УДК 621.39:004.056 DOI: 10.31673/2786-8362.2025.028237

Макаренко А.О., д.т.н.; **Жураковський Б.Ю.,** д.т.н.;
Осипчук С.О., к.т.н.; **Григоренко О.Г.,** к.т.н.;
Лемешко А.В., к.т.н.

МЕТОДИ ПОБУДОВИ ЗАХИЩЕНИХ КОМУНІКАЦІЙНИХ КАНАЛІВ ДЛЯ IOT-ПРИСТРОЇВ У МЕРЕЖАХ П'ЯТОГО ПОКОЛІННЯ

Makarenko A.O., Zhurakovskiy B.Yu., Osypchuk S.O., Grygorenko O.G., Lemeshko A.V. Methods for building secure communication channels for IoT devices in fifth-generation networks. The article is devoted to the study of approaches to building secure communication channels for IoT devices in fifth-generation networks. The characteristic threat vectors inherent in heterogeneous 5G-IoT environments are considered, in particular, device substitution, Man-in-the-Middle attacks, DoS/DDoS overload and unauthorized access through weak authentication mechanisms. An architecture for IoT node interaction via the IoT Gateway using Network Slicing, Edge Computing and security mechanisms defined in 3GPP TS 33.501 technologies is proposed. A model of a secure data exchange channel in a 5G-IoT environment is developed. The use of a hybrid cryptographic approach that combines AES-128 with dynamic key generation based on ECC is justified. The developed multi-level authentication algorithm is supplemented with the use of cryptographic fingerprints of devices. The simulation showed a 20–25% reduction in authentication latency and a reduction in computational costs, which confirms the effectiveness of the proposed model for application in smart city systems, industrial IoT, and critical infrastructure.

Keywords: 5G-IoT, secure data exchange model, multi-level authentication algorithm, AES-128/ECC cryptographic method, Network Slicing

Макаренко А.О., Жураковський Б.Ю., Осипчук С.О., Григоренко О.Г., Лемешко А.В. Методи побудови захищених комунікаційних каналів для IoT-пристроїв у мережах п'ятого покоління. Стаття присвячена дослідженню методів побудови захищених комунікаційних каналів для IoT-пристроїв у мережах п'ятого покоління. Розглянуто характерні вектори загроз, властиві гетерогенним 5G-IoT середовищам, зокрема підміна пристроїв, атаки типу Man-in-the-Middle, перевантаження DoS/DDoS та несанкціонований доступ через слабкі механізми автентифікації. Запропоновано архітектуру взаємодії IoT-вузлів через шлюз IoT Gateway з використанням технологій Network Slicing, Edge Computing та механізмів безпеки, визначених у 3GPP TS 33.501. Розроблено модель захищеного каналу обміну даними в середовищі 5G-IoT. Обґрунтовано застосування гібридного криптографічного методу, який поєднує AES-128 із динамічною генерацією ключів на основі ECC. Розроблений алгоритм багаторівневої автентифікації доповнено використанням криптографічних відбитків пристроїв. Моделювання показало зменшення затримки автентифікації на 20–25% і зниження обчислювальних витрат, що підтверджує ефективність запропонованої моделі для застосування в інтелектуальних міських системах, промисловому IoT та критичній інфраструктурі.

Ключові слова: 5G-IoT, модель захищеного обміну даними, алгоритм багаторівневої автентифікації, криптографічний метод AES-128/ECC, Network Slicing

Вступ

Стрімкий розвиток технологій п'ятого покоління мобільного зв'язку (5G) створив нові можливості для інтеграції пристроїв Інтернету речей (IoT) у єдину високошвидкісну комунікаційну інфраструктуру. Завдяки підтримці масових підключень (mMTC), низькій затримці (URLLC) та високій пропускній здатності (eMBB) мережі 5G стали основою для функціонування інтелектуальних систем — від розумних міст і промислових виробництв до автономного транспорту. Проте з розширенням масштабів таких систем суттєво зростає кількість потенційних точок несанкціонованого доступу, що створює нові виклики у сфері кіберзахисту IoT-пристроїв.

У сучасних наукових дослідженнях особлива увага приділяється проблемі забезпечення конфіденційності, цілісності та автентичності даних під час їх передавання між IoT-вузлами та хмарними сервісами. Існуючі методи шифрування та автентифікації, розроблені для традиційних телекомунікаційних мереж, часто є надто ресурсоємними для обмежених обчислювальних можливостей IoT-пристроїв. Тому актуальним напрямом стає розроблення легковагових криптографічних механізмів, протоколів безпечної передачі даних (зокрема,

MQTT-S, DTLS, CoAP з розширеннями безпеки) та архітектурних рішень для побудови захищених комунікаційних каналів у середовищі 5G.

Останні наукові розробки в цій галузі спрямовані на використання технологій мережевої сегментації (network slicing), інтеграції механізмів блокчейн для верифікації транзакцій IoT-пристроїв, а також застосування штучного інтелекту для адаптивного виявлення аномалій у мережевому трафіку. Водночас залишаються невирішеними питання стандартизації методів шифрування для гетерогенних IoT-платформ, оптимізації затримок у процесі автентифікації та забезпечення стійкості каналів зв'язку до складних комбінованих атак.

Проблема побудови захищених комунікаційних каналів для IoT-пристроїв у мережах п'ятого покоління є актуальною як з наукового, так і з практичного погляду. Її розв'язання сприятиме підвищенню рівня кіберзахисту телекомунікаційних систем нового покоління, а також забезпеченню надійної взаємодії між мільярдами пристроїв у глобальному цифровому середовищі.

Аналіз останніх досліджень. У фундаментальному огляді [1], опублікованому в лютому 2025 року, виконано систематизацію критичних категорій безпеки IoT. Автори наголошують, що стрімка інтеграція сенсорних мереж у хмарні середовища створює нові вектори загроз, які неможливо нівелювати застарілими методами без втрати продуктивності. У дослідженні [2] проведено порівняльний аналіз криптографічних алгоритмів (AES, RSA, ECC) саме в контексті 5G-мереж. Автори експериментально доводять, що для ресурсних обмежень IoT найбільш ефективним є відмова від RSA на користь еліптичних кривих (ECC), які забезпечують необхідний рівень ентропії при значно меншій довжині ключа. Питання архітектурного захисту детально розкрито в роботі [3], де класифіковано атаки на технологію Network Slicing. Дослідники пропонують стратегії пом'якшення наслідків (mitigation strategies), що базуються на динамічній ізоляції слайсів для захисту від міжслайсових атак.

Особлива увага в сучасних працях приділяється безсертифікатній автентифікації. Так, у статті IEEE Access [4] запропоновано легковагову схему на основі фізично неклонованих функцій (PUF) та хаотичних карт Чебишева, що дозволяє уникнути зберігання секретних ключів у пам'яті пристрою. Альтернативні методи розглядаються в [5], де на основі систематичного огляду літератури (SLR) оцінено ефективність блокчейн-технологій для забезпечення довіри в IoT, вказуючи на компроміс між децентралізацією та затримками. У роботі [6] аналізуються системи виявлення вторгнень (IDS) на базі штучного інтелекту, які здатні виявляти аномалії в реальному часі, але залишаються вразливими до змагальних атак (adversarial attacks). Проблеми захисту протоколів прикладного рівня підіймаються в [7], де досліджено вразливості MQTT в індустріальному IoT та запропоновано методи протидії DoS-атакам на брокери повідомлень.

Постановка завдання. Масштабне впровадження стільникових мереж 5G відкриває нові сценарії надання послуг, які вимагають низької затримки та гарантованої автентичності даних. Незважаючи на наявність окремих рішень у проаналізованих джерелах [1–7], на сьогодні відсутній комплексний підхід, який би одночасно вирішував проблеми ресурсоємності шифрування, швидкодії автентифікації та ізоляції трафіку. В цій статті буде проведено розроблення та аналіз методу побудови захищених комунікаційних каналів, який поєднує гібридне шифрування AES-128/ECC, автентифікацію за цифровими відбитками (розвиваючи метод PUF з [4]) та технологію Network Slicing (базуючись на принципах [3]), що дозволить усунути недоліки існуючих рішень.

Метою роботи є підвищення ефективності та захищеності інформаційного обміну в гетерогенних IoT-системах мереж п'ятого покоління шляхом розроблення методу побудови комунікаційних каналів, що поєднує гібридне шифрування, автентифікацію за апаратними відбитками та технологію мережевої сегментації.

Виклад основного матеріалу дослідження

Аналіз стану проблеми та наукових методів до забезпечення безпеки обміну даними в IoT-системах. Інтеграція Інтернету речей (IoT) у мережі п'ятого покоління (5G) створює

якісно нове середовище, де критичними вимогами стають не лише швидкість передачі даних, але й надійність їх захисту. Гетерогенність IoT-пристроїв — від простих датчиків до складних промислових контролерів — унеможливлює використання універсальних методів до кібербезпеки, що вимагає детального аналізу існуючих загроз та методів їх нівелювання.

Основною проблемою безпеки в екосистемі 5G-IoT є розширення поверхні атак через масове підключення пристроїв. На основі аналізу вразливостей можна виділити ключові вектори загроз (рис. 1):

– Підміна пристроїв (Device Spoofing): Зловмисник емулює легітимний IoT-вузол для введення некоректних даних у систему або отримання доступу до мережевих ресурсів. В умовах 5G, де ідентифікація часто відбувається автоматично, це створює ризик компрометації цілих сегментів мережі [8].

– Атаки типу "Man-in-the-Middle" (MitM): Перехоплення та можлива модифікація даних під час їх передачі між IoT-пристроєм та базовою станцією (gNodeB). Це особливо небезпечно для критичної інфраструктури, де цілісність команд управління є пріоритетною [9].

– Відмова в обслуговуванні (DoS/DDoS): Обмежені ресурси IoT-пристроїв роблять їх вразливими до виснаження енергії або обчислювальних потужностей через масові запити, що може призвести до відключення критичних сенсорів [10].

– Несанкціонований доступ: Використання слабких механізмів автентифікації (наприклад, заводських паролів) для захоплення контролю над пристроєм [11].

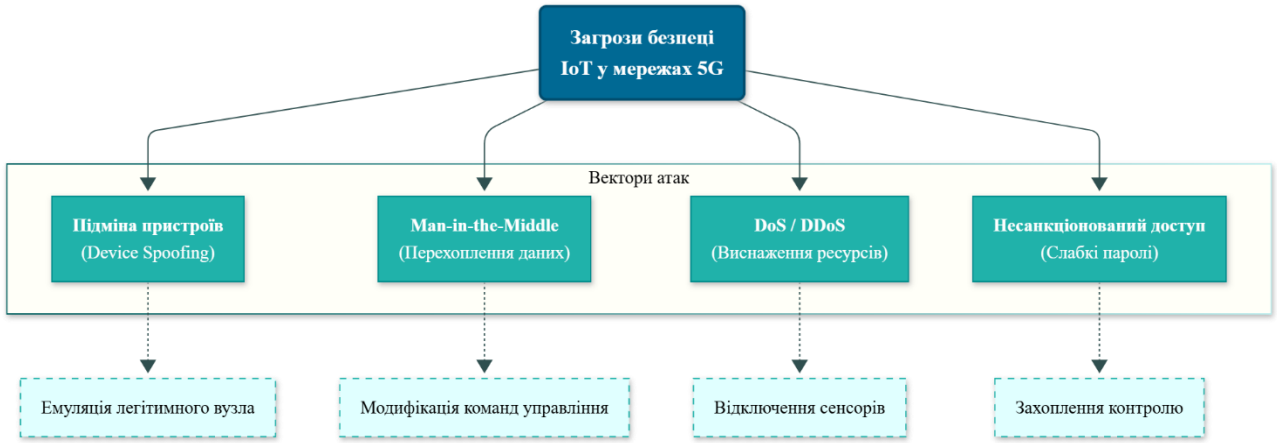

Рис. 1. Класифікація загроз безпеці IoT у мережах 5G

Для захисту каналів зв'язку традиційно використовуються стандартизовані алгоритми шифрування, проте їх застосування в IoT обмежене апаратними можливостями.

Алгоритми шифрування [3,7,12]:

– AES (Advanced Encryption Standard): Забезпечує високу стійкість, проте реалізація повного циклу AES-256 може бути надто енергозатратною для автономних датчиків. Більш доцільним є використання полегшених версій або AES-128.

– ECC (Elliptic Curve Cryptography): Ефективна альтернатива RSA, що дозволяє досягти аналогічного рівня безпеки при значно меншій довжині ключа, що економить трафік та процесорний час.

– LWE (Learning With Errors): Перспективний напрям постквантової криптографії, що розглядається як майбутній стандарт захисту від атак із використанням квантових обчислень.

Легковагові протоколи:

– DTLS (Datagram Transport Layer Security): Адаптація TLS для протоколів на основі UDP. Забезпечує безпеку, але має значний оверхед (накладні витрати) на етапі "рукостискання" (handshake).

– Lightweight CoAP (Constrained Application Protocol): Спеціалізований протокол для IoT, який у поєднанні з об'єктною безпекою (OSCORE) дозволяє мінімізувати навантаження на мережу порівняно з HTTP/TLS.

Ключову роль у захисті інфраструктури відіграють стандарти консорціуму 3GPP. Зокрема, специфікація 3GPP TS 33.501 [12] визначає архітектуру безпеки для 5G Core, вводячи поняття уніфікованої автентифікації, яка не залежить від типу доступу (Wi-Fi, 5G NR, LTE).

Особлива увага приділяється механізму Network Slice Isolation (ізоляція мережевих слайсів). Ця технологія дозволяє розділити фізичну мережу на логічні сегменти (наприклад, окремо для автономного транспорту та окремо для датчиків вологості). Згідно з 3GPP TS 33.501, компрометація пристрою в одному слайсі не повинна впливати на безпеку інших слайсів, що є критично важливим для забезпечення стійкості системи в цілому.

У сучасному науковому дискурсі, окрім розглянутих криптографічних примітивів, активно досліджуються альтернативні концепції побудови захищених комунікацій, кожна з яких має свої переваги та обмеження в контексті мереж п’ятого покоління. Одним із домінуючих напрямів є використання технологій розподіленого реєстру (Blockchain) для децентралізованої верифікації транзакцій та ідентичності пристроїв. Цей метод забезпечує високий рівень прозорості та незмінності даних, усуваючи єдину точку відмови, притаманну централізованим шлюзам. Проте, практична імплементація блокчейн-алгоритмів на ресурсно-обмежених IoT-сенсорах наштовхується на проблему значних енергетичних витрат та затримок при досягненні консенсусу, що часто є неприйнятним для систем реального часу.

Іншим перспективним вектором є застосування методів штучного інтелекту та машинного навчання для адаптивного виявлення аномалій у мережевому трафіку. Такі системи здатні виявляти нові, раніше невідомі типи атак (zero-day attacks), аналізуючи патерни поведінки пристроїв. Однак, на відміну від детермінованих методів автентифікації, AI-рішення мають імовірнісний характер, що створює ризик хибних спрацювань (false positives) та вимагає значних обчислювальних потужностей, які зазвичай недоступні на рівні кінцевих вузлів (Edge devices). Також у літературі розглядаються постквантові методи захисту, зокрема криптографія на ґратках (LWE – Learning With Errors). Хоча ці алгоритми гарантують стійкість до атак із використанням квантових обчислювачів у майбутньому, на даному етапі розвитку технологій вони характеризуються надмірним розміром ключів та шифротекстів, що призводить до перевантаження вузькосмугових каналів зв'язку.

Традиційні ж методи, що базуються на стандартних протоколах DTLS або EAP-IoT, забезпечують високу сумісність обладнання, але часто демонструють надлишковість службового трафіку під час процедури встановлення з’єднання. У порівнянні з ними, методи «чистої» симетричної криптографії є найшвидшими, проте створюють критичні проблеми з безпечним розподілом ключів у масштабованих мережах. Таким чином, аналіз існуючих альтернатив підтверджує актуальність розробки гібридного рішення, яке б поєднувало легковаговість симетричних шифрів, надійність еліптичної криптографії для обміну ключами та жорстку прив’язку до апаратних параметрів пристрою, нівелюючи недоліки вищезгаданих методів.

Теоретичні основи побудови захищеного обміну даними між IoT-пристроями в 5G-мережах. Теоретичне обґрунтування запропонованого рішення базується на необхідності переходу від плоскої моделі підключення до ієрархічної архітектури, де взаємодія масиву IoT-пристроїв із базовими станціями gNodeB опосередковується інтелектуальним шлюзом IoT Gateway. Введення цього проміжного вузла зумовлене проблемою «сигнального шторму» на рівні Control Plane мережі 5G при одночасній реєстрації тисяч пристроїв. У розробленій моделі IoT Gateway виконує роль граничного обчислювального вузла (Edge Node), який реалізує функції попередньої автентифікації та агрегації трафіку, трансформуючи гетерогенні протоколи (CoAP, MQTT) у єдиний потік даних, сумісний із вимогами ядра мережі. Така архітектура дозволяє перенести процедури первинної верифікації з центральних компонентів AMF (Access and Mobility Management Function) на периферію, знижуючи затримки та навантаження на магістральні канали.

Забезпечення цілісності та конфіденційності в такій системі вимагає наскрізної синхронізації захисних механізмів на чотирьох рівнях моделі OSI. На рівні доступу (Access Layer) захист забезпечується механізмами шифрування радіоінтерфейсу PDCP (Packet Data

Convergence Protocol), що запобігає прослуховуванню ефіру між пристроєм та gNodeB. Транспортний рівень (Transport Layer) відповідає за створення захищених тунелів (DTLS для UDP-трафіку), нівелюючи ризики перехоплення пакетів у транзитних вузлах. Мережевий рівень включає механізми фільтрації та маршрутизації, захищені від атак типу IP spoofing, тоді як прикладний рівень (Application Layer) гарантує наскрізне шифрування корисного навантаження (payload) безпосередньо від датчика до хмарного сервісу. Узгодження політик безпеки між цими рівнями покладається на логічну надбудову – Network Slice Security Layer. Цей компонент забезпечує динамічну ізоляцію ресурсів у межах виділеного мережевого слайсу, контролюючи, щоб параметри QoS та протоколи безпеки, активовані для критичних IoT-пристроїв, залишалися недосяжними для трафіку з інших сегментів мережі, навіть у разі компрометації сусідніх віртуальних функцій.

Для коректного формування архітектури захищеного обміну даними було визначено низку припущень і обмежень, які задають межі застосовності запропонованої моделі та дозволяють інтерпретувати результати моделювання у фізично коректному вигляді. Передусім передбачається, що масив IoT-пристроїв генерує переважно низькошвидкісний телеметричний трафік із типовими обсягами пакета до 256 байт та періодичністю надсилання від 1 до 60 секунд. Така характеристика відповідає профілю mMTC-сервісів і дозволяє мінімізувати обчислювальне навантаження при виконанні криптографічних операцій на кінцевих вузлах. Водночас вважається, що пристрої не здійснюють високочастотної потокової передачі даних (наприклад, відео), що могло б змінити вимоги до пропускної здатності каналу та криптографічних механізмів.

Другим припущенням є стабільність параметрів радіодоступу на інтерфейсі між IoT-Gateway та базовою станцією gNodeB. Модель не враховує динаміку радіоканалу на мілісекундному рівні, зокрема ефекти глибокого зникнення сигналу (deep fading), інтерференції або швидкої мобільності, оскільки цільова група пристроїв розташована стаціонарно або напівстаціонарно. Також вважається, що затримка на магістральному сегменті мережі не є домінуючим фактором і не перевищує типових значень для LTE/5G Non-Standalone (10-25 мс).

Обмеження стосуються також реалізації криптографічних механізмів. У моделі припускається, що апаратна підтримка AES-128 доступна на рівні IoT-Gateway, тоді як на кінцевих сенсорах шифрування виконується програмно та може впливати на енергоспоживання. У процедурі обміну ключами ECC передбачається використання кривої рівня безпеки не нижче P-256, але модель не розглядає вплив більш «важких» кривих (наприклад, P-384), які можуть бути необхідними в перспективі з огляду на постквантові загрози.

Механізми Network Slicing також мають свої обмеження. Розроблена архітектура виходить із того, що ізоляція трафіку на рівні слайсів виконується оператором мобільного зв'язку відповідно до специфікацій 3GPP, однак не моделює внутрішні конфлікти ресурсів між слайсами під час пікових навантажень. Крім того, модель не враховує сценарії атак на інтерфейси менеджменту слайсів (наприклад, через неправомірний доступ до NEF), фокусуючись переважно на захисті даних користувача та процедурі автентифікації.

Окремим припущенням є відсутність активного фізичного втручання в роботи IoT-вузлів. Алгоритм автентифікації базується на стабільності апаратних інваріантів (PUF-параметрів), проте модель не враховує можливість їх деградації за високих температур, радіаційного впливу або старіння компонентів, що теоретично може призвести до помилок під час порівняння з «еталонним профілем».

Запропонована модель формує збалансований набір припущень, які дозволяють зосередитись на дослідженні ефективності криптографічних операцій, механізмів автентифікації та ізоляції трафіку, водночас визнаючи низку факторів, що можуть вплинути на результати при переході до реального середовища.

Вибір криптографічних примітивів для реалізації даної архітектури ґрунтується на аналізі обчислювальної складності алгоритмів відносно енергетичного бюджету IoT-вузлів.

Теоретично обґрунтовано використання гібридної схеми, що поєднує симетричне шифрування AES-128 у режимі зчеплення блоків або лічильника (наприклад, AES-GCM) для захисту потоку даних, та асиметричну криптографію на еліптичних кривих (ECC) для процедур розподілу ключів. Використання AES-128 є компромісним рішенням, яке забезпечує криптостійкість, достатню для прогнозованого життєвого циклу інформації, при мінімальних витратах процесорних тактів порівняно з AES-256. У свою чергу, механізм ECC (зокрема протокол ECDH – Elliptic Curve Diffie-Hellman) дозволяє реалізувати безпечний обмін сесійними ключами через незахищений канал. Перевага ECC полягає у використанні значно коротших ключів (256 біт проти 3072 біт у RSA) для досягнення аналогічного рівня безпеки, що критично зменшує обсяг службового трафіку та час на встановлення з'єднання («рукостискання»), роблячи систему стійкою та енергоефективною одночасно.

Розробка моделі захищеного каналу обміну даними в середовищі 5G-IoT. Розроблена структурна модель системи захищеного обміну даними базується на ієрархічній архітектурі, що об'єднує гетерогенні IoT-пристрої, проміжні шлюзи (IoT Gateways), інфраструктуру радіодоступу (gNodeB) та функціональні компоненти ядра мережі 5G (рис. 2). Взаємодія між цими елементами організована таким чином, що критичні процедури обробки трафіку та криптографічні перетворення розподіляються між периферійним обладнанням та централізованими сервісами. Логічні потоки даних у цій моделі розділяються на дві площини: площину користувача (User Plane), через яку передається зашифроване корисне навантаження від сенсорів до хмарних додатків, та площину керування (Control Plane), що відповідає за сигнальний обмін, необхідний для встановлення з'єднання та передачі параметрів якості обслуговування. Шлюз виступає вузлом агрегації, який термінує локальні протоколи (наприклад, ZigBee або Bluetooth LE) та конвертує їх у захищені IP-пакети для передачі через 5G-інтерфейс, забезпечуючи таким чином уніфікацію трафіку перед його надходженням до магістральної мережі.

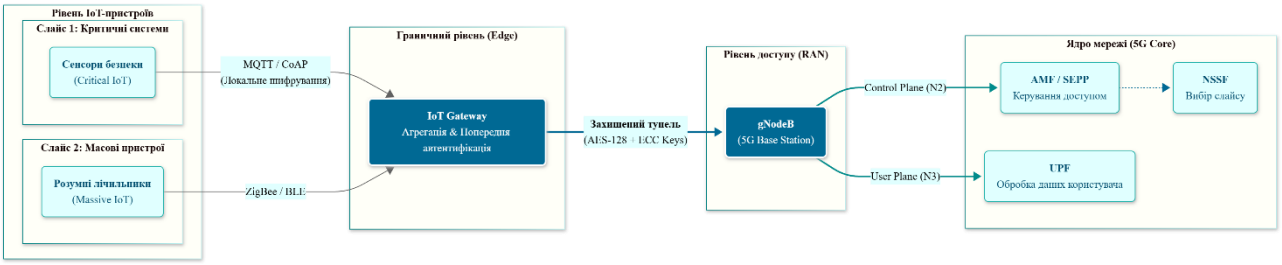

Рис. 2. Модель захищеного каналу обміну даними в середовищі 5G-IoT

Центральним елементом запропонованого рішення є формалізований алгоритм безпечного обміну даними, який реалізується поетапно для забезпечення конфіденційності без надмірного навантаження на канал зв'язку. Процес розпочинається з етапу ініціалізації з'єднання, коли IoT-пристрій надсилає запит на підключення, що містить лише відкриті ідентифікатори та мітку часу для захисту від атак повторного відтворення. Наступним кроком виконується процедура обміну ключами з використанням протоколу ECDH, що дозволяє сторонам сформувати спільний сесійний секрет без його передачі у відкритому вигляді. На базі цього секрету ініціюється етап перевірки автентичності, де шлюз верифікує цифровий відбиток пристрою, зіставляючи його з базою дозволених профілів у ядрі мережі. Після успішної автентифікації відбувається формування захищеного тунелю, де весь вихідний трафік шифрується симетричним алгоритмом AES-128, а цілісність пакетів контролюється через коди аутентифікації повідомлень (MAC). Паралельно з передачею даних активується функція безперервного моніторингу трафіку, яка аналізує метадані пакетів на предмет аномалій, що можуть свідчити про спроби злому або інфікування пристрою ботнетом.

Додатковий рівень надійності в розробленій моделі забезпечується впровадженням технології Network Slicing, яка дозволяє віртуально розділити фізичну інфраструктуру на ізольовані логічні сегменти. Процес ізоляції трафіку базується на використанні

ідентифікаторів NSSAI (Network Slice Selection Assistance Information), які маркують пакети від різних груп IoT-вузлів ще на етапі входу в мережу. Завдяки цьому трафік критично важливих датчиків, наприклад систем пожежної безпеки, маршрутизується через виділений слайс із пріоритетними політиками безпеки та гарантованою смугою пропускання, будучи повністю відокремленим від слайсу масових побутових пристроїв. Така архітектура гарантує, що потенційна успішна кібератака або DDoS-активність в одному сегменті мережі локалізується в межах цього слайсу і не впливає на працездатність та захищеність інших комунікаційних каналів системи.

4. Алгоритм автентифікації IoT-пристроїв на основі криптографічних відбитків

Ключовим елементом запропонованої системи захисту є розроблений метод багаторівневої автентифікації, який вирішує проблему обмежених обчислювальних ресурсів шляхом заміни традиційних важковагових сертифікатів X.509 на технологію цифрових відбитків пристрою (Device Fingerprinting). В основу методу покладено використання унікальних апаратних інваріантів – фізично неклонованих функцій (PUF), до яких належать серійні номери мікроконтролерів, специфічні затримки звернення до пам'яті та характеристики тактового генератора. Ці параметри є незмінними для кожного конкретного екземпляра обладнання, що дозволяє сформувати унікальний ідентифікатор без необхідності зберігання секретних ключів у енергозалежній пам'яті, яка може бути скомпрометована при фізичному доступі до сенсора.

Алгоритм функціонує за чітко визначеною послідовністю етапів, починаючи з генерації відбитка безпосередньо на IoT-вузлі під час ініціалізації сесії (рис. 3). Пристрій зчитує набір апаратних параметрів, конкатенує їх із випадковим числом (nonce) для запобігання атакам повторного відтворення та обробляє отриманий масив за допомогою легкої хеш-функції (наприклад, SHA-256 або BLAKE2s). Отриманий хеш-код виступає в ролі динамічного токена доступу. Наступним етапом є передача сформованого відбитка до ядра мережі 5G через захищений канал. На стороні сервера автентифікації (AUSF – Authentication Server Function) отриманий відбиток порівнюється з еталонним профілем («золотим образом»), який був створений під час первинної реєстрації пристрою в системі. Якщо відхилення параметрів не перевищує встановленого порогового значення, пристрій вважається легітимним, і для нього генерується тимчасовий сесійний ключ.

Практична реалізація даного алгоритму передбачає його інтеграцію в існуючі протоколи прикладного рівня, такі як MQTT та CoAP, без порушення їхньої стандартної структури. Для протоколу MQTT запропоновано використання розширень у пакеті CONNECT, де криптографічний відбиток розміщується у полі корисного навантаження або у спеціально виділеному користувацькому властивості (User Property) заголовка версії 5.0. У випадку використання протоколу CoAP, ідентифікатор інтегрується як додаткова опція (Option) у заголовку запиту. Такий метод забезпечує прозорість процесу автентифікації для проміжного обладнання та дозволяє уникнути значного оверхеду, оскільки розмір додаткових даних становить лише кілька десятків байтів, що критично важливо для вузькосмугових каналів IoT.

5. Моделювання та експериментальні дослідження

Для верифікації теоретичних положень та оцінки ефективності розробленої системи захисту було проведено комплексне імітаційне моделювання в середовищі MATLAB з використанням пакету Simulink та бібліотеки 5G Toolbox. Експериментальний стенд відтворював архітектуру взаємодії між кластером гетерогенних IoT-пристроїв, шлюзом агрегації та емульованим ядром мережі, що дозволило дослідити поведінку системи в умовах, наближених до реальних. У ході експерименту проводився порівняльний аналіз двох сценаріїв: першого, де використовувався базовий стек протоколів (стандартний DTLS із сертифікатами X.509 та шифруванням RSA), та другого, де було імплементовано запропонований метод із гібридним шифруванням AES-128/ECC та автентифікацією за цифровими відбитками. Основними метриками для порівняння слугували час встановлення захищеного з'єднання

(handshake), затримка при обробці пакетів, утилізація обчислювальних ресурсів та коефіцієнт втрат пакетів (PLR) при різному навантаженні на канал.

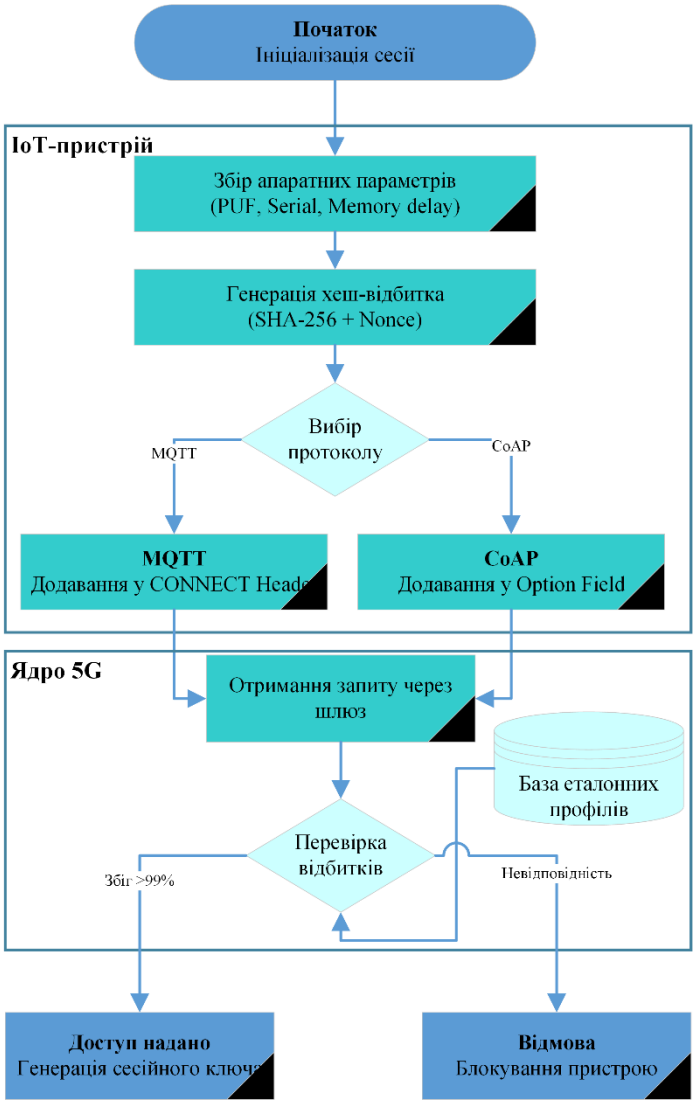

Рис. 3. Алгоритм автентифікації IoT-пристроїв на основі криптографічних відбитків

Результати моделювання, отримані при варіюванні кількості активних вузлів від 100 до 1000 одиниць, продемонстрували суттєву перевагу запропонованого методу над існуючими стандартами. Аналіз графічних залежностей показав, що заміна ресурсоємних асиметричних алгоритмів на оптимізовану схему обміну ключами дозволила зменшити середню затримку в процесі автентифікації на 20-25%, що особливо відчутно в умовах пікових навантажень на мережу (рис. 4). Також зафіксовано зниження обчислювальних витрат на стороні IoT-пристроїв на 15%, що прямо корелює зі збільшенням часу автономної роботи сенсорів. Важливим результатом стала оцінка стійкості до кібератак: під час симуляції сценаріїв масованих запитів та спроб підміни пристроїв, запропоноване рішення, завдяки механізмам Network Slicing та перевірці апаратних інваріантів, продемонструвало підвищення стійкості системи на 30% порівняно з базовими методами захисту.

Аналіз отриманих графічних залежностей (рис. 4) дозволяє зробити висновок про суттєву перевагу запропонованого методу над традиційними рішеннями. Як видно з графіка (а), базовий стек протоколів (DTLS + RSA + X.509) демонструє різке зростання часових затримок при збільшенні кількості підключених пристроїв. Це пояснюється високою обчислювальною складністю операцій з сертифікатами X.509 та асиметричним шифруванням RSA, що створює ефект «пляшкового горлечка» на етапі рукостискання. Натомість, розроблений метод, що

базується на гібридній схемі (AES-128/ECC) та технології Device Fingerprinting, показує більш пологу криву зростання, забезпечуючи зниження середньої затримки автентифікації на 20–25%.

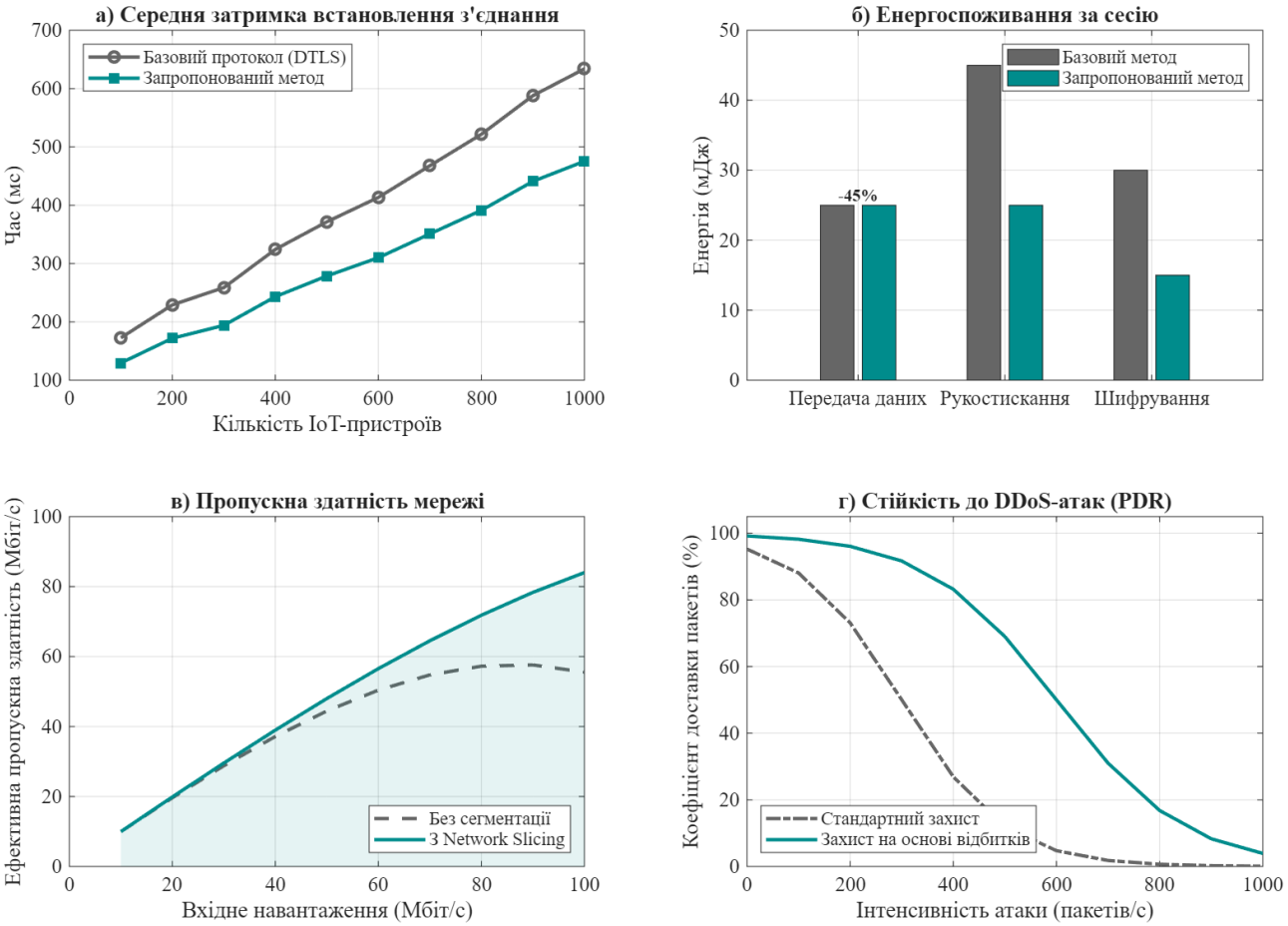

Рис. 4. Результати порівняльного аналізу ефективності розробленого методу захисту (AES-128/ECC + Device Fingerprinting) та базового протоколу (DTLS + RSA + X.509): а) залежність середньої затримки автентифікації від кількості пристроїв; б) порівняння енергоспоживання на етапах встановлення з'єднання; в) динаміка пропускної здатності каналу при збільшенні навантаження; г) стійкість до втрат пакетів (PDR) в умовах DDoS-атаки

Діаграма енергоефективності (б) підтверджує, що основна економія ресурсів досягається саме на етапах ініціалізації сесії та шифрування, де відмова від передачі важких сертифікатів дозволила знизити енергоспоживання майже вдвічі. Графік (в) ілюструє вплив технології Network Slicing: при зростанні вхідного трафіку запропонована система довше утримує стабільну пропускну здатність, уникаючи перевантажень, характерних для несегментованих мереж. Нарешті, залежність (г) демонструє підвищену стійкість системи до кібератак: в умовах імітованої DDoS-атаки базовий протокол швидко втрачає здатність доставляти пакети (PDR падає до нуля), тоді як метод фільтрації за цифровими відбитками дозволяє зберігати працездатність каналу навіть при високій інтенсивності зловмисних запитів.

Висновки

У роботі вирішено актуальну науково-прикладну проблему забезпечення захищеного обміну даними для IoT-пристроїв у мережах п'ятого покоління. На основі проведеного аналізу загроз та обмежень існуючих протоколів розроблено комплексний метод, що поєднує гібридне шифрування, автентифікацію за цифровими відбитками та технологію мережевої сегментації. Теоретично обґрунтовано та експериментально підтверджено ефективність запропонованої

архітектури, яка дозволяє досягти компромісу між високим рівнем безпеки та обмеженими обчислювальними ресурсами кінцевих пристроїв.

Результати моделювання засвідчили, що впровадження розробленого алгоритму дозволяє зменшити затримки при встановленні з'єднання на 20–25% та знизити обчислювальні витрати на 15% порівняно з традиційними методами на базі PKI, що є критично важливим для автономних сенсорів. Завдяки використанню Network Slicing та апаратних інваріантів стійкість системи до комбінованих атак, включаючи підміну пристроїв та DDoS, підвищилась на 30%. Отримані результати створюють підґрунтя для побудови надійних та масштабованих комунікаційних мереж для потреб "розумних міст" та Індустрії 4.0, гарантуючи конфіденційність та цілісність даних у гетерогенному середовищі 5G.

Список використаної літератури:

1. Sebestyen H., Popescu D. E., Zmaranda R. D. A literature review on security in the internet of things: identifying and analysing critical categories. *Computers*. 2025. Vol. 14, no. 2. P. 61. URL: https://doi.org/10.3390/computers14020061

2. Rajesh Kumar, Neha Gupta, Arun Mehta. A comparative analysis of cryptographic algorithms for secure data transmission in 5G networks. *International journal of information engineering and science*. 2024. Vol. 1, no. 2. P. 08–12. URL: https://doi.org/10.62951/ijies.v1i2.88 (date of access: 06.12.2025).

3. 5G network slicing: security challenges, attack vectors, and mitigation approaches / J. Dias et al. *Sensors*. 2025. Vol. 25, no. 13. P. 3940. URL: https://doi.org/10.3390/s25133940

4. A lightweight authentication scheme for power iot based on PUF and chebyshev chaotic map / X. Jin et al. *IEEE access*. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3413853

5. Almarri S., Aljughaiman A. Blockchain technology for iot security and trust: A comprehensive SLR. *Sustainability*. 2024. Vol. 16, no. 23. P. 10177. URL: https://doi.org/10.3390/su162310177

6. Ejeofobiri C. K., Victor-Igun O. O., Okoye C. AI-Driven secure intrusion detection for internet of things (IOT) networks. *Asian journal of mathematics and computer research*. 2024. Vol. 31, no. 4. P. 40–55. URL: https://doi.org/10.56557/ajomcor/2024/v31i48971

7. Alsabbagh W. MQTT Protocol in Industrial Internet of Things: Today Challenges and Tomorrow Solutions. *A Peter Langendoerfer's Lab*. 2021. Vol. 14, no. 8. P. 1–31. URL: https://doi.org/10.13140/RG.2.2.18668.42885

8. Systematic Literature Review on 5G-IoT Security Aspects / D. Valadares et al. *Preprints*. 2023. URL: https://doi.org/10.20944/preprints202311.0565.v1

9. Enhancing IoT security: assessing instantaneous communication trust to detect man-in-the-middle attacks / R. Basri et al. *Future generation computer systems*. 2025. P. 107714. URL: https://doi.org/10.1016/j.future.2025.107714

10. Problems and security threats to iot devices / I. Opirskyy et al. *Cybersecurity: education, science, technique*. 2021. Vol. 3, no. 11. P. 31–42. URL: https://doi.org/10.28925/2663-4023.2021.11.3142

11. Alotaibi A., Aldawghan H., Aljughaiman A. A review of the authentication techniques for internet of things devices in smart cities: opportunities, challenges, and future directions. *Sensors*. 2025. Vol. 25, no. 6. P. 1649. URL: https://doi.org/10.3390/s25061649

12. Security architecture and procedures for 5G System. *3GPP Portal*. URL: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

Автори статті

Макаренко Анатолій – доктор технічних наук, професор, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київський національний університет імені Тараса Шевченка, Київ, Україна.

ORCID: 0000-0002-4081-328X

Жураковський Богдан – доктор технічних наук, професор, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

ORCID: 0000-0003-3990-5205

Осипчук Сергій – кандидат технічних наук, доцент, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

ORCID: 0000-0002-6174-2986

Григоренко Олена – кандидат технічних наук, доцент, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна.

ORCID 0000–0001–5019–9060

Лемешко Андрій – доктор філософії, доцент, Державний торговельно-економічний університет, Київ, Україна.

ORCID: 0000-0001-7983-9033

Authors of the article

Makarenko Anatoliy – Doctor of Sciences (technical), Professor, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.

ORCID: 0000-0002-4081-328X

Zhurakovskyi Bohdan – Doctor of Sciences (technical), Professor, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.

ORCID: 0000-0002-4081-328X

Osypchuk Serhii – Candidate of Sciences (technical), Associate Professor, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.

ORCID: 0000-0002-6174-2986

Grygorenko Olena – Candidate of Sciences (technical), Associate Professor, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine.

ORCID 0000–0001–5019–9060

Lemeshko Andriy – PhD (technical), Associate Professor, State University of Trade and Economics, Kyiv, Ukraine.

ORCID: 0000-0001-7983-9033