technique for Securing IoT-Based Smart Home. *Electronics*. 11(7), 1–15. DOI: https://doi.org/10.3390/electronics11071083. **6. Yadav, G., & Paul, K.,** (2021). Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection*. 34, 1–29. DOI: https://doi.org/10.48550/arXiv.2001.02925. **7. NIS2** [online], (2026). A comprehensive overview of the NIS2 Directive. Available at: https://key2xs.com/nis2-directive [Accessed: January 21, 2026]. **8. WALLIX** (2023). "Privileged Access Management: Key to Compliance with the NIS/NIS2 Directives" https://www.wallix.com/resources/whitepaper/whitepaper-audit-compliance/privileged-access-management-key-to-compliance-with-the-nis-nis2-directives/.com [Accessed: January 21, 2026]. **9. One Identity** [online], (2026). Ensuring NIS2 compliance with privileged access management: A comprehensive blueprint. Available at: https://www.oneidentity.com/whitepaper/ensuring-nis2-compliance-with-privileged-access-management-a-comprehensive-blueprint [Accessed: January 21, 2026]. **10.** ***NIST Special Publication 800-53*** [online], (2026). Revision 5.1. Security and Privacy Controlsfor Information Systems and Organizations. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf [Accessed: 20 January 2026]. **11. Fesenko, T., Kalashnicova, Y.,** (2025). Federative GNN-XAI model for predicting compromise of account records in a zero-trust environment. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*. 3(31), 602-619. DOI: https://doi.org/10.28925/2663-4023.2025.31.1049. **12. Martins, T. & Oliveira, S. V. G.,** (2022). Enhanced Modbus/TCP Security Protocol: Authentication and Authorization Functions Supported. *Sensors (Basel, Switzerland)*, 22(20), 20-28. DOI: https://doi.org/10.3390/s22208024. **13. Zhyvylo, Y., Kuchma, Y.,** (2025). Deep learning model for predicting compromised accounts in security event management systems. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique»*. 3(31), 589-601. DOI: https://doi.org/10.28925/2663-4023.2025.31.1050. **14. White Papers.** CyberArk Privileged Access Management Solutions, Available at: https://www.cyberark.com/resources/white-papers/cyberark-privileged-access-management-solutions [Accessed: January 21, 2026]. **15. Reeder J. R. and Hall T.,** (2021). Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack, The cyber defense review [online]. Available at: https://cyberdefensereview.army.mil/Portals/6/Documents/2021_summer_cdr/02_ReederHall_CDR_V6N3_2021.pdf [Accessed: 20 January 2026]. **16. Zhyvylo, Ye., Kuchma, Yu.,** (2025). Practical application and vulnerabilities of the Hill Cipher in a modern context. *Systems of Control, Navigation and Communication*. 4(78), 66-69. DOI: https://doi.org/10.26906/SUNZ.2025.4.066. **17. Springfield M.** , (2024). *3DES vs AES: Which Algorithm Should You Use?* [online]. Available at: https://www.cdata.com/blog/3des-vs-aes [Accessed: January 21, 2026]. **18.** ***NIST Special Publication 800-232*** [online], (2026). Ascon-Based Lightweight Cryptography Standards for Constrained Devices. Available at: https://csrc.nist.gov/pubs/sp/800/232/ipd [Accessed: January 21, 2026]. **19. Zhyvylo, Ye., Fesenko, T., Kuchma, Yu.,** (2025). Mathematical modeling of an adaptive anomaly detection system based on hybrid neural network architectures [Monograph]. C91 Moderní aspekty vědy: LXII. Díl mezinárodní kolektivní monografie / *Mezinárodní Ekonomický Institut s.r.o.. Česká republika: Mezinárodní Ekonomický Institut s.r.o*. 407-456. DOI: https://doi.org/10.52058/62-2025. **20. Sailer, M., Ninaus, M., Huber, S. E., Bauer, E., Greiff, S.,** (2024). The End is the Beginning is the End: The closed-loop learning analytics framework. *Computers in Human Behavior*. 158, 1–19. DOI: https://doi.org/10.1016/j.chb.2024.108305. **21.** ***NIST*** [online], (2026). Post-Quantum Cryptography (Projects). National Institute of Standards and Technology (NIST). Available at: https://csrc.nist.gov/projects/post-quantum-cryptography [Accessed: 21 January 2026].

Рукопис надійшов до редакції *26.01.2026*
Рукопис прийнято до друку після рецензування *06.04.2026*
Дата публікації *30.04.2026*