оперувати міжнародними інформаційними системами, зобов'язані стратегічно інвестувати у підготовку кадрів, розвиток цифрових навичок міжнародних команд та формування корпоративної культури, керованої даними. Без кваліфікованого персоналу, здатного обробляти та інтерпретувати інформацію, навіть найінноваційніші технології не зможуть забезпечити стабільну управлінську перевагу на міжнародній арені.

Обґрунтоване впровадження цих технологій у глобальну економічну стратегію вимагає чіткої послідовності управлінських дій. Цей процес починається з глобального аудиту цілей та оцінки міжнародних джерел даних та IT-інфраструктури. Далі відбувається вибір інструментів, міжрегіональна інтеграція та підготовка даних для обробки, а також створення надійної транскордонної інфраструктури для передачі й захисту інформації. Завершується цикл постійним моніторингом та навчанням глобальних команд, що є основою для розвитку культури, керованої даними, та ефективного управління знаннями [1, с. 7].

У сучасній міжнародній економіці обґрунтована стратегія — це результат синтезу передових технологій (ШІ, Big Data) та кваліфікованого людського капіталу. Саме цей симбіоз, що формує корпоративну культуру, керовану даними, є єдиною запорукою стабільності та прибутковості на глобальній арені.

Список використаної літератури

[1]. Писаревська Г., "Інформаційне забезпечення управління зовнішньоекономічною діяльністю підприємства," *Економіка та суспільство*, вип. 51, с. 1-8, 2023. [Online]. Available: https://economyandsociety.in.ua/index.php/journal/article/view/2485/2404. (Accessed: 20.09.2025).

[2]. Чорненька О., "Менеджмент зовнішньоекономічної діяльності підприємства в умовах цифрової економіки," *Економіка та суспільство*, вип. 68, с. 1-6, 2024. [Online]. Available: https://economyandsociety.in.ua/index.php/journal/article/view/4862/4802. (Accessed: 20.09.2025).

[3]. Завербний А., Залізна Л., Жук О., "Особливості формування методів прийняття рішень вітчизняними підприємствами у зовнішньоекономічній діяльності: інформаційний аспект," *Економіка та суспільство*, вип. 50, с. 1-6, 2023. [Online]. Available: https://economyandsociety.in.ua/index.php/journal/article/view/2400/2321. (Accessed: 21.09.2025).

[4]. Мотузка О., Гринчак Н., "Стратегічні орієнтири розвитку зовнішньоекономічної діяльності підприємств у середовищі BANI," *Вісник Хмельницького національного університету*, вип. 1, с. 133-138, 2023. [Online]. Available: https://heraldes.khmnu.edu.ua/index.php/heraldes/article/view/704/719. (Accessed: 23.09.2025).

[5]. Бондарук В., "Цифрові технології в забезпеченні фінансової результативності суб'єктів господарювання у зовнішньоекономічній діяльності," *Економіка та суспільство*, вип. 71, с. 1-6, 2025. [Online]. Available: https://economyandsociety.in.ua/index.php/journal/article/view/5614/5551. (Accessed: 23.09.2025).

УДК 004.056.55

УПРАВЛІННЯ КЛЮЧОВОЮ ІНФОРМАЦІЄЮ В КАСКАДНИХ СИСТЕМАХ ПОТОКОВИХ ШИФРІВ

Главчев М.І., Главчева Ю.М., Гавриленко С.Ю.
(Maksym.Glavchev@khpi.edu.ua, Yuliia.Hlavcheva@khpi.edu.ua, Svitlana.Gavrylenko@khpi.edu.ua)
Національний технічний університет «Харківський політехнічний інститут» (Україна)

Робота присвячена проблемі управління ключами в каскадних потокових шифрах. Після аналізу недоліків існуючих методів пропонується вдосконалений підхід на основі пам'ять-вимогливої функції Argon2. Методика передбачає посилення початкового секрету за допомогою солі для захисту від атак перебором, після чого з отриманого розширеного ключа детерміновано генеруються всі ключі та вектори ініціалізації для каскаду. Такий підхід гарантує незалежність ключів, є універсальним для секретів з низькою ентропією та значно підвищує надійність криптосистеми..

В сучасному цифровому світі безпека передачі даних є критично важливою. Потокові шифри, завдяки своїй швидкості та низьким вимогам до ресурсів, широко застосовуються в системах реального часу, таких як мобільний зв'язок та бездротові мережі. Проте, з розвитком обчислювальних потужностей, зокрема з появою загрози квантових комп'ютерів, стійкість окремих криптографічних алгоритмів може бути поставлена під сумнів. Каскадне шифрування, що передбачає послідовне застосування кількох алгоритмів, є ефективним підходом для підвищення загальної криптографічної стійкості системи. Такий підхід ускладнює криптоаналіз, оскільки зловмиснику необхідно зламати всі алгоритми в каскаді. Однак каскадування створює нову проблему: ефективне та безпечне управління ключовою інформацією для кількох шифрів одночасно. Розробка надійних методик генерації та розподілу ключів у таких системах є актуальною задачею, спрямованою на побудову захищених та перспективних криптосистем.

Проблема управління ключами в каскадних системах вирішується кількома підходами. Найпростіший метод, пряме дублювання майстер-ключа, є небезпечним через вразливість до атак на пов’язаних ключах [1, 2]. Певним покращенням є розділення ключа, коли довгий секрет ділиться на частини. Проте цей підхід вимагає від майстер-ключа значної початкової довжини та ентропії, що не завжди практично [3].

Найбільш надійним та рекомендованим рішенням є використання функцій виведення ключів (Key Derivation Functions, KDF), що формалізовано у рекомендаціях NIST [4]. KDF — це криптографічний алгоритм, що перетворює початковий секрет (майстер-ключ) та сіль у декілька незалежних, криптографічно стійких ключів потрібної довжини. Стандартизовані реалізації, такі як HKDF 54], дозволяють ефективно "розтягнути" ентропію початкового секрету. Це унеможливлює компрометацію всієї системи, навіть якщо один з похідних ключів буде розкрито, і забезпечує високий рівень безпеки для каскадних конструкцій.

Каскадне шифрування полягає у послідовній обробці відкритого тексту кількома потоковими шифрами. Вихід одного шифру стає входом для наступного:

Шифротекст = E_k3(E_k2(E_k1(Відкритий_текст)))

де E — функція шифрування, а k1, k2, k3 — ключі для відповідних алгоритмів. Основна перевага полягає в тому, що криптостійкість каскаду визначається найсильнішим алгоритмом у ньому, а для повного зламу потрібно скомпрометувати всі алгоритми [6]. Центральною проблемою стає генерація та розподіл ключів k1, k2, ... kN. Необхідно гарантувати, щоб ці ключі були незалежними, криптографічно стійкими та згенерованими з єдиного початкового секрету (майстер-ключа) без втрати безпеки.

Напрямки, що використовуються для вирішення цієї проблеми:

- Пряме дублювання: k1 = k2 = k3 = Майстер-ключ. Просто, але небезпечно. Якщо один алгоритм має вразливість до атак на відомому ключі, вся система стає вразливою.
- Розділення ключа: Майстер-ключ = k1 | k2 | k3. Безпечніше, але вимагає довгого майстер-ключ і не захищає від аналізу залежностей між частинами ключа.
- Функція виведення ключів (KDF): (k1, k2, k3) = KDF(Майстер-ключ, Salt). Найбільш надійний з існуючих методів, що забезпечує псевдовипадковість та незалежність похідних ключів.

Пропонується вдосконалений підхід, що забезпечує максимальний рівень захисту майстер-ключа та гарантує криптографічну якість похідних ключів. Методика полягає у двохетапному процесі: посиленні початкового секрету та подальшому його детермінованому розподілі.

1. Посилення ключа (Key Hardening) за допомогою пам'ять-вимогливої KDF: На цьому етапі застосовується сучасний алгоритм, спеціально розроблений для протидії атакам перебору на спеціалізованому обладнанні (GPU, ASIC). Оптимальним вибором є Argon2, переможець змагання Password Hashing Competition. На відміну від швидких KDF (як HKDF), Argon2 навмисно є "важким": він вимагає значних обчислювальних ресурсів та обсягу пам'яті, що робить перебір надзвичайно повільним і дорогим.

Вхідні дані:

- Майстер-ключ: Початковий секрет. Метод ефективний навіть якщо цей ключ має недостатню ентропію (наприклад, є паролем).
- Сіль (Salt): Унікальне випадкове значення для кожної сесії. Унеможливлює атаки з використанням попередньо обчислених таблиць (rainbow tables).

- Параметри складності: Вартість пам'яті (memory cost), кількість ітерацій (iterations) та ступінь паралелізму (parallelism). Ці параметри дозволяють налаштувати обчислювальну складність, створюючи баланс між безпекою та продуктивністю.

- Процес: Розширений_ключ = Argon2(Майстер-ключ, Salt, параметри_складності)

- Результат: Генерується довгий псевдовипадковий ключ (наприклад, 1024 біти), стійкість якого до перебору значно перевищує стійкість початкового майстер-ключа.

2. Детермінований розподіл ключового матеріалу: Отриманий розширений ключ слугує джерелом ентропії для всіх потреб каскадної системи. Він послідовно ділиться на частини необхідної довжини для кожного потокового шифру.

k1 = перші N біт Розширеного_ключа

k2 = наступні M біт Розширеного_ключа...

Перевага генерації ключа надлишкової довжини полягає в можливості використання залишку для інших криптографічних примітивів, наприклад, для векторів ініціалізації (IV) або ключів автентифікації (MAC), що робить систему більш елегантною та ефективною.

Ця методика створює багатошаровий захист: навіть якщо один із похідних ключів буде скомпрометований, зловмисник не зможе відновити майстер-ключ або інші ключі каскаду.

Розглянемо приклад каскаду із двох потокових шифрів: ChaCha20 (потребує 256-бітний ключ та 96-бітний nonce) та AES-256 в режимі CTR (потребує 256-бітний ключ та 128-бітний IV). Сумарна потреба в ключовому матеріалі: 256 (ChaCha20 ключ) + 96 (ChaCha20 nonce) + 256 (AES ключ) + 128 (AES IV) = 736 біт.

1. Вхідні дані:

- Майстер-ключ: 256-бітний секрет, отриманий за протоколом Діффі-Геллмана.

- Сіль: Випадково згенеровані 128 біт.

2. Генерація розширеного ключа: Використовуємо Argon2id для генерації 768-бітного (96 байт) розширеного ключа з рекомендованими параметрами безпеки (наприклад, OWASP):

- Версія: Argon2id

- Кількість ітерацій (t): 1

- Вартість пам'яті (m): 65536 КБ (64 МБ)

- Паралелізм (p): 4 Розширений_ключ_768_біт = Argon2id(Майстер-ключ, Сіль, t=1, m=65536, p=4)

3. Розподілення ключового матеріалу:

- ключ_ChaCha20 (256 біт) = біти 0-255 Розширеного_ключа

- ключ_AES_CTR (256 біт) = біти 256-511 Розширеного_ключа

- nonce_ChaCha20 (96 біт) = біти 512-607 Розширеного_ключа

- IV_AES_CTR (128 біт) = біти 608-735 Розширеного_ключа

Таким чином, з єдиного посиленого джерела безпечно та детерміновано отримуємо весь необхідний криптографічний матеріал для повноцінної роботи каскаду.

Запропонована методика управління ключовою інформацією є комплексним рішенням, що забезпечує значно вищий рівень безпеки порівняно зі стандартними підходами. Її ключові переваги:

- Максимальний захист майстер-ключа: Використання обчислювально важкої KDF-функції, як Argon2, робить атаки повним перебором практично неможливими навіть за наявності спеціалізованого обладнання.

- Універсальність: Методика однаково ефективна як для високоентропійних секретів, так і для ключів з низькою ентропією (наприклад, паролів), "посилюючи" їх до необхідного рівня стійкості.

- Гарантована незалежність ключів: Детермінований розподіл матеріалу з єдиного псевдовипадкового джерела повністю усуває ризик атак на пов'язаних ключах.

- Ефективність та елегантність: Генерація ключа надлишкової довжини дозволяє централізовано забезпечувати не тільки ключі шифрування, а й інший криптографічний матеріал (IV, nonce), спрощуючи архітектуру системи.

Цей підхід є гнучким, масштабованим і дозволяє створювати криптосистеми з довготривалою стійкістю, що є критично важливим в умовах постійного зростання обчислювальних потужностей та нових криптоаналітичних загроз.

Список використаної літератури

1 J. Kelsey, B. Schneier, and D. Wagner, "Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES," in Advances in Cryptology — CRYPTO '96, vol. 1109, N. Koblitz, Ed. Berlin, Heidelberg: Springer, 1996, pp. 237–251. doi: 10.1007/3-540-68697-5_19.

2. Глачев М.І., Новикова А.В. Загальний підхід до комбінованих шифрівМеждународная научная конференция/ MicroCAD : Секція №21 - Інформати-ка і моделювання - НТУ "ХПИ", 2012. – С.12, https://repository.kpi.kharkov.ua/bitstreams/c2363a6a-9c41-4f46-aa26-530dd3282e27/download.

2 J. Katz and Y. Lindell, Introduction to Modern Cryptography, 2nd ed. Boca Raton, FL, USA: CRC Press, 2015.

3]L. Chen, "Recommendation for Key Derivation Using Pseudorandom Functions," NIST Special Publication 800-108, National Institute of Standards and Technology, Gaithersburg, MD, USA, Oct. 2009. [Online]. Available: https://www.google.com/search?q=https://doi.org/10.6028/NIST.SP.800-108

4 H. Krawczyk and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)," IETF, RFC 5869, May 2010. [Online]. Available: https://www.rfc-editor.org/info/rfc5869

5 U. M. Maurer and J. L. Massey, "Cascade Ciphers: The Importance of Being First," Journal of Cryptology, vol. 6, no. 1, pp. 55–61, 1993. doi: 10.1007/BF00191095.

УДК 004.056

ДО ПИТАННЯ СТВОРЕННЯ АЛГОРИТМУ ЗНИЩЕННЯ ІНФОРМАЦІЇ НА МАГНІТНИХ НОСІЯХ НА ОСНОВІ АНАЛІЗУ ПОСЛІДОВНОСТЕЙ

Главчев М.І., Панченко В.І.

(Maksym.Glavchev@khpi.edu.ua, Volodymyr.Panchenko@khpi.edu.ua)

Національний технічний університет «Харківський політехнічний інститут» (Україна)

У даній роботі представлено розробку та дослідження алгоритму знищення інформації на магнітних носіях, що базується на аналізі випадкових послідовностей і багатократному перезаписі даних із динамічним контролем залишкової інформації. Актуальність роботи зумовлена необхідністю підвищення надійності безпечного видалення конфіденційних даних в умовах зростання обсягів збереження та складності відновлення інформації з магнітних доменів. Запропонований алгоритм поєднує криптографічно стійку генерацію випадкових значень, їх інверсію та аналіз рівня знищення після кожної ітерації перезапису. На основі експоненціальної моделі оцінюється необхідна кількість перезаписів для досягнення цільової ймовірності відновлення. Отримані результати підтверджують, що оптимізація кількості ітерацій на основі аналітичної моделі дозволяє знизити залишкову ймовірність відновлення на кілька порядків при помірних витратах часу. Запропонований підхід може бути використаний у системах безпечного знищення інформації та засобах аудиту ІБ.

Проблема безпечного знищення інформації набуває дедалі більшої актуальності в зв'язку зі зростанням обсягів збережених даних та розвитком методів магнітної форензіки. Традиційні алгоритми багаторазового перезапису, зокрема DoD 5220.22-M або Gutmann, часто не враховують особливості залишкових магнітних ефектів, що дозволяє відновити інформацію навіть після десятків циклів перезапису. Сучасні підходи до захисту даних вимагають формалізованих і адаптивних моделей, які дозволяють оцінити ефективність знищення не емпірично, а через аналітичні показники – насамперед через параметр експоненційного зменшення λ.

Методи безпечного знищення інформації ґрунтуються на багаторазовому записі псевдовипадкових або інверсних шаблонів. У роботах [1–4] розглянуто класичні підходи (Gutmann, DoD 5220.22-M, RCMP TSSIT OPS-II). Дослідження NIST SP 800-88r1 [2] формалізує процедури очищення, але не дає моделей оцінки ймовірності відновлення.

Аналіз сучасних досліджень, проведений у роботі [5], показав широке використання статистичних методів оцінки залишкової ентропії та застосування адаптивних PRNG. Під час