УДК 004.056.5 **DOI:10.30837/rt.2025.4.223.03**

К.Є. ЛИСИЦЬКИЙ, PhD., І.В. ЛИСИЦЬКА, д-р техн. наук, І.М. ГАЛЬЦЕВА, Є.П. КОЛОВАНОВА, канд. техн. наук

ЕВОЛЮЦІЯ АРХІТЕКТУР БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ

Вступ

Історія сучасних блокових симетричних шифрів (БСШ) – це історія пошуку оптимального поєднання двох фундаментальних принципів, сформульованих Клодом Елвудом Шенноном у 1949 р.: заплутування (confusion) та дифузії (diffusion).

Сучасні ітеративні блокові шифри, що перетворюють фіксований блок відкритого тексту на блок шифротексту за допомогою багаторазового застосування раундової функції, базуються переважно на двох архітектурних моделях: Мережі Фейстеля та Мережі Підстановки-Перестановки (SPN).

Формальний початок сучасної криптографії заклав американський математик Клод Елвуд Шеннон у відомій роботі "Теорія зв'язку в секретних системах" [1]. Фундаментальні принципи, які дозволяють отримати криптографічно стійке перетворення, згідно з Шенноном:

- заплутування (Confusion): розповсюдження впливу одного знаку відкритого тексту на багато знаків шифртексту, що дозволяє приховати статистичні властивості відкритого тексту. Спрямований на ускладнення зв'язку між ключем і шифротекстом. Досягається за допомогою нелінійних операцій, насамперед через використання S-блоків (Substitution-boxes);
- дифузія (Diffusion): використовування таких шифруючих перетворень, які ускладнюють відновлення взаємозв'язку статистичних властивостей відкритого та шифрованого текстів. Спрямований на поширення впливу одного біта відкритого тексту (або ключа) на якомога більше бітів шифротексту. Досягається за допомогою лінійних операцій, таких як P-блоки (Permutation-boxes).

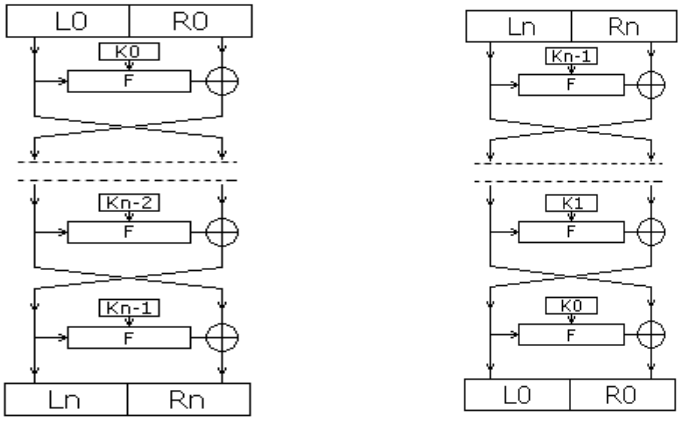
Шеннон запропонував концепцію "product ciphers", в якій послідовно застосовують операції заміни та перестановки, заклавши основи для обох головних структур БСШ. Обидві основні типові структури – Мережа Фейстеля та SPN-мережа – були розроблені в рамках одного дослідного проєкту фірми IBM під назвою Lucifer (1971–1973) [2].

1. Огляд основних типових структур БСШ

1.1. Мережа Фейстеля

Мережа Фейстеля (Feistel Network) (винахідник: Хорст Фейстель (Horst Feistel), IBM) [3, 4]. Вперше застосована у другій версії шифру Lucifer (запатентована в 1971 р.). Проєкт "Люцифер" був скоріше експериментальним, але став базисом для алгоритму Data Encryption Standard (DES). В 1977 р. DES став стандартом в США на шифрування даних і до останнього часу широко використовувався в криптографічних системах. Ітеративна структура алгоритму дозволяла спростити його реалізацію в програмних і апаратних середовищах. В 1987 р. були розроблені алгоритми FEAL і RC2. Широке поширення мережі Фейстеля отримали в 1990-і роки, коли з'явилися такі алгоритми, як Blowfish, CAST-128, TEA, XTEA, XXTEA, RC5, RC6 та ін. Ця конструкція була широко вивчена криптографами в силу її великого поширення.

Мережа Фейстеля, як відомо, має наступну структуру. Вхідний блок ділиться на кілька рівної довжини підблоків, званих гілками. У разі, якщо блок має довжину 64 біта, використовуються дві гілки по 32 біта кожна. Кожна гілка обробляється незалежно від іншої, після чого здійснюється циклічний зсув всіх гілок вліво. Таке перетворення виконується кілька циклів або раундів. У разі двох гілок кожен раунд має структуру, показану на рис. 1.



Шифрування Розшифрування

Рис. 1. Структура мережа Фейстеля

Функція F називається твірною. Кожен раунд складається з обчислення функції F для однієї гілки і побітового виконання операції XOR результату *F* з іншою гілкою. Після цього гілки міняються місцями. Вважається, що оптимальне число раундів – від 8 до 32. Важливим є те, що збільшення кількості раундів значно збільшує криптостойкость алгоритму. Можливо, ця особливість і вплинула на настільки активне поширення мережі Фейстеля, так як для більшої криптостойкості досить просто збільшити кількість раундів, не змінюючи сам алгоритм. Мережа Фейстеля є оборотною навіть у тому випадку, якщо функція *F* не є такою, тому що для розшифрування не потрібно обчислювати F^{-1}. При розшифруванні на вхід подається зашифрований текст, і ключі використовуються в зворотному порядку.

В 1988 р. Майкл Люби (Michael Luby) і Чарльз Ракофф (Charles Rackoff) дослідили криптостійкості мережі Фейстеля і довели, що якщо раундова функція є псевдовипадковою і використовувані ключі незалежні у кожному раунді, то трьох раундів буде достатньо для того, щоб блочний шифр був псевдовипадковою перестановкою, тоді як чотирьох раундів буде достатньо для того, щоб зробити сильну псевдовипадкову перестановку [5].

Псевдовипадковою перестановкою Люби і Ракофф назвали таку, яка стійка до атаки з адаптивним вибором відкритого тексту, а сильною псевдовипадковою перестановкою – псевдовипадкову перестановку стійку до атаки з використанням обраного шифрованого тексту.

Надалі, в 1997 р., Моні Наор (Moni Naor) і Омер Рейнголда (Omer Reingold) запропонували спрощений варіант конструкції Люби – Ракофф з чотирьох раундів, де в якості першого і останнього раунду використовуються дві попарно незалежні перестановки. Два середніх раунди конструкції Наор – Рейнголда ідентичні раундам в конструкції Люби – Ракофф [6].

Більшість же досліджень присвячено вивченню конкретних алгоритмів. У багатьох блокових шифрах на основі мережі Фейстеля були знайдені ті чи інші уразливості, проте в більшості випадків ці уразливості є суто теоретичними.

1.2. Мережа підстановки-перестановки (SPN)

Структура SPN була менш популярною, ніж структура Фейстеля, до 2000-х років, коли вона стала архітектурною основою для AES (Advanced Encryption Standard), демонструючи високу ефективність у програмному забезпеченні [7].

У 2000 р. було завершено міжнародний проєкт по створенню алгоритму шифрування AES (Advanced Стандарт шифрування). В результаті інтенсивної спільної роботи провідних криптологів світу було глибоко проаналізовані та досліджені властивості 15 алгоритмів – кандидатів на стандарт симетричного блочного шифра XXI століття. Після завершення проєкту досліджувався алгоритм Rijndael спеціальними підрозділами Агентства національної безпеки США на відповідність заданому рівню стійкості, можливостей і умов застосування

для захисту несекретної інформації в державних і комерційних структурах США. Таким чином, для заміни алгоритму DES і Triple DES (FIPS-46-3) було прийнято новий алгоритм симетричного блокового шифрування, який офіційно введено в дію в якості федерального стандарту США – AES (FIPS-197). Структуру SPN мережі представлено на рис. 2.

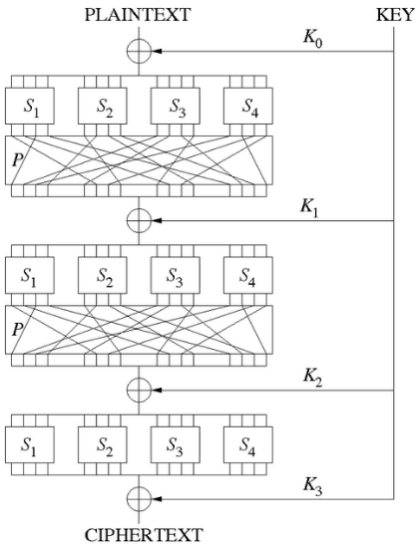


Рис. 2. Схема трираундової SPN мережі, що шифрує 16 біт вхідного тексту в 16 біт вихідного

Крім того, в 2000 р. був розпочатий проєкт NESSIE (Нові європейські схеми для підписів, цілісності та шифрування), метою якого є створення кількох криптографічних примітивів, серед яких є і симетричний блоковий шифр [8]. По суті, до цього часу проєкт уже був обраний законодавчо та було прийнято попереднє рішення про те, що серед блокових алгоритмів найкраще підходять Rijndael, Camellia і Шакал-2. Вони і були рекомендовані в якості стандартів Європейського Союзу [9].

1.3. Конструкція Лея – Мессі

Розроблена Сюецзя Леєм та Джеймсом Л. Мессі (1990) як альтернатива структурі ланцюг Фейстеля. Вона використовує операцію на основі різниці між двома половинами блоку, що забезпечує швидшу дифузію. Найвідоміший приклад – шифр IDEA [10,11]. Схема Лея – Мессі є альтернативною високорівневою конструкцією блокових симетричних шифрів. На її основі побудовано алгоритми FOX, «Мухомор» та ін. Основною перевагою схеми Лея – Мессі, як і ланцюга Фейстеля, є можливість побудови інволютивного перетворення, тобто розшифрування реалізовано практично аналогічно до зашифрування при використанні зворотного порядку раундових з'єднань [12]. Конструкція Лея – Мессі представлена на рис. 3.

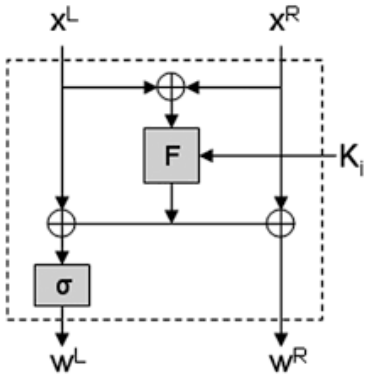


Рис. 3. Конструкція Лея – Мессі

Додатковою перевагою цієї конструкції є відсутність вимог до бієктивності раундової функції (як у SPN-структур), що спрощує розробку та реалізацію. Головна перевага схеми Лея – Мессі над мережею Фейстеля полягає у швидшій дифузії та забезпеченні бієктивності (оборотності) шифру, навіть якщо раундова функція не є інвертованою. Тобто конструкція Лея – Мессі є елегантною альтернативою, що забезпечує високу стійкість при збереженні зручності інволютивного обернення. Важливі характеристики типових конструкцій БСШ представлено у табл. 1.

Таблиця 1

Характеристики типових конструкцій БСШ

Характеристика	Мережа Лея – Мессі (LM)	Мережа Фейстеля (FN)	Мережа SPN
Поділ блоку	Ділиться на дві половини.	Ділиться на дві половини.	Обробляється як ціле.
Вимоги	Не вимагає інвертування (може бути довільною).	Не вимагає інвертування (може бути довільною).	Повинна бути інвертованою (як частина раунду).
Оборотність	Досягається легко завдяки симетричній структурі.	Досягається легко завдяки структурі.	Вимагає окремих обернених операцій у кожному шарі.
Дифузія	Дуже швидка. Змішує обидві частини одночасно.	Повільніша (інформація передається через XOR).	Дуже швидка (завдяки P-блоку).
Кількість раундів (загальна)	Зазвичай менша кількість раундів, ніж FN, для забезпечення безпеки.	Зазвичай більша кількість раундів для досягнення необхідної безпеки.	Кількість раундів середня (залежить від розміру блоку та раундової функції).
Паралелізм (шифрування)	Високий. Операції в раунді можуть виконуватись паралельно.	Низький/Середній. Обчислення лівої частини залежить від правої з попереднього раунду.	Високий. Операції в межах шару (S-блоки) можуть виконуватись паралельно.
Обернення (дешифрування)	Використовує ту саму функцію раунду та ті самі ключі в оберненому порядку.	Використовує ту саму функцію раунду та ті самі ключі в оберненому порядку.	Використовує обернені функції раунду та ключі в оберненому порядку.

1.4. Гібриди та інші конструкції

Криптографи почали активно досліджувати альтернативні структури, щоб подолати обмеження або покращити доказову безпеку класичних моделей. Наприклад узагальнена Мережа Фейстеля (GFN) використовує поділ блоку на більш ніж дві частини. Це дозволяє більш гнучко проєктувати шифри для великих блоків, як, наприклад, CAST-256 та RC6 [13]. Існують також інші архітектури або їх гібриди.

Конструкції ARX (Add-Rotate-XOR) виникли як пряма відповідь на необхідність створення надшвидких симетричних шифрів, які ідеально працюють на сучасних 32- та 64-бітних процесорах (ПК, сервери, мобільні пристрої). Конструкції ARX (Add-Rotate-XOR) особливо ефективні в програмному забезпеченні але їхня безпека повністю залежить від нелінійності модульного додавання. Приклади: ChaCha20 [14], Speck. Шифри Salsa20/ChaCha20 (хоча вони часто класифікуються як потокові шифри, їхня внутрішня функція є блоковою ARX-структурою).

Традиційні S-блоки (особливо великі, як в AES) вимагають доступу до таблиці підстановок, що може призводити до кеш-промахів (cache misses) та вносити затримки (латентність). Крім того, операції з таблицями можуть бути вразливими до атак по сторонніх каналах (timing attacks).

У ARX-конструкціях функцію нелінійного заплутування (Confusion), яку зазвичай виконує S-блок, забезпечує операція модульного додавання, оскільки вона не є лінійною, на відміну від XOR та циклічного зсуву.

Рекурсивна (вкладена) Мережа Фейстепя – це мережа Фейстеля, де сама раундова функція також є невеликою 3-раундовою мережею Фейстеля. Перетворення створює "матрьошку" з криптографічних структур. Типові приклади – шифр MISTY1 [15] та його наступник KASUMI (який використовується в стандартах мобільного зв'язку 3G/GSM) використовують цю вкладену структуру [16]. Рекурсивний дизайн спрощує математичний доказ того, що шифр є стійким до диференціального та лінійного криптоаналізу.

Ці конструкції забезпечують необхідні криптографічні властивості: плутанину (залежність шифротексту від ключа) та дифузію (поширення впливу бітів відкритого тексту по всьому шифротексту) протягом кількох раундів.

Таким чином, сучасна архітектура БСШ є прямим наслідком фундаментальних принципів Шеннона та практичних реалізацій IBM, які започаткували епоху Фейстеля та SPN, що домінує й сьогодні. Однак криптографи постійно досліджують нові архітектури для оптимізації безпеки та продуктивності у різних обчислювальних середовищах.

2. Місце БСШ у постквантовій криптографії

Алгоритм Гровера (Grover's algorithm) [17] є найвідомішою квантовою атакою на симетричні шифри. Він не "ламає" симетричні шифри, як алгоритм Шора, але прискорює атаку повним перебором (brute-force attack). Для симетричного шифру з ключем довжиною L біт, час, необхідний для повного перебору, пропорційний $O(2^L)$. Тобто Алгоритм Гровера може зменшити кількість операцій, необхідних для пошуку ключа, до $0\sqrt{2^L}$ або $0\sqrt{2^{\frac{L}{2}}}$.

Щоб зберегти необхідний "постквантовий" рівень безпеки у 2^{128}(який вважається сьогодні стандартним для довгострокового захисту), просто подвоюють довжину ключа. Саме тому AES-256 є квантово-стійким до атаки Гровера. Його 2^{128} операцій все ще залишаються обчислювально нездійсненними для будь-якого комп'ютера (навіть квантового) у доступному майбутньому [18].

Таким чином, у постквантову еру блокові симетричні шифри залишаються критично важливими і продовжуватимуть використовуватися, вимагаючи лише переходу на довші ключі (128-бітна безпека вимагає 256-бітного ключа) [19].

3. Зміна пріоритетів

Сучасна еволюція БСШ є відповіддю не лише на теоретичні атаки, але й на практичні обмеження апаратного забезпечення. З поширенням Інтернету Речей (IoT) та вбудованих систем, криптографи змістили фокус з пошуку найстійкішого шифру на пошук найефективнішого шифру для обмежених ресурсів. Традиційні шифри (як AES) були оптимізовані для програмної швидкості на потужних процесорах, використовуючи великі S-блоки (8x8 біт в AES) і складні операції (MixColumns). У легкій криптографії пріоритет змінюється.

Один з напрямків – ідея мінімалізму раундової функції. Алгоритми, орієнтовані на апаратну реалізацію, такі як PRESENT (блоковий шифр для RFID-міток), використовують дуже маленькі S-блоки (4x4 біти) та прості перестановки, щоб мінімізувати площу кристала (Gate Count) [20]. Це вимагає значного збільшення кількості раундів для компенсації повільнішої дифузії та слабшого заплутування на раунд.

Також для програмної реалізації на 32- або 64-бітних процесорах, де S-блоки можуть бути неефективними, конструкції ARX (Add-Rotate-XOR) домінують (ChaCha20, Speck) [21].

Вони використовують лише операції, які процесор виконує за один такт, забезпечуючи високу швидкість і мінімальну латентність [22].

Мінімізація Gate Count: замість швидкості, головна мета – зменшити кількість логічних вентилів (Gates) на кристалі, що прямо впливає на вартість виробництва, розмір чипа та енергоспоживання [23].

Використання простих операцій: для досягнення цієї мети шифри, подібні до PRESENT, використовують дуже маленькі S-блоки (4x4 біти): Це значно зменшує апаратні витрати на реалізацію таблиці підстановок, порівняно з 8x8 блоками AES.

Прості глобальні перестановки: складні лінійні шари (як MixColumns в AES) замінюються простими побітовими перестановками.

Компенсація для збереження криптостійкості досягається через значне збільшення кількості раундів. Наприклад, шифр PRESENT має 31 раунд, що значно більше, ніж 10 – 14 раундів AES, але його апаратний розмір залишається мінімальним.

Цей мінімалістичний підхід критично важливий для пристроїв з вкрай обмеженими ресурсами:

- RFID-мітки (ідеальне застосування PRESENT);
- бездротові сенсорні мережі (WSN);
- датчики IoT з живленням від батарейок.

Мінімалізм раундової функції – це архітектурна адаптація БСШ до вимог економічності та енергоефективності, при цьому зберігається необхідний рівень стійкості через ітеративне повторення.

Висновки

Сучасна архітектура блокових симетричних шифрів є прямим наслідком і постійною реалізацією двох фундаментальних принципів, сформульованих Клодом Шенноном у 1949 р.: Заплутування (Confusion) та Дифузії (Diffusion). Історія БСШ – це історія пошуку оптимального балансу між цими двома властивостями для забезпечення криптографічної стійкості. Цей пошук породив дві класичні ітеративні структури, розроблені IBM: мережу Фейстеля (FN) та мережу Підстановки-Перестановки (SPN).

Незважаючи на домінування SPN після конкурсу AES, криптографи активно досліджують альтернативні та гібридні конструкції (Лея – Мессі, GFN, Рекурсивна FN). Це продиктоване не лише теоретичними міркуваннями (доказова безпека, як у MISTY1), але й потребою в оптимізації для різних обчислювальних середовищ.

Симетричні блокові шифри зберігають свою критичну важливість у постквантовій криптографії. Хоча алгоритм Гровера теоретично зменшує ефективну довжину ключа вдвічі, це не призводить до їхньої повної компрометації.

Таким чином, сучасна архітектура БСШ є динамічною галуззю, що ефективно адаптується до квантових загроз та вимог мінімалізму апаратного забезпечення.

Список літератури:

1. Shannon C. E. A communication theory of secrecy systems // Bell System Technical Journal. 1949. Vol. 28, № 4. P. 656–715.
2. Feistel H. Cryptography and computer privacy // Scientific American. 1973. Vol. 228, № 5. P. 15–23.
3. Stallings W. Cryptography and Network Security: Principles and Practice (8th ed.). Pearson, 2023.
4. ISO/IEC 18033-3:2010. Information technology – Security techniques – Encryption algorithms. Part 3: Block ciphers. International Organization for Standardization, 2010.
5. Luby M., & Rackoff C. Pseudorandomness and Cryptographic Applications // Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing. ACM, 1988. P. 348–355.
6. Naor M., & Reingold O. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited // Journal of Cryptology. 1999. Vol. 12, № 1. P. 29–66.
7. NIST (National Institute of Standards and Technology). FIPS PUB 197: Advanced Encryption Standard (AES). Washington, D.C. : U.S. Department of Commerce, 2001.
8. Schneier B., & Whiting D. A performance comparison of the AES submissions // AES Conference Proceedings. NIST, 1999.

9. NESSIE Consortium. NESSIE Project Final Report. [Електронний ресурс]. 2003. URL: [Вставити офіційне посилання на звіт NESSIE].
10. Lai X., & Massey J. L. A Proposal for a New Block Encryption Standard. Advances in Cryptology–EUROCRYPT ’90. Springer, Berlin, Heidelberg, 1991. P. 389–404.
11. Preneel B. The International Data Encryption Algorithm (IDEA) // The Handbook of Security. Auerbach Publications, 2003.
12. Menezes A. J., van Oorschot P. C., & Vanstone S. A. Handbook of Applied Cryptography. Boca Raton : CRC Press, 1997. P. 250–252.
13. Schneier B., Mook D., & Mook J. The CAST-256 algorithm. Software for Data Security, 1999.
14. Bernstein D. J. ChaCha, a variant of Salsa20. Advances in Cryptology – SAC 2008. Springer, 2008. P. 138–170.
15. Matsui M. New block encryption algorithm MISTY. Fast Software Encryption – FSE ’97. Springer, 1997. P. 54–68.
16. 3GPP TS 35.202. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: KASUMI specification. 2004.
17. Grover L. K. A fast quantum mechanical algorithm for database search // Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996. P. 212–219.
18. NIST SP 800-57 Part 1 Rev. 5. Recommendation for Key Management: Part 1 – General. NIST, 2020.
19. Bernstein D. J., & Lange T. Post-quantum cryptography // Nature. 2017. Vol. 549, № 7671. P. 188–194.
20. Andres C., Biryukov A., D'Haeseleer J., Indesteege S., & Leurent G. PRESENT: An Ultra-Lightweight Block Cipher. CHES 2007. Springer, 2007. P. 450–464.
21. Bernstein D. J. ChaCha, a variant of Salsa20. Advances in Cryptology – SAC 2008. Springer, 2008. P. 138–170.
22. Eisenbarth T., Gong L., & Kniffler A. A Survey of Lightweight Cryptography Implementations on FPGAs // IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021.
23. Beaulieu S., Shors J., Smith J., Treatman-Clark S., Weeks B., & Wingers L. The SIMON and SPECK lightweight block ciphers // 4th Workshop on RFID Security, 2013.

Надійшла до редколегії 10.10.2025

Відомості про авторів:

Лисицький Костянтин Євгенійович – PhD, Харківський національнійо університет імені В. Н. Каразіна, доцент кафедри математичного моделювання і аналізу даних; навчально-науковий інститут комп’ютерних наук та штучного інтелекту; Національний аерокосмічний університет "Харківський авіаційний інститут", ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки; Україна; e-mail: constantin.lisickiy@gmail.com; ORCID: https://orcid.org/0000-0002-7772-3376

Лисицька Ірина Вікторівна – д.т.н., професор, Харківський національний університет імені В. Н. Каразіна, професор кафедри кібербезпеки інформаційних систем, мереж і технологій, навчально-науковий інститут комп’ютерних наук та штучного інтелекту; Харківський національний університет радіоелектроніки, професор кафедри безпеки інформаційних технологій; Україна; e-mail: ivlisitska@karazin.ua; ORCID: https://orcid.org/0000-0001-6758-9516

Гальцева Ірина Михайлівна – старший викладач кафедри кібербезпеки інформаційних систем, мереж і технологій; Харківський національний університет імені В. Н. Каразіна; навчально-науковий інститут комп’ютерних наук та штучного інтелекту; Україна; e-mail: irina.galceva@karazin.ua

Колованова Євгенія Павлівна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри кібербезпеки інформаційних систем, мереж і технологій; навчально-науковий інститут комп’ютерних наук та штучного інтелекту; Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій; Україна; e-mail: e.kolovanova@gmail.com; ORCID: https://orcid.org/0000-0002-0326-2394