ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції
2

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)

За загальною редакцією ***С. В. Ківалова***

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск ***М. Р. Аракелян***

ISBN 978-617-8430-61-0

© НУ «Одеська юридична академія, 2025
© Автори статей, 2025

СЕКЦІЯ 22. ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТРІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

СЕКЦІЯ 23. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Список використаних джерел:

1. Храпкін О., Кіндрат О., Чопей Р. Управління проєктами в іт-галузі: методики, інструменти та керування ризиками. *Економіка та суспільство*. 2023. № 55. URL: https://doi.org/10.32782/2524-0072/2023-55-110

2. Scrum&Agile: що це таке та кому може знадобитися? URL: https://budni.robota.ua/career/scrum-agile (дата звернення: 02.04.2025).

3. Нефьодов Л. І., Філь Н. Ю. Модель вибору Scrum-майстра із застосуванням нечітких множин. *Вісник Харківського національного автомобільно-дорожнього університету*. 2022. Вип. 97. С. 16–23.

4. Pabin M. How the Finance Industry is Shaped by Technology – A Corporate Experience. *Finance Undergraduate Honors Theses*. 2023. URL: https://scholarworks.uark.edu/finnuht/9 (дата зверення: 05.04.2025).

5. Величко С. В. Засоби та механізми протидії ddos-атакам. *Інформаційне суспільство: проблеми та перспективи :* матеріали VII Всеукраїнської науково-практичної конференції (м. Одеса, 20 травня 2022 р.) / відп. ред. Н. І. Логінова. Одеса, 2022. С. 97-99.

Ключові слов: scrum, кібербезпека, регуляторні вимоги, захист даних, аналіз вразливостей.
Keywords: scrum, cybersecurity, regulatory requirements, data protection, vulnerability analysis.

Соколов Артем Вікторович
Національний університет «Одеська юридична академія»,
професор кафедри кібербезпеки, доктор технічних наук, професор
Радуш Володимир Вячеславович
Національний університет «Одеська політехніка»,
аспірант кафедри кібербезпеки та програмного забезпечення

МЕТОД НЕДВІЙКОВОГО АФІННОГО ПЕРЕТВОРЕННЯ ДЛЯ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ ЯКОСТІ S-БЛОКІВ

Одним із ключових елементів симетричних криптографічних алгоритмів є S-блоки, від криптографічної якості яких значною мірою залежить стійкість усієї системи до відомих атак, зокрема диференціального та лінійного криптоаналізу. Основними критеріями криптографічної якості S-блоків виступають:

1. Нелінійність;
2. Строгий лавинний критерій (Strict Avalanche Criterion, SAC);
3. Критерій бітової незалежності (Bit Independence Criterion, BIC);
4. Імовірність лінійної апроксимації (Linear Approximation Probability, LAP);
5. Імовірність диференціальної апроксимації (Differential Approximation Probability, DAP);
6. Кореляційна незалежність вихідних та вхідних векторів S-блоку.

Зазначені характеристики можуть розглядатися як для компонентних булевих функцій, так і для компонентних функцій багатозначної логіки.

Важливу роль у побудові S-блоків відіграють афінні перетворення, які використовуються для підвищення їхніх криптографічних властивостей. Класичним прикладом є конструкція Ніберг, яка дозволяє отримати S-блоки зі збалансованою відповідністю основним критеріям криптографічної якості. Конструкція Ніберг являє собою композицію нелінійного степеневого перетворення з афінним перетворенням. Ця конструкція застосовуються, зокрема, у криптографічному алгоритмі AES.

Незважаючи на високу криптографічну якість S-блоків конструкції Ніберг, вони, втім, не задовольняють повністю SAC ані в сенсі булевих функцій, ані в сенсі функцій багатозначної логіки.

Задача побудови S-блоків, які б володіли ідеальними лавинними властивостями є складною, однак на сьогодні відомий метод синтезу нелінійних перетворень, що володіють ідеальною відповідністю SAC як в сенсі компонентних булевих функцій, так в сенсі компонентних булевих і 4-функцій [1].

Незважаючи на ідеальні лавинні характеристики, ці S-блоки володіють невеликими значеннями відстані нелінійності, що гальмує їх застосування на практиці.

У цій роботі запропоновано метод недвійкового афінного перетворення, який дозволяє підвищити нелінійність S-блоків, що задовольняють SAC як в сенсі булевих функцій, так і в сенсі 4-функцій.

Метою роботи є підвищення криптографічної якості S-блоків із застосуванням недвійкових афінних перетворень.

Запропонований підхід відкриває нові можливості для побудови ефективних криптографічних перетворень як при представленні булевими функціями, так і функціями багатозначної логіки.

Запропоновано модифіковану схему афінного перетворення над полем Галуа GF(4). Як продемонструвало наше дослідження, ця схема в поєднанні з S-блоками [1], які задовольняють SAC як для компонентних булевих функцій, так і для 4-функцій, дозволяє створювати S-блоки, які демонструють високу криптографічну якість. Розроблена конструкція поєднує в собі як спеціальні четвіркові матриці афінного перетворення, так і арифметичні операції над полем $GF(4)$, а також по mod4, що дозволяє ефективно впливати на нелінійність результуючих S-блоків. Відповідно до запропонованого нами методу афінне перетворення S-блоків виконується наступним чином

$$\alpha_j.S_i = \sum_{u=1}^{n} \alpha_j \times y_i R'(j,u) + C \bmod 4, \qquad (1)$$

де позначення $\alpha_j.S_i$ означає взяття j-го четвіркового розряду i-го елементу S-блока, тоді як позначення $R'(j,k)$ означає вилучення елемента з індексами (j,k) з матриці R', а знак × позначає множення в полі Галуа $GF(4)$, y_i – елемент вихідного S-блока. В якості матриць R' використовуються модифіковані конструкції

$$C_{4,21}=\begin{pmatrix} x & 0 & 0 & x_1 \\ 0 & 0 & x & x_1 \\ 0 & x & 0 & x_1 \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,22}=\begin{pmatrix} 0 & 0 & 0 & x_1 \\ x & 0 & x & x_1 \\ 0 & x & 0 & x_1 \\ 0 & 0 & 0 & 0 \end{pmatrix};$$
$$C_{4,23}=\begin{pmatrix} 0 & 0 & 0 & x_1 \\ 0 & 0 & x & x_1 \\ x & x & 0 & x_1 \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,24}=\begin{pmatrix} 0 & 0 & 0 & x_1 \\ 0 & 0 & x & x_1 \\ 0 & x & 0 & x_1 \\ x & 0 & 0 & 0 \end{pmatrix};$$
$$C_{4,31}=\begin{pmatrix} x & x_1 & 0 & 0 \\ 0 & x_1 & x & 0 \\ 0 & x_1 & 0 & x \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,32}=\begin{pmatrix} 0 & x_1 & 0 & 0 \\ x & x_1 & x & 0 \\ 0 & x_1 & 0 & x \\ 0 & 0 & 0 & 0 \end{pmatrix};$$
$$C_{4,33}=\begin{pmatrix} 0 & x_1 & 0 & 0 \\ 0 & x_1 & x & 0 \\ x & x_1 & 0 & x \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,34}=\begin{pmatrix} 0 & x_1 & 0 & 0 \\ 0 & x_1 & x & 0 \\ 0 & x_1 & 0 & x \\ x & 0 & 0 & 0 \end{pmatrix}; \quad (2)$$
$$C_{4,41}=\begin{pmatrix} x & 0 & x_1 & 0 \\ 0 & 0 & x_1 & x \\ 0 & x & x_1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,42}=\begin{pmatrix} 0 & 0 & x_1 & 0 \\ x & 0 & x_1 & x \\ 0 & x & x_1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix};$$
$$C_{4,43}=\begin{pmatrix} 0 & 0 & x_1 & 0 \\ 0 & 0 & x_1 & x \\ x & x & x_1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; C_{4,44}=\begin{pmatrix} 0 & 0 & x_1 & 0 \\ 0 & 0 & x_1 & x \\ 0 & x & x_1 & 0 \\ x & 0 & 0 & 0 \end{pmatrix}.$$

Дослідження, проведені в даній роботі, дозволили встановити, що найкращі результати за якістю показують матриці, побудовані на основі (2), які не містять у своєму складі значення 1. Розглянемо конкретну матрицю

$$R'=\begin{pmatrix} 2 & 0 & 3 & 0 \\ 0 & 0 & 3 & 2 \\ 0 & 2 & 3 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (3)$$

на основі якої із застосуванням (1) стає можливим побудувати новий S-блок, який відповідає SAC компонентних булевих і 4-функцій. Криптографічні характеристики побудованого S-блока показані в табл. 1.

У роботі запропоновано новий метод недвійкового афінного перетворення, який дозволяє підвищити рівень нелінійності криптографічних S-блоків. S-блоки [1] побудовані таким чином, щоб максимально відповідати SAC та низькій кореляції між вихідними та вхідними векторами, та мають мале значення нелінійності, яке дорівнює 80. За допомогою запропонованих у цій роботі матриць афінних перетворень над GF(4) вдалося збільшити нелінійність цих S-блоків до значення 96, зберігаючи їхню відповідність SAC компонентних булевих та 4-функцій функцій.

Таблиця 1. Криптографічні характеристики запропонованого S-блока у порівнянні з іншими конструкціями

S-box	Нелінійність	SAC	BIC нелінійність	BIC SAC	LAP	DAP	$\max\{\lvert r_{ij}\rvert\}$	SAC 4-функцій
S-блок [1]	80	0.5	83.4286	0.4967	0.5	1	0	0.5
Запропон. S-блок	96	0.5	77.7143	0.4799	0.5	1	0	0.5
S-блок [2]	111.75	0.5029	103.7143	0.5006	0.125	0.0391	0.1250	0.6094
S-блок [3]	107	0.5781	102.93	0.4991	0.1719	0.0469	0.1562	0.6406

Список використаних джерел:

1. Sokolov A. V., Radush V. V. The method for synthesis of high-quality S-boxes based on many-valued logic functions. *Informatics and mathematical methods in simulation*. 2022. Vol. 12. No. 3. P. 219-225.
2. Aydın Y., Özkaynak F. Automated Chaos-Driven S-Box Generation and Analysis Tool for Enhanced Cryptographic Resilience. *IEEE Access*. 2024. Vol. 12. P. 312-328.
3. Artuğer F., Özkaynak F. A new chaotic system and its practical applications in substitution box and random number generator. *Multimedia Tools and Applications*. 2024. 83(42). P. 90053-90067.

Ключові слова: криптографія, S-блок, афінне перетворення.
Keywords: cryptography, S-box, affine transformation.

Ахмаметьєва Ганна Валеріївна
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук, доцент
Овчинников Микола Юрійович
Національний університет «Одеська юридична академія»,
асистент кафедри кібербезпеки

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ШИРОКОСМУГОВОГО ТА ФАЗОВОГО КОДУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В АУДІОСИГНАЛІ

У сучасних умовах активного використання цифрових технологій та стрімкого розвитку штучного інтелекту зростає потреба у захисті авторських прав і цифрових даних. Одним із найефективніших інструментів у цьому контексті