***БАКУНІНА ОЛЕНА ВАЛЕРІЇВНА***

*Національний університет «Одеська юридична академія»,*
*доцент кафедри кібербезпеки,*
*кандидат фізико-математичних наук, доцент*

# КОРЕЛЯЦІЙНИЙ ІМУНІТЕТ 4-ФУНКЦІЙ, ЩО СИНТЕЗОВАНІ НА ОСНОВІ КОРЕЛЯЦІЙНО-ІМУННИХ БУЛЕВИХ ФУНКЦІЙ

Розвиток сучасних методів криптографії багато в чому пов'язаний із використанням функцій багатозначної логіки (ФБЛ), які, разом з булевими функціями, дозволяють визначити рівень реалізації концепцій дифузії та конфузії сучасних криптографічних алгоритмів [1].

В даний час відомі набори критеріїв криптографічної якості як булевих функцій [2], так і функцій багатозначної логіки [3], серед яких найважливішими є критерії нелінійності (алгебраїчна та дистанційна нелінійність), критерії лавинного ефекту (критерій поширення помилки, суворий лавинний критерій, критерій максимального лавинного ефекту) та кореляційні критерії (критерій незалежності виходу від вхідних змінних, критерій кореляційного імунітету). Проте питання взаємозв'язку між критеріями криптографічної якості ФБЛ та їх компонентних булевих функцій залишаються недослідженими. Зокрема, у відкритих джерелах не представлена інформація про кореляційний імунітет 4-функцій, які синтезовані з кореляційно-імунних булевих функцій, незважаючи на те, що подібна операція була застосована в роботі [4] для синтезу S-блоків, кореляційно імунних як в сенсі компонентних булевих функцій, так і в сенсі компонентних 4-функцій.

*Метою* цієї роботи є встановлення взаємозв'язку між кореляційними імунних булевих функцій.

Введемо необхідні нам визначення кореляційного імунітету спочатку для булевих функцій.

**Визначення 1 [2].** Булева функція $f(x)$, $x \in V_k$, називається кореляційно-імунною порядку $m$, $1 \le m \le k$, якщо вихід $y = f(x_1^k)$ і будь-яка множина з $m$ її вхідних змінних є статистично незалежними.

**Визначення 2 [2].** Підфункцією булевої функції $f(x)$, $x \in V_k$ називається функція $f'$, що отримана підстановкою в функцію $f$ констант "0" або "1" замість частини змінних. Якщо підставимо в функцію $f$ константи $\sigma_{i_1}, \dots, \sigma_{i_s}$ замість змінних $x_{i_1}, \dots, x_{i_s}$, відповідно, то отримана підфункція позначається $f^{\sigma_{i_1},\cdots,\sigma_{i_s}}_{x_{i_1},\cdots,x_{i_s}}$. Якщо замість змінної $x_i$ константа не підставлена, то $x_i$ називається вільною змінною.

Наприклад, нехай задана булева функція $f'(x_1, x_2, x_2)$, тоді її підфункціями є $f'(x_1, x_2, 0)$, $f'(x_1, x_2, 1)$, $f'(x_1, 0,0)$, $f'(x_1, 0,1)$ і т.д.

**Визначення 3 [2].** Булева функція $f(x)$, $x \in V_k$, називається кореляційно-імунною порядку $m$, $1 \le m \le k$, якщо вага Гемінга дорівнює $wt(f') = wt(f)/2^m$, для будь-якої її підфункції $f'$ від $k - m$ змінних.

У роботі [3] також були введені визначення кореляційного імунітету ФБЛ, основні з яких наведемо далі.

Для заданої послідовності $f$ ми можемо ввести вектор $K = \{K_0, K_1, \dots, K_{q-1}\}$, де $K_u$ – кількість входжень символу $u \in \{0,1, \dots, q-1\}$ в послідовність $f$.

**Визначення 4 [3].** Розбалансом послідовності $f$ назвемо значення модуля суми поелементних добутків елементів вектора $K$ на відповідні елементи експоненціального алфавіту $\{z_0, z_1, \dots, z_{q-1}\}$,

$$\Delta(f) = \left| K_0 z_0 + K_1 z_1 + \dots + K_{q-1} z_{q-1} \right|. \quad (1)$$

На основі **Визначення 4** розбаланса ФБЛ вводиться визначення незалежності виходу 4-функцій від її вхідних змінних, а також визначення кореляційного імунітету 4-функцій.

**Визначення 5 [3].** Підфункцією $q$-функції $f(x)$ називається функція $f'$, отримана підстановкою у функцію $f$ значень з множини $\{0,1,\dots,q-1\}$ замість деяких змінних. Якщо підставити у функцію $f$ константи $\sigma_{i_1}, \dots, \sigma_{i_s}$ замість змінних $x_{i_1}, \dots, x_{i_s}$, відповідно, то отримана підфункція позначається $f^{\sigma_{i_1},\cdots,\sigma_{i_s}}_{x_{i_1},\cdots,x_{i_s}}$.

**Визначення 6 [3].** Кажуть, що вихід 4-функції $f(x)$ є незалежним від групи своїх вхідних змінних $\{x_i\}$, $i = 1,\dots,m$ якщо при підстановці замість цих змінних будь-яких констант $\sigma_{i_1}, \dots, \sigma_{i_s} \in \{0,1,2,3\}$, розбаланс отриманих таким чином підфункцій становить $\Delta_{f'} = \frac{\Delta_f}{4^m}$.

**Визначення 7 [3].** Кажуть, що 4-функція $f(x)$ є кореляційно імунною порядку $m \le k$, якщо її вихід є незалежним щодо будь-якої групи з $m$ своїх вхідних змінних, тобто розбаланс її підфункцій $k - m$ змінних становить $\Delta_{f'} = \frac{\Delta_f}{4^m}$.

Для вирішення поставленого завдання було розроблено наступний алгоритм:

*Крок 1.* Пошук множини кореляційно імунних булевих функцій довжини $N = 16$, кількість яких склала $J_2 = 222$, що збігається з результатом, отриманим у роботі [5].

*Крок 2.* Знаходження суперпозиції кожної можливої пари (враховуючи перестановки), отриманих на *Кроці 1* булевих функцій, як це показано у прикладі

$$\begin{array}{rcccccccccccccccc} & & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \\ f_{20} = & \{ & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & \} \\ f_{21} = & \{ & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & \} \\ f_4 = & \{ & 0 & 0 & 0 & 2 & 1 & 3 & 3 & 3 & 3 & 3 & 3 & 1 & 2 & 0 & 0 & 0 & \}. \end{array} \quad (2)$$

На даному етапі ми отримуємо $J_4 = 222^2 = 49\ 284$ 4-функції.

*Крок 3.* Дослідження кореляційних властивостей отриманих на *Кроці 2* 4-функцій відповідно до умов **Визначення 6** та **Визначення 7**.

Виконуючи дослідження відповідно до представленого алгоритму ми отримали результати, які для зручності представимо в табл. 1.

Таблиця 1 – Результати дослідження множини 4-функцій, отриманої на основі суперпозиції кореляційно-імунних булевих функцій

| **Кореляційні властивості** | **Потужність множини** | **% від усіх отриманих 4-функцій** |
|---|---|---|
| 4-функції, вихід яких не залежить від змінної $x_1$ | 6 308 | 12.8 % |
| 4-функції, вихід яких не залежить від змінної $x_2$ | 6 308 | 12.8 % |
| Кореляційно-імунні 4-функції | 1 028 | 2.09 % |
| 4-функції загального виду | 35 640 | 72.31 % |
| Всього | 49 284 | 100 % |

Результати аналізу даних, представлених у табл. 1 приводять до висновку, що отримання кореляційно-імунної 4-функції на основі двох кореляційно-імунних булевих функцій відбувається тільки в 2.09 % випадків, що свідчить про істотні відмінності в природі кореляційного імунітету булевих функцій і ФБЛ і підтверджує необхідність дослідження сучасних криптографічних алгоритмів при їх поданні як за допомогою математичного апарату булевих функцій, так і за допомогою математичного апарату ФБЛ.

Відзначимо основні результати проведених досліджень:

1. Розроблено алгоритм вивчення кореляційних властивостей 4-функцій, синтезованих на основі кореляційно-імунних булевих функцій.

2. Визначено кількості 4-функцій, вихід яких не залежить від змінних $x_1$ або $x_2$, а також кореляційно-імунних 4-функцій, які можуть бути синтезовані на основі кореляційно-імунних булевих функцій.

3. Отримані результати характеризують рівень взаємозв'язку між кореляційним імунітетом булевих функцій і ФБЛ, які побудовані на їх основі, що є важливим для визначення кореляційних властивостей сучасних криптоалгоритмів.

### *Список використаних джерел:*


1. Shannon C. E. A Mathematical Theory of Cryptography. USA : Bell System Technical Memo, 1945, MM 45-110-02.
2. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. М. : МЦНМО, 2004. 472 с.

3. Соколов А. В., Жданов О. Н. Криптографические конструкции на основе функций многозначной логики. Монография. М. : Научная мысль, 2020. 192 с.
4. Бакунина Е. В. О существовании класса s-блоков, удовлетворяющих корреляционному иммунитету компонентных булевых функций и 4-функций. Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру: у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 21 трав. 2021 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2021. Т. 1. С. 603–606.
5. Яковлєв С. В. Збалансовані критерії якості довгострокових ключових елементів алгоритму ГОСТ 28147-89. Київ: Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія». 2009. С. 5–12.

**Ключові слова:** криптографія, кореляційний імунітет, булева функція, функція багатозначної логіки.
**Key words:** cryptography, correlation immunity, Boolean function, many-valued logic function.

***БОЙКО ВІКТОР ДМИТРОВИЧ***

*Національний університет «Одеська юридична академія», доцент кафедри кібербезпеки, кандидат технічних наук*

## ОЦІНКА ЖИВУЧОСТІ ТА СТІЙКОСТІ КОМПОНЕНТІВ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ КОГНІТИВНО-ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

Питання стійкості та живучості інформаційних систем в даний час набуває все більшої актуальності. Більшість існуючих інформаційних систем після введення в експлуатацію піддається різноманітним атакам, та з великою ймовірністю можуть бути зламані, або виведені з ладу. При цьому, якщо злому піддаються інформаційні системи, що обслуговують індустріальні та промислові комплекси (industrial control system – ICS) ризики та масштаби збитків багаторазово збільшуються.

В аналітичному звіті компанії Dragos [1] вказується, що експлойти для ICS систем існують (і активно використовуються) вже більше десяти років, при цьому загальнодоступні експлойти потрапляють до баз даних (наприклад бази даних уразливостей CVE (cve.mitre.org) ) протягом приблизно місяца. В цілому, експерти з інформаційної безпеки вказують, що на злом ICS в даний час з'явився попит і в найближчому майбутньому очікується значне збільшення пропозиції ([2]). Найбільш відомими прикладами атак в Україні можуть бути епідемії WannaCry, Petya збої української енергосистеми у 2015 році.

Типово, що розробники промислових та інфраструктурних інформаційних систем, на відміну розробників ПО «загального призначен-