© Trofimov O., Hulak H. Method for Authentication of Information Resources Based on block Cipher Encryption // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 2, pp. 72-82. © This is an open access article under the CC BY 4.0 International license.*

DOI: 10.18372/2225-5036.32.21660

МЕТОД АВТЕНТИФІКАЦІЇ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА ОСНОВІ БЛОКОВОГО ШИФРУВАННЯ

Олександр Трофімов[1], Геннадій Гулак[1,2,3]

[1] Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
[2] Інститут проблем математичних машин та систем Національної академії наук України, м. Київ, Україна
[3] Національна академія Служби безпеки України, м. Київ, Україна



ТРОФІМОВ Олександр Сергійович, аспірант.
Рік та місце народження: 2000 рік, м. Київ, Україна.
Освіта: Київський столичний університет імені Бориса Грінченка.
Наукові інтереси: адміністрування і захист баз даних та сховищ даних, моделювання програмного забезпечення та його аналіз, інформаційні технології та системи.
Публікації: більше 10 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: o.trofimov.asp@kubg.edu.ua
Orcid: 0009-0008-5760-7803



ГУЛАК Геннадій Миколайович, доктор технічних наук, професор.
Рік та місце народження: 1955 рік, м. Київ, Україна.
Освіта: ВШ КДБ.
Посада: професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка.
Наукові інтереси: кібербезпека, криптографія, криптоаналіз, математичне моделювання.
Публікації: більше 100 наукових публікацій, серед яких монографії, підручники, посібники, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: h.hulak@kubg.edu.ua
Orcid: 0000-0001-9131-9233

Анотація. *Статтю присвячено розробленню методу автентифікації інформаційних ресурсів на основі блокового шифрування, призначеного для забезпечення автентичності, цілісності та конфіденційності даних під час їх зберігання, оброблення й передавання у комп'ютерних системах та мережах. Обґрунтовано актуальність удосконалення криптографічних механізмів автентифікації в умовах зростання кількості кіберзагроз, пов'язаних із підміною інформації, несанкціонованим доступом і компрометацією інформаційних ресурсів. Проведено аналіз сучасних методів автентифікації та встановлено, що існуючі рішення не завжди забезпечують необхідний баланс між криптографічною стійкістю, швидкодією та обчислювальною ефективністю. Розглянуто особливості застосування алгоритмів блокового шифрування для формування автентифікаційних даних і визначено основні вимоги до побудови методу. Запропоновано метод автентифікації інформаційних ресурсів, що ґрунтується на генерації криптографічного ключа, блоковому перетворенні інформаційного ресурсу, формуванні автентифікаційного коду, перевірці цілісності та прийнятті рішення щодо достовірності ресурсу. На відміну від існуючих підходів, запропонований метод інтегрує процедури шифрування й автентифікації, забезпечує локалізацію змінених блоків, кількісне оцінювання автентичності та ризик-орієнтоване прийняття рішення. Формалізовано послідовність криптографічного оброблення інформаційного ресурсу, розроблено моделі формування інтегрального профілю, оцінювання автентичності й цілісності та вибору подальшої реакції з урахуванням ризику компрометації. Проведене структурно-функціональне оцінювання показало можливість локалізації змінених блоків і кількісного визначення ступеня відмінності ресурсу від еталонного стану.. Результати структурно-функціонального оцінювання підтверджують доцільність подальшої програмної реалізації та експериментального дослідження запропонованого методу в сучасних інформаційно-комунікаційних системах.*

Ключові слова: *автентифікація інформаційних ресурсів, блокове шифрування, криптографічна автентифікація, забезпечення цілісності даних, код автентифікації повідомлень, криптографічний ключ, інформаційна безпека, інформаційно-комунікаційні системи.*

Вступ

Стрімкий розвиток інформаційно-комунікаційних технологій, хмарних сервісів і розподілених інформаційних систем супроводжується постійним зростанням кількості кіберзагроз, спрямованих на порушення цілісності, автентичності та конфіденційності інформаційних ресурсів [3, 8, 23]. Одними з найпоширеніших загроз залишаються модифікація даних, підміна повідомлень, несанкціонований доступ та компрометація криптографічних ключів [6, 16-17]. За таких умов особливої актуальності набуває розроблення ефективних методів автентифікації, здатних забезпечити надійне підтвердження достовірності інформаційних ресурсів .із можливістю локалізації порушень цілісності та кількісного оцінювання достовірності інформаційного ресурсу [1, 7, 26].

Сучасні криптографічні алгоритми блокового шифрування характеризуються високою криптографічною стійкістю та широко застосовуються для захисту інформації [4, 10, 12]. Водночас їх потенціал може бути ефективно використаний не лише для забезпечення конфіденційності, а й для реалізації процедур автентифікації та контролю цілісності інформаційних ресурсів [17, 25]. Це зумовлює

необхідність створення методів, які поєднують процедури шифрування та автентифікації в єдиному криптографічному процесі, забезпечуючи підвищений рівень захисту інформації.

Наукова новизна полягає не лише в інтеграції шифрування та автентифікації, а у формуванні зваженого інтегрального криптографічного профілю інформаційного ресурсу, який поєднує локальні автентифікаційні коди блоків з урахуванням їх інформаційної значущості та критичності. Це дає змогу кількісно оцінювати ступінь автентичності, локалізувати змінені блоки та приймати ризик-орієнтоване рішення залежно від можливих наслідків компрометації ресурсу.

Теоретичне значення роботи полягає у формалізації процесу автентифікації інформаційних ресурсів на основі блокового шифрування та розробленні математичної моделі взаємодії його основних етапів. Практичне значення полягає у можливості використання запропонованого методу під час створення та модернізації криптографічних засобів захисту інформації, систем електронного документообігу, корпоративних інформаційних систем, хмарних сервісів і програмно-апаратних комплексів, де необхідно забезпечити високий рівень автентичності та цілісності інформаційних ресурсів [9, 20, 22].

Постановка проблеми

Сучасні інформаційно-комунікаційні системи функціонують в умовах постійного зростання кількості кіберзагроз, серед яких особливу небезпеку становлять атаки, спрямовані на підміну, модифікацію та фальсифікацію інформаційних ресурсів [3, 8, 23]. У таких умовах забезпечення лише конфіденційності даних уже не є достатнім, оскільки критично важливим стає підтвердження їх автентичності та цілісності [17, 26]. Використання ненадійних або недостатньо захищених механізмів автентифікації може призвести до компрометації інформації, несанкціонованого доступу, порушення функціонування інформаційних систем і значних економічних збитків.

Більшість сучасних методів автентифікації реалізують процедури шифрування та перевірки автентичності окремо, що збільшує обчислювальні витрати, ускладнює реалізацію криптографічного захисту та створює додаткові потенційні вразливості [4, 6, 10]. Незважаючи на широке використання алгоритмів блокового шифрування для забезпечення конфіденційності інформації, їх можливості щодо інтегрованого забезпечення автентичності та цілісності інформаційних ресурсів залишаються недостатньо дослідженими.

У зв'язку з цим актуальним науково-практичним завданням є розроблення методу автентифікації інформаційних ресурсів на основі блокового шифрування, який поєднує криптографічне перетворення даних із формуванням та перевіркою автентифікаційного коду в межах єдиного процесу [9, 20, 22]. Реалізація такого підходу дає змогу підвищити рівень захищеності інформаційних ресурсів, зменшити ризик їх модифікації або підміни та забезпечити ефективне застосування криптографічних засобів у сучасних інформаційно-комунікаційних системах.

Аналіз останніх досліджень і публікацій

Проблема забезпечення автентичності інформаційних ресурсів із використанням криптографічних методів активно досліджується у сучасній науковій літературі, особливо в контексті розвитку хмарних обчислень, Інтернету речей, кіберфізичних систем та постквантової криптографії. Значна частина сучасних досліджень спрямована на вдосконалення алгоритмів блокового шифрування, механізмів автентифікації повідомлень і побудову комбінованих криптографічних схем.

У роботі Roy та ін. [1] запропоновано дворівневу схему автентифікації для безпілотних літальних апаратів, яка поєднує алгоритм AES із криптографією на еліптичних кривих. Запропонований підхід забезпечує високий рівень захисту від атак повторного відтворення, модифікації та підміни повідомлень, проте використання ECC разом із AES підвищує обчислювальні витрати та ускладнює реалізацію на ресурсообмежених пристроях.

У систематичному огляді Haverkamp та Sarmah [2] досліджено сучасні підходи до поєднання криптографії та стеганографії. Автори довели, що забезпечення конфіденційності саме по собі не гарантує автентичності інформації, а тому криптографічні механізми мають доповнюватися засобами перевірки цілісності й походження даних.

У роботі Luo та ін. [3] проаналізовано застосування технології блокчейн у сучасних криптографічних протоколах. Показано, що розподілені механізми довіри забезпечують високий рівень автентифікації, однак супроводжуються значними накладними витратами та складністю інтеграції у високопродуктивні інформаційні системи.

Комплексний огляд Zhong та Gu [4] присвячено сучасним полегшеним алгоритмам блокового шифрування для ресурсообмежених середовищ. Автори відзначають, що вибір алгоритму визначається компромісом між криптографічною стійкістю, швидкодією та використанням ресурсів, а також наголошують на необхідності розроблення ефективніших методів автентифікації на основі симетричної криптографії.

У систематичному огляді Ansari та Ali [5] узагальнено сучасні полегшені криптографічні схеми для захисту IoT-систем. Встановлено, що більшість сучасних рішень реалізує взаємну автентифікацію із застосуванням ECC, хеш-функцій або комбінованих криптографічних протоколів, тоді як використання лише блокового шифрування для одночасного забезпечення автентичності та цілісності досліджено недостатньо.

У роботі Cambou та Alam [6] досліджено механізми Challenge–Response та багатофакторної автентифікації для захисту приватних криптографічних ключів. Автори показали

ефективність багатофакторних схем автентифікації, однак їх дослідження зосереджене переважно на захисті ключового матеріалу, а не інформаційних ресурсів.

У дослідженні Zhang та ін. [7] запропоновано ефективний анонімний багатоступеневий протокол автентифікації для супутникових каналів зв'язку. Протокол забезпечує високий рівень криптографічної стійкості та конфіденційності, проте характеризується складною структурою та значною кількістю криптографічних операцій.

У роботі Ganesh та ін. [8] виконано комплексний аналіз алгоритму AES, сучасних режимів його роботи, механізмів керування ключами, сфер практичного використання та перспектив застосування в умовах розвитку квантових обчислень. Автори підкреслюють, що режими автентифікованого шифрування (GCM, CCM та ін.) істотно підвищують рівень захисту інформації, однак окремого універсального методу автентифікації інформаційних ресурсів на основі блокового шифрування не запропоновано.

Таким чином, аналіз сучасних наукових праць [1–8] показав, що існуючі дослідження переважно спрямовані на вдосконалення окремих криптографічних алгоритмів, протоколів взаємної автентифікації, полегшених схем захисту або комбінованих криптографічних рішень. Водночас недостатньо дослідженими залишаються питання побудови методу автентифікації інформаційних ресурсів на основі блокового шифрування, який би інтегрував процеси шифрування, формування автентифікаційного коду та перевірки цілісності в єдиному криптографічному процесі, забезпечуючи локальне виявлення порушень цілісності, кількісне оцінювання автентичності та прийняття рішення з урахуванням ризику компрометації [10, 17, 23]. Саме розв’язанню цього наукового завдання присвячено статтю.

Мета і задачі дослідження

Метою дослідження є розроблення методу автентифікації інформаційних ресурсів на основі блокового шифрування, який інтегрує процедури шифрування, локальної перевірки автентичності, контролю цілісності та ризик-орієнтованого прийняття рішення.

Для досягнення поставленої мети необхідно вирішити такі **задачі**:

– Провести аналіз сучасних методів автентифікації інформаційних ресурсів та визначити їх переваги, недоліки й напрями вдосконалення.

– Дослідити можливості використання алгоритмів блокового шифрування для одночасного забезпечення автентичності та цілісності інформаційних ресурсів.

– Розробити метод автентифікації інформаційних ресурсів на основі блокового шифрування із визначенням послідовності основних криптографічних процедур.

– Формалізувати математичну модель процесу автентифікації та взаємодії його структурних компонентів.

– Провести структурно-функціональне оцінювання запропонованого методу, визначити його обчислювальну складність і порівняти функціональні можливості з поширеними криптографічними схемами.

Результати дослідження

На основі аналізу сучасних методів автентифікації інформаційних ресурсів встановлено, що більшість існуючих підходів розглядає блокове шифрування, формування автентифікаційного коду та контроль цілісності як окремі криптографічні процедури [10, 17, 23]. Це ускладнює узгоджене оцінювання автентичності й цілісності інформації, не забезпечує локалізації змінених блоків і не враховує наслідки компрометації ресурсу під час вибору подальшої реакції [26].

Для усунення цих недоліків запропоновано метод автентифікації інформаційних ресурсів на основі блокового шифрування, який об'єднує процеси шифрування, формування інтегрального криптографічного профілю, оцінювання автентичності, контролю цілісності та ризик-орієнтованого прийняття рішення в єдиному криптографічному циклі. Метод формалізовано взаємопов'язаними математичними моделями, що описують основні етапи його функціонування та забезпечують комплексне оцінювання достовірності інформаційних ресурсів.

Концепція методу автентифікації інформаційних ресурсів на основі блокового шифрування

Сучасні інформаційно-комунікаційні системи характеризуються високою інтенсивністю оброблення й передавання даних, що висуває підвищені вимоги до забезпечення конфіденційності, автентичності та цілісності інформаційних ресурсів [10, 23]. Традиційні підходи реалізують шифрування, формування коду автентифікації повідомлень (MAC) і контроль цілісності як окремі процеси, що збільшує обчислювальні витрати та ускладнює керування захистом інформації.

Запропонований метод ґрунтується на концепції інтегрованої криптографічної автентифікації, за якої блокове шифрування одночасно забезпечує конфіденційність і формування інтегральних ознак автентичності. Метод об'єднує процеси блокового шифрування, побудови автентифікаційного профілю, оцінювання цілісності та прийняття рішення в межах єдиного криптографічного циклу.

Метод включає одинадцять взаємопов'язаних процедур, згрупованих у сім функціональних етапів: підготовку ресурсу, блокове криптографічне перетворення, формування локальних кодів автентифікації, побудову та повторне формування інтегрального профілю, оцінювання автентичності

й цілісності, аналіз ризику та прийняття остаточного рішення.

Особливістю методу є використання зваженого інтегрального криптографічного профілю, сформованого за результатами оброблення всіх блоків з урахуванням їх значущості, взаємозв'язків і результатів криптографічного перетворення. [17, 26] Це забезпечує кількісне оцінювання ступеня зміни інформаційного ресурсу, а локалізація порушень цілісності здійснюється шляхом порівняння локальних кодів автентифікації окремих блоків.

Остаточне рішення приймається на основі інтегрального оцінювання автентичності, яке поєднує результати криптографічного перетворення, перевірки локальних ознак, оцінювання цілісності та аналізу ризику компрометації. Такий підхід забезпечує багаторівневе оцінювання стану інформаційного ресурсу та дає змогу виявляти його модифікацію, підміну, повторне відтворення й часткове спотворення.

Загальну структуру запропонованого методу автентифікації інформаційних ресурсів на основі блокового шифрування наведено на рис. 1.

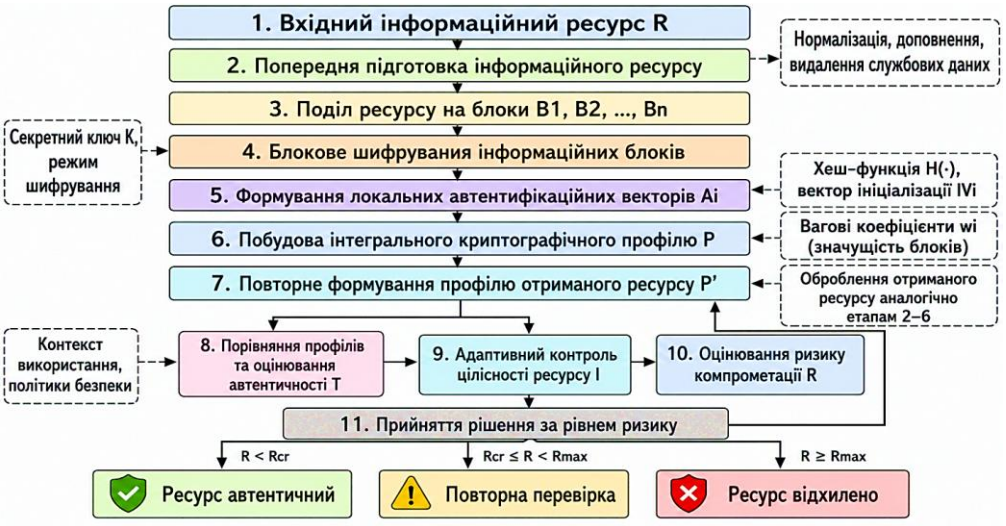


Рис. 1. Структура методу автентифікації інформаційних ресурсів на основі блокового шифрування

На рис. 1 представлено структурну схему запропонованого методу автентифікації інформаційних ресурсів на основі блокового шифрування, яка відображає послідовність виконання основних криптографічних операцій, формування інтегрального профілю автентичності, контролю цілісності, оцінювання ризику компрометації та прийняття рішення з урахуванням параметрів шифрування й контексту безпеки.

Формалізація процесу автентифікації

Під час побудови методу припускається, що порушник може перехоплювати, модифікувати, вилучати, переставляти та повторно передавати інформаційні блоки, але не має доступу до секретних ключів K_0, K_E і K_A. Канал розподілу ключів та середовище їх зберігання вважаються довіреними. Метод не спрямований на протидію компрометації кінцевого пристрою, витоку ключів через побічні канали або порушенню криптографічних примітивів.

Формалізація запропонованого методу передбачає математичний опис поділу інформаційного ресурсу на блоки, їх криптографічного перетворення та формування локальних автентифікаційних кодів. Такий підхід забезпечує однозначне представлення процесу автентифікації та створює основу для подальшого оцінювання цілісності й достовірності інформації.

Інформаційний ресурс подається множиною блоків:

$$\mathcal{R} = \{B_1, B_2, \dots, B_n\}, \quad (1)$$

де $\mathcal{R}$ – інформаційний ресурс, B_i – і-й блок інформації, n – кількість блоків.

Початковий секретний ключ K_0 формується криптографічно стійким генератором випадкових послідовностей. Для розділення функцій шифрування та автентифікації з нього виводяться незалежні підключі:

$$K_E = KDF(K_0, "ENC" \| ID_R), \quad (2)$$

$$K_A = KDF(K_0, "AUTH" \| ID_R), \quad (3)$$

де K_E– ключ блокового шифрування, K_A – ключ формування кодів автентифікації, $KDF(\cdot)$ – функція виведення ключів, ID_R – ідентифікатор інформаційного ресурсу. Різні контекстні мітки «ENC» і «AUTH» забезпечують функціональне розділення ключового матеріалу.

Для кожного блока виконується криптографічне перетворення:

$$C_i = \mathcal{E}_{K_E}^{M}(B_i; Q_i), \quad (4)$$

де $\mathcal{E}_{K_E}^{M}(\cdot)$ – криптографічне перетворення в режимі M на основі блокового шифру з ключем K_E, Q_i – режимозалежний параметр, який може містити вектор ініціалізації, nonce, лічильник або tweak.

Структура параметра Q_i визначається вибраним режимом блокового шифрування. Він повинен забезпечувати унікальність криптографічного контексту та виключати детерміноване формування однакових

шифротекстів для однакових блоків. Конкретний алгоритм і режим шифрування визначаються політикою безпеки та можуть бути реалізовані, наприклад, на основі AES у режимах, що не допускають детермінованого шифрування однакових блоків.

Для протидії атакам повторного відтворення до автентифікованих даних включається контекст свіжості:

$$F_R = \langle t_R, v_R, N_R \rangle, \quad (5)$$

де t_R – часова позначка, v_R – номер версії інформаційного ресурсу, N_R – унікальний nonce.

$$\mathcal{X}_F = \begin{cases} 1, & |t_{now} - t_R| \le \tau_{max} \wedge N_R \notin \mathcal{N}_{used} \wedge v_R > v_R^{last}, \\ 0, & \text{інакше}, \end{cases} \quad (6)$$

де $\mathcal{X}_F$ – результат перевірки актуальності контексту свіжості, t_{now} – поточний час, τ_{max} – допустиме часове вікно, $\mathcal{N}_{used}$ – множина раніше використаних nonce, v_R^{last} – номер останньої прийнятої версії ресурсу. Перевірка контексту свіжості виконується після успішної перевірки відповідного коду CMAC, оскільки значення t_R, v_R і N_R повинні бути криптографічно автентифікованими. Після прийняття ресурсу значення N_R додається до множини $\mathcal{N}_{used}$, а v_R^{last} оновлюється.

Після завершення шифрування для кожного блока формується локальний код автентифікації:

$$A_i = CMAC_{K_A}(C_i \,||\, Q_i || \, i \, || ID_R || \, F_R), \quad (7)$$

де A_i – локальний код автентифікації і-го блока, $CMAC_{K_A}(\cdot)$ – функція формування коду автентифікації на основі блокового шифру з ключем K_A, K_A – окремий ключ автентифікації, C_i – зашифрований блок, Q_i – режимозалежний параметр криптографічного перетворення, i – номер блока, ID_R– ідентифікатор інформаційного ресурсу, F_R– контекст свіжості, $||$ – позначає конкатенацію. Включення номера блока i та ідентифікатора ресурсу ID_R зв'язує автентифікаційне значення з його позицією і конкретним інформаційним ресурсом. Це запобігає перестановці, вилученню або перенесенню коректного блока до складу іншого ресурсу.

Значення інформаційної значущості S_i та критичності λ_i визначаються довіреною політикою класифікації ресурсів і не можуть змінюватися разом із переданими даними без окремої автентифікації. Інакше несанкціонована зміна вагових параметрів могла б вплинути на інтегральний профіль без модифікації самого блока.

Для використання локального коду автентифікації у подальших обчисленнях бітове значення A_i перетворюється на нормований числовий вектор:

$$\boldsymbol{a}_i = \Psi(A_i), \quad \boldsymbol{a}_i \in [0;1]^m, \quad (8)$$

де $\Psi(\cdot)$ – детермінована функція перетворення бітового коду автентифікації на m -вимірний нормований числовий вектор, m – розмірність автентифікаційного представлення. Однакові локальні коди автентифікації відображаються в однакові нормовані числові вектори, тоді як зміна зашифрованого блока, режимозалежного параметра Q_i, позиції блока, ідентифікатора ресурсу або контексту свіжості спричиняє зміну відповідного вектора $\boldsymbol{a}_i$.

Для реалізації функції $\Psi(\cdot)$ значення A_i довжиною q біт поділяється на m неперекривних фрагментів однакової довжини. Кожний фрагмент інтерпретується як невід'ємне ціле число та нормується до інтервалу [0,1]. За умови, що довжина коду q кратна розмірності m, довжина кожного фрагмента становить $d = q/m$ компоненту вектора можна визначити як:

$$a_{i,r} = \frac{int\,(A_i^{(r)})}{2^d - 1}, \quad r = 1, \dots m. \quad (9)$$

де $A_i^{(r)}$ – r–й фрагмент локального коду автентифікації, $int\,(\cdot)$ – перетворення бітового рядка на ціле число. Якщо q не кратне m, використовується попередньо визначене доповнення або поділ на фрагменти нерівної довжини з окремим нормуванням кожного компонента.

Запропонована модель забезпечує однозначне відображення кожного інформаційного блока у відповідний шифротекст, локальний код автентифікації та нормований числовий вектор, що використовуються для локальної перевірки цілісності й формування інтегрального криптографічного профілю.

Формування інтегрального криптографічного профілю ресурсу

У традиційних схемах результат автентифікації переважно має бінарний характер і визначається збігом або незбігом коду автентифікації. У запропонованому методі точна перевірка локальних кодів CMAC доповнюється формуванням інтегрального криптографічного профілю, який кількісно характеризує сукупний масштаб і значущість виявлених змін.

Інтегральний криптографічний профіль визначається виразом:

$$\mathbf{P} = \sum_{i=1}^{n} \omega_i \, \boldsymbol{a}_i, \quad (10)$$

де $\mathbf{P}$ – інтегральний криптографічний профіль інформаційного ресурсу, $\boldsymbol{a}_i$ – нормований числовий вектор і-го блока, ω_i – ваговий коефіцієнт блока, n – кількість блоків інформації. Інтегральний криптографічний профіль використовується як допоміжна кількісна характеристика сукупної відмінності інформаційного ресурсу та не замінює точного порівняння локальних кодів A_i і A_i'. Криптографічний факт цілісності встановлюється за результатами перевірки кожного CMAC, тоді як профіль $\mathbf{P}$ забезпечує агреговане оцінювання масштабу й значущості виявлених змін. Використання вагових коефіцієнтів дає змогу враховувати неоднакову інформаційну значущість окремих блоків під час формування інтегральної оцінки, що підвищує інформативність аналізу стану ресурсу. Сформований інтегральний

криптографічний профіль є основою для подальшого обчислення нормованої відстані між еталонним і поточним представленнями інформаційного ресурсу та визначення коефіцієнта автентичності.

Ваговий коефіцієнт кожного блока обчислюється за формулою:

$$\omega_i = \frac{\lambda_i S_i}{\sum_{j=1}^{n} \lambda_j S_j}, \quad \sum_{j=1}^{n} \lambda_j S_j > 0, \tag{11}$$

де ω_i – нормований ваговий коефіцієнт і-го блока, S_i – інформаційна значущість блока, що характеризує його внесок у загальну цінність інформаційного ресурсу, λ_i – коефіцієнт критичності блока, який визначає потенційний вплив його компрометації на безпеку ресурсу, $\sum_{j=1}^{n} \lambda_j S_j$ – нормувальний множник, що забезпечує виконання умови $\sum_{i=1}^{n} \omega_i = 1$.

Якщо для всіх блоків виконується $\lambda_i S_i = 0$, вагові коефіцієнти встановлюються рівномірно: $\omega_i = \frac{1}{n}$, $i = 1, \ldots, n$. Значення S_i та λ_i встановлюються відповідно до політики класифікації інформації. Вони можуть визначатися експертно, на основі типу даних, функціонального призначення блока, рівня обмеження доступу або потенційних наслідків його компрометації. Для забезпечення порівнюваності обидва параметри нормуються до інтервалу [0,1].

Використання інтегрального криптографічного профілю є ключовою особливістю запропонованого методу, оскільки забезпечує комплексне оцінювання автентичності інформаційного ресурсу з урахуванням неоднакової важливості окремих блоків даних, що підвищує точність виявлення несанкціонованих змін порівняно з традиційними схемами, які аналізують кожний блок незалежно [6, 17, 23]. Сформований інтегральний криптографічний профіль використовується як узагальнене криптографічне представлення інформаційного ресурсу, на основі якого надалі визначаються показники автентичності, цілісності та ризику компрометації.

На рис. 2 наведено послідовність формування інтегрального криптографічного профілю інформаційного ресурсу. Для кожного інформаційного блока виконується шифрування, після чого формується локальний код автентифікації, який за допомогою функції $\Psi(\cdot)$ перетворюється на нормований числовий вектор. Отримані вектори агрегуються із застосуванням вагових коефіцієнтів ω_i, що враховують значущість і критичність відповідних блоків, у результаті чого формується інтегральний криптографічний профіль. Такий профіль використовується на наступному етапі для порівняння еталонного та повторно сформованого представлень інформаційного ресурсу, визначення коефіцієнта автентичності та оцінювання цілісності.

Таким чином, сформований інтегральний криптографічний профіль забезпечує перехід від поблокового представлення результатів автентифікації до їх узагальненого кількісного опису, який використовується на наступному етапі для оцінювання автентичності інформаційного ресурсу.

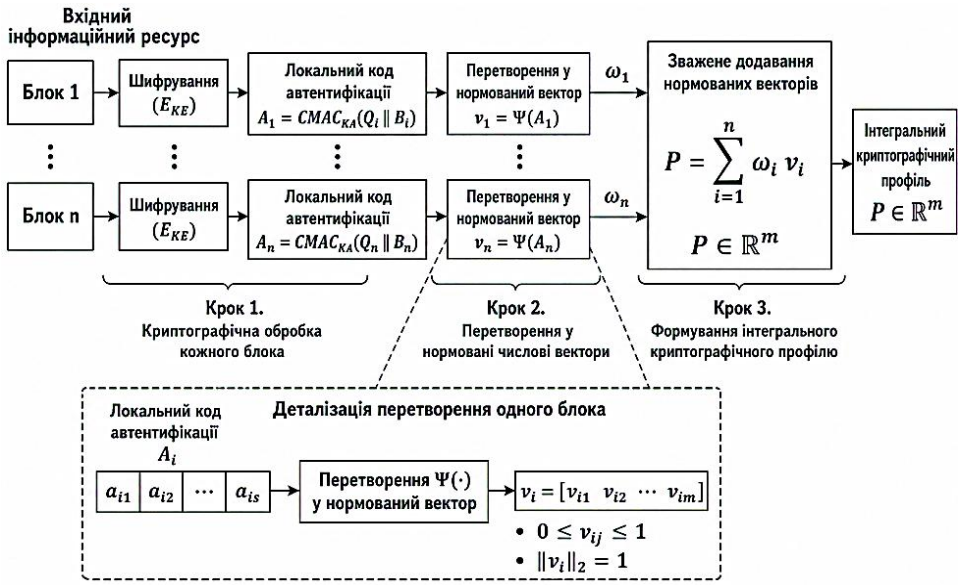


Рис. 2. Формування інтегрального криптографічного профілю

Модель оцінювання автентичності

Після надходження інформаційного ресурсу виконується повторне формування його інтегрального криптографічного профілю та порівняння з еталонним профілем, сформованим під час первинної обробки [10, 17]. На відміну від традиційних схем, що приймають рішення лише на основі збігу або незбігу криптографічних кодів, запропонований метод передбачає кількісне оцінювання масштабу виявлених відмінностей між еталонним і поточним профілями, не замінюючи точного порівняння локальних кодів автентифікації.

Для оцінювання відмінності між еталонним і поточним профілями визначається нормована криптографічна відстань:

$$\Delta = \frac{\|\mathbf{P} - \mathbf{P}'\|_2}{\|\mathbf{P}\|_2 + \|\mathbf{P}'\|_2 + \varepsilon}, \quad 0 \le \Delta < 1, \tag{12}$$

де Δ – нормована відстань між інтегральними криптографічними профілями, $\mathbf{P}$ – еталонний криптографічний профіль інформаційного ресурсу,

$\mathbf{P}'$ – криптографічний профіль, сформований після повторної обробки отриманого ресурсу, $\|\cdot\|_2$– евклідова норма, $\varepsilon > 0$– мале стабілізаційне значення, яке запобігає діленню на нуль. Значення $\Delta = 0$ відповідає повному збігу профілів, тоді як його зростання свідчить про збільшення відмінності між еталонним і повторно сформованим криптографічними представленнями ресурсу.

На основі отриманої відстані визначається коефіцієнт автентичності:

$$T = e^{-\alpha\Delta}, \tag{13}$$

де T – коефіцієнт автентичності інформаційного ресурсу, α – коефіцієнт чутливості, який визначає швидкість зменшення значення T зі збільшенням відмінності між профілями, e – основа натурального логарифма.

Якщо профілі повністю збігаються, то $\Delta = 0$ і $T = 1$. Зі збільшенням відстані між профілями значення T монотонно зменшується та кількісно характеризує ступінь їх відмінності. При цьому криптографічний факт порушення цілісності встановлюється за результатами точного порівняння локальних кодів A_i і A'_i, а коефіцієнт T використовується як допоміжна агрегована оцінка.

На рис. 3 відображено залежність коефіцієнта автентичності T від нормованої відстані Δ між еталонним і поточним інтегральними криптографічними профілями. Зі збільшенням коефіцієнта чутливості α значення T зменшується швидше, що забезпечує більш чутливе реагування методу на відмінності між профілями.

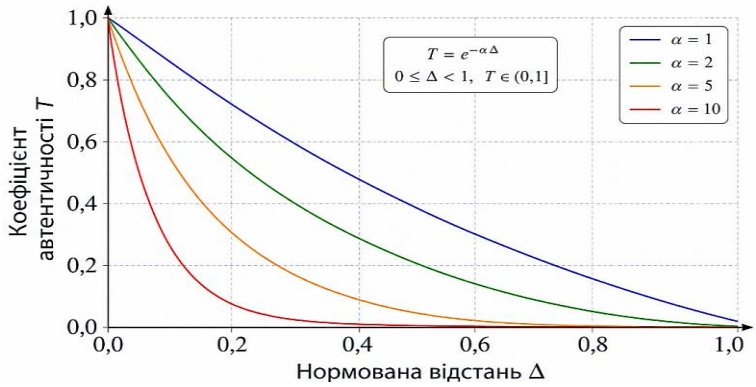


Рис. 3. Графік залежності коефіцієнта автентичності $T = e^{-\alpha\Delta}$

Інтегральна модель контролю цілісності

Для підвищення достовірності перевірки інформаційного ресурсу запропоновано інтегральну модель контролю цілісності, яка поєднує кількісну оцінку відповідності профілів із результатами точного порівняння локальних кодів автентифікації. Такий підхід дозволяє враховувати як загальний рівень відповідності криптографічного профілю, так і локальні зміни, що виникають унаслідок несанкціонованої модифікації окремих фрагментів інформації.

Інтегральний показник цілісності визначається за виразом:

$$I = \beta T + (1-\beta)\frac{1}{n}\sum_{i=1}^{n}\delta_i, \tag{14}$$

де I – інтегральний показник цілісності інформаційного ресурсу, T – коефіцієнт автентичності, β – ваговий коефіцієнт, який задає співвідношення між глобальною та локальною оцінками цілісності $(0 \le \beta \le 1)$, n – кількість інформаційних блоків, δ_i – результат перевірки автентичності і-го блока, який визначається як:

$$\delta_i = \begin{cases} 1, & A_i = A'_i, \\ 0, & A_i \neq A'_i, \end{cases} \tag{15}$$

де A_i – еталонний локальний код автентифікації і-го блока, A'_i– повторно сформований локальний код автентифікації. Значення β встановлюється політикою безпеки. За збільшення β більший вплив на показник I має агрегована відмінність профілів, а за зменшення β — частка блоків із коректними локальними кодами автентифікації. Для початкового налаштування може використовуватися $\beta = 0{,}5$, однак остаточне значення потребує експериментального обґрунтування.

Якщо всі локальні автентифікаційні коди збігаються, показник I набуває максимального значення, що відповідає повному збереженню цілісності інформаційного ресурсу. У разі виявлення змін окремих блоків значення показника зменшується пропорційно кількості порушених елементів та загальному рівню автентичності. Це забезпечує інтегральне оцінювання цілісності та дає змогу виявляти як повну, так і часткову модифікацію інформаційного ресурсу.

Модель ризику компрометації

Заключним етапом запропонованого методу є оцінювання ризику компрометації інформаційного ресурсу, що дозволяє врахувати не лише результати перевірки автентичності та цілісності, а й потенційні наслідки порушення інформаційної безпеки. На відміну від традиційних підходів, у яких рішення приймається лише за результатами криптографічної перевірки, запропонована модель враховує критичність інформаційного ресурсу та можливі втрати від його компрометації.

$$D_A = \begin{cases} \text{Автентичний}, & \delta_i = 1\ \forall i \wedge X_F = 1, \\ \text{Неавтентичний}, & \exists i : \delta_i = 0 \vee X_F = 0, \end{cases} \tag{16}$$

де D_A – криптографічний статус інформаційного ресурсу, $\mathcal{X}_F$ – результат перевірки актуальності контексту свіжості.

Ризик компрометації визначається залежністю:

$$\rho = (1 - I)c_R\ell_R, \quad (17)$$

де ρ – інтегральний ризик компрометації інформаційного ресурсу, I – інтегральний показник цілісності, $c_R \in [0,1]$ – нормований коефіцієнт критичності інформаційного ресурсу, $\ell_R \in [0,1]$ – нормований коефіцієнт потенційних втрат. За таких умов $\rho \in [0,1]$. Значення ρ_{max} визначається політикою безпеки як максимально допустимий рівень ризику для повторної перевірки ресурсу.

На основі розрахованого ризику формується рішення щодо автентичності інформаційного ресурсу:

$$D_R = \begin{cases} \text{Прийняти ресурс}, & D_A = \text{автентичний}, \\ \text{Відхилити ресурс}, & \mathcal{X}_F = 0, \\ \text{Повторна перевірка}, & D_A = \text{неавтентичний} \wedge \mathcal{X}_F = 1 \wedge \rho < \rho_{max}, \\ \text{Відхилити ресурс}, & D_A = \text{неавтентичний} \wedge \mathcal{X}_F = 1 \wedge \rho \geq \rho_{max}. \end{cases} \quad (18)$$

де D_R – рішення щодо подальшої обробки інформаційного ресурсу, D_A– його криптографічний статус, $\mathcal{X}_F$ – максимально допустимий ризик, за якого ще допускається повторна перевірка. Порушення актуальності контексту свіжості спричиняє безумовне відхилення ресурсу незалежно від значення ρ.

Запропонована модель розділяє встановлення криптографічного статусу ресурсу та вибір подальшої реакції. Будь-яке порушення контексту свіжості спричиняє відхилення ресурсу. За виявлення локальних порушень цілісності й збереження актуальності контексту рішення між повторною перевіркою та відхиленням визначається з урахуванням критичності ресурсу, потенційних втрат і розрахованого ризику компрометації [13, 15].

Для структурно-функціонального оцінювання запропонованого методу сформовано набір сценаріїв, що охоплює оброблення незміненого ресурсу, модифікацію одного або декількох блоків, перестановку блоків, підміну ресурсу та повторне відтворення попередньої версії. Сценарії призначені для перевірки логічної відповідності розроблених процедур заявленим функціям: підтвердженню автентичності, виявленню й локалізації порушень цілісності, контролю свіжості та вибору подальшої реакції з урахуванням ризику компрометації. Сформовані сценарії наведено в табл. 1

Як видно з табл. 1, незмінений інформаційний ресурс має пройти локальну криптографічну перевірку та контроль контексту свіжості, після чого може бути прийнятий системою. Модифікація, перестановка або підміна блоків спричиняє невідповідність локальних кодів автентифікації та зміну інтегральних показників, що забезпечує локалізацію порушення і формування реакції залежно від розрахованого ризику. Повторне відтворення попередньої версії розглядається окремо: порушення контексту свіжості є підставою для безумовного відхилення ресурсу незалежно від його критичності.

Результати сценарного аналізу підтверджують функціональну узгодженість складових запропонованого методу. Поблокове формування кодів автентифікації забезпечує встановлення місця порушення, інтегральний криптографічний профіль характеризує сукупний ступінь відмінності ресурсу від еталонного стану, а модель ризику визначає доцільність повторної перевірки або остаточного відхилення ресурсу.

Таблиця 1

Сценарії перевірки запропонованого методу

Сценарій	Характер порушення	Очікуваний результат
S1	Ресурс без змін	Підтвердження автентичності та прийняття ресурсу
S2	Модифіковано один блок	Виявлення й локалізація зміненого блока; повторна перевірка або відхилення залежно від ризику
S3	Модифіковано 10 % блоків	Зниження коефіцієнта автентичності та показника цілісності, зростання ризику; повторна перевірка або відхилення
S4	Переставлено блоки	Виявлення порушення позиційної цілісності; повторна перевірка або відхилення залежно від ризику
S5	Повторно передано попередню версію ресурсу	Безумовне відхилення за результатом перевірки контексту свіжості
S6	Підмінено інформаційний ресурс	Виявлення невідповідності локальних кодів автентифікації; повторна перевірка або відхилення залежно від ризику

Для визначення функціональних відмінностей запропонований метод порівняно з традиційним підходом, під яким розуміється схема послідовного шифрування інформаційного ресурсу та формування єдиного MAC-коду без поблокової локалізації змін, інтегрального оцінювання та аналізу ризику [5, 14, 19, 21]. Результати порівняння наведено в табл. 2.

Дані табл. 2 показують, що обидва підходи мають лінійну асимптотичну складність відносно кількості блоків за фіксованої розмірності профілю. Водночас запропонований метод доповнює базові процедури шифрування й автентифікації засобами поблокової локалізації, інтегрального оцінювання цілісності, аналізу ризику та багаторівневого вибору реакції. Отже, його відмінність полягає не у зміні базового класу складності, а в розширенні функціональних можливостей криптографічного контролю.

Таблиця 2

Функціональне порівняння традиційного та запропонованого методів

Критерій	**Традиційний підхід**	**Запропонований метод**
Єдиний узгоджений цикл криптографічної обробки	Ні	Так
Інтегральний криптографічний профіль	Відсутній	Формується
Локалізація змінених блоків	Відсутня за єдиного MAC	Забезпечується поблоковою перевіркою
Інтегральне оцінювання цілісності	Відсутнє	Реалізовано
Аналіз ризику компрометації	Не використовується	Реалізовано
Багаторівневе прийняття рішення	Відсутнє	Реалізовано
Асимптотична складність за фіксованої розмірності профілю	$O(n)$	$O(n)$

Для уточнення місця запропонованого методу серед поширених криптографічних конструкцій проведено його функціональне порівняння зі схемою AES-CBC + HMAC, механізмом AES-CMAC та режимом автентифікованого шифрування AES-GCM. Порівняння здійснено за наявністю функцій конфіденційності, автентичності й цілісності, можливістю локалізації зміненого блока, урахуванням критичності даних, кількісного оцінювання та протидії повторному відтворенню [14, 19, 21]. Результати наведено в табл. 3.

Таблиця 3

Порівняння запропонованого методу з поширеними криптографічними схемами

Критерій	**AES-CBC + HMAC**	**AES-CMAC**	**AES-GCM**	**Запропонований метод**
Конфіденційність	Так	Ні	Так	Так
Автентичність і цілісність повідомлення	Так	Так	Так	Так
Локалізація зміненого блока	Ні, за єдиного MAC	Ні, за єдиного CMAC	Ні, за єдиного тега	Так, за поблокового CMAC
Урахування критичності блоків	Ні	Ні	Ні	Так
Кількісне оцінювання ступеня відмінності	Ні	Ні	Ні	Так
Ризик-орієнтований вибір реакції	Ні	Ні	Ні	Так
Захист від повторного відтворення	За автентифікованого контексту свіжості та контролю повторів	За включення і перевірки контексту свіжості	За унікального nonce та контролю повторів	Так, за включення F_R до CMAC і перевірки X_F

Результати табл. 3 мають функціональний характер і не свідчать про перевагу запропонованого методу над AES-GCM, AES-CMAC або AES-CBC + HMAC за базовою криптографічною стійкістю. Відмінність запропонованого методу полягає у поблоковому формуванні кодів автентифікації, локалізації змінених фрагментів, побудові зваженого інтегрального профілю та використанні оціненого ризику для вибору подальшої реакції. Отже, стандартизовані криптографічні механізми доповнюються функціями кількісного аналізу стану інформаційного ресурсу, а не замінюються новим блоковим шифром або режимом його роботи. Такий підхід узгоджується із сучасною тенденцією адаптивного вибору криптографічних параметрів на основі динамічної довіри та поточного ризику [11, 13].

Окрім функціональних можливостей, для запропонованого методу визначено асимптотичну обчислювальну складність. Основні витрати пов'язані з поблоковим шифруванням, формуванням CMAC, перетворенням локальних кодів на числові вектори та їх зваженим агрегуванням. Загальні обчислювальні витрати можуть бути подані як:

$$\mathcal{C}_{method}(n,m) = n\,(\mathcal{C}_E + \mathcal{C}_{CMAC} + \mathcal{C}_\Psi + \mathcal{C}_\omega) + \mathcal{C}_\Delta(m) + \mathcal{C}_D \quad , \tag{19}$$

де $\mathcal{C}_E$ – витрати на шифрування одного блока, $\mathcal{C}_{CMAC}$ – витрати на формування локального коду автентифікації, $\mathcal{C}_\Psi$ – витрати на перетворення коду автентифікації на нормований числовий вектор, $\mathcal{C}_\omega$ – витрати на зважене додавання локального вектора до інтегрального профілю, $\mathcal{C}_D$ – витрати на визначення інтегральних показників і формування рішення, $\mathcal{C}_\Delta(m)$ – витрати на обчислення відстані між профілями розмірності m. За фіксованої розмірності m кожний інформаційний блок обробляється один раз, тому асимптотична складність методу відносно кількості блоків становить $O(n)$. Якщо m розглядається як змінна величина, операції формування профілю мають складність $O(nm)$.

Практичне застосування методу потребує коректного керування ключовим матеріалом, забезпечення унікальності режимозалежних параметрів Q_i, контролю контексту свіжості, захисту параметрів значущості й критичності блоків, а також обґрунтованого встановлення порогового рівня ризику. Надійність формування ключів, nonce та інших режимозалежних значень безпосередньо залежить від якості джерел ентропії та криптографічно стійких генераторів випадкових чисел [11, 24]. Водночас у ресурсно обмежених середовищах реалізація зазначених процедур має

враховувати баланс між криптографічною стійкістю, апаратними витратами та швидкодією [14, 19, 21]. Зазначені умови визначають межі коректного функціонування методу та мають бути враховані під час його програмної реалізації й подальшого експериментального оцінювання.

Висновки і перспективи подальших досліджень

У роботі розроблено метод автентифікації інформаційних ресурсів на основі блокового шифрування, орієнтований на комплексне забезпечення конфіденційності, автентичності та цілісності даних. Наукова новизна методу полягає у використанні поблокових кодів автентифікації для формування зваженого інтегрального криптографічного профілю, що дає змогу не лише встановлювати факт порушення цілісності, а й локалізувати змінені фрагменти та оцінювати загальний ступінь відмінності інформаційного ресурсу від еталонного стану.

Запропоновано розділення ключового матеріалу для процедур шифрування та автентифікації, урахування контексту свіжості й використання позиційних та ідентифікаційних ознак блоків. Це забезпечує зв'язування локального коду автентифікації з конкретним ресурсом, його структурою та актуальною версією, що створює умови для виявлення модифікації, перестановки, підміни й повторного відтворення даних.

Сформований інтегральний профіль використовується як додаткова кількісна характеристика стану ресурсу, тоді як криптографічний факт цілісності визначається шляхом точного порівняння локальних кодів автентифікації. Поєднання локального контролю, інтегрального оцінювання та аналізу наслідків компрометації дає змогу розмежувати встановлення автентичності ресурсу і вибір подальшої реакції системи залежно від його критичності.

Структурно-функціональний аналіз показав, що запропонований метод розширює можливості традиційних схем із єдиним кодом автентифікації завдяки поблоковій локалізації змін, урахуванню неоднакової значущості фрагментів даних і ризик-орієнтованому прийняттю рішень. Обчислювальна складність методу є лінійною відносно кількості блоків, що створює передумови для його застосування під час захисту інформаційних ресурсів різного обсягу.

Перспективи подальших досліджень пов'язані з програмною реалізацією методу, експериментальним обґрунтуванням параметрів оцінювання, визначенням оптимальних порогів прийняття рішень і дослідженням впливу розміру блоків на точність локалізації та швидкодію. Доцільним є також проведення порівняльного тестування з AES-GCM, AES-CMAC і схемою AES-CBC + HMAC за показниками часу оброблення, пропускної здатності, витрат пам'яті та здатності виявляти різні типи модифікації інформаційних ресурсів.

Література

[1] Roy, K. S., Sujith, M., Bhanu, B., Preethi, & Hazarika, R. A. (2024). FPGA-based dual-layer authentication scheme utilizing AES and ECC for unmanned aerial vehicles. *EURASIP Journal on Wireless Communications and Networking, 2024*, Article 91. https://doi.org/10.1186/s13638-024-02419-8

[2] Haverkamp, I., & Sarmah, D. K. (2024). Evaluating the merits and constraints of cryptography–steganography fusion: A systematic analysis. *International Journal of Information Security, 23*, 2607–2635. https://doi.org/10.1007/s10207-024-00853-9

[3] Luo, X., Chen, X., Cheng, Q., et al. (2024). A survey on the application of blockchain in cryptographic protocols. *Cybersecurity, 7*, Article 79. https://doi.org/10.1186/s42400-024-00324-7

[4] Zhong, Y., & Gu, J. (2024). Lightweight block ciphers for resource-constrained environments: A comprehensive survey. *Future Generation Computer Systems, 157*, 288–302. https://doi.org/10.1016/j.future.2024.03.054

[5] Ansari, S. A., & Ali, S. (2025). A systematic review of lightweight cryptographic schemes for security and privacy in IoT. *Discover Computing, 28*, Article 266. https://doi.org/10.1007/s10791-025-09755-3

[6] Cambou, B. F., & Alam, M. (2025). Challenge–response pair mechanisms and multi-factor authentication schemes to protect private keys. *Applied Sciences, 15*(6), Article 3089. https://doi.org/10.3390/app15063089

[7] Zhang, Y., Zhou, X., & Qin, X. (2025). An anonymous credential-based efficient staged dual-chain authentication protocol for satellite–earth links. *Journal of King Saud University – Computer and Information Sciences, 37*, Article 30. https://doi.org/10.1007/s44443-025-00017-2

[8] Ganesh, R., Khan, B. U. I., Khan, A. R., et al. (2025). A panoramic survey of the Advanced Encryption Standard: From architecture to security analysis, key management, real-world applications, and post-quantum challenges. *International Journal of Information Security, 24*, Article 216. https://doi.org/10.1007/s10207-025-01116-x

[9] Kostiuk, Y., Bebeshko, B., Kriuchkova, L., Lytvynov, V., Oksanych, I., Skladannyi, P., & Khorolska, K. (2024). Information protection and data exchange security in wireless mobile networks using authentication and key exchange protocols. *Cybersecurity: Education, Science, Technique, 1*(25), 229–252. https://doi.org/10.28925/2663-4023.2024.25.229252

[10] Chethana, R. V., Vrindavanam, J., Roy, S., & Deshmukh, P. C. (2025). A review of block ciphers and their post-quantum considerations. *IEEE Access, 13*, 57834–57846. https://doi.org/10.1109/ACCESS.2025.3554602

[11] Skladannyi, P. M., Hulak, H. M., & Kostiuk, Y. V. (2025). A fuzzy-controlled chaotic number generator for cryptographic systems with dynamic trust. *Telecommunication and Information Technologies, 4*(89), 137–147. https://doi.org/10.31673/2412-4338.2025.048916

[12] Deng, C., Li, L., Feng, J., & Yan, L. (2025). HAIL: A family of high-diffusion lightweight block ciphers for Internet of Things security. *Physica Scripta, 100*(1), Article 015273. https://doi.org/10.1088/1402-4896/ad9d8f

[13] Kostiuk, Y., Skladannyi, P., Mazur, N., Rzaieva, S., Hnatchenko, D., & Honcharenko, I. (2026). A formal model for adaptive selection of cryptographic parameters for channel protection in corporate computer networks based on dynamic trust assessment. *Cybersecurity: Education, Science, Technique, 4*(32), 20–44. https://doi.org/10.28925/2663-4023.2026.32.1111

[14] Khan, S., Inayat, K., Muslim, F. B., Shah, Y. A., Rehman, M. A. U., Khalid, A., Imran, M., et al. (2024). Securing the IoT ecosystem: ASIC-based hardware realization of the Ascon lightweight cipher. *International Journal of Information Security, 23*, 3653–3664. https://doi.org/10.1007/s10207-024-00904-1

[15] Kostiuk, Y., Skladannyi, P., Bondarchuk, A., & Hnatchenko, D. (2026). A method for cryptographically resilient event correlation in SIEM based on risk-oriented assessment

and context-hashed similarity. *Information and Telecommunication Sciences, 17*(1), 36–50. https://doi.org/10.20535/2411-2976.12026.36-50

[16] Hedabou, M. (2021). Cloud key management based on verifiable secret sharing. In *Network and system security: NSS 2021* (Lecture Notes in Computer Science, Vol. 13041). Springer. https://doi.org/10.1007/978-3-030-92708-0_18

[17] Choi, W., Hwang, S., Lee, B., et al. (2024). ZLR: A fast online authenticated encryption scheme achieving full security. *Designs, Codes and Cryptography, 92*, 3261–3316. https://doi.org/10.1007/s10623-024-01434-6

[18] Skladannyi, P., Kostiuk, Y., Rzaieva, S., Bebeshko, B., & Korshun, N. (2025). Adaptive methods for embedding digital watermarks to protect audio and video images in information and communication systems. In *Proceedings of the Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2025)* (Vol. 4016, pp. 13–31). CEUR Workshop Proceedings.

[19] Rashmi, H. C., & Guruprakash, C. D. (2024). Privacy-aware novel lightweight cryptography mechanism for IoT security. *Multimedia Tools and Applications, 83*, 76389–76404. https://doi.org/10.1007/s11042-024-18517-0

[20] Kostiuk, Y., Rzaieva, S., Khorolska, K., Mazur, N., & Korshun, N. (2025). Architecture of a software system for confidential access to information resources in computer networks. In *Proceedings of the Workshop on Cyber Security and Data Protection (CSDP 2025)* (Vol. 4042, pp. 37–53). CEUR Workshop Proceedings.

[21] Guşiță, B., Anton, A. A., Stângaciu, C. S., et al. (2025). Securing the IoT edge: A survey on lightweight cryptography, anonymous routing, and communication protocol enhancements. *International Journal of Information Security, 24*, Article 149. https://doi.org/10.1007/s10207-025-01071-7

[22] Skladannyi, P., Kostiuk, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). Model and methodology for forming adaptive security profiles to protect wireless networks under dynamic cyber threats. In *Proceedings of the Workshop on Cyber Security and Data Protection (CSDP 2025)* (Vol. 4042, pp. 17–36). CEUR Workshop Proceedings.

[23] Alonso, F., Samaniego, B., Farias, G., & Dormido-Canto, S. (2024). Analysis of cryptographic algorithms to improve cybersecurity in the industrial electrical sector. *Applied Sciences, 14*(7), Article 2964. https://doi.org/10.3390/app14072964

[24] Kostiuk, Y., Sokolov, V., Skladannyi, P., Kuzminykh, I., & Ghita, B. (2026). Cryptographically resilient random number generators based on entropy sources in information security systems. In *2026 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)* (pp. 1–6). IEEE. https://doi.org/10.1109/BlackSeaCom69760.2026.11598257

[25] Öztürk, G., et al. (2025). Secure and efficient data encryption for the Internet of Robotic Things based on Ascon. *Applied Sciences, 15*(19), Article 10641. https://doi.org/10.3390/app151910641

[26] Lo, N.-W., Huang, J.-J., & Yang, T.-C. (2025). A lightweight mutual authentication mechanism for applications utilizing low-power IoT devices. *Electronics, 14*(21), Article 4178. https://doi.org/10.3390/electronics14214178

УДК 004.056.5:004.7:656.1

Trofimov *O.*, *Hulak H.* Method for Authentication of Information Resources Based on block Cipher Encryption

Abstract. This paper presents a method for the authentication of information resources based on block cipher encryption, designed to ensure the authenticity, integrity, and confidentiality of data during storage, processing, and transmission in computer systems and networks. The relevance of improving cryptographic authentication mechanisms is substantiated in the context of the growing number of cyber threats associated with data forgery, unauthorized access, and the compromise of information resources. An analysis of contemporary authentication methods is conducted, revealing that existing solutions do not always provide an appropriate balance between cryptographic strength, processing speed, and computational efficiency. The application of block cipher algorithms for generating authentication data is examined, and the key requirements for constructing the proposed method are identified. A method for authenticating information resources is proposed, based on cryptographic key generation, block transformation of the information resource, authentication code generation, integrity verification, and decision-making regarding the authenticity of the resource. Unlike existing approaches, the proposed method integrates encryption and authentication procedures, enables localization of modified data blocks, provides quantitative authentication assessment, and supports risk-oriented decision-making. The sequence of cryptographic processing of the information resource is formalized, and models for constructing an integrated authentication profile, assessing authenticity and integrity, and selecting an appropriate response according to the risk of compromise are developed. The conducted structural and functional evaluation demonstrated the capability of the proposed method to localize modified data blocks and quantitatively determine the degree of deviation of the information resource from its reference state. The obtained results confirm the feasibility of further software implementation and experimental validation of the proposed method in modern information and communication systems.

Keywords: information resource authentication, block cipher encryption, cryptographic authentication, data integrity assurance, message authentication code, cryptographic key, information security, information and communication systems.

Трофімов Олександр Сергійович, аспірант кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Trofimov Oleksandr, Postgraduate student of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok Borys Grinchenko Kyiv Metropolitan University.

Гулак Геннадій Миколайович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Hulak Hennadii, Doctor of Technical Science, Professor, Professor of the Department of Information and Cyber Security named after Professor Volodymyr Buriachok Borys Grinchenko Kyiv Metropolitan University.

Дата надходження:	Дата прийняття:	Дата публікації:
19.06.2026	04.07.2026	21.08.2026