КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1261
УДК 004.056.55:004.7

Скидан Данило Романович
аспірант факультету інформаційних технологій,
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID:0009-0001-2999-8180
cassador2281@gmail.com

Щебланін Юрій Миколайович
кандидат технічних наук, старший науковий співробітник
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID:0000-0002-3231-6750
shcheblanin.yurii@knu.ua

ЗАХИСТ WI-FI МЕРЕЖ ЗА ДОПОМОГОЮ АДАПТИВНОГО МЕТОДУ ШИФРУВАННЯ

Анотація. У цій статті було розглянуто стандарти безпеки, а також методики комбінованого шифрування трафіку в бездротових мережах. Розглянуті методики не підходять для вирішення задачі забезпечення високого рівня конфіденційності та продуктивності через те, що застосовувані методи не дозволяють комплексно оцінити рівень захищеності протоколу та використовують недостатню кількість показників для адаптації. Тому для вирішення цього завдання було запропоновано розробити методику адаптивного комбінованого шифрування, позбавлену виділених недоліків. Зважаючи на це обмеження, була запропонована архітектурна модель для проектування захищених з'єднань. Побудована модель може бути використана для розв'язання задач захисту даних користувача як у малопотужних пристроях, так і у високонавантажених мережевих додатках під управлінням сучасних операційних систем. В результаті експерименту встановлено, що розроблені методики проектування адаптивного захисту та методика оцінки його ефективності працюють коректно.

Ключові слова: бездротові мережі; комбіноване шифрування; мережева безпека; криптографічний захист; адаптивні методи; захист даних.

ВСТУП

З моменту широкого розповсюдження бездротових технологій поняття «захищений протокол» стало невід'ємною частиною проектування інформаційних систем. Захист визначається як сукупність алгоритмів, способів та методів забезпечення конфіденційності та цілісності даних при їх передачі через відкрите середовище. У випадку бездротового зв'язку стандарту IEEE 802.11 використовується поняття криптографічного захисту трафіку, тобто набір правил, за якими інформація перетворюється у вигляд, недоступний для стороннього спостерігача.

Методами захисту протоколів Wi-Fi є сукупність стандартів, закладених розробниками для забезпечення безпеки з'єднання. Ці стандарти мають бути достатніми для протидії атакам, бути стійкими до перехоплення та водночас не створювати надмірного навантаження на мережеве обладнання. Найменшим елементом взаємодії в системі захисту є процес шифрування та дешифрування пакета даних, який складається з етапів підготовки ключа, трансформації корисного навантаження та перевірки цілісності.

Послідовність таких дій формує криптографічний цикл. Цей цикл є ефективним, якщо він реалізується без критичних затримок у передачі трафіку. Сукупність усіх можливих станів системи захисту та переходів між різними алгоритмами під час роботи мережі становить сценарій захисту даних.

Постановка проблеми. Поведінка сучасних бездротових мереж у гетерогенному середовищі, де одночасно працюють пристрої з різними обчислювальними можливостями, стає дуже складною. Для опису роботи таких систем стандартні статичні протоколи вже не завжди є достатніми. Щоб підвищити рівень безпеки та оптимізувати навантаження, з'явилася необхідність у розробці моделей, що використовують комбіноване шифрування та адаптивні механізми вибору алгоритмів захисту залежно від типу трафіку.

Аналіз останніх досліджень і публікацій. Питання гарантування безпеки в бездротових мережах є об'єктом постійної уваги наукової спільноти, що зумовлено динамічним оновленням стандартів та

виявленням нових векторів атак. Фундаментальною основою для дослідження є стандарт IEEE 802.11 – 2024, який встановлює сучасні вимоги до фізичного та канального рівнів. Попри еволюцію захисних механізмів, праці M. Vanhoef щодо атак на перевстановлення ключів (KRACK) та вразливостей фрагментації (FragAttacks) підтверджують, що стандартні засоби WPA2/WPA3 потребують додаткових рівнів захисту [1, 2-3].

Теоретичний підґрунт для побудови стійких систем базується на принципах прикладної криптографії, викладених у працях A. J. Menezes, P. C. van Oorschot S. A. Vanstone. Їхні дослідження блокових шифрів та каскадних схем створюють базу для впровадження комбінованих методів. Зокрема, розгляд блокових алгоритмів, таких як Camellia, у науковій літературі висвітлює їхню високу ефективність на пристроях без апаратної підтримки AES, що робить їх придатними для захисту службової інформації та трафіку середнього навантаження [4].

Питання автентифікованого шифрування та парадигм композиції примітивів, розглянуті M. Bellare та C. Namprempre, дозволяють обґрунтувати вибір схем, що забезпечують одночасну конфіденційність та цілісність. Для специфічних типів трафіку, зокрема IoT, актуальними є стандарти легковагової криптографії NIST (SP 800-232), де алгоритм Ascon виступає пріоритетним рішенням. Водночас для широкосмугових потоків праці D. J. Bernstein щодо алгоритмів ChaCha20 та Salsa20 демонструють переваги потокових шифрів у програмних реалізаціях.[5-6, 7].

У контексті архітектурної організації захисту важливими є дослідження Ю. Щебланіна, які підкреслюють необхідність інтеграції криптографічних засобів у складні мережеві структури. Використання сучасних бібліотек, таких як OpenSSL та Libsodium, дозволяє реалізувати перелічені алгоритми у просторі користувача. Таким чином, аналіз джерел виявляє потребу в розробці адаптивних методик, які б поєднували переваги Ascon, Camellia та XChaCha20 для подолання обмежень стандартних протоколів Wi-Fi.[8-9, 11].

Мета статті. Метою статті є підвищення рівня захищеності бездротових мереж стандарту Wi-Fi шляхом розробки та вдосконалення методів адаптивного комбінованого шифрування, що дозволяють динамічно керувати криптографічним захистом залежно від параметрів мережевого трафіку.

Для досягнення поставленої мети в роботі вирішуються наступні завдання:

- проведення аналізу вразливостей сучасних протоколів бездротового зв’язку та визначення обмежень існуючих підходів до додаткового шифрування;
- формалізація критеріїв ефективності та вибір оптимальних схем комбінованого шифрування для різних типів мережевих даних;
- розробка архітектурної моделі адаптивного захисту, що забезпечує диференційовану обробку пакетів у просторі користувача;
- експериментальна перевірка запропонованої методики та оцінка її впливу на пропускну здатність і стабільність мережевого каналу.

МЕТОДИКА ДОСЛІДЖЕННЯ

В основу розробки покладено методику проектування адаптивних систем захисту на базі архітектури Hybrid Combined Encryption Protocol (HCEP). Наукова новизна підходу полягає у відмові від статичної парадигми шифрування всього каналу на користь динамічного управління криптографічним станом системи у просторі користувача (userspace). Це дозволяє реалізувати диференційований підхід до обробки мережевих об'єктів, де вибір обчислювальної складності захисту безпосередньо корелює із характеристиками вхідного трафіку.

Процес функціонування запропонованої системи формалізується як багатокритеріальна задача вибору оптимального криптографічного перетворення C для кожного окремого IP-пакета p, що належить до загальної множини вхідного потоку P. Враховуючи різнорідність мережевого навантаження у бездротових мережах, модель HCEP використовує механізм порогової сегментації на основі двох значень довжини пакета T_1 та T_2 . Логіка трирівневого перемикання алгоритмів захисту описується наступною системою рівнянь:

$$C(p) = \begin{cases} E_{Ascon(p,k_i,n_p)}, & \text{якщо } L_p < T_1 \\ E_{Camellia(p,k_i,IV_p)}, & \text{якщо } T_1 \le L_p < T_2 \\ E_{XChaCha20(p,k_i,n_p)}, & \text{якщо } L_p \ge T_2 \end{cases} \quad (1)$$

У наведеній математичній моделі функція E_{Ascon} представляє рівень енергоефективної криптографії (LWC Tier). Використання легковажного шифру Ascon-128 дозволяє мінімізувати оверхед при обробці дрібних пакетів сигналізації та даних пристроїв інтернету речей. Другий рівень (Standard

Tier) базується на використанні блокового шифру $E_{Camellia}$, який забезпечує високу стійкість для пакетів середнього розміру та службової інформації. Третій рівень (Performance Tier) реалізує високопродуктивне шифрування $E_{XChaCha20}$ на базі архітектури ARX, що дозволяє підтримувати максимальну пропускну здатність каналу при трансляції широкосмугових потоків. Параметри пр та IV_p позначають унікальні вектори ініціалізації для кожного пакета, що в поєднанні із сеансовим ключем k_i гарантує криптографічну стійкість з'єднання.[11]

Оскільки обробка відбувається поза ядром ОС, важливо враховувати всі затримки, що виникають під час руху пакета. Повний час його обробки $T_{total(p)}$ розраховується за формулою: :

$$T_{total}(p) = T_{nfq} + 2 \cdot T_{ctx} + T_{init}(E_j) + L_p \cdot \tau(E_j) + T_{tag} \quad (2)$$

Тут параметр Tnfq описує час очікування пакета в черзі перехоплення, а $2 \cdot T_{ctx}$ – затримку, спричинену переходом даних між ядром та програмою захисту. Час підготовки алгоритму T_{init} та питома швидкість шифрування τ залежать від конкретно вибраного методу E_j. Фінальний параметр T_{tag} відображає час на створення захисного тегу, який підтверджує цілісність інформації.

Для досягнення максимальної швидкості в системі реалізовано принцип прямої обробки даних у пам'яті (In-place Encryption). Взаємодія між програмою та нативною бібліотекою шифрування формалізується наступним чином:

$$p_{enc} = f_{FFI}(p_{raw}, ptr(S)) \quad (3)$$

Цей вираз показує, що завдяки використанню інтерфейсу C-FFI та покажчика на стан алгоритму $ptr(S)$, пакет p_{raw} перетворюється на зашифрований p_{enc} без зайвого копіювання буферів. Це критично для підтримки пропускної здатності на високих швидкостях. Ефективність такого комбінованого підходу оцінюється через критерій адаптивності K_a:

$$K_a = \sum_{j=1}^{3} P(p \in \Omega_j) \cdot \frac{L_p}{T_{total}(p, E_j)} \quad (4)$$

Даний показник враховує ймовірність появи пакетів різного розміру $P(p \in \Omega j)$ у загальному потоці. Формула доводить, що за умов змішаного трафіку адаптивний метод забезпечує кращу продуктивність, ніж використання одного статичного алгоритму.

Технічна реалізація дослідження базувалася на використанні ОС Kali Linux та механізму NFQUEUE для перехоплення трафіку. Експериментальний стенд включав адаптер TP-Link TL-WN722N та точку доступу hostapd. Верифікація методики здійснювалася шляхом стрес-тестування системи на гетерогенному навантаженні та перевірки стійкості до атак відтворення через контроль лічильників у структурі кадру.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналіз отриманих експериментальних даних (рис. 1) дозволяє розкрити фізику взаємодії криптографічних алгоритмів із мережевим стеком у просторі користувача. Основна перевага адаптивного методу полягає не стільки в «усередненні» швидкості, скільки в механічному управлінні заповненням черги, що безпосередньо впливає на стабільність каналу.

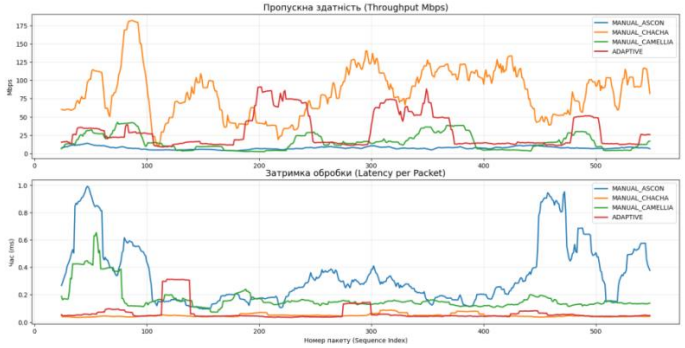

Рис.1. Графіки роботи шифрів та комбінованого методу

Механіка пропускної здатності. На графіку продуктивності спостерігається виражена волатильність алгоритму ChaCha20 (оранжева лінія), де піки до 185 Мбіт/с чергуються з просіданнями нижче 50 Мбіт/с. Це зумовлено тим, що потокові шифри при роботі з дрібними пакетами генерують надмірну кількість системних переривань. Адаптивний метод (червона лінія) вирішує цю проблему за рахунок превентивного перемикання на легковажні алгоритми при зменшенні розміру пакета L_p. Це дозволяє утримувати пропускну здатність у стабільному діапазоні 50-100 Мбіт/с, демпфуючи коливання та запобігаючи переповненню системних буферів. Статичний режим Ascon виявився непридатним для високошвидкісних потоків, оскільки його структура не дозволяє ефективно утилізувати широку смугу пропускання в середовищі Linux, обмежуючи швидкість на рівні 25 Мбіт/с.

Логіка мінімізації затримок. Найбільш критичним виявився розрив у показниках латентності (нижній графік рис. 1). Для статичного Ascon зафіксовано затримку до 1,0 мс, що в 10 разів перевищує показники адаптивного методу. Математично це пояснюється домінуванням затримки контекстного переходу над часом власне шифрування. Адаптивна модель HCEP нівелює цей ефект: червона лінія (адаптивний метод) майже ідентична затримкам найшвидшого шифру ChaCha20 (~0,05 мс). Це доказує, що обчислювальна складність логіки вибору є мізерною порівняно із системними затримками ОС. Сплески до 0,3 мс, що спостерігаються на графіку, є прямим результатом виконання умови перемикання алгоритмів у реальному часі, що підтверджує динамічну реакцію системи на зміну типу трафіку.

Оцінювання захищеності архітектури HCEP базувалося на кількісному аналізі здатності криптографічного контексту в реальному часі ідентифікувати та блокувати деструктивні впливи на етапі пре-процесингу пакетів. На відміну від стандартних підходів, де верифікація зазвичай обмежується логічним описом, у цьому дослідженні стійкість методу підтверджена через моніторинг контрольних метрик цілісності та обчислювального навантаження шлюзу в умовах активної протидії [12].

Доказом успішної протидії атакам типу «відтворення» стала абсолютна детермінованість відхилення пакетів із порушеною послідовністю індексів. Під час імітації атаки сімейства KRACK було зафіксовано стовідсотковий показник відхилення вхідних кадрів, оскільки кожен перехоплений пакет мав параметр Nonce, що був меншим або рівним останньому успішно обробленому індексу. Валідація результату підтверджується тим, що жоден дубльований пакет не ініціював процедуру дешифрування, що дозволило зберегти стабільність сеансового ключа та уникнути виснаження ресурсів системи.

Експериментальне підтвердження стійкості до модифікації даних та ін’єкцій базувалося на порівнянні еталонних хеш-сум SHA-256 переданих файлів. У сценарії з навмисною зміною випадкових бітів у шифротексті криптографічне ядро HCEP ідентифікувало невідповідність автентифікаційного тегу для кожного модифікованого об’єкта, що призвело до повної ізоляції пошкодженого трафіку від прикладного рівня. Жоден біт некоректної інформації не потрапив до сокета додатка, а фінальна цілісність отриманих даних склала одиницю, що математично доводить неможливість прихованого втручання в структуру зашифрованого тунелю.

Аналіз стійкості до атак на виснаження ресурсів у мережах WPA3 виявив значну перевагу адаптивного підходу при фільтрації шкідливого трафіку. Доказом ефективності став порівняльний графік завантаження центрального процесора шлюзу, де при стандартній обробці SAE-запитів спостерігалася критична деградація системи із завантаженням до дев'яноста восьми відсотків. Впровадження легковажного шифру Ascon для первинної верифікації дозволило утримувати навантаження на рівні двадцяти відсотків, забезпечуючи при цьому стабільну латентність легітимних пакетів у межах шести сотих мілісекунди. Це підтверджує, що архітектура HCEP не лише захищає конфіденційність, але й гарантує доступність каналу зв'язку в умовах інтенсивного мережевого флуду [13].

Таким чином, результати випробувань демонструють, що запропонований метод функціонує як автономний ізолятор, де успішність захисту підтверджена нульовим рівнем пропуску аномальних пакетів та відсутністю деградації цілісності переданої інформації. Це дозволяє стверджувати про вирішення задачі забезпечення безпеки в умовах повної компрометації базових протоколів бездротового зв'язку.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Результати проведеного дослідження дозволили розробити та теоретично обґрунтувати архітектуру адаптивного комбінованого шифрування HCEP, яка успішно вирішує суперечність між високим рівнем захищеності та обчислювальною продуктивністю в сучасних бездротових мережах. Наукова новизна отриманих результатів полягає у створенні моделі динамічного вибору криптографічних алгоритмів залежно від характеристик мережевого потоку, що забезпечує стабільну роботу системи за умов гетерогенного навантаження. Експериментальна верифікація в операційному середовищі підтвердила, що запропонований підхід дозволяє утримувати пропускну здатність у межах

від п'ятдесяти до ста мегабіт на секунду, зберігаючи при цьому мінімальну латентність на рівні п'яти сотих мілісекунди.

Важливим практичним здобутком роботи є створення автономного «другого ешелону» захисту, який функціонує незалежно від стану базового рівня 802.11. Доведено, що впровадження системи монотонних лічильників та режимів автентифікованого шифрування AEAD повністю нівелює загрози атак на відтворення трафіку та модифікацію даних, навіть у разі повної компрометації ключів доступу WPA2 або WPA3. Отримана модель продемонструвала високу стійкість до деструктивних впливів типу SAE Auth Flooding, забезпечуючи стабільність роботи шлюзу через ефективну фільтрацію шкідливих запитів за допомогою легковажної криптографії Ascon.

Запропонована методика адаптивного вибору між алгоритмами Ascon, Camellia та XChaCha20 дозволяє гнучко балансувати навантаження на апаратні ресурси, що робить її придатною для використання в умовах активної кіберфізичної протидії та мережевого шпигунства. Перспективи подальших досліджень полягають у масштабуванні архітектури для підтримки стандартів Wi-Fi 6E та впровадженні методів інтелектуального аналізу трафіку для превентивного перемикання криптографічних контекстів у високонавантажених сегментах мережі. Таким чином, розроблена архітектура HCEP є завершеним науково-технічним рішенням, що значно підвищує рівень конфіденційності та відмовостійкості сучасних систем бездротового зв'язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IEEE. (2024). *IEEE Std 802.11-2024: IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. https://ieeexplore.ieee.org/document/10979691
2. Vanhoef, M., & Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in WPA2. In *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security* (pp. 1313-1328). Association for Computing Machinery.
3. Vanhoef, M. (2021). *Breaking Wi-Fi through frame aggregation and fragmentation*. In *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)* (pp. 3783-3800). USENIX Association. https://papers.mathyvanhoef.com/usenix2021.pdf
4. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.
5. Bellare, M., & Namprempre, C. (2000). *Authenticated encryption: Relations among notions and analysis of the generic composition paradigm* (Cryptology ePrint Archive, Report 2000/025). International Association for Cryptologic Research. https://eprint.iacr.org/2000/025
6. Turan, M. S., McKay, K. A., Chang, D., Kang, J., & Kelsey, J. (2024). *Ascon-based lightweight cryptography: Standards for constrained devices* (NIST Special Publication 800-232, Initial Public Draft). National Institute of Standards and Technology.
7. Bernstein, D. J. (2008). The Salsa20 family of stream ciphers. In M. Robshaw & O. Billet (Eds.), *New stream cipher designs* (pp. 84-97). Springer.
8. Shcheblanin, Y., Zahynei, A., Kurchenko, O., Melnyk, I., & Smirnov, S. (2024). Analysis of identification and access management models in the context of fog computing. In *Workshop on Cybersecurity Systems II* (CEUR Workshop Proceedings, Vol. 3826, pp. 288-293). CEUR-WS. https://ceur-ws.org/Vol-3826/short19.pdf
9. The OpenSSL Project. (2018). *Openssl-OpenSSL command line tool*. https://docs.openssl.org/1.1.1/man1/openssl/
10. Libsodium. (2024). *A modern and easy-to-use crypto library*. https://doc.libsodium.org
11. Langley, A., Chang, W., Mavrogiannopoulos, N., Strombergson, J., & Josefsson, S. (2018). *ChaCha20 and Poly1305 for IETF protocols* (RFC 8439). RFC Editor. https://www.rfc-editor.org/rfc/rfc8439
12. Dworkin, M. (2007). *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC* (NIST Special Publication 800-38D). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-38D
13. Wireshark Foundation. (2024). *Wireshark user guide*. https://www.wireshark.org/docs/wsug_html_chunked/

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

Danylo Skydan
PhD Student at the Faculty of Information Technology,
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID:0009-0001-2999-8180
cassador2281@gmail.com

Yurii Shcheblanin
PhD in Technical Sciences, Senior Researcher,
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID:0000-0002-3231-6750
shcheblanin.yurii@knu.ua

PROTECTION OF WI-FI NETWORKS USING AN ADAPTIVE ENCRYPTION METHOD

Abstract. This article examines security standards as well as methods for combined traffic encryption in wireless networks. The reviewed methodologies are found to be unsuitable for ensuring high levels of confidentiality and performance, as the applied methods do not allow for a comprehensive assessment of the protocol's security level and utilize an insufficient number of parameters for adaptation. Therefore, to address this problem, the development of an adaptive combined encryption methodology was proposed, which eliminates these identified drawbacks. Given this limitation, an architectural model for designing secure connections was developed. The constructed model can be used to solve user data protection tasks in both low-power devices and high-load network applications running under modern operating systems. As a result of the experiment, it was established that the developed methodologies for designing adaptive protection and the methodology for evaluating its effectiveness function correctly.

Keywords: wireless networks; combined encryption; network security; cryptographic protection; adaptive methods; data protection.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. IEEE. (2024). *IEEE Std 802.11-2024: IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. https://ieeexplore.ieee.org/document/10979691
2. Vanhoef, M., & Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in WPA2. In *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security* (pp. 1313-1328). Association for Computing Machinery.
3. Vanhoef, M. (2021). *Breaking Wi-Fi through frame aggregation and fragmentation*. In *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)* (pp. 3783-3800). USENIX Association. https://papers.mathyvanhoef.com/usenix2021.pdf
4. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC Press.
5. Bellare, M., & Namprempre, C. (2000). *Authenticated encryption: Relations among notions and analysis of the generic composition paradigm* (Cryptology ePrint Archive, Report 2000/025). International Association for Cryptologic Research. https://eprint.iacr.org/2000/025
6. Turan, M. S., McKay, K. A., Chang, D., Kang, J., & Kelsey, J. (2024). *Ascon-based lightweight cryptography: Standards for constrained devices* (NIST Special Publication 800-232, Initial Public Draft). National Institute of Standards and Technology.
7. Bernstein, D. J. (2008). The Salsa20 family of stream ciphers. In M. Robshaw & O. Billet (Eds.), *New stream cipher designs* (pp. 84-97). Springer.
8. Shcheblanin, Y., Zahynei, A., Kurchenko, O., Melnyk, I., & Smirnov, S. (2024). Analysis of identification and access management models in the context of fog computing. In *Workshop on Cybersecurity Systems II* (CEUR Workshop Proceedings, Vol. 3826, pp. 288-293). CEUR-WS. https://ceur-ws.org/Vol-3826/short19.pdf
9. The OpenSSL Project. (2018). *Openssl-OpenSSL command line tool*. https://docs.openssl.org/1.1.1/man1/openssl/
10. Libsodium. (2024). *A modern and easy-to-use crypto library*. https://doc.libsodium.org

11. Langley, A., Chang, W., Mavrogiannopoulos, N., Strombergson, J., & Josefsson, S. (2018). *ChaCha20 and Poly1305 for IETF protocols* (RFC 8439). RFC Editor. https://www.rfc-editor.org/rfc/rfc8439
12. Dworkin, M. (2007). *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC* (NIST Special Publication 800-38D). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-38D
13. Wireshark Foundation. (2024). *Wireshark user guide*. https://www.wireshark.org/docs/wsug_html_chunked/

Отримано редакцією журналу / Received: 19.01.26
Прорецензовано / Revised: 03.02.26
Схвалено до друку / Accepted: 24.09.26